Побудова дієвої системи забезпечення кібернетичної безпеки вимагає від державних органів України чіткого визначення державної політики у цій сфері та випереджального реагування на динамічні зміни, що відбуваються у світі в сфері забезпечення кібернетичної безпеки [4].

Отже, ефективне державне управління у сфері забезпечення кібернетичної безпеки в Україні є необхідною умовою розвитку інформаційного суспільства. Тому, розбудова дієвої системи кібернетичної безпеки є однією з найнагальніших завдань забезпечення національної безпеки України.

Література:

1. Дубов Д. В. Стратегічні аспекти кібербезпеки в Україні / Д. В. Дубов // Стратегічні пріоритети № 4(29). – 2013. – С. 119.
2. . Малиновський В. Я. Державне управління: Навчальний посібник. – 3-тє вид., переробл. та допов. – К.: Атіка, 2009. – 608 с.
3. Баранов О. А. Про тлумачення та визначення поняття «кібербезпека» / О. А. Баранов // Правова інформатика. – 2014. - №2 (42). – С.54- 62.
4. Лук`янчук Р. В. Державне управління кібернетичною безпекою: шляхи вдосконалення в сучасних умовах / Р. В. Лук`янчук // Електронне наукове фахове видання «Державне управління: удосконалення та розвиток» [Електронний ресурс]. – Режим доступу: http://www.dy.nayka.com.ua/?op=1&z=893

Інформаційна безпека дитини та її забезпечення Національною поліцією України

Дручек О.М.
аспірант кафедри адміністративного
права та адміністративного процесу,ОДУВС
Науковий керівник: Коропатов О.М.
кандидат юридичних наук, доцент
професор кафедри адміністративного права та адміністративного процесу ОДУВС

Глобальною світовою тенденцією сьогоденняє розширення та поглиблення розвитку інформаційної складової життєдіяльності людини і суспільства. Інформація стає ефективним інструментом керуючого впливу на соціальні системи та індивідів за схемою «керуючий вплив – бажаний результат», і саме цим визначається її важливість як чинника формування безпечного середовища у сфері суспільних відносин. Тому однією із складових поняття безпеки у широкому розумінні наразі визнається інформаційна (кібер-) безпека – стан захищеності життєво важливих інтересів людини і громадянина, суспільства і держави, при якому запобігається завдання шкоди через неповноту, несвоєчасність та недостовірність поширюваної інформації, порушення цілісності та доступності інформації, несанкціонований обіг інформації з обмеженим доступом, а також через негативний інформаційно-психологічний вплив та умисне спричинення негативних наслідків застосування інформаційних технологій.

В Указі Президента України «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України»» [1] йдеться про те, що кіберзлочинність стає транснаціональною та здатна завдати значної шкоди інтересам особи, суспільства і держави, а також про поширення в Україні випадків незаконного збирання, зберігання, використання, знищення, поширення, персональних даних, незаконних фінансових операцій, крадіжок та шахрайства у мережі Інтернет. Зазначеним нормативно-правовим актом виконання завдання забезпечення інформаційної безпеки покладається на систему державних органів, серед яких – Національна поліція України. Завданнями Національної поліції у цій сфері, зокрема, є: забезпечення захисту прав і свобод людини та громадянина, інтересів суспільства і держави від злочинних посягань у кіберпросторі; запобігання, виявлення, припинення та розкриття кіберзлочинів; підвищення поінформованості громадян про безпеку в кіберпросторі.

Особливо небезпечним інформаційний простір може стати для дітей, оскільки певні ресурси інтернету містять інформацію агресивного, жорстокого, аморального чи соціально небезпечного змісту, а надання переваги віртуального світу перед реальним справляє негативний вплив на психіку, фізичне і моральне здоров’я дитини, сприяє формуванню девіантної поведінки. Почасти підлітки, через вікові особливості психології та фізіології, поводяться у Мережі віктимно, навмисно провокуючи стосовно себе вчинення протиправних чи злочинних дій. Спеціалісти відзначають, що може йтися про встановлення незаконного контакту (грумінгу) зловмисника і дитини із метою подальших злочинних

дій; кіберпереслідування; он-лайн-насилля; шахрайство; порнографію тощо [2, с. 337]. Крім того, значну небезпеку для дитини становить формування т.зв. небажаного контенту, під яким фахівці розуміють матеріали непридатного для дітей чи протизаконного змісту – ті, які пропагують порнографію, наркотики, алкоголь, тютюнокуріння, екстремізм, ксенофобію, расизм, тероризм, національну, класову, соціальну ворожнечу, нерівність, асоціальну поведінку, насилля, агресію, суїцид, азартні ігри, шахрайство тощо [3, с.19]. Наразі, на основі аналізу звернень на Національну дитячу «гарячу лінію», можна констатувати збільшення вірогідності таких небезпек для дитини в Інтернеті, як-то: кібербулінг – цькування та переслідування в Інтернеті; «порно-помста» – публікування в соцмережах особистої інформації інтимного чи еротичного характеру без згоди власника інформації; екстремальні селфі – використання небезпечних місць в якості локацій для селфі (фотографій самих себе); «смертельні квести» – поширення груп в соцмережах, у яких дітям та підліткам пропонується виконувати небезпечні для життя завдання [4]. Спеціалісти наголошують, що діти стають жертвами кіберзлочинів через ігнорування певних правил інформаційної гігієни. Зокрема, найчастіше діти припускаються помилок, пов'язаних із: геотегінгом – позначенням власного географічного місця розташування в режимі реального часу; змістом акаунтів – поширення надміру інформації про себе і своє найближче оточення; невмінням відрізняти фейки від правдивої інформації, фішингової розсилки тощо. Крім того, особливістю підліткової свідомості є відсутність критичного мислення, нестійкість власних суджень. Для більшості із них першочергову цінність мають думки та оцінки друзів по інтернет-спільноті, а не авторитет батьків чи вчителів. За інформацією ЗМІ, протягом 2016-го року кількість звернень щодо небезпек для дітей в Інтернеті від дітей, батьків та небайдужих перевищила 45 тис., у 2015-ому році –38 тис, у 2014-ому – 27 тис. [5].

Відповідно до законодавства, підрозділом Національної поліції, який наділений спеціальною компетенцією у сфері протидії кіберзлочинності, зокрема, злочинів, суб'єктом посягання яких є права дитини, є Департамент кіберполіції НП України [6]. До складу Департаменту входять структурні підрозділи, які діють за міжрегіональним принципом та безпосередньо підпорядковані начальникові Департаменту. Відповідно до законодавства, Департамент забезпечує реалізацію державної політики у сфері протидії кіберзлочинності; здійснює інформаційно-аналітичне забезпечення керівництва Національної поліції України та органів державної влади про стан вирішення питань, віднесених до його компетенції. Завдання Департаменту щодо протидії кіберзлочинам, суб'єктом посягання яких є права дитини, визначено у Положенні про Департамент кіберполіції НП України, затвердженого наказом Національної поліції від 10.11.2015 № 85 [7]. Зокрема, це: участь у формуванні та забезпеченні реалізації державної політики щодо попередження та протидії кримінальним правопорушенням, механізм підготовки, учинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку; сприяння в порядку, передбаченому чинним законодавством, іншим підрозділам Національної поліції України у попередженні, виявленні та припиненні кримінальних правопорушень. Здійснюючи функції з виконання зазначених завдань, Департамент співпрацює з Департаментами превентивної діяльності та Карного розшуку Національної поліції України та їх територіальними підрозділами, Управлінням та територіальними ювенальної превенції, іншими органами та установами у справах дітей.

Наразі одним із напрямів роботи Департаменту кіберполіції у сфері забезпечення інформаційної безпеки дітей є протидія т.зв. «групам смерті», що набули широкого поширення в інтернет-просторі України, Росії, інших країн. Так, протягом 2017 р. Департаментом було вжито заходів, у результаті яких заблоковано 170 сторінок «суїцидальних» груп; ідентифіковано 44 300 осіб як таких, що можуть бути учасниками «груп смерті»; безпосередньо від самогубства врятовано 56 дітей – учасників квесту «Синій кит» та подібних до нього [8]. Але окремі аспекти цієї роботи потребують врегулювання на законодавчому рівні. Зокрема, відсутні норми права, відповідно до яких кіберполіція чи інший державний орган могли би зобов'язати заблокувати ту чи іншу інтернет-спільноту. Наразі це можливо тільки у межах досудового розслідування або через суд, і така процедура займає декілька тижнів чи місяців, але коли йдеться про блокування небезпечного для дітей акаунту у кіберпросторі – тут важливо зробити це найоперативніше.

Зазначене вище актуалізує посилення роботи щодо навчання дітей і підлітків основам кібербезпеки; покращення взаємодії підрозділів Національної поліції України щодо забезпечення прав і свобод дитини, зокрема, права на безпечне інформаційне довкілля; удосконалення національного законодавства у цій сфері.

Література:

1.Указ Президента України «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України». [Електронний ресурс]. – Режим доступу:http://zakon2.rada.gov.ua/laws/show/96/2016.

2. Юрченко О.Ю. Проблеми безпеки дітей в соціальних мережах та Інтернеты (віктимологічний аспект) / О.Ю. Юрченко// Порівняльно-аналітичне право. – 2013. – № 3. –С. 336-338.

3. Литовченко І., Максименко С, Болтівець С. та ін. Діти в Інтернеті6 як навчити безпеці у віртуальному світі: посібник для батьків.– К: ТОВ «Видавничий будинок «Аванпост-Прим», 2010.- 48 с.

4. Де криються загрози безпеці дітей в Інтернеті? Тези із 8-ого Українського форуму з управління Інтернетом IGF-UA [Електронний ресурс]. – Режим доступу:
http://netfreedom.org.ua/de-kryyutsia-zagrozy-bezpetsi-ditei-v-interneti/.

5. «Нам телефонували діти, які були героями смертельних квестів», — директорка гарячих ліній «Ла Страда-Україна» [Електронний ресурс]. – Режим доступу:http://osvita.mediasapiens.ua/mediaprosvita/kids/

6. Постанова Кабінету Міністрів України «Про утворення територіального органу Національної поліції» : від 13.10.2015 р. № 886
[Електронний ресурс]. - Режим доступу: http://zakon2.rada.gov.ua/laws/show/830-2015-%D0%BF

7. За матеріалами сайту Національної поліції України: https://www.npu.gov.ua/uk/publish/article/2185548.

8. Представник Кіберполіції про «групи смерті»[Електронний ресурс].- Режим доступу:http://www.osvita.mediasapiens.ua/mediaprosvita/kids/

Сучасне кіберсередовище держави як театр бойвих дій

Задерейко О.В.
кандидат технічних наук,
доцент кафедри інформаційних технологій
Національний університет «Одеська юридична академія»
Логинова Н.І.
кандидат практичних наук.,
доцент кафедри інформаційних технологій
Національний університет «Одеська юридична академія»
Троянський О.В.
кандидат технічних наук, доцент
директор Інституту інформаційної безпеки, радіоелектроніки та телекомунікацій
Одеського національного політехнічного університету

Згідно з військовими доктринами більшості країн світу, виділяються традиційні поля бою: суша, море, повітря, космос і кіберпростір, які у корені відрізняються від інших полів бою. Традиційні поля бою чітко визначені, відокремлені один від одного і розділяються державними кордонами і тому є локалізовані [1].

Останніми роками в інформаційному просторі багатьох країн обговорюється питання розв'язування кібервоєн – війн, в більшості випадків яких неможливо визначити не лише учасників, час їх початку і завершення, а й важко довести сам факт застосування кіберзброї. За своїми наслідками кібервійни можна порівняти з наслідками від застосування зброї масового ураження усіх видів. Зокрема, використання кіберзброї може бути замасковане під техногенні катастрофи, системні збої в роботі комп'ютерних мереж, автоматизованих систем тощо [2].

У сфері національної кібербезпеки держави головним військово-стратегічним завданням є забезпечення її стратегічної переваги за допомогою використання технологій електромагнітного спектру (ТЕС) для безумовного досягнення національних цілей в усіх областях при повному пригніченні можливостей потенційного супротивника реалізовувати власні спрямування.

Відсутність геополітичних і природних меж для електромагнітного спектру дозволяє здійснювати активні операції з використанням ТЕС практично в будь-якому місці незалежно від існуючих державних кордонів. З урахуванням того, що швидкість передачі електромагнітного імпульсу впритул наближається до швидкості світла, ці операції можуть проводитися в режимі реального часу і здійснюватися у часі – від частки мілісекунди до днів і місяців.

Надзвичайно важливо знати головну відмінність кіберзброї від інших типів озброєнь. Будь-яка складна кіберзброя може виступати як платформа, яка спочатку впроваджується в мережі і комп'ютери, потім здійснює шпигунські функції, а в потрібний момент активізується і виступає бойовим засобом,