

ІНФОРМАЦІЙНА БЕЗПЕКА ЯК СКЛАДНИК ЦИФРОВОЇ КОМПЕТЕНТНОСТІ СУЧАСНОГО ВЧИТЕЛЯ ІНФОРМАТИКИ

Інформаційна безпека відіграє важливу роль в цифровому суспільстві та впливає на різні сфери людської діяльності. Вона стає ключовою складовою для забезпечення захисту конфіденційності, цілісності та доступності цифрової інформації. У сучасну цифрову епоху вчителям інформатики дуже важливо володіти сучасними знаннями з інформаційної безпеки, адже із зростаючою інтеграцією технологій у навчальні заклади вчителі відповідають за захист цифрової інформації учнів і забезпечення безпечного навчального середовища. Зокрема, В. Н. Ковальчук зазначає, що 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 [1].

Вчителі інформатики, які володіють знаннями з інформаційної безпеки мають можливість захистити учнів від основних потенційних онлайн-загроз та різних видів шахрайств, які можуть очікувати їх у цифровому світі. Аналіз навчальних програм з інформатики, що розроблені в межах державного стандарту базової і повної загальної середньої освіти свідчать, що вчителі, зокрема, можуть навчати учнів правилам безпечного використання інтернету, правилам безпечного користування електронною скринькою, основним ознакам спаму й фішингу, а також основним діям для захисту персональних комп'ютерів від шкідливого програмного забезпечення. Навчаючи цим основним навичкам, вчителі допомагають учням безпечно орієнтуватися в цифровому середовищі.

Інформатика є інструментарієм, за допомогою якої дитина зможе отримувати із різних джерел необхідну інформацію для розв'язання своїх завдань. Вивчення шкільного курсу інформатики є базовим для предметного застосування ІКТ і відіграє виключну роль у формуванні однієї із ключових компетентностей сучасного школяра – цифрової [2, с 141].

Також ці знання дозволяють вчителям інформатики захищати конфіденційні дані учнів. Враховуючи теперішню ситуацію, не у всіх дітей завжди є можливість для безпечного відвідування шкіл, і тому для виконання завдань, проведення занять та спілкування вчителі покладаються на цифрові платформи, і для цього вони повинні розуміти правила забезпечення конфіденційності даних і найкращі практики їх захисту.

Інформаційна безпека для сучасних вчителів інформатики буде завжди актуальною в цифровому оточенні з численними технологічними можливостями. Вона не тільки забезпечує захист вчителів як фахівців від потенційних загроз, а й впливає на якість освіти та формування цифрових навичок учнів. К.С. Варивода зазначає “інформаційна безпека безпосередньо залежить від рівня і якості освіченості молодого покоління, ступеня зрілості особистості й готовності її до самореалізації в суспільстві. Саме тому виникає гостра необхідність розширення змісту загальної середньої освіти,

використання нових компонентів таких як хмарні обчислення, великі дані, штучний інтелект, технології доповненої реальності [4], що пов'язані із навчанням підлітків інформаційної безпеки”.

Важлива роль сучасного учителя інформатики полягає в тому, щоб навчити учнів етичному використанню технологій та формуванню критичного підходу до цифрового світу, роблячи інформаційну безпеку не лише стандартом, але і цінністю, яку вчителі передають своїм учням.

Список використаних джерел

1. Ковальчук В. Н. Забезпечення інформаційної безпеки старшокласників у комп'ютерно-орієнтованому навчальному середовищі: дис. ... канд. пед. наук: 13.00.10 / Ковальчук Вікторія Наумівна. – Житомир, 2011. – 291 с.
2. Мойко О. С. Особливості формування професійної компетентності майбутніх учителів інформатики засобами інформаційно-комунікаційних технологій. Молодь і ринок. Дрогобич, 2018. No 5 (160). С. 139–144.
3. Варивода К. С. Інформаційна безпека підлітків в інтернет мережі. Молодий вчений. 2016. No 3 (30) С. 365–368.
4. Oleksiuk V., Oleksiuk O. The practice of developing the academic cloud using the Proxmox VE platform. Educational Technology Quarterly. 2022. URL: <https://doi.org/10.55056/etq.36> (date of access: 04.02.2024).