https://zakon.rada.gov.ua/laws/show/580-19/conv#Text.

4. Про затвердження Інструкції з організації роботи підрозділів ювенальної превенції Національної поліції України : наказ МВС України від 19.12.2017 № 1044. URL : https://zakon.rada.gov.ua/laws/show/z0686-18.

Ростислав МОЛЧАНОВ
доцент кафедри адміністративного права, процесу та адміністративної діяльності Дніпропетровського державного університету внутрішніх справ, кандидат юридичних наук

КІБЕРБЕЗПЕКА ДІТЕЙ ПІД ЧАС ВОЄННОГО СТАНУ

У світі, в якому технології та Інтернет стали невід'ємною частиною життя, забезпечення безпеки дітей в онлайн-середовищі стало завданням першочергового плану, особливо в умовах воєнного конфлікту. Сучасна війна – це не тільки кровопролитні бої, але й інформаційне протистояння. Інформаційний фронт є важливою складовою: «…кіберпростір визначається різноманіттям з'єднань, що одночасно переводить його в категорію зони ризику. Усі зростаючі розміри, охоплення і функції збільшують можливості як законослухняних громадян, так і ворожих гравців. Супернику необхідно лише атакувати слабку ланку мережі, щоб завоювати новий плацдарм і отримати переваги». Саме завдяки всесвітній мережі Інтернет ворогуючі сторони можуть формувати в голові у людей саме те бачення і ту позицію, котрі більш вигідні їм і направлені проти іншої сторони. Дезінформація – найпоширеніший метод маніпуляції в інформаційному просторі, особливо в умовах війни.

Окрім цього, широко застосовуються кібератаки, направлені як на офіційні державні сайти, сервери, банківські установи, так і на соціальні мережі звичайних громадян. Мета таких атак може бути різною: від банального способу заважати нормальній роботі підприємств, установ, організацій – і до отримання необхідної інформації, що має важливе значення для держави-цілі (про переміщення чи розміщення військ, розкриття планів дій, спеціальних операцій тощо), заволодіння чужими коштами тощо. Також може бути здійснено залякування населення, шантаж із метою використання особи, зокрема її психологічного стану, у своїх цілях. Тому важливим завданням як держави, так і самих громадян є захист щонайперше своїх особистих даних в інформаційному просторі. Для цього держава повинна піклуватися про те, щоб якомога більше громадян були інформаційно грамотними.

Найбільш вразливою до загроз у кіберпросторі категорією населення

можна вважати дітей. По-перше, дитина, особливо малолітня, не до кінця усвідомлює ступінь небезпеки своїх діянь. По-друге, діти є більш психологічно вразливими, ніж дорослі, а тому на них легко діють маніпуляції та психологічні прийоми, за допомогою яких ворог намагається досягнути поставленої мети.

Виразним прикладом є випадки вербування дітей російською федерацією із використанням соціальних мереж та інших доступних засобів мережі Інтернет [2]. Ще один приклад вербування дітей рф – «залучення» їх для фотографування та передачі даних (у тому числі координат) про критичну інфраструктуру через створену російськими спецслужбами гру: «в одному з додатків учасники мають шукати так звані «коробки» з віртуальними призами, які можна обміняти на електронні гроші. Під час проходження маршруту діти здійснюють фотофіксацію місцевості, об'єктів військової та критичної інфраструктури на території різних населених пунктів» [3].

Як бачимо, використання психологічної незрілості та вразливості дітей росією під час війни – це не вигадка, а реальність. Ось чому необхідно піклуватися про кіберпезпеку та кібергігєну дітей. Для цього нами було виведено певні рекомендації. По-перше, батьки та вчителі повинні роз'яснити дітям про можливі кіберзагрози та навчити їх розрізняти правдиву інформацію від дезінформації. По-друге, необхідно встановити антивірусне програмне забезпечення на пристроях дітей для захисту від потенційно небезпечних програм та файлів, котрі діти можуть встановити на свій гаджет, а також роз'яснити їм про небезпеку переходу за невідомими посиланнями. По-третє, використання батьківського контролю дозволяє відстежувати їхню активність та обмежувати доступ до небезпечних вебсайтів і контенту. І, по-четверте, дітям необхідно пояснювати важливість захисту особистих даних в мережі, говорити про те, що не можна ділитися особистою інформацією, а також слід бути обережними й уважними під час спілкування в Інтернеті. Такий комплексний підхід дозволить значно зменшити кількість випадків вербування дітей іноземними службами, а також знизити рівень загрози дітям у кіберпросторі в цілому. Слід зазначити, що ефективно вирішувати питання забезпечення кібербезпеки можливо лише при системному використанні засобів усіх структурних рівнів, зважаючи на питому вагу кожного з них для конкретної цільової групи та/або сфери застосування відповідної людиноцентричної системи [1].

Отже, кібербезпека дітей під час воєнного стану є досить важливим завданням. Тому кожен повинен робити свій внесок у забезпечення їхньої безпеки в інформаційному просторі, зокрема в мережі Інтернет. Подальші дослідження цієї проблематики доцільно зосередити на детальному вивченні структури кіберзагроз, що можуть спіткати дітей, а також методів протидії таким загрозам.

1. Биков В. Ю., Буров О. Ю., Дементієвська Н. П. Кібербезпека в цифровому навчальному середовищі. *Інформаційні технології і засоби навчання*. 2019. Т. 70. № 2. С. 313–331. URL : https://core.ac.uk/download/pdf/233898878.pdf.

2. Через канали, чати та ігри. Хто і як вербує українських підлітків під час війни. *rfi.* URL : https://www.rfi.fr/uk/україна/20230814-через-канали-чати-та-ігри-хто-і-як-вербує-українських-підлітків-під-час-війни.

3. Спецслужби рф вербували українських дітей через ігри в смартфонах. *Укрінформ.* URL : https://www.ukrinform.ua/rubric-society/3490910-specsluzbi-rf-verbuvali-ukrainskih-ditej-cerez-igri-v-smartfonah.html.

Назарій НАУМОВ
курсант ННІ права та підготовки фахівців для підрозділів Національної поліції
Науковий керівник:
д.ю.н., проф. **Роман МИРОНЮК**
(Дніпропетровський державний університет внутрішніх справ)

ОСОБЛИВОСТІ ВІДПОВІДАЛЬНОСТІ НЕПОВНОЛІТНІХ ЗА КУРІННЯ В ОСВІТНІХ ЗАКЛАДАХ

Питання паління неповнолітніми є дуже актуальним і становить вагому соціально-демографічну проблему, оскільки вживання тютюнових та нікотиновмісних виробів негативно вливає на здоров’я.

Саме тому в Україні створено нормативно-правові акти, що забороняють паління у таких місцях, як: ліфти, приміщення та території навчальних закладів, дитячі майданчики, зупинки, приміщення та території спортивних закладів, а також закладів фізичної культури та спорту тощо. Наведений перелік передбачено Законом України «Про заходи щодо попередження та зменшення вживання тютюнових виробів і їх шкідливого впливу на здоров’я населення» від 22.09.2005 [1], котрий створений із метою зменшення рівня вживання виробів із тютюну, обмеження доступу до них дітей, що забезпечує збереження їх здоров’я.

Також 08.11.2004 Міністерство освіти і науки Україні видало наказ № 855 «Про заборону тютюнокуріння в навчальних закладах і установах Міністерства освіти і науки України і затвердження заходів щодо проведення антинікотинової інформаційно-освітньої та профілактичної роботи серед дітей, учнівської та студентської молоді» [2], де вказано, що в закладах освіти заборонено вживання тютюнових виробів. Однак учні шкіл та студенти закладів професійно-технічної, вищої освіти із розвитком популярності електронних сигарет, вейпів, пристроїв для тютюнокуріння без їх згоряння