ЗВІТ
про проміжне дослідження щодо інформованості цільових аудиторій про основні аспекти кібербезпеки

Дослідження проведено за підтримки Офісу Державного департаменту США Координатора допомоги США Європі та Євразії

Травень 2023

Зміст

Список абревіатур і скорочень

CAPI	особисте опитування вдома у респондента за допомогою комп'ютера (computer assisted personal interview)
CATI	телефонне опитування за допомогою комп'ютера (computer assisted telephone interview)
ВПО	внутрішньо переміщені особи
ГІ	глибинні інтерв'ю
ФГД	фокус-групові дискусії
ЦА	цільова аудиторія
ОМС	органи місцевого самоврядування

Ключові результати

Досвід зіткнення з кіберзагрозами.

Було зафіксовано збільшення кількості випадків кіберінцидентів серед підліткової аудиторії. Так, частка підлітків, що стикалися з кіберзагрозами особисто, або чули про такі випадки від друзів, зросла порівняно з 2021 роком. Водночас, така частка серед дорослих респондентів майже не змінилася, а серед літніх людей зменшилася.

Найпоширенішими кіберзагрозами, які спіткають підлітків, є крадіжка (злам) облікових записів у соціальних мережах та крадіжка (злам) ігрових акаунтів у комп'ютерних іграх. Зріс відсоток підлітків, які повідомили про те, що вони, або їх знайомі стикалися зі зламом: щодо акаунтів у соціальних мережах зафіксоване зростання з 28% в 2021 році до 41% в 2023 році, та щодо зламу ігрових акаунтів – з 19% до 38%.

Проте, суто особистий досвід зустрічі з кіберзагрозами серед підлітків залишається найменшим: лише 11% і 12% цієї аудиторії особисто стикалися із крадіжкою (зламом) акаунтів у соціальних мережах та комп'ютерних іграх відповідно.

Серед молоді 18-25 років найбільшу загрозу становлять викрадення (злам) акаунтів у соціальних мережах; Особисто з цим стикався 21% респондентів (порівняно з 2021 роком показник зменшився на 8 відсоткових пунктів). Серед дорослих віком від 26 років найбільшою загрозою, з якою стикається приблизно кожен четвертий серед опитаних, є вимагання банківських даних, паролів і доступу до облікових записів мобільних банківських додатків і банківських рахунків (без змін порівняно з 2021 роком).

Правила кібербезпеки.

Більшість опитаних повідомляє, що має принаймні загальне уявлення про поняття «кібербезпека»: від 44% до 55% в різних аудиторіях. Молоді люди віком 18-25 років є найбільш обізнаними; 29% сказали, що добре знайомі з концепцією кібербезпеки (порівняно з 18% у 2021 році). Підлітки посіли друге місце: 23% з них знайомі з поняттям кібербезпеки. В аудиторії 26-59 років добре обізнані щодо кібербезпеки 18%, і лише 7% – серед респондентів старше 60 років.

На відміну від декларованої обізнаності про саме тільки поняття кібербезпеки, знання правил кібергігієни за самооцінкою зросло в усіх аудиторіях. Найбільша частка людей, обізнаних з правилами кібергігієни, принаймні у загальних рисах, зафіксована серед молоді 18-25 років (62%), найменша – серед аудиторії старше 60 років (42%).

Старша аудиторія продемонструвала краще дотримання правила «*У разі будь-якої підозри на зараження вашого пристрою чи компрометацію даних негайно повідомляйте відповідні органи (Кіберполіцію України), а також своїх дітей та родину*» ніж у 2021 році (37% у 2021 проти 43% у 2023 році). Слідування правилу «*По можливості використовуйте двофакторну аутентифікацію*» покращилося серед молоді 18-25 років (з 38% до 49%) та дорослих 26-59 років (з 26% до 35%).

Загальна тенденція у зміні рівня знань та слідуванні правилам кібергігієни є суперечливою. Підвищився рівень знань серед дорослих 25-59 років і людей похилого віку. Серед підлітків, частка тих, хто дотримується правил кібергігієни зменшилася порівняно з 2021 роком, тоді як підлітки залишаються найбільш обізнаною аудиторією щодо правил кібербезпеки;

Здатність розрізняти ризиковані ситуації.

Не всі аудиторії можуть відрізнити ситуації, у яких присутня кіберзагроза. Наприклад, більшість респондентів вважають ситуацію, коли «*Подруга зайшла в кафе з «безкоштовним Wi-Fi, щоб скинути гроші батькам через онлайн-банкінг*» як таку, що не має ризиків. З іншого боку, багато людей вважають використання VPN або автоматичне оновлення програмного забезпечення ризикованим, що насправді навпаки допомагає захиститися від загроз кібербезпеці.

Загалом 71% респондентів можуть правильно визначити, чи несуть загрозу кібербезпеці п'ять або більше запропонованих ситуацій із десяти. Цей показник найвищий серед молоді 18-25 років (90%). Дорослі 25-59 років посідають друге місце з показником 72%. На третьому місці підлітки (64%), а найнижчий рівень індексу – у людей похилого віку (47%). Зауважимо, що учасники навчальних програм CRDF Global можуть розрізняти ризиковані ситуації краще за всі інші аудиторії: для них індекс сягнув 96%.

Мета дослідження і методологія

Визнаючи ризики, пов'язані із чимраз більшою цифровізацією світу, CRDF Global у 2019 році розпочала програму покращення кібербезпеки в Україні, Молдові та на Західних Балканах. Програма присвячена запобіганню кібератакам шляхом створення міцної кіберінфраструктури та посилення кібербезпеки. Ця програма підтримується *Офісом Координатора допомоги США Європі та Євразії Державного департаменту США*.

Частиною програми кібербезпеки CRDF Global є проект «Інформаційна кампанія про кібербезпеку», основна мета якого – покращити обізнаність щодо загроз кібербезпеки серед широкої громадськості України.

I хвиля дослідження (базове дослідження) щодо інформованості цільових аудиторій про основні аспекти кібербезпеки і правила кібергігієни була проведена у 2021 році (серпень-вересень).

Поточна – II хвиля дослідження (середньострокове дослідження) проведена у березні 2023 року представляє проміжні результати і має на меті проаналізувати динаміку показників.

Опитування має на мені оцінити:

- рівень поінформованості цільових аудиторій про кіберзагрози;
- рівень обізнаності про основні правила кібергігієни та їх застосування у повсякденному житті;
- особистий досвід користувачів за останні місяці щодо кіберзагроз;
- здатність вирізняти потенційно загрозливі ситуації з точки зору кібербезпеки.

Цільова аудиторія основного дослідження – громадяни України, які користуються інтернетом щонайменше кілька разів на місяць.

Цільові групи респондентів:

- Підлітки 11-17 років;
- Молодь 18-25 років;
- Дорослі 26-59 років
- Люди старшого віку від 60 років.

Основний метод проведення дослідження – **кількісне опитування** за структурованим опитувальником.

Географія дослідження: вся Україна, включно із селами, за винятком АР Крим та територій, які не контролюються українською владою.

Загальна кількість респондентів основного опитування: 1224.

Кількість респондентів за цільовими групами:

- Підлітки 11-17 років: 315 респондентів;
- Молодь 18-25 років: 314 респондентів;
- Дорослі 26-59 років: 354 респонденти;
- Люди старшого віку від 60 років: 241 респондент.

Попередньо було заплановано провести однакову кількість інтерв'ю з усіма цільовими групами (по 300 інтерв'ю). Проте під час опитування дослідники стикнулися із низьким проникненням інтернету у найстаршій цільовій групі (люди віком понад 60 років). З огляду на меншу кількість людей, які регулярно користуються інтернетом, серед найстаршої вікової групи, було прийнято рішення скоротити цільову кількість інтерв'ю до 241 за рахунок збільшення цільової кількості інтерв'ю у групі 26-59 років до 354 інтерв'ю.

Метод опитування:

- для цільової групи «Підлітки» — особисте опитування вдома у респондента за допомогою комп'ютера (CAPI – computer assisted personal interview);
- для решти цільових груп — телефонне опитування за допомогою комп'ютера (CATI – computer assisted telephone interview).

Вибірка випадкова із контролем квот за статтю, віком, регіоном та розміром населеного пункту. В рамках кожної цільової групи вибірка є репрезентативною, структура відповідає структурі інтернет-користувачів за статтю, віком, регіоном та розміром населеного пункту.

Для аналізу по вибірці загалом було застосовано зважування, яке привело структуру вибірки у відповідність до структури населення України за віком.

Максимальна статистична похибка вибірки становить:

- Вибірка загалом: 2,8% ймовірністю 95%;
- Підлітки 11-17 років: 5,5% ймовірністю 95%;
- Молодь 18-25 років: 5,2% ймовірністю 95%;
- Дорослі 26-59 років: 4,6% ймовірністю 95%;

- Люди старшого віку від 60 років: 6,3% ймовірністю 95%.

Додатково було проведено **кількісне та якісне опитування контрольної групи:**

- Особи, що пройшли курси CRDF Global: 305 респондентів.

Метод кількісного опитування: онлайн інтерв'ю. Посилання на опитування надсилали фахівці Представництва CRDF Global в Україні.

Кількісне опитування проводилося за структурованим опитувальником (див. Додаток 2). В опитувальнику, зокрема, використовувалися 5-бальні та 10-бальні шкали. З точки зору аналізу позитивною оцінкою вважається оцінка 4 або 5 за 5-бальною шкалою, та 9 або 10 за 10-бальною шкалою.

Метод якісного дослідження: фокус-групові дискусії (ФГД) та глибинні інтерв'ю. Зокрема, було проведено:

- 2 онлайн ФГД зі студентами та молоддю, що були слухачами курсів з кібербезпеки від CDRF Global. В кожній ФГД взяло участь 4-6 респондентів з різних міст, частина респондентів є ВПО;
- 3 міні-ФГД з представниками місцевих органів та держслужбовцями, що були слухачами курсів з кібербезпеки від CDRF Global. В кожній ФГД взяли участь по 3 респонденти, що проживають та працюють у різних регіонах України;
- 3 глибинних інтерв'ю з вчителями, що викладають інформатику в школах та були слухачами курсів з кібербезпеки від CDRF Global. Вчителі також представляли різні регіони України.

Результати дослідження

Поведінка в інтернеті

До участі в опитуванні запрошувалися люди, які користуються інтернетом щонайменше раз на місяць – аналогічно до попередньої хвилі дослідження. Більша частина опитаних II хвилі дослідження 2023 року (93%) користуються інтернетом щодня у порівнянні з 90% у I хвилі дослідження 2021 року. Спостерігається значне збільшення часу користування інтернетом впродовж дня: 33% проти 25%. На збільшення проведення часу в інтернеті могли вплинути наслідки пандемії COVID-19 (переведення на дистанційну роботу і навчання) та результати повномасштабного вторгнення (моніторинг поточних новин) (див. Діаграма 1).

Діаграма 1. Як часто ви користуєтеся інтернетом, наприклад відвідуєте сайти, соціальні мережі, користуєтеся додатками, месенджерами? (% відповідей, серед опитаних I та II хвилі)

Також для співставлення поведінки в інтернеті були опитані респонденти, що брали участь у навчальних заходах CRDF Global, – ця група респондентів частіше користується інтернетом щоденно, понад половина проводять в інтернеті більшу частину дня (див. Діаграма 2).

Діаграма 2. Як часто ви користуєтеся інтернетом, наприклад відвідуєте сайти, соціальні мережі, користуєтеся додатками, месенджерами? (% відповідей, серед опитаних II хвилі та учасників навчань CRDF Global)

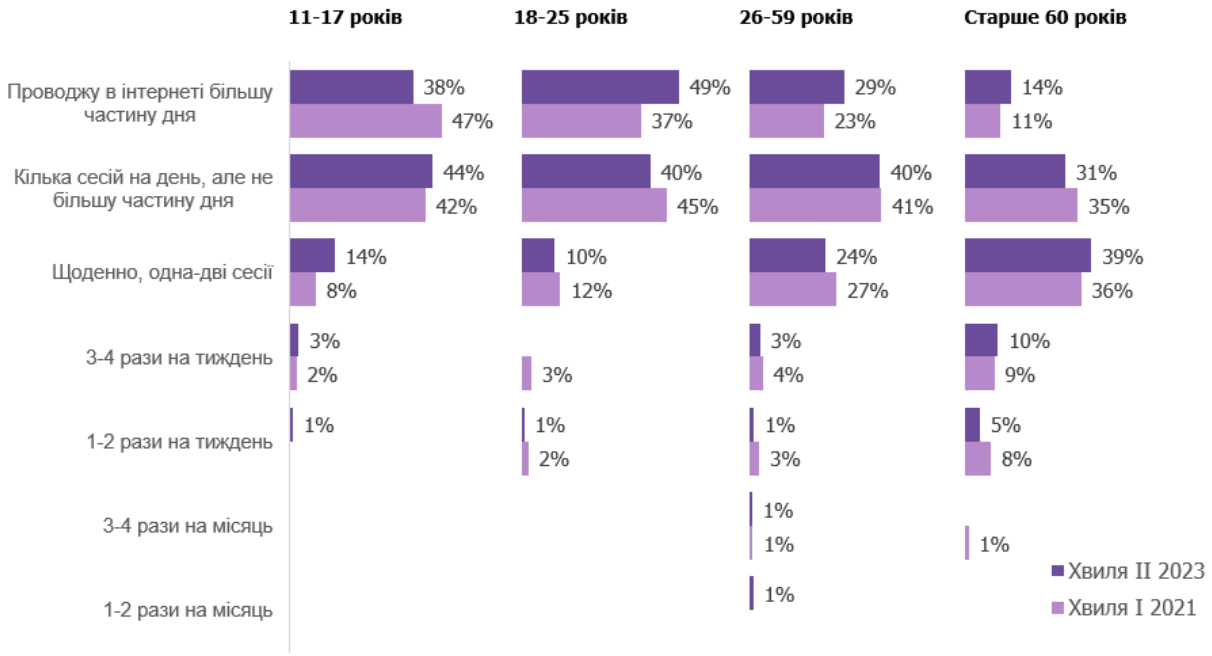
Чим старші респонденти, тим менше часу вони проводять в інтернеті. Ця тенденція була зафіксована у першій хвилі дослідження у 2021, і вона зберігається у 2023 році.

У 2023 році респонденти 18-59 років стали проводити в інтернеті більше часу, тоді як підлітки 11-17 років, навпаки, – трохи менше часу.

Так, серед підлітків 11-17 років більшу частину дня в інтернеті проводить 38% респондентів (порівняно до 47% в I хвилі 2021 року). Серед молоді 18-25 років більшу частину дня в інтернеті проводить майже половина опитаних 49% (проти 37% в I хвилі дослідження). У цільових групах 26-59 років та літніх людей 60+ частка тих, хто проводить в інтернеті більшу частину дня, також збільшилася, але зростання не настільки значне. Частка респондентів 26-59 років, які проводять в інтернеті більшу половину дня, становила 29%, а серед літніх людей – 14% (порівняно до 23% та 11% у 2021 році відповідно) (див. Діаграма 3).

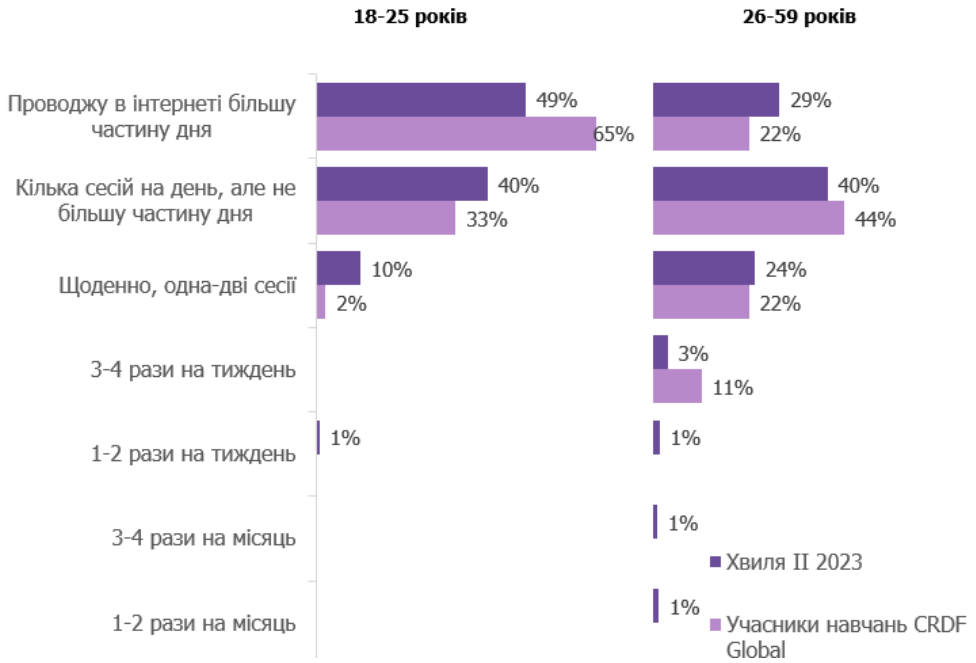
Таким чином, люди із доступом в інтернет схильні користуватися інтернетом щоденно, але літні люди переважно обмежуються 1-2 сесіями зв'язку, тоді як молодь проводить в інтернеті більшу частину дня.

Діаграма 3. Як часто ви користуєтеся інтернетом, наприклад відвідуєте сайти, соціальні мережі, користуєтеся додатками, месенджерами? Розподіл за цільовими групами (% відповідей, серед опитаних I та II хвилі)



Порівнюючи відповіді учасників навчань CRDF Global з відповідями відповідних цільових груп основного опитування, можемо говорити про те, що серед учасників молодь 18-25 років також проводить в інтернеті більшу частину дня – 65% (див. Діаграма 4).

Діаграма 4. Як часто ви користуєтеся інтернетом, наприклад відвідуєте сайти, соціальні мережі, користуєтеся додатками, месенджерами? Розподіл за цільовими групами (% відповідей, серед опитаних II хвилі та учасників навчань CRDF Global)



Обізнаність з поняттями «кібербезпека» та «правила кібергігієни»

Індикатор обізнаності українців із поняттями «кібербезпека» та «правила кібергігієни» заміряється другу хвилю поспіль через пряме запитання. Утім, перевірка, наскільки декларативне знання відповідає реальному, не входить у цілі дослідження.

Загалом рівень обізнаності про поняття «кібербезпека» та «правила кібергігієни» підвищився порівняно до даних I хвилі 2021 року. Так, відповідь «дуже добре знаю і можу пояснити іншим» обрали 19% та 14% відповідно для понять «кібербезпека» та «правила кібергігієни».

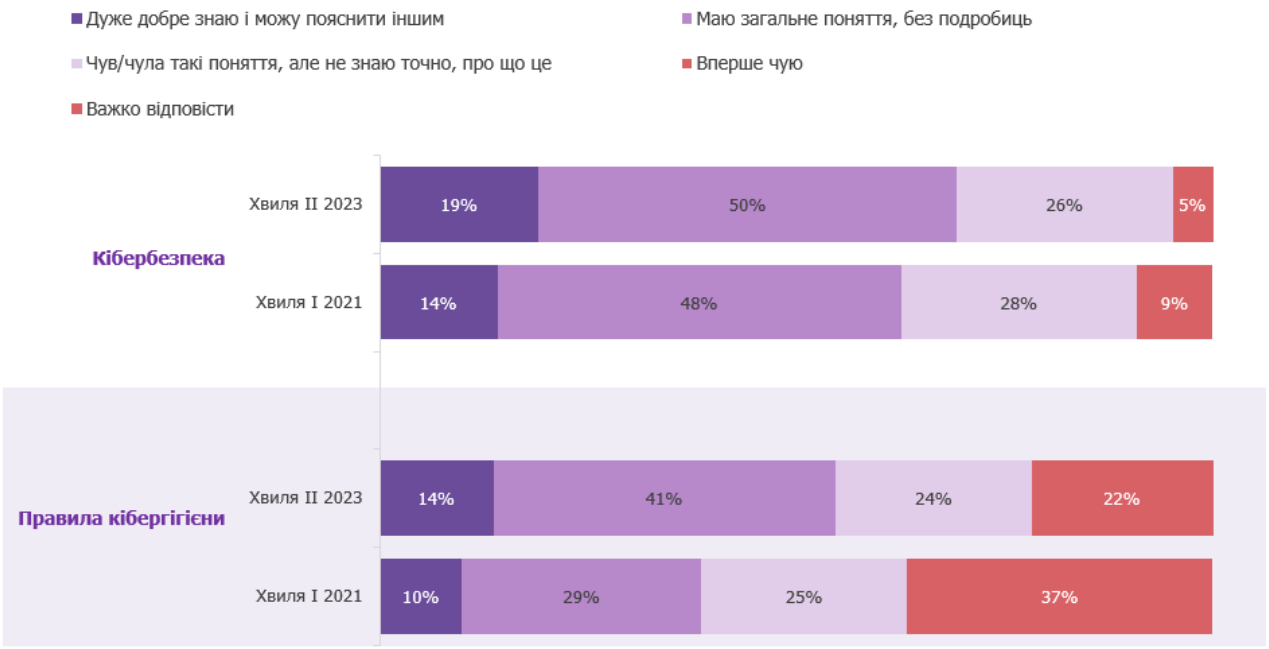
Поняття «кібербезпека» краще знайоме українцям. Загальне уявлення[1] про нього мають 69% респондентів, тоді як уявлення про «правила кібергігієни» хоча б в загальних рисах мають 55%. Утім, для обох понять досить помітним є зменшення частки відповідей «вперше чую» із відповідним зростанням частки відповідей «маю загальне поняття без подробиць». Це може говорити про зростання уваги до «правил кібергігієни» (див. Діаграма 5).

Показово, що спостерігається великий розрив у рівні ознайомленості з поняттями «правил кібергігієни» та «кібербезпека» між респондентами з числа загального населення II хвилі 2023 року та респондентами, що брали участь у навчанні CRDF Global. Так, 50% респондентів, що пройшли навчання, «дуже добре знають та можуть пояснити іншим» поняття «кібербезпека» проти 19% респондентів серед широкої громадськості; також 52% респондентів, що пройшли

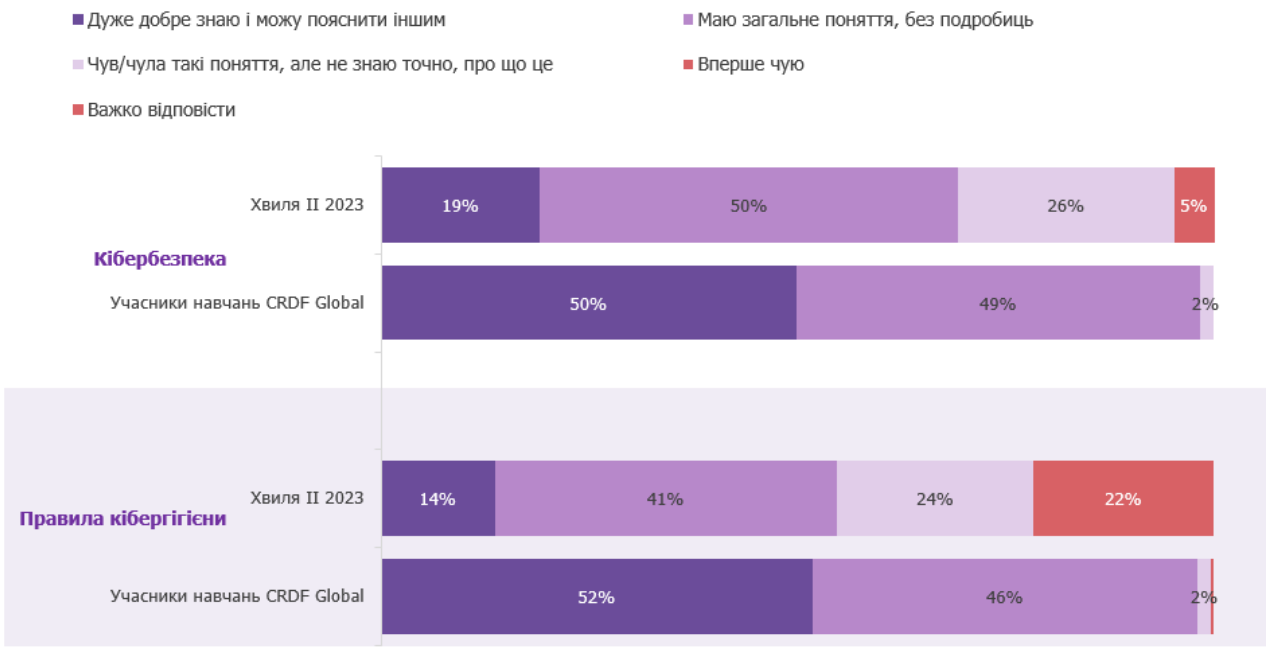
[1] Сума відповідей «Дуже добре знаю…» і «Маю загальне поняття…»

навчання, «дуже добре знають та можуть пояснити іншим» «правила кібергігієни» проти 14%, відповідно (див. Діаграма 6).

Діаграма 5. Скажіть, будь ласка, наскільки вам знайомі поняття «кібербезпека» та «правила кібергігієни»? (% відповідей, серед опитаних I та II хвилі)

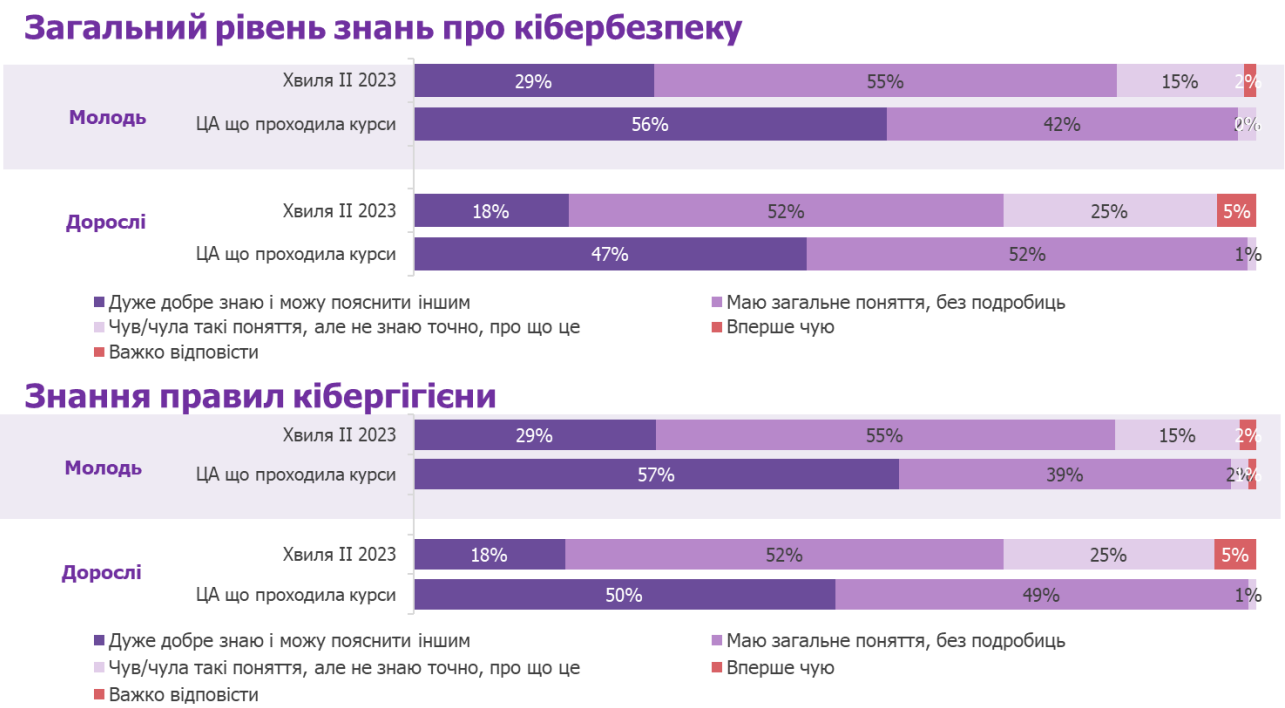


Діаграма 6. Скажіть, будь ласка, наскільки вам знайомі поняття «кібербезпека» та «правила кібергігієни»? (% відповідей, серед опитаних II хвилі та учасників навчань CRDF Global)

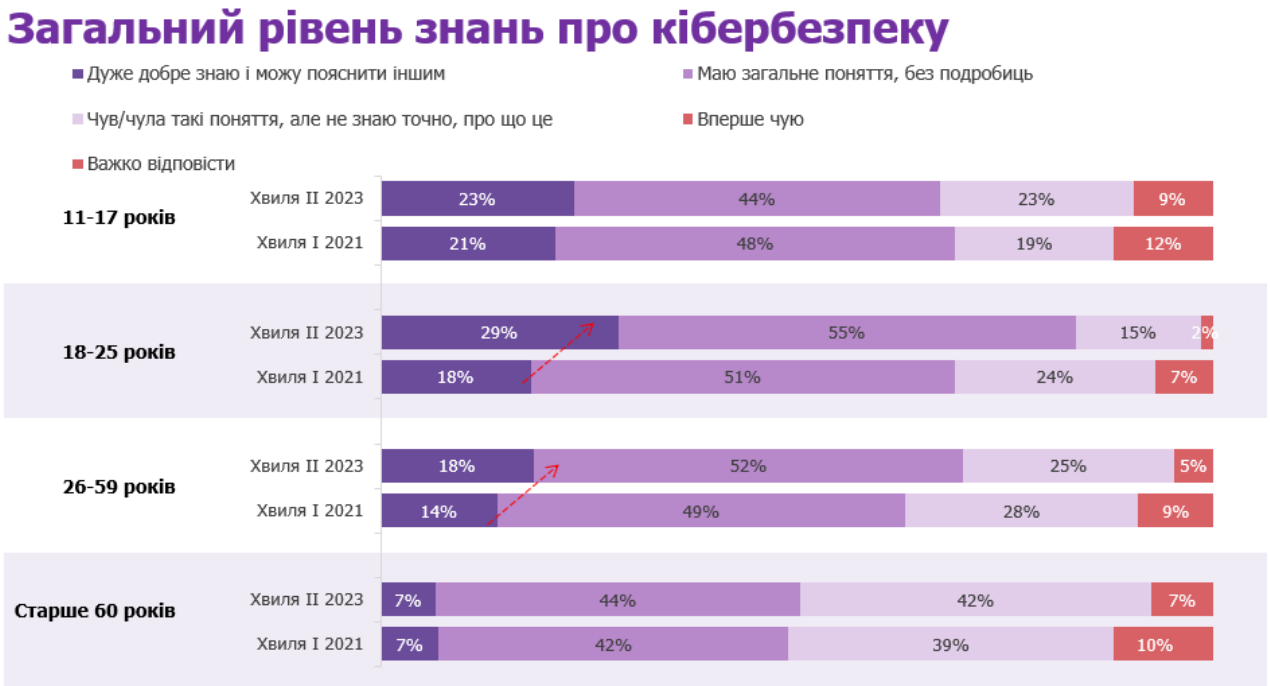


Аналогічна картина зберігається у розподілі за віковими групами: показники між загальною аудиторією і тими, хто пройшов навчання, різняться у 2-3 рази (див. Діаграма 7).

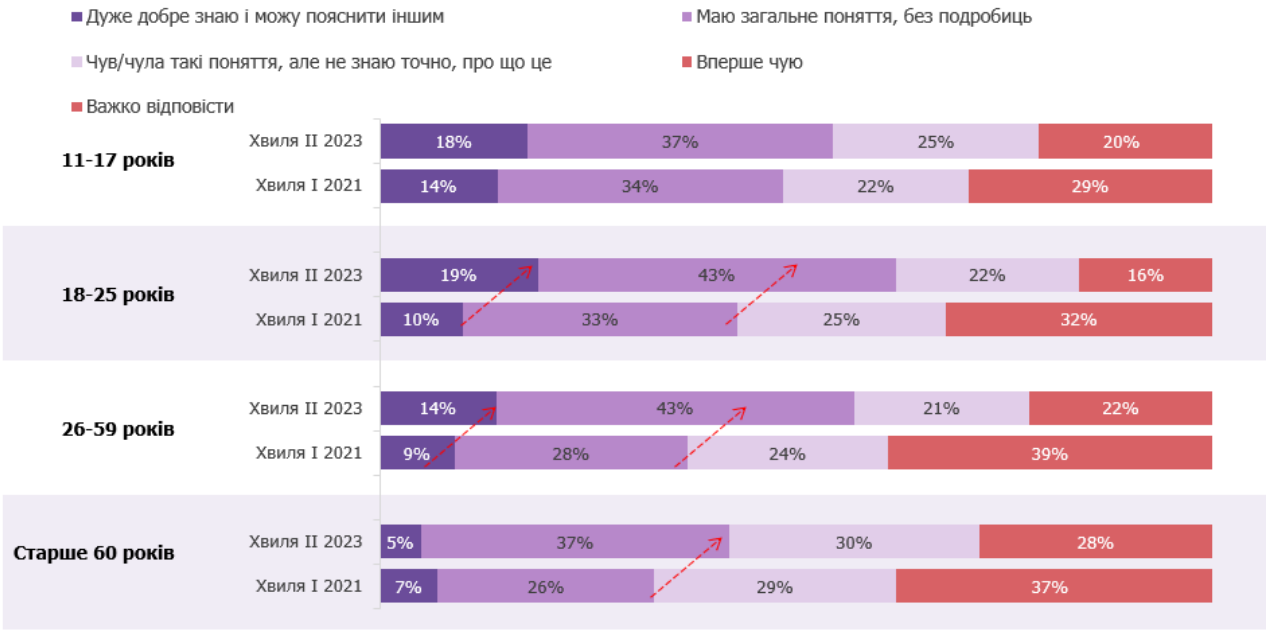
Діаграма 7. Скажіть, будь ласка, наскільки вам знайомі поняття «кібербезпека» та «правила кібергігієни»? Розподіл за цільовими групами (% відповідей, серед опитаних II хвилі та учасників навчань CRDF Global)



Діаграма 8.7 Скажіть, будь ласка, наскільки вам знайомі поняття «кібербезпека» та «правила кібергігієни»? Розподіл за цільовими групами (% відповідей, серед опитаних I та II хвилі)



Знання правил кібергігієни



Показники знання про кібербезпеку серед вікових груп 11-17 років та респондентів старше 60 років не дуже варіюють за результатами двох хвиль опитування, хоча спостерігається незначне збільшення частки відповіді «чув/чула такі поняття». Водночас, серед вікових груп 18-25 та 26-59 років зріс рівень відповідей «дуже добре знаю і можу пояснити іншим» (від 18% до 29% та від 14% до 18% відповідно). Дуже добре знання «правил кібергігієни» зросло серед усіх вікових груп, окрім опитаних старше 60 років (див. Діаграма 8).

Респонденти ФГД також вказували, що знання з кібербезпеки та кібергігієни є необхідними для будь-якого користувача цифровими пристроями, ці знання є настільки ж важливими, як правила дорожнього руху. Студенти та вчителі говорили про те, що основи знань вони отримують ще в школі, починаючи з молодших класів.

«Відбувається тотальна цифровізація суспільства, і увесь документообіг, уся документація міститься в електронному вигляді. …потрібно слідувати певним правилам для того, щоб оцю інформацію захистити. І тому правила кібергігієни – їх необхідно дотримуватись. …щоб не втратити свої дані, щоб ці дані не потрапили до рук людей, які можуть ними скористатись проти тебе або проти твоїх інтересів» (Студентка)

«…нам приходять листи вже перевірені в Департаменті кібербезпеки. Тому що зараз почастішали інформаційні атаки. …зараз тема дуже важлива, яка у всіх повинна бути на вустах» (Працівник державного сектору, головний лікар)

«Увесь свій час я впроваджував інформативну культуру, цифрову культуру серед своїх колег, тобто менеджерів закладу, району, громади, а також викладав інформатику дітям. Починаючи навіть від молодшого шкільного віку, в дітей є вже певні розуміння щодо кібербезпеки. Вони вже більш-менш обізнані із цими небезпеками і правилами. У них є намагання забезпечити певний рівень своєї конфіденційності. Але в водночас є фактичне нехтування тими правилами, тому що вони думають: «кому ми будемо такі цікаві?» (Вчитель)

Ризикована поведінка

У рамках даного дослідження було запропоновано оцінити кілька варіантів ризикованої поведінки в інтернеті. Респонденти відповідали, наскільки ці поведінкові шаблони схожі на їхню власну поведінку. Порівнюючи результати I хвилі 2021 року та поточної II хвилі 2023 року, беззмінними лідерами ризикованої поведінки є три шаблони:

- Відсутність резервних копій документів та даних (44% їх не роблять);
- Невикористання двофакторної автентифікації (44% не використовують);
- Впевненість, що користувач є нецікавим для інтернет-шахраїв (64% впевнені у цьому хоча б частково, 24% впевнені точно) (див. Діаграма 9Відсутність резервних копій документів та даних – 55%;
- Впевненість, що користувач є нецікавим для інтернет-шахраїв, – 44%;
- Невикористання двофакторної автентифікації – 37%.

Цікавим є порівняння відповідей на питання «Я відвідую російські сайти». 29% опитаних учасників навчань зазначають, що це «точно про мене» та «частково про мене», тимчасом як лише 18% опитаних II хвилі 2023 року зазначають аналогічне.

Щодо питання «Я можу вставити чужу флешку або незнайому флешку у свій комп'ютер» розрив у відповідях «точно про мене» та «частково про мене» серед учасників навчань CRDF Global та загального населення є двократним (47% та 24% відповідно) (див. Діаграма 10**Помилка! Неправильне посилання закладки.**).

Вчителі та студенти зазначають, що серед молоді та школярів було поширене використання російських сайтів, у тому числі в освітніх цілях. Через повномасштабне вторгнення використання російських ресурсів, як і російської мови, різко скоротилося серед молоді та школярів – спротив всьому російському є масовим трендом. Держслужбовці, представники ОМС зазначають, що і раніше рідко користувалися російськими, винятки – скачування необхідного, частіше неліцензійного програмного забезпечення, що також намагаються мінімізувати.

«Мене немає в російських соціальних мережах. Ще до повномасштабного вторгнення я інколи заходила на російські сайти виключно для того, щоб знайти необхідну літературу, в українському перекладі практично її не було. А в англійському все в закритому доступі, потрібно передплачувати. А російське було безкоштовне. Але зараз я все-таки дуже багато зусиль докладаю до того, щоб гуглити французькою, англійською це все. А на .ru я більше не заходжу» (Студентка)

«На жаль, у нас є дуже багато застарілої техніки, тому є потреба у якихось драйверах і так дальше. І доводиться скачувати на російських ресурсах… я застосовую VPN сервер, і відповідно через VPN сервер локалізую себе як користувача, умовно, російської федерації. І тоді скачую необхідний контент» (Працівник ОМС)

- *Діаграма 9. Я зачитаю кілька тверджень. Дайте відповідь, наскільки вони про вас?*).

Порівнюючи відповіді учасників навчань CRDF Global з відповідями респондентів II хвилі 2023 року, можемо говорити про те, що учасники навчань ретельніше уникають ризикованої поведінки в інтернеті і більше знають про небезпеку, яка може їх чекати. Тим не менше опитані учасники навчань CRDF Global зазначили, що їх «частково стосуються» такі ситуації:

- Відсутність резервних копій документів та даних – 55%;
- Впевненість, що користувач є нецікавим для інтернет-шахраїв, – 44%;
- Невикористання двофакторної автентифікації – 37%.

Цікавим є порівняння відповідей на питання «Я відвідую російські сайти». 29% опитаних учасників навчань зазначають, що це «точно про мене» та «частково про мене», тимчасом як лише 18% опитаних II хвилі 2023 року зазначають аналогічне.

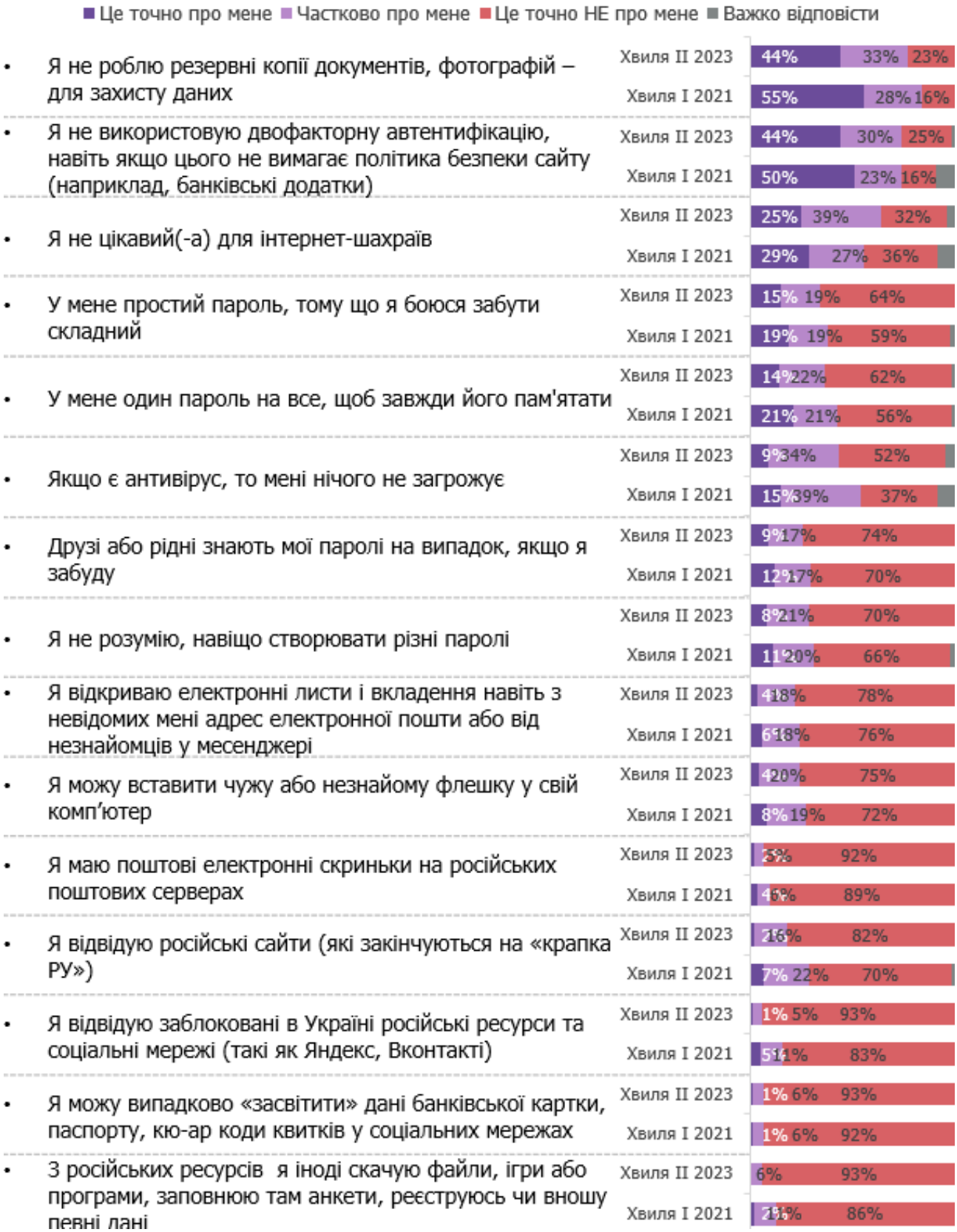
Щодо питання «Я можу вставити чужу флешку або незнайому флешку у свій комп'ютер» розрив у відповідях «точно про мене» та «частково про мене» серед учасників навчань CRDF Global та загального населення є двократним (47% та 24% відповідно) (див. Діаграма 10**Помилка! Неправильне посилання закладки.**).

Вчителі та студенти зазначають, що серед молоді та школярів було поширене використання російських сайтів, у тому числі в освітніх цілях. Через повномасштабне вторгнення використання російських ресурсів, як і російської мови, різко скоротилося серед молоді та школярів – спротив всьому російському є масовим трендом. Держслужбовці, представники ОМС зазначають, що і раніше рідко користувалися російськими, винятки – скачування необхідного, частіше неліцензійного програмного забезпечення, що також намагаються мінімізувати.

«Мене немає в російських соціальних мережах. Ще до повномасштабного вторгнення я інколи заходила на російські сайти виключно для того, щоб знайти необхідну літературу, в українському перекладі практично її не було. А в англійському все в закритому доступі, потрібно передплачувати. А російське було безкоштовне. Але зараз я все-таки дуже багато зусиль докладаю до того, щоб гуглити французькою, англійською це все. А на .ru я більше не заходжу» (Студентка)

«На жаль, у нас є дуже багато застарілої техніки, тому є потреба у якихось драйверах і так дальше. І доводиться скачувати на російських ресурсах… я застосовую VPN сервер, і відповідно через VPN сервер локалізую себе як користувача, умовно, російської федерації. І тоді скачую необхідний контент» (Працівник ОМС)

Діаграма 8. Я зачитаю кілька тверджень. Дайте відповідь, наскільки вони про вас? (% відповідей, серед опитаних I та II хвилі)



Діаграма 9. Я зачитаю кілька тверджень. Дайте відповідь, наскільки вони про вас? (% відповідей, серед опитаних II хвилі та учасників навчань CRDF Global)

Невикористання резервних копій і двофакторної автентифікації залишаються основними шаблонами ризикованої поведінки для всіх вікових груп. Для підлітків більше, ніж для решти аудиторій, характерна впевненість у тому, що вони не цікаві інтернет-шахраям: 38% впевнені у цьому, ще 28% частково впевнені (для порівняння: у I хвилі дослідження ці показники були на рівні 45% та 27% відповідно).

Також підлітки більшою мірою, ніж опитані загалом, впевнені у тому, що антивірус забезпечує повний захист.

Рівень використання одного-єдиного паролю для всіх випадків серед підлітків залишається вищим, аніж по вибірці загалом: 14% заявили, що цей шаблон поведінки повністю співпадає з їхнім (по вибірці загалом 9%). (див. Діаграма 11).

Вчителі підтверджують, що чим молодші діти, тим простіші у них паролі, також є тенденція створювати один пароль до різних акаунтів. Паролі молодших дітей можуть знати батьки, вони їх можуть передавати друзям. Старші діти більше опікуються питаннями конфіденційності, в старших класах діти більш свідомо ставляться до правил кібербезпеки. Загалом серед дітей поширене уявлення, що діти нецікаві кібершахраям, оскільки не мають банківських рахунків, не володіють фінансовими активами.

«Єдиний пароль – це є домінуюча поведінка щодо паролізації. Один пароль на все – їх правило. Єдине, що трошки радує, що діти набивають собі такий пароль, що треба непогано погратися пальцями, тобто навіть до 11 знаків, до 12 знаків і так далі. Але один на все» (Вчитель)

Діаграма 10. Я зачитаю кілька тверджень. Дайте відповідь, наскільки вони про вас? Розподіл за цільовою групою 11-17 років (% відповідей, серед опитаних I та II хвилі)

Молодь 18-25 років – залишається найбільш обережною цільовою групою з-поміж інших: вони з більшою регулярністю використовують двофакторну автентифікацію та роблять запасні копії документів і даних (а частка тих, хто цього не робить, майже удвічі менша, ніж по вибірці загалом). Важливою зміною є підвищення рівня використання двофакторної автентифікації серед даної вікової групи на 6 відсоткових пунктів у порівнянні з I хвилею 2021 року.

Також молодь меншою мірою погоджується з тим, що вони є нецікавими для інтернет-шахраїв (18% повністю погоджуються порівняно до 25% по вибірці загалом) (див. Діаграма 12).

«Я вважаю, що нецікавих людей для інтернет-шахраїв просто немає. Вони все зможуть використати, наприклад, твою сторінку в соціальних мережах будь-яким чином. Теж у знайомих був випадок, коли просто зламали сторінку і використовували її для реклами. Тому я відповім 100%, що я цікавий для всіх» (Студент)

Не можна не відзначити той факт, що хоча дана вікова група і відвідує російські сайти найчастіше, проте рівень відвідування удвічі зменшився: від 40% у I хвилі до 22% у II хвилі. Зауважимо, що серед підлітків динаміка цього показника становить 15% проти 23%, серед дорослих – 19% проти 28%, серед найстарших респондентів – 12% проти 24%.

Аналізуючи показники ризикованої поведінки вікової аудиторії 18-25 років у розрізі тих, хто проходив курси, варто звернути увагу, що хоча 10% відповіли на ситуацію «Я не роблю резервні копії документів, фотографій – для захисту даних» – «це точно не про мене», однак 62% зазначили що це «частково про мене». (див. Діаграма 13).

Також можна говорити про те, що учасники навчань CRDF Global віком від 18 до 25 років не приділяють достатньої уваги паролям. Так, 58% учасників навчань використовують так чи інакше один пароль (проти 28% серед відповідної вікової категорії респондентів II хвилі), щоб завжди його пам'ятати. 39% учасників навчань мають простий пароль, тому що я бояться забути складний (проти 16% серед респондентів II хвилі).

«Я знаю, що в мене проблема із паролями. В мене практично до всіх сторінок дуже або схожий, або зовсім однаковий пароль, що неправильно. Тому що я їх часто забуваю, і мені тоді доводиться дуже довго це відновлювати, і я зробила, що скрізь все однакове. Інколи, коли мені дуже потрібно знайти якусь інформацію, але вона знаходиться на сайті з незахищеним підключенням, я можу вимикати антивірус. Хоча я знаю, що це також робити не можна» (Студентка)

Діаграма 11. Я зачитаю кілька тверджень. Дайте відповідь, наскільки вони про вас? Розподіл за цільовою групою 18-25 років (% відповідей, серед опитаних I та II хвилі)

Діаграма 12. Я зачитаю кілька тверджень. Дайте відповідь, наскільки вони про вас? Розподіл за цільовою групою 18-25 років (% відповідей, серед опитаних II хвилі та учасників навчань CRDF Global)

Серед вікової групи 26-59 років понад половина опитаних у першій хвилі 2021 року (57%) не робили резервних копій документів та фотографій для захисту даних. У 2023 році цей показник зменшився на 13 відсоткових пунктів – до 44%.

«Резервні копії нерегулярно, але частково роблю. …багато робочої інформації, вона є в одному екземплярі, зараз активно використовую Гугл Диск. …якщо щось станеться з моїм комп'ютером, то в хмарі у мене все одно є документ. Тому зручно працювати з хмарними технологіями. Але поки що це рідко роблять, хтось досі зберігає інформацію на флешках і навіть на CD-дисках, які не є надійними носіями» (Працівник ОМС)

Майже половина (40%) опитаних даної вікової групи не використовують двофакторну автентифікацію, якщо цього не вимагає політика безпеки сайту, але загалом цей показник знизився на 8 відсоткових пунктів. Щодо паролів, то 14% опитаних мають простий пароль через страх забути складний пароль, а також 12% використовують один пароль на все для зручності (для порівняння: в 2021 році ці показники становили 19% та 20% відповідно) (див. Діаграма 14).

«…деякі паролі у мене є однакові, вони не від дуже важливих ресурсів. Але все-таки це моя вада… така звичка, все-таки це зручніше» (Працівник ОМС)

Прикметним є той факт, що переважна більшість (56%) тих, хто пройшов навчання CDRF Global у даній віковій групі, «можуть вставити чужу або незнайому флешку у свій комп'ютер» проти лише 26% опитаних даної вікової групи в II хвилі дослідження (див. Діаграма 15).

У фокус-групових обговореннях працівники державного сектору вказували, що досить часто продовжують користуватися флешками, і використання чужих флешок можливі і досить поширені. Інше порушення, що трапляється, – це передача даних цифрового підпису колегам задля скорочення процедури оформлення певних документів.

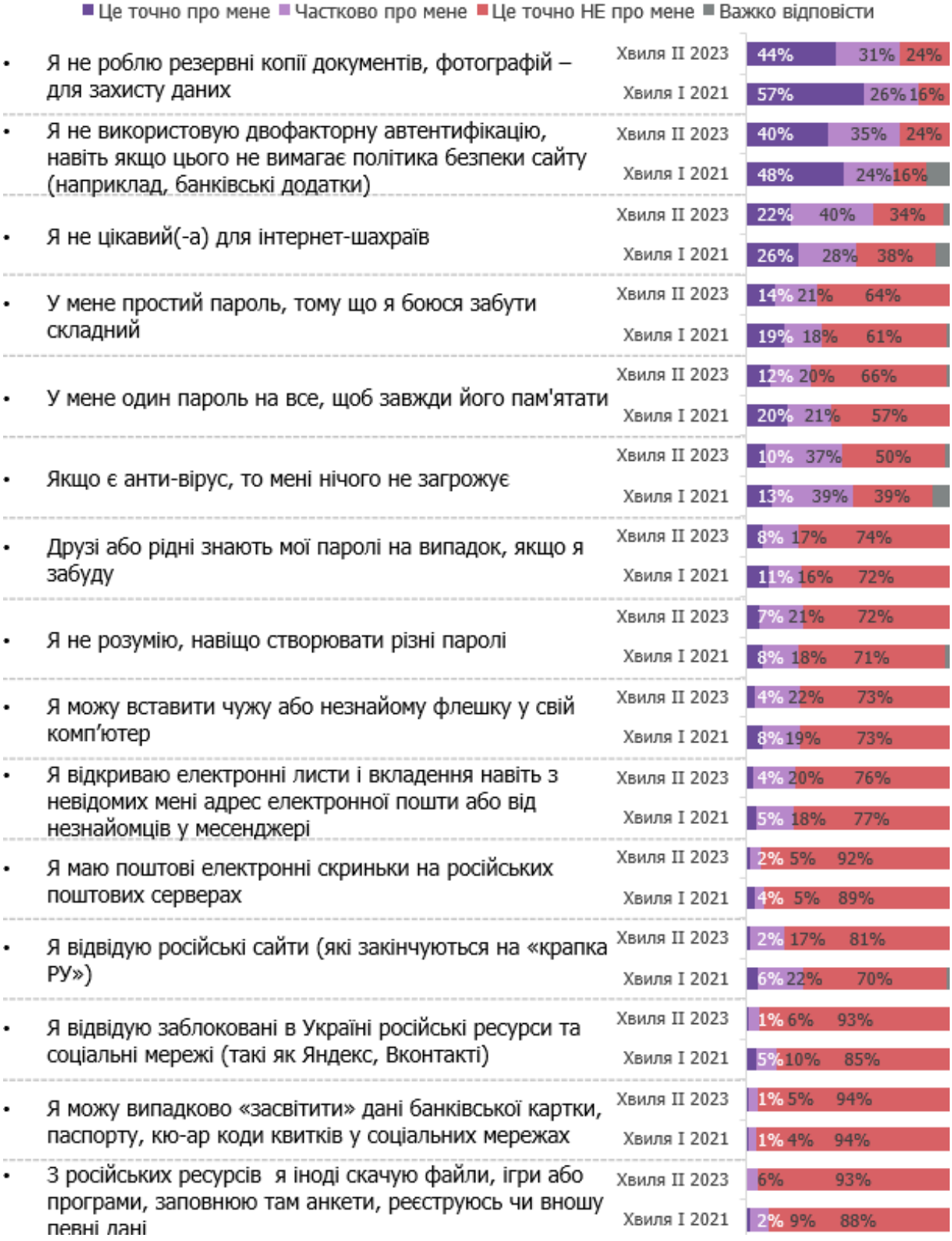
«Поширена ситуація, коли люди вважають – це флешки моїх знайомих, колег, але ж це чужі флешки. Бо ти не знаєш, де флешка була до цього. А проблема в тому, що не обов'язково людина свідомо принесе тобі вірус. Вона могла вставити свою флешку у заражений комп'ютер і принести тобі вірус. …не завжди робиш правильно. Я цього уникаю, але це поширено серед колег» (Фахівець органів освіти)

Невикористання двофакторної автентифікації залишається найбільш розповсюдженим шаблоном ризикованої поведінки серед найстаршої аудиторії (понад 60 років) порівняно з іншими віковими групами: 77% опитаних не використовують цей метод захисту. Прикметно, що даний показник зріс на 7% у порівнянні з минулою хвилею дослідження. Також люди найстаршого віку частіше за загальну аудиторію використовують один простий пароль та/або мають один пароль, щоб не забути.

Люди старшого віку, як і підлітки, часто (34%) зазначають, що вони не цікаві для інтернет-шахраїв. Старше покоління також частіше за інші вікові групи не розуміє, нащо створювати складні паролі (15% у порівнянні з 9% загалом по вибірці). Зауважимо, що цей показник знижується (в першій хвилі він становив 19% серед старшої групи та 12% по вибірці загалом), тож бачимо позитивну тенденцію.

Літні люди частіше діляться своїми паролями з друзями або рідними: 21% повністю підтримує цей поведінковий шаблон, 16% – підтримує частково (для порівняння, по вибірці загалом ці показники становлять 12% і 17% відповідно) (див. Діаграма 16).

Діаграма 13. Я зачитаю кілька тверджень. Дайте відповідь, наскільки вони про вас? Розподіл за цільовою групою 26-59 років (% відповідей, серед опитаних I та II хвилі)



Діаграма 14. Я зачитаю кілька тверджень. Дайте відповідь, наскільки вони про вас? Розподіл за цільовою групою 26-59 років (% відповідей, серед опитаних II хвилі та учасників навчань CRDF Global)

Діаграма 15. Я зачитаю кілька тверджень. Дайте відповідь, наскільки вони про вас? Розподіл за цільовою групою старше 60 років (% відповідей, серед опитаних I та II хвилі)

Респонденти, що брали участь у ФГД та ГІ, також підтвердили, що нерідко мають доступ до акаунтів та пристроїв своїх старших родичів, оскільки опікуються безпекою і можуть допомагати їм з тих чи інших питань. Зокрема, респонденти встановлюють паролі на їхні пристрої, відтак володіють цією інформацією.

Безперечно, окремим видом ризикованої поведінки залишається користування російськими поштовими скриньками, відвідування заблокованих в Україні російських ресурсів та соціальних мереж, а також відвідування російських сайтів та здійснення певних дій на них, як-от завантаження з них файлів, заповнення анкет, реєстрація, особливо в контексті подій сьогодення.

Наразі помітне зменшення відвідування російських сайтів. Наразі такі практики застосовують 18% опитаних, а у попередній хвилі дослідження цей показник був на рівні 30%. Показники відвідування російських сайтів у розрізі вікових груп у порівнянні до попередньої хвилі є такими:

- 15% серед підлітків 11-17 (23% у I хвилі дослідження);
- 22% серед молоді 18-25 (40% у I хвилі дослідження);
- 19% серед дорослих 26-59 (28% у I хвилі дослідження);
- 12% серед літніх 60+ (24% у I хвилі дослідження).

Утім, можемо припустити, що двократне зменшення рівня користування серед літніх людей може пояснюватися тим, що наразі російські ресурси та сайти є заблокованими, а користуватись сервісом VPN, який надає змогу заходити на російські домени, вони не навчились.

Також відвідування заблокованих в Україні російських ресурсів та соціальних мереж помітно зменшилось серед вікової категорії молоді 18-25 (більше ніж утричі: з 29% до 8%) та серед дорослих 26-59 (більше ніж удвічі, з 15% до 7%).

Підлітки частіше за інші групи завантажують з російських ресурсів файли, програми, проходять реєстрацію. Частка респондентів з такою поведінкою серед цієї групи становить 16%, у решти груп (молодь, дорослі та літні) така поведінка притаманна вдвічі рідше (7%, 6% та 4% відповідно).

Наразі очевидне зниження рівня користування російськими поштовими скриньками серед респондентів 18-25 років (з 17% в 2021 році до 10% у 2023 році) та підлітків 11-17 років (з 13% у 2021 році до 6% у 2023 році).

Досвід зіткнення із кіберзагрозами

Ми запропонували респондентам оцінити свій досвід зіткнення із кіберзагрозами для моніторингу ситуації та проведення порівняльного аналізу з даними попередньої хвилі дослідження 2021 року. Кожній цільовій групі було запропоновано окремий перелік кіберзагроз, які, на думку експертів, притаманні саме цій віковій групі; щодо кожної кіберзагрози респонденти могли позначити, чи траплялася така ситуація з ними особисто або з їхніми реальними або віртуальними знайомими.

Перше місце у вибірці загалом наразі посіла ситуація, коли кібершахраї вимагають дані банківських карток, паролі та доступ до облікових записів мобільних додатків. Друге місце посідає ситуація, що була лідером минулого разу, – вимагання грошей з використанням методів соціальної інженерії (маніпуляції, погрози, шантаж), а також особистих та родинних даних (через телефон та месенджери). Першу ситуацію оцінювала доросла аудиторія 26-59 років та літні респонденти 60+, а другу ситуацію оцінювали лише літні люди (див. Діаграма 17).

Серед респондентів, які брали участь у навчанні від CRDF Global, ТОП-3 ситуаціями, що траплялись з ними або з їхніми знайомими, є такі (див. Діаграма 18):

- Крадіжка (злам) облікових записів у соціальних мережах;
- Крадіжка (злам) ігрових акаунтів у комп'ютерних іграх.

Учасники фокус-груп трохи знаються на механізмах таких зламів:

«Ніхто тобі не буде писати «дай мені свою електронну адресу» через те, що людина одразу буде заблокована. Але якимись маніпуляціями намагались спочатку набити собі авторитет певний. Після цього просити вже твої дані. Деякі з моїх знайомих, в котрих була така ситуація, через необачність ці дані надали… більш прошарені питають пошту. І після цього вже підбирають пароль, майже все зараз робиться через пошту. Потім завантажують базу паролів, і підбирають його. ..дуже важливо не передавати паролі в жодному разі, і створювати саме складний пароль, який довго можна підбирати» (Студентка)

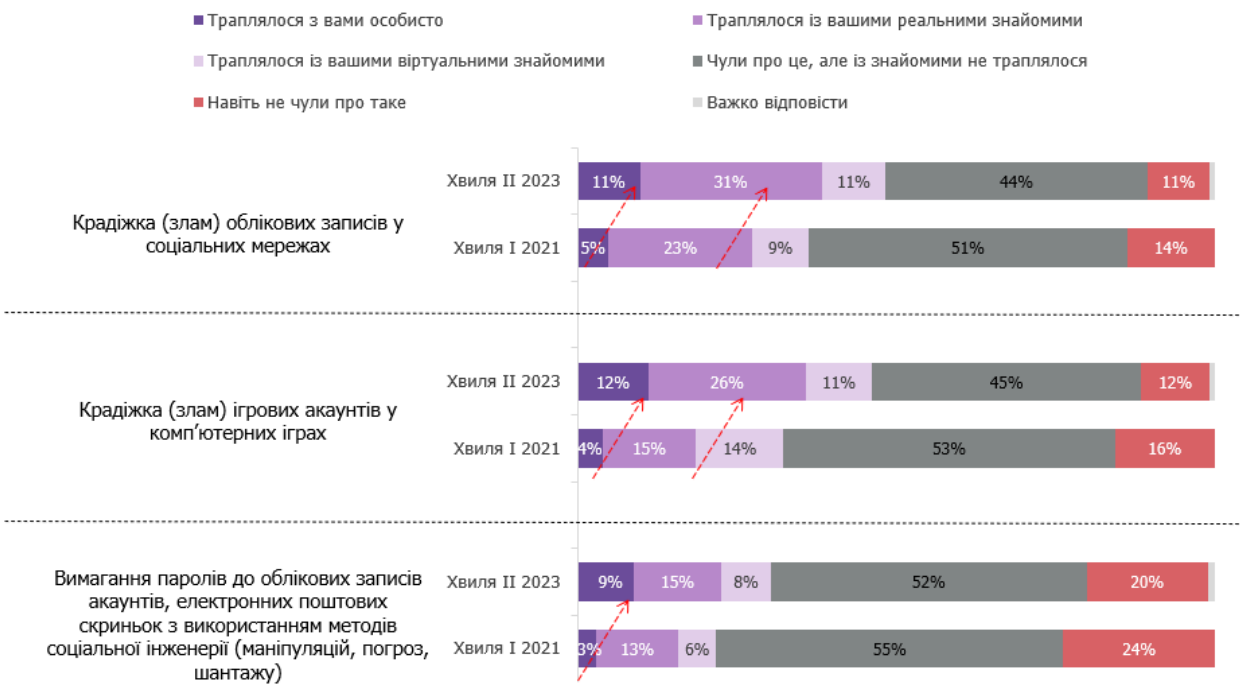
Діаграма 16. Я зачитаю списки основних загроз, які можуть спіткати користувача інтернету, а ви скажіть, чи стикалися ви особисто або ваші знайомі з такою ситуацією? (% відповідей, серед опитаних I та II хвилі)

Діаграма 17. Я зачитаю списки основних загроз, які можуть спіткати користувача інтернету, а ви скажіть, чи стикалися ви особисто або ваші знайомі з такою ситуацією? (% відповідей, серед опитаних II хвилі та учасників навчань CRDF Global)

Підлітки найчастіше наразі стикаються із крадіжкою ігрових акаунтів у комп'ютерних іграх. Цей показник загалом зріс на 15 відсоткових пунктів, якщо порівнювати з I хвилею опитування та брати до уваги ситуації, що траплялись не тільки з учасниками опитування, а й з їх знайомими. Беручи до уваги загальну картину серед даної вікової групи, доходимо висновку, що всі ситуації стали більш дотичними безпосередньо до опитаних респондентів (див. Діаграма 19)**Помилка! Джерело посилання не знайдено.**.

«…з мого спостереження, найчастіше – це є зломи соціальних мереж, власних акаунтів дітей. Далі – це є зломи за безцінь куплених ігрових акаунтів. Тобто діти часто купують за безцінок в лапках роздутий акаунт, що в ньому нібито вже є бонуси. На того, щоб грати потім в мережі і все решта. Так у мого сина відбувається, в нього кожні декілька днів зламують акаунти, бо він купує собі дешеві акаунти в деяких іграх» (Вчитель)

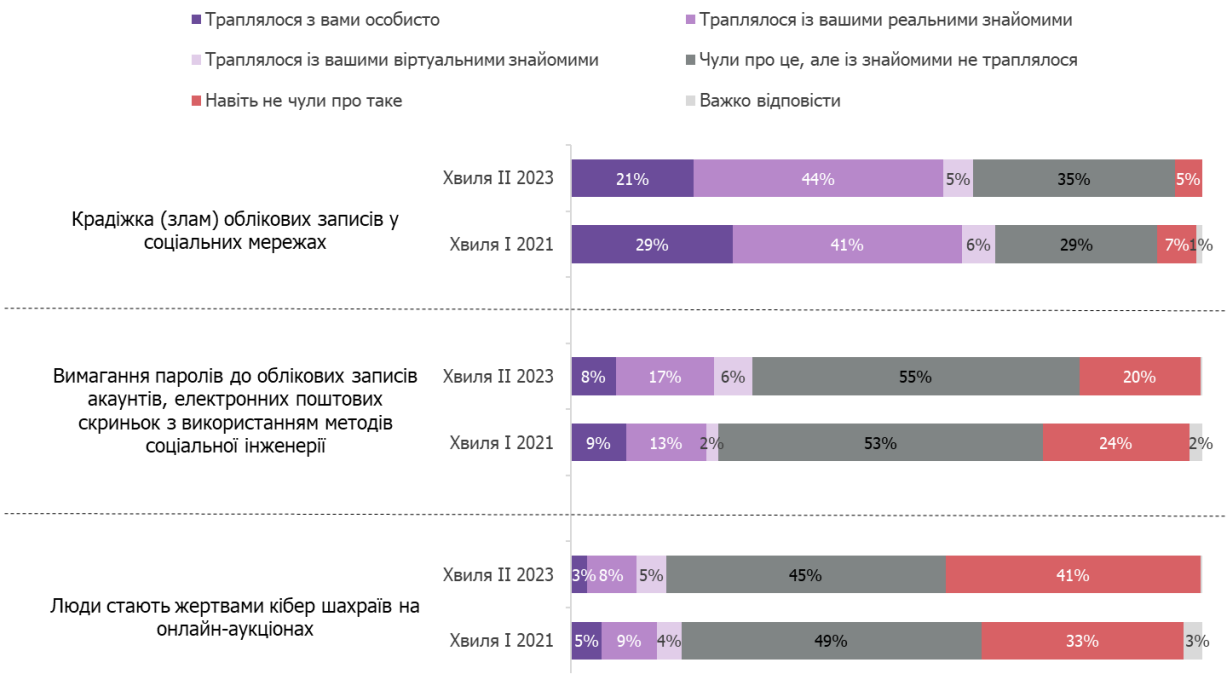
Діаграма 18. Я зачитаю списки основних загроз, які можуть спіткати користувача інтернету, а ви скажіть, чи стикалися ви особисто або ваші знайомі з такою ситуацією? Розподіл за цільовою групою 11-17 років (% відповідей, серед опитаних I та II хвилі)



Утім, найчастіше від усіх інших аудиторій із крадіжкою облікових записів у соціальних мережах продовжує стикатись молодь віком 18-25 років. Цей показник хоч і зменшився з 29% до 21%, проте залишається найвищим серед інших вікових груп (див. Діаграма 20).

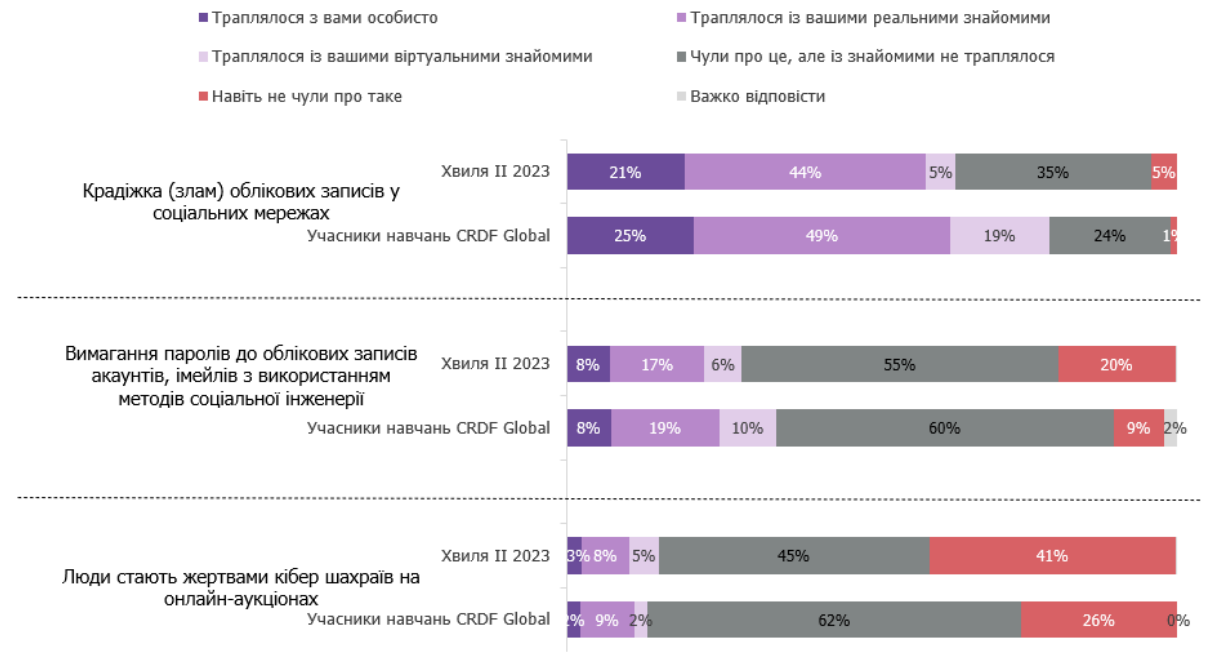
«Здебільшого я дотримуюсь майже усіх правил кібергігієни через те, що в мене був дуже негативний досвід. …сталась така ситуація, що я просто встиг перехопити доступ до свого Гугл акаунту, після цього я повністю змінив усі паролі» (Студент)

Діаграма 19. Я зачитаю списки основних загроз, які можуть спіткати користувача інтернету, а ви скажіть, чи стикалися ви особисто або ваші знайомі з такою ситуацією? Розподіл за цільовою групою 18-25 років (% відповідей, серед опитаних I та II хвилі)



Респонденти цієї вікової групи, які брали участь у навчанні від CRDF Global, стикались з кіберзагрозами так само часто, як і респонденти II хвилі опитування (див. Діаграма 21).

Діаграма 20. Я зачитаю списки основних загроз, які можуть спіткати користувача інтернету, а ви скажіть, чи стикалися ви особисто або ваші знайомі з такою ситуацією? Розподіл за цільовою групою 18-25 років (% відповідей, серед опитаних II хвилі та учасників навчань CRDF Global)



Для аудиторії віком 26-59 років найбільш розповсюдженою загрозою є вимагання банківських даних, паролів та доступу до облікових записів банківських мобільних додатків, банківських рахунків (у т.ч. через телефон, месенджери): кожен четвертий стикався з цим особисто, 28% знають про такі випадки від знайомих. Також поширеними залишаються випадки вимагання особистих даних, злам облікових записів у соціальних мережах та вимагання грошей задля розблокування роботи комп'ютерних систем (частка аудиторії, яка стикалася з цими ситуаціями особисто, становить 16%, 14% та 13% відповідно). Розповсюдженість цих кіберзагроз майже не змінилась з 2021 року (див. Діаграма 22).

«В мене особисто не було випадків шахрайств, але у знайомих так – зламувалась сторінка у Фейсбуці. …так само розсилка була, повідомлення, що потрібні кошти, перерахуйте... Також були дзвінки від шахраїв, що представлялися працівниками банку, але не вказували якого і просили надати дані карток» (Працівник ОМС)

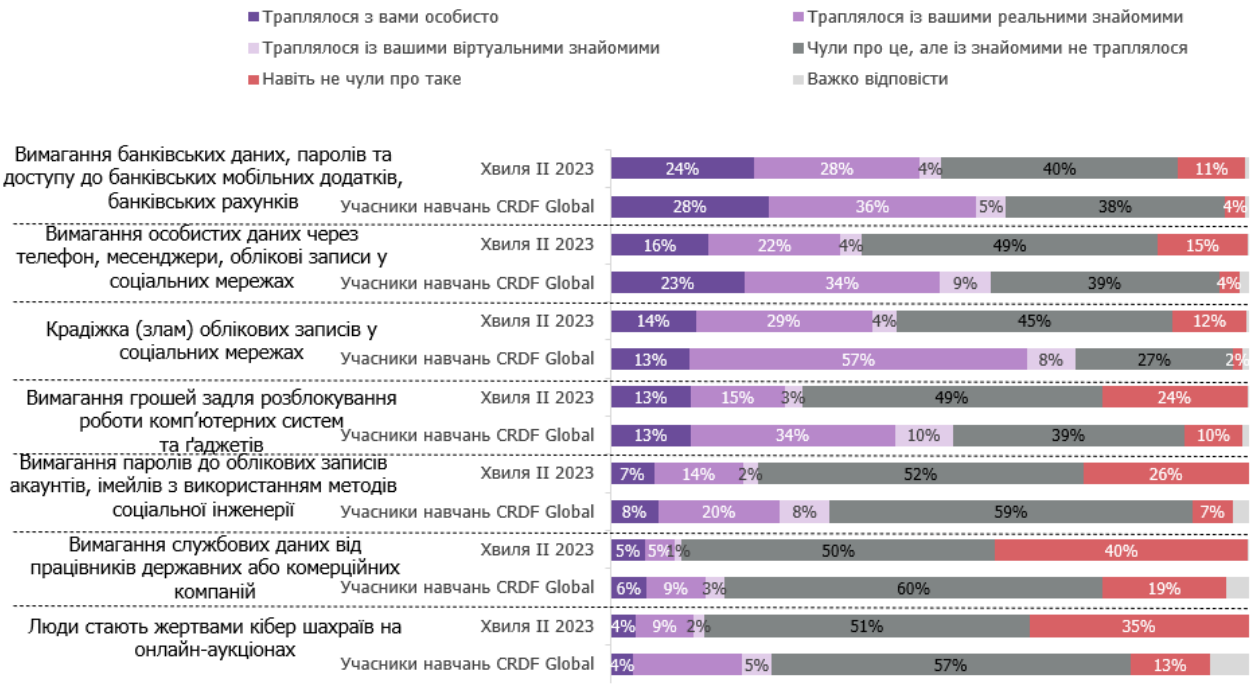
Діаграма 21. Я зачитаю списки основних загроз, які можуть спіткати користувача інтернету, а ви скажіть, чи стикалися ви особисто або ваші знайомі з такою ситуацією? Розподіл за цільовою групою 26-59 років (% відповідей, серед опитаних I та II хвилі)

При аналізі відповідей учасників навчання CRDF Global спостерігалася значна різниця: серед «віртуальних знайомих» опитаних респондентів таких ситуацій більше, аніж серед знайомих респондентів II хвилі. Зокрема, це стосується таких ситуацій (див. Діаграма 23):

- Крадіжка (злам) облікових записів у соціальних мережах – 57%
- Вимагання банківських даних, паролів та доступу до банківських мобільних додатків, банківських рахунків – 36%
- Вимагання особистих даних через телефон, месенджери, облікові записи у соціальних мережах – 34%
- Вимагання грошей задля розблокування роботи комп'ютерних систем та ґаджетів – 34%

Ймовірним поясненням може бути те, що учасники навчань можуть звертати більшу увагу на такі ситуації і частіше обговорювати їх із знайомими.

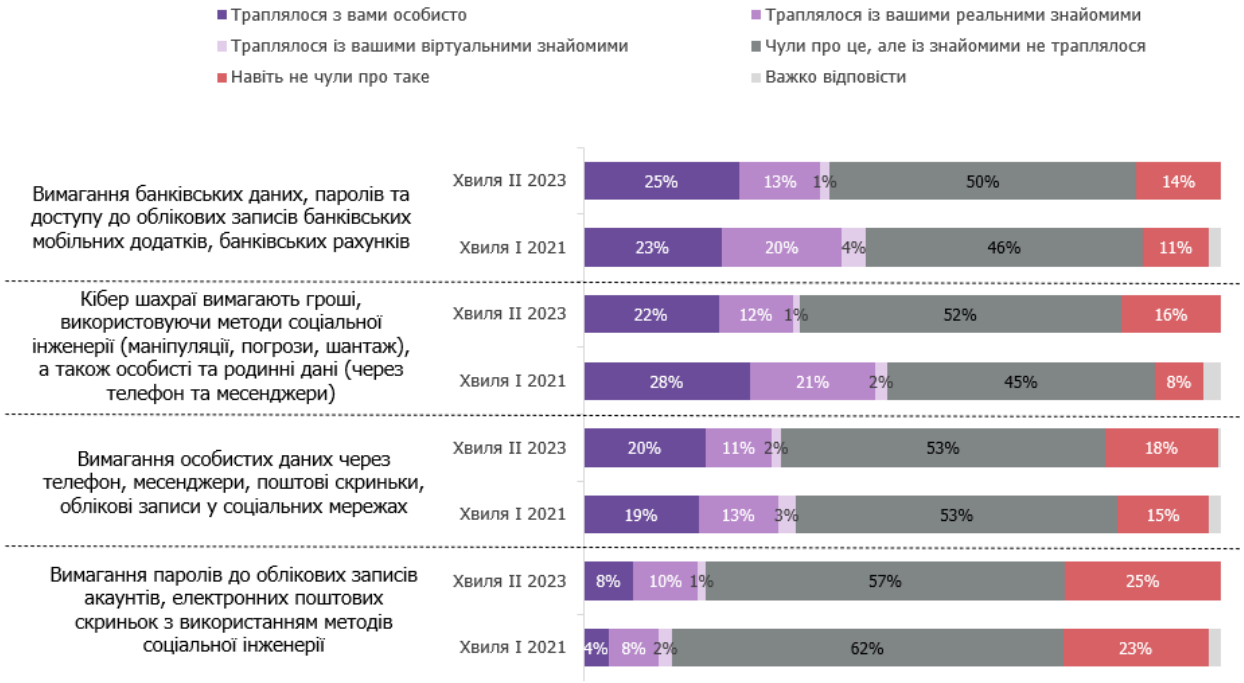
Діаграма 22. Я зачитаю списки основних загроз, які можуть спіткати користувача інтернету, а ви скажіть, чи стикалися ви особисто або ваші знайомі з такою ситуацією? Розподіл за цільовою групою 26-59 років (% відповідей, серед опитаних II хвилі та учасників навчань CRDF Global)



Літні люди продовжують стикатися із кіберзагрозами частіше за інші аудиторії. Так, із вимаганням даних банківських карт, паролів та доступу до облікових записів банківських мобільних додатків та банківських рахунків особисто стикалися 25% опитаних даної вікової групи. Ситуації, коли кібершахраї вимагають гроші, використовуючи методи соціальної інженерії (маніпуляції, погрози, шантаж), а також особисті та родинні дані (через телефон та месенджери), траплялись особисто із 22% опитаних (див. Діаграма 24).

«*Вимагали кошти у моїх батьків вночі за звільнення мене з поліції. Це дуже часте шахрайство, коли старшим людям телефонують і кажуть, що щось трапилося з їхньою дитиною. Моїм батькам здалося, що голос схожий на мій, але все-таки вони передзвонили мені, а буває, що люди переказують кошти» (Працівник ОМС)*

Діаграма 23. Я зачитаю списки основних загроз, які можуть спіткати користувача інтернету, а ви скажіть, чи стикалися ви особисто або ваші знайомі з такою ситуацією? Розподіл за цільовою групою старше 60 років (% відповідей, серед опитаних I та II хвилі)



Обізнаність із правилами кібербезпеки

У рамках даного дослідження також піднімалися питання базових правил кібергігієни. Ми надали аудиторії можливість оцінити ставлення до базових правил кібергігієни для моніторингу ситуації та відслідковування тенденцій. Серед ТОП-3 базових, найбільш вживаних правил кібергігієни залишаються:

- Не можна відправляти фото та скани особистих банківських карток та документів незнайомцям та сумнівним організаціям (89%);
- Не можна залишати пристрій без нагляду, коли він працює у публічних місцях (86%);
- Не варто відправляти контактні телефони, особисті фото незнайомцям, особливо тим, які просять оголені фотографії (83%).

З більшістю правил аудиторія обізнана (див. Діаграма 25).

Учасники курсів CRDF Global ознайомлені з усіма правилами кібербезпеки краще, ніж населення України. Однак учасники курсів дотримуються не всіх правил, зокрема:

- Не підключайтеся до загальнодоступних, невідомих або незахищених мереж Wi-Fi;
- За будь-якої підозри зараження свого пристрою або компрометації даних НЕГАЙНО повідомте відповідні органи (Кіберполіція України тощо) (див. Діаграма 26).

Респонденти на ГІ і ФГД говорили про те, що не вірять в ефективність дій кіберполіції, тому переважно не розглядають опцію звернення до спеціалізованих органів у разі порушень. Усі респонденти знають, що кіберполіція існує, але здебільшого не вважають за потрібне

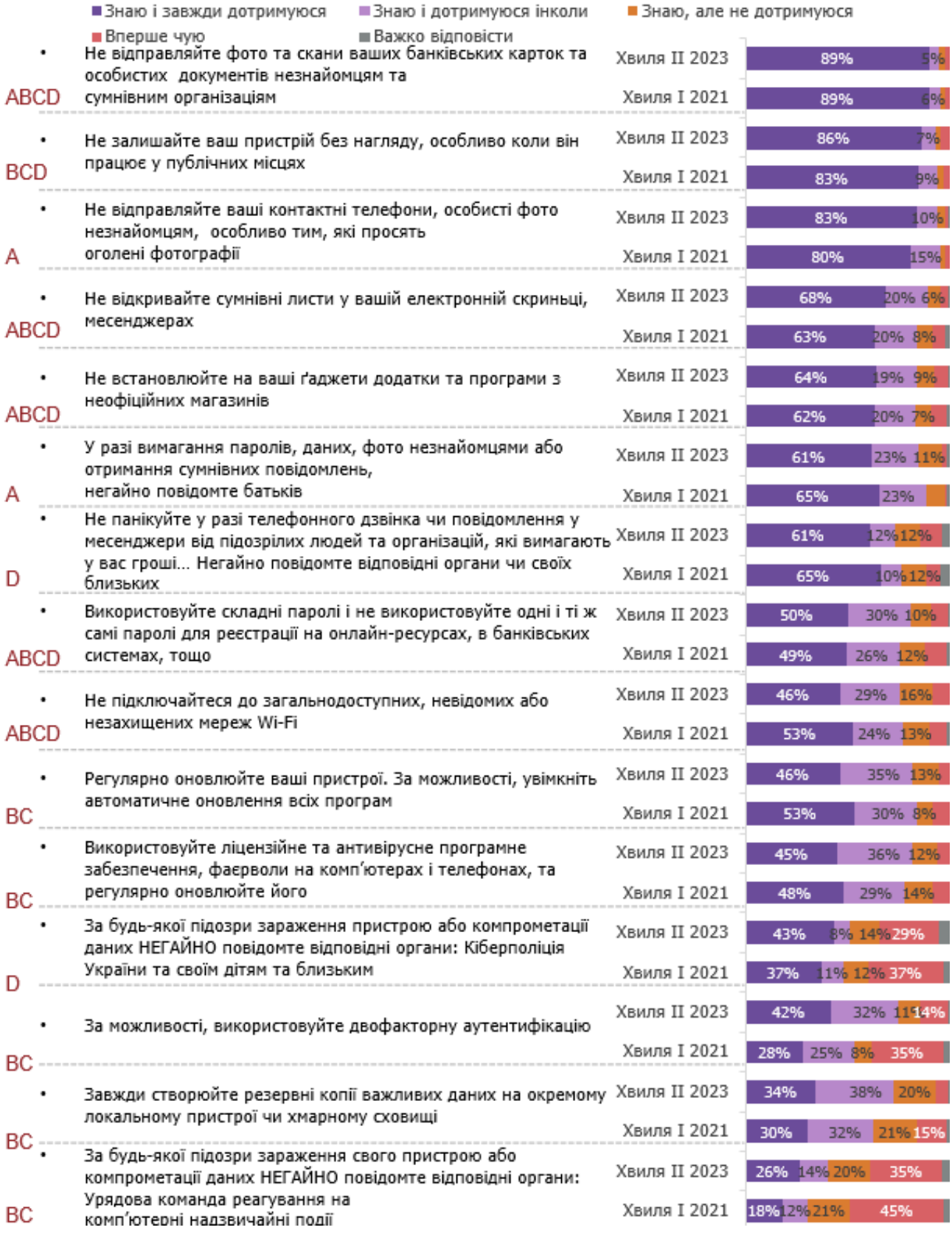
звертатися до неї у випадку незначних шахрайств, як-от злам акаунту чи дзвінок шахраїв. Окремі респонденти мали негативний досвід звернення в кіберполіцію, коли їхня заява не була розглянута. Водночас респонденти вказували, що є випадки успішних розслідувань, які одначе відбувалися під значним тиском та в фокусі уваги людей, що зверталися в органи. Респонденти з державного сектору вважають, що кіберполіція поступово набуває досвіду протистояння різним атакам, шахрайствам та вчиться розслідувати такі випадки, особливо це актуально під час війни та кіберзагроз, що йдуть від рф.

«…в поліції мені сказали, що у них є важливіші справи. У мене було таке жахливе розчарування, бо тут конкретно говорять про страшні речі, невідомо що за цим стоїть, може, там людей виловлюють і убивають у прямому ефірі, це закрита група, і мені чомусь прийшло це запрошення. Я відчувало таку відповідальність, що я повинна про це повідомити. В результаті вони зробили з цього невідомо що» (Студентка)

«Було жорстке переслідування. Потім виявилося, що цей аферист вже мав два рецидиви такого плану. Факт розслідування в моєму досвіді є, я його спостерігав. Але факт рішення проблеми, він настільки був тривалий і настільки, розумієте, слабенький, що захист життя від кіберзлочинів – про це не йдеться … особисто моя така думка, що не дай Боже комусь… навряд чи я звертався би до них як за єдиною допомогою. Можливо, зараз, на цьому етапі, коли війна, трошки їм хвоста підпалили, нашим же службам, щоб вони трошки заметушилися» (Вчитель)

«Про кіберполіцію я чув, звісно. …коли працював на державній службі, то були в нас перевірки також і від СБУ, і від Держспецзв'язку, перевіряли дотримання саме вимог кібербезпеки. Особисто мене не перевіряли, але в нас була людина, системний адміністратор. Але про перевірки ці знаю. Тому, думаю, що відповідні органи працюють, зараз у них більше роботи. Інша справа, наскільки може до них звернутися пересічна людина з тими питаннями, які ми з вами обговорювали, чи буде реакція на таке звернення» (Працівник ОМС)

Діаграма 24. Я зачитаю кілька базових правил кібергігієни, а ви скажіть, наскільки ви особисто обізнані з цим правилом? (% відповідей, серед опитаних I та II хвилі)
(A – 11-17 років; B – 18-25 років; C – 26-59 років; D – старше 60 років)



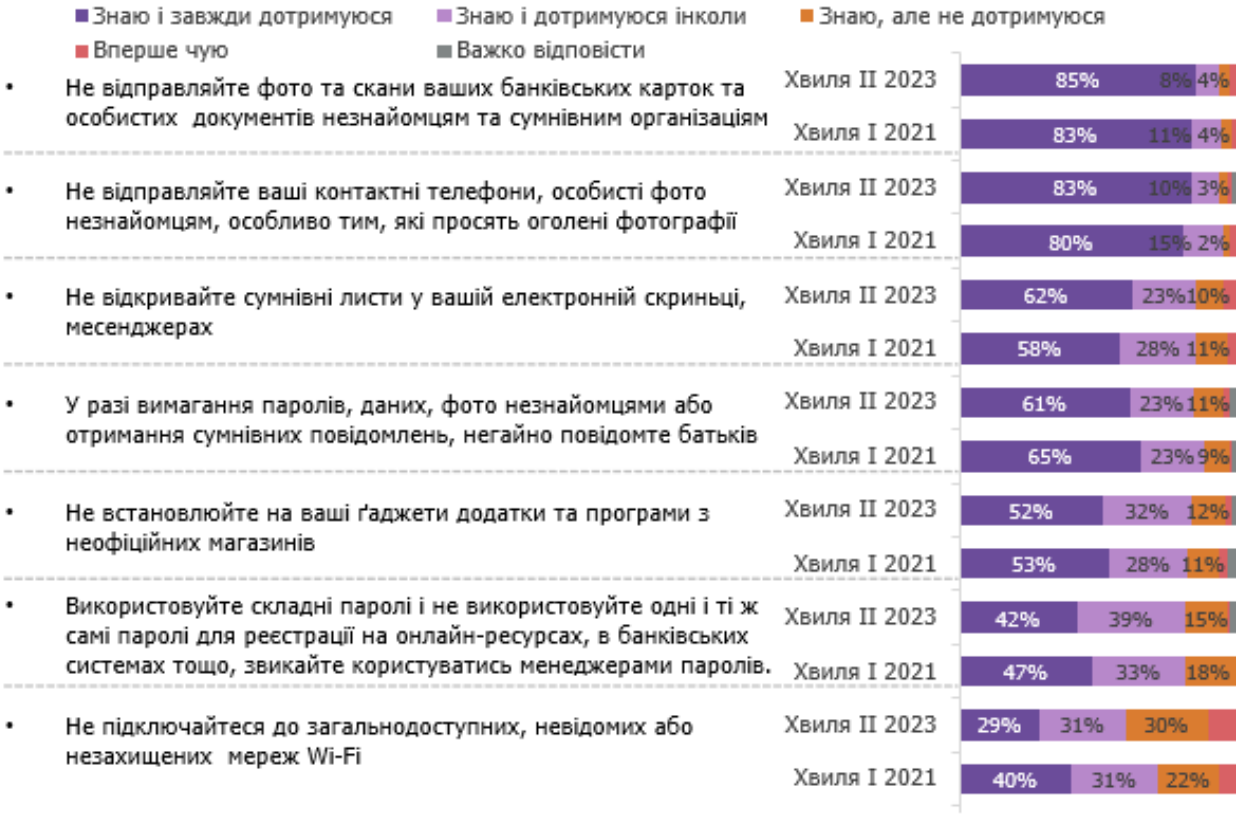
Діаграма 25. Я зачитаю кілька базових правил кібергігієни, а ви скажіть, наскільки ви особисто обізнані з цим правилом? (% відповідей, серед опитаних II хвилі та учасників навчань CRDF Global)
(A – 11-17 років; B – 18-25 років; C – 26-59 років; D – старше 60 років)

Підлітки досить добре обізнані із усіма правилами. Частка респондентів в цій аудиторії, які знають кожне правило і завжди їх дотримуються, перевищує 50% для всіх правил, окрім двох, а саме:

- Використання складних паролів і невикористання одних і тих самих паролів для реєстрації на онлайн-ресурсах, в банківських системах тощо – 42% сказали, що знають та дотримуються правил;
- Не підключайтеся до загальнодоступних, невідомих або незахищених мереж Wi-Fi – 29% зазначили, що знають та дотримуються правил.

«Дуже важко дітям та старшим людям мого віку припинити використовувати безкоштовний сервіс. Знаєте, яке є прислів'я? Що безкоштовний сервіс – в мишоловці. Це дуже поширено, навіть в нашому невеликому місті є багато можливостей скористатися безкоштовним Wi-Fi, і люди його використовують, не задумуючись про ризики» (Вчитель)

Діаграма 26. Я зачитаю кілька базових правил кібергігієни, а ви скажіть, наскільки ви особисто обізнані з цим правилом? Розподіл за цільовою групою 11-17 років (% відповідей, серед опитаних I та II хвилі)



Молодь 18-25 років також непогано знайома із більшістю запропонованих правил, хоча має дещо нижчий рівень обізнаності із шістьма останніми за рейтингом правилами, аніж підлітки. Правило щодо необхідності повідомляти відповідні органи за підозри зараження або компрометації даних мало знайоме респондентам: 36% сказали, що вперше чують про таке правило (для порівняння, у попередній хвилі цей показник був на рівні 42%). Другим за рівнем поганої обізнаності є правило щодо використання двофакторної автентифікації: 5% вперше чують про це (показник становив 15% у I хвилі дослідження).

Безперечно, молодь 18-25 років стала більше знати та частіше дотримуватись правила не відкривати сумнівні листи у електронній скриньці та месенджерах; про це говорить ріст показника на 13 відсоткових пунктів – до рівня 70% (див Діаграма 28).

«В 21 році десь восени я тільки вступила в університет. І почалась на корпоративну пошту всім-всім студентам якась дивна розсилка, якийсь лист там щось з якимось лінком. І хтось почав заходити, і там щось почалось в когось ламатись. І потім через якийсь час (дуже швидко це все відбувалось) прийшов лист від адміністрації, що ось не відкривайте незнайомі листи, в нас стався шахрайський напад, розіслали браковані листи. І тому ти розумієш, що навіть корпоративній пошті ти не можеш довіряти. Хоча, здавалось би, що це най-найбезпечніший ресурс» (Студентка)

«…мені досить довгий час приходили на пошту листи, але там була відверта абракадабра. Просто якийсь набір незрозумілих символів, вони приходили буквально кожен божий день. Я їх не могла викинути в спам, тому що були різні джерела. Я взагалі не розумію, для чого це робити, і кому це було потрібно. Але такий випадок був – очевидно, я лишила свою пошту, і хтось вирішив цим скористатись. Але я за жодних обставин не відкривала» (Студентка)

Правило щодо використання складних і різних паролів досить добре знають 91% опитаних, однак завжди його дотримуються лише 56%, що на 8 відсоткових пунктів менше, аніж у I хвилі дослідження. Однак цей показник парадоксально вищий, ніж у респондентів даної вікової групи, що пройшли навчання CRDF Global (43%) (див. Діаграма 29).

Більше половини аудиторії 26-59 років також знають і завжди дотримуються правила про складні паролі. Даний показник на загальній вибірці є вищим, ніж у I хвилі дослідження (див. Діаграма 30), але нижчим у порівнянні з тими, хто пройшов навчання CRDF Global (див. Діаграма 31).

Діаграма 27. Я зачитаю кілька базових правил кібергігієни, а ви скажіть, наскільки ви особисто обізнані з цим правилом? Розподіл за цільовою групою 18-25 років (% відповідей, серед опитаних I та II хвилі)

Діаграма 28. Я зачитаю кілька базових правил кібергігієни, а ви скажіть, наскільки ви особисто обізнані з цим правилом? Розподіл за цільовою групою 18-25 років (% відповідей, серед опитаних II хвилі та учасників навчань CRDF Global)

Діаграма 29. Я зачитаю кілька базових правил кібергігієни, а ви скажіть, наскільки ви особисто обізнані з цим правилом? Розподіл за цільовою групою 26-59 років (% відповідей, серед опитаних I та II хвилі)

Діаграма 30. Я зачитаю кілька базових правил кібергігієни, а ви скажіть, наскільки ви особисто обізнані з цим правилом? Розподіл за цільовою групою 26-59 років (% відповідей, серед опитаних II хвилі та учасників навчань CRDF Global)

Респонденти найстаршого віку залишаються все такими ж уважними та обережними. Вони знають про небезпеку щодо відправки фото та сканів банківських карток або документів незнайомцям (89% дотримуються правила цього не робити), 79% не залишає пристрій без нагляду (див. Діаграма 32).

Утім, найстарші респонденти часто (26%) навіть не знають про правило безпечного користування паролями; щодо динаміки: збільшилась частка відповіді «вперше чую» та зменшилась частка відповідей «знаю та завжди дотримуюсь» на 3 та 5 відсоткових пунктів відповідно.

Діаграма 31. Я зачитаю кілька базових правил кібергігієни, а ви скажіть, наскільки ви особисто обізнані з цим правилом? Розподіл за цільовою групою старше 60 років (% відповідей, серед опитаних I та II хвилі)

Для порівняння, наскільки кожна вікова група знає і виконує правила кібербезпеки та наскільки дані показники змінились із плином часу, ми порахували кілька інтегральних показників:

- Знають усі правила кібербезпеки;
- Застосовують усі правила кібербезпеки хоча б іноді;
- Завжди застосовують усі правила кібербезпеки.

За результатами аналізу цих інтегральних показників, підлітки 11-17 років залишаються найбільш обізнаною групою: 81% знають усі правила кібербезпеки. Утім, лише 41% виконують

усі правила хоча б інколи, а постійно виконують усі правила лише 13%. Більше того, щодо двох останніх показників зафіксовано помітний спад на близько 10 відсоткових пунктів у порівнянні з попередньою хвилею. Тим не менш, показники виконання правил у групі підлітків залишаються найбільшими серед решти цільових груп: серед молоді 18-25 років хоча б інколи виконують правила 22%, у групі 25-59 років – 18%, серед найстарших респондентів понад 60 років – майже третина (28%).

Серед усіх вікових груп помітно зросло знання правил кібербезпеки: найбільше – у віковій когорті 26-59 років (на 13 відсоткових пунктів) та старшого покоління 60+ років (на 8 відсоткових пунктів). Виконання правил збільшилось на 6 відсоткових пунктів у обох групах.

Найстарша група респондентів залишається найбільш свідомою: частка тих, хто завжди виконує усі правила, становить 14% (див. Діаграма 33).

Діаграма 32. Знання і виконання правил кібербезпеки. Розподіл за цільовими групами (% відповідей, серед опитаних I та II хвилі)

Безпека поведінки в інтернеті

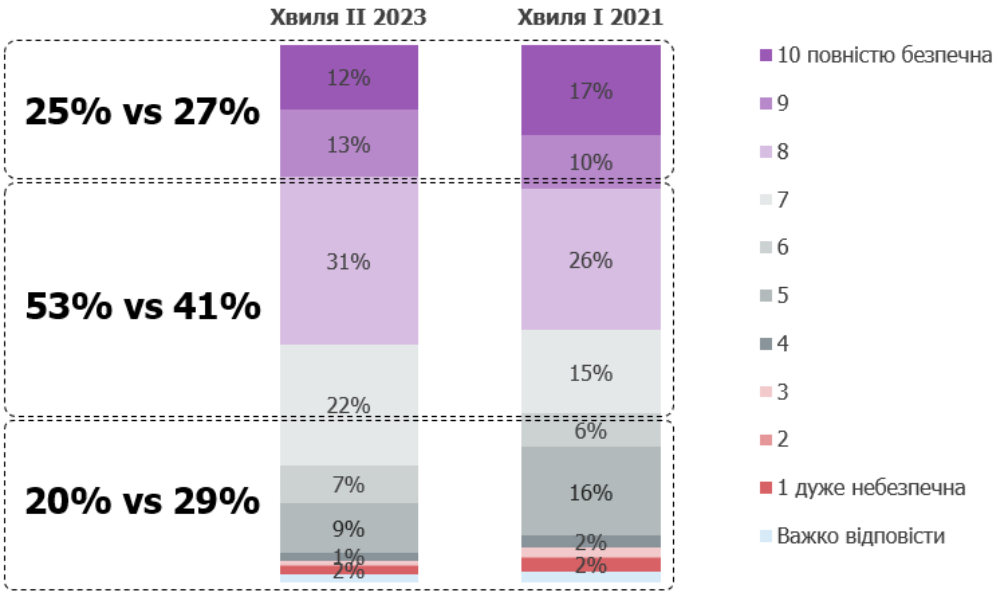
Для самооцінки власної безпечної поведінки в інтернеті респондентам було запропоновано шкалу від 1 до 10, де 1 означає «дуже небезпечна», а 10 – «повністю безпечна». На основі цієї шкали було виділено такі типи поведінки:

- Дуже небезпечна (1-6)
- Помірно безпечна (7-8)
- Повністю безпечна (9-10)

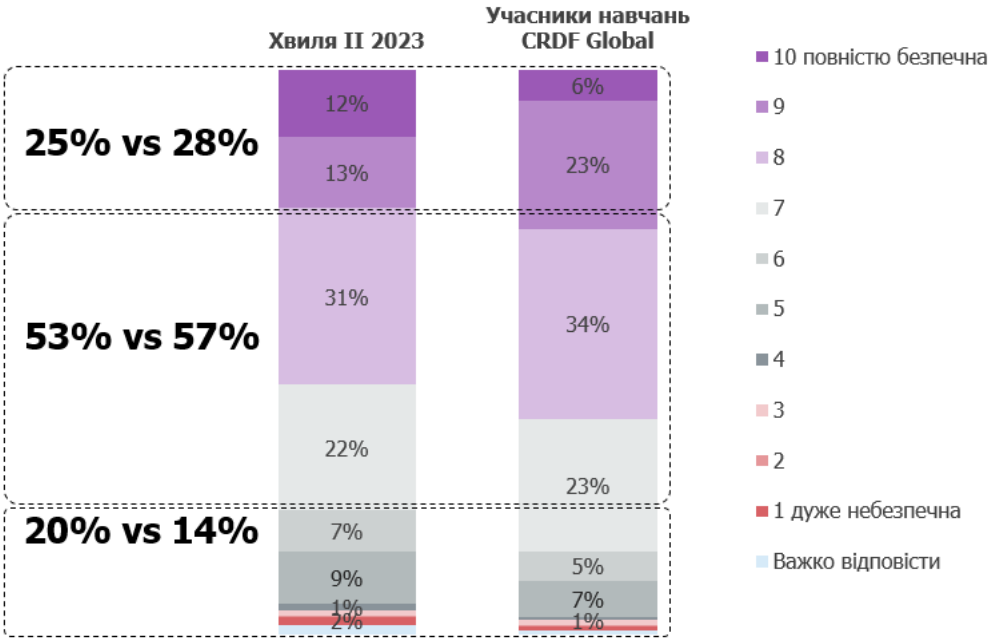
Загалом по вибірці можемо сказати, що кількість респондентів, які вважають свою поведінку в інтернеті повністю безпечною, майже не змінився (зафіксовано незначне падіння з 27% до

25%), тимчасом як відчуття помірно безпечної поведінки зросло на 12 відсоткових пунктів – від 41% до 53%. Частка тих, хто вважає свою поведінку дуже небезпечною, становить 20% (29% в I хвилі) (див. Діаграма 34**Помилка! Джерело посилання не знайдено.**). Є суттєва різниця у оцінці безпечності власної поведінки в інтернеті серед опитаних II хвилі та учасників навчань CRDF Global немає (див. Діаграма 35 та Діаграма 37), учасники навчань почуваються більш безпечно.

Діаграма 334. Загалом, наскільки безпечною ви вважаєте власну поведінку в інтернеті? (% відповідей, серед опитаних I та II хвилі)



Діаграма 345. Загалом, наскільки безпечною ви вважаєте власну поведінку в інтернеті? (% відповідей, серед опитаних II хвилі та учасників навчань CRDF Global)

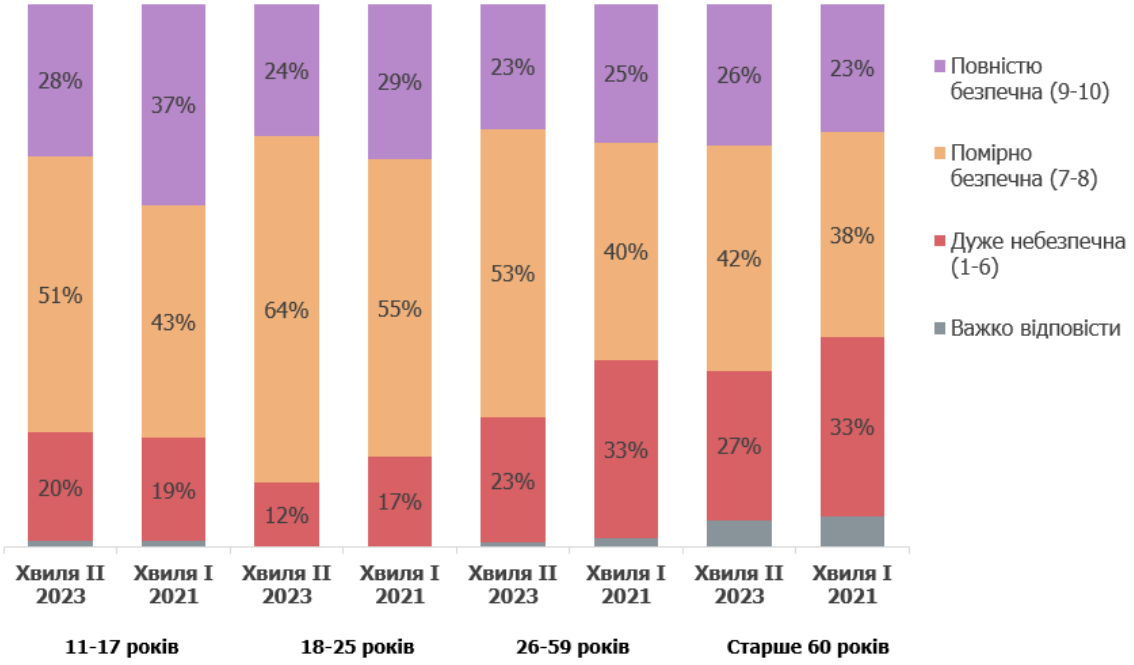


Оцінки власної безпеки значною мірою варіюють із віком: так, серед підлітків (11-17 років) та молоді (18-25 років) менше тих, хто вважає, що поводиться небезпечно (20% та 12% відповідно), тоді як серед людей старше 25 років більше тих, хто вважає перебування в інтернеті небезпечним.

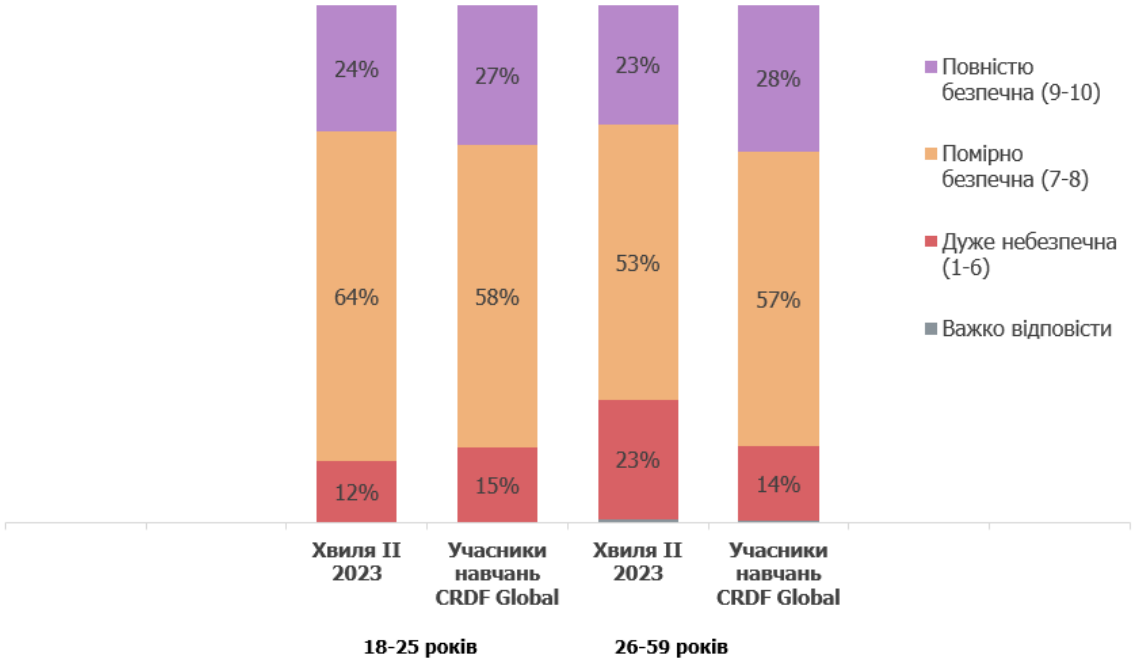
Серед підлітків найбільша частка тих, хто вважає, що поводиться повністю безпечно (28%), тоді як серед інших вікових груп ця частка хоч і не суттєво, однак менша.

Загалом серед молоді до 25 років частка тих, хто вважає свою поведінку безпечною, є більшою, ніж частка тих, хто вважає, що поводиться небезпечно (див. Діаграма 36).

Діаграма 356. Загалом, наскільки безпечною ви вважаєте власну поведінку в інтернеті? Розподіл за цільовими групами (% відповідей, серед опитаних I та II хвилі)



Діаграма 367. Загалом, наскільки безпечною ви вважаєте власну поведінку в інтернеті? Розподіл за цільовими групами (% відповідей, серед опитаних II хвилі та учасників навчань CRDF Global)



Самооцінка поведінки в інтернеті залежить від знання та виконання правил кібербезпеки: чим вище людина оцінює безпеку своєї поведінки, тим краще вона знає і частіше виконує правила кібербезпеки. Ця кореляція прослідковується для всіх вікових груп.

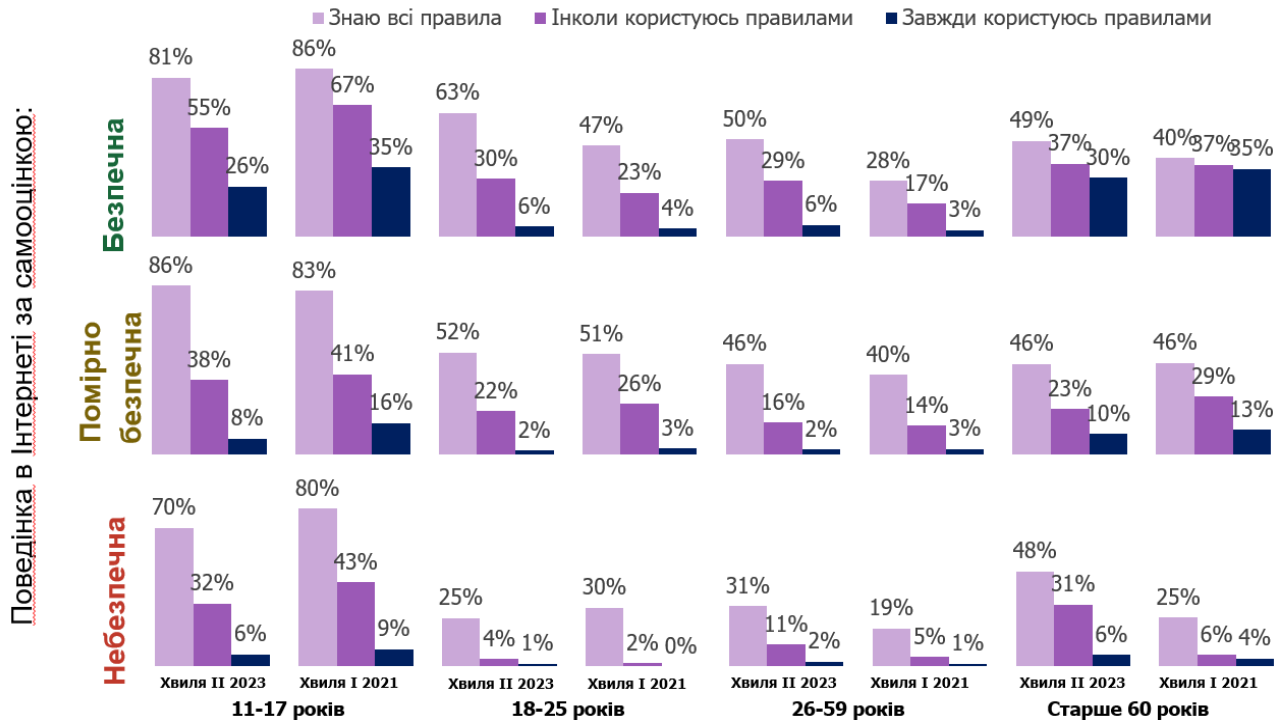
Підлітки, як найбільш обізнана група, оцінює свою поведінку за рівнем додержання правил. Для решти вікових груп самооцінка безпеки корелює передусім чергу із рівнем знання.

Група респондентів найстаршого віку (понад 60 років), які оцінюють свою поведінку як безпечну, є найбільш сумлінною групою щодо виконання правил кібербезпеки: якщо людина знає правило, вона його неухильно додержується.

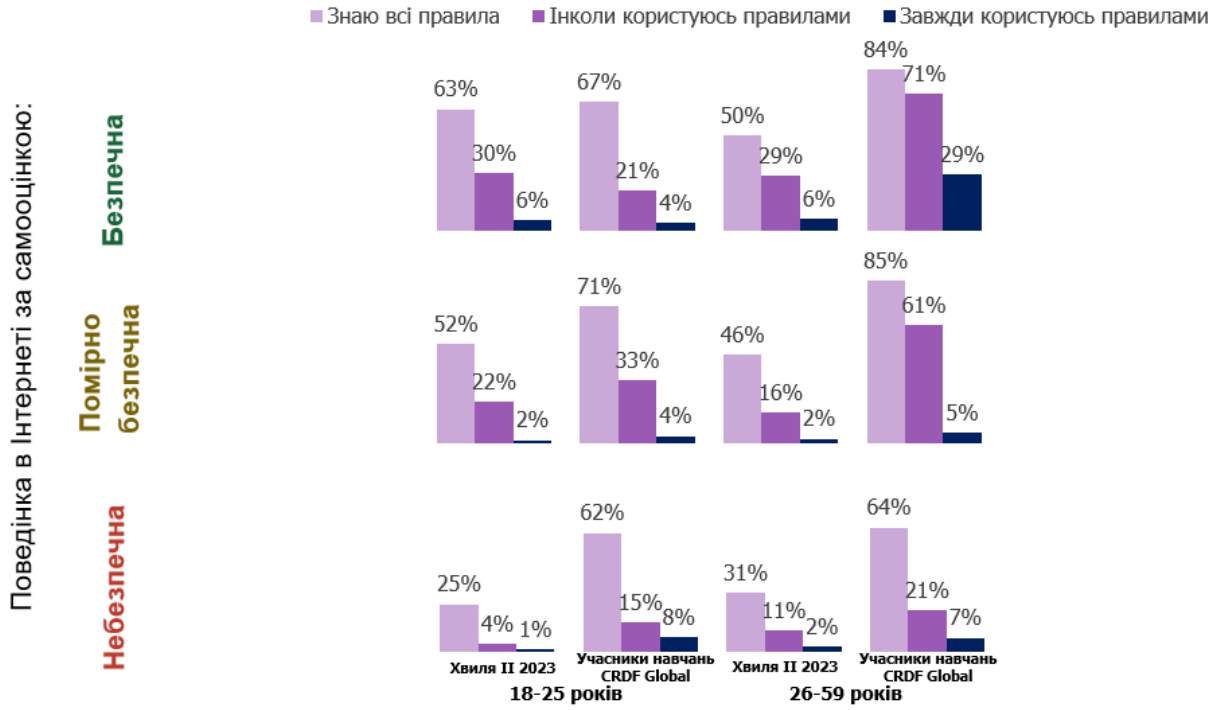
Утім, показовим є факт, що часткове виконання деяких правил також дає почуття безпеки: особливо це помітно в сегменті респондентів від 18 до 59 років: серед тих, хто вважає свою поведінку повністю безпечною, лише 6% додержуються усіх правил (див. Діаграма 38).

Навчання CRDF Global позитивно впливає на оцінку безпечності поведінки, в середньому збільшуючи її у 1,5-2 рази (див. Діаграма 39).

Діаграма 378. Знання і виконання правил кібербезпеки у розбивці за рівнем самооцінки безпеки поведінки в інтернеті



Діаграма 38. Знання і виконання правил кібербезпеки. Розподіл за цільовими групами (% відповідей, серед опитаних II хвилі та учасників навчань CRDF Global)



Респонденти під час ГІ та ФГД цілком погоджувалися, що знання правила не означає його виконання. Деколи порушення відбуваються через неуважність, деколи через брак часу, певні помилки можуть робитися автоматично, коли людина зайнята кількома справами водночас або втомлена. Респонденти здебільшого в середньому оцінювали безпеку своєї поведінки в інтернеті на 6-8 балів з 10.

Також респонденти ГІ та ФГД здебільшого відкрито говорили, що усвідомлюють небезпечність певної поведінки, коли не виконують певні правила, як-от користування ліцензійними програмами, користування антивірусом, створення складних та різноманітних паролів для різник акаунтів, використання двофакторної автентифікації тощо.

«У мене був випадок, коли я відкрила лист з незнайомої пошти просто автоматично. Так само хтось може в месенджері попросити дані, і ти можеш надіслати фотографію картки, є випадки, коли людина не задумується, тому що втомлена чи неуважна. Для мене це актуально» (Студентка)

Здатність розпізнавати ризиковані ситуації

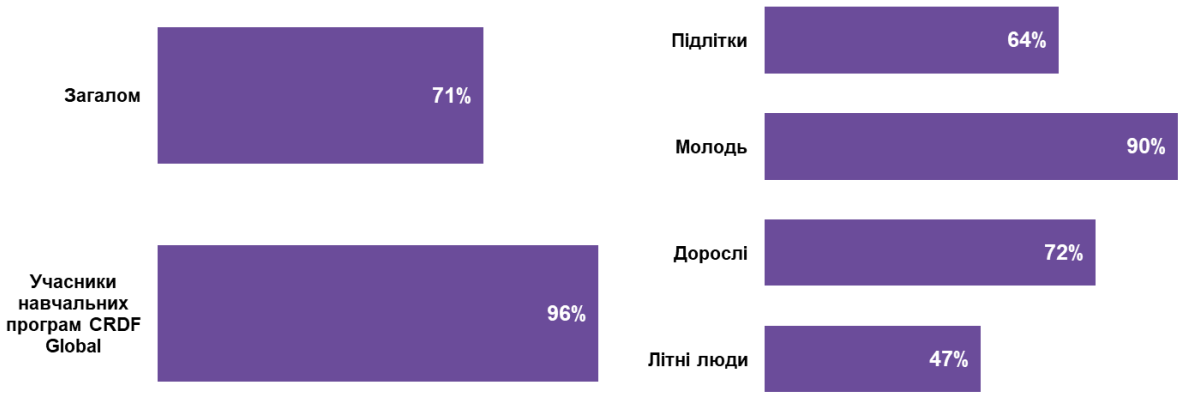
Здатність чітко розрізняти ризиковані ситуації є важливим чинником для підвищення безпеки в інтернеті. Без такої навички людина може або вважати інтернет повністю безпечним місцем і нехтувати правилами безпеки, або, навпаки, вважати, що небезпека очікує всюди і від неї неможливо захиститися.

Для оцінки, наскільки респонденти здатні розрізняти ризиковані ситуації, ми запропонували для оцінки десять прожективних ситуацій, п’ять з яких, на думку експертів CRDF Global, є безпечними, і п’ять – небезпечними. Як індикатор здатності розрізняти ризиковані ситуації ми

взяли частку респондентів, які здатні правильно розрізнити п'ять або більше ситуацій (тобто правильно позначити безпечні та небезпечні ситуації).

Результати аналізу наведені на Діаграмі 40.

Діаграма 40. Здатність розпізнавати ризиковані ситуації (частка респондентів, які правильно розпізнали від п'яти ситуацій)



Найкращі результати продемонстрували респонденти групи «молодь» (18-25 років), а також учасники навчальних програм CRDF Global – більше 90% респондентів цих сегментів правильно розрізнили більше 5 ситуацій (зауважимо, що частка респондентів, які правильно розрізнили усі 10 ситуацій, становить 1,5% серед учасників навчальних програм CRDF Global, і наближається до 0 в інших вікових групах).

Найгіршу здатність розрізняти ризиковані ситуацій продемонстрували літні люди (47%) і, неочікувано, підлітки (64%). При цьому всі аудиторії схильні позначати як «ризиковані» ті ситуації, які насправді ними не є.

Найкраще усі групи респондентів розпізнають ситуацію вимагання грошей від «нібито» друга у соціальних мережах – її розпізнала як ризиковану найбільша частка респондентів: 88% серед підлітків і від 90% серед усіх груп респондентів старше 18 років (Див. Діаграми 41-44).

Респонденти усіх вікових груп вважають, що читання листів, які падають у спам, може бути ризикованим для літніх людей, хоча просто читання таких листів не несе ризику. Таку ситуацію помилково відносять до ризикованої 68% підлітків і молоді, а також понад 75% респондентів 26-59 та 60+ років.

Також помилково відносять до небезпечної ситуацію, коли людина забуває складні паролі. Значна частка респондентів усіх вікових груп вважають, що відновлення паролів несе небезпеку: так вважають 58% підлітків, 40% молоді 18-25 років, 47% дорослих 26-59 років і 66% літніх респондентів.

Навпаки, серед загрозливих ситуацій, які помилково вважають цілком безпечними, лідером є користування підключенням через публічний вай-фай для здійснення банківських операцій. Не

вбачають небезпеки у такій ситуації 54% підлітків, 44% молоді, 55% дорослої і 35% літньої аудиторії.

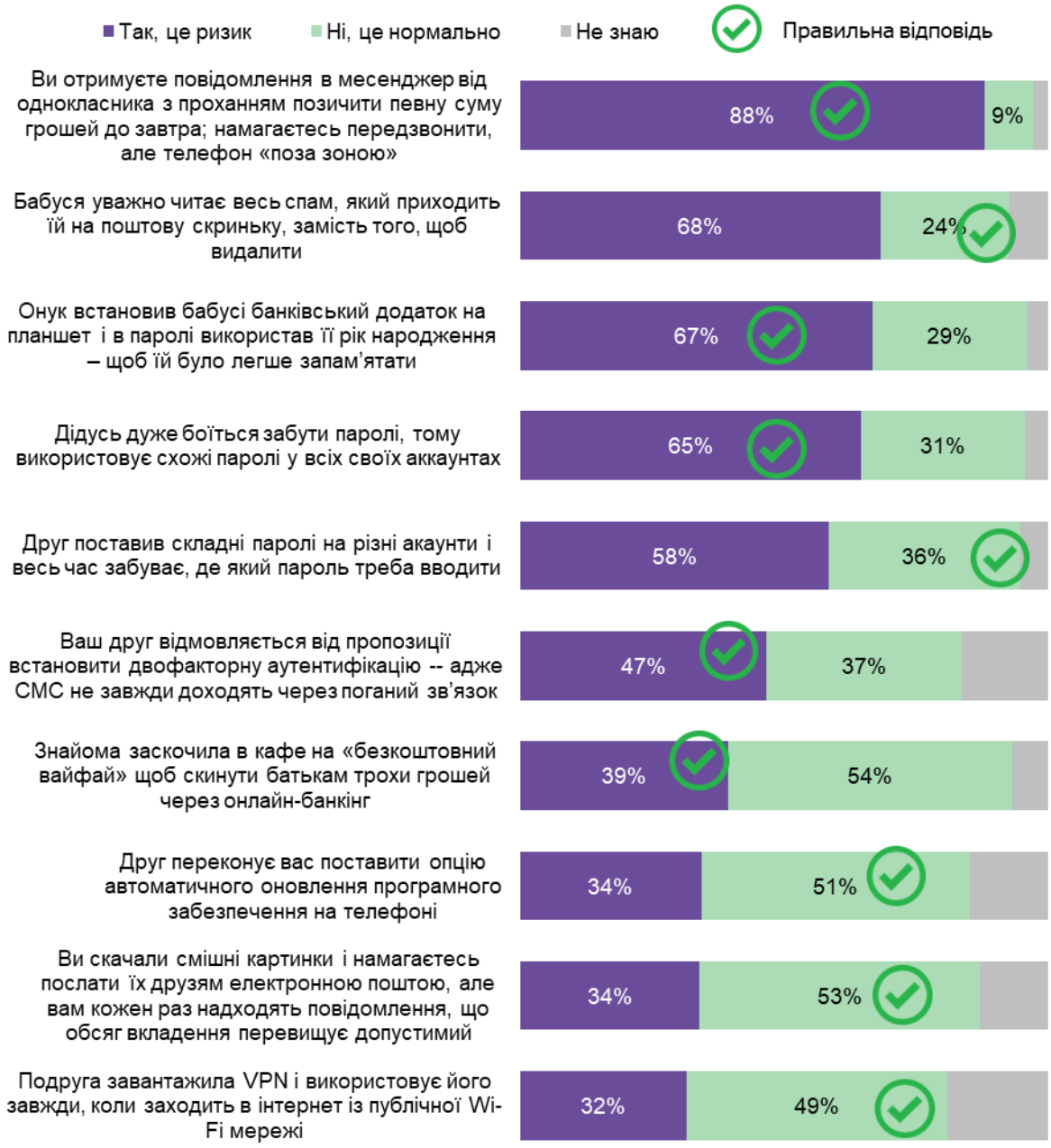
Також значна частка респондентів помилково вважать загрозливими використання VPN та автоматичного оновлення застосунків. Частка респондентів, які вважають використання VPN небезпечним, варіює від 32% серед підлітків до 52% серед дорослої аудиторії.

Автоматичне оновлення додатків на смартфоні є ризикованою поведінкою в уяві приблизно третини підлітків і молоді і близько половини дорослих і літніх респондентів.

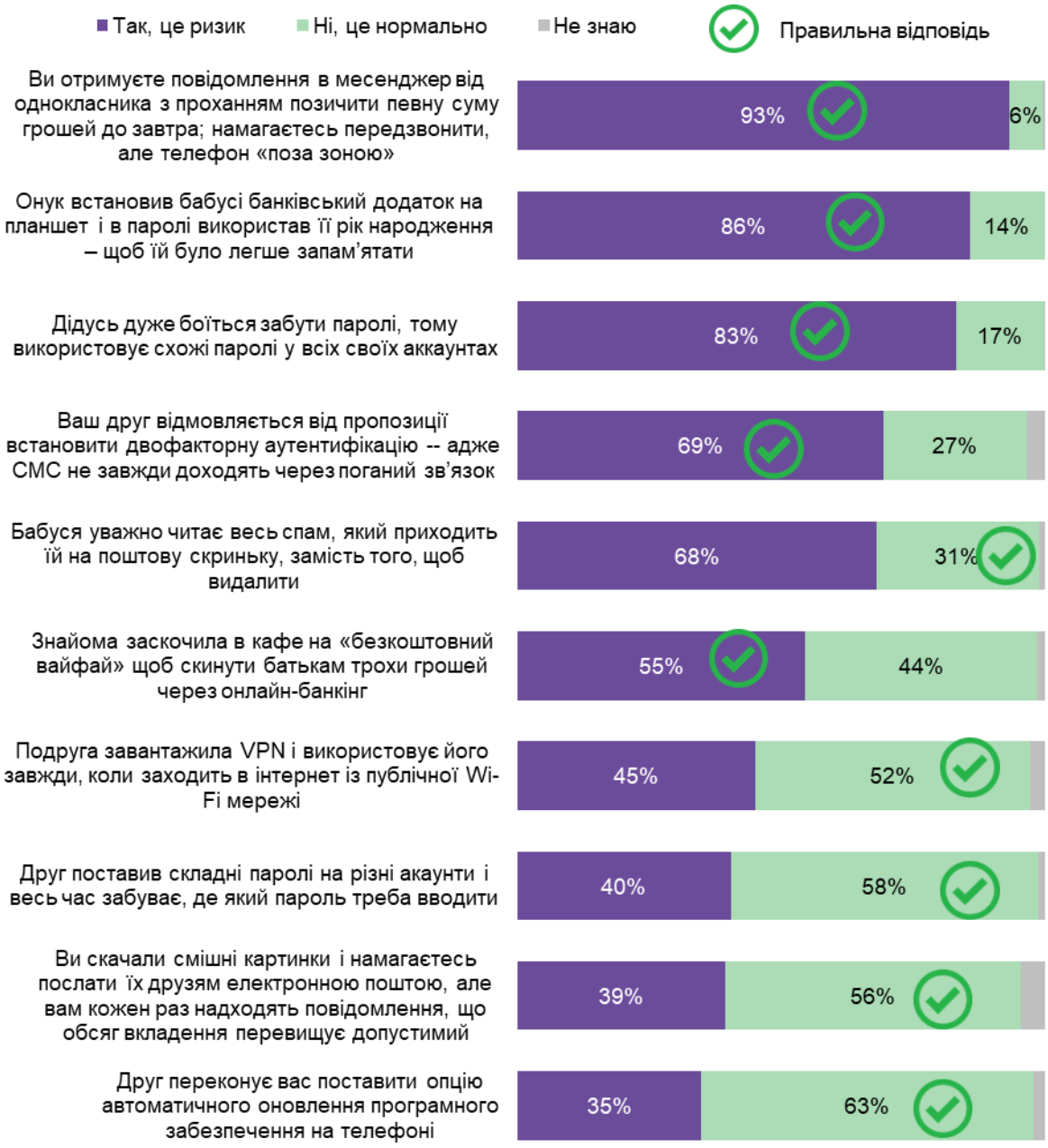
На увагу також заслуговує ситуація, коли не спрацьовує двофакторна автентифікація, наприклад СМС не приходять через поганий зв'язок. Хоча більшість респондентів вважає відмову від двофакторної автентифікації з таких причин ризикованою поведінкою, значна частка респондентів (від чверті до третини) вважає, що в умовах поганого мобільного зв’язку відмова від двофакторної автентифікації є нормальною практикою.

Учасники навчальних курсів CRDF Global продемонстрували кращу здатність розрізняти ризиковані і безпечні ситуації (Діаграма 45). Вони є єдиною аудиторією дослідження, яка розділила ризиковані й безпечні ситуації в правильному порядку. Утім, навіть ці респонденти у більшості (83%) вважають, що читання літніми людьми спаму в електронній пошті є ризикованим, тож, можливо, саме ця ситуація може стати предметом дискусій.

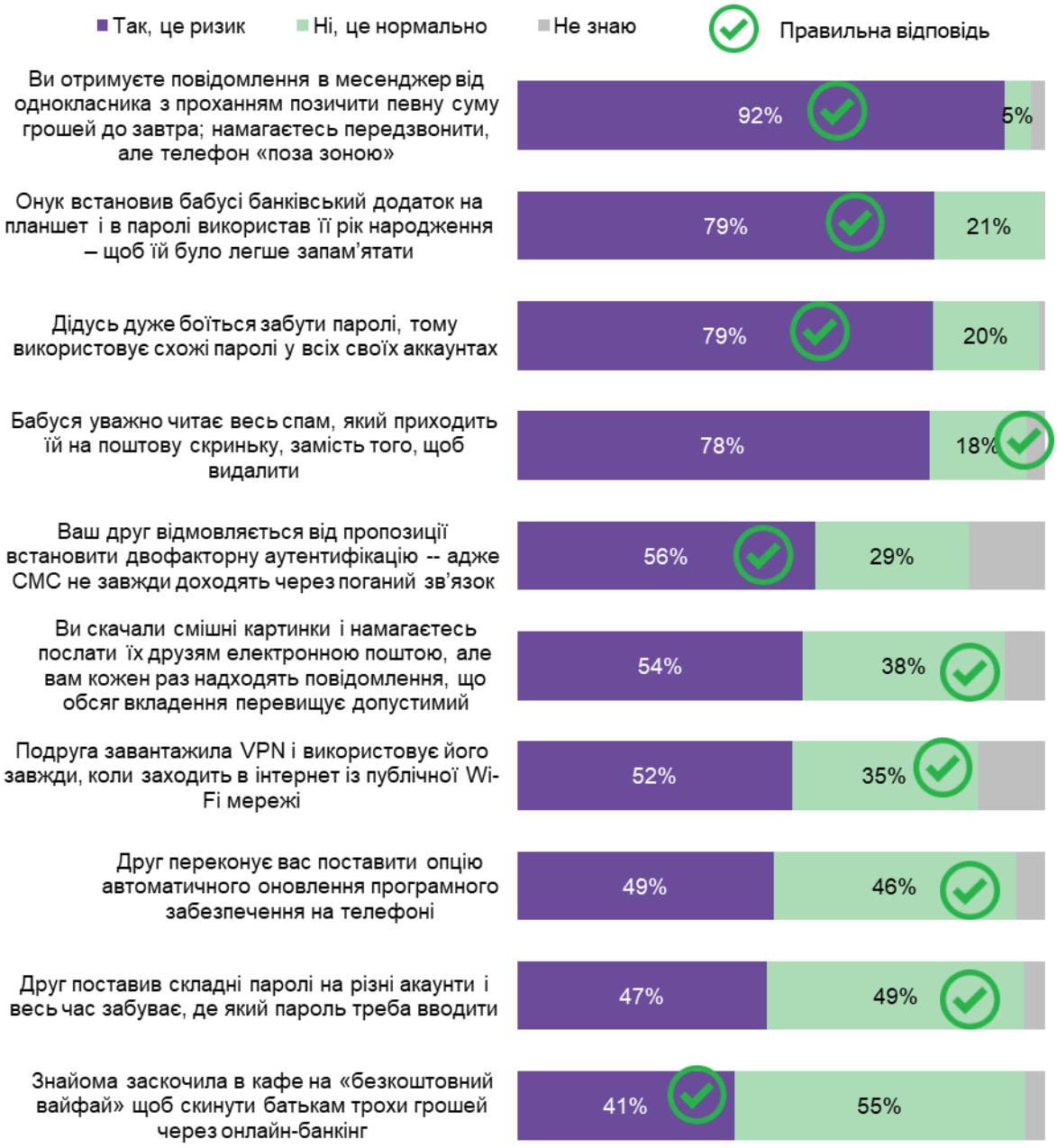
Діаграма 41. Розпізнавання ризикованих ситуацій. Розподіл за цільовою групою 11-17 років (% відповідей)



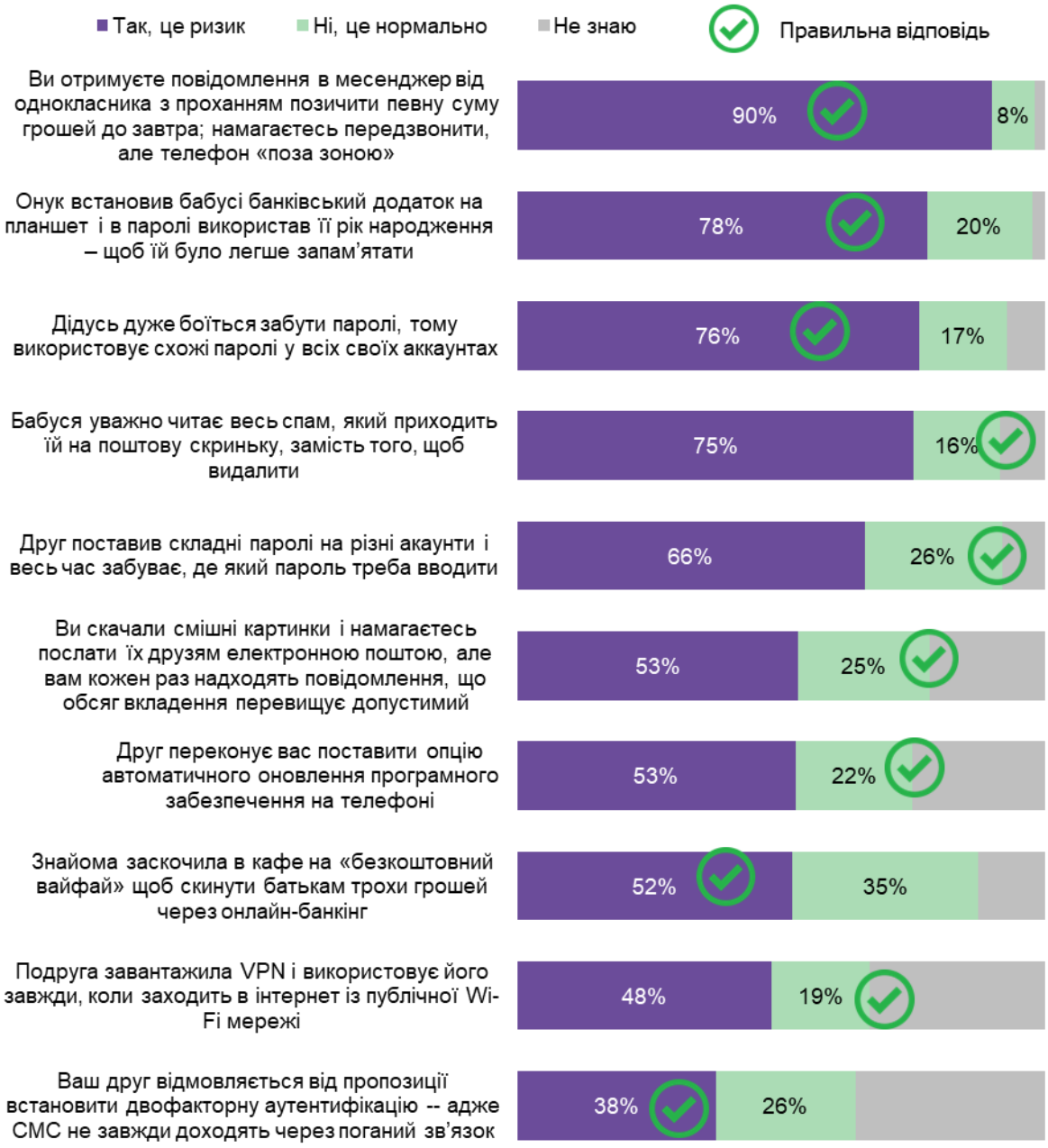
Діаграма 42. Розпізнавання ризикованих ситуацій. Розподіл за цільовою групою 18-25 років (% відповідей)



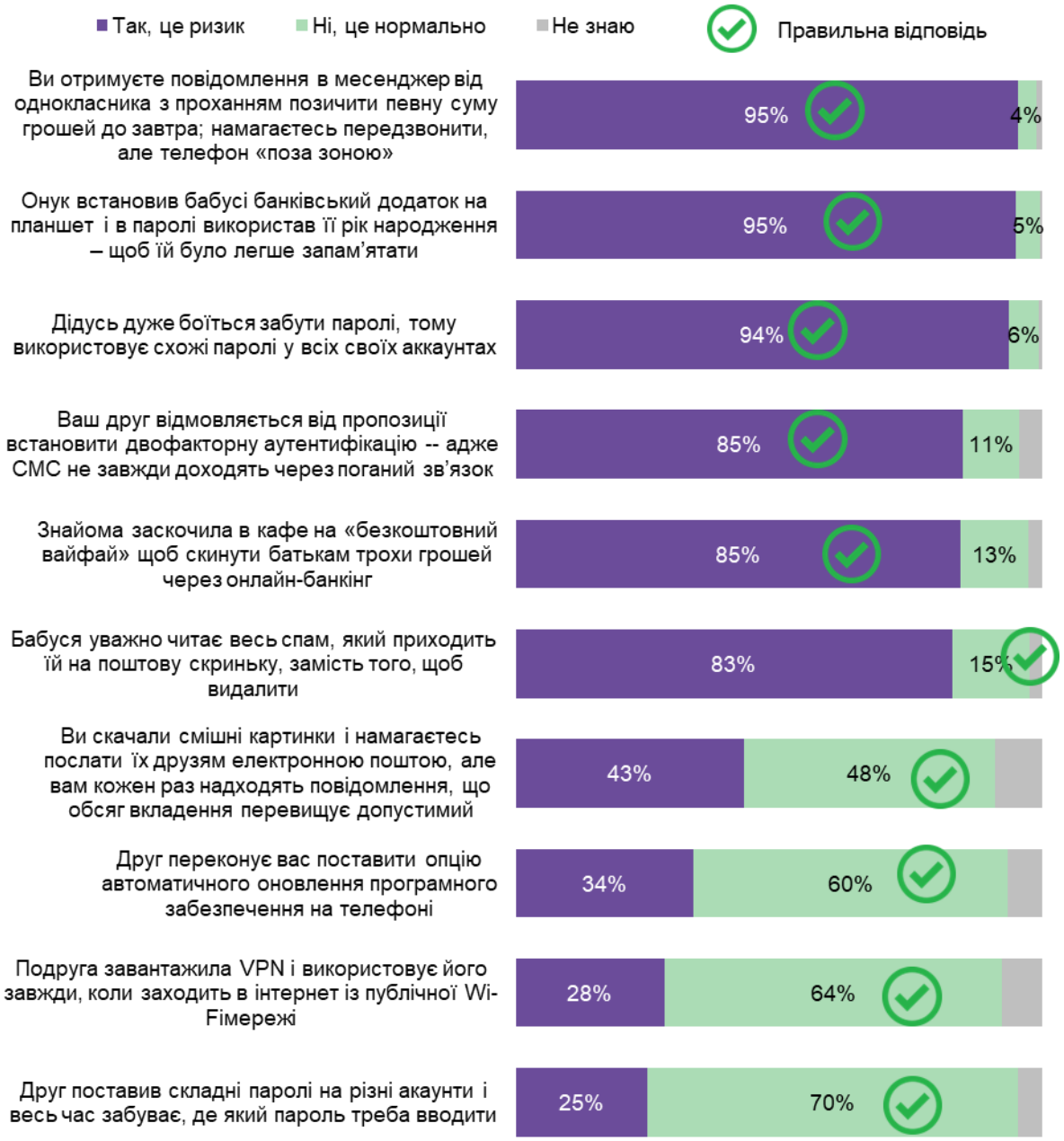
Діаграма 43. Розпізнавання ризикованих ситуацій. Розподіл за цільовою групою 26-59 років (% відповідей)



Діаграма 44. Розпізнавання ризикованих ситуацій. Розподіл за цільовою групою старше 60 років (% відповідей)



Діаграма 45. Розпізнавання ризикованих ситуацій. Розподіл за цільовою групою учасників навчальних програм CRDF Global (% відповідей)



Відгуки про курс з кібербезпеки від CRDF Global

Під час ФГД та ГІ у респондентів запитували про враження від курсу. Частина респондентів слухала курс кілька років тому, тому детальних оцінок не змогла надати. Також не всі респонденти змогли пригадати, про який саме курс ідеться, оскільки слухали кілька подібних курсів, отже не всі респонденти ідентифікували назву CRDF Global та впізнали логотип.

«Я також проходила дуже давно, декілька років тому. Я багато чого вже не пам'ятаю. Але візуально я пам'ятаю, я пригадую, що було легко сприймати цю інформацію, легко відповідати. Тобто якихось заперечень в мене не було на той час, і зараз їх також немає» (Студентка)

Більше запам'ятався курс вчителям, представникам державного сектору та ОМС, які слухали його офлайн. Для вчителів курс є більш впізнаваним, оскільки вони мотивують дітей проходити курси з кібербезпеки для школярів та отримувати сертифікати. Також вчителі регулярно працюють з матеріалами курсу, які є зручними для навчання школярів. Вчителі кажуть, що матеріали добре структуровані, нескладні, мають зрозумілу подачу, гарний дизайн та анімацію. На думку вчителів, навіть діти, що спочатку скептично ставляться до програми, потім захоплюються процесом навчання.

В усіх цільових аудиторіях респонденти говорили, що час від часу слухають курси з кібербезпеки і шукають інформацію в інтернеті. Зокрема, держслужбовці мають регулярно проходити навчання з кібербезпеки. Респонденти згадували, що є курс з цифрової грамотності від Міністерства цифрової трансформації, студенти мають курси з кібербезпеки у навчальних закладах, підлітки пригадують уроки з кібербезпеки у школі.

«…в листопаді минулого року був семінар в Луцьку з кібербезпеки для представників державних органів та самоврядування. Протягом цілого дня ми розмовляли про кібербезпеку. Потім пройшла курс для представників державних органів, про який сьогодні згадували. І також ще почала, але ще не завершила курс основи кібербезпеки від фірми «Ціско», який є на платформі Skill School безкоштовний. Також ще на платформі «Дія Освіта» є курс «Обережно кібершахраї». Там у вигляді освітнього серіалу невеличкого також його пройшла» (Працівник сфери освіти, викладач)

«Від Міністерства освіти, є НУШ із інформатики чи взагалі курси з інформатики. …там теж багато матеріалів з кібербезпеки. Курси для вчителів теж, коли готуються семінари з інформатики» (Вчитель)

На думку респондентів, в інтернеті зараз багато інформації на тему кібербезпеки. Адже тема є вкрай актуальною, шахраї є креативними, відтак необхідно постійно відслідковувати нові загрози та правила безпеки. Через велику кількість матеріалів з кібербезпеки їхні автори чи організатори курсів не завжди запам'ятовуються.

Респонденти, які добре пам'ятали курс та ідентифікували організаторів, мали найкращі враження від контенту, спікерів, подачі інформації, візуального оформлення. Суттєвих зауважень щодо покращення курсу респонденти не висловлювали. Було побажання від фахівців більше проводити курсів офлайн, оскільки онлайн інформація сприймається не так глибоко і гірше запам'ятовується. Від фахівця ІТ ОМС було зауваження, що курс, як йому видалося, був розрахований на непрофільних фахівців, тому інформація була дещо загальною, але все одно було цікаво.

«Мені сподобалась подача інформації, що вона була такою візуальною і дуже близькою. Тому що це було показано на героях у відео, як робити не можна. І ці герої були приблизно одного віку разом із нами. Це легко запам'ятовувалось» (Студентка)

«…це не був просто текст, який тяжко сприймається і взагалі його не хочеться читати. Це було дуже легко для сприйняття. Був якийсь інтерактив, і саме така подача допомагає легше зрозуміти, і тобі хочеться це зрозуміти» (Студент)

«Подача сама дуже класна. Бо мені, на жаль, приходиться дуже багато читати тексту. І таке візуальне оформлення легко сприймається. Інформація подана таким чином, що вона запам'ятовується. І висвітлені саме найважливіші такі аспекти і загальні правила. Тобі їх нескладно просто дотримуватись. І вони подані в дуже інтересному форматі. Тому візуальне оформлення дуже велику роль відіграє. До того ж, якщо її порівнювати ще з відео, то це взагалі неперевершено. Бо можна взагалі не

концентруватись на читанні курсу, а, наприклад, пити каву або чай, і дивитись, і сприймати таку інформацію. Тому дуже класно, дуже круто» (Студентка)

«Насправді курси допомагають систематизовувати інформацію. І моє враження, що цей курс розрахований трішки на людей старшого покоління. Тому що на початках мені трішки [здавалося], що гальмував процес. Хотілось би швидше, інтенсивніше якось дістатись до суті. А я це знаю, оце занадто детально розказано. Але загалом корисний курс» (Фахівець ОМС)

Рекомендації для покращення знань з теми кібербезпеки серед різних ЦА

Респонденти вважають, що тема кібербезпеки є вкрай актуальною, тому будь-які інформаційні кампанії в ЗМІ, соціальна реклама в інтернеті та ЗМІ, а також зовнішня реклама, телепередачі про можливі шахрайства та правила безпеки будуть актуальними. У плані кібербезпеки більш вразливими є старші люди 50+, у яких нижча цифрова грамотність. Хоча діти є більш легковажними у своїй поведінці, але вони постійно отримують знання про ризики та правила поведінки в школі, тому порівняно менш вразливі.

«Стосовно дорослих, можна, наприклад, на новинних каналах давати інформацію, на тих каналах, які вони дивляться … фахівці можуть давати туди якісь певні факти, певні рекомендації стосовно правил користування в Інтернеті. А більш молодшій аудиторії, мені здається, було б цікаво, якби вони проходили якісь квести на тему з кібербезпеки, інформаційна безпека, інформаційна гігієна. …якісь мультиплікаційні формати» (Студентка)

Студенти вважають себе достатньо обізнаними в сфері кібербезпеки, суттєвих проблем з доступом до інформації не мають. Одначе знання треба постійно підтримувати і оновлювати, а також бути достатньо дисциплінованими, щоб дотримуватися усіх рекомендацій та правил. Курси на зразок CRDF Global, на думку респондентів, допомагають освіжити знання та сформувати необхідну мотивацію виконувати правила безпеки. Тому регулярне навчання та самоосвіта є необхідними і будь-які навчальні можливості охоче вітаються респондентами, особливо якщо контент цікавий та креативний.

«Знання треба оновлювати, це дуже динамічна сфера, є багато нових ризиків, і правила забуваються. Тому нові курси – це корисно, необхідно весь час вчитися. І класно, якщо курс поданий легко, в цікавому, приємному форматі» (Студент)

Працівники ОМС, державного сектору та держслужбовці вказували, що суттєвою проблемою є застаріле обладнання, пенсійний вік та низька цифрова грамотність фахівців, використання неліцензійного програмного забезпечення. Найчастіше коштів на вирішення згаданих проблем немає, і, принаймні до завершення війни, суттєвих змін не буде. Є маленькі сільські й міські громади, де бюджети ніколи не були великими, відтак коштів на обладнання і захист даних немає. Часто у громадах немає навіть профільних фахівців з обов'язками системного адміністратора – усім займається особисто голова громади чи його заступник, які не є фахівцями. Ситуація з обладнанням і програмним забезпеченням, на думку респондентів, може дещо змінитися з допомогою західних партнерів, донорів і грантових коштів.

«Ми обговорюємо проблеми з фахівцями, наразі ні місцеві бюджети, ні центральний бюджет не спроможний системно вирішити проблеми цифрових загроз в державному секторі. Поки що ми працюємо в таких умовах – далеких від ідеальних. Частково проблему можна вирішити з допомогою грантів, тому допомога потрібна не лише в освіті та підвищенні цифрової грамотності фахівців, але і у вирішенні проблем з обладнанням та програмним забезпеченням» (Працівник ОМС)

Рівень цифрової грамотності серед фахівців державного сектору необхідно підвищувати, варто робити навчання обов'язковим, а сертифікати іменними. Добре, якщо за проходження курсу є якась винагорода чи мотивація, або принаймні працівник може пройти навчання в робочий час, що також є мотивацією. Якщо навчання відбувається в позаробочий час, то навряд чи воно буде високоефективним.

«Не завжди у працівників є змога приділити увагу і час навчанню, потрібно, щоб на це був виділений окремий час, бажано робочий. Щоб людина в результаті навчання отримувала іменний сертифікат, щоб участь була обов'язковою і також, щоб була певна мотивація брати участь. Якщо навчання відбувається офлайн – такий формат має більше переваг» (Працівник ОМС)

Для вчителів основною проблемою є те, що діти хоча й знають про ризики та правила безпеки, але часто їх ігнорують. Одначе вчителі оптимістично вважають, що за час навчання в школі відбувається постійне обговорення теми кібербезпеки на різних уроках, тому базові знання у дітей все-таки є. Позитивним є ефект від навчальних програм на зразок CDRF Global, вчителі вітають будь-які ініціативи, які створюють цікавий навчальний контент, особливо цікавим є ігровий контент у вигляді квестів чи комп'ютерних ігор або симуляцій. Більш затребуваний такий контент для старших класів, для молодших дітей існує достатньо цікавого контенту. Корисними будуть візити фахівців кіберполіції до шкіл, з роз'ясненням основних ризиків в сфері кібербезпеки та правил кібергігієни, а також особливостей роботи фахівців спеціалізованих правоохоронних органів.

«… крута ідея про ігри і квести. Квести – це в житті, але це треба місце і щоб хтось розробив. А можна гру розробити на телефон і планшет, всі батьки малечку дають своїм дітям телефон і планшет» (Студент)

«Маємо вносити практику. Мають бути платформи, щоби діти, учні, взагалі молоде покоління могли протестувати для себе, що таке є нехтування кібербезпекою. Щоб програми моделювали, в яку халепу може потрапити людина , яка не дотримується правил кібербезпеки. …фундаментально ввести платформи, програмні продукти, симулятори. А я розумію, що це є досить вартісний проект на рівні держави, щоби зробити такі хороші проекти. Це не просто підручник видати, це має дорожче бути. Щоби діти мали можливість вчитися, знати про сучасні проблемі на сучасних платформах. Системно, а не ситуативно… Міністерство має координувати цю річ, інвестуючи, затягуючи в своє коло структури приватні чи громадські, які займаються цим кваліфіковано. Можливо, такими глобальними проектами має займатися організація, яку ми обговорювали» (Вчитель)

Додаток 1. Опитувальник

Вітання

Доброго дня, Представництво CRDF Global в Україні проводить опитування учасників наших навчальних програм про безпеку поведінки в мережі Інтернет. Ваші відповіді суворо конфіденційні, ми не будемо питати про ваші паролі або сайти, які ви відвідуєте. Опитування триватиме до 20 хвилин, будемо вдячні, якщо ви зможете відповісти на наші питання.

Відбір респондента

S1. Скажіть, будь ласка, скільки вам виповнилося повних років?

Запишіть _____ і закодуйте

0	Менше 10 років	КІНЕЦЬ
1	11-17 років	
2	18-25 років	
3	26-59 років	
4	Більше 60 років	
5	Відмова	КІНЕЦЬ

S2. **Позначте вашу стать** *Одна відповідь*

1	Чоловік	
2	Жінка	

S3. **Як часто ви користуєтеся інтернетом, наприклад відвідуєте сайти, соціальні мережі, користуєтеся додатками, месенджерами?** *Одна відповідь*

1	Проводжу в інтернеті більшу частину дня	
2	Кілька сесій на день, але не більшу частину дня	
3	Щоденно, одна-дві сесії	
4	3-4 рази на тиждень	
5	1-2 рази на тиждень	
6	3-4 рази на місяць	
7	1-2 рази на місяць	
8	Рідше, ніж один раз на місяць	КІНЕЦЬ
9	Взагалі не користуюсь Інтернетом	КІНЕЦЬ
99	Важко сказати	КІНЕЦЬ

ОСНОВНИЙ ОПИТУВАЛЬНИК

A1. Основна тема нашої розмови – це кібербезпека та правила кібергігієни. Скажіть, будь ласка, наскільки вам знайомі ці поняття? Оберіть варіант відповіді: «дуже добре знаю і можу пояснити іншим», «маю загальне поняття, без подробиць», «чув/чула такі поняття, але не знаю точно, про що це» або «вперше чую».

Одна відповідь у стовпчику.

	кібербезпека	**правила кібергігієни**
Дуже добре знаю і можу пояснити іншим	1	1
Маю загальне поняття, без подробиць	2	2
Чув/чула такі поняття, але не знаю точно, про що це	3	3
Вперше чую	4	4
Важко відповісти (не зачитувати!)	99	99

A2. Деякі типи поведінки в інтернеті можуть бути ризикованими і призводити до негативних наслідків. Я зачитаю різні ситуації, у які потрапляють інші люди, а ви скажіть, чи вважаєте ви таку ситуацію ризикованою, чи це нормально:

Програміст, випадковий порядок тверджень!	**Так, це ризик**	**Ні, це нормально**	**Не знаю**
Онук встановив бабусі банківський додаток на планшет і в паролі використав її рік народження – щоб їй було легше запам'ятати	1	2	99
Ваш друг відмовляється від пропозиції встановити двофакторну аутентифікацію -- адже СМС не завжди доходять через поганий зв'язок	1	2	99
Знайома заскочила в кафе на «безкоштовний вай-фай» щоб скинути батькам трохи грошей через онлайн-банкінг	1	2	99
Ви отримуєте повідомлення в месенджер від однокласника з проханням позичити певну суму грошей до завтра; намагаєтесь передзвонити, але телефон «поза зоною»	1	2	99
Дідусь дуже боїться забути паролі, тому використовує схожі паролі у всіх своїх акаунтах	1	2	99
Друг переконує вас поставити опцію автоматичного оновлення програмного забезпечення на телефоні	1	2	99
Подруга завантажила VPN і використовує його завжди, коли заходить в інтернет із публічної Wi-Fi мережі	1	2	99
Бабуся уважно читає весь спам, який приходить їй на поштову скриньку, замість того, щоб видалити	1	2	99
Друг поставив складні паролі на різні акаунти і весь час забуває, де який пароль треба вводити	1	2	99
Ви скачали смішні картинки і намагаєтесь послати їх друзям електронною поштою, але вам кожен раз надходять повідомлення, що обсяг вкладення перевищує допустимий	1	2	99

А3. Я зачитаю кілька тверджень. Дайте відповідь, наскільки вони про вас. Ви можете сказати «це точно про мене», «це частково про мене» або «це точно не про мене».
Одна відповідь.

Програміст: РОТАЦІЯ РЯДКІВ		Це точно про мене	Частково про мене	Це точно НЕ про мене	Важко сказати
1	У мене простий пароль, тому що я боюся забути складний	1	2	3	99
2	У мене один пароль на все, щоб завжди його пам'ятати	1	2	3	99
3	Друзі або рідні знають мої паролі на випадок, якщо я забуду	1	2	3	99
4	Я не розумію, навіщо створювати різні паролі	1	2	3	99
5	Я не цікавий(-а) для інтернет-шахраїв	1	2	3	99
6	Якщо є антивірус, то мені нічого не загрожує	1	2	3	99
7	Я відкриваю електронні листи і вкладення навіть з невідомих мені адрес електронної пошти або від незнайомців у месенджері	1	2	3	99
8	Я можу вставити чужу або незнайому флешку у свій комп’ютер	1	2	3	99
9	Я можу випадково «засвітити» дані банківської картки, паспорту, QR коди квитків у соціальних мережах	1	2	3	99
10	Я використовую двофакторну автентифікацію, навіть якщо цього не вимагає політика безпеки сайту (наприклад, банківські додатки)	1	2	3	99
11	Я регулярно роблю резервні копії документів, фотографій – для захисту даних	1	2	3	99
12	Я відвідую російські сайти (які закінчуються .RU)	1	2	3	99
13	Я маю поштові електронні скриньки на російських поштових серверах	1	2	3	99
14	Я відвідую заблоковані в Україні російські ресурси та соціальні мережі (такі як Яндекс, Вконтакті)	1	2	3	99
15	З російських ресурсів (точка РУ) я іноді скачую файли, ігри або програми, заповнюю там анкети, реєструюсь чи вношу певні дані	1	2	3	99

A4.Я зачитаю списки основних загроз, які можуть спіткати користувача інтернету, а ви скажіть, чи стикалися ви особисто або ваші знайомі з такою ситуацією?

Кілька відповідей.

Програміст: РОТАЦІЯ РЯДКІВ		Траплялося з вами особисто	Траплялося із вашими реальними знайомими	Траплялося із вашими віртуальними знайомими	Чули про це, але із знайомими не траплялося	Навіть не чули про таке	Важко сказати	Увага, програміст: Виводити альтернативи відповідно до вікових груп **S1 = …**			
								1	2	3	4
1	Крадіжка (злам) облікових записів у соціальних мережах	1	2	3	4	5	99	x	x	x	
2	Крадіжка (злам) ігрових акаунтів у комп'ютерних іграх	1	2	3	4	5	99	x			
3	**[Формулювання для S1 =1]** Довірче вимагання паролів до облікових записів, акаунтів, електронних поштових скриньок, ігрових бонусів, банківських даних батьків з використанням методів соціальної інженерії (маніпуляцій, погроз, шантажу) та секстингу (повідомлення сексуального характеру) **[Формулювання для S1 =2,3,4]** Вимагання паролів до облікових записів акаунтів, електронних поштових скриньок з використанням методів соціальної інженерії (маніпуляцій, погроз, шантажу)	1	2	3	4	5	99	x	x	x	x
4	Люди стають жертвами кібершахраїв на онлайн-аукціонах	1	2	3	4	5	99		x	x	
5	Вимагання особистих даних через телефон, месенджери, поштові скриньки, облікові записи у соціальних мережах	1	2	3	4	5	99			x	x
6	Вимагання банківських даних, паролів та доступу до облікових записів банківських мобільних	1	2	3	4	5	99			x	x

	додатків, банківських рахунків (у т.ч. через телефон, месенджери)										
7	Вимагання грошей задля розблокування роботи комп'ютерних систем та ґаджетів (електронних пристроїв)	1	2	3	4	5	99			x	
8	Вимагання службових даних від працівників державних або комерційних компаній	1	2	3	4	5	99			x	
9	Кібершахраї вимагають гроші, використовуючи методи соціальної інженерії (маніпуляції, погрози, шантаж), а також особисті та родинні дані (через телефон та месенджери)	1	2	3	4	5	99				x

A5.Я зачитаю кілька базових правил кібергігієни, а ви скажіть, наскільки ви особисто обізнані з цим правилом. Ви можете обрати відповідь «Вперше чую», «Знаю, але не дотримуюся», «Знаю і дотримуюся інколи» або «Знаю і завжди дотримуюся».

Одна відповідь у рядку.

Програміст: РОТАЦІЯ РЯДКІВ		Вперше чую	Знаю, але не дотримуюся	Знаю і дотримуюся	Знаю і завжди	Важко сказати	Увага, програміст: Виводити альтернативи відповідно до вікових груп **S1 =**			
							1	2	3	4
1	**[Формулювання для S1 =1]** Використовуйте складні паролі і не використовуйте одні і ті ж самі паролі для реєстрації на онлайн-ресурсах, у соціальних мережах та ігрових мобільних додатках, звикайте користуватись менеджерами паролів **[Формулювання для S1 =2,3,4]** Використовуйте складні паролі і не використовуйте одні і ті ж самі паролі для реєстрації на онлайн-ресурсах, в банківських системах тощо, звикайте користуватись менеджерами паролів.	1	2	3	4	99	x	x	x	x
2	**[Формулювання для S1 =1]** Не відправляйте фото та скани банківських карток та особистих документів своїх та батьків незнайомцям та сумнівним організаціям **[Формулювання для S1 =2,3,4]** Не відправляйте фото та скани ваших банківських карток та особистих документів незнайомцям та сумнівним організаціям	1	2	3	4	99	x	x	x	x

3	**[Формулювання для S1 =1]** Не відкривайте сумнівні листи у вашій електронній скриньці, месенджерах та ігрових акаунтах **[Формулювання для S1 =2,3,4]** Не відкривайте сумнівні листи у вашій електронній скриньці, месенджерах	1	2	3	4	99	x	x	x	x
4	Не відправляйте ваші контактні телефони, особисті фото незнайомцям, особливо тим, які просять оголені фотографії	1	2	3	4	99	x			
5	Не встановлюйте на ваші ґаджети додатки та програми з неофіційних магазинів	1	2	3	4	99	x	x	x	x
6	Не підключайтеся до загальнодоступних, невідомих або незахищених мереж Wi-Fi	1	2	3	4	99	x	x	x	x
7	У разі вимагання паролів, даних, фото незнайомцями або отримання сумнівних повідомлень, негайно повідомте батьків	1	2	3	4	99	x			
8	Регулярно оновлюйте ваші пристрої. За можливості, увімкніть автоматичне оновлення всіх програм	1	2	3	4	99		x	x	
9	Використовуйте ліцензійне та антивірусне програмне забезпечення, фаєрволи на комп'ютерах і телефонах, та регулярно оновлюйте його, коли отримуєте повідомлення про оновлення системи	1	2	3	4	99		x	x	
10	Завжди створюйте резервні копії важливих даних на окремому локальному пристрої чи хмарному сховищі	1	2	3	4	99		x	x	
11	За можливості, використовуйте двофакторну аутентифікацію	1	2	3	4	99		x	x	
12	Не залишайте ваш пристрій без нагляду, особливо коли він працює у публічних місцях	1	2	3	4	99		x	x	x
13	За будь-якої підозри зараження свого пристрою або компрометації даних НЕГАЙНО повідомте відповідні органи: Урядова команда реагування на комп'ютерні надзвичайні події України, Національний координаційний центр з кібербезпеки РНБОУ, Кіберполіція України	1	2	3	4	99		x	x	
14	Не панікуйте у разі телефонного дзвінка чи повідомлення у месенджери від підозрілих людей та організацій, які вимагають у вас гроші, аби врятувати вашу родину, тварину чи близьку людину. Негайно повідомте відповідні органи чи своїх близьких у разі такого дзвінка	1	2	3	4	99				x
15	За будь-якої підозри зараження свого пристрою або компрометації даних НЕГАЙНО повідомте відповідні органи: Кіберполіція України тел. 0 800 505 170 та своїм дітям та близьким	1	2	3	4	99				x

А6.Загалом, наскільки безпечною ви вважаєте власну поведінку в інтернеті? Дайте оцінку за шкалою від 1 до 10, де 1 означає «дуже небезпечна», а 10 – «повністю безпечна».

1	2	3	4	5	6	7	8	9	10	ВВ=99

ДЕМОГРАФІЯ

D1. Назвіть, будь ласка, свій основний рід занять. *Одна відповідь*

1	Працюю за наймом
2	Зареєстрований приватний підприємець
3	Самозайнятий
4	Студент / учень
5	Веду домашнє господарство
6	Пенсіонер
7	Тимчасово не працюю, але шукаю роботу
98	Інше (запишіть)

D2. [Якщо D1= 4] Де саме ви навчаєтесь? *Одна відповідь*

1	У школі
2	В професійно-технічному навчальному закладі
3	В коледжі
4	В вищому навчальному закладі
98	Інше (запишіть)

D3. Який ваш рівень освіти? *Одна відповідь*

1	Немає початкової освіти
2	Початкова середня освіта
3	Базова загальна середня
4	Повна загальна середня
5	Спеціальна середня освіта
5	Неповна вища/початкова вища
6	Вища освіта, бакалаврат
7	Вища освіта, магістратура (спеціаліст)
99	Важко сказати

D4. Що б ви могли сказати про фінансове становище вашої сім'ї? *Зачитайте, одна відповідь*

1	Змушені економити на харчуванні
2	Вистачає на харчування. Для придбання одягу, взуття необхідно заощадити або позичити
3	Вистачає на харчування та необхідний одяг, взуття. Для таких покупок, як гарний костюм, мобільний телефон, пилосос, необхідно заощадити або позичити
4	Вистачає на харчування, одяг, взуття, інші покупки. Але для придбання речей, які дорого коштують (таких як телевізор, холодильник), необхідно заощадити або позичити
5	Вистачає на харчування, одяг, взуття, дорогі покупки. Для таких покупок, як машина, квартира, необхідно заощадити або позичити
5	Будь-які необхідні покупки можу зробити в будь-який час
99	Важко сказати

Це всі питання.

Подякуйте респондентові за участь в опитуванні!

Додаток 2. Портрет респондента

		TOTAL		TOTAL		Вік респондента							
						11-17 років				18-25 років			
		II хвиля 2023		I хвиля 2021		II хвиля 2023		I хвиля 2021		II хвиля 2023		I хвиля 2021	
		Count	Col%	Count	Col%	Count	Col%	Count	Col%	Count	Col%	Count	Col%
Стать	Чоловік	685	47.40%	570	47.47%	162	51.38%	154	51.38%	201	51.55%	159	52.94%
	Жінка	760	52.60%	630	52.53%	153	48.62%	146	48.62%	189	48.45%	141	47.06%
	TOTAL	1445	100.00%	1200	100.00%	315	100.00%	300	100.00%	390	100.00%	300	100.00%
Регіон	Київ	116	8.03%	98	8.20%	27	8.45%	22	7.42%	31	7.95%	24	8.00%
	Північ	243	16.82%	162	13.46%	94	29.95%	38	12.78%	49	12.56%	39	13.00%
	Захід	313	21.66%	295	24.55%	32	10.01%	84	27.89%	110	28.21%	83	27.67%
	Центр	325	22.49%	290	24.14%	45	14.18%	73	24.37%	92	23.59%	71	23.67%
	Південь	246	17.02%	206	17.19%	63	20.15%	49	16.34%	61	15.64%	50	16.67%
	Схід	202	13.98%	149	12.45%	54	17.27%	34	11.19%	47	12.05%	33	11.00%
	TOTAL	1445	100.00%	1200	100.00%	315	100.00%	300	100.00%	390	100.00%	300	100.00%
Розмір населеного пункту (тис. жителів)	Село	488	33.77%	352	29.29%	112	35.54%	102	34.07%	139	35.64%	102	34.03%
	0-50	311	21.52%	247	20.61%	67	21.36%	63	21.11%	81	20.77%	58	19.04%
	51-500	318	22.01%	299	24.91%	64	20.19%	64	21.41%	82	21.03%	68	22.79%
	500+	328	22.70%	302	25.19%	72	22.91%	70	23.41%	88	22.56%	72	24.14%
	TOTAL	1445	100.00%	1200	100.00%	315	100.00%	300	100.00%	390	100.00%	300	100.00%

		TOTAL		TOTAL		Вік респондента							
						26-59 років				Більше 60 років			
		II хвиля 2023		I хвиля 2021		II хвиля 2023		I хвиля 2021		II хвиля 2023		I хвиля 2021	
		Count	Col%	Count	Col%	Count	Col%	Count	Col%	Count	Col%	Count	Col%
Стать	Чоловік	685	47.40%	570	47.47%	214	48.68%	212	47.02%	108	36.01%	65	43.17%
	Жінка	760	52.60%	630	52.53%	226	51.32%	238	52.98%	192	63.99%	85	56.83%
	TOTAL	1445	100.00%	1200	100.00%	440	100.00%	450	100.00%	300	100.00%	150	100.00%
Регіон	Київ	116	8.03%	98	8.20%	36	8.18%	38	8.44%	22	7.33%	12	8.07%
	Північ	243	16.82%	162	13.46%	59	13.41%	64	14.22%	41	13.67%	18	12.02%
	Захід	313	21.66%	295	24.55%	106	24.09%	105	23.33%	65	21.67%	37	24.77%
	Центр	325	22.49%	290	24.14%	110	25.00%	108	24.00%	78	26.00%	37	24.35%
	Південь	246	17.02%	206	17.19%	72	16.36%	80	17.78%	50	16.67%	24	16.22%
	Схід	202	13.98%	149	12.45%	57	12.95%	55	12.22%	44	14.67%	22	14.56%
	TOTAL	1445	100.00%	1200	100.00%	440	100.00%	450	100.00%	300	100.00%	150	100.00%
Розмір населеного пункту (тис. жителів)	Село	488	33.77%	352	29.29%	137	31.14%	128	28.45%	100	33.33%	40	26.67%
	0-50	311	21.52%	247	20.61%	98	22.27%	94	20.90%	65	21.67%	30	20.00%
	51-500	318	22.01%	299	24.91%	103	23.41%	111	24.75%	69	23.00%	43	28.67%
	500+	328	22.70%	302	25.19%	102	23.18%	117	25.90%	66	22.00%	37	24.67%
	TOTAL	1445	100.00%	1200	100.00%	440	100.00%	450	100.00%	300	100.00%	150	100.00%

		TOTAL		TOTAL		Вік респондента							
						11-17 років				18-25 років			
		II хвиля 2023		I хвиля 2021		II хвиля 2023		I хвиля 2021		II хвиля 2023		I хвиля 2021	
		Count	Col%	Count	Col%	Count	Col%	Count	Col%	Count	Col%	Count	Col%
Основний рід занять	Працюю за наймом	380	26.30%	445	37.04%	3	0.96%	0	0.00%	127	32.61%	103	34.25%
	Зареєстрований приватний підприємець	70	4.84%	82	6.81%	0	0.00%	0	0.00%	27	6.82%	25	8.20%
	Самозайнятий	57	3.94%	58	4.82%	2	0.73%	0	0.00%	25	6.35%	20	6.66%
	Студент / учень	403	27.89%	176	14.68%	299	94.95%	299	99.63%	100	25.63%	74	24.68%
	Веду домашнє господарство	84	5.81%	111	9.25%	0	0.00%	1	0.37%	16	4.08%	33	10.94%
	Пенсіонер	263	18.20%	225	18.73%	1	0.38%	0	0.00%	0	0.00%	3	1.10%
	Тимчасово не працюю, але шукаю роботу	105	7.27%	94	7.82%	3	0.92%	0	0.00%	53	13.94%	38	12.50%
	Інше	83	5.74%	4	0.30%	6	2.05%	0	0.00%	41	10.56%	1	0.49%
	Важко сказати	0	0.00%	7	0.56%	0	0.00%	0	0.00%	0	0.00%	4	1.18%
	TOTAL	1445	100.00%	1200	100.00%	315	100.00%	300	100.00%	390	100.00%	300	100.00%
Місце навчання	У школі	259	64.27%	120	67.96%	259	86.47%	251	84.08%	0	0.00%	0	0.00%
	В професійно-технічному навчальному закладі	17	4.22%	8	4.27%	15	4.86%	12	3.91%	1	1.46%	5	6.10%
	В коледжі	37	9.18%	14	7.69%	18	6.15%	18	5.91%	19	18.84%	12	15.94%
	В вищому навчальному закладі	88	21.84%	35	20.08%	6	2.10%	18	6.11%	79	78.68%	58	77.96%
	Інше	2	0.50%	0	0.00%	1	0.42%	0	0.00%	1	1.03%	0	0.00%
	TOTAL	403	100.00%	176	100.00%	299	100.00%	299	100.00%	100	100.00%	74	100.00%

		TOTAL		TOTAL		Вік респондента							
						26-59 років				Більше 60 років			
		II хвиля 2023		I хвиля 2021		II хвиля 2023		I хвиля 2021		II хвиля 2023		I хвиля 2021	
		Count	Col%	Count	Col%	Count	Col%	Count	Col%	Count	Col%	Count	Col%
Основний рід занять	Працюю за наймом	380	26.30%	445	37.04%	200	45.34%	233	51.68%	50	16.54%	24	16.07%
	Зареєстрований приватний підприємець	70	4.84%	82	6.81%	41	9.19%	40	8.97%	2	0.69%	5	3.50%
	Самозайнятий	57	3.94%	58	4.82%	29	6.68%	28	6.17%	1	0.25%	4	2.54%
	Студент / учень	403	27.89%	176	14.68%	4	0.88%	1	0.23%	0	0.00%	0	0.00%
	Веду домашнє господарство	84	5.81%	111	9.25%	64	14.55%	59	13.03%	4	1.31%	3	1.97%
	Пенсіонер	263	18.20%	225	18.73%	25	5.57%	36	8.06%	237	78.96%	112	74.96%
	Тимчасово не працюю, але шукаю роботу	105	7.27%	94	7.82%	47	10.76%	48	10.71%	2	0.52%	1	0.96%
	Інше	83	5.74%	4	0.30%	31	7.04%	2	0.41%	5	1.73%	0	0.00%
	Важко сказати	0	0.00%	7	0.56%	0	0.00%	3	0.73%	0	0.00%	0	0.00%
	TOTAL	1445	100.00%	1200	100.00%	440	100.00%	450	100.00%	300	100.00%	150	100.00%
Місце навчання	У школі	259	64.27%	120	67.96%	0	0.00%	0	0.00%	0	0.00%	0	0.00%
	В професійно-технічному навчальному закладі	17	4.22%	8	4.27%	1	30.98%	0	0.00%	0	0.00%	0	0.00%
	В коледжі	37	9.18%	14	7.69%	0	0.00%	0	0.00%	0	0.00%	0	0.00%
	В вищому навчальному закладі	88	21.84%	35	20.08%	3	69.02%	1	100.00%	0	0.00%	0	0.00%
	Інше	2	0.50%	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%
	TOTAL	403	100.00%	176	100.00%	4	100.00%	1	100.00%	0	0.00%	0	0.00%

		TOTAL		TOTAL		Вік респондента							
						11-17 років				18-25 років			
		II хвиля 2023		I хвиля 2021		II хвиля 2023		I хвиля 2021		II хвиля 2023		I хвиля 2021	
		Count	Col%	Count	Col%	Count	Col%	Count	Col%	Count	Col%	Count	Col%
Рівень освіти	Немає початкової освіти	7	0.48%	1	0.08%	7	2.27%	2	0.71%	0	0.00%	0	0.00%
	Початкова середня освіта	160	11.07%	80	6.65%	159	50.37%	159	53.07%	0	0.00%	1	0.23%
	Базова загальна середня	156	10.80%	82	6.83%	120	37.99%	105	35.03%	12	3.13%	10	3.22%
	Повна загальна середня	171	11.83%	129	10.78%	18	5.72%	16	5.37%	58	14.91%	41	13.62%
	Спеціальна середня освіта	321	22.21%	311	25.94%	2	0.61%	5	1.58%	73	18.75%	61	20.30%
	Неповна вища/початкова вища	102	7.06%	61	5.09%	5	1.44%	13	4.25%	65	16.66%	51	16.87%
	Вища освіта, бакалаврат	158	10.93%	124	10.31%	0	0.00%	0	0.00%	77	19.70%	82	27.20%
	Вища освіта, магістратура	362	25.05%	407	33.91%	0	0.00%	0	0.00%	101	26.17%	52	17.37%
	Важко відповісти	10	0.69%	5	0.39%	5	1.59%	0	0.00%	3	0.68%	4	1.18%
	TOTAL	1445	100.00%	1200	100.00%	315	100.00%	300	100.00%	390	100.00%	300	100.00%
Фінансове становище сім'ї	Змушені економити на харчуванні	142	9.83%	119	9.94%	8	2.44%	1	0.49%	8	1.97%	17	5.61%
	Для придбання одягу, взуття необхідно заощадити або позичити	266	18.41%	218	18.15%	36	11.49%	18	5.92%	51	13.06%	29	9.62%
	Для таких покупок як гарний костюм, мобільний телефон, необхідно заощадити або позичити	373	25.81%	266	22.18%	114	36.16%	133	44.18%	104	26.74%	69	23.14%
	Для придбання речей, які дорого коштують необхідно заощадити або позичити	330	22.84%	280	23.37%	77	24.45%	66	21.99%	112	29.00%	71	23.56%
	Для таких покупок як машина, квартира необхідно заощадити або позичити	177	12.25%	189	15.78%	34	10.84%	38	12.79%	78	20.09%	63	20.99%
	Будь-які необхідні покупки можу зробити в будь-який час	67	4.64%	52	4.31%	15	4.73%	5	1.52%	21	5.49%	29	9.58%
	Важко відповісти	88	6.09%	75	6.28%	31	9.88%	39	13.12%	14	3.65%	23	7.50%
	TOTAL	1445	100.00%	1200	100.00%	315	100.00%	300	100.00%	390	100.00%	300	100.00%

		TOTAL		TOTAL		Вік респондента							
						26-59 років				Більше 60 років			
		II хвиля 2023		I хвиля 2021		II хвиля 2023		I хвиля 2021		II хвиля 2023		I хвиля 2021	
		Count	Col%	Count	Col%	Count	Col%	Count	Col%	Count	Col%	Count	Col%
Рівень освіти	Немає початкової освіти	7	0.48%	1	0.08%	0	0.00%	0	0.00%	0	0.00%	0	0.00%
	Початкова середня освіта	160	11.07%	80	6.65%	1	0.22%	2	0.33%	0	0.00%	1	0.58%
	Базова загальна середня	156	10.80%	82	6.83%	22	4.91%	17	3.69%	2	0.64%	1	0.74%
	Повна загальна середня	171	11.83%	129	10.78%	45	10.29%	57	12.68%	50	16.83%	10	6.59%
	Спеціальна середня освіта	321	22.21%	311	25.94%	134	30.31%	128	28.52%	112	37.45%	55	36.76%
	Неповна вища/початкова вища	102	7.06%	61	5.09%	14	3.08%	16	3.66%	18	5.88%	5	3.26%
	Вища освіта, бакалаврат	158	10.93%	124	10.31%	50	11.40%	46	10.20%	31	10.35%	11	7.39%
	Вища освіта, магістратура	362	25.05%	407	33.91%	174	39.41%	183	40.64%	87	28.85%	66	44.10%
	Важко відповісти	10	0.69%	5	0.39%	2	0.38%	1	0.27%	0	0.00%	1	0.58%
	TOTAL	1445	100.00%	1200	100.00%	440	100.00%	450	100.00%	300	100.00%	150	100.00%
Фінансове становище сім'ї	Змушені економити на харчуванні	142	9.83%	119	9.94%	58	13.18%	43	9.50%	68	22.69%	30	19.94%
	Для придбання одягу, взуття необхідно заощадити або позичити	266	18.41%	218	18.15%	92	20.90%	83	18.39%	87	28.89%	45	30.23%
	Для таких покупок як гарний костюм, мобільний телефон, необхідно заощадити або позичити	373	25.81%	266	22.18%	83	18.90%	87	19.22%	72	23.98%	25	16.84%
	Для придбання речей, які дорого коштують необхідно заощадити або позичити	330	22.84%	280	23.37%	113	25.71%	122	27.10%	28	9.35%	18	12.32%
	Для таких покупок як машина, квартира необхідно заощадити або позичити	177	12.25%	189	15.78%	46	10.50%	72	15.95%	19	6.47%	21	14.14%
	Будь-які необхідні покупки можу зробити в будь-який час	67	4.64%	52	4.31%	26	5.91%	21	4.64%	5	1.70%	3	1.95%
	Важко відповісти	88	6.09%	75	6.28%	22	4.90%	23	5.20%	21	6.92%	7	4.58%
	TOTAL	1445	100.00%	1200	100.00%	440	100.00%	450	100.00%	300	100.00%	150	100.00%