ПУБЛІЧНО-ПРАВОВИЙ ДИСКУРС У КОНТЕКСТІ ГЛОБАЛІЗАЦІЇ

Лефтеров Л. В. *
ад'юнкт кафедри кримінального
права та кримінології
Одеського державного університету
внутрішніх справ
(м. Одеса, Україна)
ORCID: https://orcid.org/0000-0002-3550-3498

***Lev Lefterov**, Adjunct of the Department of Criminal Law and Criminology of Odessa State University of Internal Affairs (1, Uspenska St., Odessa, Ukraine).

УДК 343.92
DOI 10.26886/2524-101X.1.2019.6

ЗАГАЛЬНОСОЦІАЛЬНІ ЗАХОДИ ЗАПОБІГАННЯ ШАХРАЙСТВУ, ЩО ВЧИНЯЄТЬСЯ ШЛЯХОМ ВИКОРИСТАННЯ ЗАСОБІВ ЕЛЕКТРОННИХ КОМУНІКАЦІЙ

GENERAL SOCIAL MEASURES WHICH PREVENT FRAUDS COMMITED BY USING OF ELECTRONIC COMMUNICATIONS

ABSTRACT

General social measures of crime prevention, as a complex of promising socio-economic and cultural-educational measures, are aimed at reducing social contradictions in all spheres of public life. These measures should belong to the reasonable economic-organizational, cultural and educational activities of state bodies, enterprises, institutions, firms, public organizations. General social prevention of cybercrime is to reduce social contradictions, crime-fighting confrontations of different layers of the population, to create the necessary conditions for the legalization

of obtaining adequate incomes by citizens, and to promote the construction of a solid foundation for the normal functioning of all social spheres. The article deals with topical issues of counteraction to cybercrime. Particular attention is paid to illegal operations for property seizure through fraud or abuse of trust, the mechanism of implementation of which is impossible without the use of electronic computing. In particular, a comprehensive study of measures to counteract this category of crimes is conducted. The results of a special criminological research, which is provided by sociological methods, questionnaires of the profile audience of respondents, are given. The criminological basis of the study is the question of general social measures for the prevention of frauds committed with the use of electronic computers (computers), automated systems, computer networks or telecommunication networks. The main aspects of the work of the units of the National Police of Ukraine, in the sphere of counteraction to cybercrime, are also considered. It is noted that the issue of the rapid development of crimes in the sphere of using electronic communication means, and first of all, frauds committed with the help of electronic computing, carries socially dangerous consequences that affect all spheres of state functioning.

The key words: cybercrime, criminology, computer crime, general social measures, frauds prevention, cyberpolice, National Police, electronic communications.

Кіберзлочинність – це швидко зростаюча галузь злочинності. Все більше злочинців використовують швидкість, зручність і анонімність Інтернету для здійснення різноманітних кримінальних дій, які не знають жодних фізичних або віртуальних кордонів, завдають серйозної шкоди і створюють реальні загрози для жертв у всьому світі.

Вивчення кримінологічного стану і тенденцій кіберзлочинності в цілому, визначення та розуміння динаміки вказаної категорії злочинності, надає змогу сформувати якісні методики їх запобігання та протидії. Звернемось до закордонного досвіду і проаналізуємо деякі статистичні дані. Відповідно до звіту ФБР США за 2017 р. про злочини в Інтернеті, Центр скарг на комп'ютерну злочинність (IC3) у 2017 році отримав близько 300 тис. звернень від жертв онлайн-шахрайства, із сумою збитків більше 1,4 млрд доларів. Іншими словами, кожного дня понад 800 громадян США ставали жертвами Інтернет-шахрайств на загальну суму більш ніж 3,5 млн доларів на добу. І вказані підрахунки включають лише зареєстровані факти правопорушень (Smith, 2017). Інтернет-шахрайство проявляється у багатьох формах та може відбуватися навіть якщо частково ґрунтується на використанні Інтернет-послуг, і в основному або повністю базується на використанні засобів електронних комунікацій.

Як бачимо, навіть у економічно розвинених державах, є грандіозні проблеми з профілактикою і протидією шахрайствам, які вчиня-

ються шляхом використання комп'ютерних технологій. Це зумовлює актуальність даної проблеми та потребує поглибленого вивчення, аналізу, а також розробки і впровадження готових професійних рішень, методичних, юридичних та загальносоціальних заходів запобігання зазначеним видам шахрайства.

В Україні відсутні точні підрахунки завданих загальних збитків від кібершахрайств Проте, є окремі показники, наприклад, за даними української міжбанківської асоціації членів платіжних систем ЕМА, у 2016 р. від Інтернет-шахрайства постраждав кожен сотий власник платіжних карт в Україні, а "дохід" від незаконних дій склав майже 340 млн гривень (11,2 млн євро) (Politeka, 2018). За іншими даними у 2017 р. збитки українських банків від незаконних дій з платіжними картками (лише як одного з напрямків кібершахрайства) становить 163,7 млн гривень (Національний банк України, 2018).

Виходячи з наведеного, метою даної статті є проведення комплексного аналізу існуючих загальносоціальних заходів запобігання шахрайствам у сфері використання інформаційних технологій, а також на підставі результатів проведеного соціологічного кримінологічного дослідження розробка більш дієвих методів запобігання і профілактики кібершахрайствам.

Наукові дослідження окремих аспектів боротьби з Інтернет-шахрайствами та кібезлочинністю загалом проводились А. М. Бабенко, І. Г. Богатирьовим, В. В. Голіною, А. К. Лебедєвим, А. Є. Користіним, В. В. Марковим тощо (Бабенко, 2013; Голіна, 2011; Марков, 2015), однак на сучасному етапі вивчення кримінологічних особливостей шахрайства, вчиненого з використанням електронно-обчислювальної техніки, виникли раніше недосліджені питання, у т. ч. аналіз факторів і змінних, які впливають на динаміку розвитку зазначеного виду злочинів в умовах сучасного розвитку боротьби з кіберзлочинністю.

Згідно зі ст. 216 Кримінального-процесуального кодексу України, слідчі органи Національної поліції здійснюють досудове розслідування кримінальних правопорушень, передбачених законом України про кримінальну відповідальність, крім тих, які віднесені до підслідності інших органів досудового розслідування. Таким чином, протидія злочинам у сфері інформаційних технологій, а також безпосередньо шахрайства, яке вчиняється шляхом незаконного використання електронно-обчислювальної техніки (що передбачено ч. 3 ст. 190 Кримінального кодексу України), здійснюються підрозділами Національної поліції.

Дослідження питання, пов'язаного з протидією і запобіганням кібершахрайствам, формує важливі моменти, які потребують глибокого вивчення. На думку В. В. Голіної, запобігання злочинності – це сукупність різноманітних видів діяльності і заходів у державі, спрямованих на вдосконалення суспільних відносин з метою усунення негативних явищ та процесів, що породжують злочинність або сприяють їй, а також недопущення вчинення злочинів на різних стадіях злочинної поведінки (Голіна, 2011, с. 27).

За нашим трактуванням вказаного поняття, запобігання злочинів є невід'ємною складовою частиною загальної системи протидії злочинності. Наприклад, розкриття злочину – це поняття оперативно-розшукове, яке означає, що злочинець знайдений, а все інше скоріше характеризує стадію розслідування злочину, ніж його розкриття, бо воно вже розкрито. Таким чином протидія кіберзлочинності – це комплекс дій, що включає: розкриття (розслідування, документування, оперативну розробку та інше), запобігання (припинення злочинної діяльності, оперативно-профілактичні заходи, кримінологічні, соціальні та превентивні заході) злочинної діяльності.

Як інтегративна система організованої протидії злочинності, запобігання злочинності включає у себе різноманітні запобіжні заходи. Для належного впорядкування запобіжних заходів, чіткого визначення рівня і напрямів запобіжної діяльності суб'єктів, їх компетенції, природи самих заходів тощо виникає необхідність їх класифікації. Існують різні класифікації запобіжних заходів з урахуванням тих цілей, які перед ними ставляться. Заходи можна класифікувати за: рівнем, масштабом, змістом, суб'єктами, об'єктами тощо. За рівнем розрізняються загально-соціальні, спеціально-кримінологічні та індивідуальні заходи запобігання злочинності; за масштабом – заходи, які здійснюються у територіальному розрізі, на окремому об'єкті, щодо групи осіб; за змістом – заходи соціально-економічного, соціально-демографічного, технічного, екологічного, правового та іншого характеру; за суб'єктами – заходи, що здійснюються органами всіх гілок влади, організаціями, трудовими об'єднаннями, установами, окремими громадянами; за об'єктами – відповідно до видів злочинів, на протидію яким вони спрямовані.

Загальносоціальне запобігання злочинності – це, насамперед, комплекс перспективних соціально-економічних і культурно-виховних заходів, спрямованих на подальший розвиток та вдосконалення

суспільних відносин і усунення або нейтралізацію причин та умов злочинності. Тому вирішальна роль у поступовому зменшенні соціальних суперечностей в усіх сферах соціального життя належить розумній господарсько-організаційній та культурно-виховній діяльності державних органів, підприємств, установ, фірм, громадських організацій тощо. Запобіжний потенціал цієї діяльності полягає у тому, що вона протидіє негативним явищам і процесам, які сприяють відтворенню або збільшенню рівня злочинів, стимулює законослухняну поведінку людини.

Загальносоціальне запобігання – це позитивний ефект продуманої соціальної політики, яка здійснюється не тільки і не стільки з метою безпосереднього попередження злочинності. Вона спрямована, перш за все, на вирішення загальних економічних і соціальних завдань держави. Як вважає В. В Голіна, загальносоціальне запобігання злочинності полягає у тому, що його здійснення зменшує соціальні суперечності, криміногенне протистояння різних верств населення, рівень безробіття, підвищує стандарт життя людей, створює необхідні умови для легалізованого одержання достатніх прибутків громадянами, сприяє побудові міцного фундаменту щодо нормального функціонування всіх соціальних сфер, виховання та контролю над дітьми і молоддю, оздоровлення морального клімату у суспільстві, впровадження високих моральних цінностей у ньому, додержання демократичних засад та ін. Прогресивні соціальні програми спрямовані на утвердження законності, поваги до конституційних прав і свобод людини, зміцнення громадського порядку, дисципліни, на вирішення проблем поєднання громадських, виробничих, сімейно-побутових інтересів жінок і сім'ї, соціальної адаптації маргінальних верств населення тощо (Голіна, 2011, с. 32).

Якщо проводити паралель між кібершахрайством та категоріями злочинності загальнокримінальної спрямованості, то важливо зазначити, що наведені загальносоціальні заходи дієві для всіх напрямків запобігання злочинності.

З метою вивчення й аналізу заходів запобігання шахрайству, що вчиняється шляхом використання засобів електронних комунікацій, нами було проведено кримінологічне дослідження на підставі експертних думок фахівців. У ході проведення збору даних використовувались спеціальні методи кримінологічного дослідження, а саме анкетування. У досліджені взяли участь 158 співробітників практичних

підрозділів кіберполіції з усіх регіональних управлінь Департаменту кіберполіції Національної поліції України. З метою збільшення територіальності знаходження профільних респондентів, зменшення часу анкетування застосовувались електроні опитувальні листи за допомогою сервісу Google Forms.

Респондентам, було запропоновано, на підставі їх професійного досвіду, виділити найбільш дієві заходи профілактики й запобігання кібершахрайствам (рис. 1).

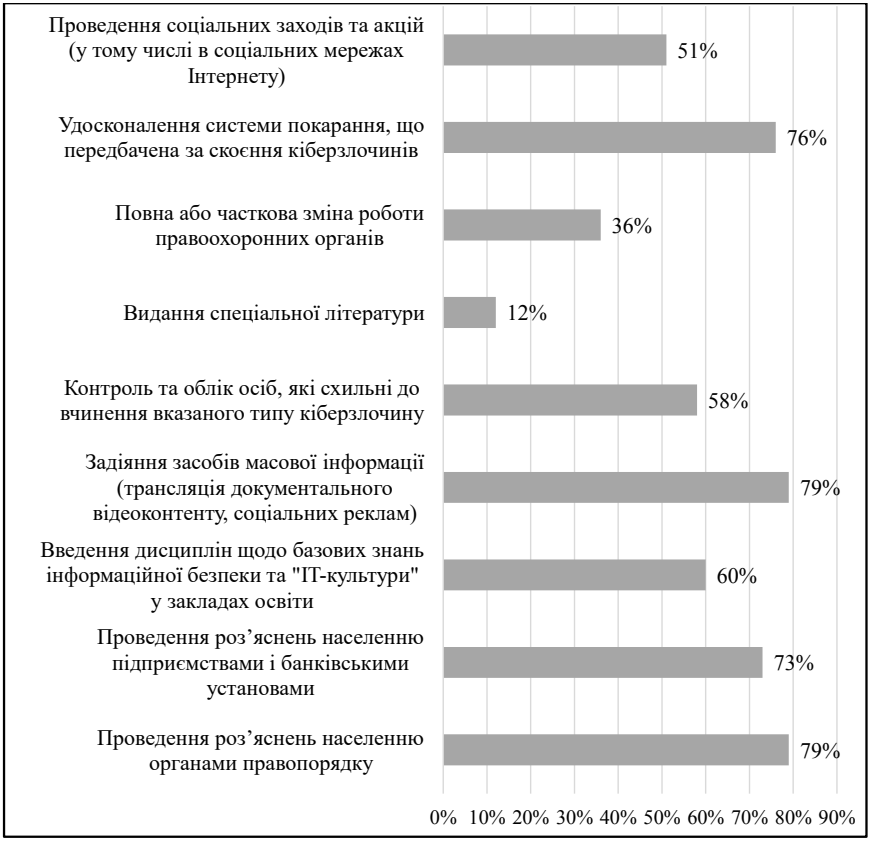

Рис. 1. Результати анкетування працівників підрозділів кіберполіції Національної поліції України за питанням "найбільш дієвих заходів профілактики кібершахрайств"

Як видно з діаграми, найбільш дієвими та продуктивними заходами профілактики кібершахрайствам, як частини загальносоціальної системи запобігання вказаній категорії злочинності, працівники профільних підрозділів протидії кіберзлочинам вважають чотири групи таких заходів.

1. Проведення роз'яснень для населення органами правопорядку отримало 79% від загальної кількості опитаних респондентів. Як загальносоціальний захід запобігання злочинності, вказані профілактичні дії спрямовані на підвищення обізнаності населення, заклик громадян до обачності та перевірки тієї або іншої інформації при поводжені з комп'ютерною технікою.

З кримінологічної точки зору зазначений метод ведення профілактики, належить до заходів інформаційного-виховного і віктимологічного характеру. Залежно від тактики і методології застосовування вказаного заходу, дії щодо підвищення обізнаності населення також можна віднести і до спеціально-кримінологічних методів запобігання кіберзлочинам.

До вказаних заходів, які необхідні з боку саме підрозділів Національної поліції, також належать:

– інформування населення про появу нових випадків шахрайств у мережі Інтернет, або тих що вчиняються з використанням засобів електронних комунікацій, у певних місцях, у певний час і певними категоріями осіб;

– роз'яснення населенню способів захисту власності від кіберзлочинців та кібершахраїв;

– інформування громадян, підприємців і керівників фірм, підприємств про необхідність звертатися до правоохоронних органів при вчинені відносно них шахрайств або інших кіберзлочинів;

– проведення бесід з населенням, особливо з молоддю, про наслідки аморального, протиправного способу життя, вчинення кримінальних правопорушень у мережі Інтернет, а також роз'яснення правової культури використання інноваційних технологій;

– попередження становлення на злочинний шлях осіб, схильних до вчинення малозначних комп'ютерних порушень (Алауханов, 2008, с. 85);

Вказаний метод безумовно має переваги з точки зору ефективності, однак несе у собі недоліки з напрямку його реалізації. По-перше, це недостатність кадрів у підрозділах Національної поліції. Як відомо,

некомплект поліцейських у Національній поліції України на початок 2018 р. становив 15,9 тис. осіб (13,6% від штатного складу) (Українські новини, 2018). По-друге, для проведення профілактичних заходів інформаційно-виховного і віктимологичного характеру з боку правоохоронних органів не визначено цільову аудиторію населення. Тобто окрім частини підприємств, установ і організацій, навчальних закладів неможливо визначити перелік громадян, на яких будуть спрямовані вказані заходи запобігання злочинам.

Додатковим заходом щодо запобігання шахрайствам, які вчиняються шляхом незаконного використання засобів електронних комунікацій 73% опитаних респондентів (працівників профільного підрозділу) вважають проведення роз'яснень населенню підприємствами і банківськими установами. Заходи, спрямовані на інформатизацію населення з боку правоохоронних органів, банківських, державних структур та приватного сектору, мають єдину мету, тому доцільно об'єднати їх до одної групи проведення профілактичних заходів інформаційного-виховного і віктимологичного характеру.

2. Наступним дієвим заходом профілактики кібершахрайствам, на думку 79% опитаних респондентів-працівників підрозділів кіберполіції, є задіяння засобів масової інформації (трансляція документального відеоконтенту, соціальної реклами). Вказані заходи профілактичних дій також доцільно віднести до заходів інформаційного характеру, однак на відміну від виховної роботи і проведення бесід, при вказаному методі використовується соціально-психологічні властивості людської свідомості. Реалізація методу розповсюдження інформаційного контенту, здійснюється шляхом задіяння засобів масової інформації (газети, журнали, телебачення, Інтернет, інформаційні ресурси, офіційні веб-сторінки державних органів влади та підприємств). Правоохоронні органи також можуть приймати участь у подібних заходах через спеціалізовані підрозділи та прес-центри Національної поліції.

3. Введення дисциплін щодо базових знань інформаційної безпеки та "ІТ-культури" (інформаційно-технічної) у закладах середньої (середньо-спеціальної) та вищої освіти не варто відносити до профілактичної діяльності Національної поліції. Вказані заходи відносяться до діяльності іншого соціального інституту, однак є не менш дієвими при запобіганні як кібершахрайствам, так й іншим категоріям злочинів. 60% опитаних кіберполіцейських вважають цей тип запобігання і профілактики ефективним.

Важливим ланцюгом, що сприятиме попередженню кіберзлочинності при навчальних та науково-практичних заходах може стати соціальна профілактика як напрям соціально-педагогічної діяльності. Метою соціальної профілактики є не лише та не стільки попередження розвитку негативних явищ, а створення умов для повноцінного функціонування суспільства та життєдіяльності окремих осіб. Соціально-педагогічна діяльність, як вважає Т. В. Журавель, передбачає обмеження поширення певних негативних явищ, що вже мають місце у суспільстві чи соціальній групі, попередження загострення таких явищ та їх наслідків, запобігання поглибленню соціальної дезадаптації осіб, яким властива девіантна поведінка. Важливо, що профілактичні дії мають бути спрямовані не лише на зміну девіантної поведінки на індивідуальному рівні, а й на обставини, що таку поведінку можуть спричиняти (Журавель, 2013).

Слід зауважити також, що вагомим напрямком впровадження учбових і науково-практичних профілактичних заходів вважається прищеплення знань із сучасної "ІТ-культури". Термін "ІТ-культура" або "інформаційна культура" має свою історію розвитку та різні трактування. У 90-х рр. XX ст. у США і країнах Західної Європи з'явився ряд концепцій інформаційної грамотності, під якою розуміється здатність людини ідентифікувати потреби в інформації, вміння її ефективно шукати, оцінювати і використовувати (Воробьев, 2012).

Крім ефективності використання інформаційних технологій, на нашу думку, "ІТ-культура" має на меті навчання т. зв. комп'ютерному етикету і правовій поведінці при поводжені з електронно обчислювальною технікою або у віртуальному просторі. Тому необхідним є більш активне запровадження дисциплін щодо базових знань інформаційної безпеки та "ІТ-культури" (інформаційно-технічної) у закладах середньої (середньо-спеціальної) та вищої освіти, у т. ч. видання спеціалізованої літератури. Однак вказані дії важко віднести до профілактичних заходів, тому лише 12% опитаних респондентів визнали зазначені заходи ефективними.

4. Далі було запропоновано ряд профілактичних заходів, які не мають на увазі роботу підрозділів Національної поліції, однак можуть також вважатись дієвими загальносоціальними засобами запобігання кібершахрайству. До них належать і проведення соціальних

заходів та акцій (у т. ч. у соціальних мережах Інтернету) (51% опитаних респондентів); контроль та облік осіб, які схильні до вчинення вказаного типу кіберзлочину (58%); удосконалення системи покарання, що передбачена за скоєння кіберзлочинів (76%); повна або часткова зміна роботи правоохоронних органів (36% опитаних респондентів).

Загалом слід зазначити, що загальносоціальною основою запобігання шахрайствам, що вчиняються шляхом використання засобів електронних комунікацій є подолання кризових явищ у країні: в економіці, політиці, суспільній ідеології і психології, соціальній сфері, правоохоронній діяльності. На цій основі перспективними також представляються профілактичні заходи, запропоновані С. В. Горлач:

– усунення, ослаблення чи нейтралізація криміногенних факторів;

– належні організаційно-управлінські заходи запобігання злочинам;

– усунення чи обмеження криміногенних факторів шляхом і в результаті формування в членів суспільства моральної позиції, орієнтованої на базові загальнолюдські цінності;

– установлення контролю за діяльністю засобів масової інформації й естради, що фактично пропагують, усупереч міжнародно-правовим зобов'язанням України, злочинний спосіб життя;

– неприпустимість таких негативних факторів, як соціальна нетерпимість, масові репресії, національна ворожнеча, відхилення від закономірностей суспільного розвитку;

– установлення міждержавного співробітництва на інформаційно-методичному рівні і при проведенні спільних операцій;

– удосконалення правових заходів профілактики розглянутої категорії злочинності (Горлач, 2014).

Отже, загальносоціальне запобігання злочинності – найважливіший аспект соціальної політики. Це соціальна реакція держави і суспільства на злочинність. Загальносоціальне запобігання створює соціально-економічні та культурні підвалини для ефективного здійснення спеціально-кримінологічного і індивідуального запобігання злочинам. Саме вказаний вид запобігання кіберзлочинності створює т. зв. підґрунтя для спеціально-кримінологічних засад діяльності підрозділів Національної поліції, пов'язаної з протидією і профілактикою злочинам у сфері інформаційних технологій.

ЛІТЕРАТУРА

Алауханов, Е.О. (2008). *Криминология.* Алматы.

Афери з банківськими картками: з рахунків українців вкрали сотні мільйонів. *Politeka.* <https://politeka.net/ua/news/401264-afery-s-bankovskimi-kartochkami-so-schetov-ukraintsev-ukrali-sotni-millionov/>

Бабенко, А.Н. (2013). Кіберзлочинність як чинник негативного впливу на криміногенну ситуацію у регіонах. *Безпека інформації,* 19, 2, 112-117.

Воробьев, Г.А. (2012). Информационная культура в развитии информационного общества. *Инновационные информационные технологии*, 1, 514-516.

Голіна, В.В. (2011). *Кримінологія.* Харків: Національний університет "Юридична академія України імені Ярослава Мудрого".

Горлач, С.В. (2014). Загальноспеціальні та спеціально-кримінологічні заходи запобігання насильницькій злочинності в Україні. *Митна справа*, 6 (2.1), 133-139.

Журавель, Т.В. (2013). *Соціальна профілактика як напрям соціально-педагогічної діяльності. Соціальна педагогіка.* Київ: Академвидав.

Кримінальний процесуальний кодекс України, 2012 (Верховна Рада України). *Офіційний сайт Верховної Ради України*. <https://zakon.rada.gov.ua/laws/show/4651-17>

Марков, В.В. (2015). До питання щодо зарубіжного досвіду протидії кіберзлочинності. *Право і Безпека*, 2, 107-113.

Національний банк України: збитки українських банків від незаконних дій з платіжними картками зменшилися вперше з 2015 року. *Офіційне інтернет-представництво Національного банку України.* <https://bank.gov.ua/control/uk/publish/article?art_id=63383127>

У Нацполіції не вистачає 16 тисяч поліцейських. *Українські новини.* <https://ukranews.com/ua/news/545357-u-nacpolicii-ne-vystachaye-16-tysyach-policeyskykh>

Smith, S.S. (2017). *Internet crime report*. <https://pdf.ic3.gov/2017_IC3Report.pdf>

REFERENCES

Afery z bankivskymy kartkamy: z rakhunkiv ukraintsiv vkraly sotni milioniv [Scams with bank cards: hundreds of millions of people were stolen from the accounts of Ukrainians]. *Politeka.* Retrieved from: https://politeka.net/ua/news/401264-afery-s-bankovskimi-kartochkami-so-schetov-ukraintsev-ukrali-sotni-millionov/ [in Ukrainian].

Alauhanov, E.O. (2008). *Kriminologija.* [Criminology]. Almati. [in Russian].

Babenko, A.N. (2013). Kiberzlochynnist yak chynnyk nehatyvnoho vplyvu na kryminohennu sytuatsiiu u rehionakh [Cybercrime as a factor of negative influence on the crime situation in the regions]. *Bezpeka informatsii.* [Information security], *no. 2*, 112-117. [in Ukrainian].

Holina, V.V. (2011). *Kryminolohiia.* [Criminology]. Kharkiv: Natsionalnyi universytet "Iurydychna akademiia Ukrainy imeni Yaroslava Mudroho". [in Ukrainian].

Horlach, S.V. (2014). Zahalnospetsialni ta spetsialno-kryminolohichni zakhody zapobihannia nasylnytskii zlochynnosti v Ukraini [General and special-criminological measures to prevent violent crime in Ukraine]. *Mytna sprava.* [Customs business]*, no. 6(2.1)*, 133-139. [in Ukrainian].

Kryminalnyi protsesualnyi kodeks Ukrainy, 2012 (Verkhovna Rada Ukrayiny). [Criminal Procedural Code of Ukraine, 2012 (Verkhovna Rada of Ukraine)]. *Ofitsiynyy sayt Verkhovnoyi Rady Ukrayiny*. [The official website of the Verkhovna Rada of Ukraine]. Retrieved from: https://zakon.rada.gov.ua/laws/show/4651-17 [in Ukrainian].

Markov, V.V. (2015). Do pytannia shchodo zarubizhnoho dosvidu protydii kiberzlochynnosti [To the issue of foreign experience in combating cybercrime]. *Pravo i Bezpeka.* [Law and Safety], *no*. *2*, 107–113. [in Ukrainian].

Natsionalnyi bank Ukrainy: zbytky ukrainskykh bankiv vid nezakonnykh dii z platizhnymy kartkamy zmenshylysia vpershe z 2015 roku [National Bank of Ukraine: losses of Ukrainian banks from illegal actions with payment cards decreased for the first time since 2015]. *Ofitsiine internet-predstavnytstvo Natsionalnoho banku Ukrainy.* [The official online representation of the National Bank of Ukraine]. Retrieved from: https://bank.gov.ua/control/uk/publish/article?art_id=63383127 [in Ukrainian].

Smith, S.S. (2017). *Internet crime report.* Retrieved from: https://pdf.ic3.gov/2017_IC3Report.pdf

U Natspolitsii ne vystachaie 16 tysiach politseiskykh [Ukrainian news. In the National Police there are not enough 16 thousand policemen]. *Ukrainski novyny.* [Ukrainian news]. Retrieved from: https://ukranews.com/ua/news/545357-u-nacpolicii-ne-vystachaye-16-tysyach-policeyskykh [in Ukrainian].

Vorob'ev, G.A. (2012). Informacionnaja kul'tura v razvitii informacionnogo obshhestva [Information culture in the development of the information society]. *Innovacionnye informacionnye tehnologii.* [Innovative information technology]*, no. 1*, 514-516. [in Russian].

Zhuravel, T.V. (2013). *Sotsialna profilaktyka yak napriam sotsialno-pedahohichnoi diialnosti. Sotsialna pedahohika.* [Social prevention as a direction of social and pedagogical activity. Social pedagogy]. Kyiv: Akademvydav. [in Ukrainian].

АНОТАЦІЯ

Лефтеров Л. В. Загальносоціальні заходи запобігання шахрайству, що вчиняється шляхом використання засобів електронних комунікацій. – Стаття.

У статті розглядаються актуальні питання протидії кіберзлочинам. Особливу увагу приділено незаконним операціям із заволодіння майна шляхом обману або зловживання довірою, механізм здійснення яких неможливий без використання електронно-обчислювальної техніки. Зокрема, проводиться комплексне дослідження заходів протидії даної категорії злочинів. Наведено результати спеціального кримінологічного дослідження, яке передбачене соціологічними методиками, – анкетування профільної аудиторії респондентів. Кримінологічною основою дос-

лідження є питання загально-соціальних заходів запобігання шахрайству, що вчиняється з використанням електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж або мереж електрозв'язку. Також розглядаються основні аспекти роботи підрозділів Національної поліції України у сфері протидії кіберзлочинам.

Ключові слова: кіберзлочинність, кримінологія, комп'ютерні злочини, загальносоціальні заходи, запобігання кібершахрайству, кіберполіція, Національна поліція, електронні комунікації.

АННОТАЦИЯ

Лефтеров Л. В. Общесоциальные меры предотвращения мошенничества, совершаемого путем использования средств электронных коммуникаций. – Статья.

В статье рассматриваются актуальные вопросы противодействия киберпреступности. Особое внимание уделено незаконным операциям по завладению имуществом путем обмана или злоупотребления доверием, механизм осуществления которых невозможен без использования электронно-вычислительной техники. В частности, проводится комплексное исследование мер противодействия данной категории преступлений. Приведены результаты специального криминологического исследования, предусмотренного социологическими методиками, – анкетирования профильной аудитории респондентов. Криминологической основой исследования является вопрос общесоциальных мер предупреждения мошенничества, совершаемого с использованием электронно-вычислительных машин (компьютеров), автоматизированных систем, компьютерных сетей или сетей электросвязи. Также рассматриваются основные аспекты работы подразделений Национальной полиции Украины в сфере противодействия киберпреступности.

Ключевые слова: киберпреступность, криминология, компьютерная преступность, общесоциальные меры, предотвращение кибермошенничества, киберполиция, национальная полиция, электронные коммуникации.