



МЕТОДИЧНИЙ ПОСІБНИК ДО ОНЛАЙН-КУРСУ

# ОСНОВИ КІБЕРБЕЗПЕКИ ДЛЯ ШКОЛЯРІВ

ДЛЯ 5-6 КЛАСІВ

2023



## **Методичні посібники розробила громадська організація “Смарт освіта”**

Курс “Основи кібербезпеки для школярів” розроблений CRDF Global в Україні в співпраці з ГО “Смарт Освіта” та технічними експертами компанії Technomatix за підтримки Державного департаменту США (Офіс із координації допомоги Європі та Євразії).

Мета курсу – зміцнення рівня обізнаності та підвищення загального рівня знань у сфері кіберзахисту здобувачів освіти, їхніх батьків та вчителів.

Курс розміщений на платформі за посиланням: [cyberkidsukraine.org](https://cyberkidsukraine.org)

Для його проходження / використання матеріалів необхідно зареєструватися. З огляду на вікові особливості школярів, матеріали курсу адаптовані для учнів 1-2 класів, 3-4 класів, 5-6 класів, 7-9 класів, 10-11 класів.

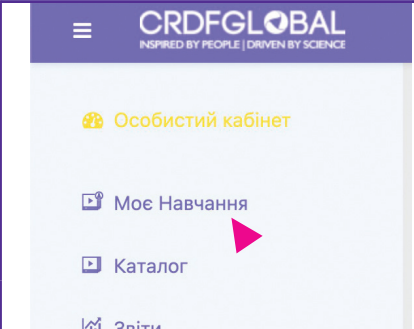
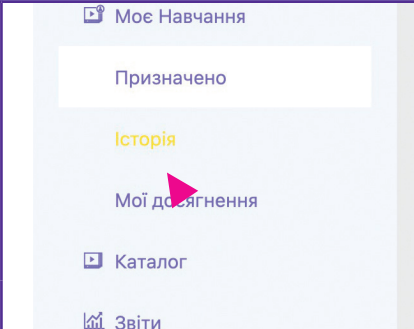
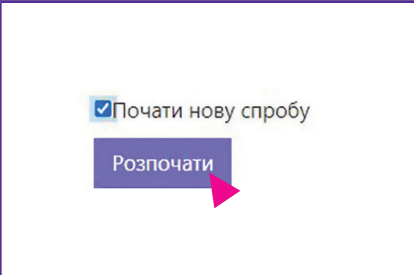
**ДЛЯ УЧНІВ 5-6 КЛАСІВ КУРС СКЛАДАЄТЬСЯ З ДЕВ'ЯТИ МОДУЛІВ,  
КОЖЕН ІЗ ЯКИХ МІСТИТЬ НАВЧАЛЬНУ ІНФОРМАЦІЮ ТА ТЕМАТИЧНІ ВПРАВИ  
ДЛЯ ПЕРЕВІРКИ ОТРИМАНИХ ЗНАНЬ**

<b>Модуль 1. Електронна пошта й шахрайство</b> <ul style="list-style-type: none"> <li>• Як захистити свою електронну пошту від злодійського шкідництва.</li> <li>• Яку суперсилу використати, щоб згенерувати надійний пароль.</li> <li>• Чому важливо зважати на те, хто, як, і що написав у вхідному листі.</li> </ul>	<b>Модуль 2. SMS-шахрайство</b> <ul style="list-style-type: none"> <li>• Чому SMS-ка про виграш може коштувати тобі кишенькових грошей.</li> <li>• Скільки вартує відповідь на повідомлення про унікальну акцію.</li> <li>• Які прийоми використовують кібершахраї, щоб виманити твої кошти.</li> </ul>
<b>Модуль 3. Цифрові сліди</b> <ul style="list-style-type: none"> <li>• Що таке цифрові сліди та як ти можеш їх залишити.</li> <li>• Яка інформація про тебе – справжня знахідка для шахрая.</li> <li>• Чому не варто розголошувати свій номер телефону.</li> </ul>	<b>Модуль 4. Пароль точно захищає?</b> <ul style="list-style-type: none"> <li>• Чому твій пароль маєш знати лише ти та твої батьки.</li> <li>• Які слова та цифри не варто використовувати в паролі.</li> <li>• Чи можливо вигадати пароль, який ніхто не вгадає.</li> </ul>
<b>Модуль 5. Онлайн-ігри та офлайн проблеми</b> <ul style="list-style-type: none"> <li>• Якими неприємностями може обернутися купівля гри на підозрілому сайті.</li> <li>• Чому не потрібно передавати будь-які свої дані чи дані батьків незнайомцям.</li> <li>• Скільки насправді може коштувати безплатна гра.</li> </ul>	<b>Модуль 6. Перевіряємо безпеку комп'ютера</b> <ul style="list-style-type: none"> <li>• Як ти можеш захистити свій комп від вірусів.</li> <li>• Навіщо для того, щоби безпечно скачувати прикольні відоси з котиками, потрібно оновлювати антивірус.</li> <li>• Чому безплатний антивірус може принести лише зайві хвороби твоєму гаджету.</li> </ul>
<b>Модуль 7. “Ми просто спілкуємося в інтернеті”</b> <ul style="list-style-type: none"> <li>• У яких чатиках сидіти безпечно, а запрошення до яких відразу варто блокувати.</li> <li>• Чому важливо ставитися дружелюбно до творчості інших в онлайні.</li> <li>• Чому пропозиції від незнайомих треба ігнорувати та швиденько розповідати про це батькам.</li> </ul>	<b>Модуль 8. “У новинах про це написали”: фейки і як їх розпізнати</b> <ul style="list-style-type: none"> <li>• Чому звідусіль так часто лунає “фейк” – що воно таке.</li> <li>• Які причини популярності неправдивих новин.</li> <li>• Кому вигідно поширювати брехню.</li> </ul>
<b>Модуль 9. Я вмію захищати інформацію</b> <ul style="list-style-type: none"> <li>• Анкетне опитування на завершення програми навчання.</li> </ul>	

Зареєстровані користувачі платформи матимуть доступ до кожного навчального модуля. У такий спосіб, учні та їхні батьки можуть проходити курс самостійно, а вчитель матиме можливість використовувати анімовані ролики та інтерактивні завдання під час навчання.

Після успішного проходження тесту, кожен користувач отримає сертифікат про те, що він опанував навчальний онлайн-курс «Базові правила інформаційної безпеки».

**ПРИМІТКА.** Якщо ви вже завершили курс для 5-6 класів, але хочете повернутися до якоїсь частини (наприклад, на уроках чи класних годинах), виконайте наступні дії.

1. Після входу в систему, оберіть меню «Моє навчання» (зліва на панелі навігації сайту).	2. Відкрийте меню «Історія», у якому знайдете завершені курси.	3. Відкрийте курс, наприклад, за 1-2 клас, оберіть потрібний модуль і зробіть позначку в клітинці.
		
4. Натисніть «Розпочати».		

## ВЧИТЕЛЮ ІНФОРМАТИКИ

### ПРИКЛАД ВИКОРИСТАННЯ КУРСУ НА УРОКАХ

Запропоновані матеріали розроблені на основі діяльнісного, особистісно орієнтованого та компетентнісного підходів. Враховані такі змістові лінії: «інформація», «дані», «цифрові пристрої», «безпека та відповідальність».

### Формування компетентностей

<b>Спілкування державною мовою</b>
<ul style="list-style-type: none"> <li>• вміння доступно й переконливо висловлювати думки;</li> <li>• висловлюватися і дискутувати на тему сучасних цифрових технологій із використанням відповідної термінології;</li> <li>• презентувати українською мовою власну чи групову діяльність, зокрема, з використанням цифрових технологій.</li> </ul>
<b>Інформаційно-комунікаційна компетентність</b>
<ul style="list-style-type: none"> <li>• розв'язувати проблеми з використанням цифрових пристроїв, інформаційно-комунікаційних технологій для власного й суспільного розвитку та добробуту;</li> <li>• дотримання правил безпеки в мережах та мережевого етикету.</li> </ul>
<b>Підприємливість та фінансова грамотність</b>
<ul style="list-style-type: none"> <li>• оцінювати й враховувати власні сильні та слабкі сторони в груповій та особистій діяльності;</li> <li>• використовувати досвід діяльності в інтернеті для вибору життєвих стратегій;</li> <li>• вміння визначати всі можливі варіанти причин виникнення проблем та їх розв'язання (які пов'язані з використанням мережі Інтернет).</li> </ul>
<b>Громадянські та соціальні компетентності</b>
<ul style="list-style-type: none"> <li>• співпрацювати й комунікувати з іншими особами для досягнення навчальних цілей;</li> <li>• дотримуватися принципів цифрового громадянства.</li> </ul>
<b>Навчання впродовж життя</b>
<ul style="list-style-type: none"> <li>• використовувати різноманітні підходи й форми навчання, можливості сучасних навчальних середовищ (зокрема, онлайн-середовищ) для побудови власної траєкторії розвитку.</li> </ul>

## ТЕМА: Я ВМІЮ ЗАХИЩАТИ ІНФОРМАЦІЮ

<b>Мета:</b>
<ul style="list-style-type: none"> <li>• навчити учнів розпізнавати основні помилки під час користування ресурсами, пристроями і програмами, аналізувати рівень безпеки в різних ситуаціях;</li> <li>• формувати в школярів культуру інформаційної безпеки для зменшення можливих негативних наслідків.</li> </ul>
<b>Завдання:</b>
<ul style="list-style-type: none"> <li>• розвивати навички аналізу інформації;</li> <li>• розвивати вміння аналізу помилкової поведінки в цифровому світі, що може призвести до негативних наслідків;</li> <li>• розвивати в учнів навички роботи в групах.</li> </ul>
<b>Необхідне обладнання:</b>
<ul style="list-style-type: none"> <li>• телевізор / проектор і екран (для роботи офлайн);</li> <li>• комп'ютери / смартфони / планшети з доступом до інтернету в дітей;</li> <li>• цифрова дошка Jamboard.</li> </ul>

### РЕКОМЕНДАЦІЇ ДЛЯ ПРОВЕДЕННЯ ТЕМАТИЧНОГО УРОКУ З ОСНОВ КІБЕРБЕЗПЕКИ У 5-6 КЛАСАХ

За тиждень до уроку сформуєте вісім груп учнів (по 2-4 дітей), які отримають випереджальне завдання (див. додаток 1) самостійно ознайомитися з матеріалами одного з модулів курсу «Основи кібербезпеки» (номер групи = номер модуля). На цифровій дошці Jamboard учні мають знайти сторінку, на якій буде вказано пройдений модуль. За допомогою нотаток діти «розкажуть» про що дізнались.

Завдання може бути розміщено на Google Диску (чи іншому сервісі хмарного зберігання) з наданням учням доступу до нього.

Також вчитель має підготувати цифрову дошку Jamboard, на якій кожна група матиме свою сторінку для роботи.

#### ПРИКЛАД

Модуль 1. Електронна пошта і шахрайство		
Ситуації, які розглядали:	Ситуація / ситуації, яка / які є найбільш небезпечна / небезпечні, на вашу думку:	Пояснення, чому ситуація / ситуації є найнебезпечнішою / найнебезпечнішими

#### РОЛЬ ВЧИТЕЛЯ / ВЧИТЕЛЬКИ

Вчитель / вчителька консультує, за потреби надає допомогу у виконанні завдань, забезпечує морально-психологічний комфорт у групах.

На уроці вчитель / вчителька організовує презентацію роботи групами, обговорення отриманої інформації, обмін враженнями від роботи та курсу.

**Тривалість уроку:** офлайн – 45 хв, дистанційне навчання – відповідно до санітарних норм.

## ХІД УРОКУ

### I. Організаційний момент (до 1 хв)

### II. Актуалізація опорних знань (до 2 хв)

Запропонуйте дітям відгадати загадку<sup>1</sup>

*Він про все на світі знає, часто час в нас забирає.  
Ми не можемо уявити, як тепер без нього жити.  
(Інтернет)*

Запитайте, чи погоджуються вони з автором щодо змісту загадки. Свою думку діти мають пояснити.

### III. Мотивація освітньої діяльності (до 2 хв)

1. Запитайте в дітей

*Чи можна нашкодити собі та іншим людям, якщо не дотримуватися правил безпеки користування інтернетом?*

2. Вислухайте відповіді.

3. Скажіть, що знання і навички, які учні отримали під час проходження модулів курсу «Основи кібербезпеки для школярів», готуючись до уроку, та здобуті на самому уроці, допоможуть убезпечити себе й інших небайдужих їм людей від багатьох проблем.

### IV. Визначення мети уроку (1-2 хв)

1. Запропонуйте учням визначити освітню мету уроку.
2. Узагальніть їхні відповіді.

### V. Учні презентують результати своєї роботи

**ПРИМІТКА.** Вчитель визначає скільки модулів курсу буде розглянуто на уроці (залежно від того, як проходитиме урок (онлайн чи офлайн), наявності часу тощо). Щоб визначити групи, які презентують свою роботу, можна витягти "секретні записки" з номером, кидати кубик, використати [random.org](https://www.random.org) тощо.

#### АЛГОРИТМ РОБОТИ

1. Групи презентують свою роботу, користуючись власними нотатками на дошці Jamboard. Однокласники можуть ставити їм запитання.
2. Учні з кожної групи мають відповісти на запитання «Що ми знали із цієї теми до проходження модуля курсу?» та «Що дізналися нового за темою модуля?»
3. За наявності часу, вчитель може відкрити 9 модуль і запропонувати учням обговорити кожну ситуацію.
4. Діти всі разом обиратимуть правильний варіант відповіді.

## VI. Завершальна частина (5 хв)

1. Запропонуйте дітям вигадати газетний заголовок до статті, яка могла б бути написана про проведений урок. Діти мають спробувати передати в заголовку основну ідею / мету уроку.

2. Рефлексія.

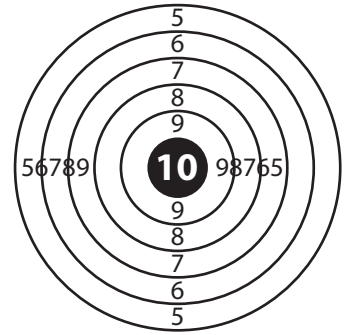
Запропонуйте дітям поділитися враженнями від уроку. Виведіть на екран зображення мішені для стрільби.

Запропонуйте учням визначити на скільки «влучно»:

- Урок був корисним?
- Чи здобуті знання та вміння знадобляться в подальшому житті?
- Чи потрібно передати ці знання батькам, друзям, іншим людям?

**ПРИМІТКА.** Під час дистанційного уроку учні можуть ставити мітки на мішені, відповідаючи на запитання.

3. Учитель акцентує на тому, що кожен тепер може пройти самостійно весь курс та отримати корисні знання і сертифікат.



Джерело: <https://ibis.net.ua/ua/products/details/mishen-dlya-pnevmatich-eskogo-oruzhya-5-10/>

## Самооцінювання

1. Кожен учень за допомогою таблиці (див. додаток 2) може оцінити свої знання та вміння з кібербезпеки.

## ДОДАТОК 1 ОСНОВИ КІБЕРБЕЗПЕКИ ДЛЯ УЧНІВ 5-6 КЛАСІВ

### Завдання групам

1. Запропонуйте батькам разом із вами зареєструватися на курс із кібербезпеки за посиланням.
2. Ознайомтеся з інформацією про цей курс.
3. Відкрийте курс за 5-6 клас, оберіть потрібний модуль, прослухайте інформацію, перегляньте анімаційні ролики та виконайте завдання.
4. На цифровій дошці Jamboard знайдіть сторінку, на якій вказано пройдений вами модуль курсу.
5. За допомогою нотаток «розкажіть» про що дізнались.



### ПРИКЛАД

### Модуль 1. Електронна пошта і шахрайство

Ситуації, які розглядали:	Ситуація / ситуації, яка / які є найбільш небезпечна / небезпечні, на вашу думку:	Пояснення, чому ситуація / ситуації є найнебезпечнішою / найнебезпечнішими
<div style="background-color: #f9a825; padding: 5px; margin-bottom: 5px; text-align: center;">«Творче завдання»</div> <div style="background-color: #ffff00; padding: 5px; margin-bottom: 5px; text-align: center;">«Пошук мінусовки»</div> <div style="background-color: #90ee90; padding: 5px; text-align: center;">«Підготовка до контрольної»</div>	<div style="background-color: #00bfff; padding: 20px; margin: 0 auto; width: 80%;">Найбільш небезпечна ситуація...</div>	<div style="background-color: #ff69b4; padding: 20px; margin: 0 auto; width: 80%;">Тому, що...</div>

6. Визначте, хто з вас презентує результати роботи на уроці.



## ДОДАТОК 2

### ТАБЛИЦЯ САМООЦІНЮВАННЯ

#### Завдання групам

Критерії для самооцінювання	Шкала для самооцінювання			
	Легко навчу інших	Трішки підготуюсь, щоб навчати інших	Я маю ще ґрунтовно підготуватися, щоб навчати інших	Маю сумніви у своїх знаннях і вміннях
Я знаю, які пастки й ризики існують в Інтернеті.				
Я вмію використовувати пошукові системи та спілкуватися так, щоби почуватися в безпеці в глобальній мережі.				
Я критично оцінюю всю інформацію, яка трапляється мені в інтернеті.				
Я аналізую рівень безпеки в різних ситуаціях. Легко виявляю пастки й ризики в інтернеті, які загрожують моїй безпеці.				
Я створюю цікавий і безпечний контент та поширюю його.				

## ДЖЕРЕЛА:

### Модуль 4. Пароль точно захищає?

1. Лінг [Електронний ресурс] // Веселі вірші – Режим доступу до ресурсу: <http://deti.e-papa.com.ua/virshi-dlya-ditei/veseli-virshi/>

### Модуль 7. Ми просто спілкуємось в інтернеті

2. Гончарова К. Чому не варто вірити «психологічним тестам» в інтернеті [Електронний ресурс] // Media Sapiens – 26.02.2020. - Режим доступу до ресурсу: <https://ms.detector.media/kiberbezpeka/post/24259/2020-02-26-chomu-ne-varto-viryty-psykhologichnym-testam-v-interneti/>
3. Про дітей та вікові обмеження у соціальних мережах: що є дійсно важливим [Електронний ресурс] // GRIDINSOFT – 14.12.2020. – Режим доступу до ресурсу: <https://gridinsoft.ua/blogs/vikovi-obmezhennya-u-sotsialnyh-merezhah/>

### Модуль 8. В новинах про це написали: фейки і як їх розпізнати

4. Брошнівська О. Брехня — нова правда. Що таке дипфейки та як їх розпізнати? [Електронний ресурс] // VECTOR – 02.11.2020. Режим доступу до ресурсу: <https://vctr.media/yak-rozpiznavatu-dipfeyki-50266/>
5. Діпфейк та дезінформація : практич. посіб. / Агнешка М. Вальорска ; пер. з нім. В. Олійника – К. : Академія української преси ; Центр Вільної Преси, 2020. – 36 с. – Режим доступу до ресурсу: [https://www.aup.com.ua/uploads/DEEPPFAKES\\_FNF\\_AUP\\_2020.pdf](https://www.aup.com.ua/uploads/DEEPPFAKES_FNF_AUP_2020.pdf)
6. Кіца М.О. Фейкова інформація в українських соціальних медіа: поняття, види, вплив на аудиторію [Електронний ресурс] // Соціальні комунікації / SOCIAL COMMUNICATIONS — Режим доступу до ресурсу: <https://bit.ly/3v3yvJE>
7. Найпоширеніші фейки про вакцинацію [Електронний ресурс] // МОЗ України – Режим доступу до ресурсу: <https://moz.gov.ua/najposhirenishi-fejki-pro-vakcinaciju>
8. Підручник: Т. В. Бакка Громадянська освіта (інтегрований курс, рівень стандарту): підруч. для 10 кл. закл. загал. серед. освіти / Т.В. Бакка, Л.В. Марголіна, Т.В. Мелешенко. — Київ : Вид-во «Оріон», 2018.
9. Савоскіна К. Хвилі фейків про коронавірус: чому виникають та як з ними боротися [Електронний ресурс] // hromadske – 07.08.2020. – Режим доступу до ресурсу: <https://hromadske.ua/posts/hvili-fejkiv-pro-koronavirus-chomu-vinikayut-ta-yak-z-nimi-borotися>
10. У лісі-лісі темному, де ходить хитрий вірус [Електронний ресурс] // КУНШТ - Режим доступу до ресурсу: <https://kunsht.com.ua/u-lisi-lisi-temnomu-bozhevilni-mifi-pro-koronavirus/>
11. У Парижі 132 роки тому відкрили збільшену копію хмельницької Ейфелевої вежі [Електронний ресурс] // UaReview – 05.06.2021. – Режим доступу до ресурсу: <https://uareview.com/eiffel-tower-khmelnitskyi/>

## ДЖЕРЕЛА ЗОБРАЖЕНЬ:

1. Антисуффражистська карикатура [Зображення] [Електронний ресурс] // ПЛОМІНЬ – Режим доступу до ресурсу: <https://plomin.club/suffragism/>
2. Ейфелева вежа [Зображення] [Електронний ресурс] // UaReview – Режим доступу до ресурсу: <https://uareview.com/eiffel-tower-khmelnitskyi/>

