ЮРИДИЧНА ПСИХОЛОГІЯ ТА ПЕДАГОГІКА. ПСИХОЛОГІЧНЕ ЗАБЕЗПЕЧЕННЯ ПРАВООХОРОННОЇ ДІЯЛЬНОСТІ

УДК 343.3/.7:004

П.П. Підюков,
доктор юридичних наук, професор,
заслужений юрист України,
О.С. Дронова,
кандидат психологічних наук,
Є.О. Варлакова,
кандидат психологічних наук

ПРОТИДІЯ КІБЕРЗЛОЧИННОСТІ – ЗАПОРУКА ЕКОНОМІЧНОЇ БЕЗПЕКИ СУСПІЛЬСТВА ТА ДЕРЖАВИ В УМОВАХ ЄВРОІНТЕГРАЦІЇ: ПСИХОТЕХНОЛОГІЧНІ Й ПРАВОВІ АСПЕКТИ

Стаття присвячена проблемі протидії кіберзлочинності в мережі Інтернет. Перелічені причини та види кіберзлочинів, ознаки шахрайства в мережі Інтернет. Запропоновані правила безпеки при роботі в мережі та прийоми протидії Інтернет-шахрайству в ситуаціях загрози безпеці дитини. Надані рекомендації щодо запобігання шахрайським проявам в мережі Інтернет.

Ключові слова: *кіберзлочинність, причини та види кіберзлочинів, ознаки шахрайства в мережі Інтернет, правила безпеки при роботі в мережі, дитяча безпека в мережі Інтернет, рекомендації щодо запобігання шахрайським проявам у мережі Інтернет.*

Статья посвящена проблеме противодействия киберпреступности в сети Интернет. Перечисленные причины и виды киберпреступлений, признаки мошенничества в сети Интернет. Предложены правила безопасности при работе в сети и приемы противодействия Интернет-мошенничеству в ситуациях угрозы безопасности ребенка. Даны рекомендации по предотвращению мошеннических проявлений в сети Интернет.

Ключевые слова: *киберпреступность, причины и виды киберпреступлений, признаки мошенничества в сети Интернет, правила безопасности при работе в сети, детская безопасность в сети Интернет, рекомендации по предотвращению мошеннических проявлений в сети Интернет.*

Paper is devoted to the problem of cybercrime in Internet. Causes and types of cyber crimes as well as the signs of fraud in Internet are stated. Safety rules in the network as well as the ways of counteraction to Internet fraud in the situations of the threat to the security of a child are suggested. Recommendations for the prevention of fraudulent manifestations in Internet are given.

Keywords: *cybercrime, causes and types of cyber crime, signs of fraud in Internet, safety rules in the network, children's safety in Internet, how to prevent fraudulent manifestations in Internet.*

На сьогодні проблема профілактики у сфері протидії злочинності з використанням комп'ютерних технологій набуває все більшої актуальності, привертаючи до себе увагу науковців і практиків, зокрема, В.В. Засанського, Т.Т. Ковальчука, О.Є. Користіна, В.А. Предборського, В.Л. Смагіна, В.І. Франчука, Є.В. Хлобистова, С.С. Чернявського та ін. Вони констатують, що величезний технічний потенціал і безмежні можливості та стрімкий розвиток світової інформатизації все частіше використовуються окремими особами з корисною метою. Створюються сприятливі передумови для вчинення злочинів новими високотехнологічними методами та засобами, дії кіберзлочинців стають дедалі майстернішими. Це становить не тільки реальну проблему для громадян і українського суспільства, але в багатьох випадках ставить під загрозу економічну і навіть національну безпеку країни, що викликає, зокрема, необхідність розробки новітніх комп'ютерних систем і технологій з підвищеним рівнем захисту та безпеки в мережі Інтернет, удосконалення законодавчої бази тощо. Втім, якщо детально проаналізувати кримінальні провадження, предметом яких є розслідування шахрайських дій, виявляється, що левова частина фізичних і юридичних осіб, що фігурують як постраждалі від шахраїв-комбінаторів, мала змогу уникнути такої сумної ролі [1, с. 14].

Наголосимо, що досвідчені аферисти – глибокі знавці людської психології. "Низка фахівців, – наголошує, наприклад, Г. Карпюк, – говорять про те, що нинішні соціально-політичні потрясіння в Україні призвели до практично неконтрольованого збільшення кількості шахраїв, які вміло заробляють, маніпулюючи найкращими людськими почуттями – співпереживанням, прагненням долучитися до доброї справи, інколи просто "тиснучи" на "жалібну" кнопку, що є в будь-кому з нас, активно використовуючи для цього Інтернет та інші можливості "кримінально-соціального інжинірингу" [1, с. 16].

Зазначене вище спонукало авторів цієї публікації проаналізувати сутність і механізми кіберзлочинності й шахрайства в мережі Інтернет, зорієнтувати пересічних громадян на вміле виявлення ознак та запобігання таким ганебним протиправним проявам, що безумовно сприятиме і зміцненню економічної безпеки нашої держави, прискорить процес її євроінтеграції [2].

Зазначимо, насамперед, що за своєю сутністю кіберзлочинність – це злочинність в так званому "віртуальному просторі". Віртуальний простір (або кіберпростір) можна визначити як модельований за допомогою комп'ютера інформаційний простір, в якому містяться відомості про осіб, предмети, факти, події, явища і процеси, представлені в математичному, символьному або будь-якому іншому вигляді, які знаходяться в процесі руху по локальних і глобальних комп'ютерних мережах, або відомості, що зберігаються в пам'яті будь-якого фізичного чи віртуального пристрою, а також іншого носія, спеціально призначеного для їх зберігання, обробки і передачі.

На відміну від традиційних видів злочинів, таких як вбивство або крадіжка, кіберзлочинність – явище відносно нове, яке виникло з появою мережі Інтернет. Слід мати на увазі, що сама природа мережі Інтернет є досить простою й сприятливою для протиправного використання. Такі її властивості, як: глобальність, транснаціональність, охоплення широкої аудиторії, анонімність користувачів, розподіл основних вузлів мережі і їх взаємозамінюваність – створюють шахраям, які використовують Інтернет, сприятливі умови для скоєння злочинів, а також дозволяють ефективно ухилятися від правоохоронних органів та відповідальності за скоєне.

Кіберзлочини – це суспільно-небезпечні діяння, які певним чином пов'язані з кіберпростором та комп'ютерною інформацією, що моделюється комп'ютерами. Причинами їх виникнення є:

1) прибутковість, адже кіберзлочинність – неймовірно прибуткова; величезні суми грошей з'являються в кишенях злодіїв у результаті глобальних фінансових афер, не кажучи вже про невеликі, але регулярні грошові суми, що незаконно надходять до них;

2) певна відсутність ризику, оскільки у віртуальному світі зловмисники зазвичай не бачать своїх жертв, а грабувати тих, до кого не можеш "дотягтися рукою", завжди набагато простіше.

Фахівці виділяють такі різновиди кіберзлочинності:

а) традиційні кіберзлочини, що вчиняються за допомогою комп'ютерних технологій та Інтернету (шахрайство з використанням ЕОМ, незаконне збирання відомостей, що становлять комерційну таємницю, шляхом несанкціонованого доступу до комп'ютерної інформації і т.д.);

б) нові злочини, що стали можливі завдяки новітнім комп'ютерним технологіям [3].

Найчастіше з використанням комп'ютера та Інтернет-мережі вчиняються такі традиційні кіберзлочини:

- порушення авторського права і суміжних прав;
- шахрайства;
- незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, обладнанням для їх виготовлення;
- ухилення від сплати податків, зборів (обов'язкових платежів);
- ввезення, виготовлення, збут і розповсюдження порнографічних предметів;
- незаконне збирання з метою використання відомостей, що становлять комерційну чи банківську таємницю.

Другий різновид кіберзлочинності – нові злочини – можна систематизувати таким чином: шахрайства з пластиковими картками; несправжні Інтернет-аукціони; шахрайства з банківськими кредитами; пошук та використання "проривів" (похибок) у програмах; розсилка фіктивних листів (спам); азартні ігри в он-лайн середовищі; викуп та реєстрація доменних імен (кіберсквотинг); крадіжка послуг (фоункрейкинг); створення вірусів; крадіжка інформації та особистих даних; викладення в електронних ЗМІ неправдивих новин [3].

Особливо небезпечними для населення серед нових кіберзлочинів є шахрайства в мережі Інтернет. Останнім часом вони набирають помітних обертів, кількість ошуканих і постраждалих від них неухильно зростає. Тому одним із найбільш простих та ефективних засобів профілактики кіберзлочинності є широка інформатизація суспільства щодо її характерних ознак, а також відповідні пильність і обачливість кожного пересічного громадянина, які б мінімізували можливість його попадання в шахрайські тенета. З цією метою вважаємо за доцільне навести найбільш типові ознаки шахрайських дій, за наявності яких громадяни можуть зрозуміти чи помітити, що їх прагнуть ошукати. Зокрема, йдеться про інтернет-оголошення з фіктивними пропозиціями (про роботу, вигідні покупки, інвестиції, участь у бізнес-проекті, пошук супутника життя тощо), які називають спамами.

По-перше, варто пам'ятати, що жодна серйозна організація не буде доходити до того, щоб ділові пропозиції робити у вигляді спамів. Їй просто цього не потрібно – по-справжньому вигідні та перспективні проекти нав'язливої реклами не потребують.

Якщо ж лист (чи оголошення) має велику кількість граматичних, орфографічних, стилістичних та інших помилок, це взагалі може свідчити про те, що його складала або неосвічена, або просто безвідповідальна людина. У разі отримання вами такого безграмотного листа у відповідь на ваше звернення, ймовірніше, що воно згенероване автовідповідачем. Тобто зловмисник навіть не намагається прочитати, що ви йому написали, а просто інформує вас про те, скільки і куди

треба перерахувати грошей (детально надаючи інформацію про "крутизну" фірми, про майбутні астрономічні прибутки тощо).

Оголошення (пропозиція) може стосуватись і вашої майбутньої роботи з обіцянкою дуже сприятливих умов та оплати праці, іноді з підтвердженням цього начебто відсканованими копіями "чеків" із вражаючими сумами, наголошенням на тому, що така робота нібито займатиме небагато часу, не вимагатиме спеціальної освіти чи підготовки, буде легкою і приємною. Єдиний критерій – вік від 16 до 60 років (чи взагалі не обмежений), при цьому шахраї можуть робити акцент на тому, що їх пропозиція буде особливо цікава лікарям, вчителям, викладачам, військовим та представникам інших професій із традиційно невисоким рівнем заробітку, з можливістю роботи "на дому" та наведенням її переваг: мовляв, навіщо вставати кожен ранок по дзвінку будильника – спіть скільки забажаєте та працюйте за вільним графіком; навіщо чекати чергову відпустку – адже набагато краще відпочивати тоді, коли вам хочеться, а не коли керівник вирішить вас відпустити; навіщо принижуватися перед керівництвом, випрошуючи відгул, краще самостійно планувати свій час і т. ін.

По-друге, будь-яка пропозиція неодмінно міститиме прохання перерахувати (перевести, заплатити тощо) певну суму за вказаними реквізитами під тим чи іншим приводом, залежно від того, що саме Вам пропонують (це може бути "плата за реєстрацію", "застава як підтвердження порядності", "інвестиції під високі відсотки", переведення грошей на "вільний гаманець", "аванс під вигідну покупку", "ставка на участь у грі" тощо). У будь-якому випадку обґрунтування платежу значення не має, важливо пам'ятати інше: якщо в пропозиції, рекламі, що надійшла до Вас через Інтернет, тощо, міститься вимога чи прохання перевести гроші – це однозначно "лохотрон".

Як правило, шахраї просять перерахувати гроші на електронний гаманець WebMoney (найчастіше), Яндекс-Гроші чи інші електронні платіжні системи. Це зумовлено тим, що при банківському чи поштовому переказі шахрая можна "вирахувати", а електронні платіжні системи гарантують повну анонімність.

По-третє, шахрайські пропозиції характеризуються тим, що в них, як правило, відсутні координати та контактні дані. Максимум, що вони надають, – електронну поштову адресу, іноді – сайт. Інакше кажучи, ні фірма, ні віртуальне казино, ні інтернет-магазин, ні "інвестиційний фонд" своєї адреси та сайту не мають. Навіть мобільний телефон (не кажучи вже про міський) зловмисники давати бояться. Якщо в оголошенні все ж присутня якась поштова адреса – це або абонентська скринька, або фальшива адреса, якої взагалі не існує, чи за якою розташована абсолютно стороння організація, яка не має до шахраїв жодного відношення. Слід врахувати й те, що фальшива адреса може бути наведена з хитрощами: наприклад, шахраї вказують досить реальну поштову адресу, вулицю, а от номер будинку – вигаданий, такий, що ненабагато відрізняється від реального. Зокрема, якщо на вулиці останній номер будинку 43, то шахраї можуть вказувати в оголошенні неіснуючий будинок № 44. Такий нехитрий прийом інколи дозволяє ввести в оману навіть тих із потенційних жертв, які непогано знають район (і це цілком природно – навряд чи Ви знаєте останній номер будинку на вулиці, де живете чи працюєте). Іноді навіть номер будинку шахраями вказується вірно, але до нього додається неіснуючий корпус чи будівля.

Якщо в шахрайській пропозиції є посилання на веб-сайт компанії – то не виключено, що цей сайт знаходиться на безкоштовному хостінгу, а якщо на платному, то строк його оренди досить мінімальний, як і розмір оплати. Чи не надто парадоксальним уявляється той факт, що "відома фірма зі світовим іменем", "успішне онлайн-казино", "Інтернет-магазин з багатомільйонними прибутками", "великий інвестиційний фонд" чи інші "рога та копита" не мають навіть 15–20 дол. США, щоб орендувати більш-менш пристойну хостінг-площадку.

По-четверте, шахрайські сайти, як правило, розробляються наспіх, містять мінімум інформації, практично не мають дизайну, нерідко складаються всього з 1-2 сторінок.

По-п'яте, на підтвердження своєї "порядності" шахраї можуть пред'явити електронні копії різних "сертифікатів". Як правило, основні реквізити на цих "сертифікатах" є нерозпізнаними. Це може стосуватися серії та номера документа, дати його видачі, найменування організації, яка видала документ, а також печаток та штампів. Але навіть якщо всі дані на сертифікаті добре читаються – не спокушайтесь: організації, яка начебто видала сертифікат, може і не існувати. З особливою підозрою варто ставитися до сертифікатів, які начебто видані зарубіжними структурами та написані іноземною мовою: перевірити наявність цієї організації ви не зможете [4].

Одним із найкращих способів уникнення шахрайства є дотримання *правил безпеки в мережі Інтернет*. Розглянемо їх детальніше.

• Перш ніж виходити в мережу, встановіть на комп'ютері ефективну антивірусну програму. Слідкуйте за тим, щоб антивірусні бази постійно були актуальними, і пам'ятайте, що у світі щогодинно з'являються нові віруси.

• Якщо ви підключаєтесь до Інтернету через телефонну лінію, ніколи не вимикайте динамік модему. Це дозволить одразу розпізнати спроби Інтернет-шахраїв несанкціоновано підключити ваш комп'ютер до того чи іншого віддаленого веб-ресурсу шляхом набору заданого номера телефону (часто це практикують поширювачі порнографічних сайтів та послуг аналогічної спрямованості).

• Ніколи не зберігайте логіни, пін-коди, номери кредитних карток та інші конфіденційні дані у відкритому вигляді, наприклад, у звичайному текстовому файлі, чи в гаманці, прикріпленому до монітору. Як показує практика, більшість афер здійснюється завдяки тому, що безпечна жертва своєчасно не потурбувалася про збереження секретних даних у надійному місці.

• Якщо Ви все ж таки бажаєте зберігати всі конфіденційні дані в одному файлі – заархівуйте цей файл та захистіть архів надійним паролем (мінімум з 16 символів). Рекомендується використовувати для цього архіватор WinRAR – як показує практика, розшифрувати такий пароль практично нереально.

• Якщо Ви почули, що модем почав самостійно набирати якийсь номер без вашої участі, терміново відключіться від Інтернету шляхом фізичного від'єднання від кабелю. Потім проскануйте комп'ютер спеціальною програмою Antispyware (антишпигунским додатком) – ймовірно, що до комп'ютера таємно під'єднали шпигунський модуль автоматичного дозвону. У підсумку це, до речі, загрожує і отриманням астрономічних рахунків від телефонної компанії.

• Не довіряйте стороннім свої рахункові дані, а також не надавайте право користуватися власними електронними гаманцями, банківськими рахунками через Інтернет тощо. На жаль, шахраями стають саме ті, кому ви найбільше довіряєте. Крім того, навіть якщо довірена особа є напрочуд чесною людиною, ваші конфіденційні дані в неї можуть просто вкрасти.

• Будьте максимально пильними та обережними при відвідуванні невідомих сторінок в Інтернеті. Сьогодні дуже поширені шпигуни та віруси, для зараження якими достатньо просто зайти на певну веб-сторінку.

• Електронну кореспонденцію, що надходить від невідомих та сумнівних відправників, перед відкриттям обов'язково перевіряйте надійною антивірусною програмою (з актуальними базами). Недотримання цього правила може призвести до того, що Ваш комп'ютер швидко перетвориться в "шпигунське гніздо".

• Після скачування з Інтернету файлів, архівів і т.п. потрібно одразу ж перевірити їх антивірусною програмою і тільки після цього розпаковувати, запускати на виконання тощо. Пам'ятайте, що багато шкідливих програм поширюються у вигляді файлів, що надсилаються, чи архівів.

• Якщо ви користуєтесь операційною системою Windows, регулярно перевіряйте її на предмет безпеки. Зокрема, своєчасно скачуйте із сайту Microsoft та встановлюйте на свій комп'ютер всі останні оновлення, які стосуються безпеки (так звані "заплатки").

• Ніколи не відповідайте на запити та листи, в яких міститься прохання вислати на зазначену адресу ваші секретні дані (логін, пароль, пін-код). Цей нехитрий спосіб – різновид так званої "соціальної інженерії".

• Якщо при відвідуванні різних ресурсів в Інтернеті (форуми, сторінки реєстрації й т. ін.) вимагається залишити про себе будь-які відомості, то вони мають містити мінімум інформації. Зокрема, ніколи і нікому не повідомляйте свої паспортні дані, домашню адресу, різні паролі тощо. Незважаючи на те, що власники та керівники багатьох Інтернет-ресурсів гарантують повну конфіденційність, не будьте наївними: якщо комусь треба отримати цю інформацію, він її отримає і може використати для шантажу, вимагання тощо.

• Після закінчення роботи в Інтернеті обов'язково від'єднуйте кабель від лінії з'єднання з Інтернетом. Пам'ятайте, що в іншому випадку ваш комп'ютер буде вразливим навіть у вимкненому стані [4].

Слід також зазначити, що останнім часом все більше дітей стають активними користувачами мережі Інтернет, отже, батьки мають навчити їх бути обачними. З цією метою варто запобігти можливому їх потраплянню в тенета кіберзлочинності, вживаючи таких заходів.

– Проінформуйте дитину про найпоширеніші методи шахрайства та навчіть її радитися з дорослими перед тим, як скористатися тими чи іншими послугам в Інтернеті.

– Установіть на її комп'ютер антивірус чи, наприклад, персональний брандмауер. Ці додатки спостерігають за трафіком та можуть бути використані для виконання більшості дій на заражених системах, найчастішими з яких є крадіжка конфіденційних даних.

– Коли ваша дитина збирається здійснити покупку в Інтернет-магазині, переконайтеся в його надійності, а якщо вже здійснює онлайн-покупки самостійно, поясніть їй і особисто продемонструйте такі *правила безпеки:*

1) ознайомтеся з відгуками покупців;

2) перевірте реквізити та назву юридичної особи – власника магазину;

3) уточніть, як довго існує магазин (за наявними даними у відповідному пошуковику чи по даті реєстрації домену (сервіс WhoIs));

4) поцікавтесь, чи видає магазин касові чеки;

5) порівняйте ціни в різних Інтернет-магазинах;

6) подзвоніть у довідкову магазину;

7) зверніть увагу на правила торгівлі Інтернет-магазину;

8) з'ясуйте, скільки точно вам доведеться заплатити.

– Поясніть дитині, що неможна відправляти надто багато інформації про себе при здійсненні Інтернет-покупок: дані рахунків, паролі, домашню адресу та номери телефонів. Пам'ятайте, що ніколи адміністратор чи модератор сайту не вимагатимуть повних даних вашого рахунку, пароль чи пін-код. Якщо хтось запитує подібні дані, будьте пильні – швидше за все, це шахраї [5].

Якщо все ж таки дитина зіштовхнулася з певними шахрайськими ризиками в мережі Інтернет, батьки мають дотримуватися таких *рекомендацій.*

• Установіть позитивний емоційний контакт з дитиною, спонукайте її до розмови про те, що сталося. Розкажіть про свою стурбованість тим, що з нею відбувається. Дитина має вам довіряти та знати, що ви хочете розібратися в ситуації та допомогти їй, а не покарати.

• Спробуйте уважно вислухати її розповідь про те, що відбулося, зрозуміти, наскільки серйозно для неї те, що сталося, та наскільки серйозно це змогло вплинути на дитину.

• Якщо дитина засмучена в результаті Інтернет-шахрайства (наприклад, хтось зламав її профіль у соціальній мережі) чи потрапила в неприємну ситуацію (витратила ваші чи власні гроші), спробуйте її заспокоїти та разом з нею розберіться в ситуації: що призвело до такого результату, які неправильні дії здійснила сама дитина та ін.

• Якщо ситуація пов'язана із насильством в Інтернеті стосовно дитини, то необхідно з'ясувати інформацію про агресора, встановити, чи існує домовленість про їхню зустріч у реальному житті, коли вона очікується і що відомо агресору про дитину: реальне ім'я, прізвище, домашня адреса, телефон, номер школи; жорстко наполягайте на уникненні зустрічей з незнайомцями, особливо без свідків, перевірте всі нові контакти дитини за останній час.

• Зберіть найбільш повну інформацію про те, що відбувається, як зі слів дитини, так і за допомогою технічних засобів: зайдіть на сторінки сайту, де була ваша дитина, подивіться перелік її друзів, прочитайте повідомлення. При необхідності скопіюйте та збережіть цю інформацію – у подальшому все може вам знадобитися (наприклад, для звернення в правоохоронні органи).

• Якщо ви не знаєте, що відбувається з вашою дитиною, бо вона стала недостатньо відверта з вами або взагалі не готова йти на контакт – зверніться за допомогою до фахівців (телефон довіри, гарячої лінії тощо), які нададуть вам відповідні рекомендації й поради, роз'яснять, чи потрібне втручання і в якій формі інших установ та організацій (МВС, МНС тощо) [5].

У зв'язку з розповсюдженням випадків шахрайства в мережі Інтернет, представники правоохоронних органів рекомендують дотримуватися таких порад:

– не звертати увагу на барвисту рекламу і миготіння банерів, що пропонують незаконні послуги – це все обман;

– ніколи не відсилати повідомлення на запит "надіслати смс", якщо з інформації не зрозуміло, на яку послугу, ціну і кому саме потрібно надіслати смс-повідомлення;

– не шукати і не користуватися послугою "скачати безкоштовно"; Інтернет не має безкоштовних послуг: якщо хтось над чимось працював або щось створював, то його послуги не можуть бути безкоштовними;

– не звертати увагу на різні гасла про пожертвування: жебраки існують лише в підземних переходах та на вокзалах, а за комп'ютером (та ще й у безлімітному Інтернеті) жебраків не буває;

– уникати різноманітних "пірамід", які в є мережі Інтернет;

– довіряти власному досвіду і не брати до уваги усілякі вихваляння щодо неіснуючих товарів або послуг, вони створюються для заманювання людини [6].

Підсумовуючи зазначене вище, варто наголосити, що в Україні, як і у більшості країн світу, проблема запобігання та протидії кіберзлочинності вимагає не тільки активізації зусиль правоохоронних органів, спецслужб, судової системи, але й обачливості користувачів Інтернет-мереж безпосередньо. Саме вміння останніх своєчасно розпізнавати і протистояти шахрайському свавіллю через демонстрацію здорового скепсису та звичку перевіряти інформацію сприятиме їх безпеці, навчить бути більш обачливими та унеможливить всі спроби шахраїв перетворити користувачів всесвітньої мережі на жертв кіберзлочинців. А це водночас значно сприятиме і зміцненню економічної безпеки нашої країни, прискоренню її інтеграції в європейський і світовий простір.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Карпюк Г.* Грані шахрайства / Г. Карпюк // Іменем закону. – 2014. – № 42 (5948). – С. 14–16.

2. *Підюков П.П.* Кіберзлочинність як суттєва перепона євроінтеграції України та серйозна загроза її економічній безпеці, правам і законним інтересам громадянського суспільства : психолого-юридична характеристика / П.П. Підюков, Т.П. Устименко, О.С. Дронова, Є.О. Варлакова, С.Л. Мазур, Т.С. Бобко // Міліція України. – 2014. – № 9–10. – С. 12–18.

3. Кіберзлочинність : проблеми боротьби і прогнози [Електронний ресурс]. – Режим доступу : http : // anticyber.com.ua/article_detail.php?id=140.

4. *Гладкий О.А.* Мошенничество в Интернете. Методы удаленного выманивания денег, и как не стать жертвой злоумышленников / О.А. Гладкий. – Питер. : Litres, 2012. – 62 с.

5. Безопасный интернет. KinderGate Родительский Контроль [Електронный ресурс]. – Режим доступу : kindergate-parental-control.com/ru/child-internet-safety/partner-advices.

6. *Морозова Т.* Інтернет-шахраї. Або як убезпечити свої фінанси. Інтернет-видання "Менщина" / Т. Морозова [Електронний ресурс]. – Режим доступу : http : // mena.org.ua/blog/internet-shahraji-abo-yak-ubezpechyty-svoji-finansy/.

Отримано 17.10.2014