

Олександр Савчук

РОЛЬ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА УРОКАХ ІНФОРМАТИКА У ПРОФІЛЬНІЙ ШКОЛІ

Анотація. У цій статті розглядаються основні аспекти інформаційної безпеки учнів профільної школи. Також представлені структурні та функціональні моделі інформаційної безпеки для учня ЗЗСО в комп'ютерному навчальному середовищі. Описані фактори, що впливають на Інтернет-безпеку старшокласників та методичні рекомендації викладання Інтернет-безпеки на шкільному уроці інформатики.

Ключові слова: інформаційна безпека, профільна школа, безпека в Інтернеті.

На сьогодні відбулися значні технологічні досягнення, швидкість інтернету вища, і в майбутньому багато шкіл залишатимуться підключеними до високошвидкісного інтернету. Однак, незважаючи на значний розвиток інформаційно-комунікаційних технологій, використання бездротових інтернет-технологій та мобільних пристроїв у шкільній освіті, все ще існує нерівномірна система доступу до інтернету, складність контролю шкіл, доступу до дітей з раннього віку не отримує належної уваги. Крім того, потенціал онлайн-ресурсів не використовується повною мірою в освіті, а їх використання часто заважає навчальній діяльності [4].

Як показав досвід найрозвиненіших країн світу, наслідком підключення до інтернету є виникнення трьох проблем: захист дітей у відкритому інформаційному середовищі (захист дітей вживу або онлайн), захист персональних даних учнів та персоналу, безпека електронного навчального середовища.

Зазначимо, що під поняттям машинного навчання слід розуміти: «штучну систему, структура та компоненти якої створюють необхідні умови для досягнення цілей та реалізації освітньої програми, і яка охоплює всі її компоненти з використанням інформаційно-комунікаційних технологій (ІКТ)» [1]. Цю проблему можна вирішити лише враховуючи їхню реальну ситуацію та залучаючи уряд, громадянське суспільство, школи та батьків до вирішення всіх питань захисту інформації дітей. У педагогічній науці питання конфіденційності

даних дітей є відносно новим і наразі не отримало широкого вивчення.. У багатьох роботах розглядається роль різних моделей захисту інформації учнів, зокрема: налаштування браузера, встановлення «батьківського контролю», безпекові програми тощо. Хоча автори надали детальні рекомендації для вчителів, батьків та учнів, основна увага приділяється рекомендаціям щодо програмного забезпечення, щоб запобігти доступу дітей до нефільтрованої (дефільтрованої) інформації. Акцент також зміщується на роль освіти та навчання у розвитку здатності дітей раннього віку справлятися із загрозами з боку інформаційного середовища. Кращих результатів можна досягти, поєднуючи програмне забезпечення та технічні засоби з освітніми та навчальними програмами, а також інституційною, законодавчою та політикою захисту даних. Тому ми вважаємо, що забезпечення безпеки повноцінно розвиненого суспільства можливе лише шляхом поєднання законів та нормативних актів, установ, освіти та навчання, програмного забезпечення та інструментів і обладнання. Інформаційна безпека учнів закладів середньої освіти – це набір заходів безпеки, інструментів та методів безпеки, розроблених для досягнення найвищих можливих умов безпеки для осіб у комп'ютерному середовищі освітньої установи. Передумовою забезпечення конфіденційності даних учнів є створення безпечного навчального середовища, що включає комп'ютерні технології. Метою та перевагами має бути конфіденційність захищеної інформації учнів під час навчання [3].

Ознайомившись з науковою літературою та методами, ми дійшли висновку, що система інформаційної безпеки середньої школи може бути моделлю для забезпечення інформаційної безпеки в середніх школах та вищих навчальних закладах, а також для електронних систем інформаційної безпеки у вищих навчальних закладах [2]. Згідно з вищезазначеними моделями, можна розподілити обов'язки між працівниками за впровадження таких необхідних систем, включаючи приклад управління всією системою. Розглянувши питання та теми, пов'язані з інформаційною безпекою в закладах середньої освіти, можна

визначити основних суб'єктів забезпечення безпеки інформації учнів, а саме: сам учень, вчитель інформатики, вчителі, персонал, адміністрація. Завданням вчителя інформатики є забезпечення безпеки комунікаційних мереж, освітніх комп'ютерних систем та учнів від інформаційних загроз та негативного впливу ІКТ. Професійна компетентність вчителя з інформаційної безпеки – це сукупність знань та розумінь, навичок, умінь, а також якостей та цінностей вчителя в галузі інформаційної безпеки та здатність ефективно та належним чином доносити їх для вирішення навчальних проблем та вирішення освітніх завдань у шкільному середовищі. Компетентність вчителя інформатики щодо забезпечення безпеки інформації учнів закладу освіти повинна враховувати необхідність захисту інформації, комп'ютерів та самих учнів від інформаційних загроз та негативного впливу ІКТ.

Виходячи з визначення інформаційної безпеки учнів [7], ми визначаємо інформаційну безпеку старшокласників як частину захисту особи щодо її онлайн-діяльності.

Ці заняття не обмежуються інтелектуальним чи соціальним розвитком дитини, а й фізичним та психічним здоров'ям особистості (комп'ютерна або ігрова залежності, шахрайство, інформаційне перенавантаження, розбещення тощо). Зі зростанням використання соціальних мереж, зокрема чатів, електронної пошти та миттєвих повідомлень, дитина піддається підвищеному ризику стати мішенню зловмисників. Жертвами онлайн-злочинців часто стають люди з вразливих категорій населення, в тому числі й діти. [2].

З педагогічної точки зору необхідно покращити навчання учнів, в ідеалі шляхом впровадження правил або «статуту» щодо правил політики безпеки користування мережею. Основні методи, що використовуються для реалізації заходів безпеки, включають інформування, моніторинг, заохочення, консультування, тимчасове обмеження (відмова в доступі), обмеження прав та привілеїв, наданих особам.

Можна запропонувати наступний перелік методичних рекомендацій.

1. Уроки організовані як лекції для всіх учнів класу, при цьому найкраще додатково відображати інформацію на екрані. Якщо можливо, урок проводиться в невеликій групі (або підгрупі класу) та надсилати матеріали учням з комп'ютера вчителя.

2. Приділяйте більше уваги створенню та моніторингу повідомлень про самозахист дітей в Інтернеті. Слід зазначити, що вербування дітей часто здійснюється на основі інформації, отриманої в Інтернеті, або через контакт дитини з незнайомцем, який потім використовує дитину для спілкування. водночас частка викритих злочинів становить менше 1%.

3. Поясніть учням, що в Інтернеті люди часто представляють себе іншими (наприклад, публікують фотографії інших людей (наприклад, знаменитостей) замість себе), не представляють себе дорослими (наприклад, старші чоловіки видають себе за молодших) та можуть «маскувати» свою особу. Важливо зазначити, що, наприклад, незнайомиць може використати дані знайомої тобі людини. Тому надання особистої інформації незнайомцю в Інтернеті та публікація її в Інтернеті (наприклад, у соціальних мережах) може бути ризикованою. Не слід зустрічатися з незнайомцями з Інтернету без інформування, дозволу чи супроводу батьків.

4. Онлайн-шахрайство покликане заробляти гроші. Від вимагання до шахрайства. Слід зазначити, що використання будь-яких онлайн-сервісів, які вимагають оплати (номери кредитних карток, текстові повідомлення або дзвінки на мобільні телефони), може здійснюватися лише за згодою батьків, оскільки це може призвести до фінансових втрат. Вся сумнівна інформація з Інтернету повинна бути перевірена незалежними джерелами.

5. Навчання в галузі інформаційної безпеки та вибір правильних ключових слів є дуже важливими. Вони наголошують, що дотримання цих правил є обов'язком самих учнів, оскільки це забезпечить їхню безпеку. Паролі важливі, оскільки вони захищають деяку з найчутливіших персональних даних і, як правило, є найслабшою ланкою для їх захисту.

Питання інформаційної безпеки для учнів ЗЗСО є дуже важливим і має свої особливості, які слід враховувати в шкільній програмі. Безпека в Інтернеті повинна розглядатися як частина інформаційної безпеки для старшокласників, а заходи інформаційної безпеки містити у собі зв'язок різних заходів, засобів та методів. Забезпечення безпеки даних для старшокласників у цифрових навчальних середовищах є колективною відповідальністю батьків, вчителів, суспільства та учнів, і ці зусилля повинні координуватися на національному рівні. Вчителі інформатики відіграють важливу роль у розвитку поведінки інформаційної безпеки серед старшокласників.

Список використаних джерел:

1. Бобало Ю. Я. Інформаційна безпека: навч. посібник / Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник, А. П. Бондарєв, С. С. Войтусік, А. Я. Горпенюк, О. А. Немкова, І. М. Журавель, Б. М. Березюк, Є. І. Яковенко, В. І. Отенко, І. Я. Тишик; за заг. ред. д-ра техн. наук, проф. Ю. Я. Бобала та д-ра техн. наук, доц. І. В. Горбатого. Львів : Видавництво Львівської політехніки, 2019. 580 с.
2. Інформатика (рівень стандарту): підруч. для 10-го (11-го) кл. закл. заг. серед. освіти / Й.Я. Ривкінд [та ін.]. Київ : Генеза, 2018. 144 с. : іл.
3. Інформаційна безпека. Підручник / В. В. Остроухов, М. М. Присяжнюк, О. І. Фармагей, М. М. Чеховська та ін.; під ред. В. В. Остроухова К.: Видавництво Ліра-К, 2021. 412 с.
4. Куницький В. Захист неповнолітніх в інформаційному просторі як об'єкт гуманітарної експертизи: український та зарубіжний досвід. Державне управління: теорія та практика. 2011. URL: <http://www.academy.gov.ua/ej/ej14/txts/Kunitskiy.pdf> (дата звернення: 20.05.2025).
5. Морзе Н. В. Основи інформаційно-комунікаційних технологій / Н. В. Морзе. К.: Видавнича група BHV, 2008. 352 с.
6. Про Стратегію інформаційної безпеки : Указ Президента України від 28 грудня 2021 р. URL: <https://zakon.rada.gov.ua/laws/show/685/2021#Text> (дата звернення: 24.05.2025).
7. Спірін О., Ковальчук В. Методика забезпечення онлайн-безпеки старшокласників у навчально-виховному процесі школи. Інформаційні технології і засоби навчання. 2011. № 1 (21). URL: <http://www.journal.iitta.gov.ua> (дата звернення: 24.05.2025).

THE ROLE OF INFORMATION SECURITY IN COMPUTER SCIENCE LESSONS IN A SPECIALIZED SCHOOL

Abstract. *This article examines the main aspects of information security for students of a specialized school. Structural and functional models of information security for a student of a secondary school in a computer learning environment are also presented. Factors affecting the Internet security of high school students and methodological recommendations for teaching Internet security in a school computer science lesson are described.*

Keywords: *information security, specialized school, Internet security.*

Науковий керівник: Олена Косовець, канд. пед. наук, доцент.