УДК 613.955:004.7

ФОРМУВАННЯ В ДІТЕЙ КОМПЕТЕНЦІЙ БЕЗПЕЧНОГО ВИКОРИСТАННЯ ІНТЕРНЕТ-МЕРЕЖІ

Варивода К. С.
ДВНЗ «Переяслав-Хмельницький державний педагогічний університет імені Григорія Сковороди», Україна, Переяслав-Хмельницький

У статті визначено основні загрози безпеці дітей у Інтернет мережі, проведено їх комплексний аналіз та подано характеристики їх впливу. Автор розкриває проблему формування безпечної поведінки дітей в Інтернет-мережі. Виділяться поради та правила Інтернет-безпеки та Інтернет-етики для дітей. Автором зроблено акцент на актуальності формування інформаційної культури особистості – дітей, їх батьків, наставників, як основного механізму розв'язання зазначеної проблеми. На основі аналізу вітчизняних та зарубіжних досліджень, концепцій, теорій та моделей автором встановлено, що процес формування безпечної поведінки дітей в Інтернет-мережі є багатоаспектним процесом, на який впливає значна кількість факторів. Автор приходить до висновку, що діяльність з формування безпечної поведінки дітей в Інтернеті має носити комплексний та міжінституційний характер і передбачати формування інформаційної культури особистості та організації безпечного процесу кіберсоціалізації.

Ключові слова: Інтернет, загроза, безпека дітей, небажаний контент, кібербулінг, кібергрумінг, комп'ютерний вірус.

Варывода Е. С. Формирование у детей компетенций безопасного использования Интернет-сети / ГВНЗ «Переяслав-Хмельницкий государственный университет имени Григория Сковороды», Украина, Переяслав-Хмельницкий.

В статье определены основные угрозы безопасности детей в Интернете, проведен их комплексный анализ и представлены характеристики их влияния. Автор раскрывает проблему формирования безопасного поведения детей в Интернет-сети. Выделяются советы и правила Интенет-безопасности и Интернет-этики для детей. Автором сделан акцент на актуальности формирования информационной культуры личности – детей, их родителей и наставников, как основного механизма решения данной проблемы. Автор приходит к выводу, что деятельность по формированию безопасного поведения детей в Интернете должна носить комплексный и межинституциональный характер и предусматривать формирование информационной культуры личности и организацию безопасного процесса киберсоциализации.

Ключевые слова: Интернет, угрозы, безопасность детей, нежелательный контент, кибербуллинг, кибергруминг, компьютерный вирус.

Varyvoda E. S. Positive and negative aspects of the interaction of contemporary youth in social networking / SHEE «Pereyaslav-Khmelnitskiy

Gregory Skovoroda State Pedagogical University», Ukraine, Pereyaslav-Khmelnytskyi.

The article is identified the main threats to the children security in Internet, conducted a comprehensive analysis of their and their effects. Author reveals the problem of formation of safe children behavior in the Internet. Advices and rules for Internet security and Internet ethics for children are marked out. Author focuses on the relevance of personal information culture development – children, parents, teachers, as the key solution to this problem. On the basis of domestic and foreign studies, concepts, theories and models by established that the formation of safe children behavior in the Internet is a multi-process, on which affects a large number of factors. It was defined that the activities related to children safer behavior in the Internet should be complex and inter-institutional. This implied formation of personal information culture and organizing a safe process of cyber-socialization.

Key words: Internet, threats, child safety, objectionable content, cyberbullying, cybergrooming, a computer virus.

Вступ. Діти значно швидше у порівняні з дорослими адаптуються до стрімких змін інформаційних технологій, легко опановують їх, випереджуючи в обізнаності щодо можливостей їх використання батьків і вчителів. Водночас, через відсутність життєвого досвіду та психологічні вікові особливості такі, як недостатня розвиненість саморегуляторних механізмів, слабкий вольовий і емоційний контроль, імпульсивність поведінки, діти є менш стійкими до інформаційних та програмно-технічних загроз. Вітчизняні та закордонні експерти зазначають, що ідеально «чиста» мережа Інтернет, тобто така, яка позбавлена загроз, у принципі неможлива. Саме тому, сьогодні є вкрай необхідними своєчасне інформування підростаючого покоління, батьків, вчителів щодо загроз мережі Інтернет та навчання їх елементарним правилам її безпечного використання.

Різноманітні аспекти впливу ІТ-технологій на психічне здоров'я дітей в Україні досліджують такі науковці, як В. Ю. Биков, Я. В. Булахова, О. М. Бондаренко, В. Ф. Заболотний, Г. О. Козлакова, О. А. Міщенко, О. П. Пінчук та ін. Причини, ознаки, вплив на розвиток суспільства та шляхи подолання інтернет-залежності серед дитячого населення розглядали в своїх працях В. В. Бурова, А. Е. Войскунський, А. Ю. Єгоров, Н. А. Кузнєцова, О. І. Лаврухіна. Проблему безпеки школярів в Інтернеті піднімають у своїх дослідженнях Н. М. Бугайова, В. В. Вовк, Т. В. Кобець, А. А. Сабліна, В. В. Черноус. Водночас, слід зазначити, що в сучасній літературі обмаль праць, присвячених висвітленню питання формування в дітей і підлітків компетентностей безпечної роботи в Інтернет мережі.

Метою написання статті є висвітлення основних он-лайн небезпек та методів формування в дітей компетенцій безпечної поведінки в Інтернет мережі.

Виклад основного матеріалу. Інтернет є чудовим інструментом для задоволення таких потреб дітей як допитливість, бажання навчитися новим речам, пізнати незвідані грані знань. Діти, проводячи свій час у Інтернеті, набувають нового статусу – статусу громадян цифрового он-лайнового світу, котрий, нажаль, немає жодних обмежень, цензури, табу чи застережень. Недосконаліть законодавства, яке б регулювало діяльність електронних ЗМІ, зумовлює те, що кожного разу, користуючись послугами Інтернету, 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. У зв'язку з цим хочемо підкреслити 4 основних загроз безпеці дітей у Інтернет мережі: залежність від Інтернету, доступ до небажаного контенту, комунікаційні загрози та електронні (кібер) загрози.

Залежність від Інтернету. Головною причиною виникнення комп'ютерної залежності у дітей психологи вважають недостатнє спілкування і взаєморозуміння з батьками, однолітками і значущими людьми. Відповідно до нових діагностичних рекомендацій, інтернет-залежною визнається людина, яка проводить в мережі декілька годин на день і у якої спостерігався щонайменше один з симптомів залежності протягом трьох місяців, зокрема: непереборне бажання ввійти в Інтернет; нездатність контролювати свій час в Інтернеті; розумове або фізичне виснаження; порушень сну і концентрації уваги; дратівливість, депресія, знервованість, труднощі у спілкуванні з людьми в реальному житті [2, с. 14].

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 в Інтернеті – 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 ін. [6, с. 172]

Комунікаційні загрози пов'язані з міжособистісними відносинами Інтернет користувачів і містять в собі небезпеку зіткнутися з психологічними нападами, які здійснюються через електронну пошту, сервіси миттєвих повідомлень (ICQ, Google talk, Skype), чати, форуми, блоги, соціальні мережи, сайти знайомств, веб-сайти, а також за допомогою мобільного зв'язку. Основними комунікаційними загрозами є: розкриття дитиною конфеденційної інформації про себе і сім'ю, кібербулінг і кібергрумінг [2, с. 18].

Розкриття дитиною конфіденційної інформації про себе і свою сім'ю зазвичай відбувається при використанні соціальних мереж. Діти 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 [6, с. 172].

Кібербулінг (англ. cyberbullying від bully – хуліган, забіяка, грубіян) – переслідування, залякування і знущання над дитиною за допомогою цифрових технологій, передачі повідомлень агресивного змісту, розміщення відеороликів, що містять знущання, розкриття анонімності акаунта на форумах і ін. Такі атаки зазвичай є регулярними з одночасним використанням декількох засобів і анонімними, що призводить до того, що залякування наносять серйозну психологічну травму дитині.

Кібергрумінг (анг. cybergrooming / child grooming) – це спілкування та встановлення довірливих відносин з дитиною з метою подальшої особистої зустрічі для вступу в статеві стосунки, фізичного нападу, шантажу, сексуальної експлуатації і насилля. Такі знайомства відбуваються у чатах, на форумах, в соціальних мережах. Злочинець видає себе за однолітка і намагається дізнатися особисту інформацію (адрес, телефон) і домовитися про зустріч. Іноді злочинці виманюють інформацію, за допомогою якої шантажують дитину, наприклад, просять надіслати особисті фотографії або провокують на непристойні дії перед веб-камерою. Кібергрумінг класифікується як кримінальний злочин [1, с. 70].

Електронні (кібер) загрози – це шкідливі програми (віруси, черв'яки, спам-атаки, шпигунські програми, боти), які можуть нашкодити комп'ютеру та порушити конфіденційність особистої інформації. Шкідливе програмне забезпечення використовує широкий спектр методів для проникнення у комп'ютер через носії інформації, електронну пошту, спам, завантажені файли і відвідування веб-сайтів. Основними різновидами електронних загроз є віруси, спам-повідомлення, фішинг, фармінг. Всі ці загрози визначаються як кібершахрайство.

Віруси. Користувачі Інтернету мають велику імовірність заразити комп'ютер вірусами. Інтернет 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. Зазвичай діти навіть не здогадуються, що скачуючи музику, фільми, текстові документи та ін., можна заразити комп'ютер шкідливим програмним забезпеченням [4, с. 11–12].

Фішинг (англ. fishing – рибальство) – підміна офіційного сайту схожим, шахрайським з метою виманювання у довірливих або неуважних користувачів мережі персональних даних. Шахраї використовують усілякі прийоми, які найчастіше змушують користувачів особисто повідомляти

конфеденційні дані. Наприклад, шляхом надсилання електронних листів із пропозицією підтвердити реєстрацію акаунта, що містять посилання на сайт, зовнішній вигляд якого копіює дизайн відомих ресурсів.

Фармінг (англ. pharming) – це процедура скритного перенаправлення жертви на помилкову IP-адресу. Шахраї створюють точну копію відомого сайту і після того, як користувач відвідає його, віруси і шпигунські програми проникають на комп'ютер. Таким чином шахраї дізнаються про всі переміщування дитини в Інтернеті і отримують доступ до особистої інформації – від адреси до паролів для входу на різні Інтернет-ресурси [2, с. 21–22].

Спам (англ. spam) – це масова розсилка шкідливих небажаних повідомлень. Вони засмічують електронну скриньку і можуть бути небезпечними для комп'ютера. Через свою анонімність вони стають відмінним інструментом для шахрайства, реклами нелегальних, підроблених та контрафактних товарів, розповсюдження порнографії та інших злочинів. Водночас, спам є засобом доставки шкідливого коду. При цьому шкідлива програма може знаходитися як у додатку до листа, так і на сайті, який відкриється за посиланням зі спам-листа. Окрім цього, спамом, як платформою, часто користуються фішери, щоб заманити користувачів на підроблені сайти, створені для розкрадання конфіденційної інформації [4, с. 17].

В сучасних умовах, у зв'язку з використанням дітьми мобільних телефонів із безперешкодним доступом до Інтернет мережі, батькам і вчителям важко контролювати, які сайти і соціальні мережі вони відвідують. Саме тому, на нашу думку основним засобом для зменшення загроз Інтернет середовища має бути інформування дітей про небезпеки в мережі Інтернет; формування в дітей компетенцій правильного, безпечного поводження в Інтернеті. У зв'язку з цим пропонуємо батькам десять правил, які сприятимуть формуванню в дітей вмінь і навичок безпечного використання Інтернет мережі:

1) *Використовуйте будильник для обмеження часу, який дитина проводить в Інтернеті.* Заздалегідь погодьте тривалість перебування в Інтернеті. Бажано визначити, який час дитина може перебувати в он-лайні, аби не нанести шкоди стану її здоров'я та не сприяти комп'ютерній залежності, яка стала великою проблемою у всьому світі. Обговоріть час перебування дитини в Інтернеті та домовтеся про використання будильника. Таким чином ви уникнете можливих конфліктних ситуацій [3, с. 17].

2) *Навчіть дитину не розголошувати свою конфіденційну інформацію* (прізвище, номер телефону, адресу, номер школи, паролі, власні фото), а особливо без вашого дозволу. При цьому особливу увагу варто зосередити на поясненні наслідків розголошення особистої інформації [7, с. 55].

3) *Використовуйте технічні засоби захисту*: функції батьківського контролю в операційній системі, антивірус та спам-фільтр. Щоб користуватися комп'ютером, необов'язково знати всі його функціональні

можливості. Запросіть спеціаліста, який налаштує операційну систему вашого комп'ютера та покаже, як працювати із батьківським контролем. Краще один раз побачити, аніж багато разів почути. Не використовуйте у себе вдома технічно незахищений комп'ютер. Окрім цього, варто також пояснити дитині необхідність використання вище зазначених програм [4, с. 57].

4) *Поясніть дитині, що завантаження деяких файлів може бути незаконним чи небезпечним* тобто може — заразити комп'ютер вірусами. Перед тим, як завантажити файли з Інтернету (музику, фільм, картинку, програму чи навіть текстовий файл), краще порадитися з вами. Було б добре для початку самостійно віднайти найбільш безпечні сайти на яких дитина з легкістю зможе завантажувати і переглядати безпечний контент. Розкажіть чому небезпечно відкривати підозрілі повідомлення електронної пошти, файли або веб-сторінки від незнайомих людей. При цьому підкресліть, що дитина завжди може звернутися за допомогою якщо в Інтернеті (у повідомленні електронної пошти, на сайті, форумі, чаті) щось незрозуміло, хвилює чи загрожує.

5) *Створіть сімейні правила он-лайн-безпеки для дітей*. Діти навчаються шляхом експериментування. Якщо ви зацікавлені у тому, аби ваша дитина навчалася не на своїх власних помилках, якомога частіше обговорюйте теми, пов'язані із Інтернетом. Так ви невимушено створите власні сімейні правила Інтернет-безпеки. Традиції, норми та правила, які закріпилися у родині, довговічні [2, с. 29].

6) *Поясніть дитині чим небезпечні зустрічі з віртуальними знайомими в реальному житті*. Підкресліть, що віртуальний співрозмовник може видавати себе за іншу людину. Саме тому, якщо в дитини є бажання зустрітися з кимось із віртуальних знайомих, їй потрібно обов'язково домовлятися про зустріч у громадському місці і повідомити про це вас [7, с. 55].

7) *Проводьте більше часу з дитиною, заохочуйте її до обговорення тем, пов'язаних з Інтернетом*. У кожного в житті трапляються помилки. Непотрібно сприймати помилки дітей як життєву проблему. Будуйте з дитиною довірливі стосунки задля того, аби бути впевненими, що у будь-якій ситуації вона вернеться за допомогою саме до вас. Щоб не сталося, ваша дитина повинна знати, що вона завжди може розраховувати на ваше розуміння та підтримку. Хороший рецепт побудови довірливих відносин – щоденне спілкування та спільне проведення вільного часу. У невимушеній атмосфері набагато легше обговорювати «складні» питання [3, с. 17].

8) *Навчайте дітей критично ставитися до інформації в Інтернеті*. Розкажіть дитині, що практично кожен може створити свій сайт, і при цьому ніхто не може проконтролювати достовірність інформації, розміщеної на такому сайті. Діти повинні навчитися відрізняти надійні джерела інформації від ненадійних і перевіряти інформацію, яку вони знаходять в Інтернеті.

Також поясніть дітям, що копіювання і вставка змісту з чужих веб-сайтів можуть бути визнані плагіатом [7, с. 55].

9) *Поясніть дитині, що Інтернет може коштувати реальних грошей*. Діти часто навіть необдумано можуть здійснювати покупки через Інтернет або оплатити певну послугу. Саме тому, важливо проговорити з дитиною, що вона обов'язково повинна радитись із вами перш ніж робити щось подібне.

10) *Навчіть дитину дотримуватись тих же правил поведінки, що і в реальному житті*. Не зважаючи на те, що Інтернет мережа надає відчуття анонімності, дитина завжди повинна пам'ятати про ввічливість і толерантність при спілкуванні з іншими он-лайн користувачами. Водночас, потрібно наголосити, що дитина не повинна відповідати на невиховані і грубі листи. Якщо вона одержуєте такі листи, то повинна повідомити вас про це [2, с. 29].

Водночас слід зауважити, що формування в дітей компетенцій безпечної роботи з Інтернетом, має бути також пріоритетом загальноосвітніх навчальних закладів. Навчання дітей правилам і нормам безпечного використання комп'ютера і Інтернету повинно проводитись *на уроках з основ безпеки життєдіяльності, біології, валеології, фізичного виховання та інформатики*. Зокрема, на уроках з основ безпеки життєдіяльності потрібно розглядати питання онлайн-безпеки користувачів, різні види шахрайств в соціальних мережах, психологічні фактори небезпек пов'язані з надмірним використанням Інтернет мережі. На уроках валеології при вивченні тем щодо режиму навчання та відпочинку, слід ознайомити дітей із значенням для здоров'я людини відпочинку, нормування навантажень та змін видів діяльності. На заняттях з фізичної культури важливо розучити вправи для зняття розумового та м'язового напруження. На уроках інформатики необхідно докладно розглянути гігієнічні, ергономічні та технічні умови безпечної експлуатації комп'ютера; важливо обговорити з учнями способи безпечної поведінки в Інтернет при відправці і отриманні електронної пошти, спілкуванні, здійсненні пошуку інформації, отриманні інформації з файлових серверів, використанні засобів електронної комерції; поняття інформаційного ресурсу, основні інформаційні ресурси суспільства, освітні інформаційні ресурси, правові та етичні аспекти при створенні та використанні інформації, принципи інформаційної безпеки.

Виховні заходи з он-лайн безпеки повинні плануватися і проводиться у навчальному закладі регулярно. Передовий педагогічний досвід свідчить, що форми проведення виховних заходів можуть бути самі різні, наприклад, бесіди, вікторини, стінні газети, батьківські збори, ігри, тренінги, дискусії тощо. Головна мета виховних заходів є усвідомлення учнями відповідальності за свої дії у «віртуальному» середовищі, засвоєння етичних норм поводження в цьому середовищі, результатом чого є формування в учнів культури і компетентності з інформаційної безпеки [4, с.24–25].

Висновки. Таким чином, варто підкреслити, що саме в родині закладаються основи поведінки дитини в реальному світі, віртуальний простір не має бути винятком. Батькам слід приділяти серйозну увагу вихованню дітей і підвищенню їхньої обізнаності щодо загроз інформаційного середовища. Необхідно пам'ятати, що комп'ютер для дітей повинен бути інструментом для навчання і розвитку, а не лише розваг та ігор. Незважаючи на широкі можливості віртуального спілкування, воно не може виключати чи замінювати реальних стосунків між людьми. Водночас, для забезпечення єдиних вимог і умов он-лайн безпеки дітей, як у школі, так і вдома, необхідною є співпраця батьків і вчителів. Вчителі повинні інформувати батьків стосовно питань Інтернет-безпеки, розробляти спільні методи і засоби для ефективного навчання дітей основним правилам безпечної поведінки в Інтернет просторі.

Література:

1. Данильчук Л. О. Ризики та небезпеки мережі Інтернет: до проблеми інформаційної захищеності дітей / Л. О. Данильчук // Педагогічний дискурс. – 2012. – Вип. 13. – С. 68–71.

2. Діти в Інтернеті: як навчити безпеці у віртуальному світі / [Литовченко І. В., Максименко С. Д., Болтівець С. І., Чепа М. А., Бугайова Н. М.]. – К.: ТОВ «Видавничий Будинок Аванпост-Прим», 2010. – 48 с.

3. Литвиненко О. В. Дитяча безпека в Інтернеті: технології та рекомендації на допомогу батькам [Електронний ресурс] / О. В. Литвиненко // Безпека дітей в Інтернеті: попередження, освіта, взаємодія : Матеріали обласної науково-методичної Інтернет-конференції (м. Кіровоград, 11 лютого 2014 р.) – Кіровоград, 2014. – С. 15–18. – Режим доступу: http://konf.koippo.kr.ua/blogs/index.php/blog2/

4. Кочарян А. Б. Виховання культури користувача Інтернету. Безпека у всесвітній мережі : навчально-методичний посібник / А. Б. Кочарян, Н. І. Гущина. – Київ, 2011. – 100 с.

5. Кузнєцова І. В. Дитина і комп'ютер: виховання особистості в інформаційному суспільстві / І.В. Кузнєцова // Обдарована дитина. – 2010. – № 6. – С. 41–46.

6. Кухарська Н. П. Загрози безпеці дітей у соціальних мережах / Н. П. Кухарська, В. М. Кухарський // Безпека інформації. – 2014. – Т. 20, № 2. – С. 169–175.

7. Паукова А. С. Ідея інформаційного захисту дітей на сторінках педагогічної преси США / А. С. Паукова // Вісник ЛНУ імені Тараса Шевченка. – 2013. – № 13 (272), Ч. 3. – С. 50–58.

References:

1. Danylchuk L. O. Ryzyky ta nebezpeky merezhi Internet : do problemy informacijnoyi zaxy`shhenosti ditej / L. O. Danylchuk // Pedagogichny`j dy`skurs. – 2012. – Vyp. 13. – S. 68–71.

2. Dity v Interneti: yak navchyty bezpeci u virtualnomu sviti / [Lytovchenko I. V., Maksymenko S. D., Boltivecz S. I, Chepa M. A., Bugajova N. M.]. – K.: TOV «Vydavnychyj Budynok Avanpost-Prym», 2010. – 48 s.

3. Lytvynenko O. V. Dytyacha bezpeka v Interneti: texnologiyi ta rekomendaciyi na dopomogu bat`kam [Elektronnyj resurs] / O. V. Lytvynenko // Bezpeka ditej v Interneti: poperedzhennya, osvita, vzayemodiya: Materialy oblasnoyi naukovo-metody`chnoyi Internet-konferenciyi (m. Kirovograd, 11 lyutogo 2014 r.) – Kirovograd, 2014. – S. 15–18. Rezhym dostupu: http://konf.koippo.kr.ua/blogs/index.php/blog2/

4. Kocharyan A.B. Vyxovannya kultury korystuvacha Internetu. Bezpeka u vsesvitnij merezhi: navchalno-metodychnyj posibnyk / A. B. Kocharyan, N. I. Gushhy`na. – Ky`yiv, 2011. – 100 s.

5. Kuznyeczova I. V. Dytyna i kompyuter: vyxovannya osobystosti v informacijnomu suspil`stvi / I. V. Kuznyeczova // Obdarovana dytyna. – 2010. – № 6. – S. 41–46.

6. Kuxarska N. P. Zagrozy bezpeci ditej u social`ny`x merezhax / N. P. Kuxars`ka, V. M. Kuxarskyj // Bezpeka informaciyi. – 2014. – T. 20, № 2. – S. 169–175.

7. Paukova A. S. Ideya informacijnogo zaxystu ditej na storinkax pedagogichnoyi presy SShA / A. S. Paukova // Visnyk LNU imeni Tarasa Shevchenka. – 2013. – № 13 (272), Ch. 3. – S. 50–58.