УКРАЇНСЬКИЙ ВИМІР КІБЕРЗЛОЧИННОСТІ КРІЗЬ ПРИЗМУ ОКРЕМИХ ТИПІВ КІБЕРЗЛОЧИНЦІВ

UKRAINIAN MEASUREMENT OF CYBER CRIME THROUGH THE PRISM OF SEPARATE TYPES OF CYBER CRIMINALS

УДК 316.422.44+316.624
DOI https://doi.org/10.32843/2663-5208.2020.11.14

Чаплик М.М.
к.і.н., доцент кафедри соціології управління
Донецький державний університет управління

У статті автором розглядаються окремі типи кіберзлочинців, які поширені в українському суспільстві, та надається загальна характеристика особливостей кожного з типів. У якості окремого типу кіберзлочинців виокремлюються хакери, які за допомогою масової культури власне й стали своєрідним символом даного різновиду протиправної діяльності. Водночас автор зауважує на багатогранності хакерства як соціального явища, яке не є тотожним кіберзлочинності, а також на зворотній стороні субкультурі хакерів і їхній ролі у протидії кіберзлочинності. Крім того, автор звертає увагу на кіберзлочинність й у контексті глобальних викликів безпеці держав та інших соціальних інститутів, зокрема крізь призму інформаційних та кібервійн. У зв'язку із цим у рамках субкультури хакерів автором виділяється окремий тип кіберзлочинців, умовно позначений ним як політичні кіберзлочинці. На відміну від дій представників криміналітету та «білокомірцевих» злочинців, їхні дії можуть не мати економічних мотивів або такі мотиви не є пріоритетними. У статті також розглядається тип правопорушників у кіберсфері, який складається із представників традиційного та організованого криміналітету, які використовують здобутки науково-технічного прогресу під час здійснення кримінальних практик. У кіберзлочинах даного типу, на думку автора, вагоме місце займають не стільки технічні знання, скільки навички соціальної інженерії. Окремо автор виділяє кіберзлочини, які вчиняють «білокомірцеві» злочинці. Через складність їхнього виявлення кіберзлочини «білих комірців» відзначаються високим рівнем латентності. У зв'язку з масовим поширенням такого різновиду правопорушень у кіберсфері, як використання неліцензійного програмного забезпечення, автор виділяє в якості окремого типу кіберзлочинців пересічного побутового (кібер)пірата. При цьому надається економічне та соціологічне пояснення поширення подібних масових протиправних практик в українському суспільстві. Серед правопорушників із числа пересічних громадян, які використовують технічні прилади та віртуальну мережу, крім піратів, автором виділяються й інші злочинці, які складають окремий тип.

Ключові слова: *кіберзлочинність, типи кіберзлочинців, хакери, кіберзлочинність криміналітету, «білокомірцеві» кіберзлочинці, піратство, криміналізація віртуального простору.*

In the article, the author considers certain types of cybercriminals that are common in Ukrainian society, and gives a general description of the characteristics of each type. Hackers stand out as a separate type of cybercriminals, who, with the help of mass culture, have actually become a kind of symbol of this type of illegal activity. At the same time, the author notes the versatility of the hacker subculture as a social phenomenon that is not identical with cybercrime, as well as on the reverse side of hacking and their role in countering cybercrime. In addition, the author draws attention to cybercrime in the context of global security challenges of states and other social institutions, in particular through the prism of information and cyber warfare. In this regard, in the framework of the hacker subculture, the author identifies a separate type of cybercriminals conditionally designated by him as political cybercriminals. Unlike felons and white-collar criminals, their actions may not have economic motives or such motives are not priority. The article also examines the type of offenders in the cyber sphere, consisting of representatives of traditional and organized criminals who use the achievements of scientific and technological progress in the implementation of criminal practices. In the cybercrimes of this type, according to the author, an important place is occupied not so much by technical knowledge as by the skills of social engineering. Separately, the author identifies cybercrime, criminals commit "white collar". Due to the complexity of their detection, white-collar cybercrimes have a high level of latency. In connection with the mass distribution of this type of offense in the cyber sphere, such as the use of unlicensed software, the author identifies ordinary (cyber) pirates as a separate type of cybercriminals. At the same time, an economic and sociological explanation is provided for the spread of such mass illegal practices in Ukrainian society. Among the offenders from among ordinary citizens who use technical devices and a virtual network, in addition to pirates, the author distinguishes other criminals who make up a separate type.

Key words: *cybercrime, types of cybercriminals, hackers, cybercrime criminality, "white-collar" cybercriminals, piracy, criminalization of virtual space.*

Постановка проблеми. Злочинність як мінливе соціально негативне явище, яке супроводжує людство протягом усієї історії його існування, в епоху інформаційних технологій набуває нових форм та ознак. Інформаційні технології проникають та швидко опановують різноманітні сфери суспільства, в тому числі і сфери, які пов'язані з отриманням прибутків, наприклад, сферу економіки, фінансів, торгівлі, або сфери, які пов'язані із суспільною та національною безпекою, приватністю особистості тощо. Дані сфери переносяться у віртуальний світ, а відтак стають вразливими для кіберзлочинців. Отже, з поширенням інформа-

ційних технологій кіберзлочинність перетворюється на вітальну проблему як усього людства та створених ним інституцій, так і окремих індивідів. Відтак і протидія кіберзлочинності потребує нових підходів та рішень.

Аналіз останніх досліджень і публікацій. Для пояснення кіберзлочинності доцільно звернутися до трактування злочинного та законного у соціологічній теорії. У даному разі, на нашу думку, видаються актуальними ідеї одного із класиків соціології Е. Дюркгайма стосовно того, що вважати нормою, а що – патологією, висловлені ним в однойменній праці [1]. Злочинність, як і інші соціальні патології, сприймається французьким соціологом як нормальне та цілком природнє соціальне явище. Даний підхід був критично сприйнятий за часів Е. Дюркгайма та продовжує піддаватися критиці в наш час. Разом із тим він допомагає пролити світло на процес криміналізації віртуального простору. Особливо доречні ідеї Е. Дюркгайма в контексті погляду на норми та девіації у віртуальному світі крізь призму явища хакерства. У віртуальному просторі хакери намагаються самовиразитися і таким чином готують інноваційні та технологічні зміни. Водночас створений «людиною технічною» віртуальний світ потребує розроблення певних правил перебування в ньому. Отже, хакери не лише йдуть в авангарді технічного прогресу, але й готують соціальні зміни та виступають провісниками нових норм моралі та права.

Під час розгляду хакерів як соціального явища заслуговують на увагу ідеї іспанського соціолога М. Кастельса, висловлені ним стосовно інформаційного суспільства. Як зазначає М. Кастельс, культура хакерів відіграє головну роль у побудові Інтернету із двох причин: 1) вона є середовищем «для видатних технічних інновацій»; 2) вона є передавальною ланкою «між знаннями, породженими техномеритократичною культурою, та підприємницькою діяльністю» [2, с. 57]. Головними елементами субкультури хакерів є свобода, яка поєднується із співробітництвом та «в кінцевому підсумку призводить до «економіки дарування», технічні інновації та «внутрішнє задоволення від процесу творчості» [2, с. 64–65]. Крім того, існують субкультури хакерів, які «базуються на політичних принципах, а також на особистому протесті» [2, с. 68].

При цьому М. Кастельс відокремлює хакерів від крекерів та кіберзлочинців. До крекерів іспанський соціолог відносить індивідуумів, які «намагаються заявити про себе, але володіють досить обмеженими технічними знаннями» [2, с. 69]. Саме крекерам, а не хакерам, він приписує поведінку «безвідповідальних комп'ютерних диваків», які «намагаються зламувати коди, незаконно проникати в системи або вносити безлад у комп'ютерний графік» [2, с. 57]. Разом із тим, на думку М. Кастельса, подібну поведінку «слід відрізняти від кіберзлочину – грабунку через Інтернет з метою особистої наживи» [2, с. 68].

Американський соціолог Р. Коллінз розглядає хакерські атаки як своєрідну форму віртуалізованого конфлікту. Вони вчиняються з метою отримання матеріальної вигоди, інформації, документів (злочини проти власності, честі та гідності та вторгнення в приватну сферу). Також вони вчиняються з метою зламу та порушення нормальної роботи будь-якого ресурсу як форма протесту або демонстрація «програмістської майстерності» [3, с. 107].

Проблема кіберзлочинності в Україні привертає увагу дослідників різних наукових напрямків, а також фахівців-практиків, у першу чергу юристів, економістів, фінансистів, соціологів, фахівців з інформаційних технологій, безпеки тощо. До розгляду різних аспектів даної проблеми звертаються у своїх роботах такі дослідники, як П. Біленчук, В. Голубєв, М. Карчевський, Н. Козак, Н. Міщук, П. Пушкаренко, В. Шелухін та інші [4; 5; 6; 7; 8; 9; 10].

Водночас серед усіх різновидів правопорушень кіберзлочини є найбільш динамічними, а відтак потенційно становлять найбільшу загрозу для людини та створених нею інституцій. Тому проблема кіберзлочинності потребує постійного вивчення та системного моніторингу для мінімізації загроз для індивіда та суспільства.

Постановка завдання. Метою даної статті є розгляд найпоширеніших типів кіберправопорушників у реаліях сучасного українського суспільства.

Виклад основного матеріалу дослідження. За даними колишнього начальника Департаменту кіберполіції С. Демедюка, серед найпоширеніших різновидів кіберзлочинів в Україні виділяються кібершахрайство, крадіжка даних банківської карти, протиправний контент, поширення шкідливого програмного забезпечення та створення майданчиків для продажу викраденої інформації [11].

За інформацією вітчизняної компанії Опендатабот, яка аналізує дані основних публічних реєстрів країни, шахрайство є найбільш популярною статтею кіберзлочинів, потім йдуть незаконне втручання в роботу комп'ютера та поширення порнографії [12].

Згідно із статистичними даними Офісу Генерального прокурора у 2019 році найбільшу кількість кіберзлочинів було обліковано за такими правопорушеннями, як: шахрайство, вчинене у великих розмірах або шляхом незаконних операцій із використанням електронно-обчислювальної техніки (ст. 190 ч. 3) – 2440; несанкціоноване втручання в роботу ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних

мереж чи мереж електрозв'язку (ст. 361) – 1137; несанкціоновані дії з інформацією, яка оброблюється в ЕОМ (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї (ст. 362) – 717; незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима, обладнанням для їх виготовлення (ст. 200) – 697 [13].

Застосовуючи метод типології, спробуємо поділити всю сукупність вітчизняних кіберправопорушників на окремі, найбільш характерні та узагальнені типи, враховуючи при цьому високий рівень латентності даного різновиду злочинності та неможливість його об'єктивного відображення у статистичних даних. На нашу думку, можна виділити шість типів кіберзлочинців, які поширені в українському суспільстві.

До представників першого типу правопорушників у кіберсфері слід віднести високоінтелектуальних злочинців, які не належать до світу традиційного криміналітету та організованої злочинності. Використовуючи усталене мовне кліше на позначення комп'ютерних зловмисників? позначимо їх таким поняттям, як «чорні» хакери (або black hat). Отже, перший тип кіберзлочинців – це власне фахівці у сфері інформаційних технологій, які використовують власні навички для протиправних дій. Наприклад, «чорні» хакери можуть зламувати віддалені сервери установ різної форми власності, приватних підприємств та окремих осіб у різних куточках світу із власної ініціативи або на замовлення. Спільнота хакерів у силу своїх здібностей у сфері комп'ютерних наук та IT-технологій, наприклад, здатна використовувати штучний інтелект для здійснення зловмисних атак, які вимагають залучення значної кількості ресурсів. Наприклад, шляхом програмування нейромережі на постійні атаки, які будуть повторюватися, поки не досягнуть результату [14].

Через те, що саме поняття «хакер» не є тотожним поняттю «кіберзлочинець», заради об'єктивності відзначимо й іншу, позитивну сторону хакерства – «білих» (white hat або етичних) хакерів, які, навпаки, протидіють кіберзлочинності та кіберзагрозам для людей та інституцій. Для забезпечення власної кібербезпеки з ними активно співробітничають провідні світові корпорації та компанії. Одним із напрямків діяльності «білих» хакерів є тестування сайтів шляхом намагання їх зламати та таким чином виявити вразливі місця, наприклад, тестування системи державних закупівель Prozorro [15]. Є випадки, коли в хакерській спільноті відбуваються переходи між «білою» та «чорною» сферами. В якості прикладу можна навести випадок із К. Мітником, який у минулому був «чорним» хакером, а наразі є провідним експертом із кібербезпеки [16].

У межах субкультури хакерів можна виділити ще один тип кіберзлочинців – умовно позначений нами як політичні кіберзлочинці. Під ним ми маємо на увазі хакерів, яких використовують інші країни, наприклад, із метою дестабілізації політичної ситуації в державі тощо. Фактично в даному разі мова йде про окремий кіберфронт у гібридних війнах як війнах нового типу, де економічні мотиви можуть мати вторинне значення. До даного типу злочинів належать масовані кібератаки на окремі держави, їхні установи та інформаційні системи, силові та безпекові структури, підприємства, інфраструктурні об'єкти, кібершпигунство і т. ін. Сюди ж належать технології з поширення дезінформації (зокрема, дипфейків – зображень та відео, які створюються штучним інтелектом та видаються справжніми [17]), наприклад, для компрометації еліти, втручання у виборчій процес, масового маніпулювання свідомістю тощо. Отже, таких кіберзлочинців можливо використовувати як у кібервійнах, так і в інформаційних війнах. Крім того, до даного типу відносяться кібертерористи, які, наприклад, вчиняють кібератаки на об'єкти критичної інфраструктури. Даний вид правопорушень може керуватися й благородною метою (наприклад, хактивізм), бути альтруїстичним та некерованим ззовні, виявлятися як форма протесту, зумовленого намаганням офіційних структур контролювати Інтернет, а неформальних структур – зберегти конфіденційність та анонімність [3, с. 107–108].

Третій тип кіберзлочинців – це особи та групи представників криміналітету, які мають кримінальний габітус або дотичні до кримінальних практик. На певному етапі свого розвитку технології потрапляють в поле зору традиційної та організованої злочинності, і зрештою, кіберзлочинність перетворюється на один із напрямків у протиправній діяльності організованого та традиційного криміналу. На даний час зафіксовано достатньо фактів того, що кіберзлочини вчиняються кримінальниками, в тому числі й із установ виконання покарань, наприклад, шляхом телефонного шахрайства з місць позбавлення волі. Керівництво даними правопорушеннями здійснюється представниками організованої злочинності, зокрема «злодіями в законі» [11]. Важливу роль у переході кіберзлочинності до поля зору традиційного та організованого криміналітету відіграє технічне спрощення здійснення окремих видів кіберзлочинів, а відтак і здатність до їх вчинення звичайними користувачами інформаційних приладів, електронних мереж та засобів зв'язку. Крім того, варто зауважити, що традиційний криміналітет застосовує не стільки нові технології, скільки використовує соціальну

інженерію в поєднанні з технічними засобами, які є здобутками науково-технічного прогресу. При цьому традиційний та організований криміналітет також використовує кіберсферу для вчинення злочинів, які були відомі кримінальному світові ще до появи комп'ютерів та Інтернету. Зокрема, здійснює торгівлю наркотиками шляхом використання даркнету або за допомогою віртуальної мережі «наркомагазинів» у соціальних мережах та месенджерах, наприклад, через Telegram. Таким же чином традиційний та організований кримінал опановує віртуальний світ для поширення інших заборонених видів товарів та послуг, відмивання грошей тощо. Анонімність, а відтак і можливість уникнути відповідальності, а також можливість для організованої транснаціональної кіберзлочинної діяльності, динаміка зростання якої, на думку експертів, вже дозволила обігнати такий прибутковий напрямок кримінальної економіки, як наркобізнес, – усе це робить технічні прилади та віртуальний світ привабливими для організованої злочинності та традиційного криміналітету.

Четвертий тип кіберзлочинців – це «білокомірцеві» злочинці, які використовують кіберсферу для вчинення злочинів в економічній, фінансовій тощо сферах. Кіберзлочини приваблюють «білих комірців» анонімністю, складністю їхнього розкриття тощо. «Білокомірцеві» злочинці можуть вчиняти традиційні економічні злочини за допомогою технічних пристроїв та віртуальної мережі. Також «білі комірці» можуть вчиняти й кіберзлочини або імітувати роль «жертв» кіберзлочинів із метою приховування власне «білокомірцевих» правопорушень. Так, екс-начальник Департаменту кіберполіції С. Демедюк зазначав про факти прикривання окремими підприємствами вигаданими кіберзлочинами з метою уникнення сплати податків, викрадення та легалізації коштів. За його словами, коли законодавець дозволив податкову відстрочку для підприємств-жертв атаки вірусу Petya у червні 2017 року, то цим скористалося багато підприємств, які, за результатами слідства, були заражені вірусом вже після атаки [11]. Вчинення кіберзлочинів «білими комірцями» збільшує їхню суспільну шкоду, адже самі злочини «білих комірців» відзначаються високою латентністю, а в поєднанні з використанням технічних приладів та віртуальної мережі рівень їхньої латентності значно зростає.

Варто зважати на окремий тип кіберзлочинців, а саме на пересічних громадян країни, які порушують авторські права. Використання піратського програмного забезпечення зберігається як масове явище в українському суспільстві. За даними дослідження Business Software Alliance (BSA) «Global Software Survey», станом на кінець 2017 року 80% встановленого на комп'ютерах програмного забезпечення в Україні не мало відповідної ліцензії [18]. Даний феномен пов'язаний із економічним зиском, який отримує пересічний житель країни від користуванням піратським програмним забезпеченням, а також іншими об'єктами авторського права та інтелектуальної власності. Поведінку такого типу правопорушників можна пояснити з точки зору економічного підходу Г. Беккера, а саме крізь призму оцінки витрат та користі, коли очікувана корисність від протиправної дії перевищує корисність, яку можна було б отримати використовуючи час та засоби законним шляхом [19, с. 293], та теорією аномії в її формулюванні Р. Мертоном, коли видається неможливим досягти приписаних у суспільстві устремлінь законним шляхом [20, с. 247]. Проблема раціональності піратства у кіберсфері детально розкривається у вітчизняних наукових розвідках [10].

Масовість поширення порушень авторського права та суміжних прав також підтверджує теорію німецького соціолога та кримінолога Ф. Зака стосовно того, що переважна більшість дорослого населення сучасного суспільства принаймні раз у житті вчиняє злочин згідно з існуючим у конкретному суспільстві кримінальним правом [21, с. 109].

У якості репрезентантів шостого типу кіберзлочинців слід виділити пересічних громадян, які вчиняють інші, крім піратства, правопорушення із застосуванням технічних приладів та віртуальної мережі. До нього не належать представники традиційного та організованого криміналітету, «білі комірці» або комп'ютерні інтелектуали – хакери. На нашу думку, це найбільш строкатий та складний у сенсі систематизації тип кіберзлочинців. Більшість кіберзлочинів даного типу лежить у площині отримання матеріальної вигоди. При цьому деякі з них можуть відрізнятися особливим цинізмом навіть серед соціальних патологій, як, наприклад, поширення дитячої порнографії або шахрайство на зборі коштів для лікування хворих дітей тощо.

Висновки з проведеного дослідження. Таким чином, правопорушення у кіберсфері є доволі поширеним соціальним явищем не лише у світі, а й в українському суспільстві, яке має високу динаміку зростання та латентність. Водночас природа цих правопорушень, а відтак і типів кіберзлочинців, які їх уособлюють, є різною. Кожен із типів кіберправопорушників має свою мотивацію до вчинення злочинів у кіберсфері. Якщо профілактика та протидія одним правопорушенням потребує інформаційної та роз'яснювальної роботи або лежить у площині зростання рівня економічного добробуту населення, то профілактика та протидія іншим кіберзлочинам полягає в поширенні знань про кібербезпеку почина-

ючи зі шкільного віку, посиленні кримінальної відповідальності на законодавчому рівні, залученні до кібербезпеки комп'ютерних інтелектуалів тощо. Відтак профілактика та протидія даним правопорушенням потребують різних підходів в залежності від окремого типу кіберзлочінців. У цілому проблема такого різновиду девіацій, як кіберзлочинність, лежить у міждисциплінарній площині і не втрачатиме актуальності в найближчій часовій перспективі, а відтак залишатиметься у фокусі уваги фахівців як на теоретичному, так і на практичному рівнях.

ЛІТЕРАТУРА:

1. Дюркгейм Э. Норма и патология. Социология преступности (Современные буржуазные теории): сб. статей / под ред. М. Вольфганга. Москва : Издательство «Прогресс», 1966. 368 с. С. 39–44.
2. Кастельс М. Галактика Интернет: Размышления об Интернете, бизнесе и обществе; пер. с англ. А. Матвеева; под ред. В. Харитонова. Екатеринбург : У – Фактория (при участии изд-ва Гуманитарного ун-та), 2004. 328 с.
3. Кучеренко И.В. Рэндалл Коллинз о виртуализации конфликта в повседневной жизни. *Философские проблемы информационных технологий и киберпространства.* 2013. Выпуск 5, № 1. С. 99–111.
4. Біленчук П.Д. Портрет комп'ютерного злочинця. Київ : B&B, 1997. 48 с.
5. Голубев В.А. Аналіз кіберзлочинності у сфері економічної безпеки. *Information Technology and Security*. 2013. № 1(3). С. 26–32.
6. Карчевський М.В. Кримінально-правова охорона інформаційної безпеки України : монографія. МВС України, Луганський державний університет внутрішніх справ імені Е.О. Дідоренка. Луганськ : РВВ ЛДУВС ім. Е.О. Дідоренка, 2012. 528 с.
7. Козак Н.С. Криміналістична характеристика осіб, які вчиняють комп'ютерні злочини. *Науковий вісник Національного університету ДПС України (економіка, право),* 2(61) 2013. С. 186–191.
8. Міщук Н. Кіберзлочинність як загроза інформаційному суспільству. *Вісник Львівського університету. Серія економічна.* 2014. Вип. 51. С. 173–179.
9. Пушкаренко П.І. Кіберзлочинність як новітній феномен тіньової економіки. *Проблеми і перспективи розвитку банківської системи України:* зб. наук. праць. Суми : УАБС НБУ, 2006. Т. 17. С. 75–82.
10. Шелухін В.А. Інтернет-піратство як раціональний вибір (з погляду моделі Г. Беккера та концепції мікро-макро переходів Дж. Колмена). *ВІСНИК НТУУ «КПІ». Політологія. Соціологія. Право.* Випуск 1/2 (33/34). 2017. С. 161–170.
11. Голова Кіберполіції: «Ваш син у поліції» приносить шахраям на «зоні» мільйон гривень на добу. URL : https://www.epravda.com.ua/publications/2018/01/15/633003/ (дата звернення: 10.01.2020).
12. За п'ять років кіберзлочинність в Україні виросла вдвічі. URL : https://www.epravda.com.ua/news/2019/10/21/652782/ (дата звернення: 10.01.2020).
13. Єдиний звіт про кримінальні правопорушення за січень-грудень 2019 р. Офіс Генерального прокурора. Статистика. URL : https://old.gp.gov.ua/ua/statinfo.html (дата звернення: 25.01.2020).
14. Використання штучного інтелекту для злому назвали головною загрозою 2020 року. URL : https://dt.ua/TECHNOLOGIES/vikoristannya-shtuchnogo-intelektu-dlya-zlomu-nazvali-golovnoyu-zagrozoyu-2020-roku-333526_.html (дата звернення: 15.01.2020).
15. «Білі» хакери шукатимуть баги в системі Prozorro. URL : https://www.epravda.com.ua/news/2019/08/16/650675/ (дата звернення: 15.01.2020).
16. Митник К.Д., Саймон В.Л. Искусство обмана. Издательство : Компания АйТи, 2004. 360 с.
17. Мацука О. Дипфейк – нові можливості, або Революція у фальсифікаціях. URL : https://dt.ua/internal/dipfeyk-novi-mozhlivosti-abo-revolyuciya-u-falsifikaciyah-308451_.html (дата звернення: 15.01.2020).
18. В Україні 80% усього програмного забезпечення є неліцензійним – дослідження. URL : https://www.unian.ua/science/10267089-v-ukrajini-80-usogo-programnogo-zabezpechennya-ye-nelicenziynim-doslidzhennya.html (дата звернення: 15.01.2020).
19. Беккер Г.С. Человеческое поведение: экономический подход. Избранные труды по экономической теории : пер. с англ. / Сост., науч. ред., послесл. Р.И. Капелюшников ; предисл. М.И. Левин. Москва : ГУ ВШЭ, 2003. 672 с.
20. Мертон Р. Социальная теория и социальная структура. Москва : АСТ: АСТ МОСКВА: ХРАНИТЕЛЬ, 2006. 873, [7] с.
21. Гилинский Я. Девиантология: социология преступности, наркотизма, проституции, самоубийств и других «отклонений». Монография. Санкт-Петербург : Издательский Дом «Алеф-Пресс», 2013. 650 с.