© Kukharska N., Kukharskyy V. Threats to children security in social networks // Ukrainian Scientific Journal of Information Security, 2014, vol. 20, issue 2, p. 169-175.

ПРИВАТНІСТЬ ТА ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ / PRIVACY & PROTECTION FROM IDENTITY THEFT

ЗАГРОЗИ БЕЗПЕЦІ ДІТЕЙ У СОЦІАЛЬНИХ МЕРЕЖАХ

Наталія Кухарська[1], Віталій Кухарський[2]

[1]Львівський державний університет безпеки життєдіяльності, Україна
[2]Львівський національний університет імені Івана Франка, Україна

КУХАРСЬКА Наталія Павлівна, к.ф.-м.н.

Рік та місце народження: 1971 рік, с. Жовтневе, Теребовлянський район, Тернопільська область, Україна.
Освіта: Львівський державний університет імені Івана Франка (з 1999 року – Львівський національний університет імені Івана Франка), 1993 рік.
Посада: доцент кафедри управління інформаційною безпекою з 2011 року.
Наукові інтереси: інформаційна безпека, математичне моделювання.
Публікації: більше 60 наукових публікацій, серед яких навчальні посібники, наукові статті, матеріали та тези доповідей на конференціях.
E-mail: kukharska.n@ngmail.com

КУХАРСЬКИЙ Віталій Михайлович, к.ф.-м.н.

Рік та місце народження: 1972 рік, с. Гряда, Жовківський район, Львівська область, Україна.
Освіта: Львівський державний університет імені Івана Франка (з 1999 року – Львівський національний університет імені Івана Франка), 1994 рік.
Посада: доцент кафедри прикладної математики з 2003 року.
Наукові інтереси: математичне моделювання, інформаційна безпека, e-government, e-learning.
Публікації: більше 40 наукових публікацій, серед яких посібники, статті.
E-mail: vetaley@franko.lviv.ua

Анотація. *Останнім часом соціальні мережі стали невід'ємним атрибутом життя дітей. Підростаюче покоління, шаленіючи від соцмереж, рідко усвідомлює наслідки своєї надмірної відкритості та гіперкомунікативності у віртуальному просторі. Кількість дітей – завсідників соцмереж – дедалі збільшується завдяки технології Wi-Fi та новим можливостям доступу до Інтернету з мобільних телефонів, смартфонів, ноутбуків, ігрових консолів, планшетів і т.п. Батьки через свою необізнаність щодо Інтернет-загроз дитячій безпеці, як правило, не бачать нічого поганого у тому, що їхнє чадо має сторінки у соціальних мережах. Водночас, питання, що стосуються забезпечення безпеки підростаючого покоління у соцмережах, потребують нагального скоординованого вирішення. У статті зроблено акцент на актуальності формування інформаційної культури особистості – дітей, їх батьків, наставників, як основного механізму розв'язання зазначеної проблеми; визначено основні загрози безпеці дітей у соціальних мережах; проведено їх комплексний аналіз та подано характеристики їх впливу.*

Ключові слова: *соціальна мережа, загроза, безпека дітей, небажаний контент, кібербулінг, кібергрумінг, секстінг, комп'ютерний вірус.*

Феномен соціальних мереж з'явився майже два десятиріччя тому: створений Ренді Конрадом класичний веб-сайт Classmates.com був відкритий для відвідувачів у 1995 році. Нині кількість його користувачів понад 50 мільйонів [1]. Позаяк, сьогодні у пересічних українців на слуху зовсім інші соціально-мережні ресурси: Facebook, Twitter, «ВКонтакте», «Одноклассники». До речі, аналогічних сервісів у всьому світі зараз налічується понад тисячу.

А ось, початком популярності соціальних мереж прийнято вважати 2003-2004 р.р., коли були введені в дію LinkedIn, MySpace і Facebook. У країни пострадянського простору мода на соціальні сервіси прийшла дещо пізніше. Водночас, як свідчать результати різних досліджень: протягом останніх років продовжує спостерігатися динаміка зростання зацікавленості соцмережами. Так, Європейська дослідницька компанія InSites Consulting підрахувала, що у світі різними сервісами соціальних мереж у 2012

році користувалося більше 1,5 млрд. осіб і щонайменше дві третини користувачів робило це щоденно [2]. А у лютому 2014 року засновник найбільшої у світі соцмережі Facebook Марк Цукерберг (Mark Zuckerberg), привітавши на своїй сторінці 1,23 (!) мільярдну армію її користувачів з десятилітнім ювілеєм мережі, прозвітував про зростання прибутку Facebook за попередній 2013 рік у 28 разів і пообіцяв, що у наступному десятилітті соціальні мережі будуть використовуватися не тільки для обміну даних, а й будуть допомагати шукати відповіді на питання і вирішувати складні проблеми [3].

В Україні також відстежується стійка тенденція щодо збільшення кількості користувачів соцмереж. Так, згідно з даними компанії Gemius Ukraine, gemiusAudience – Fusion Panel, у січні 2014 року три таких веб-сайти («ВКонтакте», Facebook, «Одноклассники»), перебуваючи в десятці найбільш відвідуваних, налічували сумарно понад 22 мільйони користувачів (real users), що на 6,26 % більше, ніж попереднього місяця [4]. Щоправда, і це слід визнати, таке проведене нами сумування дещо спотворює уявлення про реальну кількість людей, задіяних у функціонуванні соціальних Інтернет-ресурсів, так як деякі з користувачів мають профілі в кількох соціальних мережах і користуються ними не рідше, ніж раз на місяць.

Соціальні мережі, незважаючи на те, що вони – явище порівняно нещодавнє, відразу отримали колосальний відгук у підростаючого покоління. Більше половини (52 %) тих дітей та підлітків, що користуються Інтернетом, не уявляють себе поза інформаційним полем соцмереж [5]. Для них соціальні мережі – частина життя. Така шалена популярність соцмереж загалом і в молодіжної аудиторії зокрема має пояснення. По-перше, це зручний і зрозумілий інтерфейс, по-друге, широке охоплення інтересів користувачів: у соцмережах можна інтерактивно спілкуватися з друзями, залишати повідомлення, обмінюватися зображеннями, відео та музикою.

Безумовно, соціальні мережі – одне із найбільших досягнень людства. Вони є ефективним способом комунікації та самоутвердження. Активність в соціальних мережах – атрибут мобільності та динамічності сучасного життя. Проте, нажаль, більшість молодих людей досі не мають розуміння того, до яких наслідків може призвести їх необдумана он-лайн-поведінка в соціальних мережах на кшталт Facebook та Вконтакте. Відомий жарт: «Комп'ютер дає змогу вирішувати всі ті проблеми, яких до його появи не було» зокрема стосується і соціальних мереж.

Сьогодні соціальні мережі виступають привабливою платформою для різного роду кіберзлочинців. Причина цього криється у властивостях, котрі притаманні усім без винятку соцмережам і котрі можуть бути використані зловмисниками у явно не шляхетних цілях. Такими властивостями, зокрема, є:

− велика користувацька база;

− встановлені зв'язки довір'я як між окремими користувачами, так і між групами користувачів;

− високий розподіл бази користувачів за географічним і часовим параметрами;

− необізнаність щодо питань інформаційної безпеки завсідників соціальних мереж.

Мета статті – виявити основні загрози, з якими зустрічаються в соціальних мережах діти, найбільш уразлива категорія користувачів мережі Інтернет.

Відомим широкому загалу є факт: діти значно швидше у порівняні з дорослими адаптовуються до стрімких змін інформаційних технологій, легко опановують їх, випереджуючи в обізнаності щодо можливостей їх використання батьків. Разом з тим, діти через відсутність життєвого досвіду та психологічні вікові особливості такі, як недостатня розвиненість саморегулятивних механізмів, слабкий вольовий і емоційний контроль, імпульсивність поведінки, є менш стійкими до інформаційних та програмно-технічних загроз.

Як зазначають вітчизняні та закордонні експерти, ідеально «чиста» мережа Інтернет, тобто така, яка позбавлена загроз, у принципі неможлива. Користувачам залишається хіба що намагатися максимально знизити рівень їх прояву. У сучасному суспільстві вплив он-лайн-інформаційного простору на формування молодої особистості, нажаль, є ще не достатньо усвідомлюваним. По між тим, фахівці наголошують [6]: надмірна зацікавленість молодими людьми сервісами мережі Інтернет та багатогодинне проведення ними часу у її тенетах є причиною:

− порушення критичного ставлення до себе і своїх вчинків, втрати раціональності та цілеспрямованості поведінки;

− неспроможності несформованої особистості адекватно і раціонально моделювати своє майбутнє; нереалістичності її планів, надмірної безкомпромісності у виборі життєвих цілей;

− пасивності, дефіциту енергії в реальному житті, емоційної скутості та байдужості в реальних стосунках;

− парасоціального спілкування.

Проблеми, пов'язані з недотриманням дітьми правил безпечної поведінки в соціальних мережах, вимагають нагального вирішення, оскільки ситуація, яка склалася на сьогодні, доволі драматична Втримати дітей від користування соцмережами неможливо. Вікові обмеження при реєстрації, що вводяться адміністраторами соціальних мереж, не діють. Діти приховують вік і заводять нелегальні аккаунти (англ. account) на Facebook й інших мережах. Три чверті опитаних осіб до 16 років мають персональні профілі. Батьки не можуть або не хочуть контролювати цей процес. Згідно з результатами досліджень «Київстар» лише у 18 % випадків дорослі слідкують за тим, які сайти відвідує дитина [7]. Пояснення цьому різні – хтось просто байдужий, хтось до кінця не розуміє наскільки деякі ресурси Інтернет-мережі можуть бути небезпечними, а хтось не вміє користуватися журналом відвідування сайтів.

Вважаємо, сьогодні є вкрай необхідними своєчасне інформування підростаючого покоління, батьків, вчителів щодо загроз мережі Інтернет та навчання їх елементарним правилам безпечного

спілкування у соціальних мережах. Адже, хто попереджений, той і озброєний.

Зрозуміло, загрози безпеці, які чигають на дітей (тут доречно зауважити, Конвенція ООН з прав дитини визначає дитину як особу у віці до 18 років) у соціальних мережах, стосуються не лише юних громадян України, але і усіх дітей у всіх частинах світу.

Розглянемо та докладно опишемо загрози безпеці дітей у соціальних мережах, розбивши їх на великі групи.

Залежність від соціальних мереж. Розвиток телекомунікаційних та комп'ютерних технологій сприяє поширенню явища, яке сучасна соціальна психологія визначила як «самотність в натовпі». Соціальні мережі через їх здатність створювати специфічний ефект присутності за рахунок високого рівня «іммерсивності» (занурення в середовище) призводять до виникнення проблеми залежності (адикції). Вона більш небезпечна ніж, приміром, залежність від комп'ютерних ігор. Якщо доступ до Інтернету зникає, залежний від соцмереж користувач відчуває «велике горе». З'являються психологічні проблеми такі, як депресія, поганий сон, виникають конфлікти в реальному житті. Якщо дитина перебуває в соціальних мережах більше 4 годин на добу, то вона удвічі частіше страждає від депресії і втричі частіше – від порушення сну, ніж та, яка проводить в соціальних мережах менше часу [8].

Більшість дослідників проблеми Інтернет-адикції погоджуються [9], що основними факторами, які приваблюють і, як наслідок, провокують виникнення залежності від соціальних мереж, є такі:

– анонімність соціальних взаємовідносин між учасниками;

– можливість приховати/розкрити фобії, комплекси і таємні потяги;

– можливість зміни ідентифікації (імені, статі, віку, національності, зовнішності);

– подолання власної внутрішньої ураженості;

– реалізація уявлень, фантазій;

– «психологічний ексгібіціонізм»;

– компенсація психологічних комплексів завдяки участі в неформальних об'єднаннях;

– проведення часу в середовищі подібних до себе;

– «інформаційний вампіризм».

Загалом фактори виникнення та умови формування мережевої залежності можна поділити на дві групи:

– кібернетичні – об'єктні умови і фактори, пов'язані із властивостями кіберсередовища;

– індивідуально-психологічні – суб'єктні фактори, пов'язані з особистісними властивостями кіберкористувачів.

Соціальні мережі змінюють спосіб спілкування дітей з ровесниками, спосіб доступу до інформації, спосіб висловлення думки, спосіб розміщення і спільного використання творчого контенту. У дітей, які виросли в соціальних мережах, втрачаються навички міжособистісного спілкування; розвивається синдром гіперактивності; відзначається підйом психотичних проявів, таких як марення, неспокій, сплутаність свідомості, тривога, підвищена вразливість; формується відчуття безкарності; відсутні знання про добро і зло, про моральні закони соціуму, про межі поведінки і т.д. Потенційна небезпека надто активної поведінки у соціальних мережах має у педіатрії свою назву – «Facebook-депресія». У соцмережах спілкування "перекочовує" зі світу реального у віртуальний, і по той – інший бік екрану, нажаль, живе доволі значний відсоток дітей. Слід визнати, спілкування, у форматі подібних комунікаційних ресурсів, навряд чи може претендувати на статус повноцінного, це радше – квазіспілкування. До речі, китайськими лікарями Інтернет-залежність офіційно визнано хворобою, яку відповідно лікують в клініках.

Цікавими є також результати дослідження [10], проведеного групою вчених під керівництвом Пауля Кіршнера (Paul Kirschner) в одному з американських університетів, які довели факт зниження академічної успішності на 20 % у студентів, що активно користуються соціальними мережами. Крім того ними виявлено: ті студенти, які не захоплюються соцмережами, приділяють навчанню в середньому на 88 % більше часу (йдеться про час самостійної підготовки до занять).

Інший діяч, член редакційної ради енциклопедії «Британіка», що зажив слави «порушника спокою» в світової ІТ-спільноти, Ніколас Kapp (Nicholas Carr) у своїй резонансній книзі «The Shallows», стверджує: Інтернет привів до «побіжного читання, поспіху, відволікання думки і поверхневого засвоєння знань» [10] .

Розходження між реальним "я" та створеним у соцмережах образом. Сучасний віртуальний кібернетичний простір має вплив, до кінця незбагнений суспільством, на визначення стилю життя молодих людей. Слово «віртуальний» у масовій свідомості сприймається як щось ілюзорне, умовне, уявне і це недарма, адже з латині virtualis – це вигаданий, уявний. У свій час психологи визначали таке поняття, як ескапізм (англ. escape – втекти, втеча, врятуватись) – прагнення особистості ухилитися від реалій життя, сховатися у світі вигаданому, примарному, бажання знайти прихисток там, де можна відчувати себе більш комфортно – у світі ілюзій, фантазій. Кожен користувач у соцмережах може придумати собі цілком нове «амплуа», нову поведінку, нове життя. І малоймовірно, що випадкові «друзі» з «павутиння» колись дізнаються правду. У цьому своєму вигаданому «новому житті» молода людина не зобов'язана відповідати за свої висловлювання і навіть дії та вчинки – тим паче, що вона це робить не від себе, а значить може поводитися як завгодно. Останнім часом багато хто «заводить» навіть по кілька аккаунтів у різних соціальних мережах, щоб мати можливість «надівати» різні соціальні маски. У представників різноманітних дослідницьких напрямів у зв'язку з цим явищем з'являються запитання, що не мають однозначних відповідей: «Чи ці маски приховують реальне «я», чи є фігурами Бажання? Можливо, вони – енергетичні вампіри? Або одноразові фішки в комп'ютерних іграх? Як можна встановити з ними зв'язок? Яка їх

онтологія?» Не викликає сумніву лише той факт, що поява цифрових двійників ускладнила проблему людської ідентичності.

Доступ до небажаного контенту. Під небажаним контентом розуміємо нелегальні та шкідливі матеріали, що не відповідають віковим особливостям дітей і негативно впливають на стан їх фізичного та психічного здоров'я.

Контентні загрози у соціальних мережах – це матеріали (тексти, зображення, аудіо, відеофайли, посилання на сторонні ресурси), які містять насильство, агресію, еротику і порнографію, нецензурну лексику, інформацію, що розпалює расову ненависть, пропаганду анорексії і булімії, суїциду, азартних ігор, наркотичних речовин і т.д.

Беззаперечно, соціальні мережі є чудовим інструментом для задоволення таких потреб дітей як допитливість, бажання навчитися новим речам, пізнати незвідані грані знань. Діти, проводячи свій час у соцмережах, набувають нового статусу – статусу громадян цифрового он-лайнового світу, котрий, нажаль, немає жодних обмежень, цензури, табу чи застережень. Недосконалість законодавства, яке б регулювало діяльність електронних ЗМІ, зумовлює те, що кожного разу, користуючись послугами соціальних мереж, діти опиняються в ніким неконтрольованому просторі з величезною кількістю інформації, у тому числі і шкідливою, що, безперечно, має негативний вплив на розвиток їх внутрішнього світу та сприйняття навколишнього середовища. Згідно з статистичними даними [11] в п'ятірку найбільш популярних у дитячому середовищі пошукових запитів входить слово «порно», а цього «добра» у соціальних мережах достатньо. І провина у цьому навіть не адміністраторів соціальних мереж, котрі докладають максимум зусиль, щоб відфільтровувати подібні тематичні групи, а користувачів, які безперервно створюють ресурси такого змісту, переміщують їх із групи в групу, випереджаючи дії служби безпеки. Більше того, гарантовано, і це є серйозним приводом для хвилювання, що дитина, блукаючи тенетами соціальних мереж, зіткнеться із небажаним контентом, навіть якщо вона цього і на прагнула.

Розкриття дитиною конфіденційної інформації про себе і свою сім'ю. Відкритість соціальних мереж дає змогу зловмисникам легко реалізувати метод атаки «маскарад» – користувачі самі надають багато особистих даних. Вони сприймають соціальні мережі як електронні щоденники, забуваючи про те, що на відміну від їх паперових аналогів соціальні мережі загальнодоступні. Інформація, яка розміщена на сайтах соцмереж, доволі часто нагадує досьє на користувача і тому, природно, викликає інтерес у сторонніх людей. Існує навіть таке поняття, як «викрадення особистості». Сучасні соціальні мережі пропонують користувачу вказати про себе майже все: фото, відео, зв'язки, хобі, освіту, інформацію про місце навчання, праці, громадські місця, в яких буває, особисті думки і т.д. Такі «вимоги» діти сприймають як необхідність, і заносять особисту інформацію в усі графи. Згідно з результатами досліджень ЮНІСЕФ «Покоління UaNet» [5], багато дітей, активно спілкуючись в соцмережах, вказує номер мобільного телефону (46%), домашню адресу (36%), тощо. Складається враження, що для збору приватної інформації не обов'язково вдаватися до «зовнішнього спостереження» чи прослуховування засобів зв'язку – достатньо лише зайти в мережу Інтернет. Тим більше, що не завжди у користувача, який в свій час розмістив інформацію, є можливість її вилучити. Бо навіть у випадку вилучення даних, вони можуть залишитися у кеші пошукових серверів (наприклад, збережені Яндексом сторінки), а якщо інформація проіснувала достатньо довго – то попасти в webarchive.org.

Джерело ukrDay попереджає [12]: Facebook, «Вконтакте», «Одноклассники» та їм подібні – потенційні інформатори. Безкарна, здавалося б, публічність у цих сервісах – питання часу. У базі даних зібраний гігантський компромат на всіх користувачів, який готовий, як переконаний ukrDay, опинитися в руках спецслужб. Підтвердження цьому – описане в Інтернет-ресурсах відкриття, зроблене на підставі тестувань австралійським технологом Ніком Цубріловічем (Nik Cubrilovic) – Facebook впровадив алгоритм, що дає змогу стежити за відвідуваннями його користувачами інших сайтів навіть у випадку, коли ті вийшли із сторінки соцмережі [13]. Коли користувач натиснув на кнопку «Вихід», Facebook замість того, щоб видалити cookie, просто підмінює їх, створюючи видимість виходу і водночас зберігаючи інформацію про аккаунт користувача та інші унікальні дані, на основі яких може ідентифікувати його. Зараз Facebook порівнюють з панoптикумом – ідеальною, за проектом англійського філософа Джеремі Бентама (Jeremy Bentham), будівлею для в'язниці, наглядач якої має можливість спостерігати за всіма ув'язненими, проте ув'язнені ніколи не знають у який саме момент стежать за ними.

До речі, нещодавно арсенал кіберзлочинців та Інтернет-маркетологів поповнився новим засобом крадіжки особистих даних – соціальними ботами. Соціальні боти (англ. socialbot) – це програми, створені для імітації поведінки людей в соціальних мережах. Основним їх завданням є продукування несправжніх профілів, здатних ефективно викрадати персональні дані користувачів соціальних спільнот, а також штучно викликати, вводячи в оману, їх інтерес до тих чи інших веб-ресурсів. За інформацією канадських вчених з University of British Columbia Vancouver зараз придбати подібний набір скриптів можна в Інтернеті всього за 29 $ [14]. Тобто подібні технології не просто існують, а й доступні для кожного охочого. Використовування таких програм можливе і для інших цілей: для розповсюдження спаму, шкідливого програмного забезпечення, проведення прихованих рекламних кампаній і т.д.

Перехід від віртуальних стосунків до реальних. Подамо статистичні дані тайських дослідників [15]: 24 % дітей віком 7–11 років зустрічалися з друзями, з якими познайомилися через соціальні мережі. Ще 24 % дуже б хотіли це зробити. Більшість дітей ішли на зустріч зі своїми друзями, а 25 % були самі без супроводу (незважаючи на свій вік). У 58 % випадків зустріч з «другом» була неприємним сюрпризом, тому що діти зрозуміли, що їхній віртуальний «друг»

брехав про себе. Підлітки були здивовані при зустрічі з тими, з ким мали зв'язки в Інтернеті в 48 % і шоковані у 28 %. Причини ті ж самі.

Кібербулінг (англ. cyberbullying від bully – хуліган, забіяка, грубіян, гвалтівник) – переслідування повідомленнями, що містять образи, агресію, залякування; хуліганство; соціальне бойкотування за допомогою використання сучасних електронних технологій, у тому числі різних сервісів соціальної мережі.

Волонтерами Київського психологічного центру «Територія психотерапії та тренінгу «Психолог» проведене незалежне опитування київських школярів віком від 10 до 16 років [16]. В опитуванні прийняли участь 346 охочих учнів. 62 % опитаних визнали застосування по відношенню до себе електронних технологій, які можна розцінювати проявом кібертероризму. Частіше всього це була нецензурна лайка (49 %); пропозиції відвідати порносайт, переглянути відео із сценами насильства (26 %). Майже щочетвертого користувача мережі ображали, над ним насміхались. 26 % респондентів засвідчували випадки шантажу та погроз на свою адресу. 54 % молодих людей це дратувало, 40 % відчували сором, у 14 % опитаних це викликало страх. Майже 4 % жертв кібербулінгу звертались за психологічною допомогою.

Згідно з дослідженнями компанії Harris Interactive [17] більшість тінейджерів стверджують, що їхні однолітки займаються кібербулінгом, бо вважають це кумедним заняттям (81 %); хочуть помститися комусь (64 %); сприймають свою жертву хронічною невдахою (45 %). Підлітки також переконані: кібербулери тому такі активні, бо не бояться відплати.

Методи кібербулінгу, використовувані у соціальних мережах для залякування і цькування своїх «потенційних жертв», вражають різноманітністю і «вишуканістю»:

− Злам сторінки для отримання особистої інформації про її власника з метою подальшого використання цієї інформації для шантажувань.

− Блокування аккаунта жертви.

− Розсилання масових скарг і претензій на власника аккаунта.

− Створення аккаунта від імені жертви (англ. impersonation – удавання кого-небудь) та використання його для дискредитації цієї особи.

− Переслідування (англ. harassment – приставання, домагання) – довготривале регулярне надсилання своїй «потенційній жертві» повідомлень, шантажування якимись фактами з її життя.

− Троллінг (англ. trolling – «ловля риби на блешню») – розміщення в соціальних мережах провокаційних повідомлень з метою викликати флейм («суперечку заради суперечки») і тим самим спровокувати конфлікти між учасниками, взаємні образи шляхом порушення правил етичного кодексу Інтернет-взаємодії, тощо.

− Флеймінг (англ. flaming – розпалювати) – це обмін, як правило, короткими емоційними репліками між двома користувачами соцмережі – агресором (іноді, їх може бути декілька) і «потенційною жертвою». Мета агресора – принизити «жертву» і отримати від цього моральне задоволення. Деколи така дискусія перетворюється на затяжний конфлікт – холівар (англ. holiwar – священна війна).

− Онлайн-відчуження (остракізм, ізоляція, соціальне бойкотування). Будь-якій людині, а тим більше дитині, притаманне бажання бути прийнятим у суспільстві. Кіберостракізм у соцмережах проявляється у вигляді відсутності відповіді на миттєві повідомлення, а також через виключення із списку друзів чи групи. Відчуження у віртуальному просторі сприймається як соціальна смерть і може призвести до повного емоційного руйнування дитини.

− Хеппіслепінг (англ. happy slapping – щасливе ляскання) – так називають відеоролики, в яких зняті сцени насильства над «потенційною жертвою». Найчастіше подібні ролики розміщуються, зрозуміло, без згоди жертви на таких ресурсах, де їх може переглядати велика кількість людей. Під цей критерій ідеально підпадають соціальні мережі.

Кібергрумінг (англ. cybergrooming). Спеціальний термін «грумінг» означає встановлення дорослими людьми дружніх відносин з дитиною з метою вступу в сексуальний контакт. Знайомство в соціальній мережі здійснюється ними найчастіше від імені однолітка дитини. Он-лайн-хижаки добре знаються на особливостях дитячої психіки. Вони в курсі останніх музичних новинок і їм все відомо про хобі, якими найчастіше цікавляться діти. Вони уважно вислуховують дітей і «співчувають» їхнім проблемам. Спілкуючись особисто («в приваті»), кіберзлочинці входять у довіру до неї, намагаються дізнатися особисту інформацію і домовитися про зустріч. І вже під час зустрічі діти з'ясовують, що їх віртуальний друг зовсім не той, за кого себе видавав в Інтернеті: це доросла людина з корисливими і навіть "хворими" планами щодо їх стосунків. До речі, за статистикою onGuard Online [18], 22 % молодих осіб у віці від 16 до 24 років взагалі не знають людей, з якими вони «дружать» віртуально. І це дуже насторожує.

Найбільш вразливими до кібергрумінгу є молоді люди, яким притаманні такі риси:

− вони початківці в он-лайні й незнайомі з «мережевим етикетом»;

− хочуть спробувати у житті щось нове, авантюрне;

− активно шукають уваги та дружби;

− бунтівні;

− ізольовані або самотні;

− їх приваблюють субкультури, що існують за межами їхнього власного, контрольованого батьками, світу.

Секстінг (англ. sexting – sex і texting, тобто «секс» і «обмін повідомленнями») – це своєрідний аналог ексгібіціонізму, пересилання особистих фотографій, повідомлень інтимного змісту за допомогою сучасних засобів зв'язку, в тому числі, засобами соціальних мереж.

Вперше термін «секстінг» був ужитий у 1997 році в журналі Sunday Telegraph, і з тих пір і слово, і саме явище набули досить широкого поширення. Американські медики опублікували у журналі

Archives of Pediatrics and Adolescent Medicine результати соціологічного дослідження, що стосується звичок сучасних підлітків. Середній вік опитаних – 15,8 років. 28 % опитаних підлітків зізналися, що фотографували себе без одягу та пересилали ці пікантні зображення своїм знайомим, 57 % заявили, що отримували повідомлення з проханням надіслати подібні світлини [19].

Ні психологи, ні соціологи, ні представники влади поки що не визначилися, як ставитися до секстінгу. Самі ж підлітки не бачать в секстінгу нічого особливого: багато з них вважає це свого роду грою, «повітряним поцілунком XXI століття», а для деяких – це спосіб добитися популярності серед однолітків, форма самовираження і знак довір'я. За статистикою, серед підлітків найчастіше секстінгом «займаються» закохані, надсилаючи один одному відверті фотографії. Друга за популярністю причина секстінгу – бажання похизуватися пригодами перед іншими, а третя – прагнення привернути увагу свого об'єкта обожнювання.

Споживацькі загрози. Зловмисники під різними приводами змушують дітей у соціальних мережах підключатися до платних послуг. На жаль, діти не завжди помічають підступ і не звертаються за допомогою до дорослих. Як приклад, можна навести послугу передплати на «преміальні» номери. Дитина прийнявши рішення «закачати» яку-небудь «безкоштовну» програму на кшталт сервісу для обміну миттєвими повідомленнями ICQ або будь-яку іншу програму, останнє, що вона буде читати і то недбало (у чому не має сумніву), це умови угоди під час завантаження дистрибутиву. А вони, як правило, містять пункт про обов'язкову передплату на пропоновані сервіси. Таким чином і з'явиться заборгованість перед сайтом, котру необхідно буде погасити.

Ще один приклад. Сьогодні майже всі азартні комп'ютерні ігри перекочували в додатки соціальних мереж. Для оплати використовується внутрішня валюта соціальної мережі. Відомі випадки, коли діти для підняття свого рейтингу витрачали реальні гроші батьків (шляхом надсилання SMS) за "золоті", використовувані в грі, монети.

Віруси. Користувач соцмереж має велику імовірність заразити комп'ютер вірусами. Соціальні сайти, пропонуючи широкий набір сервісів, як ігрових, так і для завантаження інформації різноманітної форми та змісту – фотографій, музики, відео, неявно піддають загрозі комп'ютер їх користувачів, оскільки останні можуть, під виглядом додатку скачати вірус чи троянську програму. Зацікавившись змістом листа від, так званого, друга, дитина, не задумуючись, вибере посилання, яке може перевести її на сайт, що завантажує на комп'ютер всілякі шкідливі програми. Серед таких програм, зокрема, можуть бути:

– програми клавіатурних шпигунів (англ. keylogger) – це програми, які відслідковують усі дії користувача на комп'ютері та інформацію, що на ньому вводиться, з метою її викрадення. Якщо користувач здійснює покупки або користується он-лайн-банкінгом на цьому ж комп'ютері, то такі програми, зрозуміло, можуть викрасти паролі та логіни для Інтернет-банкінгу, дані про платіжну карточку, включаючи її номер, PIN-код та ім'я власника;

– вінлокери (англ. winlocker) – програми, які перекривають зображенням весь екран, пропонуючи при цьому користувачу заплатити певну, як правило, немалу суму, щоб розблокувати комп'ютер. Дуже часто вінлокери використовують світлини порнографічного змісту, супроводжуючи її погрозою заявити про користувача комп'ютера, як про любителя забороненого, у правоохоронні органи;

– потрапляння в бази розсилки спаму. Якщо електронна адреса користувача з'явиться у відкритому доступі, то вона з легкістю може потрапити до кіберзлочинця, який буде атакувати її незліченою кількістю спаму.

Зрозуміло, позбавлення від описаних комп'ютерних вірусів і подібних їм потребуватиме значних часових і фінансових витрат.

Висновки

Усе викладене вище – не привід робити крок назад, відмовляючись від благ кібер-цивілізації. Наведена інформація – заклик об'єднати зусилля всіх членів суспільства – уряду, різних фондів, комерційних структур, міжнародних організацій, громадянського суспільства, сімей та, власне, самих дітей. Лише глобальна скоординована реакція на розглянуті проблеми дасть змогу реалізувати право дітей на захист в умовах необмеженого їх доступу до сучасних інформаційно-комунікативних технологій. Маємо глибоке переконання: безпечної поведінки у віртуальному просторі на засадах дотримання загальновизнаних правил етикету та поваги до свобод оточуючих потрібно вчити з раннього віку, прищеплюючи принципи цивілізованого спілкування, у тому числі, засобами масової комунікації.

Література

[1] Первая в мире социальная сеть [Электронный ресурс]. – Режим доступа : http://wd-x.ru/first-social-network/

[2] Social Media around the World 2012 (by InSites Consulting) [Electronic recourse]. – Access mode: http://www.slideshare.net/InSitesConsulting/social-media-around-the-world-2012-by-insites-consulting

[3] Facebook виповнилося 10 років: Цукерберг розповів про плани соцмережі на наступне десятиліття [Електронний ресурс]. – Режим доступу : http://dt.ua/TECHNOLOGIES/facebook-vipovnilosya-10-rokiv-cukerberg-rozpoviv-pro-plani-socmerezhi-na-nastupne-desyatilittya-136804_.html

[4] Рейтинг сайтов Украины – исследование аудитории Интернета gemiusAudience: охват аудитории, посетители сайта [Электронный ресурс]. – Режим доступа : http://www.audience.com.ua/pages/display/visitors

[5] Безпека молоді в Інтернеті: Дослідження ЮНІСЕФ в Україні, Росії та Туреччині [Електронний ресурс]. – Режим доступу : http://www.unicef.org/ukraine/ukr/media_18561.html

[6] Мироненко А. В. Темпоральні виміри Інтернет-реальності [Електронний ресурс] / А. В. Мироненко // Психологічні та педагогічні проблеми Інтернет-реальності : наук.-практ. сем., 14 лютого 2012 р. : тези доп. – Київ, 2012. – Режим доступу: http://ispp.org.ua/podiy_37.htm

[7] Литовченко І. В. Діти в Інтернеті: як навчити безпеці у віртуальному світі [Електронний ресурс] /[І. В. Литовчеко, С. Д. Максименко, С. І. Болтівець та Ін]. – К. Вид-во ТОВ "Видавничий будинок "Аванпост-Прим", 2010. – 48 с. – Режим доступа: http://bezpeka.kyivstar.ua/f/2/materials/the_benefit_for_parents/A5_Ukrainian.pdf

[8] Берегите детей от социальных сетей [Электронный ресурс]. – Режим доступа : http://eduinspector.ru/2013/09/04/beregite-detej-ot-socialnyh-setej/

[9] Мельник Г. С. Исследования Интернет-зависимости в медиапсихологии [Электронный ресурс] / Г. С. Мельник. – Режим доступа : http://ru-cyberpsy.blogspot.com/2011/04/blog-post_12.html

[10] Доведено негативний вплив соціальних мереж на успішність [Електронний ресурс]. – Режим доступу : http://aratta-ukraine.com/news_ua.php?id=11408

[11] Брачевський С. Категорії загроз для дітей в Інтернеті [Електронний ресурс] / С. Брачевський. – Режим доступу : http://krosha.net/article10022013kategorii-zagroz-ditej-internet.html

[12] За нами следят через Интернет [Электронный ресурс]. – Режим доступа : http://ukrday.com/hi-tech/novosti.php?id=477

[13] Logging out of Facebook is not enough [Electronic recourse]. – Access mode : http://www.nikcub.com/posts/logging-out-of-facebook-is-not-enough

[14] Socialbots used by researchers to «steal» Facebook data [Electronic recourse]. – Access mode : http://www.bbc.co.uk/news/technology-15553192

[15] Безпечне користування сучасними інформаційно-комунікативними технологіями : методичні рекомендації [Електронний ресурс] / [О.А. Удалова, О.В. Швед, М.В. Євсюкова та Ін]. – К. : Україна, 2010. – 72 с. – Режим доступу : http://lib.selyam.net/tw_files2/urls_102/116/d-115783/7z-docs/1.pdf

[16] Тичковський Є. Що таке кібербулінг? Чи потрібно з ним боротись [Електронний ресурс]. – Режим доступу : http://psiholog.com.ua/node/11?q=node/673

[17] Moessner Chris Cyberbullying [Electronic recourse]/ Chris Mossner // Trends&Tudes. – 2007. – V. 6, Issue 4. – P. 1-4. – Access mode : http://www.ncpc.org/resources/files/pdf/bullying/Cyberbullying%20Trends%20-%20Tudes.pdf

[18] Касперский Е. Дети и соцсети. Проблема, которую лучше решить поздно, чем никогда [Электронный ресурс] /Е. Касперский. – Режим доступа : http://e-kaspersky.livejournal.com/64468.html?thread=2221012

[19] Temple Jeff R. Teen Sexting and Its Association With Sexual Behaviors [Electronic recourse]/[Jeff R. Temple, Jonathan A. Paul, Patricia van den Berg and Et.] // Archives of Pediatrics & Adolescent Medicine. – 2012. – V. 166, No.9. – P. 828-833. – Access mode : http://archpedi.jamanetwork.com/article.aspx?articleid=1212181

УДК 004.77:004.56 (045)

Кухарская Н.П., Кухарский В.М. Угрозы безопасности детей в социальных сетях

Аннотация. *В последнее время социальные сети стали неотъемлемым атрибутом жизни детей. Подрастающее поколение, обезумев от соцсетей, редко осознает последствия своей чрезмерной открытости и гиперкоммуникативности в виртуальном пространстве. Количество детей, являющихся завсегдатаями соцсетей, все увеличивается благодаря технологии Wi-Fi и новым возможностям доступа к Интернету с мобильных телефонов, смартфонов, ноутбуков, игровых консолей, планшетов и т.п. Родители из-за своей неосведомленности по Интернет-угрозам детской безопасности, как правило, не видят ничего плохого в том, что их чадо имеет страницы в социальных сетях. Одновременно вопросы по обеспечению безопасности подрастающего поколения в соцсетях требуют неотложного скоординированного решения. В статье сделан акцент на актуальности формирования информационной культуры личности – детей, их родителей и наставников, как основного механизма решения данной проблемы; определены основные угрозы безопасности детей в социальных сетях; проведен их комплексный анализ и представлены характеристики их влияния.*

Ключевые слова: *социальная сеть, угрозы, безопасность детей, нежелательный контент, кибербуллинг , кибергруминг, секстинг, компьютерный вирус.*

Kukharska N., Kukharskyy V. Threats to children security in social networks

Abstract. *Recently, social networks have become an inherent part of children's lives. Younger generation, which is a big fan of social networks are rarely aware of the consequences of their excessive and hyper communicative openness in virtual space. The number of children who are regular users of social networks, increased by introducing Wi-Fi technology and a new form of access to the Internet from mobile phones, smart phones, laptops, gaming consoles, tablets, etc. Parents because of their lack of knowledge on the issues of child safety on the Internet tend to see nothing wrong in the fact that their child has a page on social networks. However, issues relating to the safety of the younger generation in social networks require urgent coordinated solution. The article focuses on the relevance of personal information culture development – children, parents, teachers, as the key solution to this problem; it is identified the main threats to the children security in social networks; conducted a comprehensive analysis of their and their effects.*

Key words: *social network, threats, child safety, objectionable content, cyberbullying, cybergrooming, sexting, a computer virus.*

Отримано *21 травня 2014 року*, затверджено редколегією *10 червня 2014 року*