педагогічному менеджменті / Г. М. Тимошко // Проблеми освіти : наук. зб. – Київ, 2014. – Вип. 74. – Ч. 1. – С. 73–79.

8. Тимошко Г. М. Сучасні тенденції розвитку організаційної культури керівника ЗВО на засадах іміджелогії / Г. М. Тимошко // Вісник ЧНПУ ім Т.Г. Шевченка. – Чернігів : ЧНПУ, 2014. – Вип. 122 – С. 276–279.

ФОРМУВАННЯ ІНФОРМАЦІЙНО-БЕЗПЕКОВОЇ КУЛЬТУРИ ЗДОБУВАЧІВ ОСВІТИ

Войтович І. С.[1], Войтович В. І.[2], Войтович О. П.[3]
Рівненський державний гуманітарний університет
E-mail: [1]ihor.voitovych@rshu.edu.ua, [2]vladyslav.voitovych@rshu.edu.ua, [3]oksana.p.voitovych@rshu.edu.ua

Запропоновано авторське визначення інформаційної безпеки особистості, що формується, куди включено захищеність її життєво важливих інтересів та процес набуття особистістю таких якостей, за наявності яких ніякі інформаційні впливи на неї неспроможні викликати деструктивні думки і дії. Розглянуто види загроз: для особистісної безпеки, витоку персональних даних, загрози для персональних комп'ютерів. Розроблено практичні рекомендації, адресовані батькам і педагогам, які допоможуть розв'язати виховну проблему, відповідно до вікових і психологічних особливостей дітей і підлітків.

В умовах сучасних глобальних та регіональних інформаційних протистоянь, деструктивних комунікативних впливів, зіткнення різновекторних національних інформаційних інтересів, поширення інформаційної експансії та агресії, захист національного інформаційного простору та гарантування інформаційної безпеки стають пріоритетними стратегічними завданнями сучасних держав у системі глобальних інформаційних відносин.

Збереження інформаційного суверенітету, формування ефективної системи безпеки в інформаційній сфері є актуальною проблемою для України, яка часто є об'єктом зовнішньої інформаційної експансії, маніпулятивних пропагандистських технологій та руйнівного інформаційного вторгнення. Можемо сказати, що інформаційна безпека – це стан захищеності, тобто вона є властивістю системи мінімізувати інформаційні загрози. Для окремої особистості існують одні загрози, для суспільства інші, для держави – ще інші. Поширивши цю тезу, можемо вказати, що для дітей і молоді існують інші види загроз з огляду на вікові та психологічні особливості, а для сформованої, зрілої особистості, не несе загрози, те для дитини може виявитися не-

безпечним. Несформованість психічної, вольової, емоційної сфери, недостатній рівень розвитку критичного мислення дітей і підлітків з одного боку, і часто вільний, неконтрольований доступ до джерел інформації, веде до підпадання їх під негативний інформаційний вплив, котрий може проявитися, як у деструктивних діях, так і в формуванні морально спотвореної особистості.

Настільки людина сприйнятлива до психологічних впливів, загроз інформаційного середовища, наскільки в неї розвинені особистісні якості: психологічна стійкість, сила власних переконань, сила волі, критичне мислення. Отож, можна сказати, що несформована дитяча особистість, в силу її психічних особливостей, є найбільш уразливою до таких впливів.

Під інформаційною безпекою особистості, що формується, ми будемо розуміти, з одного боку, стан захищеності її життєво важливих інтересів, а з іншого – процес набуття особистістю таких якостей (вольових, інтелектуальних, емоційних), за наявності яких ніякі інформаційні впливи на неї неспроможні викликати деструктивні думки і дії, що призводять до негативних відхилень на шляху її стійкого прогресивного розвитку. Нове розуміння інформаційної безпеки вимагає переосмислення ролі освіти в процесі виховання нового покоління, здатного адекватно вписатися в новий інформаційний світ.

Зауважимо, що оскільки людина визначається найбільшою цінністю педагогіки гуманізму, тому й інформаційно-психологічна безпека учнів представляється основною домінантою інформаційної безпеки особистості.

Розглянемо докладніше, які види загроз породжує новітній інформаційний простір для людини. Виходячи з [1–3; 7], виділимо такі види загроз:

1) Загрози для особистісної безпеки:

− ознайомлення з матеріалами небажаного змісту (порнографія, ненормативна лексика, суїцидального характеру, сектантські, расистські та ненависницькі, вибухові речовини, хакерські сайти),

− отримання недостовірної інформації,

− залежностей (комп'ютерної, ігрової, Інтернет і т.ін.),

− спілкування з небезпечними людьми (шахраями, збоченцями, гриферами і т.ін),

− вчинення протиправних дій (хакерство, порушення авторських прав і т.ін.);

2) Загрози витоку персональної інформації:

– розголошення конфіденційних даних (прізвища, імені, адреси, номерів кредитних карток, телефону тощо);

3) Загрози для персональних комп'ютерів:

– проникнення вірусів,

– завантаження шкідливого активного коду,

– завантаження програм з прихованими функціями: троянів, клавіатурних шпигунів тощо.

Проаналізувавши проблеми, пов'язані з входженням дитини у світ новітніх технологій, можемо сказати, що завданням є розробити практичні рекомендації, адресовані батькам і педагогам, які допоможуть розв'язати виховну проблему, відповідно до вікових та психологічних особливостей дітей і підлітків. Батьки та вчителі мають займати активну позицію у формуванні інформаційно-безпекової культури молоді [4; 6].

У дошкільному і молодшому шкільному віці добір відповідних до віку ігор забезпечить розвиток мислення, пам'яті, уяви, швидкості та допоможе «граючись» підготуватися до школи. Батькам корисно пам'ятати, що добір відповідного до віку програмного забезпечення може сприяти розвитку здібностей дітей (малювання, музика, дизайн, графіка, програмування, web-дизайн тощо). Педагогічно виважений добір комп'ютерних та Інтернет-ресурсів може забезпечити допомогу в навчанні і виконанні шкільних завдань Слід пам'ятати, що деперсоналізований характер відомостей та спілкування в Інтернеті заважають їх адекватній оцінці. Тому необхідним є налаштування дитини (особливо, якщо їй менше 10 років) на перевірку достовірності відомостей з Інтернету. Довірливі відносини між батьками та дітьми, допоможуть у доборі й оцінюванні інформаційних ресурсів лише за наявності активної позиції батьків і їх авторитету як джерела педагогічно виважених відомостей. Також для цієї категорії дітей необхідним є блокування батьками джерел загрозливих відомостей (що проповідують насильство, що збуджують агресію і страхи, суїциди, щодо виготовлення вибухових речовини, відомостей порнографічного характеру тощо) і налаштування дитини на самоусунення від завідомо небезпечних відомостей та онлайн-контактів [4].

Для середнього шкільного віку основними завданнями батьків є виявлення прихованих змістів, контекстів (цілей джерела інформації) за спільного користування відомостями, налаштування на недовіру (додаткова перевірка джерел інформації) [5].

У підлітковому віці під час оцінювання інформаційних ресурсів, слід співвідносити їх із загальноприйнятими соціально адекватними нормами поводження, з прийнятими в родині моральними цінностями, позиціями. За сумісного перегляду (сприйняття інформації) потрібно допомагати дитині у виробленні власної думки.

У шкільному середовищі під час формування інформаційно-безпекової культури особливу увагу слід приділяти розвитку критичного мислення, навичок аналізу, пошуку і збереження даних, виробленню власної думки дітей. Використання засобів морального виховання дозволить оцінювати інформаційні ресурси з позицій добра і зла, суспільної моралі й користі. Вказаним цілям має сприяти створення внутрішньо шкільного інформаційного середовища із соціально-корисними інформаційними ресурсами [5].

Комплексний підхід до інформаційної безпеки вимагає поєднання таких заходів по відношенню до користувачів-учнів: контроль з боку вчителя (перш за все візуальний), контроль і реагування на несанкціоновані дії програмних засобів захисту, реагування персоналу, вчителя при виникненні небезпечних ситуацій і застосування відповідних виховних заходів. [4]. Відповідно до світового досвіду, можливою формою цього документу є підписана учнями, їхніми батьками і вчителями письмова угода, що визначає порядок використання Інтернету та інформаційних ресурсів. Ці правила повинні обов'язково включати інструкцію з публікації в Інтернету особистих даних учнів, їхніх фотографій, аудіо- і відеоматеріалів і тощо.

Література

1. Liedel K., 2014, Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego. Torun: Wyd-wo Adam Marszałek. 96 s.

2. Безпека в Інтернеті. Microsoft, 2023. URL: https://support./microsoft.com/uk-ua/office/безпека-в-інтернеті-ce495131-eb83-4dc7-acea-/6304a220372e

3. Варивода К. Інформаційна безпека підлітків в Інтернет-мережі. *Молодий вчений*. 2016. Т. 3, № 30. С. 365–368.

4. Дем'яненко В. М., Ковальчук В. Н. Методичні рекомендації з інформаційної безпеки навчального комп'ютерного комплексу. Київ : ІІТЗН НАПН України, 2014. С. 27, 31, 39.

5. Павелків Р. В. Вікова психологія : підручник. Київ : Кондор, 2015. 469 с.

6. Підгорна Т., Берест І. Деякі аспекти організації інформаційної безпеки учнів. *Педагогіка і психологія професійної освіти*. 2014, № 6. С. 70–78.

7. Про Доктрину інформаційної безпеки України, 2017 : *Указ Президента України від 25.02.2017 № 47/2017*. URL: https://www./president.gov.ua/documents/472017-21374