техніко-правових інструментів цифрового суверенітету, а й суспільної стійкості до маніпуляцій [2].

На цьому тлі особливої ваги набуває Рекомендація ЮНЕСКО з етики ШІ (2021), яка містить принципи, орієнтовані на забезпечення прав людини, прозорість, недискримінацію, безпеку та інклюзію при використанні штучного інтелекту [4]. Її положення можуть стати основою для імплементації національного законодавства України у сфері ШІ.

Отже, формування цифрового суверенітету України потребує поєднання технічної незалежності, етичного правового регулювання, освітніх програм та міжнародної інтеграції стандартів. Без цього держава залишатиметься вразливою до зовнішніх технологічних впливів.

**Список використаних джерел**

1. Компанієць Ф. Контроль над хмарою – контроль над майбутнім. *Speka – онлайн-медіа про підприємництво та технології.* URL: https://speka.media/cifrovii-suverenitet-jevropi-9qy53k.

2. Цифрові пропагандисти та інформаційний суверенітет. Як захистити свої права в онлайн-епоху. *Інститут Просвіти.* URL: https://iprosvita.com/tsyfrovi-propahandysty-ta-informatsijnyj-suverenitet-iak-zalyshytysia-neoshukanym-ta-zakhystyty-svoi-prava-v-onlajn-epokhu/

3. Милосердна І.М. Цифровий суверенітет держави: наукова риторика та реальні зміни. *Репозитарій ПНПУ ім. К. Д. Ушинського.* URL: http://dspace.pdpu.edu.ua/bitstream/123456789/21794/1/25.pdf.

4. Recommendation on the Ethics of Artificial Intelligence. UNESCO, 2021. URL: https://unesdoc.unesco.org/ark:/48223/pf0000381137.

5. Regulation (EU) 2024/1365 of the European Parliament and of the Council of 13 March 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1365.

**Ковальова Дар'я Юріївна,**
*слухач навчально-наукового інституту поліцейської діяльності Національної академії внутрішніх справ*

## ЗАХИСТ ДІТЕЙ ТА ВРАЗЛИВИХ ГРУП У ЦИФРОВОМУ СЕРЕДОВИЩІ

Цифрове середовище стало невід'ємною частиною повсякденного життя, і воно надає безліч можливостей для дітей та молоді, зокрема в навчанні, соціалізації, культурному обміні і навіть у професійному розвитку. Однак, разом із цими можливостями виникають нові загрози для здоров'я та безпеки, особливо для дітей та вразливих груп. Цифровий простір парадоксально поєднує у собі освітні можливості й механізми впливу, які часто використовуються

зловмисниками у своїх психологічних стратегіях, що ставить під загрозу права дітей, їхнє фізичне та психологічне благополуччя.

Основними ризиками, які можуть виникнути для дітей у цифровому середовищі, є кібербулінг, шахрайство, маніпуляції, педофілія онлайн, а також доступ до шкідливого контенту. Кібербулінг є серйозною загрозою для психічного здоров'я дітей, оскільки вони можуть зазнати насмішок, погроз чи переслідувань в соціальних мережах та інших цифрових платформах. Діти, як правило, не мають достатньої обізнаності для того, щоб виявити небезпечні ситуації та відреагувати на них відповідно.

Крім того, цифрові платформи часто слугують середовищем для популяризації деструктивних наративів, таких як радикалізація і насильство. Це особливо небезпечно для підлітків, які ще формують своє світосприйняття та мають вразливу психіку. Дослідниця феномену сексуальних злочинців Анна Солтер, у своїй книзі «Хижаки» детально описує, як зловмисники використовують довіру, емоційний зв'язок та психологічні вразливості дитини для реалізації своїх цілей. У цифровому середовищі ці механізми лише посилюються завдяки можливості довготривалого прихованого контакту та імітації безпечних стосунків [1].

Останнім часом в мережі Інтернет дуже розповсюджені такі явища, як секстинг, тобто інтимне листування з дитиною, а також ґрумінг – встановлення дружніх відносин, входження в довіру до дитини з метою подальшої особистої зустрічі для вступу в сексуальні відносини, експлуатації чи шантажу. Нерідко діти стають жертвами секстингу, тому що не вбачають в цьому реальної загрози, вважаючи це нешкідливим, простим способом отримання компліментів на рахунок своєї зовнішності за допомогою схвальних коментарів чи «лайків» [2]. Але досить часто жертва примушується до участі в порнографічних сценаріях через шантаж із використанням інформації, яка попередньо була зібрана про неї в Інтернеті, адже була у відкритому доступі.

До останнього часу в Україні подібні діяння не розглядалися в площині кримінального законодавства (лише в лютому 2021 року було криміналізоване домагання дитини в сексуальних цілях, в тому числі з використанням інформаційно-телекомунікаційних систем або технологій (ст. 156-1 Кримінального кодексу України) [3]), тоді як в деяких країнах вже є судові рішення, якими визнано факти зґвалтування через Інтернет. Зокрема, ще в 2017 році у Швеції засудили чоловіка, який таким чином зґвалтував 27 дітей, змушуючи їх виконувати сексуальні дії з використанням веб-камери, записуючи їх на відео або демонструючи в прямому ефірі [2].

Захист дітей у цифровому середовищі потребує чіткої правової регламентації. Національні законодавчі органи повинні створювати та впроваджувати закони, які сприяють захисту дітей від цифрових загроз. Одним з таких кроків є впровадження законів, що зобов'язують інтернет-платформи блокувати доступ до небезпечного контенту, а також застосовувати механізми перевірки віку користувачів.

Процес розслідування кіберзлочинів, які стосуються дітей, повинен враховувати особливості збору доказів в Інтернеті. Оскільки інтернет-

платформи часто не мають можливості безпосередньо перевірити вік користувачів, це потребує інтеграції нових механізмів моніторингу та фільтрації контенту на рівні законодавства.

Для забезпечення безпеки дітей у цифровому середовищі важливо підвищувати рівень цифрової грамотності серед усіх учасників освітнього процесу. Це включає навчання дітей основам кібербезпеки, навичкам захисту персональних даних, а також вмінням критично оцінювати інформацію в Інтернеті. Включення курсів з цифрової грамотності в шкільні програми є необхідним кроком для підготовки молоді до реалій сучасного інформаційного середовища.

Батьки та освітяни відіграють важливу роль у забезпеченні безпеки дітей у цифровому середовищі. Так, Анна Солтер наголошує на центральній ролі батьків у запобіганні сексуальному насильству, у тому числі — в умовах цифрової доби. Вона критикує наївність, довірливість і небажання бачити загрози навіть тоді, коли вони очевидні [1]. Для захисту дітей від небезпек Інтернету важливо активно контролювати їхню активність, встановлювати обмеження на доступ до шкідливого контенту та регулярно проводити бесіди про правила безпечного використання мережі. Це також включає заходи обережності при спілкуванні з незнайомими людьми онлайн, усвідомлення небезпек кібербулінгу, важливість захисту персональних даних та безпеку фінансових операцій.

Підсумовуючи вищевикладене, слід зазначити, що забезпечення цифрової безпеки дітей – це багаторівнева система, в якій поєднуються право, психологія, освіта, технічна інфраструктура та культура довіри. Лише інтегрований підхід може забезпечити стійкий захист від тих загроз, які з кожним роком стають дедалі складнішими й витонченішими.

**Список використаних джерел:**

1. Хижаки. Педофіли, ґвалтівники та інші сексуальні злочинці: хто вони такі, як вони діють і як ми можемо захистити себе та своїх дітей / пер. З анг. О. Татаренко. Харків: Вид-во «Ранок»: Фабула, 2022. 288 с.

2. Іонан В.В Інтернеті що 5 хв. відбувається сексуальне насильство над дитиною. Як це зупинити? *Українська правда*. 2020. URL: https://life.pravda.com.ua/columns/2020/02/4/239800/.

3. Про внесення змін до деяких законодавчих актів України щодо імплементації Конвенції Ради Європи про захист дітей від сексуальної експлуатації та сексуального насильства (Ланцаротської конвенції): Закон України від 18 лютого 2021 р. № 12560-IX. URL: https://zakon.rada.gov.ua/laws/card/1256-20.