DOI https://doi.org/10.30525/978-9934-26-277-7-143

RISKS AND THREATS TO CHILDREN IN THE DIGITAL ENVIRONMENT AS A SUBJECT OF CRIMINOLOGICAL RESEARCH

РИЗИКИ ТА ЗАГРОЗИ ДЛЯ ДІТЕЙ В ЦИФРОВОМУ СЕРЕДОВИЩІ ЯК ПРЕДМЕТ КРИМІНОЛОГІЧНОГО ДОСЛІДЖЕННЯ

Lubenets I. H.
Candidate of Sciences in Jurisprudence,
Senior Researcher, Leading Researcher
State Research Institute of the Ministry
of Internal Affairs of Ukraine
Kyiv, Ukraine

Лубенець І. Г.
кандидат юридичних наук,
старший дослідник,
провідний науковий співробітник
Державний науково-дослідний
інститут МВС України
м. Київ, Україна

На сьогодні, більшість населення у світі, у тому числі й в Україні, користуються Інтернетом та різними інформаційними технологіями. Цифрове середовище поступово охоплює всі сфери життя людини. На електронний документообіг переходять державні органи, а ефективність діяльності у банківській сфері, сфері транспорту та більшості підприємств ґрунтується на комунікації, що здійснюється за допомогою сучасних засобів зв'язку. Складно переоцінити величезний вклад інформаційних технологій у розвиток освіти і науки, оскільки в сучасних умовах дистанційне навчання стало порятунком для студентів та школярів. Науковці також мають можливість проводити онлайн-заходи, користуватися цифровими бібліотеками та публікувати наукові доробки. Одночасно, з розвитком інформаційних технологій зазнали змін більшість суспільних явищ і процесів, що зумовило трансформацію наукового світогляду. Ми цілком погоджуємося з Б.М. Головкіним, який зазначає, що предмет науки кримінології не може залишатися незмінним, його межі будуть розширюватися та охоплювати нові об'єкти соціальної дійсності [1, с. 170]. І це не дивно, оскільки завдяки використанню новітніх інформаційно-комунікаційних технологій значна кількість «звичайних» кримінальних правопорушень перейшла сьогодні до категорії так званих «кіберзлочинів» в широкому сенсі цього слова.

На сьогоднішній день кримінальні правопорушення та інші протиправні діяння, що вчиняються у цифровому середовищі, актуальна проблема, з якою у XXI столітті зіштовхнулась більшість країн світу. Причому її масштаби і ступінь гостроти постійно зростають. Жертвою вищеназваних протиправних діянь може бути будь-яка людина, яка користується сучасними засобами комунікації або мережею Інтернет. Часто їх жертвами стають неповнолітні, оскільки вони є найактивнішими користувачами Інтернету та інших засобів комунікації.

Слід зазначити, що з стрімким розвитком інформаційних технологій з'являються нові та удосконалюються існуючі способи скоєння правопорушень, у тому числі стосовно дітей. Це пояснюється певними особливостями правопорушень та інших антисуспільних діянь, які вчиняються в цифровому середовищі, що відрізняють їх від «звичайних» протиправних посягань та значно підвищують їх суспільну небезпечність. Зокрема, це:

– відносна комфортність, тобто готування та скоєння злочину здійснюється практично не відходячи від «робочого місця»;

– доступність, обумовлена тенденцією постійного зниження цін на комп'ютерну техніку та засоби комунікації;

– віддаленість об'єкта злочинних посягань, який може перебувати за тисячі кілометрів від місця скоєння злочину;

– велика множинність кіберзлочинів, яка полягає в тому, що суб'єкт злочину за допомогою комп'ютерних технологій протягом короткого періоду часу може вчинити декілька тисяч протиправних діянь;

– складність виявлення, фіксації і вилучення криміналістично-значущої інформації (слідової картини злочину) при виконанні слідчих дій для використання її в якості речового доказу і т. ін.;

– велика швидкість вчинення кіберзлочинів, які відбуваються практично миттєво і тому потребують швидкої реакції у відповідь;

– постійне оновлення форм та способів вчинення кіберзлочинів, яке здійснюється на тлі вдосконалення інформаційних технологій. Це вкрай утрудняє визначення ступеня та географії поширеності зазначених злочинів, прогнозування тенденцій змін її параметрів [2, с. 130].

Проаналізувавши вітчизняну та іноземну наукову літературу щодо переліку ризиків та загроз стосовно дітей в цифровому середовищі, необхідно сказати, що єдиної класифікації не існує. Це пояснюється кількома факторами: залежністю від аспекту дослідження ризиків,

критеріїв (параметрів) класифікації, наявності й ефективності застосування в конкретній країні механізму протидії та запобігання окремим ризикам, а також розвиненості системи навчання онлайн-користувачів (особливо дітей) безпечному поводженню в цифровому середовищі.

На наш погляд, найбільш вдалу класифікацію ризиків та загроз стосовно дітей в цифровому середовищі пропонує у своїй науковій роботі Солдатова Г.У. [3], де виокремлюються:

– **Контентні ризики** – виникають у процесі зіткнення з матеріалами, що містять протизаконну, неетичну та шкідливу інформацію, таку як: насильство, агресію, порнографію, нецензурну лексику, пропаганду суїциду та самопошкодження (селфхарм), наркотичних речовин, расизму, а також принижує почуття власної гідності тощо. Діти також нерідко виступають «творцями» шкідливого контенту, наприклад, коли пересилають посилання на шкідливий контент;

– **Комунікаційні ризики** – пов'язані з міжособистісними відносинами онлайн-користувачів, в результаті яких неповнолітній може стати жертвою протиправних посягань, таких як: кіберпереслідування, кібербулінг, кібернасильство, секстинг, грумінг, шантаж, вимагання, соціальний інжиніринг та ін.;

– **Споживчі ризики** – здебільшого охоплюють наступне коло дій: від платних підписок до небезпечного онлайн-шопінгу та фішингу;

– **Технічні ризики** – стосуються можливість пошкодження ПЗ, інформації, порушення її конфіденційності або зламу облікового запису, викрадення паролів та персональної інформації зловмисниками за допомогою шкідливого ПЗ (вірусів) та інших загроз (наприклад, шляхом відкриття електронного листа від незнайомця, що містить шкідливе програмне забезпечення чи переходу на незнайомими посиланнями тощо);

– **Інтернет залежність** – непереборний потяг до надмірного збільшення «екранного часу». У підлітковому середовищі найчастіше проявляється у формі захоплення відео-іграми, нав'язливої потреби спілкування в чатах, цілодобовому перегляді фільмів та серіалів у Мережі тощо [3, с. 98].

Слід вказати, що будь-яка класифікацію є умовною. Наприклад, схиляння до суїциду поєднує в собі ознаки двох видів ризиків: негативного контенту (аудіо, відео, література) з небезпечним контактом (спілкування на теми суїциду та самопошкодження в соцмережах, чатах, форумах тощо).

Одночасно, враховуючи зміни та вплив факторів реального життя, постійне удосконалення новітніх інформаційних технологій, постає необхідність у періодичному оновлюванні переліку онлайн-ризиків та загроз. Наприклад, в умовах війни в Україні країна-агресор розгорнула, так званий, другий фронт (кібервійну), де цифрове середовище використовується з метою маніпуляцій та дестабілізації ситуації в країні, збоїв у роботі державних інституцій, крадіжки конфіденційних даних, псування техніки, поширення фейків, вербування населення, у тому числі, дітей та ін. Окремої уваги потребують випадки залучення українських дітей російськими військовими до опосередкованої участі у збройному конфлікті, зокрема, для розвідки військових позиції та переміщення військової техніки, коригування вогню тощо. Втягування дітей до вищенаведеної діяльності російськими військовими нерідко здійснюється в цифровому середовищі: через Telegram, Facebook, месенджери тощо. І це не дивно, адже втрата особистих соціальних зв'язків, погіршення економічного становища сім'ї через втрату роботи батьками – все це спонукає дитину шукати нових друзів у цифровому середовищі, а також можливості підробітку. Одночасно, такі факти вимагають швидкого реагування з боку правоохоронних органів, а також наукового пошуку нових способів виявлення та запобігання їм.

Отже, у зв'язку із сьогоднішньою складною ситуацією, а також враховуючи зростанням рівня доступу до сучасних цифрових технологій, більшість з яких стали невід'ємною та, навіть, буденною складовою нашого щоденного вжитку (мобільний телефон, Інтернет тощо), проблема забезпечення безпеки дитини в цифровому середовищі лише посилюється.

Тому вивчення закономірностей і можливостей інформаційних технологій та цифрового середовища, а також їх використання у новітніх дослідженнях з метою запобігання та протидії злочинності (у тому числі стосовно дітей), виступає одним з базових шляхів розвитку сучасної кримінологічної науки.

Література:

1. Головкін Б. М. Теперішнє і майбутнє кримінології. *Проблемы законности*. 2020. № 149. С. 168–184.

2. Європіна І. В. Види протиправних діянь у сфері новітніх інформаційних технологій. *Вісник Академії адвокатури України*. 2010. № 3(19). С. 129–136.

3. Солдатова Г. У. Цифровое детство: компетентность и безопасность. Проекты Фонда развития Интернет. 2021. 126 с. URL: https://cutt.ly/rMCehnw

DOI https://doi.org/10.30525/978-9934-26-277-7-144

DESIGNING A HELP SYSTEM FOR DETECTING PC MALFUNCTIONS AND RECEIVING ADVICE ON THEIR ELIMINATION

ПРОЕКТУВАННЯ ДОВІДКОВОЇ СИСТЕМИ ПО ВИЯВЛЕННЮ НЕСПРАВНОСТЕЙ ПК ТА ОТРИМАННЯ ПОРАД З ЇХ УСУНЕННЯ

Lubko D. V.
Candidate of Technical Sciences, Associate Professor, Associate Professor at the Department of Computer Science
Dmytro Motornyi Tavria State Agrotechnological University
Zaporizhzhia, Ukraine

Лубко Д. В.
кандидат технічних наук, доцент, доцент кафедри комп'ютерних наук
Таврійський державний агротехнологічний університет імені Дмитра Моторного
м. Запоріжжя, Україна

Метою роботи є проектування довідкової системи для виявлення несправностей ПК та отримання порад по їх усуненню, за допомогою якої можна буде попереджати ці несправності [1, с. 15]. Якщо вони все ж трапилися – усувати їх, та проводити періодичне діагностування різних окремих комплектуючих вашої комп'ютерної техніки. Цільова аудиторія даного програмного забезпечення – це по-перше домашні користувачі та фахівці-початківці сервісних центрів з початковою та середньою комп'ютерною освітою. Дана довідкова система – це фактично інструмент для швидкого діагностування деяких частин ПК, а саме – апаратної частини, зовнішніх пристроїв та операційної системи або всіх частин одночасно. Головне завдання даної системи – надати особам, які не володіють в досконалості знаннями влаштування персональних комп'ютерів (або ноутбуків), чітку та детальну інформацію щодо існуючих дефектів системи, причин їх виникнення та варіантів вирішення проблеми та їх усунення.