УДК: 343.2:343.4 (477)

Таволжанський Олексій Володимирович –
кандидат юридичних наук,
асистент кафедри кримінології та кримінально-виконавчого права
Національного юридичного університету імені Ярослава Мудрого

Oleksii V. Tavolzhanskyi –
candidate of juridical sciences,
teaching assistant at criminology and penal law department,
Yaroslav Mudryi National Law University
(77, Pushkinskaya str., Kharkiv, Ukraine)

Кримінологічні аспекти кіберзлочинності у сучасних умовах

У статті визначено кримінологічні ознаки кіберзлочинності, окреслено законодавче підґрунтя боротьби з кіберзлочинністю в Україні та світі. Наведено деякі проблеми нормативного врегулювання кіберзлочинності. Визначено механізм їх вирішення. Проаналізовано актуальні питання у сфері запобігання кіберзлочинності, які потребують вирішення.

Ключові слова: *кіберзлочинність, комп'ютерна злочинність, боротьба з кіберзлочинністю, Інтернет, протокол Transmission Control Protocol / Internet Protocol (TCP/IP), інформаційна безпека, кіберсфера.*

В статье определены криминологические признаки киберпреступности, очерчена законодательная основа борьбы с киберпреступностью в Украине и мире. Приведены некоторые проблемы нормативного урегулирования киберпреступности. Определен механизм их решения. Проанализированы актуальные вопросы в сфере предотвращения киберпреступности, которые требуют решения.

Ключевые слова: *кибепреступность, компьютерная преступность, борьба с киберпреступностью, интернет, протокол Transmission Control Protocol / Internet Protocol (TCP/IP), информационная безопасность, киберсфера.*

O.V. Tavolzhanskyi Criminological Aspects of Cyber Crime in Modern Conditions

The analysis is complicated by the fact that this type of crime associated with the use of technical means, special skills and knowledge. The use of telecommunication devices connected via the protocol TCP / IP (literal meaning: Transmission Control Protocol / Internet Protocol, or in translation, transmission control protocol / intranet protocol), which allows to combine different network (hereinafter, including - Internet) is an integral part of life.

The article presents a range of subjects, which according to current legislation deal with cybercrime prevention, particularly the Ministry of Defense of Ukraine, Security Service of Ukraine, the National Police of Ukraine, the National Bank of Ukraine, intelligence agencies and the State Service for Special Communications and Information Protection Ukraine.

We have analyzed the structure of cybercrime in the context of plurality. The author emphasized that cybersecurity of Ukraine should be a priority issue that requires urgent intervention by building legal system including through appropriate legal settlement law.

Keywords: *cybercrime, computer crime, the fight against cybercrime, Internet Protocol Transmission Control Protocol / Internet Protocol (TCP/IP), information security, cyber sphere.*

Постановка проблеми. Реалії сьогодення все частіше підштовхують людство до процесів глобалізації. Використання телекомунікаційних пристрої поєднаних за допомогою протоколу TCP/IP (дослівне значення: Transmission Control Protocol/ Internet Protocol, або в перекладі: протокол управління передаванням / внутрішньомережевий протокол), який дозволяє

об'єднувати різні мережі (далі, у тому числі – Інтернет) стає невід'ємною частиною життя. Вимкнення Інтернету на добу є такою ж, а може і більшою, проблемою для людини, як відключення електроживлення, чи водопостачання.

Існування так званих гаджетів у життєдіяльності людини розширює можливості, надає багато додаткових механізмів і способів її реалізації, зокрема уникнути від зайвого багажу витрат, пришвидшує процес обміну інформації, і як наслідок є невід'ємним інструментом отримання надприбутків. Але такі додаткові можливості не завжди використовуються в законних цілях. Інноваційний розвиток поєднаний з побічним негативним явищем злочинного спрямування – злочинами пов'язані з використанням електронно-обчислювальної техніки, систем та комп'ютерних мереж приєднаних до глобальної мережі або використання електронно-обчислюваних машин при вчиненні злочину.

Такий стан речей дозволяє впевнено стверджувати в необхідності поєднання зусиль провідних науковців і практиків до врегулювання правовідносин, що бурхливо виникають, та удосконалення діючого законодавства в кіберсфері, задля зменшення ризику для правослухняних громадян потрапити в пастку кіберзлочинців.

Аналіз останніх досліджень та публікацій. Серед провідних фахівців, що займались питаннями вдосконалення законодавства, як при обробці, зберіганні чи використанні інформації, так і в сфері боротьби із проявами кіберзлочинності можна виділити Д.С. Азарова, В.М. Бутузова, К.К. Горяинов, А.П. Гаджиєв, А.Л. Осипенко, В.О. Голубєва, М.В. Гуцалюка, В.П. Захарова, М.С. Исеченко, М.В. Карчевського, С.А. Кузьміна, М.Ю. Літвінова, О.В. Манжая, О.В. Орлова, О.В. Потій, Ю.В. Степанова та ін.

Невирішені проблеми. Не дивлячись на те, що проблема кіберзлочинності знаходиться у «полі зору» вчених, її окремі питання потребують більш ґрунтовного опрацювання. Тому **метою цієї статті** є окреслення основних кримінологічних ознак кіберзлочинності та її структури, надання кримінологічної оцінки сучасному нормативному врегулюванню забезпечення кібербезпеки.

Виклад основного матеріалу. Національну правову базу щодо врегулювання кібеправовідносин складають: Конституція України, яка гарантує захист інформації, Кримінальний кодекс України, Конвенція Ради Європи «Про кіберзлочинність», Закони України «Про телекомунікації», «Про Національну поліцію», «Про основи національний безпеки України», «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», укази Президента України, інші нормативно-правові акти.

Злочинність – це історично обумовлене і мінливе соціальне явище, яке проявляє себе у виді множинності злочинів, має територіально-часовий та кількісно-якісний вимір [1, 56]. Характерними ознаками наділена і кіберзлочинність.

Кіберзлочинність (або ще по іншому називають злочинність в сфері інноваційних технологій, комп'ютерні злочини тощо) є *історично обумовленим і мінливим явищем*. Цей вид злочинності поряд з такими поняттями як економічна злочинність, організована злочинність, корупція, легалізація злочинних доходів хоча і з'явилось нещодавно, але міцно увійшло у понятійний апарат кримінологів і практичних працівників. Не так давно злочинам в кіберсфері на національному рівні приділялась незначна увага, вважалось, що кіберзлочинність може представляти реальну загрозу лише в далекому майбутньому, тепер майже ні в кого не виникає сумнівів, що частка кіберзлочинності в структурі злочинності України значно збільшилася.

Характеристика злочинність як *соціального* явища передбачає актуальність питання для всього суспільство і відповідно потребує наявності стратегії держави в усіх сферах запобігання злочинності. Не є виключенням і кіберсфера. Безумовно необхідно погодитись з думкою Головкіна Б.М., який зазначає, що у масштабі суспільства між кількістю контингенту злочинців і кількістю контингенту жертв злочинів, існує певний паритет зумовлений рівновагою кримінальної і віктимної форм поведінки, їх взаємною трансформацією, зв'язком станів між рівнями та злочинності [2, 94]. Контингент жертв кіберзлочинів сягає величезних масштабів.

Безумовно необхідним і своєчасним є підписаний Президентом України Указ, яким приведено в дію рішення РНБО України від 27.01.2016 "Про Стратегію кібербезпеки України" (далі, у тому числі — Стратегія). Метою створення вказаного документу є "створення умов для безпечного функціювання кіберпростору, його використання в інтересах особи, суспільства і держави" (там само).

Цим же документом визначено коло суб'єктів, що займаються забезпеченням кібербезпеки: Міноборони України, СБУ, Національна поліція України, НБУ, розвідувальні органи і чомусь також віднесено Державну службу спеціального зв'язку та захисту інформації України. Стратегією визначено, що це не поодинокі суб'єкти, а система органів. Хоча система передбачає наявність чіткої ієрархії і підпорядкованості, а вище наведені суб'єкти хоча і відносяться до однієї гілки влади, все ж таки залишаються окремими відомчими одиницями.

Стратегією встановлюється комплекс заходів, пріоритетів та напрямів забезпечення кібербезпеки України, зокрема, створення і оперативну адаптацію державної політики, спрямованої на розвиток кіберпростору та досягнення сумісності з відповідними стандартами ЄС та НАТО; формування конкурентного середовища у сфері електронних комунікацій, надання послуг із захисту інформації та кіберзахисту; залучення експертного потенціалу наукових установ, професійних та громадських об'єднань до підготовки проектів концептуальних документів у цій сфері; підвищення цифрової грамотності громадян та культури безпекового поводження в кіберпросторі; розвиток міжнародного співробітництва та підтримку міжнародних ініціатив у сфері кібербезпеки, в тому числі поглиблення співпраці України з ЄС та НАТО [3].

Множинність як ознака злочинності також притаманна кіберзлочинності. Майже кожен корисливий злочин, передбачений діючим Кримінальним Кодексом України (далі, у тому числі – КК) може бути вчинений з використанням сервісів Інтернету. Суспільство все частіше страждає, зокрема, від розповсюдження порнографічних матеріалів, продажу наркотичних засобів, вогнепальної та холодної зброї, шахрайства, шантажу, корупції через Інтернет. Деякі протиправні дії здійснюються на інноваційному, навіть високотехнологічному рівні, і можуть бути кваліфіковані правоохоронними органами лише умовно. Нормативне регулювання не завжди встигає за новітніми технологіями.

У 2001 р. комітетом міністрів Ради Європи була затверджена Конвенції про кіберзлочинність . Україною вказана Конвенція була ратифікована у 2005 році (далі, у тому числі – Конвенція) [4]. Аналізуючи положення вищеназваного міжнародного акту можна дійти висновку, що українське законодавство в кіберсфері не повністю відповідає світовим нормативам, тим більше сучасним умовам, про окремі з таких невідповідностей буде йти нижче.

Існують різні підходи до розуміння структури кіберзлочинності. Конвенцією, зокрема, перелічуються такі групи видів злочинів: правопорушення, пов'язані з комп'ютерами: (а саме: підробка, пов'язана з комп'ютерами, шахрайство, пов'язане з комп'ютерами); правопорушення, пов'язані зі змістом (а саме: правопорушення, пов'язані з дитячою порнографією: розповсюдження або передача дитячої порнографії за допомогою комп'ютерних систем; реалістичні зображення неповнолітньої особи, задіяної у явно сексуальній поведінці); правопорушення, пов'язані з порушенням авторських та суміжних прав (а саме: правопорушення, пов'язані з порушенням авторських та суміжних прав).

У кримінальному законі термін кіберзлочин не вживається, а використовуються дещо застарілі терміни (розділ 16 і в ст.ст. 163, 176, 177, 190, 200 КК України) – як ЕОМ тощо. Сучасні інформаційно-комунікаційні технології можуть використовуватися для здійснення терористичних актів, зокрема шляхом порушення штатних режимів роботи автоматизованих систем керування технологічними процесами на об'єктах інфраструктури. Більшого масштабу набуває політично вмотивована діяльність у кіберпросторі у вигляді атак на урядові та приватні веб-сайти в мережі Інтернет.

Виникає логічне питання чи можна кіберзлочинність вважати окремим видом злочинності, способом вчинення злочину, обтяжуючою обставиною тощо. На жаль

однозначної відповіді на це питання на тепер немає.

Аналізуючи структуру кіберзлочинності в розрізі множинності не можна оминути не вирішене нормативно на національному рівні питання корпоративної відповідальності (або відповідальності юридичної особи). Так зокрема, щодо корпоративної відповідальності частина 1 статті 12 Конвенції визначає, кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для забезпечення того, щоб юридична особа могла нести відповідальність за кримінальне правопорушення, встановлене відповідно до цієї Конвенції, яке було вчинене на її користь будь-якою фізичною особою, як індивідуально, так і в якості частини органу такої юридичної особи. Така фізична особа має займати керівну посаду в рамках юридичної особи, в силу: повноважень представляти цю юридичну особу; повноважень приймати рішення від імені цієї юридичної особи; повноважень здійснювати контроль в рамках цієї юридичної особи. Хоча не визначаючи кіберзлочин окремим видом посягання на своєрідне коло правовідносин, не можна чітко зрозуміти, в яких випадках можливе притягнення до відповідальності юридичної особи. Хоча подібної практики в Україні з моменту ратифікації Конвенції не було і не може бути.

Також в ч. 2 цієї ж статті Конвенції зазначається, що на додаток до випадків, вже передбачених у пункті 1 цієї статті, кожна Сторона вживає заходів для забезпечення того, щоб юридична особа могла понести відповідальність у разі, коли недостатній нагляд чи контроль, який мав здійснюватися особою, вказаною у пункті 1, створив можливість вчинення кримінального правопорушення, встановленого відповідно до цієї Конвенції, на користь такої юридичної особи фізичною особою, яка діяла під її контролем. Встановлення відповідальність за створення можливості вчинення кримінального правопорушення є ще більш дискусійним.

Структуру кіберзлочинності можна розглядати під кутом об'єктів, що частіше потрапляють під кібератаку, зокрема в рамках цього дослідження звернемо увагу на декілька поширених протиправних дій:

1. Віруси або навмисно пошкоджене програмне забезпечення. Приміром в кіберпросторі з'являються такі загрози, як «ransomware» (в пер. з англ. – викуп), шантажуючі програми, які вимагають внесення відповідної суми оплати. 23.12.2015 року мала місце дещо незвична для України подія. Масова кібер атака на керівні енергопостачальні об'єкти привела до відключення електроенергії. У ряді міст та селищ Чернівецької області, Прикарпаття, Київщини залишилися без електрики (близько 220 000 споживачів електроенергії, що становить близько 1% всього енергопотреблітелей країни) [5]. Було ще декілька атак по тепер загроза повністю не винищена. Хоча така схема має і "мінуси" для злочинців, зокрема, тривалість у часі, складнощі при отриманні коштів. Окремо розрізняють такий вид кібератаки, як кібернапад з метою нанесення емоційної шкоди, метод залякування – «кібербуллінг». Кібербуллнг також відомий, як «підлітковий терор». Є ще близьке до цього поняття — «кібер мобінг», що означає масове цькування, також за допомогою різних каналів комунікації в інформаційному просторі. Окрім того використовується щодо українських користувачів мережі Інтернет у політичному контексті.

2. Бібліотеки агресивної реклами, відомі як Madware, все частіше здійснюють крадіжку з пристроїв приватну інформацію користувачів, стверджує Symantec [6]. Програми що потрапляють на пристрій з рекламою. Мобільні програми можуть не лише заважати при звичайному легальному використанні пристрою, а й взагалі перенаправляти, злочинцям персональні та інші дані що будуть введені користувачем (банківські данні, адреса, геоданні, контакти, медіафайли, паролі тощо). Програма типу «madware», що без дозволу може налаштовувати гаджет іншим чином, встановлювати інше програмне забезпечення (створює не бажані посилання, запуск додаткових інформаційних посилань, змінює налаштування вже встановленого програмного забезпечення). Тільки за останній рік кількість програм, що містять найбільшагресивні типи «madware», зросла більше ніж на 200 %. На сьогодні загрозливі програми надсилають платні SMS-повідомлення, а перераховані кошти дістаються хакерам та зловмисникам.

3. Соціальні мережі. Фінансування соціальних мереж формує нову серію загроз. Адже користувачі Інтернету з кожним днем усе з більшою довірою ставляться до різного роду соціальних мереж (наприклад, Vkontakte, Odnoklassniki, Mail.Ru Agent, Skype, Viber, Instagram, Facebook, Twitter тощо), включаючи обмін своїми особистими даними й купівлю спеціальної мережевої чи ігрової валюти і так званих віртуальних подарунків іншим користувачам [7]. Із зростанням рівня монетизації соціальні мережі надають своїм активним користувачам можливість надсилати один одному також справжні подарунки у вигляді матеріальних цінностей, а не лише нематеріального об'єкта, в соціальних мережах відбувається зростання грошового обігу, що дає хакерам нові можливості для формування загроз та здійснення атак.

4. Платіжні операції в системі он-лайн та інтернет-банкінг (приміром, внутрішньодержавні: Альфа-експрес, Софт, "FLASHPAY", Privat24, тощо), при яких кіберзлочинцями, використовуються викрадені персональні дані особи або здійснюється спонукання користувачів розголосити додаткові дані неофіційним соцмережам (через СМС повідомлення з пропозиціює надати пароль, отримання додаткових бонусів, інших матеріальних благ, емейли, тощо).

5. Так звані Е-гаманці: «ГлобалМані», «24NONSTOP», «Фінансовий світ», «ІнтерПейСервіс», «FLASHPAY», тощо, все частіше використовуються злочинцями, можуть бути не належним чином захищені зі сторони користувача, що потенційно веде до крадіжки особистої інформації. А в міру широкого впровадження зручних технологій мобільних платежів, саме мобільні телефони стануть представляти для хакерів ще більшу цінність. Даний процес схожий на загрозу «Firesheep», що працює спеціально для перехоплення чужих Wi-Fi сесій, а тому можна вже в найближчий час очікувати створення й появи на ринку спеціальних хакерських програм, які будуть перехоплювати особисту платіжну інформацію користувачів та застосовувати її з користю для зловмисників.

6. «Хмарні» носії інформації типу «Cloud» (наприклад, e-Dysk, iCloud, Google Drive, тощо). Включення до конкретної корпоративної мережі незахищених пристроїв, які накопичують інформацію, а після цього вона осідає вже на інших «хмарних» носіях, а це в свою чергу різко підвищує ризик витоку інформації або потенційного захоплення особистих незахищених даних. У результаті, встановлення користувачами нових програм призводить до зараження всієї системи [8]. Існують і інші кіберзлочини.

Окремої уваги заслуговує *ознака кіберзлочинності щодо територіально-часового та кількісно-якісний виміру*. Транскордонний характер кіберзлочинів становить серйозну проблему як для науковців так і для правоохоронних органів. Як влучно зазначає Горянінов К.К.: ця особливість багатьох кіберзлочинів зумовлює постійне ускладнення в міжнародному масштабі норм та правил, пов'язаних з виявленням та ідентифікацією злочинців, проведенням розслідувань та судових переслідувань за фактами транскордонних комп'ютерних злочинів [9, 245]. Серйозні проблеми виникають щодо того, відповідно до закону якої держави має нести відповідальність особа, яка вчинила злочин, перебуваючи в одній державі, в той час як об'єкт злочинного посягання розташовується в іншому. Як зауважують експерти «реальні простору стискаються в віртуальної реальності, і зовсім безглуздо вибудовувати в ній державні кордони». Відповідно застосування до виникаючих в глобальній мережі правовідносин локальних правових норм внутрішнього законодавства не може бути ефективно без урахування і зв'язку з законодавством інших країн, міжнародним правом. Ознака простору (як тереторіального так і часового) для кіберзлоченузлочинів є досить специфічною. Кіберзлочини пов'язані з використанням телекомунікаційної техніки. Можна казати про існування "віртуального простору", у якому вчиняються злочини цього виду [10, 10].

Віртуальний простір розглядається як особливий інформаційний простір, що моделюється за допомогою засобів комп'ютерної техніки, у якому: присутні специфічні інформаційні об'єкти (комп'ютерні програми, дані й т.п.) [11, 48]; в цьому просторі можуть знаходитись данні про людей, об'єктів реальності, факти, подій, процесів, представлені у логічному, символьному або будь-якому

іншому вигляді, та знаходяться у процесі руху від одного сервера до іншого, що зберігаються у пам'яті будь-якого пристрою.

Кіносередовище існує завдяки комп'ютерним системам, у яких рухається або зберігається інформація і має вивчатись з урахуванням цієї особливості.

Висновки: забезпечення кібербезпеки є одним із першочергових завдань, що стоїть перед державою. Останнє передбачає: побудову власної законодавчої системи, у тому числі через врегулювання правовідносин шляхом прийняття спеціального закону; внесення змін до кримінального законодавства задля «заповнення» існуючих прогалин і приведення у відповідність з міжнародними стандартами; забезпечення додержання національної стратегії з кібербезпеки, постійне доповнення її відповідними заходами; розробку і введення до навчального навантаження студентів дисциплін, пов'язаних із питаннями кібербезпеки; організацію систематичного широкомасштабного інформування населення про загрози, що можуть мати місце при використанні сервісів Інтернет.

Список використаних джерел:

1. Кримінологія: Загальна та Особлива частини: підручник/ В. В. Голіна, Б. М. Головкін, М. Ю. Валуйська, О. В. Лисодєд та ін..; за ред. В. В. Голіни і Б. М. Головкіна. – Х. : Право, 2014 – 512 с.

2. Головкін Б. М. Кримінологічне поняття віктимізації / Б. М. Головкін // Наук. вісн. Міжнар. гуманіт. ун-ту. Серія: Юриспруденція. – 2015. – № 15. – С. 93–96.

3. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» // Офіційний вісник України від 29.03.2016. – № 23. – Стор. 69. – Ст. 899.

4. Конвенція про кіберзлочинність // Офіційний вісник України від 10.09.2007. – № 65. – Стор. 107. – Ст. 2535.

5. Расследование кибератаки на Украину: как вирус сломал облэнерго [Електронний ресурс]. – Режим доступу : http://biz.liga.net/all/it/stati/3251987-rassledovanie-kiber-ataki-na-ukrainu-kak-virus-slomal-oblenergo.htm.

6. Internet Threats Rising! How do you drive your security program with confidence? [Електронний ресурс]. – Режим доступу : https://www.brighttalk.com/webcast/5691/179777.

7. Социальные сети побеждают поисковиков [Електронний ресурс]. – Режим доступу : http://chip.com.ua/854408.html.

8. IT Security at the Speed of Business: Security Provisioning with Symantec Data Center Security [Електронний ресурс]. – Режим доступу : https://www.symantec.com/content/dam/symantec/docs/white-papers/it-security-at-the-speed-of-business-en.pdf.

9. Горяинов К. К. Транснациональная преступность: проблемы и пути решения / К. К. Горяинов , А. П. Исеченко, Л. В. Кондратюк. – М. : ИНФРА–М, 1997. – 386 с.

10. Гаджиев М. С. Криминологический анализ преступности в сфере компьютерной информации: по материалам Республики Дагестан : автореф. дис. на соискание учен. степени канд. юрид. наук : 12.00.08 / М. С. Гаджиев. – Махачкала, 2004. – 19 с.

11. Осипенко А. Л. Борьба с преступностью в глобальных компьютерных сетях: международный опыт : монография / А. Л. Осипенко. – М. : Норма, 2004. – 432 с.

References

1. Kryminolohiya: zahalna ta osoblyva chastyny : pidruchnyk/ V. V. Holina, B. M. Holovkin, M. Yu. Valuyska, O. V. Lysodied ta in..; za red. V. V. Holiny i B. M. Holovkina. – Kh. : Pravo, 2014 – 512 p.

2. B. M. Holovkin, Kryminolohichne poniattia viktymizatsii / B. M. Holovkin // Nauk. visn. Mizhnar. humanit. un-tu. Seriya: Yurysprudentsiia. – 2015. – No. 15. – Pp. 93–96.

3. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 27 sichnia 2016 roku "Pro Stratehiiu kiberbezpeky Ukrainy" // Ofitsiinyi visnyk Ukrainy vid 29.03.2016. – No. 23. – Stor. 69. – St. 899.

4. Konventsiia pro kiberzlochynnist // Ofitsiynyi visnyk Ukrainy, ofitsiine vydannia vid 10.09.2007. – No. 65. – Stor. 107. – St. 2535.

5. Rassledovanie kiberataki na Ukrainu: kak virus slomal oblenergo [Elektronnyi resurs]. – Rezhym dostupu : http://biz.liga.net/all/it/stati/3251987- rassledovanie-kiber-ataki-na-ukrainu-kak-virus-slomal-oblenergo.htm.

6. Internet Threats Rising! How do you drive your security program with confidence? [Elektronnyi resurs]. – Rezhym dostupu : https://www.brighttalk.com/webcast/5691/179777.

7. Sotsialnie seti pobezhdayut poiskovikov [Elektronnyi resurs]. – Rezhym dostupu : http://chip.com.ua/854408.html.

8. IT Security at the Speed of Business: Security Provisioning with Symantec Data Center Security [Elektronnyi resurs]. – Rezhym dostupu : https://www.symantec.com/content/dam/symantec/docs/white-papers/it-security-at-the-speed-of-business-en.pdf.

9. K. K. Goryainov, Transnatsionalnaya prestupnost: problemi i puti resheniya / K. K. Goryainov, A. P. Isechenko, L. V. Kondratyuk. – M. : INFRA–M, 1997. – 386 p.

10. M. S. Gadzhiev, Kriminologicheskiy analiz prestupnosti v sfere kompyuternoy informatsii: po materialam Respubliki Dagestan : avtoref. dis. na soiskanie uchen. stepeni kand. yurid. nauk : 12.00.08 / M. S. Gadzhiev. – Makhachkala, 2004. – 19 p.

11. A. L. Osipenko, Borba s prestupnostyu v globalnikh kompyuternikh setyakh :mezhdunarodniy opit : monografiya / A. L. Osipenko. – M. : Norma, 2004. – 432 p.