АНАЛІЗ ОПИТУВАННЯ З КІБЕРГІГІЄНИ СЕРЕД УЧНІВ 7–11 КЛАСІВ

Попередні результати

ЗМІСТ

ВСТУП

В епоху цифрових технологій, коли діти починають користуватися інтернетом у ранньому віці, навички кібергігієни стають критично важливими. Дослідження Google Україна показує, що більшість українських дітей 5–8 років проводять онлайн 1–3 години на день, а 79% підлітківу віці 13–17 років – понад 3 години щодня, причому 73% з них активно користуються соцмережами. Це розширює можливості для навчання та спілкування, але й несе значні ризики: фішинг, шкідливе ПЗ, витік персональних даних та кібербулінг. Ситуація доповнюється все активнішим використанням підлітками месенджерів, соцмереж, хмарних сервісів та онлайн-банкінгу, часто без належного розуміння технічних та етичних аспектів безпеки.

Попри наявність кампаній із цифрової грамотності в Україні, практичне навчання кібергігієні часто залишається фрагментарним. Рівень цифрової безпеки серед школярів суттєво відрізняється, залежно від віку, доступу до технологій та шкільних ініціатив. Недостатня обізнаність в цьому питанні може призвести до реальних фінансових та психологічних збитків.

З метою оцінки рівня знань та навичок кібергігієни серед учнів 7–11 класів, експертами ГО ЦАРЕП було проведено дослідження в одній зі столичних середніх шкіл Києва. Хоча вибірка обмежена, навіть ці отримані результати можуть відображати загальні тенденції у міському шкільному середовищі та можуть слугувати орієнтиром для подальшого освітнього планування, досліджень і розробки програм кібергігієни.

МЕТОДОЛОГІЯ

Опитування було проведено серед учнів 7–11 класів однієї з київських шкіл, кожен з яких відповів на одні й ті самі 14 питань, що стосуються знань та навичок у сфері цифрової безпеки. В опитуванні взяли участь загалом 138 учнів. Кожне питання мало три варіанти відповіді: Так , Ні або Не впевнений . Результати кожного класу були згруповані та зведені у відсотки відповідей по кожному питанню. Варто зазначити, що вибірки учнів 8–11 класів були менші за вибірку 7-х, тому результати для старших класів можуть бути менш репрезентативними і містити більшу варіативність.

У цьому дослідженні розглядається розподіл відповідей за класами, тематична класифікація запитань, вікова динаміка знань і навичок у кожній темі, а також взаємозв’язок між рівнем обізнаності та практичними діями учнів. На основі виявлених

тенденцій сформульовано освітні рекомендації для підвищення рівня кібергігієни школярів.

ТЕМАТИЧНА КЛАСИФІКАЦІЯ ПИТАНЬ

П'ятнадцять запитань опитування можна згрупувати за кількома тематичними напрямами кібергігієни. Нижче наведено класифікацію питань за темами (в дужках зазначено номери питань анкети, згідно з якими вони зображені на рис. 1):

- **Загальна кібергігієна та обізнаність** – питання **1–3** (наявність уроків з кібергієни; обізнаність з основними інтернет-загрозами; вміння протидіяти цим загрозам).
- **Фішинг** – питання **4–5** (знання, що таке фішинг; вміння протидіяти фішингу).
- **Шкідливе програмне забезпечення (віруси, malware)** – питання **6–7** (знання терміну шкідливе ПЗ ; навички протидії шкідливому ПЗ).
- **Кібербулінг** – питання **8–9** (знання, що таке кібербулінг; знання, як протистояти кібербулінгу).
- **Парольна безпека** – питання **10–11** (розуміння поняття надійні паролі ; оцінка надійності власних паролів).
- **Двофакторна автентифікація (2FA)** – питання **12–13** (знання, що таке двофакторна автентифікація; використання 2FA для своїх облікових записів).
- **Антивірусне програмне забезпечення** – питання **14** (чи користується учень антивірусними програмами на своїх пристроях).

Така класифікація допомагає проаналізувати тенденції в розрізі змістових блоків. Нижче розглянуто, як **змінюються рівень знань та навичок у кожній із цих тематичних категорій від 7 до 11 класу,** а також виявлено деякі прогалини між обізнаністю і практикою.

РОЗПОДІЛ ВІДПОВІДЕЙ ЗА КЛАСАМИ

На **рисунку 1** зображено heatmap, що ілюструє частку учнів (у відсотках), які відповіли Так на кожне з 14 питань, для кожної паралелі з 7-го по 11-й клас. Кожний стовпчик відповідає окремому питанню, а рядок – класу. Інтенсивність кольору в

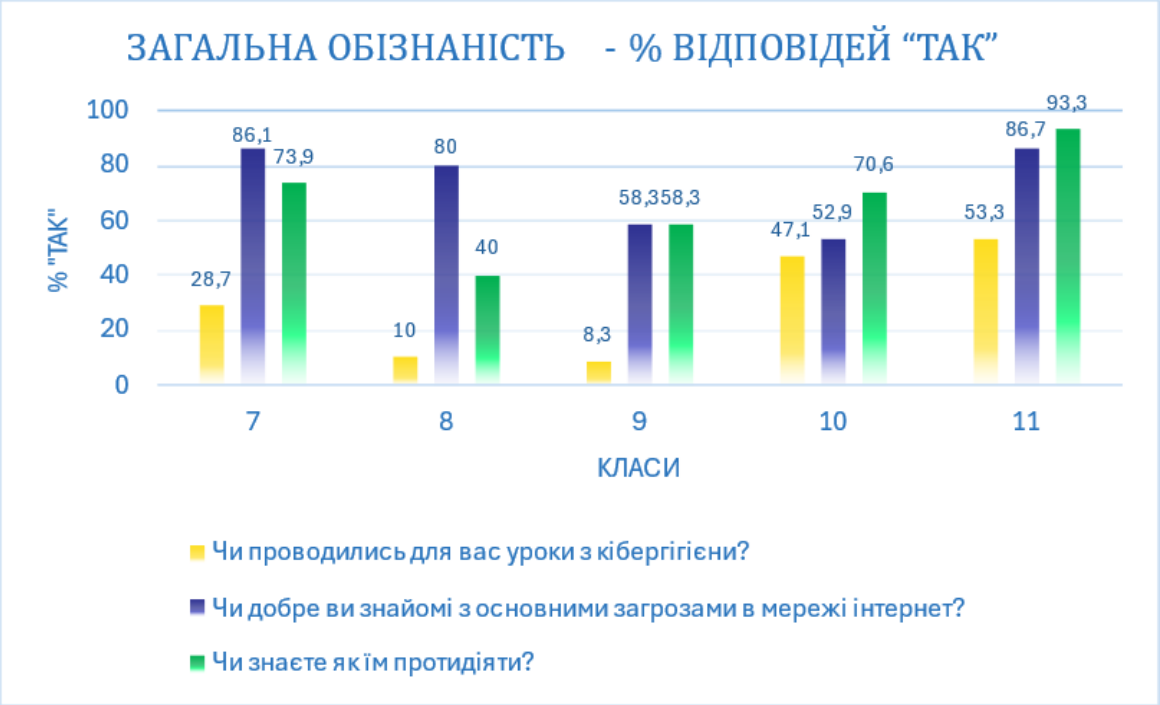
клітинках відповідає відсотку позитивних відповідей (Так): темніші клітинки червоного кольору означають нижчий відсоток учнів, які ствердно відповіли на дане питання, світліші (до зеленого включно) – вищий.

Загальний огляд матриці відповідей виявляє кілька чітких тенденцій. По-перше, **учні старших класів у більшості випадків демонструють вищу обізнаність та кращі навички кібергігієни,** ніж молодші. Це помітно за більш насиченим світлим кольором в верхніх рядках рис. 1 для багатьох питань. Наприклад, для питань про фішинг, шкідливе ПЗ, двофакторну автентифікацію (2FA) та антивіруси частка відповідей Так суттєво зростає від 7-го до 11-го класу. По-друге, є теми, в яких навіть наймолодші учні вже досить обізнані – зокрема, поняття кібербулінгу знайоме майже всім учням починаючи з 7-го класу (для питання Чи знаєте ви що таке кібербулінг? у 7-х класах ~95% відповіли Так). По-третє, **питання, пов'язані з практичними діями чи навичками, зазвичай мають нижчий відсоток «Так», ніж питання на знання**. Наприклад, у 7-х класах значно менше учнів вміють протидіяти фішингу, ніж просто знають, що це таке. Така різниця між теорією та практикою простежується майже в кожній темі.

ДИНАМІКА ЗНАНЬ ТА НАВИЧОК ЗА ТЕМАМИ

Загальна обізнаність та навчання (уроки кібергігієни і базові загрози)

Загальна обізнаність та навчання (уроки кібергігієни і базові загрози)
Перші три питання стосуються загальної підготовки учнів: чи проводилися для них уроки з кібергігієни (питання 1), чи вважають вони себе обізнаними з основними інтернет-загрозами (питання 2) та чи знають, як протидіяти цим загрозам (питання 3). **Результати показують значний розрив між формальним навчанням і впевненістю учнів у своїх знаннях** (рис. 2).



Лише **28,6% семикласників зазначили, що мали уроки з кібергігієни**, причому у 8–9 класах цей показник ще нижчий (близько 10% і 8% відповідно). Хоча очевидний висновок полягає в тому, що більшість учнів молодших класів **не отримували систематичних знань з кібергігієни в школі**, однак така характеристика може бути передчасною: значний відсоток учнів, які вказують на наявність уроків кібергігієни може свідчити про те, що не всі учні чітко ідентифікували ті чи інші уроки як такі, що присвячені кібергігієні. В будь-якому випадку отримані дані свідчать, що у 10–11 класах ситуація поліпшується – вже ~47% десятикласників і 53% одинадцятикласників чітко повідомили про наявність таких уроків.

Попри брак формального навчання в 7–8 класах, **суб'єктивна впевненість учнів у своїй обізнаності з кіберзагрозами доволі висока**. Вже в 7-му класі 85,7% учнів відповіли, що добре знайомі з основними інтернет-загрозами, і цей показник залишається високим у всіх класах (в 11-му – 93,3%). Можливі джерела цих знань – власний досвід, інформація з інтернету, поради батьків або фрагментарні згадки на інших уроках.

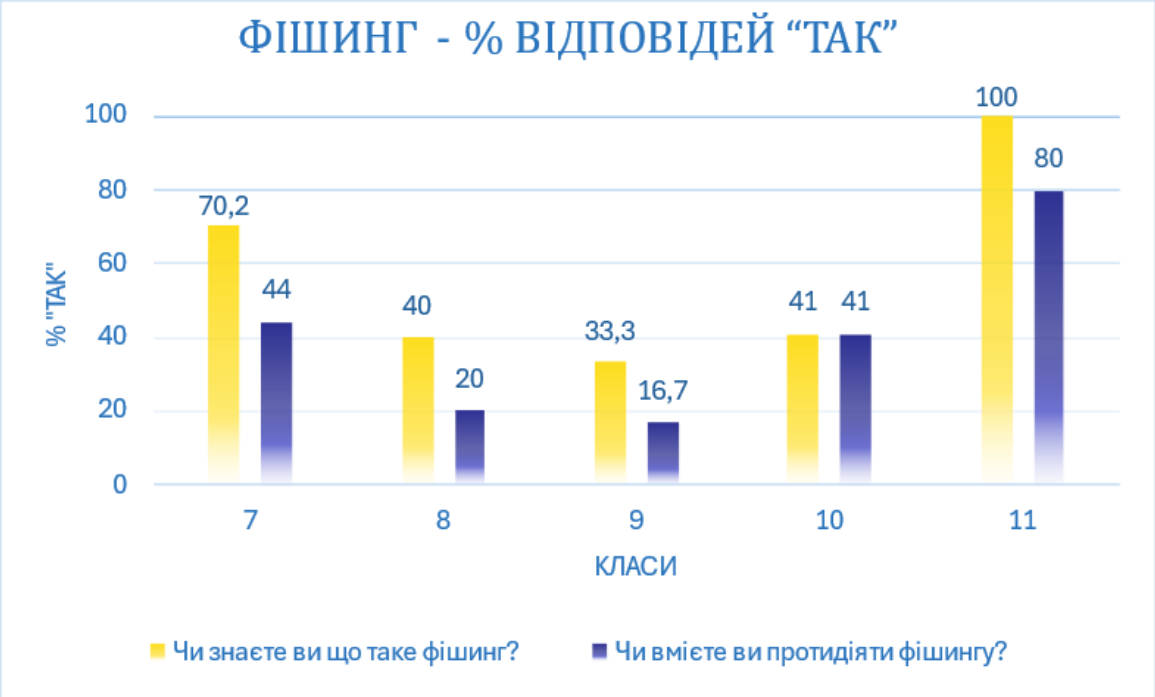
Водночас **реальні навички протидії загрозам відстають від заявленої обізнаності**, особливо в середніх класах. У 7-му класі 73,8% учнів відповіли, що знають як діяти, щоб убезпечитися від інтернет-загроз – показник лише дещо менший за рівень обізнаності (85,7%). Однак у 8-му класі цей відсоток падає до 40% (проти 80%

обізнаних), тобто виникає розрив: багато восьмикласників, які вважають себе обізнаними, **не впевнені, як протидіяти загрозам (тільки половина обізнаних знає, що робити)**. У 9-му класі ситуація вирівнюється (58% обізнані і 58% знають, як діяти), а у старших – покращується: в 10-му класі 52,9% проти 70,6%, в 11-му – вже 86,7% проти 93,3%. Це може свідчити, що зі зростанням віку та, можливо, із появою уроків з кібергігієни, учні набувають практичних навичок і рекомендацій щодо дій у разі кіберзагроз. Втім, навіть у випускному класі близько 13% опитаних не знають, як протидіяти інтернет-атакам, попри те що майже всі вважають себе обізнаними.

Таким чином загальною тенденцією є те, що старші класи демонструють більшу і обізнаність, і здатність протидії, ніж молодші. Проте наявний **розрив між формальною освітою та самоосвітою** (багато учнів знають про загрози без спеціальних уроків) і **розрив між знаннями та діями** (особливо у 7–8 класах, де практичні навички сильно поступаються рівню впевненості в знаннях). Це вказує на потребу більш раннього та практично орієнтованого навчання з кібергігієни.

Фішинг

Питання 4–5 оцінювали розуміння учнями поняття фішингу та вміння розпізнавати/протидіяти таким атакам. **Обізнаність про фішинг суттєво зростає з віком**, хоча є нестандартні коливання в середніх класах (рис. 3). У 7-му класі 70,2% опитаних



знали, що таке фішинг. В 8-му і 9-му класах цей відсоток дещо нижчий (40% та 33,3% відповідно), ймовірно через малу кількість респондентів в цій групі або непоширеність теми фішингу серед цих груп. Натомість у 10-му класі рівень знань повертається до ~41%, а серед одинадцятикласників досягає 100% – **усі опитані випускники знають про фішинг**.

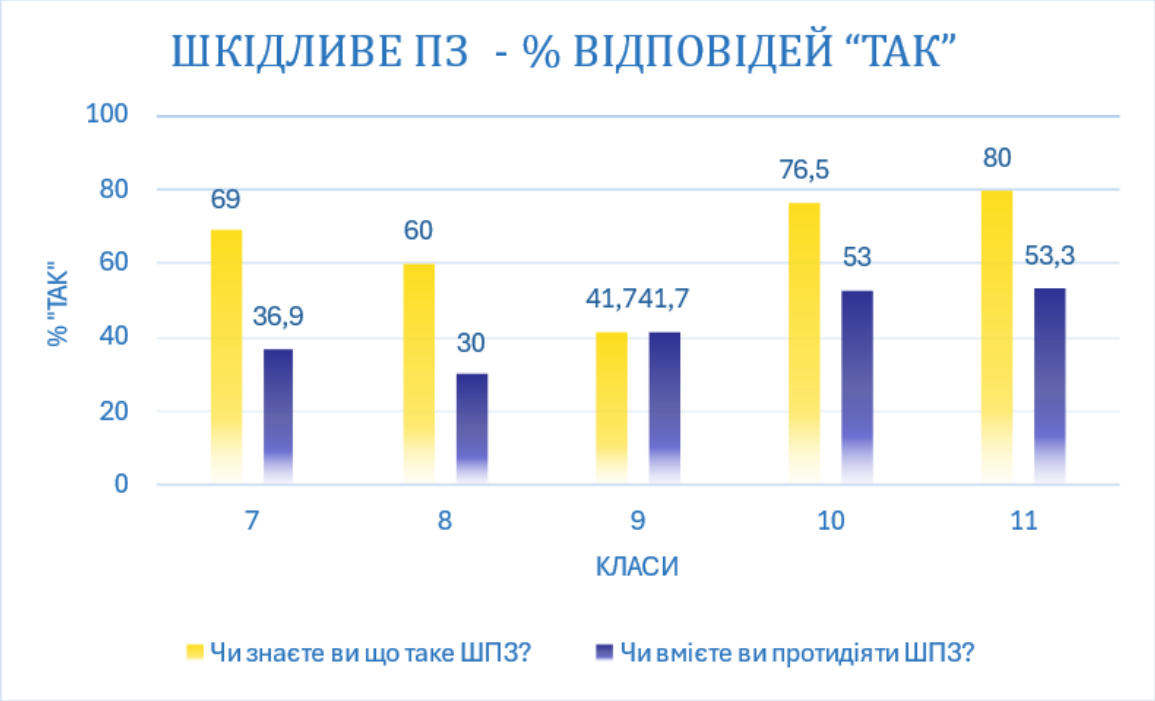
Навички протидії фішингу відстають від обізнаності на всіх вікових етапах. В 7-му класі лише 44% учнів вміють протидіяти фішингу, при тому що 70% знають, що це таке. Це означає, що близько третини семикласників мають уявлення про фішинг, але не знають, як правильно реагувати на фішингові загрози (наприклад, розпізнати підробний вебсайт чи підозріле повідомлення). У 8–9 класах як знання, так і навички дуже низькі (лише 20% восьмикласників і 16,7% дев'ятикласників вміють протидіяти фішингу).

Починаючи з 10-го класу, спостерігається значне покращення: майже половина десятикласників (41%) вже вміє протидіяти фішингу, а в 11-му класі – 80%. Кожен п'ятий одинадцятикласник, знаючи про фішингові загрози, не відчуває повної впевненості в тому, як їх уникнути.

Вікова динаміка фішингу демонструє позитивний тренд: загалом від 7-го до 11-го класу грамотність у цій сфері зростає. Проте у середній школі (8–9 класи) є просідання, що може бути пов'язано з відсутністю навчання саме в цьому періоді. Можливо, учні дізнаються про фішинг пізніше, у 10–11 класах, коли ця тема вводиться в курс інформатики чи класних годин. Це вказує на доцільність **включення теми фішингу до навчальної програми раніше**, аби вирівняти знання і вміння вже у середній школі.

Шкідливе програмне забезпечення (віруси та інше)

Питання 6–7 стосуються шкідливого програмного забезпечення (ШПЗ): чи знають учні це поняття і чи вміють протидіяти вірусам, malware тощо. **Тенденція подібна до фішингу** – знання з віком покращуються, навички також зростають, але є суттєвий розрив між ними, особливо у молодших (рис. 4).



Близько 69% семикласників знають, що таке шкідливе програмне забезпечення (віруси, трояни тощо). Цей рівень плавно знижується у 8-му (60%) та 9-му (41,7%) класах – знову ж, імовірно через невеликі вибірки або різницю в інформованості. У 10-му класі обізнаність різко зростає до 76,5%, а в 11-му – до 80%. Тобто **більшість старшокласників вже розуміють, що таке комп’ютерні віруси та інші шкідливі програми**. Випускники, хоч і не всі мали формальні уроки, можливо, набули цих знань з власного досвіду (віруси на домашньому ПК, смартфоні) або знову ж таки через навчальну програму з інформатики.

Навички протидії шкідливому ПЗ значно слабші. Лише 36,9% семикласників відповіли, що вміють протидіяти таким загрозам. У 8-х класах – 30%, у 9-х – 41,7%. Цікаво, що в 9-му класі частка тих, хто вміє протидіяти, дорівнює частці обізнаних (41,7%); це може означати, що практично всі дев’ятикласники, котрі знають про віруси, також знають, як з ними боротися – але сам відсоток обізнаних був доволі низьким у цій групі. У 10-му класі частка навичок підвищується до ~53%, і цей рівень утримується в 11-му (53,3%).

Відрив між знанням і практикою у темі вірусів помітний у всіх вікових групах. Наприклад, серед 11-класників 80% знають про загрозу, але лише 53% мають навички протидії. У молодших класах розрив ще більший: у 7-му класі 69% vs 37% означає, **що половина тих, хто чув про віруси, не знають, що з ними робити**.

Віковий профіль показує помітне покращення після 9-го класу, що може вказувати на **ефективність навчання або набуття самостійного досвіду в старшій школі**. Проте результат 10–11 класів (≈53% з навичками) є небездоганним – майже половина навіть старших учнів фактично беззахисні перед загрозами malware через брак навичок.

Кібербулінг

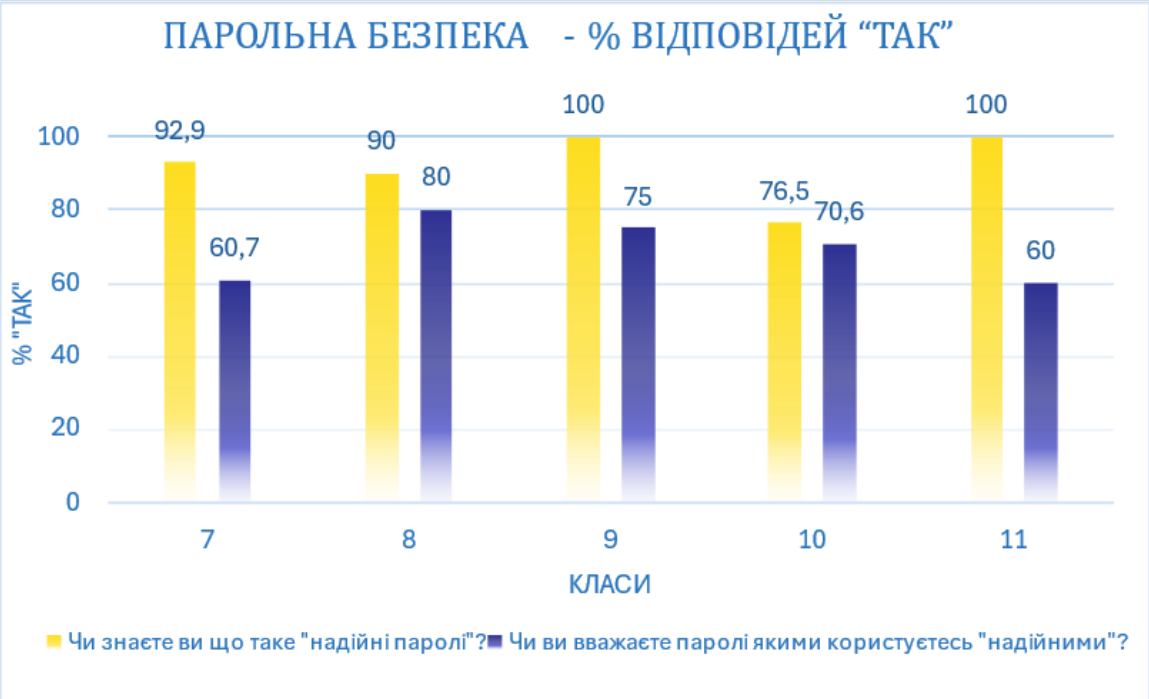
Питання 8–9 стосуються кібербулінгу – чи знають учні, що це таке, і чи знають, як протистояти кібербулінгу. На відміну від технічних аспектів кіберґігієни, **тема кібербулінгу вже добре відома навіть наймолодшим учням**. За даними опитування, майже всі 7-класники (95,2%) знають це поняття, і цей показник лише збільшується у часі: у 8-му класі показник 80%, у 9-му 100%, 10-му – 82,4% та в 11-му класі знову 100% респондентів обізнані з кібербулінгом. Це свідчить про те, що **поняття онлайн-цькування широко відоме молоді**.

Знання, як протистояти кібербулінгу, теж досить поширене, хоча цей показник нижче за обізнаність про явище. В 7-му класі 85,7% учнів відповіли, що знають, як реагувати на кібербулінг. У 8-му класі 70% обізнані, як протистояти (проти 80% тих, хто знає термін). **Найбільший дисбаланс спостерігся у 9-му класі**: хоча всі 100% дев'ятикласників чули про кібербулінг, тільки 58,3% знають, як з ним боротися. Можливо, це випадковість, пов'язана з малою вибіркою учасників, або

ж є свідченням того, що частині підлітків не вистачає конкретних знань/навичок реагування (наприклад, як повідомити про булінг, до кого звернутися, як себе убезпечити). У 10-му класі вже 76,5% знають, як протидіяти, а в 11-му – 86,7%. Отже, серед старшокласників переважна більшість не лише розуміє, що таке кібербулінг, але й знає, як діяти у таких ситуаціях. Загалом можна констатувати, що **різниця між знанням про явище і умінням діяти** у випадку кібербулінгу найменша серед усіх тематик опитування.

Парольна безпека (надійні паролі)

Питання 10–11 спрямовані на оцінку того, чи розуміють учні концепцію надійних паролів і чи вважають, що паролі, якими вони користуються, є надійними. Результати показують, що **майже всі учні знають, що таке «надійний пароль», але далеко не всі застосовують цю практику до власних паролів** (рис. 6).



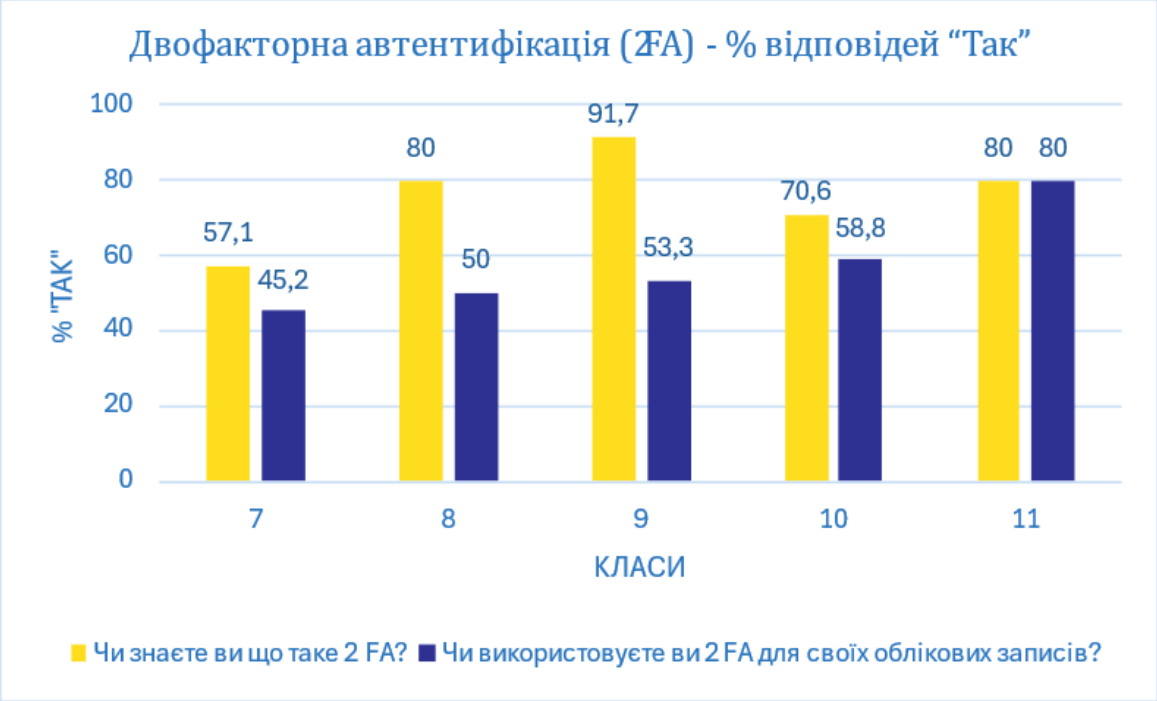
Вже у 7-му класі 92,9% респондентів відповіли, що знають, що означає надійний пароль . Цей показник лише трохи знижується у 8-му класі (90%) і сягає 100% у 9-му. У 10-му класі спостерігається певний спад обізнаності (76,5%), можливо, через специфіку вибірки, але в 11-му класі всі опитані знову одностайно знають це поняття (100%). Отже, **розуміння важливості надійних паролів є практично повсюдним серед учнів**.

Однак, коли мова заходить про **власні паролі учнів**, впевненість у їхній надійності суттєво менше. Лише 60,7% семикласників вважають паролі, якими вони користуються, надійними. У 8-му класі цей показник підвищується до 80%, у 9-му становить 75%, а у 10-му – 70,6%. Цікаво, що в 11-му класі тільки 60% опитаних сказали Так , що їхні паролі надійні – тобто **40% випускників або знають, що їхні паролі не відповідають вимогам надійності, або сумніваються в цьому**.

Ключовий висновок: значна частина учнів, вважає що добре обізнана з концепцією надійних паролів , однак з різних причин **не дотримується цих принципів на практиці**. Вікова динаміка практично не показує лінійного тренду – відсоток впевнених у своїх паролях коливається: максимум 80% (8 клас) і мінімум 60% (7 і 11 класи).

Двофакторна автентифікація (2FA)

Питання 12–13 перевіряли, чи знають учні про двофакторну автентифікацію (2FA) та чи користуються нею для захисту своїх облікових записів. Результат опитування вказує на те, що хоча **двофакторна автентифікація є відносно новою концепцією для школярів, однак старшокласники здебільшого вже її освоїли** (рис. 7).

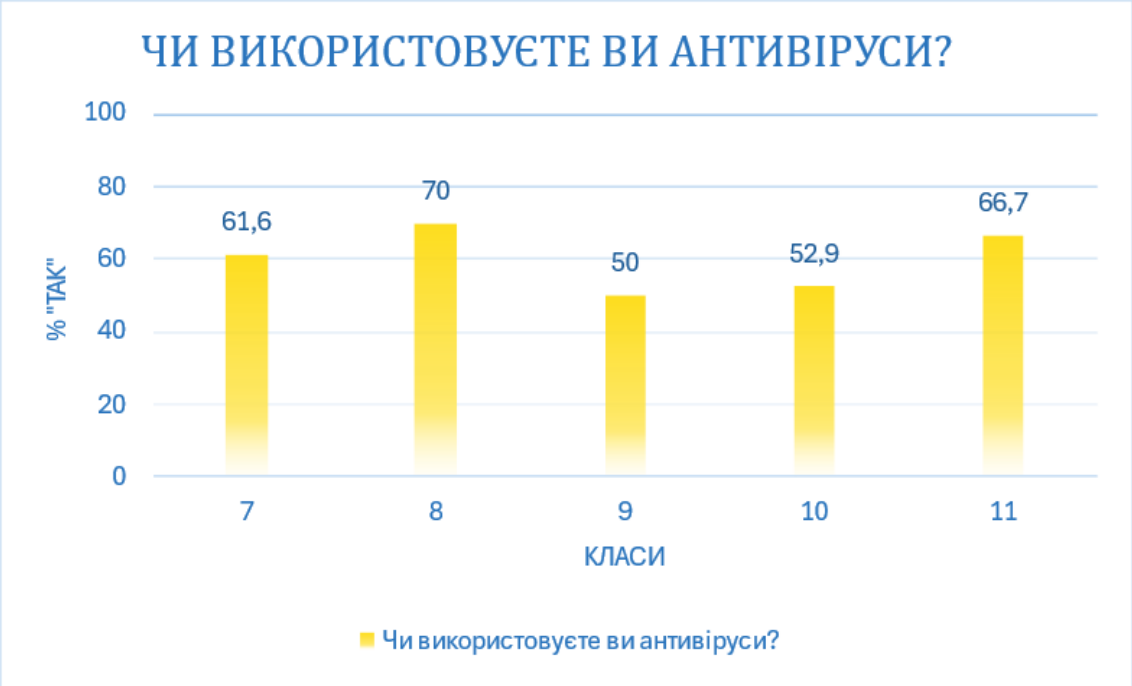


Лише 57,1% семикласників знають, що таке 2FA. Тобто майже половина 12-13-річних поки не знайомі з цим способом захисту акаунтів. У 8-му класі обізнаність різко зростає до 80% – можливо, ця тема потрапила в поле зору частини учнів (наприклад, хтось стикався з необхідністю ввімкнути 2FA у соцмережах чи іграх). Найкраще обізнані виявилися дев'ятикласники – 91,7% знають про 2FA. У 10-му класі знання дещо менше (70,6%), але в 11-му знову 80%. Отже, **близько 3/4 старших підлітків знають про двофакторну автентифікацію**.

Щодо **безпосереднього використання 2FA**, то в 7-му класі тільки 45,2% учнів користуються подвійним захистом для своїх акаунтів. Це очікувано нижче, ніж рівень обізнаності (57%), але різниця не критична – тобто майже всі, хто знає про 2FA в 7-му класі, намагаються її застосовувати. У 8-му класі 50% користуються (при 80% обізнаних). У 9-му класі ситуація найбільш позитивна: 83,3% опитаних дев'ятикласників зазначили, що використовують 2FA, що майже наздоганяє рівень обізнаність - 91,7%. У 10-му класі показники трохи менше – лише 58,8% користуються 2FA (при 70,6% обізнаних). В 11-му класі показовий результат: **80% знають і 80% користуються**. Тобто серед випускників практично кожен, хто чув про двофакторну автентифікацію, вже запровадив її.

Використання антивірусів

Остання тема стосується використання антивірусного захисту на пристроях (питання 14). Це питання менше про знання, а більше про особисті звички і дії учнів.



У 7-му класі тільки 61,6% учнів відповіли ствердно на питання Чи користуєтесь ви антивірусами на своїх пристроях? , тобто близько 38% не використовують жодного антивірусу. В 8-му класі 70% користуються (третина – ні), в 9-му – лише 50% (половина учнів без антивірусного захисту). У 10-му класі 52,9%, в 11-му – 66,7%. Цифри коливаються, але можна сказати, що **в середньому близько двох третин школярів мають антивірус**. Слід зазначити, що дослідження не виявило чіткої тенденції залежності в цьому питанні за віком: пік використання припадає на 8-й клас (70%), потім зниження в 9-му (50%) і знову поступове зростання в 11-му (~67%).

ВЗАЄМОЗВ'ЯЗОК ЗНАНЬ І ДІЙ

Аналізуючи всі теми разом, можна помітити чітку закономірність: **у кожній сфері кібергігієни рівень теоретичної обізнаності перевищує рівень практичних навичок або реальних дій**. Цей взаємозв'язок (або скоріше, розрив) проявляється у таких парах питань:

- Фішинг: значно більше учнів знають, що це таке, ніж тих, хто вміє йому протидіяти (особливо це було виражено у 7–8 класах). Навіть у 11 класі при 100% обізнаності **тільки 80% мають навички протидії**.
- Шкідливе ПЗ: на всіх етапах кількість учнів, знайомих з поняттям вірусів, перевищує кількість тих, хто знає, як діяти при вірусній атаці. Наприклад, серед 10-класників 76,5% знають про шкідливі програми, але лише 53% вміють боротися – **практичний розрив близько 23 процентних пунктів**.
- Кібербулінг: тут розрив менший, але все ж є – майже у кожному класі на 5–15% менше учнів знають, як протидіяти булінгу, ніж тих, хто просто обізнаний про нього.
- Паролі: практично всі знають про вимоги до надійних паролів, але суттєва частка визнає, що їхні власні паролі не відповідають цим вимогам. Тут розрив не просто в уміннях, а в реальних діях/звичках: **знання не конвертується у безпечну поведінку** (особливо у випадку старшокласників, які критичніше оцінили свої паролі).
- 2FA: у молодших класах розрив великий (знають 57%, використовують 45% – в 7 класі), проте у старших він майже зникає (в 11 класі 80% і знають, і використовують). Проте загалом на рівні середньої школи 2FA ще не стала звичною дією навіть для тих, хто про неї вже чув.

Отже, можна зробити висновок, що більшість учнів мають базове уявлення про ключові поняття (інколи це уявлення приходить раніше, ніж формальна освіта). Але ці теоретичні знання не повною мірою конвертуються у практичні – частина школярів з різних причин цього не робить або не вміє робити.

Виразним позитивом є те, що є теми, де різниця між знанням і дією зменшується з віком. Наприклад, двофакторна автентифікація: старшокласники практично зрівнялися у знанні і впровадженні. Це ж стосується кібербулінгу – в 11 класі 86,7% знають, як протидіяти, при 100% обізнаності про явище.

ВИСНОВКИ ТА РЕКОМЕНДАЦІЇ

Проведене дослідження виявило низку сильних та слабких сторін у знаннях і поведінці школярів щодо кібергігієни. До сильних можна віднести високу обізнаність учнів про базові поняття кібербезпеки: більшість знають про інтернет-загрози, фішинг, віруси, правила створення паролів, двофакторну автентифікацію, усвідомлюють проблему кібербулінгу. Більше того, значна частина старшокласників вже перетворила ці знання в конкретні дії – користується 2FA, вміє протидіяти фішингу, критично оцінює силу своїх паролів. Негативним сигналом є те, що істотна частка учнів (особливо у середніх класах) не має достатніх практичних навичок: вони або не навчені, як діяти у разі кіберзагроз, або нехтують такими діями. Крім того, дуже багато підлітків залишаються без базового технічного захисту (антивірус, надійні паролі і 2FA) попри активне життя онлайн.

На основі результатів можна сформулювати такі рекомендації для освітніх програм та виховної роботи:

- **Практична спрямованість навчання**. Школярі потребують більше практичних навичок, що потребує більшої кількості тренінгів: спільне дослідження прикладів фішингових листів, моделювання ситуації з відповіддю на підозрілий лист, спільного налаштування 2FA тощо.
- **Безперервність і послідовність тематик**. Аналіз показав провали в середніх класах по деяких темах (обізнаність про фішинг, віруси). Рекомендується вибудувати навчальну програми так, щоб **кожна тема кібербезпеки піднімалася декілька разів на різних етапах з поглибленням**. Наприклад, у 7-му класі – базово про паролі і булінг; в 8-му – додати фішинг і віруси; в 9-му – повторити, плюс 2FA і соціальна інженерія; в 10–11 – розглянути складніші питання (фішинг в

соцмережах, фінансове шахрайство, персональні дані).

- **Залучення учнів до обговорення та обміну досвідом**. Оскільки старші учні мають вищий рівень кібергігієни, корисно використовувати підхід рівний рівному : проводити зустрічі, де старшокласники діляться з молодшими реальними випадками, радять інструменти захисту, розповідають, як вони самі стикалися з вірусом чи фішингом і що з того вийшло. Такий формат часто більш переконливий для дітей, ніж лекція від дорослого.