УДК 004.056.53

Єрмак А.Р., Алексєєва С.А.

Національний університет «Одеська політехніка»

КІБЕРБЕЗПЕКА МОЛОДІ: РОЛЬ ОСВІТИ У ФОРМУВАННІ БЕЗПЕЧНОЇ ПОВЕДІНКИ В ЦИФРОВОМУ ПРОСТОРІ

Вступ. Сучасне суспільство переживає епоху масштабної цифровізації, що охоплює всі сфери життя. Молодь є найактивнішою категорією користувачів цифрових технологій: понад 75% підлітків мають мобільні телефони, які використовуються для спілкування, навчання та розваг, а більше половини відвідують соціальні мережі кілька разів на день. Водночас, інтенсивне використання цифрових технологій супроводжується зростанням кількості та складності кіберзагроз, спрямованих саме на молоде покоління.

Статистика свідчить про серйозність проблеми: за даними DQ Institute, майже 70% дітей та підлітків у світі зазнали впливу кіберризиків у 2023 році [1]. Дослідження показують, що 91% підлітків ділилися своїми зображеннями онлайн, а більшість з них також розголошували персональні дані, такі як місцезнаходження, електронна адреса.При цьому 95% витоків даних у 2024 році були пов'язані з людським фактором, що підкреслює критичну важливість освітніх ініціатив у сфері кібербезпеки [2].

Глобальний контекст також тривожний: за дослідженням CheckPoint, глобальні кібератаки зросли на 30% у другому кварталі 2024 року, досягнувши 1636 атак на організацію щотижня. Особливу тривогу викликає той факт, що молодь, попри високий рівень технічної грамотності, демонструє низьку культуру кібербезпеки: використовує слабкі паролі, ігнорує оновлення безпеки та неусвідомлено розголошує персональні дані в соціальних мережах.

Ця ситуація загострюється відсутністю системного підходу до навчання основ кібербезпеки в освітніх закладах України, що створює значний розрив між рівнем цифрової активності молоді та їхньою здатністю захищати себе від кіберзагроз у цифровому просторі.

Мета: Обґрунтувати необхідність системного впровадження освіти з кібербезпеки для молоді та визначити ключові напрями формування культури безпечної поведінки в цифровому просторі.

1. Аналіз кіберзагроз для молоді

Цифрове середовище, в якому сьогодні зростає молодь, характеризується безпрецедентним рівнем інтерактивності та відкритості. За даними Pew Research Center, 73% підлітків щодня відвідують YouTube, включаючи 15%, які описують своє використання як "майже постійне", а близько 60% щодня відвідують TikTok[3]. У 2023 році 77% учнів старших класів використовували соціальні мережі кілька разів на день. Така інтенсивна цифрова активність створює широкий спектр кіберзагроз.

Фішинг та соціальна інженерія. Молоді користувачі є особливо вразливими до фішингових атак через недостатній досвід розпізнавання шахрайських повідомлень. Зловмисники активно використовують популярні серед молоді

платформи для поширення шкідливих посилань, створення фейкових профілів та виманювання персональних даних.

Кібербулінг. У 2024-2025 роках з'явилися нові форми кібербулінгу: підлітки використовують штучний інтелект для створення підроблених, неприйнятних зображень своїх однокласників і потім розповсюджують їх. Це призводить до серйозних психологічних наслідків для жертв, які відчувають інтенсивну втрату контролю над своїм цифровим іміджем.

Витік персональних даних у соціальних мережах. Молоді користувачі часто не усвідомлюють довгострокові наслідки публікації особистої інформації онлайн. Вони розміщують дані про своє місцезнаходження, навчальні заклади, розклад дня, що може бути використано зловмисниками для різних цілей - від таргетованих атак до фізичного переслідування.

Шкідливе програмне забезпечення. Завантаження неліцензійного контенту, ігор, додатків з неперевірених джерел часто призводить до зараження пристроїв молоді шкідливими програмами, включаючи програми-вимагачі, шпигунське ПЗ та криптомайнери.

Аналіз поведінкових патернів молодих користувачів виявляє декілька ключових проблем, що підвищують їхню вразливість до кіберзагроз.

Ризикована онлайн-активність. Молодь демонструє схильність до експериментування в цифровому просторі без належної оцінки ризиків. Це включає спілкування з незнайомцями, участь у сумнівних онлайн-активностях, обмін особистими фотографіями та відео без розуміння можливих наслідків.

Відсутність навичок кібергігієни. Базові практики кібербезпеки, такі як використання надійних паролів, двофакторна аутентифікація, регулярне оновлення програмного забезпечення, часто ігноруються молодими користувачами. Вони використовують однакові прості паролі для різних сервісів, не перевіряють налаштування приватності в соціальних мережах, не роблять резервні копії важливих даних.

Довіра до неперевірених джерел. Молодь часто не володіє навичками критичної оцінки інформації в цифровому середовищі. Вони можуть довіряти фейковим новинам, переходити за підозрілими посиланнями, завантажувати файли з незнайомих джерел, не перевіряючи їхню автентичність та безпечність.

Ілюзія анонімності та безкарності. Багато молодих людей вважають, що їхні дії в інтернеті є анонімними і не матимуть реальних наслідків. Це призводить до необережної поведінки, публікації компрометуючого контенту, участі в незаконних онлайн-активностях.

Ці особливості поведінки, поєднані з відсутністю систематичної освіти з кібербезпеки, створюють критичну вразливість молодого покоління до широкого спектру кіберзагроз у цифровому просторі.

2. Роль освіти у формуванні безпечної поведінки

Освіта відіграє ключову роль у формуванні цифрової культури молодого покоління. Вона забезпечує не лише технічну підготовку користувачів, а й розвиток усвідомленого ставлення до власної діяльності в інформаційному просторі. Формування культури безпечної поведінки вимагає системного підходу, який охоплює всі рівні освіти - від школи до університету.

Система освіти України перебуває на етапі поступового впровадження тематики кібербезпеки в навчальні програми. У шкільному курсі інформатики передбачено базові знання про безпечну роботу в мережі, захист персональних даних і правила поведінки в соціальних медіа[4]. Однак навчання має фрагментарний характер, бракує системності та практичної спрямованості. У закладах вищої освіти основна увага зосереджена на професійній підготовці фахівців з кібербезпеки, тоді як формування базової цифрової культури серед широкої молодіжної аудиторії залишається недостатньо розвиненим. Позитивну роль відіграють освітні ініціативи МОН України та громадських організацій, однак вони мають локальний характер.

У провідних країнах світу (США, Велика Британія, Сінгапур, Канада) освіта з кібербезпеки є частиною національних стратегій цифрової трансформації. Навчання здійснюється безперервно: від початкової школи, де діти опановують основи цифрової етики, до університетів, які пропонують прикладні курси та симуляційні тренінги. Поширеною практикою є проведення CTF-змагань, хакатонів, використання ігрових платформ і симуляторів кіберзагроз. Ефективним також визнано підвищення кваліфікації педагогів, що забезпечує сталість і якість навчального процесу.

Сучасні підходи передбачають використання гейміфікації, інтерактивних платформ, симуляцій та навчальних ігор, що сприяють підвищенню мотивації учнів. CTF-змагання, освітні хакатони та квести розвивають логіку, командну взаємодію та інтерес до практичного застосування знань. Інтеграція основ кібербезпеки у шкільні предмети, онлайн-курси та позакласну діяльність створює умови для формування культури безпечної поведінки з раннього віку.

3. Виклики та перспективи

Розвиток кібербезпеки в українській освіті супроводжується низкою суттєвих викликів, що стримують формування ефективної системи підготовки молоді до безпечної діяльності у цифровому середовищі. Одним із ключових бар'єрів є брак кваліфікованих викладачів, здатних поєднувати педагогічні навички з актуальними знаннями у сфері інформаційної безпеки. Більшість педагогів не мають спеціальної підготовки з питань кіберзахисту, тому передавання учням практичних навичок відбувається обмежено або поверхово.

Ще однією проблемою є відсутність стандартизованих навчальних матеріалів. Освітні програми, які стосуються цифрової безпеки, часто створюються окремими ентузіастами, громадськими організаціями чи IT-компаніями без єдиних методичних підходів і державного регулювання. Це призводить до нерівномірного рівня знань серед учнів різних навчальних закладів. Водночас, стрімкий розвиток інформаційних технологій і швидкість зміни кіберзагроз роблять існуючі навчальні матеріали швидко застарілими, що вимагає постійного оновлення змісту освіти.

Перспективи вдосконалення освіти з кібербезпеки пов'язані передусім із формуванням національної стратегії цифрової безпеки в освіті. Така стратегія має визначити єдині стандарти, компетентнісну модель та механізми реалізації на всіх рівнях освіти. Важливим напрямом є створення адаптивних навчальних програм,

здатних швидко реагувати на нові виклики у сфері інформаційних технологій. Одночасно необхідно інвестувати у підготовку викладацьких кадрів, організовуючи системні курси підвищення кваліфікації, стажування та спільні освітні ініціативи з представниками IT-сектору.

Велике значення має розвиток партнерства між закладами освіти, IT-компаніями та кіберспільнотою. Таке співробітництво дозволяє інтегрувати у навчальний процес реальні кейси, симуляції кіберінцидентів, практичні тренінги та хакатони. Спільні проєкти сприяють формуванню у молоді прикладних навичок і створюють міст між академічними знаннями та реальними потребами ринку праці.

Висновок. Результати аналізу свідчать, що формування культури безпечної поведінки неможливе без системного освітнього підходу. Освіта має стати центральним елементом національної політики кіберзахисту, спрямованої на підготовку свідомих та відповідальних користувачів цифрового простору. Практична значущість полягає у можливості впровадження розроблених підходів у навчальні програми різних рівнів освіти. Перспективними напрямами подальших досліджень є розробка цифрових симуляторів, методів гейміфікації та оцінювання рівня кіберкомпетентності учнів.

Перелік використаних джерел.

1. DQ Institute. Cyber risk exposure among children and adolescents. Security Magazine, 2023. URL: https://www.securitymagazine.com/articles/100099-almost-70-of-children-and-adolescents-have-been-exposed-to-cyber-risks

2. Mimecast. State of Human Risk Report 2024 SC Media, 2025. URL: https://www.scworld.com/news/95-of-data-breaches-involve-human-error-report-reveals

3. Chang V. Cybersecurity for children: an investigation into the application of social media. Taylor & Francis, 2023.URL: https://www.tandfonline.com/doi/full/10.1080/17517575.2023.2188122#abstract

4. Міністерство освіти і науки України. Модельні навчальні програми для 5-9 класів Нової української школи. URL: https://mon.gov.ua/osvita-2/zagalna-serednya-osvita/osvitni-programi/modelni-navchalni-programi-dlya-5-9-klasiv-novoi-ukrainskoi-shkoli-zaprovadzhuyutsya-poetapno-z-2022-roku