УДК 342.7+004.7
Вадим Сергійович СЕЛЮКОВ
кандидат юридичних наук, доцент кафедри адміністративної діяльності поліції факультету № 3 Харківського національного університету внутрішніх справ
ORCID: https://orcid.org/0000-0002-6690-6484
Вікторія Сергіївна МАКАРЕНКО
кандидат юридичних наук, доцент кафедри адміністративної діяльності поліції факультету № 3 Харківського національного університету внутрішніх справ
ORCID: https://orcid.org/0000-0003-3310-0684

ПРОБЛЕМНІ АСПЕКТИ, ЩО ЗАЧІПАЮТЬ ПРАВА ТА ІНТЕРЕСИ ЛЮДИНИ В МЕРЕЖІ ІНТЕРНЕТ

Мережа Інтернет є однією з головних складових частин кіберпростору в цілому. Поширення та стрімке удосконалення технологій, що надають можливість спілкуватися з усім світом є важливим досягненням сучасного суспільства.

Але поряд із позитивними аспектами поширення способів комунікації та розповсюдження інформації виникають і негативні явища, які в свою чергу створюють загрозу не лише для власників інформації, а і дня усього суспільства.

В рамках даного дослідження хочеться звернути увагу лишена деякі негативні явища, що виникають і проявляються за допомогою Інтернет ресурсів. По-перше, питання інформаційної та кібербезпеки є досить актуальним у світлі дотримання прав і свобод людей. По-друге, кіберпростір є значим «полем» для здійснення злочинної діяльності, а також протиправних та нігілістичних проявів. По-третє, безконтрольність розповсюдження інформації не тільки підриває авторитет держави або її окремих органів, а й призводить до нехтування правами і свободами людей. По-четверте, оцифрування великої кількості інформації, що захищається Законом України «Про захист персональних даних».

У своєму дослідженні І.О. Громико та Т.І. Сахарчук визначають інформаційну безпеку України як захищеність державних інтересів, за якої забезпечується запобігання, виявлення і нейтралізація внутрішніх та зовнішніх інформаційних загроз, збереження інформаційного суверенітету держави і безпечний розвиток міжнародного інформаційного співробітництва.[1] Лілія Олексюк визначає інформаційну безпеку як збереження конфіденційності, цілісності та доступності інформації.[2] Враховуючи два наведені визначення варто підкреслити, що іноді автори досить по-різному трактують поняття інформаційної безпеки, але сутність її має дуалістичний характер, тобто інформаційну безпеку варто розглядати у двох цих напрямах: як стан захищеності інформації та захист інтересів особи та держави, інформація про яких міститься в мережі.

Стосовно визначення змісту поняття кібербезпеки, то досі не існує нормативного визначення даного терміну хоча у нормативних документах повсякчас воно використовується. Кібербезпека зазвичай стосується заходів і дій, спрямованих на захист кіберпростору в цивільній і військовій сферах від загроз, які можуть завдати шкоди взаємозалежним мережам та інформаційній інфраструктурі або є пов'язаними з ними. Кібербезпека спрямована на збереження доступності та цілісності мереж та інфраструктури, а також конфіденційності інформації, яка міститься в них.[3] ISACA дає таке визначення кібербезпеки: «Захист інформаційних активів шляхом боротьби із загрозами безпеці інформації, яка обробляється, зберігається та передається за допомогою інформаційних систем, що взаємодіють за допомогою мереж.»[4]

Отож, враховуючи зміст визначених вище понять, доцільно зазначити, що існування проблемних питань у стані безпеки в цілому, та безпеки у кіберпросторі та мережі Інтернет зокрема, є досить актуальною проблемою сьогодення. Крім того, простота та чисельність фактів порушення прав людини у кіберпросторі останнім часом стрімко зростає, що є наслідком неспроможності суб’єктів, що покликані забезпечувати інформаційну та кібербезпеку в Україні, організувати відповідну захищеність, а також неосвіченість населення стосовно девіантних вчинків та дій в мережі Інтернет. Систематичне порушення прав людини на конфіденційність листування, на свободу слова, на приватність, на честь та гідність, на захист від шахрайських та інших дій, що стають можливими в умовах розвитку інформаційних технологій є нагальною проблемою в сучасному українському суспільстві.

Збільшення числа злочинів, що вчиняється з використанням мережі Інтернет пов’язане з можливістю вчиняти такі діє суб’єктом не особливо переймаючись про те, що його можуть швидко встановити та затримати. Сучасні технологічні можливості дають змогу правопорушнику маскувати

свою діяльність або шифрувати її без особливих труднощів. Використання VPN сервісів, електронних гаманців та інших технічних засобів дало поштовх для росту злочинності, яка вчиняється саме цим способом. З точки зору адміністративної діяльності та можливості захисту прав і свобод людей варто казати, що нормативно врегулювати даний аспект проблем неможливо, окрім як визначити суб'єктів, що мають здійснювати діяльність по боротьбі зі злочинністю у кіберпросторі. Але, нажаль, можливості держави нині не дозволяють користуватися такими технологіями, що б забезпечили дієвий захист прав і законних інтересів суспільства та держави від протиправних посягань у цьому напряму.

Також варто відзначити, що права людини обмежуються там де починаються права іншої людини. Так, право на свободу слова має досить спірний аспект. Поширення інформації, що принижує гідність особи або наклеп чи інші способи висловлювання є досить розповсюдженими в мережі. Але нині жодного факту притягнення до відповідальності за такі дії немає. Крім того, в контексті забезпечення правовиховної функцій держави, відсутній контроль за змістом інформації, що поширюється. На сьогодні досить активно збільшується кількість Інтернет-блогерів, які отримують популярність шляхом розповсюдження контенту, зміст якого впливає на формування негативного ставлення до правоохоронних органів та до системи права України в цілому. До того ж, набуло широкомасштабних розмірів правове безкультур'я: від сфери повсякденних відносин між людьми до діяльності вищих законодавчих органів держави, від центрального управлінського апарату до його низових ланок. Це небезпечне соціальне явище може стати серйозною перешкодою на шляху соціально-економічних і державно-правових реформ.[5, с. 26] На теренах Інтернету є статті, які описують способи ухилення від сплати податків [6], способи обману алкотестера[7], прийоми зменшення облікованої електроенергії[8]. Таке «зловживання прогалинами» у законодавстві, в тому числі і поліцейськими, призводить до вироблення звички порушувати закон, зневажливо ставитися до права.

Мода на поширення інформації про діяльність органів влади у засобах масової інформації та, особливо, мережі Інтернет, є досить актуальною. Але інформацію щодо щоденної діяльності вказаних органів дивитися нецікава, а контент, де проводяться провокації або моральне знущання над працівниками органів влади та і взагалі населенням є досить затребуваним. Тому поширення такого контенту є доречним для блогерів, які не завжди коректно ведуть себе, наприклад, з працівниками поліції. Тут постає необхідність у впровадженні цензури щодо таких дій.

І останнє, але не менш важливий проблемний аспект це оперуваннями базами даних з інформацією, яка підпадає під визначення персональних даних. Візьмемо хоча бази даних з нормами авто, телефонами та ПІБ, якими оперують зловмисники та розповсюджують за допомогою меседжеру Telegram. Надання такої інформації без згоди особи, щодо якої надано цю інформацію є прямим порушенням Закону України «Про захист персональних даних».

Тому, як **висновок** хочеться підсумувати, що забезпечення належного рівня інформаційної та кібербезпеки на сучасному етапі в Україні можливе лише шляхом акцентованої підготовки фахівців у цій сфері та розвитку фінансування розвитку інформаційних технологій. Прийняття нормативно-правових актів у даній сфері хоча і є важливим шляхом подолання вказаних проблем, але без залучення відповідних спеціалістів та розробки відповідного технічного обладнання такі проблеми визначити неможливо.

Список бібліографічних посилань:

1. І.О. Громико та Т.І. Сахарчук Інформаційна безпека України. Тези доповідей 2-ї Міжнародної науково-практичної конференції "Безпека та захист інформації в інформаційних системах" (на базі Харківського національного економічного університету) 29-30 квітня 2009 року. [Електронний ресурс]: https://www.researchgate.net/publication/290447930_Informacijna_bezpeka_Ukraini_Tezi_dopovidej_2-i_Miznarodnoi_naukovo-prakticnoi_konferencii_Bezpeka_ta_zahist_informacii_v_informacijnih_sistemah_na_bazi_Harkivskogo_nacionalnogo_ekonomicnogo_universit [accessed Nov 13 2018].

2. Лілія Олексюк Кібербезпека та/або права людини [Електронний ресурс]: http://vaibit.org.ua/wp-content/uploads/2017/07/%D0%92%D0%90%D0%86%D0%91%D0%86%D0%A2.pdf

3. Європейська комісія, Спільне звернення до Європейського парламенту, Ради, Європейського соціально-економічного комітету та Комітету регіонів – Стратегія ЄС із кібербезпеки: відкритий, надійний і безпечний кіберпростір, Брюссель, 2 липня 2013 р., с. 3 [Електронний ресурс]: http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1667

4. ISACA, Глосарій з кібербезпеки, 2014 р. [Електронний ресурс]: http://www.isaca.org/KnowledgeCenter/Documents/Glossary/Cybersecurity_Fundamentals_glossary.pdf

5. Тополь Ю.О. Правовий нігілізм : стан, детермінанти та можливі шляхи подолання. Вісник Хмельницького інституту регіонального управління та права. 2004. № 4. С. 25–33.

6. Способы обхода налоговых выплат. URL: http://workion.ru/sposoby-obxoda-nalogovyx-vyplat.html

7. Как обмануть алкотестер? URL: https://proboknet.livejournal.com/552095.html

8. Остановка ЛЮБОГО счетчика. Хитрая проводка. Остановить счетчик без магнита. Бесплатное электричество. URL:https://www.youtube.com/watch?v=BjJPgrlJDv4

Одержано _____.2018