МВС України
Харківський національний університет
внутрішніх справ

Координатор проектів ОБСЄ в Україні

АКТУАЛЬНІ ПИТАННЯ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ ТА ТОРГІВЛІ ЛЮДЬМИ

**Збірник матеріалів
Всеукраїнської науково-практичної
конференції**

(23 листопада 2018 року, м. Харків)

Харків
ХНУВС
2018

УДК 342.738(477)

Наталія Олександрівна ФІЛІПСЬКА,
кандидат юридичних наук,
викладач кафедри конституційного і міжнародного права
факультету № 4 (кіберполіції)
Харківського національного університету внутрішніх справ;
ORCID: https://orcid.org/0000-0002-9558-9422

ДЕЯКІ ПИТАННЯ РЕАЛІЗАЦІЇ МІЖНАРОДНИХ СТАНДАРТІВ У СФЕРІ КІБЕРБЕЗПЕКИ

Розвиток технологій та сучасних засобів зберігання інформації, спілкування є безперечним та одним із найвагоміших досягнень людства. У сьогоднішньому світі тенденція глобалізації, пов'язана із швидким розвитком технологій, має надзвичайно тісний зв'язок із глобальною мережею Інтернет та проблемами дотримання прав людини у цій сфері. Зокрема, це стосується права на приватність та на захист інформації про особу. Не завжди існуюче у певних організаціях та закладах програмне забезпечення в змозі протистояти атакам хакерів та захистити персональні дані особи, які містяться в закритих інформаційних базах.

Щоденне використання високотехнологічних пристроїв більшістю населення земної кулі не лише оптимізує життя та спрощує доступ до корисної інформації, а й може бути загрозою для тієї інформації, що охороняється законом. Все більша кількість осіб у різних країнах світу стають жертвами атак кіберзлочинців та кібершахраїв та телефонних шахраїв. Приватна інформація особи часто стає доступною та використовується для скоєння злочинів. Тому безпека та захист інформації стали проблемою номер один цього століття.

Високий рівень освіченості молоді у галузі сучасних інформаційних технологій, негативна тенденція до зниження рівня життя в Україні, високий рівень безробіття та обмежені можливості працевлаштування є чинниками того, що особи заради наживи або із власних мотивів використовують свої знання з метою заволодіння приватною інформацією про особу. Експерти зазначають, що Україна – дуже важливий центр хакерства, поряд із Росією, Бразилією, Китаєм та меншою мірою – Індією [1, с. 91].

За даними Міжнародної торгової палати, злочинність у сфері кіберпростору зростає пропорційно кількості користувачів глобальної мережі Інтернет [2, с. 41]. У травні 2017 року журнал Форбс виклав дані статистичних досліджень щодо рівня злочинності у світовому кіберпросторі. Серед «позитивних» лідерів були названі Швеція, Фінляндія та Норвегія, як країни, що мають найнижчий процент кібератак на бази даних як корпорацій та банків, так і приватних осіб. Також журнал Форбс назвав трійку «негативних» лідерів – Китай, Тайвань та Туреччина. Згідно цих же статистичних даних, у 2013 році більше, ніж половина (54%) випадків кібершпіонажу були здійснені у Сполучених Штатах [9]. Тож, все більша кількість осіб у різних країнах світу стають жертвами атак кіберзлочинців.

Аналізуючи цю проблему, слід зауважити, що необхідність захисту прав людини на приватність була визначена у 80-х роках XX століття. Так, у 1981 році держави – члени Ради Європи ухвалили Конвенцію про захист осіб у зв'язку з автоматизованою обробкою персональних даних (ратифікована Україною у 2010 році). У преамбулі цього міжнародного договору йдеться про усвідомлення необхідності поширення гарантії прав й основоположних свобод кожної людини, зокрема права на повагу до недоторканості приватного життя, з огляду на зростання транскордонного потоку персональних даних, які піддаються автоматизованій обробці [4].

Пізніше, у 2001 році Радою Європи було складено та ухвалено ще один міжнародний договір – Конвенцію про кіберзлочинність (ратифікована Україною у 2005 році). Її прийняття свідчить про те, що питання у даній галузі у світі не лише не вирішені, а й набувають ескалації. Як ми зазначали раніше, це пов'язано із значним та бурхливим розвитком високих технологій, розширенням сфер їх використання та появою осіб, основним професійним завданням яких є отримання інформації, яка міститься в електронних ресурсах, злочинним шляхом (хакерів). Так виникла потреба у визначенні спільної кримінальної політики, спрямованої на захист суспільства від кіберзлочинності, між іншим, шляхом створення відповідного законодавства і налагодження міжнародного співробітництва [5].

Право на приватне життя та його захист визнано та закріплено у 1950 році в одному із основних міжнародних документів з прав людини – Конвенції ООН про захист прав людини і основоположних свобод у статті 8 «Право на повагу до приватного і сімейного життя» [6]. Там, зокрема, визнається право кожної особи на повагу до свого приватного життя. На наш погляд, з огляду на сучасність та на певні зміни, які відбулися у світі протягом останніх 50-60 років, поняття приватності невід’ємно пов'язано і зі зберіганням особою приватної інформації. Ми маємо на увазі як інформацію, яка міститься у банківських базах даних, так і інформацію, яка зберігається в інтернет-ресурсах та у приватних пристроях.

Не викладає сумніву та теза, що для ефективної боротьби зі злочинами, пов'язаними з порушенням права на приватність та права на інформацію, необхідна консолідація зусиль багатьох держав, взаємодія та взаємодопомога як при вжитті превентивних заходів, так і при розслідуванні скоєних злочинів, бо такі злочини часто мають транснаціональний характер. Дії, які мають вживати держави – учасниці даного міжнародного договору, як справедливо зазначено у документі, мають бути спрямовані на зупинення дій, спрямованих проти конфіденційності, цілісності і доступності комп'ютерних систем, мереж і комп'ютерних даних, а також зловживання такими системами, мережами і даними.

Аналізуючи стан державних правових гарантій забезпечення захищеності приватної інформації в Україні, можна зазначити, що Конституція України дає гарантії таємниці листування, телефонних розмов, телеграфної та іншої кореспонденції. Не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди [7]. Законом України «Про основні засади забезпечення кібербезпеки в Україні» від 05.10.2017 у ст. 1 визначено низку понять (кібератака, кіберпростір, кібербезпекиа, кіберзахист тощо), об'єкти кібербезпеки та кіберзахисту, основним з яких є конституційні права і свободи людини і громадянина (ст. 4) [8].

Крім того, Указом Президента України від 15 березня 2016 року № 96/2016 затверджено «Стратегію кібербезпеки України», метою якої є створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави [9]. У цьому документі акцентовано увагу на тому, що кіберпростір поступово перетворюється на окрему, поряд із традиційними «Земля», «Повітря», «Море» та «Космос», сферу ведення бойових дій, у якій все більш активно діють відповідні підрозділи збройних сил провідних держав світу (розділ 2 «Загрози кібербезпеці»). Але слід зазначити, що у даному акті відсутні дані щодо вжиття заходів, спрямованих на захист права людини, громадянина на приватність.

Кримінальне законодавство має низку норм, які передбачають відповідальність за злочини у сфері кібербезпеки. Зокрема, ст. 190 «Шахрайство» передбачає покарання за вчинення незаконних операцій з використанням електронно-обчислювальної техніки; ст. 361-2 «Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації» розділу XVI «Використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» Кримінального кодексу України – покарання за несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або

на носіях такої інформації, створеної та захищеної відповідно до чинного законодавства [10].

Таким чином, на загальнодержавному рівні створено засади національної системи кібербезпеки як сукупності політичних, соціальних, економічних та інформаційних відносин разом із організаційно-адміністративними, технічними заходами державного і приватного секторів та громадянського суспільства. Визначено, хоч і дещо недосконало, кримінальне покарання за дії, які посягають на суспільні відносини в інформаційній сфері. Тому, на наш погляд, було б доцільно вивчити та, можливо, запозичити позитивний досвід деяких країн, які мають позитивні результати як превентивної діяльності, так і заходів по боротьбі з порушеннями прав людини на приватність та інформацію у кіберпросторі.

Список бібліографічних посилань

1. Скулиш Є. Д. Посилення відповідальності в контексті підвищення ефективності боротьби із кіберзлочинністю. *Правова інформатика*. 2013. № 4 (40). С. 90-97.

2. Селико Ю., Прохоров А.. Internet – отмычка для комп'ютера. *Компьютер-пресс*. 2002. № 3. С. 40-43.

3. Kevin Murnane. Cyber Security: The World's best and worst presented with a well-designed infographic // Forbs, May 4, 2017. **URL:** https://www.forbes.com/sites/kevinmurnane/2017/05/04/cyber-security-the-worlds-best-and-worst-presented-with-a-well-designed-infographic/#376154dd4416 (дата звернення: 07.06.2017).

4. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних 1981 року // БД «Законодавство України» / ВР України. URL: http://zakon.rada.gov.ua/laws/show/994_326 (дата звернення: 07.10.2018).

5. Конвенція про кіберзлочинність від 23.11.2001 // БД «Законодавство України» / ВР України. URL: http://zakon.rada.gov.ua/laws/show/994_575 (дата звернення: 17.09.2018).

6. Конвенція ООН про захист прав людини і основоположних свобод 1950 року // БД «Законодавство України» / ВР України. URL: http://zakon.rada.gov.ua/laws/show/995_004 (дата звернення: 19.09.2018).

7. Конституція України : закон України від 28.06.1996 № 254к/96-ВР // БД «Законодавство України» / ВР України. URL: http://zakon.rada.gov.ua/laws/show/254к/96-вр (дата звернення: 10.10.2018).

8. Про основні засади забезпечення кібербезпеки України : закон України від 05.11.2017 № 2163-VIII // БД «Законодавство України» / ВР України. URL: http://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 17.09.2018).

9. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» : указ Президента України // БД «Законодавство України» / ВР України. **URL:** http://zakon.rada.gov.ua/laws/show/96/2016 (дата звернення: 17.09.2018).

10. Кримінальний кодекс України від 01 вересня 2001 року // БД «Законодавство України» / ВР України. URL: http://zakon.rada.gov.ua/laws/show/2341-14 (дата звернення: 17.09.2018).

Одержано 26.10.2018