© О.М. Спірін, В.Н. Ковальчук, 2011
ISSN 2076-8184. Інформаційні технології і засоби навчання. 2011. №1 (21).
Режим доступу до журналу: http://www.journal.iitta.gov.ua

УДК 373.1:004.056

Спірін Олег Михайлович, доктор педагогічних наук, головний науковий співробітник, Інститут інформаційних технологій і засобів навчання НАПН України

Ковальчук Вікторія Наумівна, асистент кафедри прикладної математики та інформатики, Житомирський державний університет імені Івана Франка

МЕТОДИКА ЗАБЕЗПЕЧЕННЯ ОН-ЛАЙН БЕЗПЕКИ СТАРШОКЛАСНИКІВ У НАВЧАЛЬНО-ВИХОВНОМУ ПРОЦЕСІ ШКОЛИ

Анотація

У статті проаналізовано проблеми забезпечення інформаційної безпеки школярів у загальноосвітньому навчальному закладі й розроблено систему заходів, які необхідні для її забезпечення. Розглянуто структурну і функціональну модель забезпечення інформаційної безпеки старшокласника у комп'ютерно орієнтованому навчальному середовищі. З’ясовано особливості забезпечення он-лайн безпеки старшокласників і методики навчання Інтернет безпеки у шкільному курсі інформатики. Уточненні поняття «забезпечення інформаційної безпеки старшокласника», «он-лайн безпека старшокласника».

Ключові слова: он-лайн безпека старшокласників, забезпечення інформаційної безпеки старшокласника, методика навчання Інтернет безпеки.

Постановка проблеми. Нині спостерігається значний прогрес технологій, зростання швидкості Інтернету, а в найближчому майбутньому більшість шкіл будуть під’єднані до швидкісного Інтернету на постійній основі. Та, не зважаючи на значний розвиток інформаційно-комунікаційних технологій, використання технології бездротового Інтернету і мобільних пристроїв у шкільній освіті, усе ще спостерігається нерівномірне забезпечення рівня доступу шкіл до мережі Інтернет, не знаходять належної уваги проблеми попередження доступу дітей до небажаного контенту. До того ж можливості Інтернет-технологій не повною мірою використовуються в навчанні, а часто їх використання взагалі відволікає дітей від навчального процесу.

Аналіз публікацій. Одним із завдань, визначених у Концепції державної цільової програми «Сто відсотків» [13], є «забезпечення інформаційної безпеки та

централізованого фільтрування несумісного з навчальним процесом контенту». Питання он-лайн безпеки дітей висвітлюється в низці статей [1, 6, 9, 17, 18, 20], а також посібників і веб-ресурсів [2, 7, 8, 16]. Варто зазначити, що кількість англомовних веб-ресурсів, присвячених цій проблематиці, налічує десятки тисяч, а кількість україномовних ресурсів не перевищує й десяти. У педагогічній науці дослідження питань інформаційної безпеки (ІБ) школярів лише розпочинаються [4, 14, 19, 21]. Поряд із цим суттєвим є доробок науковців з методики викладання питань інформаційної безпеки в школі і педагогічних ВНЗ (Бочаров М. І., Бухаркіна М. Ю., Волкова Т. В., Зеркіна О. В., Калінін І. А., Клімонтова Г. Н., Ломаско П. С., Танова Е. В., Орел І. Ю., Поляков В. П., Перьков М. О., Самоделова Л. О., Чусавітіна Н. Г. та ін.).

Невирішені питання. Відомо, що в США доступ до Інтернету з 2000 року мали всі школи, а в Україні процес забезпечення такого доступу для всіх шкіл лише добігає завершення. Поряд із цим, починаючи із середини 90-х років у США і Європі розробляються сайти, створюються громадські організації і навчально-тренінгові програми для учнів, учителів і батьків, присвячені он-лайн безпеці. В Україні до розв’язання цієї проблеми звернулися лише останні два роки завдяки зусиллям низки неурядових і комерційних організацій. Безсумнівно, що проблема безпеки дитини в Інтернеті є важливою і складною, а досвід України у питаннях забезпечення безпеки дітей в Інтернеті досить обмежений. Бракує відповідних україномовних веб-ресурсів й обізнаності з цими питаннями вчителів інформатики, батьків та інших зацікавлених осіб. Варто сподіватися, що необхідні заходи не обмежуватимуться проведенням щорічного дня безпечного Інтернету, а політика держави в освітній галузі з цього напряму стане системною і виваженою й буде, зокрема, реалізовуватися шляхом відповідної підготовки і перепідготовки вчителів інформатики.

Значним недоліком є також відсутність в Україні цілеспрямованої державної політики щодо застосування у школах спеціальних контент-фільтруючих програм. Для порівняння, у розвинених країнах приділяється значна увага на державному рівні для розробки і запровадження у школах таких програм, а в Росії така програма розробляється з 2006 року. Державою фінансується не лише розробка таких програм, але й підтримка бази даних цих програм у актуальному стані. Це дуже важливо, оскільки більшість з цих програми діють за принципом білих і чорних списків і вимагають постійного оновлення, аналогічно до антивірусних програм.

Отже, спостерігається відставання України від розвинених країн у галузі інформатизації, застарілість технічного і програмного забезпечення, недостатня кількість і компетентність обслуговуючого персоналу, не розробленість нормативної бази [13]. Можемо констатувати, що на даний час в Україні склалась ситуація, коли забезпеченню інформаційної безпеки старшокласників у комп'ютерно орієнтованому навчальному середовищі (КОНС) загальноосвітнього навчального закладу не приділяється достатньої уваги.

Мета статті полягає у комплексному розгляді проблем забезпечення інформаційної безпеки старшокласника у комп'ютерно орієнтованому навчальному середовищі; розробці взаємопов'язаної системи заходів, що необхідні для її забезпечення; у розробці структурної і функціональної моделі забезпечення ІБ старшокласника у КОНС; у з'ясуванні особливостей забезпечення он-лайн безпеки старшокласників і методики навчання Інтернет безпеки у шкільному курсі інформатики; в уточненні базових понять дослідження «забезпечення інформаційної безпеки старшокласника», «он-лайн безпека старшокласника».

Виклад основного матеріалу. Як засвідчує досвід найбільш розвинених країн світу, наслідком підключення мережі до Інтернету є виникнення трьох проблем: безпеки дітей у відкритому інформаційному просторі (Інтернет або он-лайн безпека дітей), захисту персональних даних учнів і співробітників, безпеки комп'ютерно орієнтованого навчального середовища (КОНС) (рис. 1).

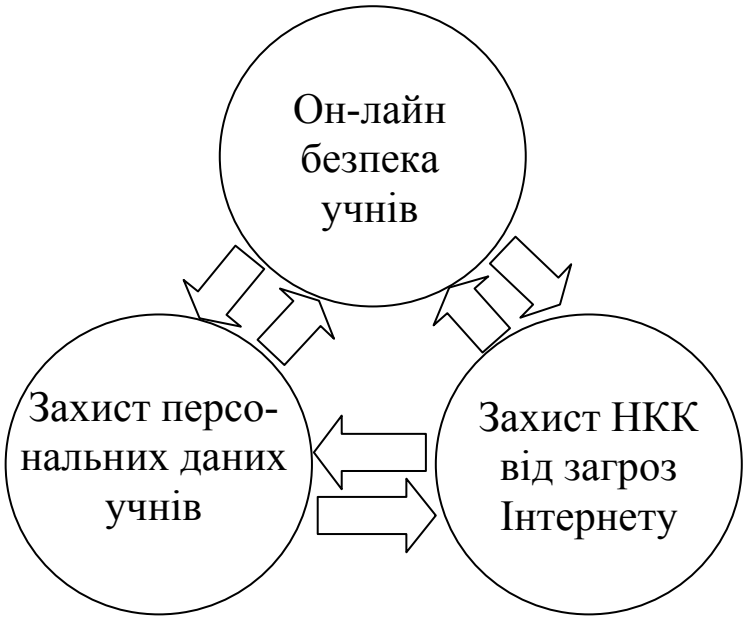


Рис. 1. Взаємозв'язок основних проблем ІБ у ЗНЗ

Зазначимо, що під КОНС будемо розуміти: «штучно побудовану систему, структура і складові якої створюють необхідні умови для досягнення цілей і реалізації безпечного навчально-виховного процесу, а всі компоненти передба-

чають переважне використання інформаційно-комунікаційних технологій (ІКТ)» [11]. Ці проблеми можливо вирішити лише враховуючи їх тісний взаємозв'язок і консолідуючи зусилля держави, громадських організацій, школи, батьків у розв'язанні всієї сукупності основних проблем інформаційної безпеки неповнолітніх.

У педагогічній науці питання інформаційної безпеки дитини є досить новими і мало дослідженими на даний час. Однією з перших і найбільш близьких до теми нашого дослідження є робота Саттарової Н. І. [19], оскільки в ній автор розглядає проблему інформаційної безпеки школяра під час роботи в Інтернеті у загальноосвітній установі у процесі навчання інформатики. Дисертантка з'ясовує ефективність різних моделей забезпечення інформаційної безпеки школяра, зокрема: налаштування браузера, фільтруючі програми, сімейний фільтр, імітація Інтернету. І хоча автором розроблені ґрунтовні рекомендації педагогам, батькам і учням, однак основна увага приділена програмним методам попередження доступу дітей до небажаної інформації (контент фільтрації). А в роботі Малих Т. О. [14], акцент перенесений на роль навчання і виховання у розвитку здатності молодшого школяра протистояти загрозам інформаційного середовища. Оптимальний результат може бути досягнутий поєднанням програмно-технічних засобів (Саттарова Н. І.) і навчально-виховних заходів (Малих Т. О.), а також організаційних, нормативно-правових заходів з ІБ. Тому ми вважаємо, що забезпечення комплексної безпеки особистості, що формується, можливо лише за поєднання нормативно-правових, організаційних, навчально-виховних, просвітніх, програмно-технічних заходів і засобів. ***Забезпечення інформаційної безпеки старшокласника*** *– це взаємопов'язана сукупність заходів, засобів і методів захисту, призначених для досягнення стану захищеності життєво важливих інтересів особистості у комп'ютерно орієнтованому навчальному середовищі.* Умовою забезпечення інформаційної безпеки старшокласника є створення безпечного комп'ютерно орієнтованого навчального середовища. Метою і результатом має слугувати формування інформаційно безпечної особистості випускника.

Суттєвим питанням є визначення суб'єктів інформаційної безпеки старшокласника, тобто тих, хто несе відповідальність за забезпечення цієї безпеки. У своїй статті Барна О. говорить про «необхідність об'єднання зусиль усіх зацікавлених сторін: батьків, вчителів, громадськості та самих дітей» [1], однак у поданій там же схемі, що називається: «Підходи до забезпечення уникнення загроз з Інтернету», не досить

чітко структурованими залишилися питання ієрархії взаємної відповідальності вказаних суб'єктів забезпечення ІБ. У посібнику Юдіна О. К. і Богуша В. М. [3: 30] зазначено, що існують рівні ІБ, а саме: держави, суспільства, особи. На рівні держави повинно бути здійснено нормативно-правове регулювання питань інформаційної безпеки неповнолітніх, організовано «забезпечення інформаційної безпеки і централізоване фільтрування несумісного з навчальним процесом контенту» [13], ініційовано оновлення змісту навчальних програм, підручників з питань безпеки Інтернету в курсі інформатики. На рівні суспільства діють такі суб'єкти: громадські організації, загальноосвітні навчальні заклади, батьки. Активну роль у поширенні знань з онлайн безпеки серед дітей, батьків, учителів шляхом проведення тренінгів і створення навчального порталу (Он-ландія безпечна веб-країна) відіграють громадські й комерційні організації [16, 2, 8]. Далі будемо розглядати питання забезпечення інформаційної безпеки старшокласників у загальноосвітніх навчальних закладах, оскільки саме вони є найменш дослідженими у наш час.

Проаналізувавши науково-методичну літератури, з'ясували, що основою для організації забезпечення інформаційної безпеки у ЗНЗ може слугувати модель забезпечення комплексної інформаційної безпеки в середній загальноосвітній і професійній школі [4], а також модель системи інформаційної безпеки навчального комп'ютерного комплексу [12]. На основі згадуваних моделей можливим є розподіл відповідальності між персоналом за проведення відповідних видів заходів, а також виявлення ієрархії управління системою комплексних заходів з ІБ. Проведений аналіз об'єктів і суб'єктів інформаційної безпеки в умовах ЗНЗ дозволяє виділити основні суб'єкти забезпечення ІБ школярів, це: сам учень, учитель інформатики, учителі-предметники, технічний персонал, дирекція школи. На думку Бочарова М. І., «провідна роль у забезпеченні та навчанні ІБ в середньому загальноосвітньому закладі належить вчителю інформатики, який буде здатний навчати і забезпечувати комплексну ІБ в середньому закладі» [4]. Завдання вчителя інформатики полягає в організації захисту інформаційних ресурсів, навчального комп'ютерного комплексу (НКК) і учнів від найбільш вірогідних інформаційних загроз і негативних наслідків ІКТ. Це дає можливість сформулювати таке визначення. ***Професійна компетентність учителя інформатики з інформаційної безпеки*** – це сукупність знань і розуміння, умінь, навичок, а також особистісних ставлень і ціннісних орієнтацій учителя в галузі інфор-

маційної безпеки, та здатність автономно і відповідально демонструвати їх для розв'язування типових професійних задач і вирішення проблем інформаційної безпеки, що виникають у реальних умовах навчально-виховного процесу школи. Компетентність вчителя інформатики в частині забезпечення інформаційної безпеки старшокласників має враховувати потреби захисту персональних даних учнів, персональних комп'ютерів і власне учнів від найбільш вірогідних інформаційних загроз і негативних наслідків ІКТ. Результатом діяльності вчителя інформатики та інших суб'єктів інформаційної безпеки (адміністрація школи, технічний персонал) має бути забезпечення інформаційної безпеки всіх вище перерахованих об'єктів (рис. 2).

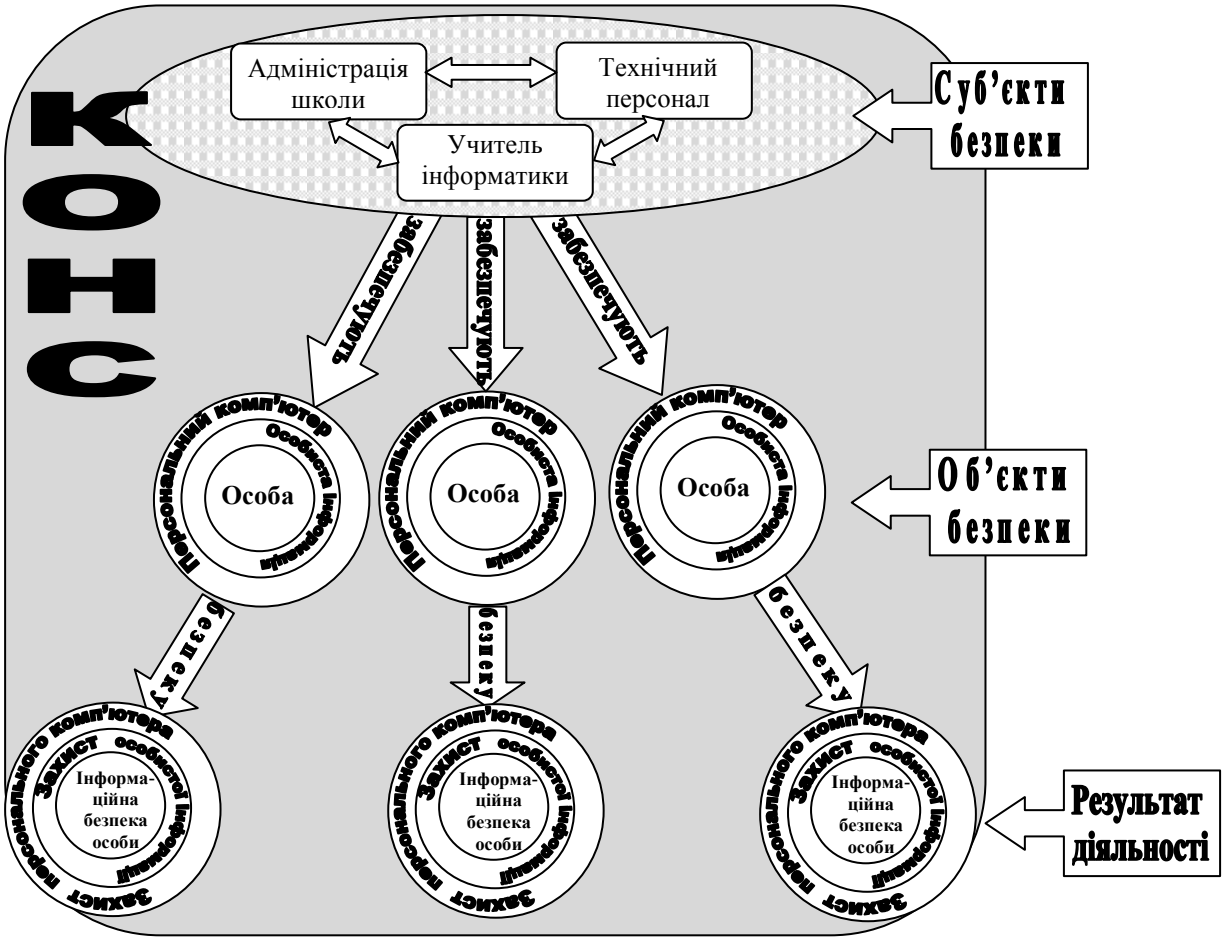


Рис. 2. Структурна модель забезпечення інформаційної безпеки старшокласників у КОНС

Описаний далі комплекс заходів, а також запропонований Шишкіною М. П. модельний підхід до побудови комп'ютерно орієнтованого навчального середовища, дозволив нам запропонувати структурну і функціональну модель забезпечення ІБ старшокласника у КОНС (рис. 2 і рис. 3), у першій з яких «відтворюється внутрішній склад системи та відношення між її елементами», а інша «відображає функції, які ви-

конує об’єкт, що моделюється, або його складові, характерні риси діяльності системи, розвитку» [22].

На функціональній моделі (рис. 3) розглянуто комплекс заходів з інформаційної безпеки, показано, які суб’єкти проводять ці заходи, а також на формування яких якостей старшокласника вони спрямовані. Зображено, що основою формування інформаційно безпечної особистості випускника є безпека КОНС, як середовища соціалізації особистості. Безпека КОНС забезпечується комплексом програмно-апаратних засобів і організаційних, навчально-виховних, процедурних заходів. Мета забезпечення ІБ старшокласника є формування інформаційно безпечної особистості, яка здійснюється на основі навчання і виховання відповідних якостей і здатностей особистості: дисциплінованості, компетентності і культури ІБ.

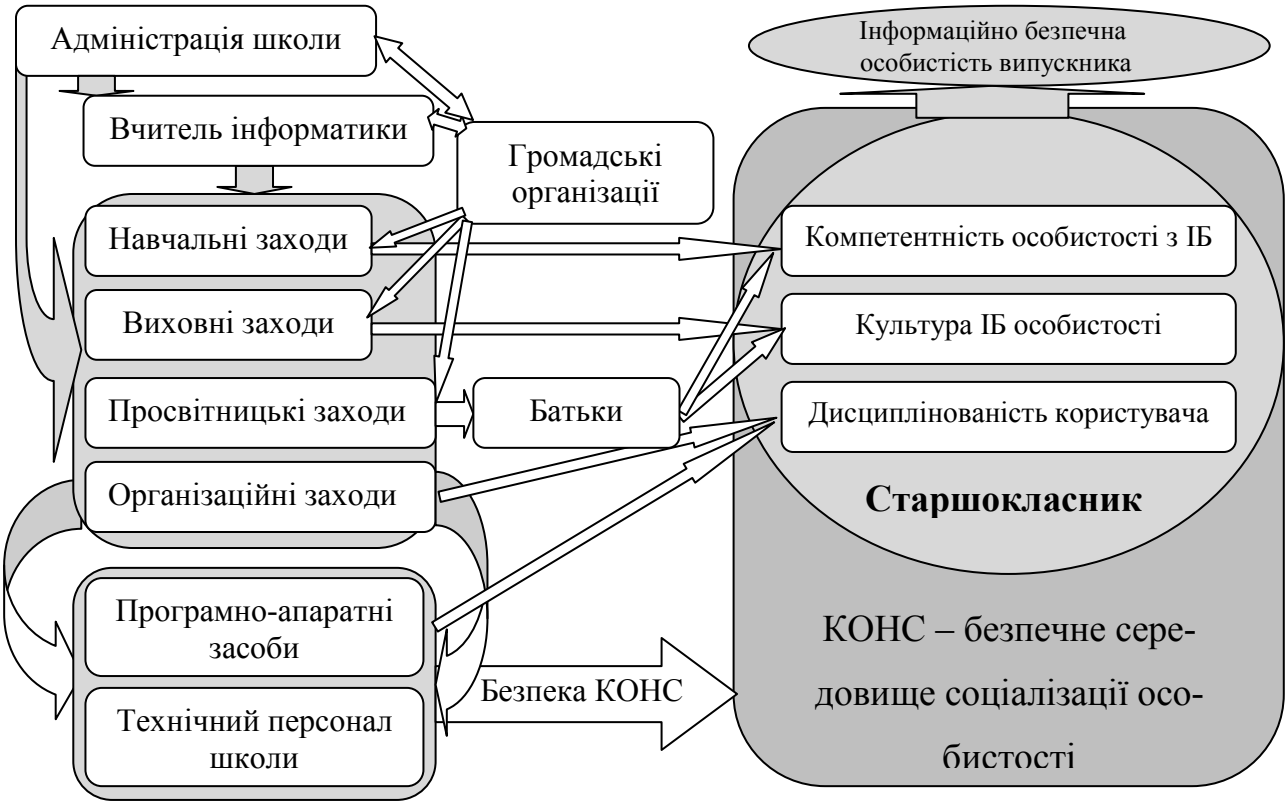


Рис. 3. Функціональна модель забезпечення інформаційної безпеки старшокласника у КОНС

Особливості забезпечення он-лайн безпеки старшокласників у навчально-виховному процесі школи

Базуючись на визначенні інформаційної безпеки старшокласника [11] під онлайн безпекою старшокласника будемо розуміти складову частину інформаційної безпеки особистості, яка стосується діяльності її в Інтернеті.

Особливістю сучасного розвитку ІКТ є те, що наслідки їх безконтрольного застосування впливають не лише інтелектуальний чи моральний розвиток дитини, але загрожують особистій безпеці (викрадення, пограбування, розбещення тощо), а також фізичному і психічному здоров'ю (комп'ютерно-ігрова залежність, інформаційне перевантаження, гіподинамія тощо). «Користуючись засобами Інтернет-комунікації, насамперед чат-кімнатами, електронною поштою та миттєвими повідомленнями, дитина піддається загрозі стати об'єктом онлайнового хижака. Зловмисники цієї категорії користуючись тим, що завдяки анонімності Інтернету в он-лайні можна досить швидко встановлювати довірливі відносини. Жертвами онлайнових хижаків найчастіше стають недосвідчені молоді люди.» [15: 342].

Згідно дослідження, проведеного Кафедрою превентивної освіти і соціальної політики ЮНЕСКО у партнерстві з «Майкрософт Україна», багато дітей безтурботно розміщують особисту інформацію і ходять на зустрічі з віртуальними знайомими. Зокрема насторожує легковажне ставлення дітей усіх вікових груп – а особливо 15–17 років – до розповсюдження особистої інформації, що демонструє необхідність всебічного системного підходу до навчання дітей основам безпеки в Інтернеті [16]. Отже, основну увагу слід приділяти саме особистій безпеці школярів і навчанню їх оцінювати ризики і небезпеки Інтернету, не розголошувати особисті дані при забезпеченні їх он-лайн безпеки.

Однією з основних проблем для вихователів є не контрольованість Інтернету як джерела інформації, відомостей і даних. Оскільки глобальна комп'ютерна мережа містить багато матеріалів, які не тільки не є корисними для дітей, але й можуть завдати шкоду їх психічному, моральному чи навіть фізичному здоров'ю. Поряд із підсиленням батьківського і вихователського контролю за тим, що саме діти роблять в Інтернеті, – такий контроль є часто малоефективний з огляду на недостатню компетентність педагогів і батьків щодо застосування програм-фільтрів, що блокують звертання до відомих адрес із сумнівним змістом [10: 33]. Однак, за словами Паррі Афтаб, відомого спеціаліста з питань безпеки дітей в Інтернеті, кращий фільтр, який може дійсно забезпечити безпеку дитини в мережі й розв'язати багато інших проблем, – у голові в самої дитини, а дорослим потрібно тільки «налаштувати» цей фільтр [17]. Основна роль у забезпеченні власної безпеки належить особистості, тому провідну роль у недопущенні доступу старшокласників до матеріалів, несумісних із завданнями навчан-

ня, особливо за переважної відсутності контент-фільтруючих програм у школі і вдома, є навчання і виховання з метою формування інформаційно безпечної особистості.

Ще однією особливістю Інтернет-комунікацій можна назвати низку неадекватних дійсності уявлень про Інтернет, які побутують у суспільній свідомості: ілюзія анонімності, ілюзія безпечності, ілюзія безкарності. Як зазначає М. А. Бенкс [5: 158], онлайновий світ має два аспекти, які впливають на інформаційну безпеку особи. По-перше, користувач відчуває анонімність. Тобто інші користувачі не можуть вас бачити, як наслідок, здається, що можна робити й говорити все що завгодно. Користувач втрачає пильність і обережність. Вдавана безпека кіберпростору шкодить самій людині. Другий аспект – це «нереальність» середовища Інтернет. Багатьом здається, що інший користувач Інтернету реальний не більше, ніж який-небудь символ у комп'ютерній грі. Користувач забуває, що, не зважаючи на не можливість фізичного контакту, інший користувач може нанести шкоду і може виявитися в реальності не тим, за кого себе видає. Відчуття фізичної безпеки асоціюється з безпекою взагалі і тому неповнолітні користувачі Інтернету часто стають жертвами злочинів, наприклад, викрадення, сексуального розбещення й експлуатації, залякування, пограбування, шахрайства. У формуванні адекватного дійсності сприйняття Інтернету в старшокласників доцільним є використання методики, запропонованої Дітковською Л. А. [9], а саме порівняння небезпек і запобіжних заходів у реальному житті та в мережі Інтернет.

Комплекс заходів із забезпечення он-лайн безпеки старшокласників

Комплексний підхід до інформаційної безпеки вимагає поєднання певних заходів відносно користувачів-учнів: контроль з боку вчителя (перш за все, візуальний), контроль і реагування на несанкціоновані дії (НСД) програмних засобів захисту, реагування персоналу, учителя у разі виникнення НДС і застосування відповідних виховних заходів. Під несанкціонованими діями ми будемо розуміти дії, що заборонені політикою безпеки і конкретизовані в правилах користувачів.

До ***організаційних заходів*** належать, перш за все, розробка, впровадження і контроль за виконанням правил політики безпеки для користувачів-учнів. Контроль за виконанням покладено на вчителів і обслуговуючий персонал. Правила щодо доступу до Інтернету, встановлені в школі, повинні бути формалізовані, тобто мати вигляд обов'язкового документа. Відповідно до світового досвіду можливою формою цього

документа є підписана учнями, їхніми батьками і вчителями письмова угода, що визначає порядок використання Інтернету – тобто формалізовані правила набувають рис «колективної угоди». Ці правила повинні обов’язково включати інструкцію з публікації в Інтернеті особистих даних учнів, їхніх фотографій, аудіо- і відеоматеріалів тощо.

Частина правил політики безпеки, що стосується доступу учнів до Інтернету, має бути повідомлена їм перед початком відповідних занять. Найкращий варіант – коли вчитель виконує роль не доглядача, а консультанта. Цього можна спробувати досягти, провівши бесіду з дітьми, де їм буде докладно розказано про небезпеки, що існують в Інтернеті, необхідно навчити їх правильно виходити з непередбачуваних ситуацій. Інструкції з безпечного використання Інтернету повинні бути роз'яснені учням до того, як вони одержать доступ до Інтернету або їм нададуть індивідуальні адреси електронної пошти. На закінчення бесіди варто пояснити обмеження на використання Інтернету й обговорити їх з дітьми. Спільно посилити безпеку використання мережі Інтернет набагато простіше.

Програмно-апаратні засоби безпеки реалізують через систему управління (контролю) доступу користувачів до ресурсів, яка включає ідентифікацію та автентифікацію користувачів, управління (контроль) доступу до ресурсів, протоколювання й аудит дій користувачів. Програмно-апаратні засоби мають гарантувати захищеність критично важливих компонентів програмного забезпечення (ПЗ) НКК від несанкціонованих і помилкових дій користувачів. У правилах розмежування доступу необхідно заборонити доступ цих користувачів до системних областей диску, а також заборонити модифікацію ними програмного забезпечення, навчальних та інших важливих даних. Рекомендується забезпечити доступ в Інтернет тільки з тих комп'ютерів, що постійно знаходяться в полі зору вчителя. Також варто використовувати програми, що дають можливість відображати вміст екранів усіх комп'ютерів на моніторі вчителя і тим самим дозволяють стежити за діяльністю учнів. Основними програмно-апаратними засобами попередження доступу школярів до небажаного контенту є програми контент-фільтрації. Більш детально вказані питання розглянуто у [12: 44–50].

Виховні заходи з он-лайн безпеки повинні плануватися і проводиться у навчальному закладі регулярно. Передовий педагогічний досвід свідчить, що форми прове-

дення виховних заходів можуть бути самі різні, наприклад, бесіди, вікторини, стінні газети, батьківські збори, ігри, тренінги, дискусії тощо.

Важливу роль виховні заходи відіграють у реалізації політики безпеки НКК. Оскільки вони використовуються як для попередження НСД, так і для впливу на порушників правил безпеки з метою їх перевиховання. Дуже важливо встановити правила покарання тих, хто зловживає доступом; порушення можуть бути і не настільки значними, але повинні бути обговорені, а за серйозні провини мають бути передбачені серйозні заходи покарання.

Варто зазначити, що з кожним роком зростає кількість працівників, які так чи інакше використовують у своїй повсякденній роботі інформаційні технології. Також, безсумнівно, зростає роль інформаційної безпеки як неодмінної складової будь-якої інформаційної системи. Найуразливішою ланкою будь-якої системи безпеки були і будуть люди. Тому майбутнього кваліфікованого працівника неможливо уявити без необхідних базових знань з інформаційної безпеки. Важливу роль відіграє не лише навчання, але й виховання, оскільки лише воно забезпечує засвоєння морально-етичних норм у галузі інформаційних технологій.

Правила інформаційної безпеки для користувачів-учнів, з педагогічної точки зору, повинні сприяти вихованню учнів, зокрема доцільно преміювати учнів (розширювати права) за хорошу поведінку і «карати» за погану. Основні методи, які використовують для безумовного виконання політики безпеки користувачами, є інформування, контроль, спонукання, попередження, тимчасова заборона (відмова в доступі), зменшення наданих прав і привілеїв (як користувача НКК) та інші.

Головна мета виховних заходів є усвідомлення учнями відповідальності за свої дії навіть у «віртуальному» середовищі, засвоєння етичних норм поводження в цьому середовищі, результатом чого є формування в учнів культури і компетентності з інформаційної безпеки.

Просвіта батьків з питань інформаційної безпеки

Враховуючи розширення змісту діяльності вчителя інформатики, що стосується надання інформаційно-консультаційних послуг учителям, батькам, учням, а також широкого розповсюдження домашніх персональних комп'ютерів (ПК), вагомою складовою його компетентності є вміння переконувати батьків у необхідності захисту дітей від шкідливої інформації. Для забезпечення єдиних вимог і умов он-лайн безпеки

учнів, як у школі, так і вдома, необхідною є співпраця батьків і вчителів. З відомостями про небезпеки онлайнового середовища варто ознайомити не лише учнів, але й батьків. До того ж одним з основних завдань вчителя інформатики є навчити дітей і підлітків уникати небезпек мережі Інтернет. Як утримати учнів від доступу до вебсайтів, що містять непристойні матеріали, і від контакту з особами, що представляють для них загрозу? Щоб захистити учнів і переконати в необхідності цього їхніх батьків, необхідно вжити заходів, спрямованих на запобігання будь-яких несанкціонованих вторгнень в інформаційний простір школи. Варто одержати згоду батьків на прийняття рішень, що можуть викликати ризик для дітей, і спробувати зробити їх учасниками прийняття рішень. Для цього вчителі повинні розповісти батькам, з якою метою вони використовують Інтернет у школі, які можуть бути небезпеки і як вони контролюють ризики. Повідомлення має бути ясним і чітким (закінченим), і надавати всі важливі відомості так, щоб найменш обізнані з питань використання комп'ютерів батьки змогли б їх зрозуміти.

Необхідність консультації батьків про можливості використання програмного забезпечення і технічної реалізації, не допущення доступу дітей до шкідливої інформації через домашній ПК вимагає набуття майбутніми вчителями компетентностей з питань інформаційної безпеки.

Основні компоненти методики навчання он-лайн безпеки старшокласників на уроках інформатики

Одним із завдань нашого дослідження є експериментальна перевірка ефективності методики забезпечення інформаційної безпеки старшокласника, у частині, що стосується методики навчання питанням он-лайн безпеки. Було розроблене відповідне методичне забезпечення, зокрема, презентація, матеріали для тестування, інструктивні матеріали для вчителів інформатики. Для розробки презентації і тесту було використано матеріали сайту Онляндія. Розглянемо основні елементи запропонованої методики (повний варіант матеріалів розміщено в мережі «Вчитель-новатор»).

Слайд №1. Демонструється тема уроку: «Безпека в Інтернеті».

Слайд №2. Показуються види загроз Інтернету: для особи, персональних даних, комп'ютера.

Слайд №3. Описуються шкідливі програми й особливості комп'ютерних вірусів і хробаків.

Слайд №4. Описуються поняття хакера і програми-троянця.

Слайд №5. Описується уявлення про комп'ютерну безпеку.

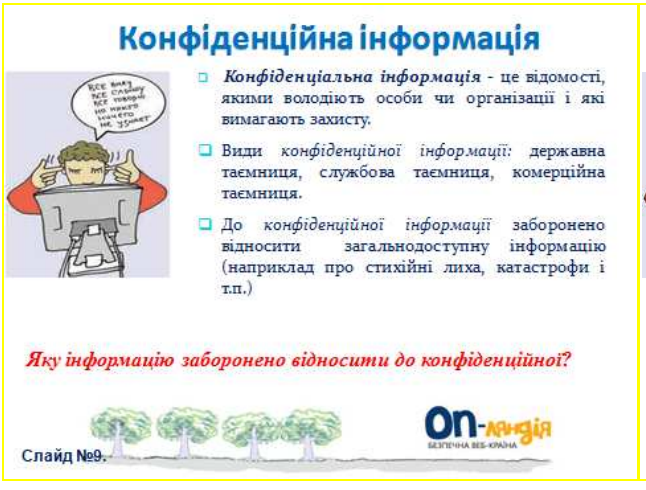
Слайд №6. Роз'яснюються методи захисту даних: архівування, шифрування.

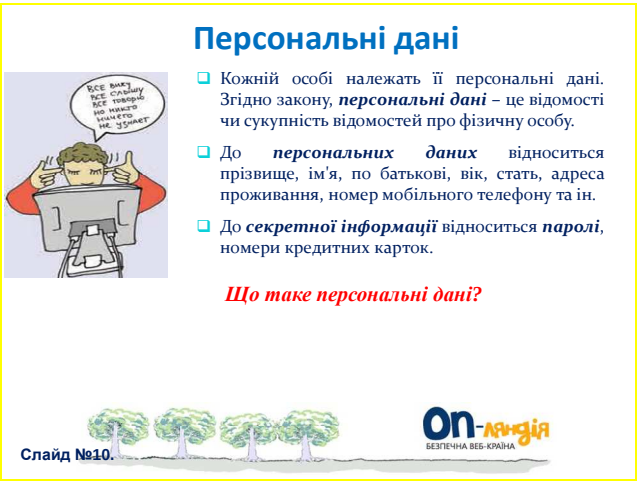
Слайд №7. Звертається увага учнів на те, що закони, які діють в Інтернеті, самі подібні до законів реального життя.

Слайд №8. Порівнюються дозволені й недозволені дії в Інтернеті.

Слайд №9. Пояснюється, що таке конфіденційна інформація.

Слайд №10. Дається уявлення про персональні дані.





Слайд №11. Дається уявлення про особисту безпеку.

Слайд №12. Розповідається про такі загрози для дітей, як викрадення і розбещення.

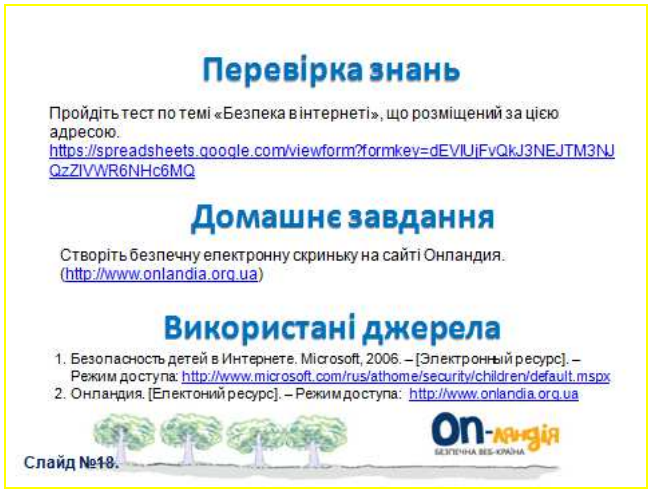
Слайд №13. Розповідається про такі загрози, як пограбування і залякування.

Слайд №14. Дається уявлення про шахрайство в мережі.

Слайд №15. Наводяться основні правила особистої безпеки в Інтернеті.

Слайд №16. Роз'яснюється, що таке стійкий і нестійкий пароль.

Слайд №17. Перехід на тест до цієї теми.



Методичні рекомендації для вчителів

1. Урок проводиться у формі лекції для всього класу; поряд із цим доцільно проектувати слайди на екран. Якщо є можливість, то урок проводиться для підгрупи;

при цьому доцільно здійснювати трансляцію слайдів з учительського комп'ютера на учнівські.

2. Бажано залучати учнів до сумісного пошуку відповіді на питання, що виділені червоним кольором на слайдах.

3. Особливу увагу в презентації і тестуванні приділено питанням особистої безпеки дітей в Інтернеті. Варто зазначити, що неодноразовими є випадки викрадення дітей за допомогою відомостей, отриманих з Інтернету, або спілкування жертви-дитини з незнайомцем, який потім викрав дитину. При цьому частка розкритих злочинів не перевищує 1%.

4. Необхідно довести до відома учнів, що люди в Інтернеті часто видають себе за інших (наприклад, розміщуючи чужу фотографію (наприклад, відомої особи) замість своєї), можуть представлятися іншими іменами, вказувати менший вік (наприклад, дорослі чоловіки представляються підлітками), навіть «змінювати» стать. Необхідно наголосити, що знайомий з Інтернету може виявитися зовсім не тією людиною. Тому небезпечно видавати персональну інформацію на прохання незнайомців з Інтернету й поміщувати таку інформацію в Інтернеті (наприклад, у соціальних мережах). Не можна йти на зустріч з незнайомцем з Інтернету без дозволу або супроводу батьків.

5. Шахрайство в Інтернеті має за мету заробляння грошей. Від звичайного випрошування грошей, до явного обману. Варто наголошувати, що використовувати будь-які сервіси Інтернету, які вимагають оплати (номерів кредитних карток, надсилання повідомлень чи здійснення дзвінка з мобільного телефону), можна лише з дозволу батьків, бо це може призвести до втрати коштів. Необхідно всю сумнівну інформацію з Інтернету перевіряти з інших незалежних джерел.

6. Особливо важливим є питання правил безпечної поведінки в Інтернеті й добору стійких паролів. Наголосіть, що дотримання цих правил необхідно самим учням, оскільки забезпечить їхню особисту безпеку. Паролі ж є важливими, оскільки захищають іншу важливу особисту інформацію, і є, як правило, найслабшою ланкою захисту.

7. На останньому слайді є посилання на адресу тесту в Інтернеті.

Проведене дослідження дає підстави для таких **висновків.**

Питання забезпечення он-лайн безпеки старшокласників є дуже важливими і мають свої особливості, на які варто звертати увагу під час навчально-виховного процесу в школі. Он-лайн безпеку потрібно розглядати як складову інформаційної безпеки старшокласника, а підходи до вирішення проблем ІБ у ЗНЗ повинні включати комплекс взаємопов'язаних заходів, методів і засобів. Забезпечення ІБ старшокласників у КОНС вимагає об'єднання зусиль батьків, учителів, громадськості та самих дітей і координації цих зусиль на державному рівні. Провідна роль у формуванні інформаційно безпечної особистості випускника належить вчителю інформатики. Застосування запропонованої методики навчання он-лайн безпеки дозволяє підвищити компетентність учнів з вказаних питань.

Подальших досліджень потребує питання визначення співвідношення понять «інформаційна безпека особистості», «культура інформаційної безпеки особистості», «безпечна соціалізація особистості». Потребують подальших досліджень організаційно-педагогічні проблеми застосування контент-фільтрації під час доступу до ресурсів і сервісів мережі Інтернет у вітчизняних загальноосвітніх навчальних закладах.

Список використаної літератури.

1. *Барна О.* Безпека дітей в Інтернеті: як діяти? / О. Барна // Нові інформаційні технології в освіті для всіх: інноваційні методи та моделі / Збірник праць VI Міжнародної «Нові інформаційні технології в освіті для всіх: інноваційні методи та моделі». – К.: IRTC, 2009. – С. 193–201.

2. Безпека дітей в Інтернеті. – [Електронний ресурс] // Сайт Microsoft. – 2006. – Режим доступу: http://www.microsoft.com/rus/athome/security/children/default.mspx.

3. *Богуш В. М.* Інформаційна безпека держави / В. М. Богуш, О. К. Юдін. – К.: «МК-Прес», 2005. – 432 с.

4. *Бочаров М. И.* Обучение будущих педагогов совместному с администрацией обеспечению комплексной безопасности образовательного учреждения / М. И. Бочаров // Информатика и образование. – 2010. – №2. – С. 93–96.

5. *Бэнкс М. А.* Информационная защита ПК : пер. с англ. / М. А. Бэнкс. – К.: ВЕК+; М.: Энтроп ; СПб.: Корона-Принт, 2001. – 269 с.: рис.

6. *Василенко Н.* Этот многоликий Интернет: можно ли защитить детей от «плохой» информации и приучить к полезной? / Н. Василенко // Директор школы. – 2004. – №7. – С. 66–69.

7. *Джонсон С.* Как уберечь детей от опасностей Интернета: вирусов, программ-шпионов, порносайтов, всплывающих окон / Саймом Джонсон; [перевод с англ. А. Е. Ивановой]. – М.: НТ Прес, 2006. – 304 с.: ил.

8. Діти в Інтернеті: як навчити безпеці в віртуальному світі / І. В. Литовченко, С. Д. Максименко, С. І. Болтівець та ін. – К.: Вид. ТОВ Видавничий будинок «Аванпост-Прим», 2010. – 48 с. – (Посібник для батьків).

9. *Дітковська Л. А.* Для кого Інтернет може бути небезпечний [Електронний ресурс] / Л. А. Дітковська // Інформаційні технології і засоби навчання. – 2007. – №3.– Режим доступу: http://www.ime.edu-ua.net/em3/content/07dladbm.htm.

10. Информационно-психологическая безопасность (определение и анализ предметной области) / Смолян Г. Л., Зараковский Г. М., Розин В. М., Войскунский А. Е.; Ин-т систем. анализа РАН. – М.: ИСА, 1997. – 52 с.

11. *Ковальчук В. Н.* Інформаційна безпека старшокласника у комп'ютерно орієнтованому навчальному середовищі / В. Н. Ковальчук // Інноваційні інформаційно-комунікаційні технології навчання математики, фізики, інформатики у середніх і вищих навчальних закладах: зб. наук праць за матеріалами Всеукр. наук.-метод. конф. молодих науковців, 17–18 лют. 2011 р. – Кривий Ріг: КДПУ, 2011. – С. 304–307.

12. *Ковальчук В. Н.* Система інформаційної безпеки навчального комп'ютерного комплексу: метод. рекоменд. – Житомир: ЖДУ, 2009. – 84 с.

13. Концепція Державної цільової програми впровадження у навчально-виховний процес загальноосвітніх навчальних закладів інформаційно-комунікаційних технологій «Сто відсотків» на період до 2015 року. Затверджено розпорядженням Кабінету Міністрів України від 27 серпня 2010 р. № 1722-р.

14. *Малых Т. А.* Педагогические условия развития информационной безопасности младшего школьника: дис. ... канд. пед. наук 13.00.01 / Малых Тетьяна Александровна; Иркут. инст. повышения квалиф. работ. образ. – Иркутск, 2008. – 168 с.: іл.

15. Морзе Н. В. Основи інформаційно-комунікаційних технологій / Н. В. Морзе. – К.: Видавнича група BHV, 2008. – 352 с.

16. Онландия. – [Електронний ресурс]. – Режим доступу: http://www.onlandia.org.ua.

17. Проблема: Интернет в школах. – [Електронний ресурс]. – Режим доступу: http://sp.sz.ru/01_02_05_03_.html.

18. *Прохоров А.* «Приличный» Интернет в школе и дома. – [Електронний ресурс] // КомпьютерПресс. – 2007. – №2. – Режим доступу: http://www.compress.ru/article.aspx?id=17262&iid=799.

19. *Саттарова Н. И.* Информационная безопасность школьников в образовательном учреждении: дис. ... канд. пед. наук 13.00.01 / Саттарова Надежда Ивановна; С.-Петерб. акад. последиплом. пед. образования. – С.-Петерб., 2003. – 215 с.: ил.

20. *Степанов В.* Меры безопасности при работе в Интернете / В. Степанов // Шкільна бібліотека. – К.: Київська правда. – 2009. – № 7 – С. 71–73.

21. *Федосов А. Ю.* Обеспечение информационной безопасности школьников / А. Ю. Федосов // Педагогическая информатика. – 2010. – № 1. – С. 32–37.

22. *Шишкіна М. П.* Модельний підхід у побудові комп'ютерно-орієнтованого навчального середовища // Мат-ли VI Міжнародної науково-практичної конференції «Інформатизація освіти та дистанційна форма навчання: сучасний стан та перспективи розвитку». – Суми, січень-жовтень 2004 р. – С. 17–21.

МЕТОДИКА ОБЕСПЕЧЕНИЯ ОН-ЛАЙН БЕЗОПАСНОСТИ СТАРШЕКЛАССНИКОВ В УЧЕБНО-ВОСПИТАТЕЛЬНОМ ПРОЦЕССЕ ШКОЛЫ

Спирин Олег Михайлович, доктор педагогических наук, главный научный сотрудник, Институт информационных технологий и средств обучения НАПН Украины, г. Киев

Ковальчук Виктория Наумовна, ассистент кафедры прикладной математики и информатики, Житомирский государственный университет имени Ивана Франко, г. Житомир

Аннотация

В статье проанализированы проблемы обеспечения информационной безопасности школьников в общеобразовательном учебном заведении и разработана совокупность мер, необходимых для ее обеспечения. Рассмотрены структурная и функциональная модель обеспечения информационной безопасности старшеклассника в компьютерно ориентированной учебной среде. Выяснены особенности обеспечения он-лайн безопасности старшеклассников и методики преподавания вопросов Интер-

нет безопасности в школьном курсе информатики. Уточнены понятия «обеспечение информационной безопасности старшеклассника», «он-лайн безопасность старшеклассника».

Ключевые слова: он-лайн безопасность старшеклассников, обеспечение информационной безопасности старшеклассника, методика преподавания вопросов Интернет безопасности.

METHODIC OF THE ON-LINE SAFETY OF THE SENIOR PUPILS IN THE TEACHING AND EDUCATIONAL PROCESS AT SCHOOL

Spirin O., Doctor of pedagogical sciences, Chief Researcher, Institute of Information Technologies and Learning Tools of NAPS of Ukraine, Kyiv

Kovalchuk V., assistant of the Department of applied mathematics and informatics, Zhytomyr Ivan Franko State University, Zhytomyr

Resume

The problems of the pupils' information safety at general education establishment are considered in the article. A set of necessary measures keeping up the safety are developed. The structural and functional model of senior pupils information safety is overviewed for the computer oriented environment. There are described in details the peculiarities of the online safety of senior pupils and methodic of Internet safety teaching in the course of Informatics at school. Detail definitions of the concepts «keeping up and enabling the information safety for senior pupils», «on-line safety of senior pupils» are given.

Keywords: on-line safety of senior pupils, keeping up and enabling the information safety for senior pupils, methodic of teaching the Internet safety issues.

Матеріал надійшов до редакції 24.02.2011 р.