# Оцінка рівня зрілості кіберосвіти: стан в Україні

**Аналітичне дослідження**

**травень 2025**

# ВДЯЧНІСТЬ

Громадська організація “Центр аналізу та розробки ефективних політик” висловлює щиру вдячність Європейському агентству з кібербезпеки (ENISA), зокрема експертам Evangelos Kantas, Dimitra Liveri, Christina Skouloudi та Aikaterini Christaki, за цінну підтримку, надану методологію дослідження та професійні рекомендації щодо її ефективного застосування. Завдяки вашому сприянню наше дослідження стало більш ґрунтовним та якісним.

# АВТОРИ ДОСЛІДЖЕННЯ

Світлана Дубова, Голова Правління ГО ЦАРЕП
Оксана Матвієнко, експерт ГО ЦАРЕП
Наталія Парченко, експерт ГО ЦАРЕП

Оцінка рівня зрілості кіберосвіти: стан в Україні : аналіт. дослідження / [Дубова С.В., Матвієнко О.В., Парченко Н.В.]. – Київ : ЦАРЕП, 2025. – 32 с.

# ЗМІСТ

# ВСТУПНЕ СЛОВО

Поряд із зростанням використання цифрових технологій протягом останніх десятиліть, проблематика кібербезпеки привертає дедалі більшу увагу через зростання ризиків, пов'язаних із крадіжкою та пошкодженням особистих і корпоративних даних. Попри значну роль експертів у сфері кібербезпеки для захисту критичної інформації та інфраструктури, їхньої кількості недостатньо, аби забезпечити належний захист для всіх користувачів інтернету. Тому одним із ключових шляхів розв'язання цієї проблеми стає підвищення рівня знань про кібербезпеку серед широких верств населення, охоплюючи всі вікові групи, зокрема молоде покоління.

Особливу увагу важливо приділити школярам, які вже з раннього віку активно взаємодіють із цифровим простором і є критично важливою цільовою групою для формування навичок безпечної поведінки в інтернеті. На рівні держави саме інтеграція тематики кібербезпеки в шкільні навчальні програми та освітні заходи здатна суттєво підвищити рівень цифрової обізнаності молоді. Це, своєю чергою, може сприяти їхній зацікавленості в професійному виборі сфери кібербезпеки, що в перспективі допоможе розв'язати проблему кадрового дефіциту на ринку праці в цій галузі.

Рівень зрілості систем освіти з питань кібербезпеки суттєво відрізняється між країнами. Агенція ЄС з питань кібербезпеки (ENISA) вже здійснила дослідження рівня зрілості освітніх систем країн Європейського Союзу, визначивши ключові виклики, з якими стикаються держави-члени, а також виокремила найкращі практики впровадження кібербезпекової освіти. Оскільки Україна активно рухається шляхом європейської інтеграції, вона має запозичувати передовий європейський досвід, водночас чітко розуміючи власні виклики та потреби в галузі кібербезпекової освіти.

Це дослідження, проведене за методологією ENISA, є першою спробою комплексної оцінки рівня зрілості української шкільної системи освіти в сфері кібербезпеки, що дозволяє визначити сильні сторони та проблемні аспекти національної освітньої системи, а також окреслити шляхи її подальшого вдосконалення.

*Голова Правління*
*Світлана Дубова*

# МЕТОДОЛОГІЯ

Це дослідження стало можливим завдяки люб'язно наданій ENISA методології, що була використана ними для підготовки дослідження "Cybersecurity Education Maturity Assessment"[1]. Методологія складається з 25 питань, 18 з яких підлягають кількісній оцінці, а ще 7 спрямовані на виявлення якісних характеристик розвитку системи початкової та середньої освіти. Питання зосереджені в 3-х макроблоках: Урядування (Governmental), Стратегія (Strategic) та Операційні заходи (Operational).

Урядування містить такі підблоки:

- Регуляторна база (Regulatory framework) – оцінка наявної в країні регуляторної бази, яка визначає обов'язковість кібербезпекової освіти та визначення обсягів її викладання.
- Політики (Policies) – оцінка наявності чи відсутності спеціальної політики, розробленої щодо освіти з кібербезпеки в початковій та середній школі.
- Підтримка (Support) – наявність будь-яких національних програм, які підтримують кібербезпекову освіту, а також розроблених рекомендацій/настанов для підтримки цієї освіти.

Стратегія визначає

- Національну стратегію (National Strategies) – визначення того, чи є питання кібербезпекової освіти на рівні шкіл частиною національної стратегії кібербезпеки.
- План дій (Action Plan) – чи існують національні освітні стратегії / їх плани дій, що підтримують впровадження кібербезпекової освіти в школах.
- Співпрацю (Cooperation) – чи налагоджено міждержавну, національну чи регіональну співпрацю в питаннях, пов'язаних з кібербезпековою освітою.

Операційні заходи мають визначити

- Забезпечення навчання (Provision of education) - фактичне введення кібербезпекового компонента в програми навчання початкової та середньої школи.
- Наявність механізму оцінювання (Implementation evaluation mechanism) – чи існують інструменти моніторингу успішності навчання та контролю його якості.

Базова модель дослідження ENISA передбачає проведення глибинних інтерв'ю з експертами та подальший аналіз отриманих результатів. У межах цього дослідження ця методологія була адаптована шляхом перетворення опитувальника для інтерв'ю на сукупність питань, які були офіційно спрямовані до державних органів (МОН), що

відповідають за реалізацію політики у сфері освіти. Тому, дослідження відбувалось у декілька етапів:

- Кабінетне дослідження під час вивчення нормативних та стратегічних документів, що регулюють процес навчання для початкової та середньої освіти, а також ключові стратегічні напрямки кібербезпеки, закріплені на рівні національних стратегічних документів. Також цей етап дослідження охопив аналіз публічно доступних даних про заходи кіберосвіти, що здійснювались різними стейкхолдерами й відповідали цілям дослідження.
- Аналіз результатів запитів, надісланих до урядових структур, що опікуються питаннями початкової та середньої освіти.

Базова методологія не вказує, як саме має трактуватись поняття "кібербезпекова освіта" і які питання охоплювати. Ми врахували те, що "кібербезпекова освіта" охоплює:

- кібергігієну (як мінімально необхідні базові знання та навички для персонального захисту від кіберзагроз);
- навички, пов'язані з кібербезпекою (наприклад, збереження та відновлення даних чи робота з хмарними системами);
- поглиблені знання, які безпосередньо пов'язані з темою кібербезпеки: криптографія та шифрування, розуміння кіберзагроз та ландшафту загроз, захист комп'ютерних систем та керування інструментами захисту, робота VPN тощо.

Водночас варто підкреслити, що для подальшого практичного застосування терміну "кібербезпекова освіта" (cybersecurity education) доцільно додатково визначити його зміст.

Базова методологія пропонує такий поділ рівнів зрілості кібербезпекової освіти:

| Рівень зрілості | Показник | Коментар |
|---|---|---|
| Не існує | 0 - 20% | Держава все ще не визначилась щодо своєї політики стосовно освіти з кібербезпеки. Відсутні політичні чи стратегічні межі, стратегії (кібербезпекові чи освітні) не порушують тему кібербезпекової освіти, не існує планів дій чи дорожніх карт у цій сфері. У школах ця тема не впроваджується, а освіта з кібербезпеки недоступна в початкових або середніх класах. |
| Початковий/Епізодичний | 20 - 40% | Держава не має чітко визначеного підходу до кібербезпекової освіти в початковій та середній освіті. Однак у державі можуть бути певні загальні цілі щодо такої освіти та впроваджуються окремі заходи з кібербезпекової освіти. Існують окремі програми для досягнення цієї мети, імплементуються деякі вимоги європейського законодавства. Водночас щодо шкільної освіти з кібербезпеки немає конкретної політичної та стратегічної основи, хоча і є певні рекомендації та правила, які стосуються цієї теми. |
| Ранній | 40 – 60 % | Є чіткий національний підхід до впровадження кібербезпекової освіти. Існують щонайменше початкові політики, плани дій, дорожні карти та інші ініціативи, які безпосередньо впливають на освіту з кібербезпеки на всіх рівнях (від початкової школи до старших класів). Крім того, починають залучати активних стейкхолдерів. |

| | | |
|---|---|---|
| Стабільний | 60 – 80 % | Держава має чітку стратегію надання та поширення кібербезпекової освіти, яка підтримується політичними ініціативами й програмами, до яких залучені різні стейкхолдери. Практики та заходи запроваджуються однаково на національному та регіональному рівнях. Діяльність визначена та задокументована з чітким розподілом ресурсів та управлінням, установленими термінами реалізації. Застосовується довгострокове бачення, і кібербезпека є важливою частиною навчальних програм у початковій та середній школі. |
| Оптимізований/ Адаптивний | 80 – 100 % | Щодо освіти з кібербезпеки є не лише окрема Стратегія, але й відбувається постійний процес оцінювання: визначаються пріоритети, оперативно проводиться оптимізація, існує надійна система показників реалізації, є коротко-, середньо- та довгострокові цілі. Ефективність освітньої діяльності з кібербезпеки регулярно досліджується та контролюється за допомогою усталеної системи показників.<br><br>Визначаються фактори успіху, виклики та прогалини в реалізації заходів, а програми, ініціативи та стратегія оптимізуються та коригуються. |

Слід зазначити, що однією з особливостей методології ENISA є нелінійний спосіб оцінки зрілості по конкретним контролям. Для цілої низки контролів оцінка може бути лише “Так” чи “Ні” і не враховувати наявні проміжні зусилля країн щодо впровадження контролів. В деяких випадках це призводить до того, що навіть якщо країна має очевидний прогрес з реалізації контролю, його оцінка буде все одно “0%” зрілості.

# ОСНОВНІ РЕЗУЛЬТАТИ

## I. Урядовий рівень

### 1.1. Регуляторна база

*Контроль 1. Наявність нормативно-правової бази, визначення цілей і обсягу (наприклад, процесів і тем) щодо освіти з кібербезпеки*

Україна має обов'язкові нормативні вимоги щодо вивчення основ кібербезпеки як частини базової середньої освіти. Зокрема, у 2020 році ухвалено "Державний стандарт базової середньої освіти" (Постанова КМУ від 30 вересня 2020 р. № 898, далі – Стандарт базової освіти)[2], у якому зазначено, що однією з ключових компетентностей школярів є "інформаційно-комунікаційна компетентність, що передбачає впевнене, критичне й відповідальне використання цифрових технологій для власного розвитку та спілкування; здатність безпечно застосовувати інформаційно-комунікаційні засоби в навчання та інших життєвих ситуаціях, дотримуючись академічної доброчесності". Базуючись на цій нормі, Стандарт базової освіти вимагає, щоб уже в 5-6 класах учні дотримувались основ безпечної поведінки в цифровому середовищі та основних засад академічної доброчесності [6 МОВ 3.2.3] та "взаємодіяли з іншими особами у цифровому середовищі, дбаючи про безпеку [6 МОВ 3.2.3-1]", а в 7-9 класах – "дотримувались основ безпечної поведінки в цифровому середовищі, розпізнавали деякі прояви маніпулятивних впливів у цифровому середовищі та уникали їх [9 МОВ 3.2.4-1]".

Додаток 13 до Стандарту базової освіти ("Інформатична освітня галузь"), вказує, що базові знання школярів мають стосуватись таких тем, як: "Шкідливе програмне забезпечення і боротьба з ним", "Інформаційна безпека", а також "Безпечне користування інтернетом". Засвоюючи ці знання, вони повинні вміти "захищати себе й цифрові пристрої від типових кіберзагроз".

Додаток 14 до Стандарту базової освіти "Вимоги до обов'язкових результатів навчання учнів в інформатичній освітній галузі" вказує, що вже у 5-6 класах учні мають "дотримуватись правил кібербезпеки" і "виокремлювати інформацію та обговорювати ситуації булінгу, зокрема кібербулінгу", а в 7-9 класах – "дотримуватись принципів кібербезпеки, самостійно застосовувати процедури організації інформаційної безпеки для себе, власних пристроїв і даних", протидіяти булінгу.

Крім Стандарту базової освіти, діє ще й Державний стандарт базової і повної загальної середньої освіти (далі – Стандарт повної освіти)[3] , затверджений ще в 2011 році. Він має втратити чинність 1 вересня 2026 року й бути повністю замінений Стандартом базової освіти, однак наразі є чинним документом. Він також визначає

необхідність опанування учнями знань "про інформаційну безпеку суспільства та особистості". Для цього учень має розуміти "цілі застосування і способи функціонування засобів захисту даних, поняття шкідливих програм, здійснювати захист даних від шкідливих програм, сутність та важливість інформаційної безпеки для людини й суспільства в цілому".

***Висновок. Кібербезпекові освітні питання загалом визначені вже на рівні загального освітнього стандарту. Хоча кібербезпека так і не змогла стати окремим, самостійним освітнім напрямом, але її природно розглядають як частину більш широкого курсу "Інформатика". Водночас їх обсяг не дозволяє широко висвітлити цю проблему в школах, а надто створити умови, які б заохотили дітей до глибшого вивчення кібербезпеки.***

*Рівень зрілості за методологією ENISA: 100%*

*Контроль 2. Наявність нормативно-правових вимог до навчальних програм для закладів початкової та середньої освіти (усіх класів) щодо освіти з кібербезпеки*

Українська модель системи шкільної освіти базується на максимально тісному зв'язку між Стандартом і типовими освітніми програмами, що визначають загальні вимоги до знань учнів і фактично є орієнтирами для будь-яких навчальних програм. Типові освітні програми розробляються, затверджуються МОН на базі Державного стандарту (що затверджується Розпорядженням КМУ) та мають конкретизувати знання учнів з різних предметів. Типові освітні програми стають основою для навчальних програм, у яких визначають очікувані результати навчання і кількість годин, виділених на вивчення теми/розділу в певному класі. Навчальні програми є основою для модельних навчальних програм, які розробляються фахівцями (зокрема вчителями) для безпосереднього впровадження в школах. Типові освітні програми обов'язково мають бути пов'язані з вимогами Стандарту.

Оскільки Стандарт містить певні вимоги до кібербезпекової освіти, то й усі типові освітні програми мають такі компоненти (оцінка програм буде подана у розділі "Контроль 15"). Водночас слід зазначити, що так само, як і Стандарт, типові освітні програми не розглядають кібербезпекову освіту як окремий, самостійний компонент, а лише як складову загального курсу "Інформатика".

**Висновок. Контроль реалізований: державний освітній стандарт чітко регулює вимоги до базового наповнення освітніх курсів для школярів усіх рівнів.**

*Рівень зрілості за методологією ENISA: 100%*

*Контроль 3. Нормативна база ЄС імплементована в національне законодавство*

Методологія ENISA не вказує прямо на перелік європейських регуляторних актів, що мають значення в контексті цього дослідження, але ключовою тут є Директива

(ЄС) 2022/2555 Європейського Парламенту та Ради від 14 грудня 2022 року про заходи для високого загального рівня кібербезпеки в Союзі (NIS2 Директива)[4]. Текст Директиви (зокрема, стаття 7) указує на обов'язковість "сприяння та розвитку освіти, навчання з кібербезпеки, навичок кібербезпеки, підвищення обізнаності та ініціатив у сфері досліджень і розробок, а також інструкції щодо належної практики кібергігієни та контролю, що спрямовані на громадян, зацікавлені сторони та організації" як частини Національної стратегії кібербезпеки будь-якої країни-члена ЄС.

Наразі Україна знаходиться в процесі імплементації цієї Директиви й 17 квітня 2025 року Президент України підписав Закон "Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури"[5] , який має імплементувати більшу частину вимог NIS2 в Україні. Ухвалений документ дійсно закріплює за Держспецзв'язком обов'язки щодо "організації та здійснення заходів з підготовки кадрів, підвищення рівня знань і навичок, проведення навчань, розроблення та реалізації освітніх і просвітницьких програм", однак відсутні згадки про те, що це стосується і шкільної освіти.

Завдання, пов'язані з NIS2 Директивою, містить і чинна Стратегія кібербезпеки України:

- ціль К2 "Професійне вдосконалення, кіберобізнане суспільство та науково-технічне забезпечення кібербезпеки", яка прямо вказує, що в результаті реалізації Стратегії "цифрові навички, кіберобізнаність щодо сучасних кіберзагроз та протидії їм стануть невід'ємними елементами освіти кожного громадянина України";
- одна з цілей Стратегії – "розробка Загальнонаціональної програми кіберграмотності, спрямованої на підвищення рівня цифрової грамотності населення України, зокрема, шляхом додавання питань стосовно цифрових навичок, кіберобізнаності щодо сучасних кіберзагроз та протидії їм до навчальних програм загальної середньої, професійної (професійно-технічної), фахової передвищої та вищої освіти".

Однак наразі відсутні дані про те, що така загальнонаціональна програма була ухвалена як окремий документ чи існує офіційно затверджений урядовий документ, який можна трактувати як таку програму. Водночас тема цифрових навичок була додана до навчальних програм загальної середньої освіти.

***Висновок. Незважаючи на чіткий курс України на транспонування європейського законодавства в українську практику, наразі цей пункт залишається реалізованим частково, але з позитивною тенденцією до повного виконання.***

*Рівень зрілості за методологією ENISA: 0%*

## 1.2. Політики

*Контроль 4. Наявність спеціальної політики, розробленої щодо освіти з кібербезпеки в межах загальної середньої освіти*

В Україні немає окремих політик щодо кібербезпеки в освіті загалом або кібербезпеки в початковій та середній школах, а також інших схожих політик чи стратегічних документів.

***Висновок. Пункт не реалізований.***

*Рівень зрілості за методологією ENISA: 0%*

## 1.3. Підтримка

*Контроль 5 - Наявність національної програми (програм) для сприяння охопленню освіти з кібербезпеки в усіх класах початкової та середньої освіти*

Наразі в Україні немає жодної окремої національної програми з цього питання. Тематично найближчою до вказаної теми є "Стратегія цифрового розвитку інноваційної діяльності України на період до 2030 року"[6], яка хоча й містить окремий пункт щодо кібербезпекової тематики, однак не охоплює шкільний рівень – "створення інноваційного кластера, який об'єднає науково-дослідні інститути, заклади вищої освіти, стартапи та приватні компанії у сфері кібербезпеки". Також цей документ містить окрему Стратегічну ціль 1, пов'язану з модернізацією шкільної освіти (на всіх рівнях) з метою її адаптації до нових викликів та підготовки інноваційних кадрів. Однак він переважно зосереджений на загальному контексті просування важливості STEM-освіти й не містить прямих згадок про кібербезпеку.

***Висновок. Пункт не реалізований.***

*Рівень зрілості за методологією ENISA: 0%*

*Контроль 6. Наявність вказівок і рекомендацій для сприяння впровадженню освіти з кібербезпеки в початкових і середніх класах*

Відповідно до зібраних матеріалів, освітній процес з питань кіберосвіти лише частково забезпечений належними вказівками та рекомендаціями.

У 2021 році була розроблена та затверджена Типова програма підвищення кваліфікації педагогічних працівників з розвитку цифрової компетентності[7]. Програма складається з п'яти модулів, одним із яких є модуль "Безпека в цифровому суспільстві та освітньому середовищі". За цією Програмою, організації, які здійснюють підвищення кваліфікації вчителів, можуть розробляти власні програми, використовуючи її як практичну настанову. Крім того, заклади підвищення кваліфікації (післядипломної педагогічної освіти) розробляють окремі модулі для

вчителів, за якими навчають їх, як викладати інформатику, до складу якої входить кібербезпекова компонента[8].

У 2024 році МОН затвердив[9] новий професійний стандарт "Вчитель закладу загальної середньої освіти", у якому описано компетентності, необхідні для забезпечення виконання відповідних трудових функцій, зокрема інформаційно-цифрова компетентність як здатність орієнтуватися в інформаційному просторі, здійснювати пошук і критично оцінювати інформацію. Ця компетентність передбачає, що вчитель знає правила безпеки в цифровому середовищі, розуміє наслідки впливу цифрової інформації на людину, уміє критично оцінювати її правдивість тощо, тобто майже той самий набір компетентностей, які вимагаються від школярів за Національним освітнім стандартом.

Крім того, окремі методичні матеріали розроблені та доступні вчителям і популяризуються через сайт МОН. Наприклад, результат спільного проєкту МОН та Google "Безпека дітей в інтернеті". У його межах створено відповідний сайт[10], на якому для шкільних учителів є низка методичних матеріалів, зокрема посібник із безпеки дітей в інтернеті "Обачність. Пильність. Захист. Доброзичливість. Сміливість"[11]. Це комплексний підручник, укладений відповідно до вимог МОН, чітко тематизований і спрямований на впорядковане вивчення основ кібербезпеки в 2-6 класах. МОН також сприяє поширенню методичних матеріалів про проблеми безпечного використання мережі "Інтернет", але вони більшою мірою зосереджені на питаннях кібербулінгу та секстингу[12].

***Висновок. Контроль реалізований частково. Хоча МОН створило необхідну нормативну основу та настанови у вигляді типових програм та стандартів, однак саме методична складова залишається недостатньо опрацьованою. Окремі матеріали існують (наприклад, підручник, розроблений за підтримки Google), проводяться окремі активності (загальнонаціональні уроки кібергігієни), однак вони є епізодичними та несистемними, а підготовлені та поширені методичні матеріали не охоплюють усі освітні рівні (наприклад, підручник від Google, орієнтований лише на учнів 2-6 класів).***

*Рівень зрілості за методологією ENISA: 0%*

*Загальна оцінка рівня зрілості домену "Урядовий рівень"*


Рис.1. Показник зрілості домену "Урядовий рівень" в порівнянні з середньоєвропейським значенням

# II. Стратегія

## 2.1. Національні стратегії

*Контроль 7. Питання освіти з кібербезпеки включені до національної стратегії кібербезпеки*

Попри те, що чинна Стратегія кібербезпеки України[13] була прийнята ще в 2021 році, вона містить завдання, пов'язане із додаванням питань кібербезпекової освіти до навчальних планів усіх рівнів. Зокрема, у межах стратегічної цілі "Професійне вдосконалення, кіберобізнане суспільство та науково-технічне забезпечення кібербезпеки" (К2) мали б розробити Загальнонаціональну програму кіберграмотності, спрямовану на підвищення рівня цифрової грамотності населення України, зокрема "шляхом включення питань стосовно цифрових навичок, кіберобізнаності щодо сучасних кіберзагроз та протидії їм до навчальних програм загальної середньої, професійної (професійно-технічної), фахової передвищої та вищої освіти". Це завдання було визначено й у Плані реалізації Стратегії кібербезпеки України[14], ухваленому 1 лютого 2022 року. Відповідне завдання було закріплене за Кабінетом Міністрів України, Міністерством освіти і науки України, Міністерством цифрової трансформації України та основними суб'єктами національної системи кібербезпеки, його мали реалізувати ще до кінця 2023 року. Наразі відсутні дані про факт виконання цього завдання Стратегії.

***Висновок. Питання важливості кібербезпекової освіти є невід'ємною частиною ключового національного стратегічного документа в сфері кібербезпеки – Стратегії кібербезпеки України. Одне із завдань цього документа вимагає впровадити кібербезпекову освіту до навчальних програм загальної середньої, професійної (професійно-технічної), фахової передвищої та вищої освіти.***

*Рівень зрілості за методологією ENISA: 100%*

*Контроль 8. Тематика кібербезпеки включена до національної освітньої стратегії*

На момент написання цього аналітичного дослідження Стратегія розвитку освіти й науки до 2030 року все ще була в процесі підготовки[15]. Однак, крім цього базового документа, Україна має ще низку стратегічних документів у сфері розвитку освіти. Аналіз цих документів показує, що в них немає відповідної інформації про кібербезпекову освіту, або згадано лише побіжно.

У серпні 2020 року було ухвалено "Концепцію розвитку природничо-математичної освіти (STEM-освіти)"[16], а в січні 2021 – План дій з її реалізації[17] . Хоча документ стосується масштабного впровадження STEM-освіти в Україні на всіх рівнях (починаючи від дошкільної освіти), ані кібербезпека, ані цифрові безпекові навички в ньому не згадані.

У "Стратегії розвитку вищої освіти в Україні на 2022-2032 роки"[18] про кібербезпекову освіту нічого не сказано. Єдина непряма згадка – "забезпечення умов для професійного розвитку наукових і науково-педагогічних працівників, зокрема програм постдокторальних досліджень та програм розвитку цифрових компетентностей". Але йдеться саме про цифрові (не кібербезпекові) навички викладацького складу. Для реалізації цього пункту є лише одне завдання: "запровадження державної програми постійного професійного розвитку науково-педагогічних працівників, забезпечення розвитку цифрових компетентностей наукових і науково-педагогічних працівників", однак у ньому теж не вказано чи йдеться про питання кібербезпеки.

У квітні 2023 року Урядом було схвалено "Концепцію безпеки закладів освіти[19]. Зважаючи на об'єктивну безпекову ситуацію, він здебільшого присвячений питанням фізичної безпеки освітніх закладів. Водночас у тексті Концепції згадується і проблема "відсутності в закладах освіти систем зовнішнього та внутрішнього відеоспостереження", а також "низький рівень обізнаності дітей щодо кіберзагроз та формування безпечної поведінки в інтернеті". Однак для вирішення цих проблем документ пропонував лише одне загальне завдання: "запровадження в освітній процес закладів освіти програм, спрямованих на формування у здобувачів освіти правової поведінки, запобігання конфліктам та правопорушенням, здобуття навичок щодо безпечної поведінки в інтернеті". Виконавцями Концепції визначено

МОН, МВС, Національну поліцію, обласні, Київську міську, державні (військові) адміністрації, заклади освіти (за згодою); термін виконання – 2023-2024 роки. Індикатором виконання документа (у частині кібербезпекової освіти) була кількість запроваджених програм та просвітницьких заходів: 2023 рік – п'ять програм та просвітницьких заходів, 2024 рік – 10 програм та просвітницьких заходів. Наразі невідомо чи було реалізовано це завдання і з яким результатом. У 2025 році до цієї Концепції було внесено зміни[20], однак цей показник залишився незмінним, а отже, це завдання не планують надалі реалізовувати.

У лютому 2024 року було затверджено "План заходів з реалізації Концепції громадянської освіти в Україні"[21]. У документі є поняття "інформаційна безпека" як частина громадянської освіти, але лише в контексті медіаграмотності та критичного мислення. Будь-які згадки про кібербезпеку чи цифрові навички, пов'язані з безпекою, у документі відсутні.

***Висновок. Хоча Україна все ще не має Стратегії розвитку освіти й науки на довгострокову перспективу (яка зважаючи на попередні напрацювання МОН та авторів шкільних курсів буде містити тематику кібербезпеки), однак має низку інших, більш локальних за охопленням та тематикою стратегічних документів, що стосуються сфери шкільної освіти. Водночас з чотирьох таких документів лише один мав окремі згадки про питання кібербезпекової освіти.***

*Рівень зрілості за методологією ENISA: 66%*

## 2.2. Плани дій

*Контроль 9. Розроблено план заходів з питань освіти з кібербезпеки*

Наразі відсутні документи, що можуть бути прямо ідентифіковані як плани дій з питань освіти з кібербезпеки. Водночас МОН здійснює низку кроків, які опосередковано пов'язані з цим питанням. Так для виконання пункту 1.24 Плану організації підготовки проєктів актів та виконання інших завдань, необхідних для реалізації Закону України від 6 червня 2024 № 3788-IX "Про дошкільну освіту", МОН розроблено проєкт Концепції цифрової гігієни дітей дошкільного віку, який станом на момент підготовки цього дослідження був на погодженні в Міністерстві юстиції України[22] . Хоча порушене в Концепції питання напряму не потрапляє в межі досліджуваної групи (дошкільна освіта), однак це формує базу для подальшої структури навчання школярів.

***Висновок. Пункт не реалізований.***

*Рівень зрілості за методологією ENISA: 0%*

*Контроль 10. Розроблено план заходів щодо впровадження кібербезпеки в початковій та середній освіті*

**Відповідні документи в Україні не розроблялись і не ухвалювались.**

***Висновок. Пункт не реалізований.***

*Рівень зрілості за методологією ENISA: 0%*

*Контроль 11. Наявність ініціатив (на національному та/або регіональному рівнях) для покращення конкретних аспектів освіти з кібербезпеки (конкретні теми та аспекти), які не залежать від Плану заходів*

**В Україні реалізуються численні проєкти (здебільшого – національного рівня), що спрямовані на покращення конкретних аспектів освіти з кібербезпеки:**

- **Міністерством цифрової трансформації України та МОН за підтримки програми EU4DigitalUA створено IT-студії – цифрові освітні ресурси з інформатики для учнів та вчителів (https://it-osvita.diia.gov.ua/), це новий підхід до навчання з максимальним фокусом на практику та застосування навичок у реальних ситуаціях, зокрема у питаннях кіберзахисту та кібергігієни;**
- **у 2024 році стартувала всеукраїнська інформаційно-освітня кампанія з кібергігієни, організована за підтримки Державного департаменту США, яка націлена на різні вікові групи населення. Ініціатором та організатором кампанії є Представництво Фонду цивільних досліджень і розвитку США в Україні (CRDF Global в Україні) за підтримки Державного департаменту США;**
- **у 2023 році запущено навчальну програму Her CyberTrack, створену спеціально для жінок, яка фінансується Міністерством закордонних справ Німеччини та реалізується спільно з Міжнародним союзом електрозв'язку (МСЕ), Німецьким товариством міжнародного співробітництва (GIZ) та Управління ООН з наркотиків і злочинності; програма розширює можливості жінок у сфері кібербезпеки за трьома окремими програмами, доступними на платформі Академії МСЕ;**
- **у 2023-2024 роках компанія KPMG провела захід "Cyber Day", спрямований на популяризацію знань з кібербезпеки для школярів. У 2023 році відбулось 2 онлайн-уроки (один для школярів віком від 7 до 10 років і другий для вікової групи 11-17 років), до якого долучились декілька тисяч осіб. У 2024 році було проведено аналогічні уроки, але вони охопили вже майже 100 000 осіб;**
- **у 2022-2024 роках ГО "Смарт освіта" спільно з CRDF Global в Україні розробили безкоштовний онлайн-курс "Основи кібербезпеки для школярів". Цей курс допомагає учням відрізняти правду від фейків, безпечно спілкуватися в інтернеті**

та захищати свої дані від шахраїв. Курс складається з п'яти частин, адаптованих для різних вікових груп: 1–2, 3–4, 5–6, 7–9 та 10–11 класів. Для вчителів розроблено методичні посібники, які дозволяють проводити як окремі заняття, так і серії уроків з кібербезпеки;

- у партнерстві з Google запущено платформу для освітян, школярів і їхніх батьків Безпека дітей в інтернеті" (https://beinternetawesome.withgoogle.com/uk_ua), що містить корисні інструменти та ресурси з кібербезпеки, які допомагають молодому поколінню безпечно й упевнено досліджувати онлайн-світ;
- ГО "Інститут кібербезпеки та аналітики" спільно з організацією Street Child Ukraine та за фінансової підтримки Infosys Springboard розробили сертифікований відеокурс "Кібергігієна та кібербезпека для педагогів", який доступний на платформі Infosys Springboard;
- у межах проекту ЮНІСЕФ "Повернення до формального та неформального викладання і навчання в громаді для учнів і підлітків, зокрема ВПО", що реалізовувався у 2022-2024 рр. У ГО "Тех Стартап Скул" відбулося підвищення кваліфікації вчителів Львівської області за темою "Доступність та безпека цифрового освітнього простору";
- запущено проєкт CyberTeens від ГО "Наукова асоціація кібербезпеки України", метою якого є підвищення обізнаності школярів з питань кібергігієни через навчальну онлайн-платформу, що сприятиме їхньому захисту в інформаційному просторі від соціальних та цифрових загроз, кібершахраїв та буде відповідною підтримкою їхнього психосоціального благополуччя (https://e.surl.li/ksqyni);
- МОН фінансує перспективні дослідницькі проєкти молодих науковців у сфері кібербезпеки. Наприклад, у 2024 році було затверджено проєкт "Методи, моделі та програмні засоби управління інцидентами кібербезпеки в критичній інфраструктурі держави" (наказ МОН від 27.12.2024 №1801);
- за сприяння Міністерства освіти і науки України створено освітні серіали "Школа без цькувань. Учителю", "Школа без цькувань. Батькам", які формують цілісне розуміння явища цькування та пропонують підходи для протидії булінгу (https://e.surl.li/lhqqol). У закладах освіти здійснюються заходи, спрямовані на запобігання та протидію булінгу (цькуванню) в закладі освіти, зокрема організація безпечного користування мережею "Інтернет" під час освітнього процесу; контроль за використанням засобів електронних комунікацій неповнолітніми здобувачами освіти під час освітнього процесу;
- Інститут спеціального зв'язку та захисту інформації КПІ ім. Сікорського (заклад освіти Держспецзв'язку) здійснює проєкт "Кібергігієна в школах України" та проводить онлайн-уроки для учнів закладів загальної середньої освіти. Станом на

жовтень 2023 року цей проект охопив 280 загальноосвітніх шкіл, гімназій, ліцеїв, а більше ніж 17 000 учнів відвідали відповідні уроки з кібергігієни[23];

- за підтримки МОН періодично проводяться всеукраїнські уроки із кібергігієни, до яких залучені провідні експерти та компанії, що опікуються питаннями кібербезпеки[24] ;
- за ініціативи одного з міжнародних донорів та підтримки МОН щонайменше один раз відбувся дводенний семінар "Основи кібербезпеки: кібергігієна та методи викладання"[25] для освітян.

***Висновок. Загалом вказане завдання реалізоване: відповідні матеріали готуються та є публічно доступними і для школярів, і для викладачів. Водночас складно не зауважити, що більшість з цих ініціатив спрямовані виключно на кібергігієну, тобто базові знання про власну кібербезпеку. Вони є критично важливою основою для набуття подальших знань, але загалом мало впливають на глибше розуміння учнями основ кібербезпеки, не заохочують їх до її вивчення як окремого напряму діяльності. Отже, лише побіжно сприяють безпосередньо кібербезпековій освіті в школі.***

*Рівень зрілості за методологією ENISA: 100%*

## 2.3. Співпраця

*Контроль 12. Наявність міждержавного співробітництва з іншими державами-членами ЄС (іншими країнами загалом) щодо освіти з кібербезпеки, включно із співпрацею з бізнесом, урядовими установами, школами та вищими навчальними закладами*

Наразі невідомо про системну міждержавну співпрацю, яка б стосувалась саме питань освіти з кібербезпеки в школах. Державні органи проводять окремі заходи та взаємодії з міжнародними партнерами, які опосередковано стосуються цього питання і можуть у подальшому стати основою для дійсно продуктивних проєктів міжнародного співробітництва. Наприклад, представники МОН[26] взяли участь у Саміті майбутнього в межах Генеральної Асамблеї ООН, де обговорювалися питання цифрової трансформації освіти, та заході цифрового освітнього альянсу Digital Transformation Collaborative, організованого UNESCO, GPE, UNICEF та ITU на полях Саміту. Також у співпраці з Міністерством цифрової трансформації МОН провело перший спільний воркшоп за підтримки Інноваційного хабу ЮНІСЕФ, Естонського центру міжнародного розвитку (ESTDEV), Могилянської стратегічної агенції та міжнародних лідерів з розвитку EdTech-екосистеми: Google, Microsoft, OpenAI, AI4Good. За результатами воркшопу вдалося сформувати спільне бачення ключових викликів, які будуть впливати на розвиток та трансформацію освіти.

***Висновок. Міждержавне співробітництво з іншими державами-членами ЄС (іншими країнами загалом) фактично не сформоване, але є окремі спроби, що***

***можуть у майбутньому призвести до його появи.***

*Рівень зрілості за методологією ENISA: 66%*

*Контроль 13. Співпраця між групами зацікавлених сторін на національному рівні з питань освіти з кібербезпеки (бізнес, урядові установи, школи та вищі навчальні заклади).*

Частково співпраця існує, але не є масштабною та системною саме в галузі шкільної освіти. Щорічно в жовтні в Україні проходить місячник кібербезпеки – різноманітні заходи, що спрямовані на підвищення поінформованості українських громадян про кібербезпекові питання. Заходи місячника охоплюють і шкільну освіту, де відбуваються уроки кіберграмотності. Ці події координуються урядовими структурами, але до їх реалізації залучені численні приватні компанії та громадські організації.

Також можна відзначити проєкт КіберБрама (спільний проєкт Консультативної місії Європейського Союзу в Україні, Департаменту кіберполіції Національної поліції України, ГО "МІНЗМІН" та компанією Yedynka), у межах якого не лише здійснюється практичні заходи з протидії дезінформації, але й розроблено навчальні матеріали з основ цифрової безпеки для учнів усіх класів (від 1 до 11)[27]. Це проєкт, який реалізується в межах міжнародної технічної допомоги й демонструє спільну (партнерську) участь державного органу, громадянського суспільства та приватного сектору.

***Висновок. Ініціативи національного масштабу існують, але їх небагато. Лише одна з них чітко зосереджена на питаннях шкільної освіти, а в іншій – шкільна кіберосвіта є лише частиною ширшої діяльності. Фактично обсяги співпраці на національному рівні здаються обмеженими з погляду залучених учасників та кількості кібербезпекових проєктів.***

*Рівень зрілості за методологією ENISA: 33%*

*Контроль 14. Співпраця між групами зацікавлених сторін на регіональному рівні з питань освіти з кібербезпеки (бізнес, урядові установи, школи та вищі навчальні заклади).*

У межах дослідження не вдалось знайти приклади таких ініціатив.

***Висновок. Пункт не реалізований.***

*Рівень зрілості за методологією ENISA: 0%*

*Загальна оцінка рівня зрілості домену "Стратегічний рівень"*

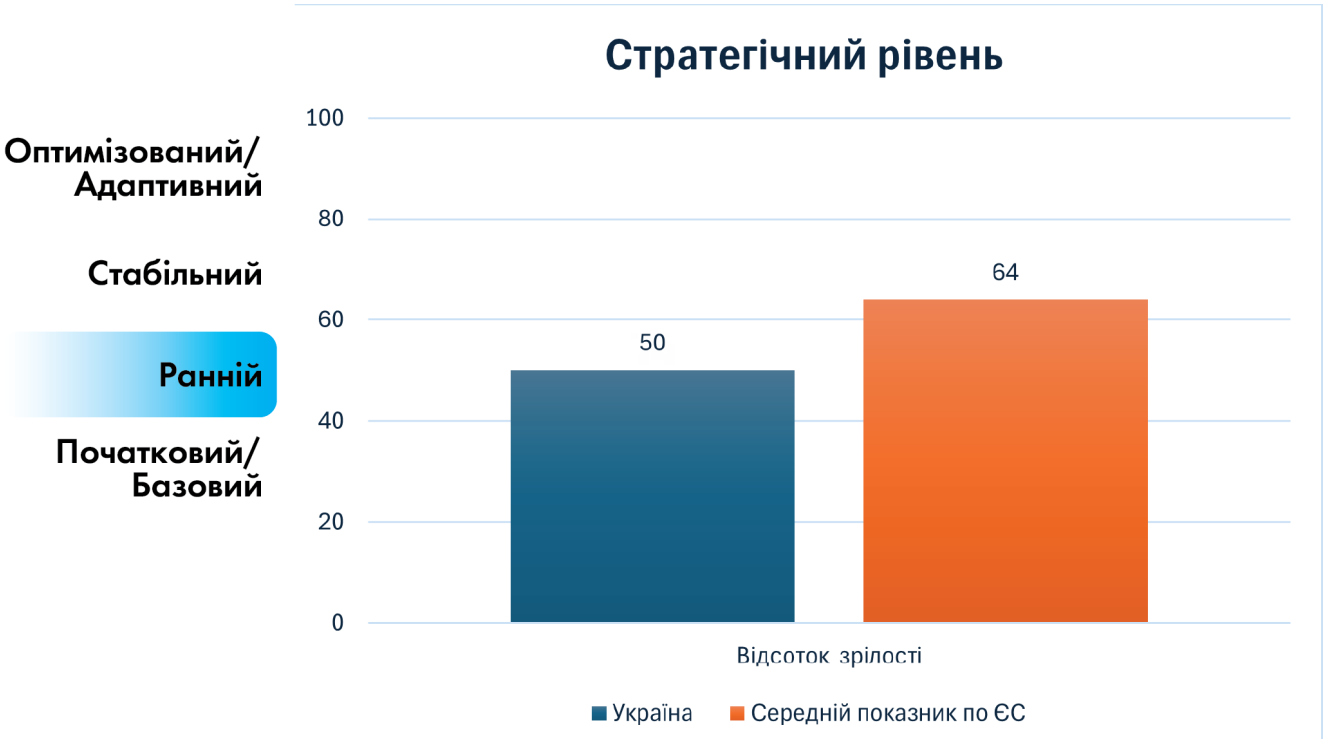


Рис.2. Показник зрілості домену "Стратегічний рівень" у порівнянні з середньоєвропейським значенням

# III. Операційні заходи

## 3.1. Забезпечення освіти з кібербезпеки

*Контроль 15. Додавання теми кібербезпеки до шкільної програми*

Для початкової освіти МОН запропонував дві типові освітні програми[28] за різними редакціями – Олександри Савченко та Романа Шияна. Лише типова освітня програма Романа Шияна містить помітні елементи кібербезпекової освіти. Типова освітня програма Олександри Савченко до них майже не звертається.

Так "Типова освітня програма для 1-2 класу"[29] Романа Шияна передбачає вивчення теми "Правила поведінки й безпеки в інтернет-просторі", яке має відбуватись у межах освітньої лінії "Відповідальність та безпека в інформаційному суспільстві", що спрямована на створення безпечних умов для учнів під час роботи з цифровими пристроями й у мережах, що передбачає "захист особистої інформації, формування принципів етичного, доброзичливого та відповідального спілкування через мережі, навички й можливості захисту власного інформаційного простору, фізичного та психологічного здоров'я". Це передбачає цілу низку освітніх заходів, у результаті яких учні мають набути таких знань та умінь:

- дотримуватися безпечного режиму роботи з цифровими пристроями;
- повідомляти про своє самопочуття дорослим;

- аргументувати необхідність конфіденційності паролів;
- зберігати конфіденційність особистої інформації;
- розпізнавати інформацію небезпечного змісту та повідомляти про це дорослим;
- звертатися по допомогу, коли є сумніви щодо змісту чи особистості співрозмовника в мережах і реальному житті.

Щоб досягнути цього, школярі 1-2 класів мають засвоїти правила безпеки під час роботи з цифровими пристроями; опрацювати матеріали про засоби та способи збереження особистої інформації, а також ті, які полегшують спілкування із людьми з особливими освітніми потребами, теорію про пін-коди й паролі (текстові, графічні, цифрові, тактильні, фотопаролі, паролі-зображення тощо), їхнє призначення та доцільне використання, вікові обмеження на перегляд сторінок і створення акаунтів; уміти організувати робоче місце, розпізнавати небезпечні теми та співрозмовників; виявляти джерела проблем і допомоги; дотримуватися правил етичного спілкування в мережах і реальному житті; знати, як уникнути цькування і діяти у випадку булінгу в цифровому середовищі.

Схожою є ситуація з аналогічною програмою Шияна для 3-4 класу[30], яка має окремий блок "Відповідальність та безпека в інформаційному суспільстві". Зокрема, це вміння порівнювати надійні та ненадійні паролі, розрізняти, яку інформацію можна і заборонено поширювати публічно, краще розуміти, де отримати допомогу у випадку тривожних ситуацій. Вочевидь цей обсяг знань та кількість годин (1 година на тиждень в межах курсу "Інформатика") не достатній, але тематика є.

Для учнів 5-9 класів наразі діє "Типова освітня програма для 5-9 класів закладів загальної середньої освіти"[31], однак вона не визначає ніяких вимог до безпосередніх знань учнів. Цей документ здебільшого зосереджений на питаннях порядку організації навчальних програм нижчого (шкільного) рівня та підходів до його створення.

Для 5-6 класів створено 6 варіантів модельних навчальних програм[32]. Загалом усі програми містять ті чи ті елементи тематики кібербезпеки, хоча лише одна з них повноцінно інтегрує їх у процес навчання, роблячи кібербезпеку частиною майже кожного елементу. Майже в усіх програмах згадуються проблеми фішингу, безпеки пристроїв, персональних даних, відстеження власного цифрового сліду та протидії кібербулінгу. Крім того, в одному з випадків розробники програми прямо пропонують додати тематичний курс "Кібербезпека" як додатковий до основної програми.

Для учнів 7-9 класів також розроблено 6 варіантів модельних програм, і в кожній з них є питання кібербезпеки, хоча і подано нерівномірно. Лише в одній програмі є тематичний напрям "Безпека", який стосується питань кібербезпеки впродовж навчання в усіх трьох класах (включно з питаннями не лише з кібергігієни, а й ширшого спектру: резервне копіювання даних, використання ліцензійного ПЗ,

програми для захисту комп'ютера, антивірусні програми, функції браузера, призначені для гарантування безпеки, захист від спаму тощо). Ще одна програма акцентує увагу на таких технологіях, пов'язаних з питаннями кібербезпеки, як: робота VPN, моделі надання хмарних сервісів (IaaS, PaaS, SaaS), рівні доступу до мережевих документів, взаємозв'язок складових інформаційних систем і мереж, кодування та шифрування даних тощо. Інші програми, хоч і містять окремі елементи кібербезпеки, але розподілено їх нерівномірно й без чіткої системи (наголошуємо на програмі для учнів 9-го класу).

Для 10 та 11 класів є дві навчальні програми: базового (стандартного) та профільного (поглибленого вивчення) рівня. Порівняно з програмами для 5-9 класів, ці менш деталізовані щодо їх змістової складової, але містять елементи кібербезпекової освіти. У програмі стандартного рівня передбачено[33] , що учні після її вивчення зможуть "дотримуватись правил безпечної роботи в інтернеті, розуміти принципи інформаційної безпеки". Крім цих базових знань, учні можуть обрати окремий варіативний блок (варіативний модуль), серед яких є і "Інформаційна безпека" (17 годин)[34] (наразі МОН не має таких для шкіл, у яких обрано цей варіативний блок). Це поглиблений курс вивчення основ інформаційної безпеки, який містить матеріали для поглиблення знань не лише з основ кібергігієни (протидія фішингу, спаму, надійні паролі тощо), але й типових загроз у сфері кібербезпеки: несанкціонований доступ до інформаційних ресурсів та інформаційно-телекомунікаційних систем; бот-мережі (botnet); DDoS-атаки (Distributed Denial of Service); крадіжка коштів; "крадіжка особистості" (Identity Theft); основні ненавмисні й навмисні штучні загрози; технічні й програмні засоби добування інформації. Також учні мають навчитися, як протидіяти кіберзагрозам, як побудувати систему кібербезпеки для певної IT системи, як відбувається ідентифікація та аутентифікація користувачів, криптографія, виявлення атак, міжнародні стандарти інформаційної безпеки тощо. Цікаво, що програма для профільного (тобто поглибленого) навчання інформатики[35] практично не містить кібербезпекових елементів, є лише загальне поняття про "інформаційну безпеку", рівні та протоколи інформаційної безпеки, керування ризиками в інформаційних системах.

Окрім того, за даними МОН[36] у 2023 році розроблені та схвалені до використання в освітньому процесі закладів загальної середньої освіти навчальні програми курсів за вибором для учнів 10–11 класів: "Вступ до кібербезпеки", "Основи кібербезпеки", "Безпека в цифровому просторі".

***Висновок. В освітньому просторі початкової школи наразі функціонує декілька освітніх програм, кожна з яких має освітню кібербезпекову змістову лінію, однак лише одна з них містить дійсно поглиблену кібербезпекову складову. Фактично, можна сказати, що для початкової школи освіта з кібербезпеки є обов'язковим та невід'ємним елементом, але потребує більшої деталізації. Для середньої та***

***старшої школи ситуація складніша: якщо для середньої кібербезпекова тематика представлена в усіх варіантах навчальних програм, то в старшій школі є лише додатковим курсом "Інформаційна безпека".***

*Рівень зрілості за методологією ENISA: 84%*

*Контроль 16. Наявність курсів/тренінгів (у різних форматах), які сприяють доступності та зацікавленості темою освіти з кібербезпеки*

За даними МОН, проводяться численні заходи, щоб підвищити рівень знань про безпечне використання сучасних інтернет-ресурсів. Зокрема, йдеться про цикли інформаційно-просвітницьких заходів щодо медіаграмотності та навичок інформаційної безпеки для школярів та їх батьків. Також відбувається поширення матеріалів про безпеку та позитивне використання цифрових технологій дітьми та молоддю, функціонують факультативи та гуртки з інформатики. Однак, аналізуючи публічний простір, ми знайшли лише незначну кількість повідомлень про такі активності.

Міністерство цифрової трансформації України також вживає заходів, щоб спростити доступ дітей до кібербезпекової освіти. Було створено сайт Дія.Освіта[37], на якому є численні освітні курси, зокрема й із кібербезпеки. На ньому розміщено 6 роликів (із залученням відомих українців), які є освітніми матеріалами для школярів: "Про кібербулінг для підлітків"[38], "Цифрова безпека для початківців"[39], "Кібергігієна: як захиститися від фішингу"[40], "Кібергігієна: як захиститися від фішингу"[41], "Обережно! Кібершахраї"[42], "Онлайн-безпека для підлітків"[43].

Слід зауважити, що в Україні існує значна кількість позашкільних курсів[44] із кібербезпеки для дітей, які дозволяють розширити та поглибити знання учнів про певні сфери кібербезпеки. Однак і в цьому випадку кількість таких курсів є недостатньою.

***Висновок. Контроль реалізований. Окремі курси чи спроби держави та громадського/приватного сектору є, але часто вони не систематичні.***

*Рівень зрілості за методологією ENISA: 100%*

*Контроль 17. Наявність тренінгів з кібербезпеки для учнів у школі (як факультативні чи додаткові заняття)*

Наразі невідомо про наявність додаткових курсів чи тренінгів для школярів, які б відбувались системно та постійно. У школах майже немає можливостей проводити такі додаткові курси через низку причин[45]:

- високий рівень навантаження вчителів і учнів;

- насичена обов'язкова програма навчання;
- недостатня кількість методичних матеріалів для якісного навчання за цією тематикою;
- відсутність належної кваліфікації у вчителів, аби проводити такі курси/тренінги.

Додаткові курси та тренінги здебільшого орієнтовані на посилення кібергігієни учнів і не пов'язані з поглибленим вивченням кібербезпеки.

***Висновок. Наразі невідомо про систематичне проведення тематичних тренінгів, або інформація про них не є частиною публічного інформаційного простору.***

*Рівень зрілості за методологією ENISA: 0%*

## 3.2. Наявність механізмів оцінки

*Контроль 18. Наявність механізму моніторингу з конкретними показниками для вимірювання ефективності впроваджених освітніх ініціатив з кібербезпеки (наприклад, показники рівня участі, розвитку навичок, кількості студентів, які вирішили продовжити кар'єру в галузі кібербезпеки тощо)*

Наразі моніторинг ефективності набутих кібербезпекових знань (за конкретними показниками) не відбувається і планів його запроваджувати немає. Однак частково така оцінка знань учнів з питань кібербезпеки все ж здійснюється під час підсумкового оцінювання безпосередньо або на вебплатформах (наприклад, "Всеукраїнська школа онлайн") за відповідними темами предмету "Інформатика". Міністерство цифрової трансформації створило низку необов'язкових тестових інструментів ("Кіберграм", "Цифрограм"), але вони потребують істотного доопрацювання, аби їх можна було використати як системний інструмент оцінки знань.

***Висновок. Контроль не реалізовано.***

*Рівень зрілості за методологією ENISA: 0%*

*Загальна оцінка рівня зрілості домену "Операційні заходи"*

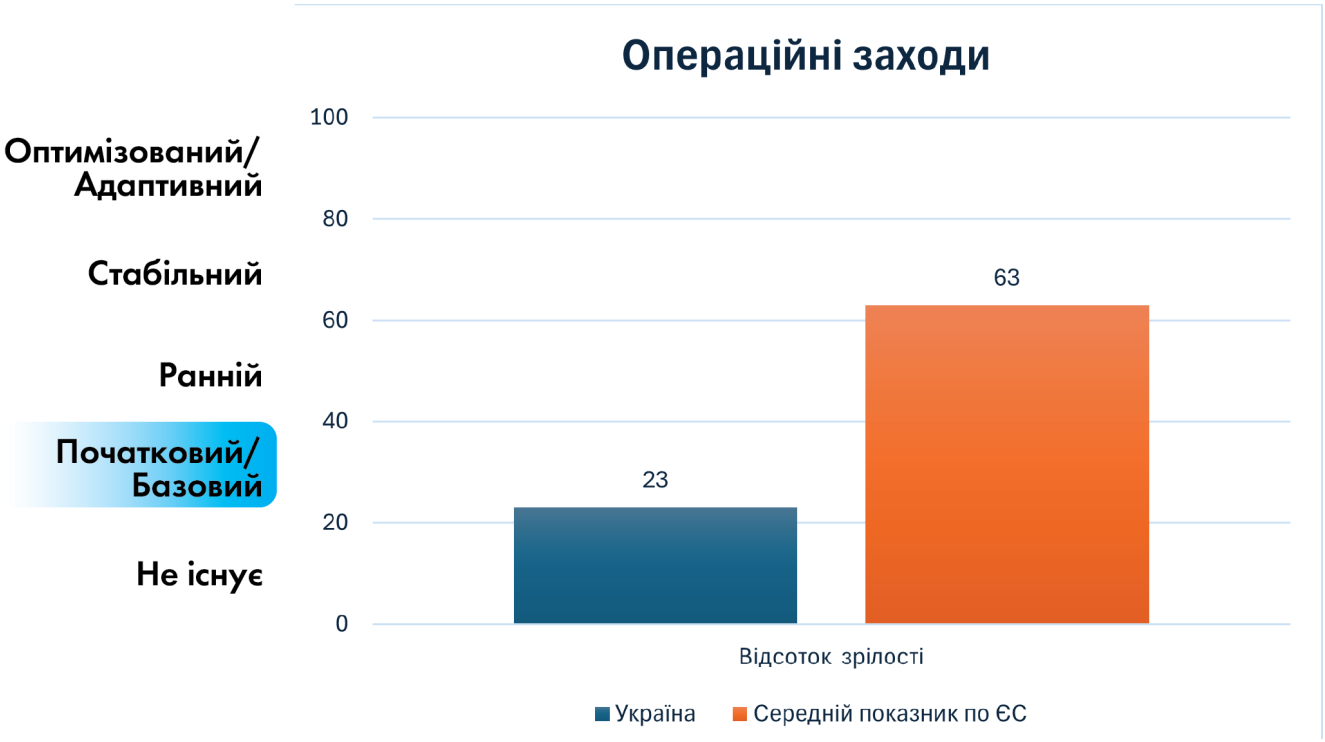


Рис.3. Показник зрілості домену "Операційні заходи" у порівнянні з середньоєвропейським значенням

# ВИСНОВКИ

На загальнодержавному рівні приділено увагу питанням кібербезпеки в освіті. Відомо про те, що інформацію про навички кібергігієни додано до державного освітнього стандарту, також їх опрацьовують  під час вивчення курсу "Інформатика". На жаль, через обмежену кількість навчальних годин учні не можуть поглиблено вивчати кібербезпеку. Не створено й належних умов для зацікавлення школярів цією галуззю. Попри відсутність прямої згадки про імплементацію європейського кібербезпекового законодавства в профільних освітніх документах, Україна фактично впроваджує відповідні норми, зокрема Директиви NIS2, які охоплюють питання кібербезпекової освіти.

До негативних аспектів належить відсутність цілеспрямованої державної політики щодо освіти з кібербезпеки в початковій та середній школі, а також національних програм, спрямованих на її інтеграцію в навчальний процес.

Державою забезпечено базову нормативну основу та загальні настанови з кібербезпекової освіти у вигляді типових програм і стандартів. Проте методичне забезпечення залишається недостатнім, бракує підтверджень системного забезпечення вчителів методичними матеріалами для учнів усіх вікових груп. Окремі ініціативи в цій сфері наявні, але часто є епізодичними й не охоплюють усі освітні рівні.

Позитивним моментом є згадка питань кібербезпекової освіти в національній Стратегії кібербезпеки України, де визначено конкретне завдання щодо її впровадження в школах. Однак інформація про практичну реалізацію цього пункту наразі відсутня у відкритих джерелах. Міжнародна співпраця у сфері шкільної кіберосвіти є несистематичною, хоча окремі ініціативи починають розвиватися. Регіональна взаємодія між зацікавленими сторонами практично відсутня, або інформація про неї не доступна. На національному рівні співпраця з різними стейкхолдерами є більш активною, проте лише один приклад безпосередньо стосується шкільної освіти.

Стратегічне планування розвитку кібербезпекової освіти залишається слабким. Досі відсутня національна освітня стратегія, що ускладнює визначення місця кібербезпекової освіти в загальній системі. Попри наявність локальних стратегій розвитку шкільної освіти, питання кібербезпеки в них не згадано. Як наслідок, відсутні комплексні плани заходів із питань кібербезпекової освіти на різних рівнях середньої школи.

В Україні реалізується значна кількість національних ініціатив, спрямованих на підвищення знань учнів, батьків та вчителів з окремих аспектів кібербезпеки. Однак більшість із них сфокусовані переважно на кібергігієні, тобто базових правилах безпечної поведінки в онлайн-середовищі. Хоча ці знання є фундаментом, їх замало

для формування глибокого інтересу школярів до основ кібербезпеки та стимулювання здобуття освіти в майбутньому в цій галузі.

Освіта з кібербезпеки, особливо з кібергігієни, інтегрована в усі освітні програми. Проте лише в деяких з них приділено цьому питанню достатньо уваги. Вони пропонують учням ширший спектр знань, ніж поняття особистої кібербезпеки. Варто наголосити, що в початковій школі кібербезпекова освіта представлена ширше й глибше, що можна пов'язати із впровадженням Нової Української Школи та оновленням навчальних матеріалів з урахуванням цифрових тенденцій. Очікується, що в старшій школі кібербезпекова складова також поступово зростатиме. Складнішою є ситуація в 10-11 класах, де, попри наявність елементів кібергігієни в усіх навчальних програмах, лише спеціальний курс "Інформаційна безпека" забезпечує поглиблене вивчення тем, безпосередньо пов'язаних з кібербезпекою. Отже, у середній та старшій школі кібербезпекова освіта переважно є факультативною, а не обов'язковою складовою навчального процесу.

Ситуація з позашкільною освітою в галузі кібербезпеки є неоднозначною. Існують окремі приватні курси, а також спроби держави та громадського сектору, проте вони не мають системного та всеосяжного характеру. Відсутні чіткі дані про систематичне проведення тематичних тренінгів у школах для учнів та вчителів, або ця інформація не є публічною.

Проблемою залишається відсутність ефективного механізму моніторингу та конкретних показників для оцінки результативності впроваджених освітніх ініціатив з кібербезпеки (таких, як рівень залучення, розвиток навичок, кількість учнів, які обирають кар'єру в кібербезпеці тощо). Наразі складно оцінити рівень засвоєння учнями знань і навичок з кібербезпеки та вплив шкільної освіти на їхнє подальше навчання в цій галузі.

# РЕКОМЕНДАЦІЇ

- ***Національна освітня стратегія.*** Україна потребує Національної освітньої стратегії, яка б чітко артикулювала важливість кібербезпекової освіти на всіх рівнях, зокрема в школі. Цей документ важливий для подальшого та довгострокового планування дій урядових інституцій держави в цій галузі.
- ***Стратегія розвитку кібербезпекової освіти на шкільному рівні.*** Хоча Національна освітня стратегія може задати загальний вектор, однак шкільна система освіти потребуватиме окремого документа, який визначить очікувані цілі держави щодо майбутнього кібербезпекової освіти в школі. Ця стратегія має охопити всю шкільну систему освіти - від початкових до старших класів.
- ***Плани імплементації стратегій.*** Затвердження стратегічних документів дозволить розпочати процес довгострокового планування шкільної кібербезпекової освіти, але вони потребуватимуть конкретніших планів реалізації, що ґрунтуватимуться на методології SMART (або аналогічній), забезпечуючи чіткі й зрозумілі результати діяльності держави та всіх стейкхолдерів.
- ***Міжнародна співпраця.*** Україні потрібна активніша міжнародна співпраця в питаннях кібербезпекової освіти в школі. Наразі вона не достатня й епізодична. Україна вже має підписані угоди про співпраці з низкою європейських кібербезпекових агентств, наприклад, з агентством ENISA. Крім того, Україна є членом ITU, що робить можливим започаткування спільних міжурядових проєктів, спрямованих на просування кібербезпекової освіти в школах із використанням найкращих світових практик.
- ***Регіональні ініціативи.*** Якщо на національному рівні існує значна кількість освітніх кібербезпекових ініціатив, то на регіональному рівні їх майже немає. Часто саме на регіональному рівні краще зрозумілі конкретні проблеми освітніх закладів та особливості впровадження там ініціатив у галузі кібербезпекової освіти. Водночас пошук регіональних партнерів не має стати ще одним елементом навантаження на шкільні колективи, а бути одним із завдань Департаментів освіти обласних адміністрацій.
- ***Загальнонаціональна ініціатива щодо кібербезпекової освіти.*** Наразі в Україні відсутня загальнонаціональна ініціатива (аналогічна за масштабами до просування STEM-освіти), яка б стосувалась освіти з кібербезпеки в школах. Це ускладнює системну взаємодію різних стейкхолдерів навколо такої ідеї, адже відсутня сама платформа, де вони могли б обговорити чи скоординувати дії в її просуванні. Така ініціатива могла б бути створена або на базі МОН, або в одному з основних суб'єктів національної системи кібербезпеки України.

- ***Забезпечення методичними матеріалами.*** Вчителі та школярі потребуватимуть усе більшої кількості методичних матеріалів. Це дозволить максимально спростити процес викладання кібербезпекових тем та їх засвоєння школярами. Наразі таких матеріалів ще не достатньо, або вони слабко агреговані в єдині навчальні комплекси.
- ***Тренінги з кібербезпеки та підвищення кваліфікації.*** Учителі дотримуються норм викладання кібербезпеки за програмою, але постійні тренінги та курси підвищення кваліфікації змогли б істотно спростити цей процес, зробивши його прогнозованим, повторюваним і якіснішим.
- ***Система оцінки якості знань.*** Україна потребує загальнонаціональної системи оцінки якості шкільної кібербезпекової освіти не лише як складової питань курсу "Інформатика", а як окремого модуля оцінювання. Є спроби (наприклад, Міністерства цифрової трансформації), які закладають підґрунтя для впровадження такої системи, але потребують доопрацювання, щоб використовувати її масово для оцінки знань школярів.

# ДЖЕРЕЛА ТА ПРИМІТКИ


1 https://www.enisa.europa.eu/publications/cybersecurity-education-maturity-assessment

2 https://zakon.rada.gov.ua/laws/show/898-2020-%D0%BF#Text

3 https://zakon.rada.gov.ua/laws/show/1392-2011-%D0%BF#Text

4 https://eur-lex.europa.eu/eli/dir/2022/2555/2022-12-27/eng

5 https://itd.rada.gov.ua/billInfo/Bills/Card/44275

6 https://winwin.gov.ua/assets/files/WIN-WIN_%D0%A1%D1%82%D1%80%D0%B0%D1%82%D0%B5%D0%B3%D1%96%D1%8F%20%D1%96%D0%B-D%D0%BD%D0%BE%D0%B2%D0%B0%D1%86%D1%96%D0%B9%20%D0%B4%D0%BE%D0%BA%D1%83-%D0%BC%D0%B5%D0%BD%D1%82.pdf

7 https://mon.gov.ua/npa/pro-zatverdzhennya-tipovoyi-programi-pidvishennya-kvalifikaciyi-pedagogich-nih-pracivnikiv-z-rozvitku-cifrovoyi-kompetentnosti

8 Лист-відповідь МОН №1/5173-25 від 18.03.2025 на запит НГО ЦАРЕП

9 https://mon.gov.ua/npa/pro-zatverdzhennia-profesiinoho-standartu-vchytel-zakladu-zahalnoi-sered-noi-osvity

10 https://beinternetawesome.withgoogle.com/uk_ua

11 https://storage.googleapis.com/gweb-interland.appspot.com/uk-ua/hub/pdfs/2021/bia_curricu-lum_2023.pdf

12 https://mon.gov.ua/news/rekomendatsii-dlya-batkiv-i-osvityan-shchodo-zakhistu-ditey-u-sotsialnikh-mere-zhakh-ta-interneti

13 https://www.president.gov.ua/documents/4472021-40013

14 https://www.president.gov.ua/documents/372022-41289

15 https://www.ukrinform.ua/rubric-society/3770487-strategia-rozvitku-osviti-i-nauki-do-2030-roku-ko-li-i-cogo-ocikuvati.html

16 https://zakon.rada.gov.ua/laws/show/960-2020-%D1%80#Text

17 https://zakon.rada.gov.ua/laws/show/131-2021-%D1%80#Text

18 https://zakon.rada.gov.ua/laws/show/286-2022-%D1%80#Text

19 https://zakon.rada.gov.ua/laws/show/301-2023-%D1%80#Text

20 https://zakon.rada.gov.ua/laws/show/202-2025-%D1%80#Text

21 https://osvita.ua/doc/files/news/914/91405/65c60ece409a3499331898.pdf

22 Лист-відповідь МОН №1/5173-25 від 18.03.2025 на запит НГО ЦАРЕП

23 https://cip.gov.ua/ua/news/navchayemo-shkolyariv-kibergigiyeni-doluchaitesya-do-onlain-urokiv

24 Наприклад: https://mon.gov.ua/news/ekspertni-porady-z-kiberhihiieny-dlia-uchniv-811-klasiv-vidbuv-sia-vseukrainskyi-urok-iz-kiberhihiieny ; https://mon.gov.ua/news/21-zhovtnya-navchalni-sesii-dlya-uchniv-molod-shikh-ta-starshikh-klasiv-z-pitan-kiberbezpeki ; https://www.youtube.com/watch?v=xMvDCcoYWhM ; https://www.youtube.com/watch?v=yfAT_PM86rc

25 https://mon.gov.ua/news/na-zakarpatti-startuvali-navchannya-z-kiberbezpeki-dlya-osvityan

26 Лист-відповідь МОН №1/5173-25 від 18.03.2025 на запит НГО ЦАРЕП

27 https://stopfraud.gov.ua/cybersecurity-in-education/materialy-dlya-navchannya-uchniv-kiberbezpet-si-i277

28 https://mon.gov.ua/osvita-2/zagalna-serednya-osvita/osvitni-programi/tipovi-osvitni-programi-2

29 https://mon.gov.ua/static-objects/mon/sites/1/zagalna%20serednya/programy-1-4-klas/2022/08/15/Typova.osvitnya.prohrama.1-4/Typova.osvitnya.prohrama.1-2.Shyyan.pdf

30 https://mon.gov.ua/static-objects/mon/sites/1/zagalna%20serednya/programy-1-4-klas/2022/08/15/Typova.osvitnya.prohrama.1-4/Typova.osvitnya.prohrama.3-4.Shyyan.pdf

31 https://mon.gov.ua/static-objects/mon/sites/1/zagalna%20serednya/programy-5-9-klas/2024/09.08.2024/typova-osvitnya-prohrama-dlya-5-9-klasiv-zzso-1120-vid-09082024.pdf

32 https://mon.gov.ua/osvita-2/zagalna-serednya-osvita/osvitni-programi/modelni-navchalni-programi-dlya-5-9-klasiv-novoi-ukrainskoi-shkoli-zaprovadzhuyutsya-poetapno-z-2022-roku

33 https://mon.gov.ua/storage/app/media/zagalna%20serednya/programy-10-11-klas/2018-2019/in-formatika-standart-10-11.docx

34 Слід уточнити, що вибіркові модулі для розширення курсу добирає учитель, спираючись при цьому на профіль навчання навчального закладу, запити, індивідуальні інтереси і здібності учнів, регіональні особливості, матеріально-технічну базу та наявне програмне забезпечення. Реалізація профільного навчання під час викладання курсу може здійснюватися як шляхом розширення змісту окремих тем, так і добором профільно-орієнтованих навчальних завдань.

35 https://mon.gov.ua/storage/app/media/zagalna%20serednya/programy-10-11-klas/2018-2019/01/10-11-profilniy-riven.docx

36 Лист-відповідь МОН №1/5173-25 від 18.03.2025 на запит НГО ЦАРЕП

37 https://osvita.diia.gov.ua/

38 https://osvita.diia.gov.ua/courses/cyberbullying

39 https://osvita.diia.gov.ua/courses/cybernanny

40 https://osvita.diia.gov.ua/courses/kibergigiena-ak-zahistitisa-vid-fisingu

41 https://osvita.diia.gov.ua/simulators/cyber-hygiene-how-to-protect-yourself-from-phishing

42 https://osvita.diia.gov.ua/courses/attention-cyber-fraudsters

43 https://osvita.diia.gov.ua/simulators/e-safety-teens-simulator

44 Наприклад: https://itosvita.com/program ; https://go-mother.com/course/cyber-security-hacking/ ; https://cloud.itstep.org/networks-and-cybersecurity ;

45 Список причин верифіковано авторами дослідження через низку глибинних інтерв'ю з викладачами дисципліни "Інформатика"