

ЗАХИСТ ДІТЕЙ ВІД СУЧАСНИХ ЗАГРОЗ В КІБЕРПРОСТОРІ

Корнієнко М. В., Ковальова О. В.

ВСТУП

Кіберпростір, тобто середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних¹, є невід'ємною частиною життя сучасної людини. Сучасне покоління дітей народжується та зростає в умовах швидкого розвитку цифрових технологій. Діти мають цифровий слід ще до того, коли починають ходити та говорити. Від стаціонарних комп'ютерів Інтернет перейшов до смартфонів, що дає змогу дітям перебувати весь час онлайн: спілкуватися, підтримувати стосунки, грати, шукати і обмінюватися інформацією, що є позитивною стороною інтернет-комунікацій, однак ці процеси не позбавлені і негативного забарвлення, що полягає у поширенні в онлайн-середовищі небезпечних тенденцій, які несуть загрозу життю і здоров'ю дітей. Таким чином, кіберпростір несе в собі великий інформаційний та освітній потенціал, проте водночас містить ризики та загрози, які особливо загострюються в умовах воєнного стану. Це пов'язано як з тим, що діти більше часу проводять в кіберпросторі, враховуючи зокрема поширений дистанційний формат навчання, а також так і з появою нових ризиків та загроз, обумовлених війною.

Слід зазначити, що наразі в правовому полі та науковому середовищі відсутнє єдине тлумачення термінів «ризики», «загрози» та «небезпеки», а також розуміння їх співвідношення. Метою даного монографічного дослідження не є етимологічний та термінологічний дискурс (це питання потребує окремого ґрунтовного наукового дослідження), тому в межах нього ми використовуємо термін «загрози», оскільки саме він переважно використовується в контексті кібербезпеки в національному законодавстві, хоча в закордонних дослідженнях більше

¹ Про основні засади забезпечення кібербезпеки України: Закон України від 0 жовтня 2017 року № 2163-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text>. (дата звернення: 01.07.2024).

використовують термін «ризика («risks»²)». Так, посилення спроможностей національної системи кібербезпеки для ефективної протидії *кіберзагрозам* у сучасному безпековому середовищі є одним із напрямів реалізації пріоритетів національних інтересів України та забезпечення національної безпеки³. При цьому під *кіберзагрозою* слід розуміти наявні та потенційно можливі явища і чинники, що створюють *небезпеку життєво важливим національним інтересам* України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об'єктів⁴. В свою чергу *національні інтереси України* – це життєво важливі інтереси людини, суспільства і держави, реалізація яких забезпечує державний суверенітет України, її прогресивний демократичний розвиток, а також *безпечні умови життєдіяльності і добробут* її громадян⁵. Безумовно, безпека дітей становить національний інтерес України, особливо в умовах воєнного стану. *Охорона дитинства*, тобто система державних та громадських заходів, спрямованих на забезпечення повноцінного життя, всебічного виховання і розвитку дитини та захисту її прав, визначається як стратегічний загальнонаціональний пріоритет, що має важливе значення для забезпечення національної безпеки України⁶.

Загрози безпеці дітей в кіберпросторі можна визначити як наявні та потенційно можливі явища і чинники, що створюють *небезпеку життєдіяльності і добробуту* дітей, справляють негативний вплив на їх фізичний, психічний, моральний розвиток та поведінку. Важливо вживати правових та організаційних заходів, спрямованих на виявлення, аналіз та попередження загроз в кіберпросторі з метою забезпечення безпеки та найкращих інтересів дітей.

² Classifying known and emerging online risks for children: a child practitioners' perspective. URL: https://core-evidence-eu.s3.amazonaws.com/documents/WP5_online-forum-III_event-report.pdf. (дата звернення: 01.07.2024).

³ Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України»: Указ Президента України від 14 вересня 2020 року № 392/2020. URL: <https://zakon.rada.gov.ua/laws/show/392/2020#Text>. (дата звернення: 01.07.2024).

⁴ Про основні засади забезпечення кібербезпеки України: Закон України від 05 жовтня 2017 року № 2163-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text>. (дата звернення: 01.07.2024).

⁵ Про національну безпеку України: Закон України від 21 червня 2018 року № 2469-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2469-19#n355>. (дата звернення: 01.07.2024).

⁶ Про охорону дитинства: Закон України від 26 квітня 2001 року № 2402-III. URL: <https://zakon.rada.gov.ua/laws/show/2402-14#Text>. (дата звернення: 01.07.2024).

1. Сучасні загрози безпеці дітей в кіберпросторі

Кіберпростір, як і реальний простір має свої особливості та специфічні загрози, назви яких доволі часто є іншомовного походження. Наприклад, такі явища, як секстинг, сексторшен, онлайн-грумінг, флеймінг, тролінг, тощо. Особливістю кіберпростору є його стрімкий розвиток, тому постійно з'являються нові загрози для безпеки дітей. Деякі з них миттєво набувають масового характеру (наприклад, в свій час групи смерті на кшталт «Синього кита») та поступово зникають з кіберпростору, проте більшість загроз має довготривалий (наприклад, віртуальні челенджі) або постійний характер (наприклад, кібербулінг, сексторшен, грумінг). Відповідно до дослідження Global Online Safety Survey 2024 67% підлітків повідомили, що зазнавали ризиків в Інтернеті⁷.

Одна із найбільш комплексних класифікацій ризиків заподіяння шкоди дітям, пов'язаних з використанням цифрового середовища, була запропонована мережею «EU Kids Online», відповідно до якої такі ризики в 2010 році були поділені на 3С: «content» (*ризики контенту* – дитина отримує попередньо виготовлений медіа контент, який може негативно вплинути на неї – наприклад, порнографія, зображення з мотивами насильства, катування, неправдива, маніпулятивна інформація, контент, пов'язаний з радикалізацією чи підтримкою ідей расистського, нацистського, дискримінаційного характеру тощо); «contact» (*ризики контакту* – діти можуть брати участь у взаємодіях, які загрожують їм – наприклад, грумінг, домагання, вербування екстремістськими угрупованнями, експлуатація тощо); «conduct» (*ризики поведінки* – діти беруть участь у взаємодіях між однолітками, які можуть виявитися згубними, – наприклад, обмін сексуальним контентом, кібербулінг, переслідування, підбурювання до заподіяння собі шкоди, фішинг, інша протиправна діяльність), а з 2018 року доповнилися 4С – «contract» (*ризики угод* – діти можуть погодитися на угоди, яких вони не розуміють в силу віку та досвіду, або отримати доступ до небезпечних товарів чи послуг (наприклад ножів, наркотиків, азартних ігор тощо). В 2021 році організація «CO:RE – Діти онлайн: дослідження та докази» доповнила дану класифікацію, звернувши увагу на «cross-cutting risks» (*наскрізні ризики* – вони можуть додатково супроводжувати будь-які інші ризики, наприклад розголошення персональних даних та приватної інформації, шкода психічному та

⁷ Global Online Safety Survey Results. URL: <https://www.microsoft.com/en-us/digitalsafety/research/global-online-safety-survey>. (дата звернення: 25.06.2024).

фізичному здоров'ю (надмірне використання, позбавлення сну), нерівність та дискримінація)⁸.

Global Online Safety Survey під час щорічного аналізу класифікує ризику в Інтернеті для дітей на: *особисті* (мова ворожнечі, кібербулінг, харасмент, аб'юз, погрози насильством); *неправдиву інформацію* (включає також дезінформацію); насильницький контент (графічне насильство та кров у реальному світі, терористичний і екстремістський контент); *сексуальні* (домагання, експлуатація, насильство, поширення інтимних фото без згоди); *самоушкодження* (суїцидальний контент та контент з самоушкодженнями). Так, звіт 2024 року демонструє, що серед ризиків, з якими стикаються діти в Інтернеті, найбільш розповсюдженою є неправдива інформація (50%); 44% дітей зазначали про особистісні ризику (з них 35% – мова ворожнечі, 20% – кібербулінг, харасмент та аб'юз, 16% – погрози насильством); 34% опитаних зустрічались з насильницьким контентом (з них 27% – графічне насильство та кров у реальному світі; 11% – терористичний і екстремістський контент); про сексуальні ризику зазначали 21% дітей (при цьому 14% вказали на сексуальні домагання; 10% – поширення інтимних фото без згоди; 8% – сексуальну експлуатацію та насильство); 14% дітей зустрічали в кіберпросторі контент з самоушкодженнями або суїцидом⁹.

Розглянемо окремі сучасні загрози безпеці дітей в кіберпросторі, зокрема онлайн грумінг, кібербулінг, секстинг, сексторшен, сталкінг, фішинг.

Онлайн грумінг – це побудова дорослим/групою дорослих осіб довірливих стосунків з дитиною (підлітком) з метою подальшого сексуального насильства онлайн чи у реальному житті. Термін «грумінг» не закріплено у міжнародному праві. В деяких юридичних системах, зокрема в Канаді, використовується термін «заманювання», а в Україні – «домагання дитини для сексуальних цілей» (ст. 156-1 Кримінального кодексу України).

Кібербулінг – психологічне, фізичне, економічне чи сексуальне насильство, тобто будь-яке умисне діяння (дія або бездіяльність) із застосуванням засобів електронних комунікацій, яке систематично вчиняється стосовно дитини або дитиною стосовно іншого учасника освітнього процесу. Наприклад, дитину цькують однокласники в Інтернеті за її зовнішній вигляд, відсутність дорогих речей, пишуть у

⁸ Livingstone, S., & Stoilova, M. (2021). The 4Cs: Classifying Online Risk to Children. (CO:RE Short Report Series on Key Topics). Hamburg: Leibniz-Institut für Medienforschung | Hans-Bredow-Institut (HBI); CO:RE - Children Online: Research and Evidence. <https://doi.org/10.21241/ssoar.7181>. (дата звернення: 25.06.2024).

⁹ Global Online Safety Survey Results. URL: <https://www.microsoft.com/en-us/digitalsafety/research/global-online-safety-survey>. (дата звернення: 25.06.2024).

приватні повідомлення образливі коментарі із невідомих акаунтів, домальовують до фото будь-що і публікують це на своїх сторінках, поширюють плітки та неправдиву інформацію про дитину, навмисно виключають її з онлайн-середовища. За даними одного із досліджень 2020 року кібербулінг має вплив на 45% дітей у всьому світі¹⁰. В Україні наразі використовується вузьке тлумачення на нормативно-правовому рівні терміну булінг із застосуванням засобів електронних комунікацій, яке прив'язане виключно до освітнього процесу. Однак, наразі на розгляді в Верховній Раді України перебуває законопроект № 6393-д від 09 червня 2023 року, яким передбачено розширення сфер життя дітей, які потребують захисту від булінгу, зокрема, у спорті, культурі, оздоровленні й відпочинку, лікуванні тощо¹¹. До різновидів кібербулінгу іноді відносять такі явища, як *флеймінг* – обмін короткими гнівними коментарями на форумах та в чатах, та *хепіслепінг* – напади на дитину в реальному житті та зйомка їх на відео для розміщення їх в Інтернеті.

Секстинг – це обмін власними фото-, відео- та текстовими матеріалами інтимного характеру, із застосуванням сучасних засобів зв'язку: мобільних телефонів, електронної пошти, соціальних мереж тощо. Наприклад, підлітки добровільно надсилають один одному свої оголені фото в приватні повідомлення. З правової точки зору такі діяння не є протиправними, проте вони можуть емоційно нашкодити дитині та створюють загрозу шантажу, вимагання та маніпуляцій, посилення залежності через страх опублікування матеріалів, вчинення сексуального насильства щодо дитини. Світова статистика свідчить, що секстинг це явище, яке поширене серед 22% дівчат та 18% хлопців до 18 років¹².

Сексторієн – це налагодження незнайомцями довірливих стосунків в Інтернеті з дитиною з метою отримання приватних матеріалів, інтимних фото та/або відео, шантажування ними та вимагання грошей чи додаткових матеріалів. Часто злочинці використовують несправжні профілі підлітків для налагодження контакту або залякують створити неіснуючий сексуалізований контент – поєднуючи обличчя дитини з тілом іншої людини через спеціальні додатки, якщо дитина не зробить те, що вони вимагають. Згідно дослідження Глобального інституту безпеки дітей Childlight, понад 300 мільйонів дітей у всьому світі

¹⁰ 2020 Child online safety index. URL: <https://www.dqinstitute.org/wp-content/uploads/2020/02/2020COSIRreport.pdf>. (дата звернення: 25.06.2024).

¹¹ Проект Закону про внесення змін до деяких законів України щодо запобігання насильству та унеможливлення жорстокого поводження з дітьми № 6393-д від 09 червня 2023 року. URL: <https://itd.rada.gov.ua/billInfo/Bills/Card/42087>. (дата звернення: 25.06.2024).

¹² Teenage Sexting Statistics. URL: <https://www.guardchild.com/teenage-sexting-statistics/>. (дата звернення: 25.06.2024).

постраждали від сексуального насильства в Інтернеті, 3,5% дітей зіштовхувались з сексуальним вимаганням («sexual extortion»)¹³. Наслідки сексторшену мають однаковий вплив на дівчат та хлопців будь-якого віку. Згідно досліджень Transparency International, 1 з 3 дітей, які мали досвід сексторшену, наносили собі шкоду, вчиняли спроби самогубства через отриману психологічну травму¹⁴. Більшість, хто зіштовхнувся з цим явищем, повідомляють про відчуття самотності, високої тривоги та депресивні думки.

Сталкінг (переслідування) – це умисна поведінка, яка полягає в повторному здійсненні загрозливої поведінки, спрямованої на іншу особу, що змушує його чи її боятися за свою безпеку. Це можуть бути дії, спрямовані на постійне спостереження та/або привертання уваги за допомогою соціальних мереж, дзвінків (як на мобільний телефон, так і у месенджерах), докучання та слідкування в кіберпросторі. Стамбульська конвенція, яка була ратифікована Україною у 2022 році, тобто вже під час дії воєнного стану, наголошує на важливості криміналізації даного діяння¹⁵.

Фішинг є одним із різновидів соціальної інженерії та може полягати у «зламуванні» поштових скриньок, серверів, сторінок у соціальних мережах з метою отримання особистої інформації дитини. Як правило, фішинг розрахований на недостатні навички з питань кібергігієни та як наслідок перехід за посиланнями, надісланими в повідомленні, які ведуть на несправжню сторінку сайту, на якій особа вводить справжню інформацію своїх логінів, паролів, банківських реквізитів, тощо. Після отримання цих даних, правопорушники можуть зняти гроші з рахунків дитини, вимагати грошей за повернення доступу до облікових записів в соціальних мережах та месенджерах, використовувати облікові записи дитини для прохання грошей у її знайомих, тощо.

Всі розглянуті нами сучасні загрози безпеці дітей в кіберпросторі об'єднує поміж іншим те, що їх назви мають іншомовне походження, тому вони не закріплені на нормативно-правовому рівні в Україні або взагалі, або саме з такою назвою. Термінологія має значення, особливо в питаннях виявлення та розслідування правопорушень, вчинених за допомогою Інтернету, на території різних країн. Неправильне вживання термінів може призводити до непорозуміння між колегами з різних

¹³ Into the Light Index. URL: <https://intothelight.childlight.org/>. (дата звернення: 25.06.2024).

¹⁴ Breaking the silence around sextortion. The links between power, sex and corruption. URL: https://images.transparencycdn.org/images/2020_Report_BreakingSilenceAroundSextortion_English.pdf. (дата звернення: 25.06.2024).

¹⁵ Конвенція Ради Європи про запобігання насильству стосовно жінок і домашньому насильству та боротьбу із цими явищами. URL: https://zakon.rada.gov.ua/laws/show/994_001-11#n2. (дата звернення: 25.06.2024).

країн, застосування невідповідних процедур, уникнення правопорушниками відповідальності та несвоєчасного захисту постраждалих осіб. Важливо слідкувати за появою нових термінів, усвідомлювати, які із них закріплені в правових документах, а які ні, як співвідносяться назви правопорушень, закріплених в міжнародних документах і національному законодавстві тощо.

В умовах воєнного стану особливої уваги потребують такі види загроз безпеці дітей в кіберпросторі як шкідливий (неналежний) контент та втягнення дітей в протиправну діяльність.

Дослідження організації «Ofcom» в Великобританії продемонструвало, що 32% дітей віком від 8 до 17 років, які користуються Інтернетом, бачили щось неприємне або тривожне. Діти всіх вікових груп вчиняють потенційно ризиковану поведінку в Інтернеті: 40% дітей зізнаються, що вказали фальшивий вік, щоб отримати доступ до нового сайту чи програми¹⁶. *Неналежний контент* – це контент, який не призначений за віком. *Шкідливий контент* – це контент, який може завдати шкоду дитині або спонукати її до небезпечних дій. Слід зазначити, що в національному законодавстві визначення даних явищ не закріплені. При цьому в ст.42 Закону України «Про медіа» з метою захисту дітей зазначається про обмеження поширення у матеріалах медіа (крім фільмів) інформації, що може завдати шкоди фізичному, психічному або моральному розвитку дітей та надається перелік такого контенту: 1) надмірне зосередження уваги на насильстві, а саме поширення висловлювань або зображень насильства, які не є обґрунтованими або є надмірними в контексті відповідної програми чи публікації; 2) позитивна оцінка нанесення, заподіяння самому собі каліцтва або вчинення самогубства, підбурювання до таких дій, надмірна і необґрунтована деталізація засобів і обставин самогубства; 3) демонстрування жорстокого поводження з тваринами, методів умертвіння тварин, демонстрація великим планом такої, що вмирає, або жорстоко понівеченої тварини, крім випадків, якщо така демонстрація необхідна для популяризації гуманного ставлення до тварин, за умови попередження глядачів про сцени жорстокості; 4) позитивна оцінка вандалізму; 5) позитивна оцінка злочинного діяння або ідеалізація злочинця, надмірно деталізовані моделювання злочинних дій та/або демонстрація дій, відтворення яких дітьми може бути небезпечним для їхнього здоров'я і життя; 6) позитивна оцінка

¹⁶ Children and parents: media use and attitudes report 2024. URL: <https://www.ofcom.org.uk/media-use-and-attitudes/media-habits-children/children-and-parents-media-use-and-attitudes-report-2024-interactive-data/>. (дата звернення: 25.06.2024).

залежності від наркотичних, токсичних, психотропних речовин, тютюну чи алкоголю, а також від інших речовин, які використовуються або можуть використовуватися з метою одурманення, захоплення їх вживання, виробництва, розповсюдження чи придбання, крім творів мистецтва; 7) нецензурні висловлювання, слова, непристойні жести, крім випадків використання у творах мистецтва або відтворення у повідомленнях про новини дня або поточні події, що мають характер звичайної прес-інформації; 8) заклики грати в азартні ігри, спонукання до участі в азартних іграх, крім випадків, передбачених законами України; 9) демонстрація великим планом тіла померлої, такої, що вмирає, або жорстоко понівеченої людини, крім випадків, якщо така демонстрація необхідна для ідентифікації особи, за умови попередження глядачів про сцени жорстокості¹⁷. Онлайн-медіа можуть поширювати таку інформацію за умови забезпечення належного попередження про потенційну шкідливість такої інформації для дітей. На наш погляд, недоцільним є вичерпність такого переліку. Так, до неналежного та шкідливого контенту можуть також відноситись, наприклад, публікації результатів обстрілів, фото/відео/прямі трансляції із подібних локацій, порноконтент тощо. Згідно з результатами одного із досліджень, більшість (83%) дітей в Україні побачили вперше сексуальний контент у віці 7-13 років, 59,8% побачили його неочікувано самостійно, 12,6% - хтось показав неочікувано, лише 7,8% самостійно шукали подібний контент¹⁸. Наслідками перегляду неналежного контенту дітьми можуть бути: психологічна травматизація від побаченого; нав'язливе переживання страху; нормалізація насильства, ранніх ставевих відносин, ризикованої поведінки; нездорові очікування щодо інтимних стосунків; виникнення суїцидальних намірів тощо. Перегляд порнографії у дитячому віці нормалізує раннє сексуальне експериментування та заохочує сексуальну активність задовго до того, як діти будуть емоційно, соціально чи інтелектуально готові до цього. Часто такий матеріал зображає секс як випадковий, незахищений та насильницький.

Під час воєнного стану чимало людей втратили домівки і родинні накопичення, що спонукає дітей та їх батьків шукати способи заробітку. Брак інформації про загрози в кіберпросторі, їх причини та способи захисту у дітей призводять до того, що вони стають легкою мішенню для російських військових, які вербують їх для пошуку та збору

¹⁷ Про медіа: Закон України від 13 грудня 2022 року № 2849-IX. URL: <https://zakon.rada.gov.ua/laws/show/2849-20#Text>. (дата звернення: 01.07.2024).

¹⁸ Сексуальне насильство над дітьми та сексуальна експлуатація дітей в Інтернеті в Україні: аналітичний звіт. URL: <https://drive.google.com/file/d/1qPWJZ140hv24dZJcC1mJv7yVwbrMVIEK/view>. (дата звернення: 25.06.2024).

розвідувальної інформації. Адже якщо діти недостатньо знають про цифрову безпеку та загрози в інтернеті, а їх ще й мотивують грошима, зростає ризик того, що їх *втягнуть у протиправну діяльність*. Це створює загрозу вже не лише фізичному, психічному та моральному розвитку дитини, а й національним інтересам України в контексті збереження її територіальної цілісності та суверенності. Підбурюючи дітей до протиправної діяльності, самі зловмисники прагнуть залишатися в стороні та уникнути кримінальної відповідальності. Під час втягнення дітей у протиправну діяльність доросла особа, як правило, здійснює фізичне насильство або психологічний вплив через переконання, залякування, підкуп, обман тощо. Непоодинокими є випадки, коли діти готові виконувати протиправні дії, в тому числі адміністрування каналів в соціальних мережах та месенджерах, спрямованих на підбурювання до протиправних, доведення до самогубства, надання координат розташування українських військових, поширення інформації про розташування військ і роботу ППО; надання інформації за винагороду, знищення майна військовослужбовців тощо. Дорослим слід усвідомлювати, чому діти погоджуються на це, які шляхи втягнення використовують правопорушники та що можуть зробити батьки для захисту своїх дітей від цієї загрози. Так, по-перше, в кіберпросторі діти особливо вразливі через феномен “Ілюзія спальні”, адже вважають, що вдома вони в цілковитій безпеці і не розуміють, як дії в онлайн середовищі можуть призвести до негараздів у реальному житті. Важливо фокусувати їх увагу на тому, що дії, зроблені онлайн, мають наслідки у офлайн світі. По-друге, діти, які цікавляться онлайн іграми, можуть спокуситись на пропозицію, яка викликає інтерес. Наприклад, сфотографувати якийсь об’єкт за донат у грі, або надіслати фото/приватну інформацію про батьків або саму дитину за «скін», «бокс», «лутбок». Важливо формувати у дітей розуміння реальної небезпеки таких пропозицій та неухильного настання відповідальності за їх вчинення. Також діти можуть погодитись виконувати протиправні дії в результаті шантажу, залякування, погроз. Тому важливо, щоб в оточенні дитини була доросла особа, якій вона довіряє і може розповісти про будь-які неприємності, з якими зіштовхнулася, в тому числі в кіберпросторі. Якщо такої дорослої особи немає, важливо інформувати дітей про можливість отримати підтримку та консультацію, звернувшись до спеціалізованих «гарячих» ліній. Це також сприятиме подоланню ще однією із можливих причин потрапляння в небезпечні ситуації в кіберпросторі – психологічній вразливості дітей під час війни (розірвані соціальні контакти, внутрішнє переміщення, біженці, батьки вирішують проблеми і не приділяють достатньо часу дітям).

Динамічний розвиток цифрових технологій в умовах сучасних геополітичних викликів обумовлює появу нових загроз для безпеки дітей в кіберпросторі. Тому діяння правопорушників не завжди можуть відповідати традиційно відомим на національному рівні юридичним складам правопорушень. Водночас завжди важливо: ідентифікувати та документувати протиправність таких діянь; шукати відповідні норми у ратифікованих Україною міжнародних та європейських документах; залучати до таких справ адвокатів, які можуть допомогти звернутись до ЄСПЛ для захисту порушених прав дитини, якщо в національному законодавстві немає відповідної норми; завжди діяти в найкращих інтересах дитини. Крім того, важливо проводити періодичні дослідження розповсюджених загроз для безпеки дітей в кіберпросторі. Адже, завдання дорослих – своєчасно виявляти нові види загроз та вживати всіх можливих правових та організаційних заходів, спрямованих на попередження настання шкідливих наслідків для дітей.

2. Правові та організаційні засади захисту дітей від загроз в кіберпросторі

Правові засади захисту дітей від загроз в кіберпросторі включають в себе як міжнародні та європейські стандарти, так і національне законодавство. Правові документи в кожній із цих груп можна поділити на загальні – ті, що в цілому присвячені забезпеченню та захисту прав дітей і в яких поміж іншим висвітлені питання забезпечення прав дітей в цифровому середовищі, та спеціальні – ті, що безпосередньо присвячені захисту прав дітей в кіберпросторі.

До загальних правових актів на міжнародному рівні можна віднести:

– *Конвенцію ООН про права дитини*. Хоча у Конвенції право дитини на захист від «онлайн» насильства над дітьми безпосередньо не згадується, Комітет з прав дитини у *Коментарі № 25 (2021) про права дитини в цифровому середовищі* підтверджує зобов'язання держав-учасниць захищати дітей від усіх форм насильства в цифровому середовищі.

– *Цілі сталого розвитку 2030*. Ціль 16.2 полягає в тому, щоб до 2030 року покласти край нарузі, експлуатації та всім формам насильства і тортур щодо дітей. Щоб знизити ризики, які несе в собі цифровий світ, і водночас зробити так, аби більше дітей та молодих осіб могли користуватися його благами, уряди, представники громадянського суспільства, місцеві спільноти, міжнародні організації та галузеві підприємства повинні об'єднати свої зусилля задля спільної мети.

Серед спеціальних актів на міжнародному рівні слід згадати:

– Люксембурзькі рекомендації¹⁹ – метою цього документа є надання інструкцій щодо розуміння та використання різних термінів і понять, з якими можуть стикатися у своїй роботі установи, які працюють над запобіганням і викоріненням усіх форм сексуальної експлуатації та сексуального насильства над дітьми. Слід зазначити, що у Люксембурзьких рекомендаціях наголошується на тому, що термін «дитяча порнографія» створює небезпеку, ніби дії вчиняються за згодою дитини і є законним матеріалом сексуального характеру. Від терміну «дитяча порнографія» поступово відмовляються, оскільки в ньому використано лексику, що не орієнтована на постраждалу особу, та яка може ненавмисно узаконити матеріали із сексуальним насильством над дітьми через застосування слова «порнографія»²⁰. Слід використовувати термін «матеріали (сексуального) насильства щодо дітей», а не «дитяча порнографія»²¹. Проте національне законодавство поки що не враховує дану рекомендацію.

– Глобальний посібник із удосконалення законодавчої бази для захисту дітей від сексуальної експлуатації та насильства в Інтернеті²². Має на меті надати вказівки щодо того, як зміцнити законодавчу базу для захисту дітей від сексуальної експлуатації та насильства в Інтернеті, зокрема: у законодавстві має бути визначено «контактну точку» для отримання повідомлень та надання негайної допомоги з метою розслідування злочинів, пов'язаних із сексуальною експлуатацією та насильством над дітьми в Інтернеті; необхідно створити спеціалізовані слідчі підрозділи правоохоронних органів, до повноважень яких входить розслідування випадків сексуальної експлуатації та насильства над дітьми в Інтернеті; «таємні розслідування» повинні бути дозволені, але регулюватися законом і відповідати міжнародним правовим стандартам; забезпечити можливість притягнення до відповідальності за спробу вчинити сексуальне насильство та експлуатацію дитини, навіть якщо фактично вчинення правопорушення було б неможливе (для охоплення випадків,

¹⁹ Luxembourg Guidelines. URL: <https://ecpat.org/luxembourg-guidelines/>. (дата звернення: 25.06.2024).

²⁰ Appropriate terminology. URL: <https://www.interpol.int/en/Crimes/Crimes-against-children/Appropriate-terminology>. (дата звернення: 25.06.2024).

²¹ Guidelines for Law Enforcement First Responders in Child Sexual Abuse and Exploitation Cases. URL: https://www.europol.europa.eu/cms/sites/default/files/documents/Grace%20Guidelines%202022_Public_0.pdf. (дата звернення: 25.06.2024).

²² Глобальний посібник із удосконалення законодавчої бази для захисту дітей від сексуальної експлуатації та насильства в Інтернеті. URL: <https://www.unicef.org/reports/legislating-digital-age>. (дата звернення: 25.06.2024).

коли правоохоронні органи прикидаються дитиною, іншим правопорушником («замовником») або співучасником). Дані рекомендації наразі не враховані на національному рівні.

До загальних правових актів на європейському рівні можна віднести:

– Стратегію Ради Європи з прав дитини (2022-2027) «Права дитини на практиці: від стабільної реалізації до спільного новаторства»²³, яка в тому числі акцентує увагу на житті без насильства та правах дитини в цифровому середовищі.

– Рекомендацію Комітету міністрів Ради Європи CM/Rec(2009)10 щодо інтегрованих національних стратегій захисту дітей від насильства²⁴, в якій наголошено, що особи, що відповідають за медіа, повинні цілком усвідомлювати свою відповідальність за все, що стосується демонстрації насильства та поширення потенційно шкідливого для дітей контенту. Це може втілюватися шляхом усунення чи блокування доступу до шкідливих матеріалів або через розробку автоматизованих систем класифікації контенту, впровадження механізмів контролю та подання скарг щодо якості контенту, тощо. Закон України «Про медіа» частково враховує дані рекомендації.

– Рекомендацію Комітету міністрів Ради Європи Rec(2001)16 щодо захисту дітей від сексуальної експлуатації²⁵, в якій серед заходів пропонується залучити постачальників послуг Інтернет до підвищення обізнаності про сексуальну експлуатацію та її ризики; визнати, що для правоохоронних органів необхідно мати можливість використовувати дані з'єднання для відстеження підозрілого контенту, а потім знаходити, ідентифікувати та допитувати тих, хто редагує чи поширює дитячу порнографію або заохочує чи підбурює до дитячої проституції; надавати інформацію батькам, опікунам, усім іншим, хто відповідає за дітей, і самим дітям про ризики сексуальної експлуатації в Інтернеті, форми, які вона може мати, і про те, як обмежити доступ до неї; створити гарячі лінії та заохочувати громадян повідомляти про випадки дитячої порнографії чи заохочення до дитячої проституції на веб-сайті, що дозволить відповідним правоохоронним органам вжити конкретних заходів.

²³ Стратегія Ради Європи з прав дитини на 2022-2027 роки «Права дитини на практиці: від стабільної реалізації до спільного новаторства». URL: <https://rm.coe.int/coe-strategy-for-the-rights-uk/1680a774c4>. (дата звернення: 25.06.2024).

²⁴ Керівні принципи політики Ради Європи щодо комплексних національних стратегій із захисту дітей від насильства. URL: <https://rm.coe.int/168046eb82>. (дата звернення: 25.06.2024).

²⁵ Recommendation Rec(2001)16 of the Committee of Ministers to member states on the protection of children against sexual exploitation. URL: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805e2c81. (дата звернення: 25.06.2024).

– *Стратегію ЄС з прав дитини*²⁶, яка акцентує увагу на шести тематичних сферах, які є пріоритетними для ЄС, серед яких «Цифрове та інформаційне суспільство: ЄС, де діти можуть безпечно орієнтуватися в цифровому середовищі та використовувати його можливості». Наголошено на важливості підтримувати акції медіаграмотності як частину освіти, розвивати здатність дітей критично оцінювати онлайн-контент, виявляти дезінформацію та образливі матеріали; підтримувати та сприяти роботі центрів безпечного Інтернету, а також підтримувати дитячі телефони довіри та гарячі лінії.

Серед спеціальних актів на європейському рівні слід згадати:

– *Конвенцію про кіберзлочинність (Будапештську конвенцію)*²⁷, в якій наголошується на важливості криміналізації: а) виготовлення дитячої порнографії з метою її розповсюдження за допомогою комп'ютерних систем; б) пропонування або надання доступу до дитячої порнографії за допомогою комп'ютерних систем; с) розповсюдження або передачі дитячої порнографії за допомогою комп'ютерних систем; д) здобуття дитячої порнографії за допомогою комп'ютерних систем для себе чи іншої особи; е) володіння дитячою порнографією в комп'ютерній системі чи на комп'ютерному носії інформації.

– *Конвенцію Ради Європи про захист дітей від сексуального насильства та сексуальної експлуатації (Лансаротську конвенцію)*²⁸, в якій серед іншого наголошено, що діти мають знати про ризики, пов'язані з сексуальною експлуатацією та сексуальним розбещенням, і мати можливість захистити себе. Незважаючи на те, що Конвенція ратифікована Україною ще у 2012 р., 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), а також одержання доступу до дитячої порнографії (ст. 301-1 ККУ) та проведення видовищного заходу сексуального характеру, у тому числі з використанням інформаційно-телекомунікаційних систем або

²⁶ Захист прав дітей у цифровому світі – один із стратегічних пріоритетів Європейської Комісії. URL:

<https://www.nrada.gov.ua/zahyst-prav-ditej-u-tsyfrovomu-sviti-odyn-iz-strategichnyh-priorytetiv-yevropejskoyi-komisiyi/>. (дата звернення: 25.06.2024).

²⁷ Конвенція про кіберзлочинність. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text. (дата звернення: 25.06.2024).

²⁸ Конвенція Ради Європи про захист дітей від сексуальної експлуатації та сексуального насильства. URL: https://zakon.rada.gov.ua/laws/show/994_927#Text. (дата звернення: 25.06.2024).

технологій, за участю неповнолітньої особи (ст. 301-2 ККУ)²⁹. Комітет Лансароте уточнив дію Конвенції щодо цифрового середовища, прийнявши низку документів, зокрема: Висновок про зображення та/або відеоматеріали непристойного чи явно сексуального характеру за участю дітей, які створюються, пересилаються та отримуються дітьми (6 червня 2019 року); Пояснювальний висновок про можливість застосування Лансаротської конвенції до сексуальних злочинів проти дітей, вчинених за допомогою інформаційних і комунікаційних технологій (ІКТ) (12 травня 2017 року).

– *Рекомендацію Комітету міністрів Ради Європи CM/Rec(2009)5 про заходи щодо захисту дітей від шкідливого контенту та поведінки та сприяння їх активній участі в новому інформаційному та комунікаційному середовищі*³⁰, в якій наголошується, що неможливо повністю усунути небезпеку впливу дітей на контент або поведінку, що несе ризик заподіяння шкоди, і що медіаграмотність для дітей, батьків і педагогів залишається ключовим елементом у забезпечення узгодженого захисту дітей від таких ризиків.

– *Рекомендацію Комітету міністрів Ради Європи CM/Rec(2014)6 «Посібник з прав людини для інтернет-користувачів»*³¹, основний меседж якої: права та основоположні свободи людини (у тому числі дитини) діють однаковою мірою офлайн та онлайн.

– *Рекомендацію Комітету міністрів Ради Європи CM/Rec(2018)7 щодо Керівних принципів поваги, захисту та реалізації прав дитини в цифровому середовищі та Посібник з питань прав дитини в цифровому середовищі для органів державної влади*³², у якому в тому числі перелічені основні ризики та загрози, пов'язані із цифровим середовищем, які здатні негативно вплинути на фізичне, емоційне та психологічне благополуччя дитини.

²⁹ Про внесення змін до деяких законодавчих актів України щодо імплементації Конвенції Ради Європи про захист дітей від сексуальної експлуатації та сексуального насильства (Лансаротської конвенції): Закон України від 18 лютого 2021 року. URL: <https://zakon.rada.gov.ua/laws/show/1256-20#Text>.

³⁰ Recommendation CM/Rec(2009)5 of the Committee of Ministers to member states on measures to protect children against harmful content and behaviour and to promote their active participation in the new information and communications environment. URL: [https://wcd.coe.int/ViewDoc.jsp?Ref=CM/Rec\(2009\)5&Language=lanEnglish&Ver=original&Site=CM&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogo=FFAC75](https://wcd.coe.int/ViewDoc.jsp?Ref=CM/Rec(2009)5&Language=lanEnglish&Ver=original&Site=CM&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogo=FFAC75). (дата звернення: 25.06.2024).

³¹ Посібник з прав людини для інтернет-користувачів та пояснювальний меморандум. URL: <https://tm.coe.int/16802e3e96>. (дата звернення: 25.06.2024).

³² Посібник з питань прав дитини в цифровому середовищі для органів державної влади. URL: <https://rm.coe.int/prems-091920-gbr-2576-it-handbook-ukr-web/1680a2dbeb>. (дата звернення: 25.06.2024).

– Директиву ЄС 2011/93/ЄС щодо протидії сексуальному насильству та сексуальній експлуатації дітей та дитячій порнографії³³, в якій визначені злочини стосовно дітей на сексуальному підґрунті, у тому числі з використанням інформаційно-комунікаційних технологій. Щодо діяльності правоохоронних органів стосовно розслідування таких правопорушень в Директиві зазначається про можливість для правоохоронних органів використовувати приховану особу в Інтернеті.

– *Цифрове десятиліття для дітей та молоді: нова європейська стратегія кращого Інтернету для дітей (BIK+)*³⁴, яка пропонує дії навколо трьох стовпів: 1) безпечний цифровий досвід, захист дітей від шкідливого та незаконного онлайн-контенту, поведінки та ризиків і покращення їхнього добробуту завдяки безпечному цифровому середовищу, яке відповідає віку; 2) розширення цифрових можливостей, щоб діти здобували необхідні навички та вміння безпечно та відповідально виражати себе в онлайн-середовищі; 3) активна участь, повага до дітей, надання їм права голосу в цифровому середовищі.

До загальних правових актів на національному рівні можна віднести:

– Закон України «Про охорону дитинства»³⁵, ст. 10 якого присвячена праву на захист від усіх форм насильства.

– Закон України «Про основні засади забезпечення кібербезпеки в Україні»³⁶, який визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки.

³³ Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32011L0093>. (дата звернення: 25.06.2024).

³⁴ Communication from the Commission to the European parliament, the Council, the European economic and social committee and the Committee of the regions a digital decade for children and youth: the new European strategy for a better Internet for kids (BIK+). URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2022:212:FIN>. (дата звернення: 25.06.2024).

³⁵ Про охорону дитинства: Закон України. URL: <https://zakon.rada.gov.ua/laws/show/2402-14#n2>. (дата звернення: 30.06.2024).

³⁶ Про основні засади забезпечення кібербезпеки в Україні: Закон України від 05 жовтня 2017 року № 2163-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text>. (дата звернення: 30.06.2024).

– *Постанову Кабінету Міністрів України «Про забезпечення соціального захисту дітей, які перебувають у складних життєвих обставинах» від 1 червня 2020 р. № 585*³⁷, якою затверджений порядок забезпечення соціального захисту дітей, які перебувають у складних життєвих обставинах, у тому числі дітей, які постраждали від жорстокого поводження, зокрема в кіберпросторі.

– *Закон України «Про медіа»*³⁸, в якому зазначається, що на території України в медіа та на платформах спільного доступу до відео забороняється поширювати порнографічні матеріали, а також матеріали, що заохочують сексуальну експлуатацію та насильство над дітьми, демонструють статеві відносини дітей, використовують образ дітей (візуальний запис образу дітей) у видовищних заходах сексуального чи еротичного характеру.

Також слід згадати *Стратегію кібербезпеки України*³⁹ та *План реалізації*⁴⁰, який містить ряд пунктів щодо дітей: 1) п. 17 передбачає розробку концептуальних підходів щодо реалізації державної політики у сфері забезпечення прав громадян у кіберпросторі (особливо найбільш вразливих груп населення, насамперед дітей); 2) п. 90 передбачає поглиблення співпраці з міжнародними організаціями у сфері захисту дітей від сексуального онлайн-насильства.

Слід зазначити, що проєкт Національної стратегії захисту прав дітей в цифровому середовищі на 2021 – 2026 роки, розроблений Міністерством цифрової трансформації України, так і не був прийнятий. Відсутність спеціального стратегічного документу на національному рівні безумовно негативно впливає на комплексність діяльності у цій сфері та відсутність належної гармонізації національного законодавства з положеннями міжнародних та європейських стандартів.

В контексті національного законодавства окрему увагу слід звернути на *відповідальність за вчинення протиправних дій щодо дітей або*

³⁷ Про забезпечення соціального захисту дітей, які перебувають у складних життєвих обставинах: постанова Кабінету Міністрів України від 01 червня 2020 року № 585. URL: <https://zakon.rada.gov.ua/laws/show/585-2020-%D0%BF#Text>. (дата звернення: 30.06.2024).

³⁸ Про медіа: Закон України від 13 грудня 2022 року № 2849-IX. URL: <https://zakon.rada.gov.ua/laws/show/2849-20#Text>. (дата звернення: 01.07.2024).

³⁹ Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України": Указ Президента України від 26 серпня 2021 року № 447/221. URL: <https://zakon.rada.gov.ua/laws/show/447/2021#Text>. (дата звернення: 25.06.2024).

⁴⁰ Про План реалізації Стратегії кібербезпеки України: рішення Ради Національної безпеки і оборони України від 30 грудня 2021 року: Указ Президента України від 1 лютого 2022 року № 37/2022. URL: <https://zakon.rada.gov.ua/laws/show/n0087525-21#Text>. (дата звернення: 25.06.2024).

дітьми в кіберпросторі. За протиправні діяння щодо дітей винні несуть покарання відповідно до законодавства України. Це не залежить від того, відбулося правопорушення онлайн чи офлайн. Те, що в нормах права, які передбачають відповідальність за вчинення правопорушення, не зазначається безпосередньо спосіб їх вчинення за допомогою інформаційно-комунікаційних технологій, не означає, що у такому разі відповідальність не наставатиме. Внаслідок протиправних діянь щодо дітей, вчинених з використанням інформаційно-комунікаційних технологій, настають різні види юридичної відповідальності.

Так, *до адміністративної відповідальності* можливе притягнення за вчинення наступних правопорушень: поширення неправдивих чуток (ст. 173-1 КУпАП); вчинення домашнього насильства, насильства за ознакою статі, невиконання термінового заборонного припису (ст. 173-2 КУпАП); булінг (цькування) учасника освітнього процесу (ст. 173-4 КУпАП). У разі, якщо протиправне діяння щодо дитини було вчинено особою, яка не досягла віку відповідальності, *до адміністративної відповідальності можуть бути притягнені батьки останньої або особи, що їх замінюють.*

Настання *кримінальної відповідальності* тягне вчинення зокрема таких правопорушень: вчинення домашнього насильства (ст. 126-1 ККУ); торгівля людьми (ст. 149 ККУ); сексуальне насильство (ст. 153 ККУ); примушування до вступу в статевий зв'язок (ст. 154 ККУ); вчинення дій сексуального характеру з особою, яка не досягла шістнадцятирічного віку (ст. 155); розбещення (ст. 156 ККУ); домагання дитини для сексуальних цілей (ст. 156-1 ККУ); порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер (ст. 163 ККУ); одержання доступу до дитячої порнографії, її придбання, зберігання, ввезення, перевезення чи інше переміщення, виготовлення, збут і розповсюдження (ст. 301-1 ККУ); проведення видовищного заходу сексуального характеру за участю неповнолітньої особи (ст. 301-2 ККУ) тощо. Перелік правопорушень, безумовно, не є вичерпним. Окремий фокус уваги слід звернути на можливе настання *відповідальності батьків (опікунів, піклувальників)* потерпілої від таких правопорушень дитини відповідно до ст. 166 ККУ «Злісне невиконання обов'язків по догляду за дитиною або за особою, щодо якої встановлена опіка чи піклування» у разі, якщо правопорушення щодо дитини спричинило тяжкі наслідки і було вчинено в результаті їх злісного невиконання обов'язків по догляду за дитиною.

Крім відповідальності фізичних осіб за вчинення протиправних дій стосовно дітей в Інтернеті в Україні передбачена також відповідальність

юридичних осіб. Так, Закон України «Про медіа»⁴¹ передбачає настання *відповідальності медіа* у вигляді фінансових санкцій за: поширення інформації, що може завдати шкоди фізичному, психічному або моральному розвитку дітей; поширення порнографічних матеріалів, а також матеріалів, що заохочують сексуальну експлуатацію та насильство над дітьми, демонструють їхні статеві відносини, використовують образ дітей (його візуальний запис) у видовищних заходах сексуального чи еротичного характеру; порушення вимог щодо нерозголошення інформації про дитину без письмової згоди хоча б одного з батьків або законних представників, за винятком випадків, якщо це здійснюється в найкращих інтересах дитини.

Одним з факторів, які сприяють протиправним діям дітей в Інтернеті є вплив підбурювачів та організаторів з числа дорослих осіб, які самі прагнуть залишатися в стороні та уникнути кримінальної відповідальності. Слід пам'ятати, що за *втягнення неповнолітніх у протиправну діяльність* (як офлайн, так і офлайн) передбачена кримінальна відповідальність (ст.304 ККУ).

Крім адміністративної та кримінальної відповідальності за вчинення протиправних дій стосовно дітей в інтернеті, може наставати *цивільно-правова відповідальність*, зокрема у вигляді відшкодування потерпілій стороні завданої моральної шкоди.

Зважаючи на стрімкий розвиток цифрових технологій, правове регулювання відповідальності за протиправні дії в кіберпросторі, зокрема щодо дітей, не встигає своєчасно реагувати на загрози, які виникають. Можна провести аналогію з протидією наркотичним засобам та психотропним речовинам: поки одні із нових засобів або речовин будуть внесені у перелік заборонених, з'являють нові. Проте відсутність відповідальності за певні загрози в кіберпросторі не означає, що можна бездіяти. Консолідація зусиль для недопущення використання кіберпростору в протиправних цілях відповідно до п.9 ч.1 ст. 7 Закону України «Про основні засади забезпечення кібербезпеки України»⁴² є одним із принципів забезпечення кібербезпеки. Важливо вчити дітей, батьків та тих, хто працює з дітьми, як зберігати докази для притягнення винних до відповідальності, на яких ресурсах можна знайти інформаційну та психологічну підтримку. Наразі в Україні існують різні платформи, зокрема: Урядова консультаційна лінія з питань безпеки

⁴¹ Про медіа: Закон України від 13 грудня 2022 року № 2849-IX. URL: <https://zakon.rada.gov.ua/laws/show/2849-20#Text>. (дата звернення: 01.07.2024).

⁴² Про основні засади забезпечення кібербезпеки України: Закон України від 05 жовтня 2017 року № 2163-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text>. (дата звернення: 01.07.2024).

дітей в інтернеті 1545 (далі 3); чат-бот проєкту #stop_sexтинг⁴³; чат-бот «Кіберпес»⁴⁴; портал повідомлень про контент, який зображає сексуальне насильство над дітьми <https://report.iwf.org.uk/ua>.

Серед *організацій на міжнародному, європейському та національному рівні, які спеціалізуються на захисті дітей від загроз в кіберпросторі*, слід зазначити:

– *Міжнародний союз електрозв'язку (ITU)*, який започаткував ініціативу «Захист дитини в цифровому середовищі» (COP), покликаний об'єднати партнерів в інтересах створення безпечних і таких, що розширюють безпечні можливості в цифровому середовищі для дітей у цілому світі⁴⁵. ITU підготовлено рекомендації щодо захисту дітей у цифровому середовищі^{46 47}.

– *INHOPE* – міжнародна мережа гарячих ліній для повідомлень про матеріали сексуального насильства та сексуальної експлуатації щодо дітей онлайн⁴⁸. Держави-члени впровадили процедури «виявити та видалити» щодо контенту, який містить сексуальну експлуатацію та насильство щодо дітей, через національні гарячі лінії, за допомогою яких користувачі можуть повідомити про відповідні матеріали. Станом на 2024 рік мережа включає 54 гарячі лінії у 50 країнах. Щодо видалення контенту, то часто воно можливе без залучення правоохоронних органів, залежно від домовленості між операторами гарячих ліній, правоохоронними органами та провайдерами (наприклад, у Франції, Угорщині, Польщі, Португалії, Великій Британії тощо). У деяких країнах правоохоронні органи інформують провайдерів про необхідність видалення протиправного контенту (зокрема у Німеччині, Болгарії, Естонії, Фінляндії, Словаччині), а у деяких – необхідне рішення суду з можливістю, щоправда, тимчасово блокувати контент до винесення відповідного рішення (Кіпр та Хорватія). Якщо контент, що містить сексуальну експлуатацію та насильство щодо дітей, знаходиться у юрисдикції третьої країни, то держави-члени ЄС використовують

⁴³ Чат-бот проєкту #stop_sexтинг. URL: <https://stop-sexting.in.ua/chatbot/>. (дата звернення: 01.07.2024).

⁴⁴ Чат-бот «Кіберпес». URL: <https://chats.viber.com/kiberpes>. (дата звернення: 01.07.2024).

⁴⁵ Child Online Protection. URL: <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/COP/COP.aspx>. (дата звернення: 01.07.2024).

⁴⁶ COP 2020 Guidelines. URL: <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/COP-2020-Guidelines.aspx>. (дата звернення: 01.07.2024).

⁴⁷ Захист дітей у цифровому середовищі: рекомендації для органів державної влади. URL: <http://surl.li/wwwlct>. (дата звернення: 01.07.2024).

⁴⁸ INHOPE. URL: <https://www.inhope.org/EN/the-facts>. (дата звернення: 01.07.2024).

ресурси мережі INHOPE для його видалення, у інших випадках, гарячі лінії спрямовують звернення до відповідальних правоохоронних органів у цих країнах (часто через Європол чи Інтерпол). Здебільшого правоохоронні органи або галузеві регулятори формують список протиправних веб-сторінок та передають його провайдерам.

– *Insafe* – всевітня мережа центрів обізнаності, що сприяють безпечному та відповідальному використанню Інтернету молодими людьми⁴⁹. Кожен національний центр проводить просвітницькі та просвітницькі кампанії, працює з телефонною лінією довіри та тісно співпрацює з молоддю. *Insafe* підтримує кампанію День безпечного Інтернету, який щорічно відзначається приблизно у 180 країнах по всьому світу⁵⁰, в тому числі і в Україні⁵¹.

– *Інтерпол* – допомагає поліції виявити постраждалих від сексуальної експлуатації та насильства дітей шляхом аналізу фото і відео, знайдених в Інтернеті або на вилучених пристроях. Важливе значення має Міжнародна база даних зображень сексуальної експлуатації дітей (ICSE), яка використовує складне програмне забезпечення для порівняння зображень, щоб встановити зв'язки між постраждалими та місцями⁵².

– *Європейський центр боротьби з кіберзлочинністю (ЕСЗ) Європолу* надає допомогу та сприяє обміну досвідом у боротьбі з розповсюдженням матеріалів про жорстоке поводження з дітьми в онлайні середовищі, а також бореться з усіма формами злочинної поведінки в Інтернеті проти дітей, як-от грумінг, непристойні матеріали, створені власними силами, сексуальне вимагання та прямі трансляції в Інтернеті⁵³.

– *Проект #stop_sexting*⁵⁴, в рамках якого функціонує чат бот, розроблені рекомендації батькам та вчителям, а також розроблені та розміщені на офіційному сайті проекту матеріали з питань захисту дітей від насильства та експлуатації в Інтернеті. Проект має інтернет-портал

⁴⁹ About Safer Internet Day. URL: <https://www.saferinternetday.org/about>. (дата звернення: 01.07.2024).

⁵⁰ Safer Internet Day in your country. URL: <https://www.saferinternetday.org/in-your-country>. (дата звернення: 01.07.2024).

⁵¹ Ukraine Safer Internet Day Committee. URL: <https://www.saferinternetday.org/in-your-country/ukraine>. (дата звернення: 01.07.2024).

⁵² Our response to crimes against children. URL: <https://www.interpol.int/Crimes/Crimes-against-children/Our-response-to-crimes-against-children>. (дата звернення: 01.07.2024).

⁵³ Child Sexual Exploitation. URL: <https://www.europol.europa.eu/crime-areas-and-statistics/crime-areas/child-sexual-exploitation>. (дата звернення: 01.07.2024).

⁵⁴ Офіційний сайт проекту. URL: <https://stop-sexting.in.ua/>. (дата звернення: 01.07.2024).

повідомлень про матеріали, що зображують сексуальне насильство над дітьми⁵⁵. Всі повідомлення, які надсилаються через даний портал, обробляються громадською організацією Internet Watch Foundation (IWF), яка має відповідні політики щодо видалення контенту, який містить зображення сексуального насильства над дітьми.

У 2022 році в Україні було проведено оцінку ситуації щодо кібербезпеки дітей 10-18 років, за результатами якої в тому числі наголошено на необхідності привертати більше уваги до питань кібербезпеки дітей в Інтернеті саме під час війни та вимушеного переміщення великої кількості осіб⁵⁶. Важливим інструментом цього є якісна профілактика. Профілактична діяльність, спрямована на загрози для дітей в кіберпросторі, має ґрунтуватись на комплексному підході. Комплексний підхід, по-перше, пов'язаний з колом суб'єктів, які здійснюють таку діяльність: це і заклади освіти, і громадські (неурядові) організації, і органи (підрозділи) Національної поліції. При цьому важливо звернути увагу на належну взаємодію між всіма суб'єктами профілактики для забезпечення охоплення різних учасників освітнього процесу (учні, батьки, педагоги) та всіх здобувачів освіти, враховуючи їх вік та особливості розвитку. Також важливим фокусом уваги має бути належний рівень підготовки суб'єктів профілактики з цих питань, оскільки регулярно з'являються нові загрози для дітей в кіберпросторі. Переважно фахівці зосереджують увагу виключно на кібербулінгу, при цьому не обізнані з такими загрозами, як секстинг, онлайн ґрумінг, флеймінг, сексторшен тощо. По-друге, комплексність профілактичної діяльності стосується змістовного наповнення профілактичних (превентивних) заходів, спрямованих на забезпечення безпеки дітей в кіберпросторі. Завдання глобального суспільства полягає, з одного боку, у розробці й побудові досвіду для підлітків, який допомагає їм скористатися можливостями Інтернету, з іншого – у пом'якшенні проблем у житті, які частково опосередковані цифровими технологіями⁵⁷. Дійсно, зважаючи на неможливість та недоцільність заборони користуватись Інтернетом в сучасному світі, важливо навчити дітей користуватись ним безпечно, своєчасно розпізнавати загрози, а також знати, як реагувати на них. Профілактичні заходи для захисту

⁵⁵ Як повідомити про небажаний контент. URL: <https://stop-sexting.in.ua/send/>. (дата звернення: 01.07.2024).

⁵⁶ Звіт дослідження: Швидка оцінка ситуації щодо кібербезпеки дітей 10-18 років. Київ, 2022. С. 31-33. URL: <http://surl.li/pmxfoq>. (дата звернення: 01.07.2024).

⁵⁷ Palfrey J., Gasser U., Maclay C., Beger G. Digital natives and the three divides to bridge. In *The State of the World's Children*. 2011. Chapter 1: The emerging generation. P. 14-15. URL: http://www.unicef.org/sowc2011/pdfs/SOWC-2011-Main-Report_EN_02092011.pdf. (дата звернення: 01.07.2024).

дітей в кіберпросторі мають включати різні тематичні складові: необхідно забезпечити цифрову грамотність дітей, щоб гарантувати, що вони можуть отримувати вигоду від використання технологій, не наражаючись на небезпеку; важливо показати дітям приклад шкоди, якої можна зазнати в цифровому середовищі, проте це буде ефективно лише в тому разі, якщо це буде зроблено в межах ширшої програми цифрової грамотності, яка має відповідати віку та фокусуватися на навичках і компетенціях. Говорячи про шкоду, важливо одразу фокусуватись і на правилах безпеки, а також надавати контакти, за якими діти можуть звернутись по допомогу у разі необхідності; важливо, щоб програма навчання безпеки в цифровому середовищі включала принципи соціального та емоційного навчання, позаяк вони допоможуть дітям зрозуміти емоції та керувати ними, а отже, мати здорові стосунки на основі поваги як в цифровому середовищі, так і в реальному світі⁵⁸.

На нашу думку, враховуючи комплексність питань захисту дітей від загроз в кіберпросторі, крім розробки та прийняття тематичної Національної стратегії, яка має ґрунтуватись на аналізі сучасних загроз для безпеки дітей в кіберпросторі, з врахуванням викликів воєнного стану, доцільним є створення тематичної міжсекторальної робочої групи у складі Координаційної ради з питань захисту та безпеки дітей з внесенням відповідних доповнень у Положення про неї.

ВИСНОВКИ

Діти активно взаємодіють як з реальним, так і з кіберпростором, в кожному з яких можна зустріти загрози. Загрози безпеці дітей в кіберпросторі можна визначити як наявні та потенційно можливі явища і чинники, що створюють небезпеку життєдіяльності і добробуту дітей, справляють негативний вплив на їх фізичний, психічний, моральний розвиток та поведінку. Важливо вживати правових та організаційних заходів, спрямованих на виявлення, аналіз та попередження загроз в кіберпросторі з метою забезпечення безпеки дітей.

Динамічний розвиток цифрового середовища та виклики воєнного стану обумовлюють появу нових та стрімке поширення наявних загроз безпеці дітей в кіберпросторі, серед яких окрему увагу слід звернути на такі явища, як онлайн ґрумінг, кібербулінг, секстинг, сексторшен, фішинг, неналежний (шкідливий) контент, втягнення дітей в протиправну діяльність тощо. Важливо періодично досліджувати сучасні загрози безпеці дітей в кіберпросторі з метою своєчасного

⁵⁸ Захист дітей у цифровому середовищі: рекомендації для органів державної влади. URL: <http://surl.li/wwwlct>. (дата звернення: 01.07.2024).

вжиття правових та організаційних заходів, спрямованих на їх попередження та профілактику.

Профілактична діяльність, спрямована на забезпечення безпеки дітей в кіберпросторі, має ґрунтуватись на комплексному підході, який стосується: 1) кола суб'єктів, які залучаються до проведення відповідних профілактичних заходів та їх взаємодії; 2) кола осіб, які мають бути охоплені відповідними профілактичними заходами (діти, батьки, педагогічні працівники); 3) широкого підходу до змісту профілактичних заходів, та врахування сучасних викликів та загроз. Важливо, щоб суб'єкти профілактики були обізнані щодо сучасних загроз в кіберпросторі, отже доцільно передбачити механізми підвищення їх кваліфікації з цих питань.

Досвід України щодо формування правового та організаційного забезпечення захисту дітей від загроз в кіберпросторі має переважно фрагментарний характер, не в повній мірі відповідає міжнародним та європейським стандартам. Комплексність даного питання обумовлює доцільність розробки окремого тематичного стратегічного документу на національному рівні та створення тематичної міжсекторальної робочої групи у складі Координаційної ради з питань захисту та безпеки дітей. Це сприятиме більш системному підходу до захисту дітей від загроз в кіберпросторі.

АНОТАЦІЯ

Воєнний стан актуалізує питання захисту дітей від сучасних загроз, які існують не лише в реальному світі, а й в кіберпросторі. В межах монографічного дослідження запропоновано визначення поняття «загрози безпеці дітей в кіберпросторі», розглянуто наявні класифікації ризиків та звернуто увагу на найбільш поширені сучасні загрози безпеці дітей в кіберпросторі. Наголошено, що втягнення дітей у протиправну діяльність є особливо небезпечними в умовах воєнного стану, оскільки може спричинити шкоду не лише психічному і фізичному здоров'ю дитини, а й національній безпеці в контексті територіальної цілісності та суверенності.

Підкреслено важливість вжиття правових та організаційних заходів, які мають враховувати міжнародні та європейські стандарти захисту прав дітей в цифровому середовищі. Наведено перелік загальних та спеціальних тематичних правових документів на міжнародному, європейському та національному рівнях із зазначенням їх ключових фокусів уваги. Звернуто увагу на необхідність гармонізації тематичного національного законодавства з міжнародними та європейськими стандартами.

Акцентовано увагу на важливості комплексного підходу до профілактичної діяльності, спрямованої на забезпечення безпеки дітей в кіберпросторі, та розкрито його складові.

Підкреслена роль окремих організацій на міжнародному, європейському та національному рівнях, співпраця з якими посилить діяльність, спрямовану на захист дітей від загроз в кіберпросторі, а також запропоновано ряд заходів, спрямованих на забезпечення системного підходу в цій сфері.

Література

1. Конвенція про кіберзлочинність. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text. (дата звернення: 25.06.2024).

2. Конвенція Ради Європи про запобігання насильству стосовно жінок і домашньому насильству та боротьбу із цими явищами. URL: https://zakon.rada.gov.ua/laws/show/994_001-11#n2. (дата звернення: 25.06.2024).

3. Конвенція Ради Європи про захист дітей від сексуальної експлуатації та сексуального насильства. URL: https://zakon.rada.gov.ua/laws/show/994_927#Text. (дата звернення: 25.06.2024).

4. 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 року. URL: <https://zakon.rada.gov.ua/laws/show/1256-20#Text>.

5. Про медіа: Закон України від 13 грудня 2022 року № 2849-IX. URL: <https://zakon.rada.gov.ua/laws/show/2849-20#Text>. (дата звернення: 01.07.2024).

6. Про національну безпеку України: Закон України від 21 червня 2018 року № 2469-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2469-19#n355>. (дата звернення: 01.07.2024).

7. Про основні засади забезпечення кібербезпеки України: Закон України від 05 жовтня 2017 року № 2163-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text>. (дата звернення: 01.07.2024).

8. Про охорону дитинства: Закон України від 26 квітня 2001 року № 2402-III. URL: <https://zakon.rada.gov.ua/laws/show/2402-14#Text>. (дата звернення: 01.07.2024).

9. Проект Закону про внесення змін до деяких законів України щодо запобігання насильству та унеможливлення жорстокого поводження з дітьми № 6393-д від 09 червня 2023 року. URL: <https://itd.rada.gov.ua/billInfo/Bills/Card/42087>. (дата звернення: 25.06.2024).

10. Про забезпечення соціального захисту дітей, які перебувають у складних життєвих обставинах: постанова Кабінету Міністрів України від 01 червня 2020 року № 585. URL: <https://zakon.rada.gov.ua/laws/show/585-2020-%D0%BF#Text>. (дата звернення: 30.06.2024).

11. Про План реалізації Стратегії кібербезпеки України: рішення Ради Національної безпеки і оборони України від 30 грудня 2021 року: Указ Президента України від 1 лютого 2022 року № 37/2022. URL: <https://zakon.rada.gov.ua/laws/show/n0087525-21#Text>. (дата звернення: 25.06.2024).

12. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України»: Указ Президента України від 14 вересня 2020 року № 392/2020. URL: <https://zakon.rada.gov.ua/laws/show/392/2020#Text>. (дата звернення: 01.07.2024).

13. Глобальний посібник із удосконалення законодавчої бази для захисту дітей від сексуальної експлуатації та насильства в Інтернеті. URL: <https://www.unicef.org/reports/legislating-digital-age>. (дата звернення: 25.06.2024).

14. Захист дітей у цифровому середовищі: рекомендації для органів державної влади. URL: <http://surl.li/wwwlct>. (дата звернення: 01.07.2024).

15. Захист прав дітей у цифровому світі – один із стратегічних пріоритетів Європейської Комісії. URL: <https://www.nrada.gov.ua/zahyst-prav-ditej-u-tsyfrovomu-sviti-odyn-iz-strategichnyh-priorytetiv-evropejskoyi-komisiji/>. (дата звернення: 25.06.2024).

16. Звіт дослідження: Швидка оцінка ситуації щодо кібербезпеки дітей 10-18 років. Київ, 2022. С. 31-33. URL: <http://surl.li/pmxf0q>. (дата звернення: 01.07.2024).

17. Керівні принципи політики Ради Європи щодо комплексних національних стратегій із захисту дітей від насильства. URL: <https://rm.coe.int/168046eb82>. (дата звернення: 25.06.2024).

18. Офіційний сайт проекту #stop_sexтинг. URL: <https://stop-sexting.in.ua/>. (дата звернення: 01.07.2024).

19. Посібник з прав людини для інтернет-користувачів та пояснювальний меморандум. URL: <https://rm.coe.int/16802e3e96>. (дата звернення: 25.06.2024).

20. Посібник з питань прав дитини в цифровому середовищі для органів державної влади. URL: <https://rm.coe.int/prems-091920-gbr-2576-it-handbook-ukr-web/1680a2dbeb>. (дата звернення: 25.06.2024).

21. Сексуальне насильство над дітьми та сексуальна експлуатація дітей в Інтернеті в Україні: аналітичний звіт. URL: <https://drive.google.com/file/d/1qPWJZ140hv24dZJcCImJv7yVwbrMVIEK/view>. (дата звернення: 25.06.2024).

22. Стратегія Ради Європи з прав дитини на 2022-2027 роки «Права дитини на практиці: від стабільної реалізації до спільного новаторства». URL: <https://rm.coe.int/coe-strategy-for-the-rights-uk/1680a774c4>. (дата звернення: 25.06.2024).

23. Чат-бот проєкту #stop_sexтинг. URL: <https://stop-sexting.in.ua/chatbot/>. (дата звернення: 01.07.2024).

24. Чат-бот «Кіберпес». URL: <https://chats.viber.com/kiberpes>. (дата звернення: 01.07.2024).

25. Як повідомити про небажаний контент. URL: <https://stop-sexting.in.ua/send/>. (дата звернення: 01.07.2024).

26. About Safer Internet Day. URL: <https://www.saferinternetday.org/about>. (дата звернення: 01.07.2024).

27. Appropriate terminology. URL: <https://www.interpol.int/en/Crimes/Crimes-against-children/Appropriate-terminology>. (дата звернення: 25.06.2024).

28. Breaking the silence around sextortion. The links between power, sex and corruption. URL: https://images.transparencycdn.org/images/2020_Report_BreakingSilenceAroundSextortion_English.pdf. (дата звернення: 25.06.2024).

29. Classifying known and emerging online risks for children: a child practitioners' perspective. URL: https://core-evidence-eu.s3.amazonaws.com/documents/WP5_online-forum-III_event-report.pdf. (дата звернення: 01.07.2024).

30. Child Online Protection. URL: <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/COP/COP.aspx>. (дата звернення: 01.07.2024).

31. Child Sexual Exploitation. URL: <https://www.europol.europa.eu/crime-areas-and-statistics/crime-areas/child-sexual-exploitation>. (дата звернення: 01.07.2024).

32. Children and parents: media use and attitudes report 2024. URL: <https://www.ofcom.org.uk/media-use-and-attitudes/media-habits-children/children-and-parents-media-use-and-attitudes-report-2024-interactive-data/>. (дата звернення: 25.06.2024).

33. Communication from the Commission to the European parliament, the Council, the European economic and social committee and the Committee of the regions a digital decade for children and youth: the new European strategy for a better Internet for kids (BIK+). URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2022:212:FIN>. (дата звернення: 25.06.2024).

34. COP 2020 Guidelines. URL: <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/COP-2020-Guidelines.aspx>. (дата звернення: 01.07.2024).

35. Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation

of children and child pornography, and replacing Council Framework Decision 2004/68/JHA. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32011L0093>. (дата звернення: 25.06.2024).

36. Guidelines for Law Enforcement First Responders in Child Sexual Abuse and Exploitation Cases. URL: https://www.europol.europa.eu/cms/sites/default/files/documents/Grace%20Guidelines%202022_Public_0.pdf. (дата звернення: 25.06.2024).

37. Global Online Safety Survey Results. URL: <https://www.microsoft.com/en-us/digitalsafety/research/global-online-safety-survey>. (дата звернення: 25.06.2024).

38. INHOPE. URL: <https://www.inhope.org/EN/the-facts>. (дата звернення: 01.07.2024).

39. Internet World Stats. 2022. URL: <https://www.internetworldstats.com/stats.htm>. (дата звернення: 01.07.2024).

40. Into the Light Index. URL: <https://intothelight.childlight.org/>. (дата звернення: 25.06.2024).

41. Livingstone, S., & Stoilova, M. (2021). The 4Cs: Classifying Online Risk to Children. (CO:RE Short Report Series on Key Topics). Hamburg: Leibniz-Institut für Medienforschung | Hans-Bredow-Institut (HBI); CO:RE - Children Online: Research and Evidence. <https://doi.org/10.21241/ssor.7181>. (дата звернення: 25.06.2024).

42. Luxembourg Guidelines. URL: <https://ecpat.org/luxembourg-guidelines/>. (дата звернення: 25.06.2024).

43. Our response to crimes against children. URL: <https://www.interpol.int/Crimes/Crimes-against-children/Our-response-to-crimes-against-children>. (дата звернення: 01.07.2024).

44. Palfrey J., Gasser U., Maclay C., Beger G. Digital natives and the three divides to bridge. In *The State of the World's Children*. 2011. Chapter 1: The emerging generation. P. 14-15. URL: http://www.unicef.org/sowc2011/pdfs/SOWC-2011-Main-Report_EN_02092011.pdf. (дата звернення: 01.07.2024).

45. Recommendation Rec(2001)16 of the Committee of Ministers to member states on the protection of children against sexual exploitation. URL: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805e2c81. (дата звернення: 25.06.2024).

46. Recommendation CM/Rec(2009)5 of the Committee of Ministers to member states on measures to protect children against harmful content and behaviour and to promote their active participation in the new information and communications environment. URL: [https://wcd.coe.int/ViewDoc.jsp?Ref=CM/Rec\(2009\)5&Language=lanEnglish&Ver=original&Site=CM&BackCol](https://wcd.coe.int/ViewDoc.jsp?Ref=CM/Rec(2009)5&Language=lanEnglish&Ver=original&Site=CM&BackCol)

orInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFA
C75. (дата звернення: 25.06.2024).

47. Safer Internet Day in your country. URL: <https://www.saferinternetday.org/in-your-country>. (дата звернення: 01.07.2024).

48. Teenage Sexting Statistics. URL: <https://www.guardchild.com/teenage-sexting-statistics/>. (дата звернення: 25.06.2024).

49. Ukraine Safer Internet Day Committee. URL: <https://www.saferinternetday.org/in-your-country/ukraine>. (дата звернення: 01.07.2024).

50. 2020 Child online safety index. URL: <https://www.dqinstitute.org/wp-content/uploads/2020/02/2020COSIRreport.pdf>. (дата звернення: 25.06.2024).

Інформація про авторів:

Корнієнко Максим Вікторович,

доктор юридичних наук, професор,

проректор Одеського державного університету внутрішніх справ

вул. Успенська, 1, м. Одеса, 65000, Україна

Ковальова Олена Володимирівна,

кандидат юридичних наук, доцент, старший науковий співробітник,

професор кафедри адміністративної діяльності поліції

Одеського державного університету внутрішніх справ

вул. Успенська, 1, м. Одеса, 65000, Україна