ПИТАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

УДК 354.42/.44

Гавловський Владислав Данилович – начальник відділу Міжвідомчого науково-дослідного центру з проблем боротьби з організованою злочинністю при Раді національної безпеки і оборони України, кандидат юридичних наук, старший науковий співробітник

До питання захисту персональних даних у соціальних мережах

У статті в правовому та кримінологічному аспектах досліджуються проблемні питання, пов'язані з викраденням через соціальні мережі та наступним протиправним використанням персональних даних індивідів. Обґрунтовано пропозиції щодо протидії такому явищу.

Ключові слова: інформаційна безпека, Інтернет, соціальні мережі, викрадення персональних даних, крадіжка особистості, шахрайство.

Сьогодні автоматизовані системи, реалізовані на основі комп'ютерних мереж, перетворилися у невід'ємний елемент життєзабезпечення різноманітних сфер суспільного життя, без яких неможливе повноцінне існування та розвиток суспільства та держави в цілому.

Президентом України 2011 рік проголошено роком інформаційного суспільства. Останнім часом динаміка розвитку інформаційного суспільства в Україні є стабільно позитивною, незважаючи на вкрай низьке виконання завдань Національної програми Інформатизації та незадовільний стан використання сучасних інформаційних технологій у сфері державного управління. Сьогодні Україна утримує середні позиції у світових рейтингах розвитку інформаційного суспільства. І це не стільки завдяки імплементації найсучасніших інформаційно-телекомунікаційних технологій, скільки за рахунок "наздоганяючого" запровадження, наприклад, телекомунікаційного чи стільникового мобільного зв'язку. Так, відповідно до індексу мережевої готовності Україна посідає 82 місце серед 134 країн світу. Але рейтинги свідчать,

що протягом останніх років, на тлі інших країн, темпи зростання інформаційного суспільства в Україні постійно сповільнюються [1].

В Україні стрімко та динамічно формується масова Інтернет-аудиторія та специфічне "мережеве" соціокультурне середовище. За даними Міжнародної консалтингової компанії J'son & Partners Consulting, Україна, поряд з іншими країнами СНД, є світовим лідером за темпами збільшення аудиторії "соціальних мереж": щорічний приріст становить близько 30 %, і на сьогодні налічує понад 8 млн осіб [2].

Соціальні мережі є частиною Інтернету, вони являються джерелами інформації. Суспільство поступово входить у залежність від нормального функціонування соціальних мереж і це змушує виробляти нові підходи до захисту інтересів особистості, суспільства, держави у цій сфері.

Актуальність даної проблеми пов'язана з тим, що у зв'язку з появою нового простору для спілкування й, фактично, можливостей для реалізації найрізноманітніших цілей – зокрема комерційних, ділових, особистих та ін., виникають нові види та способи незаконного використання інформаційних масивів соціальних мереж в Інтернеті для вчинення різного роду протиправних, а подекуди й злочинних акцій. Розвитком нових технологій сприяє вдосконаленню методів і способів учинення традиційних, як правило, корисливих видів злочинів (шахрайства, вимагання, крадіжок тощо), відбувається розголошення та протиправне використання конфіденційної інформації, що стосується особистого життя людини, порушуються конституційні права громадян. Крім того, сучасний стан накопичення та збереження персональних даних особи у соціальних мережах створює плідне підґрунтя для втягування наших співгромадян іноземними спецслужбами, терористичними та іншими злочинними організаціями у протиправну діяльність. Діюча сьогодні в Україні система захисту особи неспроможна забезпечити ефективний захист наших співвітчизників не лише від реально вчиняємих щодо них протиправних дій з використанням викрадених з соціальних мереж їхніх персональних даних, а й від постійно зростаючих реальних і потенційних загроз.

Безпосередньо науковим дослідженням проблем захисту персональних даних займалися В. М. Брижко, О. О. Баранов, К. І. Беляков, І. Б. Жиляєв, Р. А. Калюжний, Д. В. Ланде, В. М. Фурашев, В. С. Цимбалюк, М. Я. Швець та інші, проте на сьогодні наукові дослідження загальних проблем викрадення персональних даних через соціальні мережі вітчизняними вченими фактично не проводились. Представлена праця є одним із перших елементів у формуванні підґрунтя для розробки вкрай необхідної наукової концепції протидії цьому небезпечному явищу та його наслідкам як для конкретних осіб, так і суспільства в цілому.

Отже, метою даної роботи є дослідження загальних правових і кримінологічних проблем інформаційної безпеки, пов'язаних із викраденням персональних даних (особистості) через соціальні мережі, а також визначення організаційних і правових напрямів їх вирішення з боку держави.

З розвитком інформаційних технологій віртуалізуються відносини між людьми і, як негативний наслідок цього процесу, виникають як нові види злочинів, так і вдосконалюються технології вчинення "традиційних" злочинів. Процес становлення та розвитку соціальних відносин у новому інформаційному середовищі достатньо не підкріплений ні відповідними законодавчими актами, ні моральними установками. Останнім часом отримали розповсюдження такі злочинні дії як "крадіжка особистості" (англ. Identity theft), під якою розуміють діяння, коли протиправно вилучаються та (або) використовуються персональні дані людини (індивіда) з метою незаконного отримання матеріальної вигоди чи інших протиправних діянь. Такого злочину окремо, звичайно, не передбачено кримінальним законом жодної держави. Особливо широке поширення крадіжки особистості набули в США у другій половині минулого століття завдяки впровадженню послуг, що надаються віддалено, без особистої присутності, зокрема, широкому розповсюдженню номера соціального забезпечення SSN (Social Security number) як посвідчення особи. SSN – дев'ятизначний номер, що присвоюється громадянам і резидентам США, основним призначенням якого є податковий облік працівників і пенсійний облік. Останнім часом номер SSN став національним ідентифікаційним номером, його часто вимагають при вступі на роботу, в банках для відкриття рахунків, при наданні медичних послуг тощо.

Номери записуються у вигляді: ***-**-**** (номер регіону, номер групи, послідовний номер в даній групі). Дані номери є персональною інформацією і шахраї прагнуть дістати легальні номери, здійснивши тим самим так звану крадіжку особистості. До речі, ці номери на чорному ринку США, за даними CioWorld, коштують від 16 до 30 доларів. Відповідно до офіційного звіту Федеральної комісії по торгівлі (FTC, США) кількість скарг, пов'язаних із викраденням персональних даних, останнім часом стрімко зростає і на сьогодні набула загрожуючих масштабів у зв'язку з ростом обсягів комунікаційних послуг. Так, у 2010 році до Федеральної комісії по торгівлі надійшло 250 854 скарги, пов'язані з крадіжками персональних даних. Це становить близько 19 % від загальної кількості скарг про шахрайства.

Варто зазначити, що серед скарг в останні роки зростає такий вид шахрайств як вимагання грошей під виглядом родичів і від імені різних державних структур, громадських організацій і т. ін. з метою

отримання персональних даних. Їх кількість у 2010 році становила 60 158 випадків. Особливо багато скарг надходить від обманутих власників мобільних телефонів, блоггерів, а також користувачів соціальних мереж [3].

Варто констатувати, що соціальні мережі є плідним й дуже зручним підґрунтям для шахрайства та інших протиправних діянь, що вчиняються у шахрайський спосіб. При цьому шахрайство може бути як прямим – у класичному варіанті діяння, що підпадає під дію Кримінального кодексу, так і таким, коли одномоментного розкрадання коштів не відбувається, проте стають відомими персональні дані користувача або відбувається зараження комп'ютера жертви певними видами шкідливих програмам, які в подальшому, перехоплюючи на себе управління, негласно контролюють усі дії користувача.

І що цікаво, значну частину персональних даних користувачі соціальних мереж повідомляють добровільно. При реєстрації користувачі повідомляють про себе чимало особистої інформації – це прізвище, ім'я та по-батькові, дата народження, номер телефону (домашній, робочий, стільниковий), електронна пошта тощо. Потім користувач починає розміщувати інформацію про себе – адреси (домашня та робоча), факти зі свого особистого життя, рід занять, захоплення, національність, віросповідання, групу крові, номер ICQ, Skype ідентифікатор, нік в IRC, інші контактні дані систем миттєвого обміну повідомленнями, адресу домашньої сторінки в Інтранеті, відомості про свою родину, перенесені хвороби, партійну приналежність, коло друзів, колег, ділових партнерів тощо. Також може бути розміщено кілька фотокарток чи аватар користувача. Акаунт користувача також може містити різні статистичні характеристики перебування користувача в системі: дату, час і тривалість останнього входу та перебування в системі, адреси, використані при підключенні комп'ютера та ін. Тобто, кожен аккаунт – це сховище персональних даних і повний архів листування.

Варто звернути увагу, що більшість користувачів навіть не здогадуються про те, наскільки широкому колу осіб надана ними інформація може стати відомою, не усвідомлюють і фактично не можуть усвідомити реальну й потенційну небезпеку можливого протиправного використання накопиченої протягом тривалого часу та відповідним чином аналітично обробленої їх персональної інформації щодо фактично всіх сфер їхнього особистого та службового життя.

Власники багатьох соціальних мереж запевняють користувачів, що їх інформація є особистою й закритою від сторонніх осіб. Але, як мінімум, її знають власники соціальних мереж, у яких користувач зареєстрований. Як максимум, – всі. Власники можуть використовувати цю інформацію з метою розвитку свого бізнесу чи надавати особисті дані

користувачів на запити, наприклад, поліції або спецслужб. Використовуючи пошук інформації, в аккаунтах користувачів знаходять і пропонують якісь послуги. Як приклад, соціальна мережа Mail. ru, після введення інформації про навчання, автоматично пропонує однокласників і однокурсників.

Зокрема, більш складний аналіз інформації проводиться при рекламних технологіях. При цьому аналізується інформація, яка добровільно надається користувачем, а також аналізується його поведінка в соціальній мережі – недобровільно надана інформація. На сьогодні багато соціальних мереж використовують можливості поведінкової реклами, тобто користувачам показується реклама на основі аналізу як самих простих даних – статі, звичок чи професії, так і аналізу складних систем відслідковування та аналізу дій користувачів.

Крім того, є бажаючі отримати доступ до персональної інформації як заради розіграшу чи жарту, так і з метою зламати сторінку в соціальній мережі, викрасти паролі, отримати доступ до поштових скриньок для ознайомлення з кореспонденцією, використання персональних даних з подальшою дискредитацією користувачів, учинення злочинів тощо. Впевненість користувачів у тому, що їхня інформація надійно захищена паролем, не відповідає дійсності.

Зламати аккаунт у соціальній мережі можна кількома способами. Серед найбільш поширених можна назвати наступні.

Часто буває нескладно дізнатися пароль у самого користувача, особливо якщо з ним встановлено довірчі відносини.

Самим простим способом є підбір пароля до аккаунта “вручну”, для чого достатньо добре вивчити користувача і простим уведенням номера його телефону чи дати народження, ім’я або прізвища, набору простих поєднань цифр, наприклад “12345”, можна отримати доступ до аккаунту чи електронної пошти.

На багатьох сайтах, у т. ч. електронній пошті, існує можливість відновити пароль, якщо його забули, відповівши на секретне питання. На це питання також можливо знайти відповідь, вивчивши власника, знаючи його оточення чи встановивши іншу інформацію. Як приклад, “страва, якій я віддаю перевагу”, “мій паспорт”, “колір мого автомобіля” тощо.

Ефективним способом злому електронної пошти є брутфорс – перебор усіх можливих варіантів. Із соціальними мережами це робити складніше, тому що розробниками передбачено лише три спроби на введення пароля, після чого, як правило, програма просить увести набір якихось символів, які висвітлюються на екрані. Це зроблено для захисту аккаунтів від програм-роботів, які автоматично підбирають паролі. А електронна адреса дозволяє підбирати пароль незліченну кіль-

кість разів, що є зручним для зловмисників. І, отримавши доступ до електронної пошти, на сторінку соціальної мережі потрапити вже не складно, наприклад, використавши кнопку "Забули пароль?".

Паролі можливо отримувати також за допомогою програм – спеціальних вірусів "троянів", які проникають до комп'ютера жертви з якимось файлом, викрадають паролі та відправляють їх зловмиснику. Крім троянів існує інше спеціальне програмне забезпечення для злому паролів, зокрема додаток до брутфорса (генератор паролів), утиліти для розшифровки файлів cookies, клавіатурні перехоплювачі та цілий ряд інших програм для злому паролів і проникнення до комп'ютера.

Слід відмітити, що значна кількість викрадення паролів відбувається з вини самих користувачів. Це і недостатній досвід роботи на комп'ютері, і неуважність, довіра до різних повідомлень, дозвіл роботи на власному комп'ютері, користування Інтернетом у Інтернет-кафе чи при безкоштовному безпровідному (Wi-Fi) доступу до Інтернету тощо.

В якості прикладу створення фішінгових сайтів, які виглядають точною копією іншого сайту і мають схожу адресу з відмінністю в 1–2 символи, можна назвати заміну Інтернет-адреси vkontakte. ru новою адресою vkontahte. ru. Тим чи іншим способом заманюють на цей сайт і коли користувач уводить логін і пароль, його перенаправляють на справжній сайт, а пароль стає відомий зловмисникам.

Зловмисники активно крадуть паролі та логіни до соціальних мереж, які, за даними експертів "Лабораторії Касперського", на чорному ринку коштують усього близько 5 доларів США [4].

Як бачимо, зламати пароль й отримати доступ до електронної пошти чи аккаунту користувача соціальної мережі не є великою проблемою.

І якщо раніше викрадали лише персональні дані користувачів, то останнім часом нерідко відслідковують поведінку, соціальні зв'язки і пристрасті конкретного користувача соціальних мереж.

Ізраїльські вчені розробили і продемонстрували математичну модель, яка в онлайн режимі на протязі певного часу здійснює таке відслідковування. За допомогою таких програм, зібравши найбільш конфіденціальну інформацію про користувача мережі Інтернет, можна створити віртуального двійника людини і використовувати цю копію в своїх цілях. Із знайомими жертви можна спілкуватися на її ж лексиконі, оперувати фактами із особистого життя, тобто як би викрадати особистість потерпілого.

При цьому, якщо викрадення персональних даних було вчинено з метою отримання матеріальної вигоди, то можна змінити паролі, замінити кредитні картки чи здійснити ще якісь дії, але коли зловмисники через соціальні мережі вивчали поведінку, звички, пристрасті жертви, коло її знайомих тощо, то це змінити швидко або часто взагалі не-

можливо. При цьому користувачі нерідко приймають рішення про знищення своїх даних із соціальних мереж. Але ця інформація залишається на серверах. І користувачі соціальних мереж досить часто скаржаться з цього приводу. Є. Касперський зауважує, що потрібно пам'ятати, що потрапило в Інтернет, залишається там назавжди.

Як приклад, співробітники ФБР затримали хакера-збоченця, який проникав у комп'ютери молодих жінок і неповнолітніх дівчат, викрадав персональну інформацію та слідкував за ними через їх вебкамери і мікрофони. Погрожуючи розповсюдженням цієї інформації, чоловік примушував надавати йому їх непристойні фотографії та відео. Використовуючи соціальні мережі, він відрекомендовувався молодою жінкою чи подругою жертви і пропонував переглянути фільм, який знаходився у прикріпленому файлі. Адреса хакера не викликала недовіри і жінки, натиснувши на файл, заражали свої комп'ютери вірусом трояном, за допомогою якого він міг зчитувати інформацію та слідкувати більш ніж за 200 жінками. ФБР розглядало такі дії як примушування до сексу.

Варто звернути увагу, що зловмисники із соціальних мереж використовують у своїх цілях найрізноманітнішу інформацію. Наприклад, користувач поділився з друзями інформацією, що їде на відпочинок чи в відрядження і його не буде певний час вдома, цим можуть скористатися зловмисники. Але ще простіше про це можна дізнатися, скориставшись, наприклад, сайтом Openbook, де можна здійснити запит за ключовими словами і дізнатися, хто з користувачів Facebook зараз перебуває у короткостроковій відпустці. Знайти будинок, із якого поїхала людина, не становить проблеми.

Як приклад, використання злочинцями соціальної мережі Facebook для квартирних крадіжок. Троє злочинців із міста Нашуа штату Нью-Гемпшир США відстежували сторінки цієї соціальної мережі й з'ясовували, коли не буде вдома потерпілих, які самі незадовго до крадіжок у своєму блозі на Facebook оголошували, що вони їдуть у відпустку чи бізнес-поїздку і будуть відсутні вдома на протязі кількох днів. Поліція довела 18 фактів крадіжок, пов'язаних із моніторингом соціальної мережі. До речі, поліції вдалося розкрити ці злочини тільки завдяки тому, що одним із викрадених предметів виявився особливий вид феєрверку, який вони запустили у громадському місці. Один із поліцейських побачив це і вистежив місце проживання одного з підозрюваних.

Необхідно констатувати, що кількість злочинів, учинених із використанням інформації, викраденої із соціальних мереж, постійно зростає. Крім того, аналітики вважають, що зростання кількості таких злочинів пов'язано зі збільшенням кількості дітей, підлітків і молоді у соціальних мережах. На жаль, вони погано уявляють собі наслідки

відкритості та гіперкомунікативності. Молоді люди не розбірливі в контактах і недостатньо знайомі між собою, крім того, здебільшого взагалі незнайомі з privacе-налаштуваннями профілів. І це не рідко призводить до тяжких наслідків. За даними OnGuard Online – 22 % користувачів соціальних мереж від 16 до 24 років взагалі не знайомі з людьми, з якими вони "дружать" [5].

Згідно з дослідженнями, проведеними Інтернет-провайдером TalkTalk, кожна двадцята дитина у віці 6–15 років спілкувалася з незнайомцями через веб-камеру, а кожна п'ятдесята зустрічалася з незнайомцем особисто після спілкування з ним у мережі Інтернет [6]. Немає ніякої гарантії, що приватна інформація з профілів потрапить до людей з недобрими намірами. Так, цього року окружний суд Єрусалима виніс обвинувальний висновок 22-річному мешканцю Східного Єрусалима за неодноразове згвалтування 12-річної дівчинки, з якою він познайомився в соціальній мережі Facebook [7], а англійську дівчинку-підлітка було вбито чоловіком, який видавав себе на Facebook за підлітка [8].

Європейською комісією було проведено опитування 25 тисяч дітей в 25 країнах–членах ЄС. Згідно з результатами дослідження, 38 % дітей віком від 9 до 12 років і 77 % дітей віком від 13 до 16 років мають профайли у соціальних мережах, таких як Facebook, Hyves, Tuenti, Nasza-Klasa, SchuelerVZ та ін. Близько 25 % опитаних дітей, які користувалися соціальними мережами, зазначили, що їхні профайли є відкритими для всіх користувачів [9].

Інститутом соціології НАН України проведено дослідження, яке включало в себе опитування 1200 дітей, батьків і учителів у 11 містах України, які продемонстрували необізнаність про потенційні ризики для дітей в мережі Інтернет. Майже половина опитаних дітей готові були розкрити приватну інформацію про себе, про свою родину, переслати свої фотокартки незнайомим особам [10].

Хотілося б звернути увагу ще й на безконтрольність з боку батьків, учителів та інших осіб, які не звертають особливої уваги на спілкування дітей в соціальних мережах. Більшість батьків (76 %) навіть не цікавляться, які сайти відвідує їхня дитина, при тому, що батьки (87 %) вважають, що саме вони повинні навчати дітей правилам користування мережею Інтернет і контролювати їх. До речі, відповідно до дослідження, проведеного Інтернет-провайдером TalkTalk, 62 % із 500 опитаних британських дітей повідомили, що обманюють батьків з приводу того, чим займаються в он-лайні, а 53 % респондентів зізналися, що видаляють історію браузера, щоб батьки не змогли перевірити, які ресурси вони відвідували [6].

На сьогодні є слушною думка Е. Касперського про те, що потрапило в Інтернет, – може залишитися там назавжди. І в майбутньому наші діти

можуть пожалкувати про свою поведінку й залишені сліди в соціальних мереж. Як приклад, половина британських роботодавців відкидала шукачів вакансій, виявивши на них компромат на Facebook [8].

Звертає на себе увагу й той факт, що деякі соціальні мережі майже ідеально створені для прикриття, за необхідності, розвідувально-пошукової діяльності спецслужб та організацій щодо збору різнопланової, придатної для наступного аналітичного дослідження особистісної інформації. Проте, ця проблематика потребує ґрунтовного самостійного дослідження, у цій статті ми дуже коротко зупинимося на деяких прикладах пасивних пошукових аспектів.

Зокрема, на особливу увагу заслуговує соціальна мережа odnoklassniki. ru. За оцінкою співробітників спецслужб вона є класичним прикладом збору розвідувальної інформації. Така потужна систематизація даних по містах, навчальних закладах, підприємствах, військових частинах із зазначенням дати служби, особистих даних громадян із фотокартками, такими розділами як "мої друзі", "друзі друзів", "співтовариства", і т. ін., відсутня навіть у спецпідрозділів. Вона є довідником для іноземних спецслужб.

У цій соціальній мережі відкрито структуру базування військових частин. Лише на цьому сайті представлено понад 3 000 військових частин і спецпідрозділів із чітким зазначенням нинішнього місця дислокації в РФ. Крім того, структура порталу дає можливість у будь-який час вийти на зв'язок із діючими військовослужбовцями, а при необхідності – отримати від них потрібну інформацію.

За кордоном військові відомства ставляться до подібних ресурсів насторожено. Ще рік тому американським солдатам було заборонено заходити із службових комп'ютерів на сторінки соціальних мереж. Але після дослідження, яке проводилося на замовлення Пентагону, виявилося, що соціальні мережі можуть бути корисними для покращення іміджу армії та вербування новобранців. "Соціальні мережі – це не тимчасова мода. Якщо армія буде їх ігнорувати, вони нікуди не дінуться. Якщо не можна ігнорувати, значить, потрібно навчитися користуватися без загрози для безпеки" – говориться в новоствореній інструкції по використанню військовослужбовцями – U. S. Army Social Media Hanadbook.

Готуючи цей документ, американці добре вивчили досвід використання соціальних мереж військовослужбовцями інших країн, особливо негативний. Так, у березні 2010 року армії оборони Ізраїлю довелося відмінити заплановану операцію на Західному березі, після того як один із бійців анонсував її на своїй сторінці в Facebook. "У середу ми зачистимо Катанах і в четвер, дай бог, повернемося додому", – написав солдат, при цьому навів час початку операції та номер свого підрозділу.

Підсумовуючи викладене, необхідно зазначити, що наразі з'явився новий і доволі небезпечний простір інформаційного обміну, що станом на

сьогодні практично перебуває поза межами правого регулювання і контролю з боку суспільства та держави.

Отже, виникає негайна потреба у розробці:

системи заходів правового регулювання доступу до персональної інформації в соціальних мережах (необхідно чітко врегулювати права та обов'язки власників, адміністрації та технічного персоналу соціальних мереж щодо використання, зберігання та захисту персональної інформації;

основних засад юридичної відповідальності за незаконне розголошення, розповсюдження та використання персональної інформації, що накопичується в інформаційних масивах соціальних мереж;

кримінологічного та правового поняття "крадіжка особистості";

системи обмежень щодо використання соціальних мереж деякими спеціальними категоріями громадян (військовослужбовців, працівників правоохоронних органів, окремих категорій державних службовців і секретоносіїів).

Список використаних джерел

1. Інформаційне суспільство в Україні : глобальні виклики та національні можливості : [аналіт. доп.] / Д. В. Дубов, О. А. Ожеван, С. Л. Гнатюк. — К. : НІС, 2010. — С. 8–9.

2. Социальные сети в странах СНГ развиваются активнее остального мира [Електронний ресурс] / J'son & Partners Consulting. — 11 трав. 2010 р. — Режим доступу :

http:// rumetrika. rambler. ru/revien/2/4327.

3. Кража личности – персональных данных в США приобретает угрожающие масштабы [Електронний ресурс] / "The Federal Trade Commission", США. — 8 берез. 2011 р . — Режим доступу :

http://perevodika. ru/articles/17943. html.

4. Всемирная сеть мошенников. Жертвой киберпреступников может стать каждый [Електронний ресурс] / Георгий Крымов. — Режим доступу :

http://cripo. com. ua/? sect_id=6&aid=115837.

5. Е. Касперский заявил о физической опасности соцсетей / [Електронний ресурс]. — Режим доступу :

http://www. cnews. ru/news/top/index. shtml?2011/05/19/440795.

6. Каждый четвертый британский ребенок получал или отправлял порноснимки по e-mai [Електронний ресурс] / Эльвира Кошкина. — Режим доступу :

http://net. compulenta. ru/501284.

7. Социальные сети – обман и преступления / [Електронний ресурс]. — Режим доступу :

http:// jerusalem. israelinfo. ru/news/1703.

8. Улица больше не воспитывает детей ! / [Електронний ресурс]. — Режим доступу :

http://maaslug. org. ua/novosti/ulica-bolshe-ne-vospityvaet-detej. html.

9. Соціальні мережі небезпечні для дітей [Електронний ресурс]. — Режим доступу :
http://dovgolit. com/? newsid=1181.
10. Исследование : 11 украинских детей пытались купить в Интернете наркотики / [Електронний ресурс]. — Режим доступу :
http://korrespondent. net/tech/technews/1006131.

В статье в правовом и криминологическом аспектах исследуются проблемные вопросы, связанные с похищением через социальные сети и последующим противоправным использованием персональных данных индивидов. Обоснованы предложения относительно противодействия такому явлению.

The article deals with the examination in the legal and criminology aspects of the problems concerning the theft by the use of the social networks and follow-up illegal use of the personal data of the individuals. The propositions concerning the counteraction this phenomenon are grounded.

Стаття надійшла до редакції журналу 23 червня 2011 року.