УДК 343.92

КРИМІНОЛОГІЧНИЙАНАЛІЗ ШАХРАЙСТВ, УЧИНЕНИХ ІЗ ВИКОРИСТАННЯМ КОМП'ЮТЕРНИХ МЕРЕЖ

CRIMINOLOGICAL ANALYSIS OF FRAUDS COMMITTED WITH THE USE OF COMPUTER NETWORKS

Лефтеров Л.В.
ад'юнкт кафедри кримінального права та кримінології Одеського державного університету внутрішніх справ

Проведено кримінологічний аналіз шахрайств, скоєних із використанням комп'ютерних мереж. З'ясовано, що специфіка кіберзлочинів полягає в технічних аспектах, динаміці проникнення та доступності Інтернету. Визначено чинники й умови вчинення кібершахрайств, а також основні складники, які впливають на зниження рівня кіберзлочинності.
Ключові слова: кримінологічний аналіз, шахрайства, комп'ютерні мережи, Інтернет, кіберзлочинність.

Проведен криминологический анализ мошенничеств, совершенных с использованием компьютерных сетей. Выяснено, что специфика киберпреступлений заключается в технических аспектах, динамике проникновения и доступности Интернета. Определены факторы и условия совершения кибермошенничества, а также основные составляющие, которые влияют на снижение уровня киберпреступности.
Ключевые слова: криминологический анализ, мошенничества, компьютерные сети, Интернет, киберпреступность.

Criminological analysis of frauds committed with the use of computer networks was carried out. It is revealed that the specificity of cybercrime is in the technical aspects, the dynamics of penetration and the availability of the Internet. The factors and conditions of cybercrime committing, as well as the main components that influence the reduction of cybercrime, are determined.
Key words: criminological analysis, frauds, computer networks, Internet, cybercrime.

Постановка проблеми. В епоху високих інформаційних технологій, використання електронних пристроїв, програмних продуктів, персональних комп'ютерів та складних комп'ютерних комплексів, спрямованих на вдосконалення та полегшення життя людини, є одним із найпоширеніших явищ. За даними Організації Об'єднаних Націй (далі – ООН), у 2011 р. щонайменше 2,3 мільярди людей, або більше однієї третини від загальної чисельності населення планети, мали доступ до Інтернету [1]. 2018 р. доступ до мобільного широкосмугового Інтернету отримали вже майже 70% від загальної кількості населення світу. Тому стан злочинності в кіберпросторі є однією з найбільш актуальних суспільних і наукових проблем. Кіберзлочинність становить загрозу для безпеки всіх сфер життєдіяльності суспільства, завдає шкоди господарському сектору, негативно впливає на соціальний та економічний розвиток держави, загрожує основам національної безпеки України.

Особливе місце серед кіберзлочинів посідає шахрайство, що вчиняється з використанням електронно обчислювальних машин (далі – ЕОМ) та комп'ютерних мереж. Показники скоєння злочинів цієї категорії кожного року збільшуються, а методи, способи та механізм підготовки і реалізації злочинних схем стають все більш складними. Тенденції злочинності, на яких ґрунтується сучасна кримінологічна теорія і практика, не повною мірою враховують технічний, соціальний та психологічний складники кіберзлочинності. Саме цей факт впливає на ускладнення криміногенної ситуації в Україні, зумовлює пошук та винайдення нових заходів запобігання кіберзлочинності. Удосконалення системи протидії та запобігання шахрайствам, скоєним із використанням комп'ютерних технологій, можливе лише на основі комплексних знань про основні закономірності функціонування, поширення та детермінації злочинності на регіональному, державному та міжнародному рівнях.

Метою статті є проведення кримінологічного аналізу шахрайств, що вчиняються з використанням ЕОМ і комп'ютерних мереж, вивчення чинників та умов скоєння кібершахрайств, а також визначення основних складників, які впливають на рівень кіберзлочинності.

Виклад основного матеріалу. За даними української міжбанківської асоціації членів платіжних систем ЕМА, 2016 р. від інтернет-шахрайства постраждав кожен сотий власник платіжних карт в Україні, а «дохід» від незаконних дій становив майже 340 мільйонів гривень (11,2 мільйони євро) [2]. Дана статистика свідчить про недостатнє вивчення кримінологічних особливостей зазначеної категорії злочинів, а також недосконаліть українського законодавства, яке все ще перебуває на етапі адаптації до сучасних тенденцій інформаційно-технічного розвитку.

Шахрайство, скоєне з використанням електронно-обчислювальної техніки, є як видом кіберзлочину, так і вагомою частиною загальної злочинності. Відповідно до ч. 3 ст. 190 Кримінального кодексу (далі – КК) України, шахрайство, вчинене шляхом незаконних операцій із використанням електронно-обчислювальної техніки, передбачає покарання у вигляді позбавлення волі на строк від трьох до восьми років [3]. Зазначена норма повною мірою дає кримінально-правове визначення діям, які належать до кіберзлочинності.

Нами досліджені абсолютні показники кількості зареєстрованих шахрайств, які належать до категорії кіберзлочинів. Аналіз інформації проводився згідно з офіційними даними статистики Генпрокуратури України у вигляді єдиного звіту про кримінальні правопорушення, зареєстровані в Єдиному реєстрі досудових розслідувань (далі – ЄРДР) на території України у 2013–2018 рр. [4]. Так, встановлено, що із січня 2013 р. по червень 2018 р. на території України зафіксовано і внесено до ЄРДР 19 654 фактів шахрайства, скоєного з використанням електронно-обчислювальної техніки (злочини, які передбачені ч. 3 ст. 190 КК України).

Новизна даного виду злочинності та методи скоєння таких шахрайств зумовили відсутність статистичних даних за більш тривалий період часу, що, у свою чергу, виключає можливість якісного відстеження динаміки злочинності за роками. Якщо детально вивчити зміни показників, то можна встановити науково з'ясовні закономірності (рис. 1).

2013 р. на території України зафіксовано і внесено до ЄРДР 3 320 фактів, з яких встановлені особи й оголошено про підозру за 1 047 кримінальними провадженнями.

2014 р. зафіксовано і внесено до ЄРДР 2 740 фактів, з яких встановлені особи й оголошено про підозру за 1 241 кримінальним провадженням.

2015 р. зареєстровано 3 633 кримінальних проваджень, з яких розкрито 1 318 злочинів. У 2016–2017 рр. на території України відкрито 3 578 і 4 808 кримінальних проваджень відповідно, за якими оголошено про підозру у 2016 р. за 878 випадками, у 2017 р. за 2 103 провадженнями. Станом на 1 червня 2018 р. (за 5 місяців) виявлено та зареєстровано 1 575 кримінальних проваджень, з них розкрито 557 злочинів [4].

Як бачимо з вище наведених показників, кількість розкритих злочинів значно нижче кількості зареєстрованих. Даний факт не є аномальним, оскільки злочинність здебільшого перебуває «на крок попереду» щодо правоохоронної діяльності. Головною особливістю динаміки комп'ютерного шахрайства в Україні є його поступове збільшення 2018 р. порівняно із 2013 р., але не по прямій, а по кривій лінії, що наочно спостерігається на рис. 1. Таке збільшення пов'язано з тимчасовим зниженням злочинності у 2014 і 2016 рр.

Ще одним статистичним показником кримінологічного дослідження кібершахрайств є кількість злочинів, скоєних у складі груп. 2013 р. оголошено про підозру за 145 кримінальними провадженнями, за злочинами, скоєними в складі групи (попередня змова осіб, у складі організованої злочинної групи або організації). 2014 р. пред'явлено підозру за 57 кримінальними провадженнями. 2015 р. виявлено 182 таких злочинів, 2016 р. – 130, 2017 р. – 246 кримінальних проваджень. За 5 місяців 2018 р. оголошено про підозру за 42 кримінальними провадженнями, за кіберзлочинами, скоєними в складі групи (рис. 2). Даний показник також, як і попередні статистичні дані, має динаміку поступового, але нелінійного зростання.

Для виявлення регіональних показників кібершахрайства проаналізована статистика за справами, зареєстрованими в ЄРДР 2017 р., за кожною адміністративно-територіальною одиницею України (крім тимчасово окупованих регіонів). Встановлено, що основна частка кіберзлочинності припадає на територію міста Києва (650 кримінальних проваджень) і Одеської області (638 кримінальних проваджень). Крім того, багато шахрайств із використанням електронно-обчислювальної техніки зафіксовано в Запорізької області (368 кримінальних проваджень), а також у Миколаївській (337), Харківській (207), Дніпропетровській (204) і Львівській областях (148) [4].

Різниця в рівні структури і динаміки злочинності невипадкова. Це пов'язано з демографічними, економічними, соціальними, культурними, організаційними, національними, екологічними, правовими, реєстраційними й іншими особливостями тієї чи іншої місцевості (етнічний склад населення, проживання більшості населення регіону в містах чи селах тощо). Тому, як зазначають В.М. Кудрявцев та В.Є. Емінов, вивчення географії злочинності має велике значення для порівняльної кримінології під час аналізу причин злочинності й її змін, для вироблення ефективних заходів її попередження в окремих регіонах і на територіях [5, с. 233].

Так, беручи до уваги демографічний чинник, можна зробити висновок, що на динаміку злочинності даної категорії впливають передусім кількість і щільність населення окремо взятого регіону. Згідно з даними Державної служби статистики, середня чисельність населення в м. Києві 2017 р. становила 2 930 141 осіб, без урахування міграцій і осіб, які тимчасово відвідували столицю України [6].

Рис. 1. Показники кількості шахрайств, скоєних із використанням електронно-обчислювальної техніки

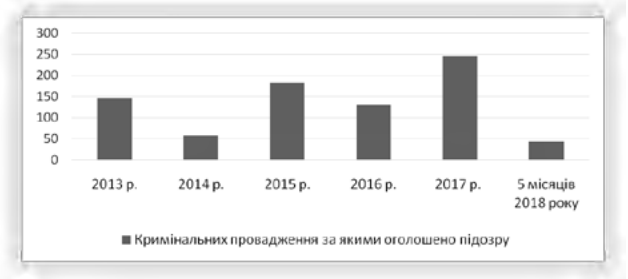

Рис. 2. Кількість кіберзлочинів, скоєних у складі злочинних груп

В Одеській області 2017 р. постійна чисельність населення становила 2 384 796 осіб, а також понад 2,2 мільйона осіб, які відвідали регіон у курортний період і міжсезоння [7]. Крім того, у даних регіонах наявний підвищений рівень застосування Інтернету в багатьох сферах економічної та повсякденної діяльності.

Суттєвим чинником, який впливає на кіберзлочинність в Україні, є Інтернет, що виступає основним знаряддям комп'ютерного шахрайства. 2018 р. Інтернет-асоціацією України (ІнАУ) спільно з холдингом Factum Group Ukraine проведено дослідження репрезентативного населення України віком від 15 років і старше. За результатами проведених досліджень установлено, що динаміка проникнення Інтернету має показники, за якими 65% населення (21,35 млн) станом на 2018 р. є регулярними користувачами мережі Інтернет, у 67% населення (21,9 млн) підключено домашній Інтернет [8].

Чинником, який також впливає на злочинність даної категорії, є мобільність доступу до мережі. Так, 57% інтернет-користувачів використовують для доступу мобільний телефон або смартфон; 45% – домашній переносний персональний комп'ютер; 39% – стаціонарний персональний комп'ютер; 15% – планшетний персональний комп'ютер; 10% – робочий комп'ютер [8].

На думку А.Ф. Зелінського, «порівняно низький коефіцієнт злочинності в Україні – це результат насамперед винятково високої латентності (прихованості) злочинів і погано поставленого обліку» [9, с. 111]. Отже, поглиблене кримінологічне дослідження шахрайств, скоєних із використанням комп'ютерних мереж, неможливе без аналізу такого додаткового показника, як латентність злочинності.

Щодо встановлення показників конкретних видів латентної злочинності, то ефективність статистичних методів дещо зменшується. Ефективними методами виявлення латентних економічних злочинів є соціологічні методи. Ті ж самі методи можна застосовувати в дослідженні латентності кібершахрайств. У сучасних умовах активного розвитку інформаційних технологій також потрібно всілякo використовувати можливості глобальної мережі Інтернет для виявлення латентних злочинів (наприклад, розміщувати відповідні опитування користувачів мережі).

Усі наведені статистичні дані не є точними і відображають лише загальну картину криміногенної обстановки в Україні. Крім того, не враховано дані про злочини, про які не було проінформовано правоохоронні органи завчасно. Є низка причин, за якими потерпілі можуть не заявляти в органи правопорядку про скоєні щодо них шахрайства з використанням електронно-обчислювальної техніки. Цей факт є заважає розкриттю кібершахрайств. Причинами такого становища, на нашу думку, є особливі обставини, пов'язані з низкою економічних, політичних і територіальних детермінант. Серед них можна назвати рівень довіри до органів влади. За результатами соціологічного дослідження, проведеного 2017 р. соціологічною компанією Taylor Nelson Sofres (TNS) на тему «Ставлення населення до реформи поліції в Україні», виявлено, що поліція характеризується досить високим рівнем довіри порівняно з іншими соціальними інститутами й організаціями. 2017 р. зросла довіра до національної поліції, а також до засобів масової інформації [10].

Значний вплив на високий рівень латентності кіберзлочинності загалом та відмову потерпілих громадян від офіційного звернення до органів правопорядку є особливий момент, який, на нашу думку, був неврахований у дослідженнях щодо «довіри до поліції». Це психологічний та соціальний стан кожного окремого громадянина, який став жертвою кібершахрайства. Ідеться про стан потерпілого від комп'ютерного шахрайства, в якому він сам дає оцінює власну поведінку або дії, наслідками яких стали обман, зловживання довірою та завдання шкоди постраждалому. Так званий «позор», думки потерпілого про свою віктимність, недосвідченість, наївність, нездатність орієнтуватися в умовах розвитку соціуму стримують від оприлюднення факту ошуканості, зокрема від звернення до правоохоронних органів. Вілдсутність звернення також зумовлена ситуацією, коли завданий жертві збиток, як вважає С.В. Молчанов, не відповідає моральним витратам, які на неї очікують під час офіційного розгляду звернення до органів Національної поліції [11].

Серед потерпілих від шахрайства з використанням електронної обчислювальної техніки найбільше осіб середнього віку. В основному це категорія найактивніших інтернет-користувачів віком від 25 до 50 років. Також чимала частка потерпілих припадає на вікову категорію вище 50 років, у зв'язку з низьким рівнем знань у тій чи іншій технічній сфері (пенсіонери, дорослі люди не мають достатнього рівня обізнаності про високі інформаційні технології та методи захисту в мережі Інтернет).

Кіберзлочини є одними з найскладніших діянь щодо підготовки, скоєння, методів і тактики документування їх правоохоронними органами. Якщо об'єднати зазначені складності з механізмами обману і зловживання довірою, передбачені шахрайством, в арсенал кіберзлочинців надходить незліченна кількість способів для здійснення незаконних дій із використанням комп'ютерної техніки, спеціальних технічних інструментів для роботи з платіжними даними, а також Інтернету. Проведений нами аналіз дозволив визначити основні складники, які впливають на тимчасові зниження рівня кіберзлочинності, а саме:

– правові та законодавчі складники. На боці протидії кіберзлочинності перебуває ціла державна система у вигляді законодавчої і виконавчої гілок влади, зі своїми нормами права (спрямованими на протидію злочинам і сприяння боротьбі з кіберзлочинами). Чинником стримування злочинності є навіть малі зміни в правових нормах або в процесах реформування державних органів (зокрема, утворення 2015 р. підрозділу кіберполіції Національної поліції України, створення спеціальних відділів протидії кіберзлочинності в структурі Служби безпеки України);

– приватний сектор і банківська система, які також надають підтримку в боротьбі з кібершахрайством у межах своїх прав. Контролювання фінансових потоків відіграє не останню роль, особливо щодо шахрайств, скоєних із використанням систем віддаленого банківського обслуговування;

– профілактика і досвід. Основним чинником, який виключає можливість комп'ютерних шахраїв довгий час використовувати ті самі способи вчинення злочинів, є профілактика, набутий підрозділами Національної поліції (іншими органами правоохоронної спрямованості) досвід, проведення бесід, оприлюднення проблеми в засобах масової інформації тощо. Так само не малу роль відіграють процесуальні та правові прецеденти, які використовуються під час розслідування і документування кримінальних правопорушень органами досудового розслідування Національної поліції України, прокуратури й оперативними підрозділами з боротьби з кіберзлочинністю.

Зазначимо, що швидке вирішення проблем кіберзлочинності неможливе, проте оптимізація роботи з боротьби як з даним видом шахрайства, так і з кіберзлочинністю загалом є першочерговим завданням держави. Йдеться про зміни в законодавстві (конституційна, адміністративна, кримінальна, цивільна і господарська галузі права), а також остаточна реорганізація і створення додаткових органів із контролю, убезпечення, протидії правопорушенням у сфері високих інформаційних технологій.

Висновки. Шахрайство, скоєне з використанням електронно-обчислювальної техніки, справді істотно впливає на економіку держави загалом, відображає рівень економічної безпеки приватного сектора, банківської та фінансової системи тощо. Розвиток кіберзлочинності і її кримінологічні особливості дуже сильно відрізняються від

злочинності загальнокримінальної спрямованості. Зростання кількості шахрайств із використання комп'ютерних мереж залежить від збільшення ступеня проникнення високих інформаційно-програмних технологій у повсякденне життя населення України. Крім того, підвищення кваліфікації правоохоронних органів (спеціальних підрозділів із боротьби з кіберзлочинністю), удосконалення методів протидії, досвід, профілактика породжують необхідність винаходу злочинцями все нових видів кібершахрайства.

Проведений кримінологічний аналіз шахрайств, скоєних із використанням комп'ютерних мереж, засвідчив поступове, хоча і нелінійне, зростання комп'ютерного шахрайства в Україні останнім часом. Установлено, що основна частка кіберзлочинності припадає на територію міста Києва й Одеської області. Зазначені злочини, як і більшість інших, загалом пов'язані з демографічними, економічними, соціальними, культурними, організаційними, правовими й іншими особливостями тієї чи іншої місцевості. Але специфіка кіберзлочинів полягає в технічних аспектах, динаміці проникнення та доступності Інтернету. Крім того, наявність латентної кіберзлочинності зумовлює психологічну обстановку безкарності таких суспільно небезпечних діянь, що спричиняє поширення злочинної діяльності з використанням ЕОМ і комп'ютерних мереж.

Особи, які постраждали від шахрайств, скоєних із використанням комп'ютерних мереж, мають загальні типологічні риси й особливості, тому надалі для запобігання зазначеним видам злочинів необхідний більш ґрунтовний кримінологічний та соціально-психологічний аналіз потерпілих від кіберхшахрайства.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Киберпреступность: проблемы борьбы и прогнозы. URL: http://cripo.com.ua/processes/?p=164985/.

2. Статут Української міжбанківської Асоціації членів платіжних систем «ЄМА»: затверджений рішенням конференції 2006 р. м. К. С. 21.

3. Кримінальний кодекс України: Закон від 5 квітня 2001 р. № 2341–II. Відомості Верховної Ради України. 2001. № № 25–26. Ст. 131.

4. Про зареєстровані кримінальні правопорушення та результати їх досудового розслідування: статистична інформація Генпрокуратури України. URL: https://www.gp.gov.ua/ua/stat.html.

5. Криминология: учебник / под ред. В.Н. Кудрявцева, В.Е. Эминова. М.: Юрист, 2004. 734 с.

6. Дані Головного управління статистики в м. Києві. URL: http://kiev.ukrstat.gov.ua/p.php3?c=3216&lang=1.

7. Дані Головного управління статистики в Одеській області. URL: http://od.ukrstat.gov.ua/arh/demogr/demogr1_2017.htm.

8. Результати дослідження «Проникновение интернета в Украине» // Factum Group Ukraine. 2018. URL: https://inau.ua/proekty/doslidzhennya-internet-audytoriyi.

9. Зелинский А.Ф. Криминология: учеб. пособие. Харьков: Рубикон, 2000. 187 с.

10. Результати дослідження «Ставлення населення до реформи поліції в Україні». URL: https://www.slideshare.net/MIA_Ukraine/ss-74067458.

11. Молчанов С.В. Мораль справедливости и мораль заботы: зарубежные и отечественные подходы к моральному развитию. Вестник Московского университета. Серия 14 «Психология». 2011. № 2. С. 59–72.