



**RS Global**  
Journals

**Scholarly Publisher**  
**RS Global Sp. z O.O.**  
ISNI: 0000 0004 8495 2390

Dolna 17, Warsaw, Poland 00-773  
Tel: +48 226 0 227 03  
Email: editorial\_office@rsglobal.pl

---

<b>JOURNAL</b>	International Academy Journal Web of Scholar
<b>p-ISSN</b>	2518-167X
<b>e-ISSN</b>	2518-1688
<b>PUBLISHER</b>	RS Global Sp. z O.O., Poland
<b>ARTICLE TITLE</b>	Information Security Risks of Child's Safety in the Turbulent Information Environment from the Position of the State Management
<b>AUTHOR(S)</b>	Panchenko Oleg
<b>ARTICLE INFO</b>	Panchenko Oleg. (2020) Information Security Risks of Child's Safety in the Turbulent Information Environment from the Position of the State Management. International Academy Journal Web of Scholar. 7(49). doi: 10.31435/rsglobal_wos/30092020/7147
<b>DOI</b>	<a href="https://doi.org/10.31435/rsglobal_wos/30092020/7147">https://doi.org/10.31435/rsglobal_wos/30092020/7147</a>
<b>RECEIVED</b>	30 July 2020
<b>ACCEPTED</b>	17 August 2020
<b>PUBLISHED</b>	01 September 2020
<b>LICENSE</b>	 This work is licensed under a <b>Creative Commons Attribution 4.0 International License</b> .

---

© The author(s) 2020. This publication is an open access article.

# ІНФОРМАЦІЙНІ РИЗИКИ БЕЗПЕКИ ДИТИНИ У ТУРБУЛЕНТНОМУ ІНФОРМАЦІЙНОМУ СЕРЕДОВИЩІ З ПОЗИЦІЇ ДЕРЖАВНОГО УПРАВЛІННЯ

**Панченко Олег Анатолійович**

*Доктор медичних наук, професор, Заслужений лікар України, директор ДЗ «Науково-практичний медичний реабілітаційно-діагностичний центр МОЗ України»,  
Президент Громадської організації «Всеукраїнська професійна психіатрична ліга», Україна  
ORCID ID: <https://orcid.org/0000-0001-9673-6685>*

**DOI: [https://doi.org/10.31435/rsglobal\\_wos/30092020/7147](https://doi.org/10.31435/rsglobal_wos/30092020/7147)**

---

## ARTICLE INFO

**Received:** 30 July 2020

**Accepted:** 17 August 2020

**Published:** 01 September 2020

---

## KEYWORDS

information risks,  
information security,  
information environment,  
social network,  
spam,  
viruses,  
phishing,  
trolls,  
haters,  
cyber bullying.

## ABSTRACT

The transition to an informational lifestyle significantly increases the creative potential of society as a whole, and the individual in particular. Along with this, there is a significant increase of the load on the human's mind under conditions of increasing flows of information and its turbulence. The information environment essentially becomes the main source of information for a person, has a direct impact on his mental activity, on the formation of his social behavior. A person is forced to live in this environment, to perceive its realities adequately, to adapt to information threats from this environment. The awareness of these threats has led to careful attention to information security. A child, being a specific member of a society, nevertheless acts as a full-fledged participant in information relations, and must be in such a state of protection, in which there is no risk associated with information causing harm to his health, physical, mental, spiritual and moral development.

A child in his development, processing information, actively assimilates social experience, as well as a system of social connections and relationships, and subsequently reproduces all this in his life. In the course of this process, he acquires the qualities, values, beliefs and forms of behavior that he needs for normal life.

Ensuring the information security of a child implies protection because of the destabilizing effect of information on health and mental, spiritual and moral development; creation of conditions for the information environment for positive socialization and individualization of the personality, optimal social, personal, cognitive and physical development, preservation of somatic, mental and psychological health and well-being, the formation of a positive worldview. The latter is possible when determining the main directions of state policy in the interests of children and the key mechanisms for its implementation, based on the generally recognized principles and norms of the international law.

---

**Citation:** Panchenko Oleg. (2020) Information Security Risks of Child's Safety in the Turbulent Information Environment from the Position of the State Management. *International Academy Journal Web of Scholar. 7(49)*. doi: [10.31435/rsglobal\\_wos/30092020/7147](https://doi.org/10.31435/rsglobal_wos/30092020/7147)

---

**Copyright:** © 2020 **Panchenko Oleg**. This is an open-access article distributed under the terms of the **Creative Commons Attribution License (CC BY)**. The use, distribution or reproduction in other forums is permitted, provided the original author(s) or licensor are credited and that the original publication in this journal is cited, in accordance with accepted academic practice. No use, distribution or reproduction is permitted which does not comply with these terms.

---

**Вступ.** Вплив, який чинять інформаційні процеси на всі сфери життєдіяльності суспільства, актуалізує найважливіші питання соціального буття, в тому числі питання інформаційних взаємодій і протидія різного роду інформаційним ризикам. Істотне зростання ролі інформаційного середовища веде до того, що цілеспрямовані або ненавмисні дії на

---

інформаційне середовище зовнішніх або внутрішніх факторів можуть завдавати серйозної шкоди цим інтересам і є загрозою для безпеки людини і суспільства. Усвідомлення цих ризиків спричинило пильну увагу до інформаційної безпеки.

Ставлення до інформації в сучасному суспільстві зазнає істотне переосмислення. Людина змушена перебувати в інформаційному середовищі, частина якої містить інформацію, що ускладнює або перешкоджає адекватності сприйняття і розуміння людиною навколишнього світу і самого себе. Інша ж частина містить цілеспрямовані джерела інформаційно-психологічного впливу, які вводять людину в оману, діють врозрив його інтересам і завдаючи йому шкоди.

Дитина, з її несформованою психікою, вимагає більш пильної уваги з точки зору інформаційних ризиків. Важливість цієї проблематики вимагає адекватного реагування суспільства в цілому, вчених на вироблення превентивних заходів по нейтралізації негативного інформаційного впливу.

**Результати досліджень.** Людство займається отриманням, накопиченням, обробкою і створенням нової інформації на всьому протязі його еволюції, причому обсяг інформації в сучасному суспільстві стрімко збільшується. Згідно цивілізаційної типології Тофлера ми живемо в епоху інформаційної революції [1], яка реалізується у вигляді процесу інформатизації практично всіх сфер життя суспільства і життєдіяльності людини.

Людство впритул підходить до межі, за якою інформаційне середовище стає по суті основним джерелом інформації для людини, безпосередньо впливає на його психічну діяльність, на формування його соціальної поведінки.

Інформаційне середовище, стаючи все більш важливою і невід'ємною частиною навколишнього середовища, пред'являє до людини зростаючі адаптивні вимоги. Людина змушена жити в цьому середовищі, адекватно сприймати її реалії пристосовуватися до інформаційних ризиків з боку цього середовища. Найбільш небезпечним джерелом загроз є істотне розширення можливості маніпулювання свідомістю людини за рахунок формування навколо нього індивідуального "віртуального інформаційного простору", а також можливості використання технологій впливу на його психічну діяльність [2].

*Ризик* – це можливі події, явища і процеси, наслідки яких можуть мати несприятливий вплив на різні аспекти стану людського життя. (в тому числі і на інформаційну безпеку). Подібне трактування має і поняття «загроза». Різниця полягає в тому, що загроза – це ймовірна можливість завдання шкоди, а ризик вимірює, оцінює цю загрозу, дає уявлення щодо конкретного виразу ймовірності завдання шкоди. В той же час загроза – це пасивне явище, яке потенційно може перетворитись на активне (дію) – вплив. Небезпека – це конкретна форма прояву загрози, створена впливом, деструктивний характер якої є цілком усвідомленим та беззаперечним.

Можна стверджувати, що ступінь загрози та її перехід у форму небезпеки характеризується рівнем ризику, який, в свою чергу, визначається ймовірністю настання та впливом на особистість. Тобто за прийняттого рівня ризику негативний вплив факторів зовнішнього та внутрішнього середовища розглядається як загроза особистості, а за досягнення критичного рівня ризику загроза приймає форму небезпеки.

Викладені сентенції дозволяють трактувати інформаційні ризики безпеки дитини у турбулентному інформаційному середовищі як сукупність умов, факторів та явищ, під дією яких можливе порушення стану інформаційної безпеки дитини, її психологічного стану, або створення небезпеки її життєво важливим інтересам.

В.М. Фурашев зазначає, що інформаційна загроза – це з одного боку такий внутрішній чи зовнішній інформаційний вплив, що створює небезпеку зміни напрямку, темпів прогресивного розвитку індивідуумів чи суспільних утворень, а з іншого боку – це небезпека для останніх стати жертвою негативного інформаційного впливу [3].

Під негативним впливом стосовно дитини слід розуміти «таку дію інформації, або дію за допомогою інформації з використанням спеціальних засобів і технологій, яка завдає шкоди фізичному чи психічному здоров'ю дитини, або спонукає її до девіантної поведінки» [4]. Поряд із поняттям «інформаційний вплив» використовується і «інформаційно-психологічний вплив», оскільки він пов'язаний із втручанням у внутрішній психологічний та психічний стан дитини через її свідомість та підсвідомість, із використанням інформаційних технологій, що призводить до негативних і деструктивних наслідків для дитячої психіки.

Дитяча психіка дуже вразлива по відношенню до інформаційних впливів внаслідок несформованості найважливіших психічних функцій і структур, що забезпечують адекватну переробку інформації і психологічний захист особистості. Виходячи з соціальних контекстів розвитку, внутрішньої позиції дитини і її ставлення до світу, інформаційна безпека дитини повинна враховувати два аспекти: захист від негативного впливу інформаційного середовища і розвиток умов, що забезпечують позитивну соціалізацію та індивідуалізацію дитини. Тобто, *інформаційна безпека дитини* – це захищеність дитини від дестабілізуючого впливу інформації на здоров'я і психічний, духовний, моральний розвиток; створення умов інформаційного середовища для позитивної соціалізації та індивідуалізації особистості, оптимального соціального, особистісного, пізнавального і фізичного розвитку, збереження соматичного, психічного та психологічного здоров'я і благополуччя, формування позитивного світосприйняття [5].

Радзівєвська О.Г. розділяє ризики та загрози для дитини на індивідуальні та суспільні [6]. *Індивідуальні* – це такі ризики і загрози, що викликані негативними інформаційними впливами, направленними на індивідуальну свідомість та підсвідомість дитини, які можуть призводити до деструктивних наслідків, негативно впливати на формування особистості, її фізичне, психічне чи моральне здоров'я, та викликати девіантну поведінку. *Суспільні* – це такі ризики і загрози, що викликані негативними інформаційними впливами, спрямованими на суспільну свідомість, які можуть призвести до дисбалансу у суспільних відносинах, порушувати суспільні норми та викликати девіантну поведінку дитини у соціумі через дію деструктивного інформаційного впливу на її індивідуальну свідомість, що призводить до формування хибних світоглядних позицій, видозмінених моральних, етичних та загальнолюдських цінностей й порушення її комунікативних навичок.

Виявлення загроз в ІС має свої складнощі через ряд причин, серед яких:

- заподіяння шкоди відбувається у ментальному просторі;
- практично неможливо визначити ступінь заподіяння шкоди;
- ступінь заподіяння шкоди залежить від індивідуальних психофізичних особливостей людини та її емоційно-психологічного стану;
- настання наслідків заподіяння шкоди відтерміновано в часі;
- визначення деяких загроз можливе лише постфактум, після виявлення наслідків діяння;
- не існує єдиного інструментарію виявлення загроз, лише опосередковані методи комплексного аналізу психофізичного, суспільно-політичного та інформаційно-технічного чинників.

Розглядаючи властивості ІС, ми акцентували увагу на тому, що великі обсяги інформації, що циркулюють в ІС, змінюють як саму людину, так і сутність суспільних відносин. Щодо дитини, то вона не спроможна зосередити увагу на конкретній тематиці, відбуваються психофізичне виснаження, втомленість та зміни емоційного стану (збудження чи заторможення). Відсутність належного рівня концентрації уваги разом з мозаїчністю (кліповістю) подачі інформації сучасними засобами передачі інформації (телебачення, Інтернет), призводить до поверхневого її сприйняття, і це може призвести до зниження інтелектуального рівня дитини, її вміння аналізувати, зіставляти, оцінювати, узагальнювати та використовувати інформацію. В протидії негативним інформаційним впливам такі вміння можуть бути недостатніми, особливо у випадку цілеспрямованих маніпулятивних дій на свідомість дитини.

ІС не завжди пропонує істинні цінності, а підмінює їх системою символів та ілюзорних норм. Прикладом такої підміни понять є реклама, особливо – політична, де істина підмінюється красивим образом, створюється ілюзія позитиву і приховується інша його сторона. Через відсутність аналітичних фільтрів, дитина такі образи сприймає як істинні та вбудовує їх у власну систему поглядів та цінностей. В подальшому ці образи слугуватимуть їй як еталонні. Це призведе до видозміни свідомості дитини, викривлення її світосприйняття та основних цінностей. Дитина з видозміненою свідомістю, вступаючи у суспільні відносини, змінюватиме і саме суспільство.

Другим фактором, що несе суттєву загрозу для формування особистості у дитини, є медіанасилля, яке впливає на свідомість та підсвідомість дитини. Беззаперечним є й той факт, що збільшення агресії на екрані провокує підвищення агресивної поведінки дитини в

реальному житті, а відтак – збільшення агресії у суспільстві [7]. Слід також звернути увагу і на агресивні комп'ютерні ігри, що становлять загрозу не лише психологічному, але й фізичному здоров'ю дитини та викликають залежність. Діти, які часто грають в агресивні комп'ютерні ігри, не до кінця усвідомлюють нереальність подій у грі і, перебуваючи у стресовій ситуації під дією психологічного навантаження, можуть переносити здобуті тут навички у реальне життя. Зважаючи на захоплення в іграх вбивства призами і подарунками, у дитини створюється хибне враження: що насилля – це добре. Це значно спотворює у неї уявлення про основні моральні цінності [8]. Також приймаючи до уваги воєнну ситуацію на сході України, великий ріст інформаційних атак і фейків, що розповсюджуються засобами масової інформації по всій країні, необхідно визнати велику проблему в збереженні психологічного, психічного та соматичного здоров'я дітей та підлітків [9].

Найбільш небезпечним, на наш погляд, є негативний вплив соціальних мереж. У визначенні інформаційної безпеки дитини було виділено однією із складових – створення умов інформаційного середовища для позитивної соціалізації та індивідуалізації особистості.

Соціалізація відбувається упродовж усього життя людини, при цьому традиційні форми соціалізації включають два види – первинну і вторинну. Первинна соціалізація відбувається з дитинства у межах родинних зв'язків, вторинна – у межах соціальних інститутів і соціальних контактів поза межами безпосереднього життєвого середовища людини [10]. І саме соціальні мережі все більше впливають на вторинну соціалізацію людини. Під впливом мережевого суспільства змінюється стиль життя людей, зокрема звичні канали отримання інформації, характер міжособистісних взаємин, структура дозвілля, відбувається інтенсивне вироблення нових моделей взаємодії з середовищем. Безумовно, все це впливає на безперервний процес соціалізації молоді людини. Більш того, Інтернет є не тільки потужним агентом вторинної соціалізації, але й виграє конкуренцію в інститутів, які реалізують первинну соціалізацію. Цьому сприяє динаміка сучасного життя, криза традиційних інститутів і цінностей.

Як відомо, будь-яка діяльність спрямована на задоволення потреб. Спеціально проведені дослідження дозволили визначити певне коло потреб, які підлітки задовольняють за допомогою соціальних мереж та Інтернету, а саме:

- потреба у самостійності (у процесі соціалізації ця потреба припускає, в першу чергу, прагнення до незалежності від батьків);
- потреба у самореалізації та визнанні (зазвичай підліткам вкрай необхідно відчувати себе особливими та необхідними);
- потреба у пізнанні та визнанні (молоді люди хочуть відчувати себе важливою частинкою певної групи і суспільства загалом);
- задоволення соціальної потреби у спілкуванні, у приналежності до групи за інтересами, в любові, адже підлітковий період – це час, коли людина прагне знайти схожих собі за інтересами, вподобаннями;
- потреба у володінні (підліток має на меті бути обізнаним з усіма подіями, що відбуваються навколо нього);
- пізнавальна потреба (володіння новими знаннями сприяє досягненню визнання з боку однолітків і самореалізації);
- у результаті використання соціальних мереж виникає відчуття повного контролю і володіння ситуацією, що задовольняє потребу в безпеці – одну з базових у системі потреб людини [11].

Завдяки соціальним мережам підлітки проявляють свою індивідуальність, тільки вже не стандартними способами, закладеними процесом перетворення від індивіда до сталої особистості, а завдяки комп'ютерним технологіям.

Дані статистики за 2018 рік показують ([12-14]):

- 95% дітей у віці від 13 до 18 років мають постійний доступ до смартфонів, і 45% з них говорять, що знаходяться он-лайн «практично завжди»;
- 22% підлітків заходять в улюблені соцмережі не менше 10 разів на день;
- 88% підлітків спостерігали в соцмережах, як хтось був злим або жорстоким по відношенню до іншої людини;
- 41% підлітків вже мав негативний досвід в соцмережах;

- 22% підлітків втратили друзів із-за своїх дій в соцмережах, 25% - зіткнулися в реальному житті з проблемами через те, що написали в своїх постах, у 6% це викликало труднощі в школі;
- 29% дітей спілкувалися в соціальних мережах з незнайомими людьми;
- 29% сексуальних злочинів мають передісторію в соціальних мережах;
- 66% дорослих користувачів Facebook не мають поняття, як користуватися налаштуваннями конфіденційності;
- 55% батьків, які мають дітей 12 років і молодше, відповіли, що їхні діти вже зареєстровані в Facebook. Більш того 76% відсотків з них самі допомогли в цьому дітям;
- тільки 10% дорослих розмовляли "по душам" зі своїми дітьми 10 років і молодше про безпечну поведінку в соціальних мережах;
- 67% підлітків знають, як приховати від батьків те, чим вони займаються в соцмережах.

Безперечно, використання соцмереж як джерела нової інформації, інструмента самовираження, спілкування має певні плюси. Але, якщо дорослі, можуть фільтрувати інформацію, то з дітьми зовсім інша історія. Їх психіка не «загартована». Посидівши в соцмережах, діти можуть відчувати себе емоційно вигорілими, відчувати депресію. Крім того, спілкуючись здебільшого через месенджери, а не лицем до лица, діти не можуть навчитися розпізнавати емоції співрозмовника і зчитувати мову тіла, вираз обличчя і інтонацію, тобто вони втрачають невербальну частину інформації.

Формування більш слабких соціальних навичок спілкування не єдина небезпека, з якою може зіткнутися дитина в соціальних мережах.

*Спам, віруси, фішинг.* Небажані послання рекламного характеру з підозрілими посиланнями можуть з'являтися як в коментарях, так і в особистих повідомленнях. Причому, в адресанта часто значаться знайомі профілі: спамери зламують чужі акаунти, щоб робити масові розсилки друзям їх власників. Часто спамери створюють фейкові акаунти, що дублюють уже існуючі, щоб подружитися, втертися в довіру, а потім виконати свою місію – закидати непотрібною інформацією, заманити на свій сайт або спонукати скачати документ. Поширені види спаму:

- реклама будь-яких товарів або послуг;
- повідомлення про виграш в лотерею або отримання спадщини;
- лист щастя / нещастя;
- прохання підтвердити дані;
- привабливі пропозиції грошового заробітку;
- прохання позичити грошей або допомогти фінансово.

*Тролі.* Так називають тих, хто залишає коментарі з певною метою – спровокувати конфлікт або яскраву емоційну реакцію (викликати злість або гнів). Тому тональність їхніх висловлювань завжди недобррозичлива, це цілком може бути безглуздий жарт про маму, критика творчості дитини або його зовнішності, перебріхування фактів і пр. Зазвичай, коментарі тролів жодним чином не пов'язані з контентом, під яким їх написали. Тролі рідко постять і залишають коментарі від свого особистого імені. Привілей тролів – анонімність, а значить, однією з причин тролінгу може бути бажання висловити те, що дитина не змогла б висловити знайомому безпосередньо. Можливо, він давно її ображає в реальному житті – у дворі або школі. Інша причина тролінгу може полягати в тому, що діти 12-17 років тільки-тільки починають приміряти на себе соціальні ролі, і нехай не завжди їх вибір можна назвати раціональним, тролінг в мережі здається їм нешкідливим (на рівні «приколу» або «Пранк»).

*Хейтери.* Хейтерами називають в соцмережах тих, хто всіляко намагається нівелювати заслуги успішних людей. Чужі невдачі радують хейтера більше, ніж власний успіх. Принижуючи інших, вони самостверджуються. Серед причин, чому користувачі стають хейтерами, часто називають такі:

- їх засмучує, що у іншої дитини є те, чого немає у них;
- вони вважають, що дитина не гідна популярності і слави, яку має;
- в минулому у них з цією дитиною був конфлікт або, навпаки, дружні відносини, які погано закінчилися;

- вони заздять;
- їм не вистачає уваги і любові.

*Кібербулінг.* В основному кібербулінг характерний для дітей 12-17 років, саме вони найчастіше використовують Інтернет для залякування, переслідування, погроз або приниження своїх однолітків. Ознаки кібербулінгу:

- в особистих повідомленнях у соцмережах безліч загроз від одного або кількох людей за короткий проміжок часу;
- дитині приходять повідомлення від соцмереж, що на неї поскаржилися за неприйнятну поведінку (скаржитися відразу кілька людей, щоб зробити дитину ізгоєм навіть в соцмережах);
- її відзначають в постах, де опубліковані принизливі фотожаби, відео, образливі жарти, жорстокі хештеги;
- у акаунта дитини з'явився клон, який агресивно поводить по відношенню до інших користувачів і таким чином псує репутацію дитини;
- в соцмережах поширюється контент, який висміює дитину, його зовнішній вигляд або поведінку.

*Групи смерті.* Це такі он-лайн квести в соціальних мережах, з якими пов'язують кілька смертей підлітків 15-16 років в Україні та Росії (синій кит, Момо і т. д.). Дітям пропонують виконувати різні завдання – від цілком «невинних» типу підйому о 4.20 ранку або перегляду фільмів-жахів і до таких екстремальних, як нанесення собі каліцтв і самогубство.

Підсумовуючи, варто підкреслити ще одну особливість. Діти дуже безпечні щодо інформації про членів родини, дозвілля, оприлюднення персональних даних, спілкування з незнайомцями. Це створює сприятливі умови для використання соціальних мереж із злочинною метою. Крім цього, акаунт будь-якого користувача також може містити різні статистичні дані перебування користувача в мережі: дату, час, тривалість, адреси, використані при підключенні комп'ютера та ін. Тобто, кожен акаунт – це сховище персональних даних і повний архів листування. Більшість користувачів навіть не здогадуються про те, наскільки широкому колу осіб конфіденційна інформація може стати відомою, не усвідомлюють реальну й потенційну небезпеку можливого протиправного використання відповідним чином аналітично обробленої їх персональної інформації щодо фактично всіх сфер їхнього особистого життя.

Окреслені масштаби і гострота існуючих проблем в сфері інформаційної безпеки, що виникають в умовах турбулентного сьогодення формують нові виклики. А отже, інтереси майбутнього країни та її безпеки настійно вимагають від органів державної влади України, регіонального керування, органів місцевого самоврядування, громадянського суспільства організація невідкладних заходів для поліпшення становища дітей та їх захисту. Останнє можливе при визначенні основних напрямків державної політики в інтересах дітей і ключових механізмів її реалізації, що базуються на загальноновизначених принципах і нормах міжнародного права [9].

Інструментом практичного вирішення багатьох питань у сфері інформаційної безпеки дитинства буде доцільна реалізація пріоритетних національних проектів "Здорова дитина" та "Якісна освіта", цільових програм. Прийняття низькі найважливіших законодавчих актів, спрямованих на попередження найбільш серйозних загроз здійснення прав дітей, а саме розробка Закону «Про інформаційну безпеку дітей», у якому буде чітко визначення наступних понять «інформаційна безпека», «інформаційна грамотність», «інформаційний імунітет», «медіаграмотність». Даний Закон визначить правові основи радикального перетворення інформаційного простору українського суспільства з урахуванням потреби формування соціального середовища, сприятливого для повноцінного психічного і морально-духовного розвитку дітей.

#### **Висновки.**

1. Дитина, будучи активним учасником суспільних відносин в інформаційній сфері, є найбільш незахищеним їх суб'єктом в силу вікового онтогенезу та підвищеної інформаційної вразливості, тому вона потребує особливого захисту з боку держави.

2. Інформаційна безпека дітей є нагальною проблемою і потребує державного регулювання, тим самим формуючи єдиний підхід органів державної влади, органів місцевого самоврядування, інститутів громадянського суспільства та громадян до визначення цілей,

завдань, напрямків діяльності і першочергових заходів щодо вирішення найбільш актуальних проблем організації сприятливого інформаційного середовища для повноцінного розвитку дітей.

3. Невідкладними діями щодо вирішення проблем інформаційної безпеки є розробка Закону «Про інформаційну безпеку дітей», який визначив би, інформаційні загрози і шляхи протистояння ним, а також сприяв би визначенню регламентації захисту дітей від інформації, що завдає шкоди їх здоров'ю та розвитку, розробки критеріїв оцінки стану інформаційної безпеки дітей і підлітків.

#### ЛІТЕРАТУРА

1. Панченко О.А. Информационная безопасность личности: монография /Панченко О.А., Банчук Н.В. - Киев: КИТ, 2011. - 672с.
2. Емельянов Г.В., Стрельцов А.А. Проблемы обеспечения безопасности информационного общества // Распределенная конференция «Технологии информационного общества 98 – Россия». [Электронный ресурс]. - Режим доступа: <http://www.iis.ru/events/19981130/streltsov.ru.html>. (дата обращения: 14.07.2020)
3. Фурашев В. М. Державно-правові проблеми інформаційної безпеки людини і суспільства в умовах інтеграції України у світовий інформаційний простір. Запобігання новим викликам та загрозам інформаційній безпеці України: правові аспекти: матеріали наук.-практ. конф. / 06 жовт. 2016 р. / Упоряд.: В. М. Фурашев. Київ: НТУУ «КПІ імені Ігоря Сікорського». Вид-во «Політехніка». 2016. С. 7-24.
4. Радзівська О.Г. Проблеми негативних інформаційних впливів на дитину в Україні в умовах збройного протистояння. Науковий вісник Ужгородського національного університету. Серія Право. Випуск 42. 2017. С.197-200.
5. Панченко О.А. Информационная безопасность ребенка: Монография. Киев. КВИЦ. 2016. 380с.
6. Радзівська О.Г. Дитина у глобалізованому інформаційному просторі: реальні та потенційні загрози. Інформація і право. № 4(19). 2016. С. 29-38.
7. Брайант Д., Томпсон С. Основы воздействия СМИ. М.: Издательский дом «Вильямс». 2004. 424 с.
8. Медиа-насилие: детям прививают страсть к убийству. Интервью с полковником Дэвидом Гроссманом. [Электронный ресурс]. - Режим доступа: <http://www.pravoslavie.ru /jurnal/783.htm> (дата обращения: 10.07.2020).
9. Панченко О.А., Кабанцева А.В. Державне регулювання інформаційної безпеки дітей. Матеріали Міжнародної науково-практичної інтернет-конференції «Тенденції і перспективи розвитку науки і освіти в умовах глобалізації». (28 лютого 2020 г.) Переяслав - 2000. Вып. 56. С. 39-42.
10. Соціологія: підручник / за ред. В. Г. Городяненка. 3-тє вид., переробл. і доп. К.: ВЦ «Академія». 2008. 544 с.
11. Вплив соціальних мереж на формування особистості підлітків. Науковий звіт. [Електронний ресурс]. - Режим доступу: <https://vipsoft.blob.core.windows.net/contest/041cf057f5dfb5204385e35b82eed715.pdf> (дата звернення: 14.07.2020).
12. Социальные сети. Как защитить ребенка. [Электронный ресурс]. - Режим доступа: <https://shcherbakovs.com/how-to-protect-kids-in-social-media/> (дата обращения: 14.07.2020).
13. Teens, Social Media&Technology 2018. Retrieved from: <https://www.pewresearch.org/internet/2018/05/31/teens-social-media-technology-2018/> (date of access: 14.07.2020).
14. Social Media Statistics. Retrieved from: <https://www.guardchild.com/social-media-statistics-2/> (date of access: 14.07.2020).