УДК 34:004]–053.2(4/9)

І.Г. Лубенець,
кандидат юридичних наук, провідний науковий співробітник
ДНДІ МВС України, м. Київ, Україна,
ORCID ID 0000-0003-2597-0356,
І.П. Багаденко,
кандидат юридичних наук, старший науковий співробітник,
провідний науковий співробітник ДНДІ МВС України,
м. Київ, Україна,
ORCID ID 0000-0002-3350-4411

ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДИТИНИ: АНАЛІЗ ЗАРУБІЖНОГО ДОСВІДУ[1]

У статті досліджені питання правового забезпечення інформаційної безпеки дитини. Проаналізовано практики захисту неповнолітніх від шкідливого та загрозливого Інтернет-контенту, поширені в багатьох країнах світу, але різні за механізмом здійснення. Пропонуються матеріали, що складають правову основу захисту дітей від небезпечного Інтернет-контенту та розкривають способи його фільтрації у Франції, США, Китаї, Канаді та Великобританії. Дослідження проведене з метою запозичення позитивного досвіду та можливості втілення його в Україні.

Ключові слова: *неповнолітні, діти, шкідливий Інтернет-контент, дитяча порнографія, кібербулінг, "гаряча лінія", правова основа, блокування, механізм фільтрації.*

В статье исследованы вопросы правового обеспечения информационной безопасности детей. Проанализированы практики защиты несовершеннолетних от вредоносного Интернет-контента, распространенные во многих странах, но разные по механизму осуществления. Предлагаются материалы, составляющие правовую основу защиты детей от небезопасного Интернет-контента и раскрывающие способы его фильтрации во Франции, США, Китае, Канаде и Великобритании. Исследование проводилось с целью заимствования положительного опыта и возможности внедрения его в Украине.

Ключевые слова: *несовершеннолетние, дети, вредоносный Интернет-контент, детская порнография, кибербуллинг, "горячая линия", правовая основа, блокирование, механизм фильтрации.*

Різноманітні засоби комунікації, мережа Інтернет є невід'ємною частиною сучасного суспільства в цілому та дітей зокрема. З одного боку, це засіб підвищення ерудиції та навичок спілкування, а з другого, – ситуація підвищеного ризику зіткнення з деякими загрозами віртуального світу: кібернасильством, шахрайством, порнографією, використанням особистої інформації в злочинних цілях тощо.

Різні аспекти проблеми впливу Інтернету на формування особистості дітей, їх морального розвитку вивчались зарубіжними та вітчизняними вченими такими, як: В.С. Батиргареєва, Д. Бірн, В.В. Голіна, Б.М. Головкін, І.М. Даньшин, А.І. Дол-

[1] Продовження в наступному номері.

гова, С.Н. Еніклопов, І.С. Кон, В.В. Костицький, О.Р. Михайленко, М.М. Назаров, Л.А. Найдьонова, В.В. Пушкарь, Д. Річардсон, Г.У. Солдатова, А.П. Тузов, І.К. Туркевич, С.А. Фіалкіна, В.І. Шакун та інші.

Враховуючи велику кількість різноманітних інформаційних ресурсів, було вирішено на цьому етапі дослідження відібрати для вивчення вибіркову групу країн з різним рівнем соціально-економічного розвитку, різними політико-правовими системами тощо.

Так, у Франції регулюючими органами є Міністерство національної освіти та молоді [1], а також Вища аудіальна рада (CSA) [2] (обидва органи державні).

Правова основа та механізм фільтрації шкідливого контенту. У Франції передбачено блокування контенту в межах національної зони за загальноєвропейською "гарячою лінією" INHOPE (станом на червень 2018 р. "гаряча лінія" нараховує 45 членів у 40 країнах [3]); фільтрація трафіку всередині країни і зарубіжного трафіку (за законодавством знаходиться під юрисдикцією правоохоронних і судових органів країни) за "чорним списком".

Міністерством національної освіти здійснюється впровадження систем автоматичного контролю – централізованих фільтрів, які обмежують доступ школярів до сайтів расистської, антисемітської і неофашистської спрямованості.

Фільтрація здійснюється на підставі двох "чорних списків" Інтернет-ресурсів. Перший включає порнографічні ресурси і містить близько 400000 сумнівних сайтів і 150–200 спірних сайтів, які додаються в список і розглядаються щодня; другий список включає расистські й антисемітські ресурси. Він складений відповідно до загальноєвропейського проекту з розвитку безпечного Інтернету (Safer Internet Action Plan [4]).

У Франції діє ефективна система суспільно-державного партнерства для припинення дитячої порнографії. Крім Інтернет-сайтів громадських організацій, які розповідають про Інтернет-загрози, методи їх нейтралізації і містять "гарячі лінії" для прийому повідомлень про небезпечний контент, кібер-приниження, домаганнях і загрози (e-enfance.org, internetsanscrainte.fr, netecoute.fr, point-decontact.net), "гаряча лінія" є також у МВС Франції. За допомогою цієї лінії можна, натиснувши кнопку "СИГНАЛ", передати повідомлення про шкідливий контент чи поведінку, з якою зіштовхнулась особа при використанні Інтернету [5]. На сайті МВС можна знайти сторінки інформації, поради фахівців щодо ефективного захисту будь-якої особи, зокрема дитини, при використанні Інтернету.

У 1998 р. Французькою асоціацією Інтернет-провайдерів AFA (сьогодні – AFPI) створений портал, який не тільки інформує про Інтернет-загрози і способи їх нейтралізації, а й надає можливість залишити повідомлення про виявлені ресурсі, що містять, в тому числі, дитячу порнографію. Доступ до таких ресурсів блокується членами AFPI, які отримують оброблену і перевірену інформацію від співробітників порталу.

15 лютого 2011 р. Конституційною Радою Франції прийнято Закон LOPSI-2 "Закон, спрямований на забезпечення внутрішньої безпеки країни" [6]. У ньому передбачено такі заходи регулювання та контролю мережі Інтернет:

– здійснення обов'язкової фільтрації мережі Інтернет для припинення поширення дитячої порнографії, на підставі складених МВС Франції спільно з громадськими організаціями "чорних списків", а також негайного блокування ресурсів, що містять дитячу порнографію, за поданням МВС Франції (без необхідності подання судового рішення);

– введення кримінальної відповідальності за використання підробленої IP-адреси при доступі в Інтернет (санкція: позбавлення волі на строк до 1 року і грошовий штраф у розмірі до 15 тисяч євро);

– введення кримінальної відповідальності за використання Інтернету для вчинення дій від імені третіх осіб, якщо це спричинило порушення їх (третіх осіб) спокою або зазіхання на їх честь і гідність (санкція: позбавлення волі на строк до 1 року і грошовий штраф в розмірі до 15 тисяч євро). Зокрема, у Кримінальному Кодексі Франції (ст. 222-33-2-2 "Кібербулінг (кіберзалякування, кіберпереслідування)) зазначено: "Неодноразове переслідування людини словесно чи поведінкою, метою або наслідком яких є погіршення її життєвих умов, що призводять до порушення її фізичного або психічного здоров'я, – карається однорічним ув'язненням та штрафом у розмірі до 15 тисяч євро, коли ці факти призвели до повної непрацездатності упродовж восьми днів або не призвели до непрацездатності" [7];

– заборона на створення і поширення будь-якими засобами, в тому числі через засоби масової інформації (ЗМІ), повідомлень та інших закликів, націлених на неповнолітню аудиторію, до участі їх в іграх, що несуть загрозу їх фізичній безпеці;

– легалізація дистанційного встановлення поліцейськими підрозділами на комп'ютери осіб, підозрюваних у скоєнні злочинів, спеціальних програм, що дозволяють реєструвати і передавати в поліцію дані про дії, що здійснюються користувачами персональних комп'ютерів (тільки за рішенням суду).

Для підвищення обізнаності школярів з приводу небезпек в Інтернеті у 38 департаментах країни спільно з силами жандармерії проводяться спеціальні уроки для учнів останніх класів початкової школи (9–11 років). Їх мета – попередити молоде покоління про небезпеку мережі Інтернет. Упродовж 45 хвилин учням розповідають про те, що їх можуть примушувати до сексуальних зв'язків, зазивати в секти, підштовхувати до самогубств, показують відеоролики зі свідченнями однолітків – жертв агресії в Інтернеті. Наприкінці циклу таких уроків школярам пропонують скласти іспит на володіння правилами поведінки в мережі та видають Інтернет-посвідчення за аналогією до водійських прав [8].

У США регулюючими органами є Федеральна комісія зі зв'язку США (USA Federal Communication Commission, FCC) [9], Національна рада з кібербезпеки. Федеральна комісія із зв'язку регулює міждержавні та міжнародні зв'язки по радіо, телебаченню, Телеграму, супутнику і кабелю в усіх 50 штатах та в окрузі Колумбія на території США. Комісія є федеральним органом, контрольованим Конгресом, відповідальним за впровадження і забезпечення дотримання законів і нормативних актів Америки в галузі зв'язку.

Правова основа та механізм фільтрації шкідливого контенту. Закон "Про захист дітей в Інтернеті" (The Children's Internet Protection Act 2000 – CIPA) [10] зобов'язує школи та публічні бібліотеки, що отримують фінансування з федерального бюджету, при наданні дітям доступу до Інтернету встановлювати фільтри чи відповідне блокуюче програмне забезпечення [11].

Федеральний закон США "Про захист недоторканності приватного життя дітей" (The Children's Online Privacy Protection Rule (COPPA)) [12] регулює відносини, що тісно пов'язані зі збором у мережі фізичними чи юридичними особами персональної інформації у дітей віком молодше 13 років. Закон встановлює, що для отримання інформації від дітей необхідний дозвіл батьків чи опікунів. Оператор, який збирає таку інформацію, зобов'язаний захищати недоторканність приватного життя дітей.

Зусилля Національної ради з кібербезпеки (National Cyber Security Alliance, NCSA) [13] спрямовані на побудову державно-приватного партнерства в галузі освіти та підвищення обізнаності користувачів для забезпечення безпеки та конфіденційності інформації в Інтернеті, дотримання культури кібербезпеки та реагування на кіберзлочини. Проведені NCSA дослідження виявили та обґрунтували необхідність проведення професійного розвиваючого навчання вчителів щодо

питань, пов'язаних з онлайн-безпекою. Відзначається, що запропоновані правила та принципи саморегулювання COPPA для забезпечення захисту персональної інформації підлітка в Інтернеті потребують вжиття додаткових заходів захисту дітей від потенційно шкідливої інформації в Інтернеті, у тому числі шляхом удосконалення механізмів отримання дозволів батьків на збір інформації від дітей, "батьківського контролю", поліпшення процесів моніторингу веб-сайтів на наявність шкідливого контенту, підвищення обізнаності батьків із питань забезпечення безпеки в Інтернеті, визначення правил використання підлітками Інтернет-пристроїв, а також широкого спектра додатків та веб-сайтів.

У 2006 році п'ять головних Інтернет-компаній країни оголосили про свій намір об'єднатися з Національним центром проти викрадення, зловживання та експлуатації дітей [14], щоб розпочати кампанію по запровадженню технологій для боротьби з інтернет-злочинцями, які експлуатують дітей. Так, на сьогодні *AOL*, *Yahoo!*, *Microsoft*, *EarthLink* та *United Online* фінансують технічну коаліцію з NCMEC, при цьому розвивають і впроваджують технології, які дозволяють запобігати протиправній діяльності Інтернет-злочинців щодо експлуатації дітей. Тобто це інформаційно-координаційний центр країни та загальний центр звітності з усіх питань, пов'язаних із запобіганням та попередженням віктимізації дітей. NCMEC веде боротьбу проти викрадення, зловживання і експлуатації, оскільки кожна дитина заслуговує на безпечне дитинство.

Федеральним законом США "Акт про кібербезпеку" 2009 (Cybersecurity Act of 2010) [15] владі надані значні повноваження у сфері безпеки комп'ютерних мереж. Окрім іншого, зазначається необхідність підвищення обізнаності користувачів про ризики у сфері інформаційної безпеки. Зокрема, відповідно до ст. 301 Розділу III Закону Міністрові торгівлі доручено розробити та впровадити національну кампанію з підвищення обізнаності населення щодо кібербезпеки. Стаття також зобов'язує Міністра освіти організувати впровадження навчальних програм для школярів (відповідно до віку) щодо кібербезпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Міністерство національної освіти та молоді. URL: http://www.education.gouv.fr (дата звернення: 11.11.2018).
2. Вища аудіальна рада. URL: https://www.csa.fr/Proteger (дата звернення: 11.11.2018).
3. INHOPE. URL: http://www.inhope.org/gns/who-we-are/at-a-glance.aspx (дата звернення: 11.11.2018).
4. Alliance to better protect minors online. URL: https://ec.europa.eu/digital-single-market/en/alliance-better-protect-minors-online (дата звернення: 12.11.2018).
5. MINISTERE DE L'INTERIEUR. URL: https://www.internet-signalement.gouv.fr/PortailWeb/planets/Accueil!input.action (дата звернення: 05.11.2018).
6. Loi d'orientation et de programmation pour la performance de la sйcuritй intйrieure.URL: https://www.senat.fr/dossier-legislatif/pjl09-292.html (дата звернення: 11.11.2018).
7. Про що йдеться у законі про cyberbullying. URL: https://www.e-enfance.org/que-dit-la-loi-le-cyberharcelement (дата звернення: 12.11.2018).
8. *Polevaya O., Boyer F.* L'ecole francaise face a ses problemes. URL: http://rusoch.fr/fr/politique/problemy-francuzskoj-shkoly.html (дата звернення: 05.11.2018).
9. Федеральна комісія зі зв'язку США. URL: https://www.fcc.gov/ (дата звернення: 05.11.2018).
10. The Children's Internet Protection Act 2000 (CIPA). URL: https://www.fcc.gov/consumers/guides/childrens-internet-protection-act (дата звернення: 12.11.2018).
11. *Кузьміч А.* Законодавче регулювання та способи фільтрації шкідливого інтернет-контенту: міжнародний досвід. URL: http://telpu.com.ua/archives/1872 (дата звернення: 19.11.2018).
12. The Children's Online Privacy Protection Rule (COPPA). URL: https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule (дата звернення: 12.11.2018).
13. Національна рада з кібербезпеки (NCSA). URL: https://www.isao.org/resource-library/training/national-cyber-security-alliance-ncsa-online-safety-tips/ (дата звернення: 12.11.2018).
14. Національний інформаційно-координаційний центр. URL: http://www.missingkids.org/home (дата звернення: 05.11.2018).

15. Cybersecurity Act of 2010. URL: https://www.congress.gov/bill/111th-congress/senate-bill/773 (дата звернення: 05.11.2018).

REFERENCES

1. Ministry of National Education and Youth. URL: http://www.education.gouv.fr (Date of Application: 11.11.2018) [in Ukrainian].
2. Higher Auditory Council. URL: https://www.csa.fr/Proteger (Date of Application: 11.11.2018) [in Ukrainian].
3. INHOPE. URL: http://www.inhope.org/gns/who-we-are/at-a-glance.aspx (Date of Application: 11.11.2018) [in English].
4. Alliance to better protect minors online. URL: https://ec.europa.eu/digital-single-market/en/alliance-better-protect-minors-online (Date of Application: 12.11.2018) [in English].
5. MINISTERE DE L'INTERIEUR. URL: https://www.internet-signalement.gouv.fr/PortailWeb/planets/Accueil!input.action (Date of Application: 05.11.2018) [in French].
6. Loi d'orientation et de programmation pour la performance de la sйcuritй intйrieure.URL: https://www.senat.fr/dossier-legislatif/pjl09-292.html (Date of Application: 11.11.2018) [in French].
7. Pro shcho ydetsya u zakoni pro kiberbulling? "What is the Bill on Cyberbullying about?" URL: https://www.e-enfance.org/que-dit-la-loi-le-cyberharcelement (Date of Application: 12.11.2018) [in Ukrainian].
8. *Polevaya, O., Boyer, F.* L'ecole francaise face a ses problemes. URL: http://rusoch.fr/fr/politique/problemy-francuzskoj-shkoly.html (Date of Application: 05.11.2018) [in French].
9. USA Federal Communications Commission. URL: https://www.fcc.gov/ (Date of Application: 05.11.2018) [in Ukrainian].
10. The Children's Internet Protection Act 2000 (CIPA). URL: https://www.fcc.gov/consumers/guides/childrens-internet-protection-act (Date of Application: 12.11.2018) [in English].
11. *Kuzmich, A.* Zakonodavche rehulyuvannya ta sposoby filtratsiyi shkidlyvoho internet-kontentu: mizhnarodnyy dosvid. "Legislative Regulation and Methods of Filtering Harmful Internet Content: International Experience". URL: http://telpu.com.ua/archives/1872 (Date of Application: 19.11.2018) [in Ukrainian].
12. The Children's Online Privacy Protection Rule (COPPA). URL: https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule (Date of Application: 12.11.2018) [in English].
13. Natsionalna rada z kiberbezpeky (NCSA). "National Cybersecurity Council (NCSA)". URL: https://www.isao.org/resource-library/training/national-cyber-security-alliance-ncsa-online-safety-tips/ (Date of Application: 12.11.2018) [in Ukrainian].
14. Natsionalnyy informatsiyno-koordynatsiynyy tsentr. "National Information and Coordination Center". URL: http://www.missingkids.org/home (Date of Application: 05.11.2018) [in Ukrainian].
15. Cybersecurity Act of 2010. URL: https://www.congress.gov/bill/111th-congress/senate-bill/773 (Date of Application: 05.11.2018) [in English].

UDC 34:004]–053.2(4/9)

I.H. Lubenets,
Candidate of Juridical Sciences, Leading Researcher, State Research Institute MIA Ukraine, Kyiv, Ukraine,
ORCID ID 0000-0003-2597-0356,
I.P. Bahadenko,
Candidate of Juridical Sciences, Senior Research Associate, Leading Researcher, State Research Institute MIA Ukraine, Kyiv, Ukraine,
ORCID ID 0000-0002-3350-4411

LEGAL PROVISION OF INFORMATION SECURITY OF THE CHILD: ANALYSIS OF FOREIGN EXPERIENCE

The number of Internet users is growing daily. The most active part of Internet users are young people and children. Particular concern is the increased negative impact on children of malicious Internet content and mass media, as well as hidden threats of Internet. In particular, information about aggressive, asocial, and unsafe

content can be placed in an unprotected information space, which adversely affects the health and especially the psyche of the child.

Consequently, the problem of information security of the child today is highly relevant and determines the need to address issues related to streamlining the information space of the country, in particular, by introducing an effective model of legal regulation in this area. Therefore, in many developed countries, norms and prohibitions have been established regarding the dissemination of information that may adversely affect the process of forming the moral development of minors, cause aggression, social maladjustment, etc.

Today, the global Internet community needs to solve three interrelated problems: insurance of freedom of speech, restriction of malicious content and protection of personal data. That is, the task of each state is to respect human rights on the Internet and ensure the protection of a person (child) from malicious content without violating the right to freedom of speech.

Due to the fact that this problem is relevant for most countries of the world, each of them has its own experience in addressing the issue of ensuring the protection of children in the information space. Therefore, the paper is devoted to the analysis of the practice of protecting minors from malicious Internet content, which is common in many countries, but differs in the mechanism of implementation. It offers materials that constitute the legal basis for the protection of children from unsafe Internet content and search of ways to filter it, in France, the USA, China, Canada and the UK.

The study and synthesis of the legal basis and the filtering mechanism for malicious Internet content in foreign countries are carried out with the aim of borrowing positive experience and the possibility of an implementation in Ukraine.

Keywords: minors, children, malicious Internet content, child pornography, cyberbulling, “hot line”, legal basis, blocking, filtering mechanism.

Отримано 28.11.2018