практичної значущості фізики, хімії чи біології безпосередньо у своєму фаху є найсильнішим мотиватором до навчання.

Природничо-наукова картина світу, сформована через призму професії, дозволяє майбутньому спеціалісту бачити не лише вузькопрофесійні алгоритми, а й глибинні першопричини процесів (від квантової механіки в ІТ до термодинаміки в енергетиці чи біохімії в агросекторі). Це забезпечує безпеку, екологічність та інноваційність його майбутньої діяльності.

Успішна реалізація цього підходу вимагає системного оновлення навчально-методичного забезпечення. Подальші дослідження мають бути спрямовані на розробку спеціалізованих міждисциплінарних комплексів, задачників та інтегрованих курсів, які б враховували специфіку кожної окремої спеціальності у закладах фахової передвищої освіти.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Мохун М.С., Калаур С.М. Історико-педагогічний аналіз становлення поняття «природничо-наукова картина світу» та його сучасні інтерпретації в контексті STEM-освіти. *Сучасні інформаційні технології та інноваційні методики навчання: досвід, тенденції, перспективи*: матеріали XVI міжнар. наук.-практ. інтернет-конф., м. Тернопіль, 6-7 листопада 2025 р. С. 296-299.
2. Формування природничо-наукової компетентності старшокласників у процесі навчання фізики : методичний посібник / Л. В. Непорожня. – К. : ТОВ «КОНВІ ПРІНТ», 2018. –204 с.

**МУЛЛАКАЄВ Роман**
*учитель інформатики Хустської СШ І-ІІІ ступенів №1 імені А.Волошина,*
*студент І курсу магістратури*
*спеціальності «Технології та інформатика»*
*Хмельницького національного університету*

## КІБЕРБЕЗПЕКА В СУЧАСНОМУ ОСВІТНЬОМУ СЕРЕДОВИЩІ: ВИКЛИКИ, РИЗИКИ ТА ІННОВАЦІЙНІ ШЛЯХИ ЇХ ПОДОЛАННЯ

У тезах досліджено проблематику кібербезпеки в сучасному освітньому середовищі в умовах активної цифровізації. Проаналізовано основні загрози, ризики та вразливості освітніх систем, визначено рівень готовності учасників освітнього процесу до протидії кіберзагрозам. Розглянуто сучасні програмні рішення та інструменти, що застосовуються для забезпечення інформаційної безпеки. Запропоновано комплексний підхід до формування безпечного цифрового освітнього середовища.

Цифрова трансформація освіти стала невід’ємною складовою сучасного суспільства. Використання дистанційного навчання, електронних журналів,

освітніх платформ, відеоконференцій та хмарних сервісів значно розширило можливості доступу до знань. Водночас це призвело до зростання кіберризиків, які можуть негативно впливати на стабільність освітнього процесу.

Особливої актуальності проблема кібербезпеки набуває в умовах глобальних викликів, зокрема воєнного стану та масового переходу на онлайн-навчання. Освітні установи стають об'єктами кібернападів, що потребує системного підходу до захисту інформаційних ресурсів.

1. Проблематика кібербезпеки в освітньому середовищі. Освітній сектор є одним із найбільш уразливих до кіберзагроз через:

- велику кількість користувачів (учні, студенти, педагоги);
- використання особистих пристроїв (BYOD – Bring Your Own Device);
- недостатній рівень технічного захисту;
- низьку обізнаність користувачів щодо кіберзагроз.

До основних проблем належать:

- відсутність централізованих політик кібербезпеки;
- використання слабких паролів;
- відсутність двофакторної аутентифікації;
- неконтрольований доступ до навчальних ресурсів;
- недостатній рівень фінансування кіберзахисту.

2. Основні кіберзагрози та ризики. Серед найпоширеніших загроз у сфері освіти можна виділити:

- Фішинг – отримання доступу до облікових записів через підроблені листи або сайти.
- Шкідливе програмне забезпечення – віруси, трояни, ransomware, що блокують або знищують дані.
- Витік персональних даних – несанкціоноване поширення інформації про учнів і викладачів.
- Кібербулінг – психологічний тиск у цифровому середовищі.
- DDoS-атаки – перевантаження серверів освітніх платформ.

Ризики включають:

- порушення конфіденційності;
- втрату даних;
- переривання навчального процесу;
- фінансові збитки;
- зниження довіри до освітніх установ.

3. Рівень цифрової грамотності як фактор безпеки. Однією з ключових причин вразливості є недостатній рівень цифрової грамотності. Більшість користувачів:

- не розпізнають фішингові повідомлення;
- використовують однакові паролі;
- нехтують оновленнями програмного забезпечення;
- не знають базових правил кібергігієни.

Тому формування цифрової компетентності є критично важливим елементом забезпечення кібербезпеки.

4. Сучасні програмні рішення у сфері кібербезпеки освіти. У сучасному освітньому середовищі широко використовуються такі інструменти:

1. Антивірусні програми (Microsoft Defender, Avast, ESET).

2. Платформи для безпечного навчання (Google Workspace for Education, Microsoft 365 Education ).

3. Системи управління доступом (двофакторна аутентифікація, Single Sign-On).

4. Засоби захисту мережі (VPN-сервіси, міжмережеві екрани)

5. Інструменти моніторингу (системи виявлення вторгнень (IDS/IPS), журнали аудиту доступу).

6. Освітні ресурси з кібербезпеки (онлайн-курси, тренінгові платформи, симулятори кіберзагроз)

5. Шляхи вирішення проблем кібербезпеки. Для ефективного забезпечення кібербезпеки необхідно впроваджувати комплекс заходів:

Організаційні:

- розробка політик інформаційної безпеки;
- регулярне навчання персоналу;
- контроль доступу до даних.

Технічні:

- використання сучасних систем захисту;
- регулярне оновлення програмного забезпечення;
- резервне копіювання даних.

Освітні:

- інтеграція курсів кібербезпеки в навчальні програми;
- підвищення цифрової грамотності;
- проведення інформаційних кампаній.

Державні:

- нормативне регулювання;
- фінансова підтримка освітніх установ;
- створення національних стратегій кібербезпеки.

Кібербезпека є ключовим елементом сучасного освітнього середовища. В умовах цифровізації освіти зростає кількість загроз, що вимагає системного підходу до їх подолання. Ефективне поєднання технічних, організаційних та освітніх заходів дозволяє створити безпечне освітнє середовище та забезпечити захист усіх учасників освітнього процесу.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Закон України «Про основні засади забезпечення кібербезпеки України». – Київ, 2017.

2. Концепція розвитку цифрової економіки та суспільства України. – Київ, 2018.

3. Коваленко В. В. Інформаційна безпека в освіті. – Київ, 2020. – 256 с.

4. Петренко О. С. Кібербезпека в освіті // Освітні технології. – 2021. – №3. – С. 45–52.

5. ENISA. Cybersecurity in Education. – 2022.