

Міністерство освіти і науки України
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Факультет соціології і права
Кафедра інформаційного права та права інтелектуальної власності
Науково-дослідний інститут інформатики і права
Національної академії правових наук України

ВПЛИВ ПАНДЕМІЇ КОРОНОВІРУСУ COVID-19 НА ПРАВА, СВОБОДИ І БЕЗПЕКУ ЛЮДИНИ В ІНФОРМАЦІЙНІЙ СФЕРІ

Матеріали науково-практичної студентської конференції

12 травня 2020 р.

Київ
КПІ ім. Ігоря Сікорського
2020

УДК 34:004]:616-036.21(06)
В80

Вплив пандемії коронавірусу COVID-19 на права, свободи і безпеку людини в інформаційній сфері: Матеріали науково-практичної студентської конференції / 12 травня 2020 р., м. Київ / Упоряд. : Фурашев В. М., Петраєв С. Ю.— Київ : Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського» Вид-во «Політехніка». 2020. — 196 с.

Матеріали конференції присвячені розгляду питань впливу пандемії коронавірусу COVID-19 на права, свободи і безпеку людини в інформаційній сфері.

Участь у конференції взяли виключно студенти, в основному Київського політехнічного інституту імені Ігоря Сікорського різних спеціальностей та спеціалізацій.

Доповіді учасників конференції можуть бути корисними для організаторів навчальних процесів та здобувачів вищої освіти, а також спеціалістів у сферах правотворення, правозастосування, правоохоронної діяльності.

Матеріали подано у авторській редакції.
Упорядники: Фурашев В. М., Петраєв С.Ю.

Оформлення обкладинки:
Лабораторія технічної естетики та дизайну ФСП КПІ ім. Ігоря Сікорського
designlab.kpi.ua@gmail.com
Балашов Д. В. (balashov.dim@gmail.com)

Рекомендовано до друку:

Вченою радою факультету соціології і права

Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського». Протокол № 10 від 23.06.2020.

Вченою радою Науково-дослідного інституту інформатики і права

Національної академії правових наук України.

Протокол від № 5 від 21.05.2020.

ISBN 978-966-990-002-9

© Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», 2020
© Науково-дослідний інститут інформатики і права НАПрІ України, 2020
© Колектив авторів

ЗМІСТ

Горошко О. А., Гарантії прав і свобод людини в сфері інформації.....	6
Семененко М., Адаптація законодавства України з питань захисту прав і безпеки людини в інформаційній сфері до законодавства Європейського Союзу.....	10
Правосуд Р. О., Деякі аспекти адаптації законодавства України з питань захисту прав і безпеки людини в інформаційній сфері до законодавства ЄС.....	15
Звичайна А. О., Право на інформацію в умовах карантину.....	18
Балінська В. О., Ярош І. С., Неприпустимість порушення принципів інформаційних відносин під час карантину у діяльності ЗМІ	23
Мухамедзянов А. І., Вплив пандемії коронавірусу COVID-19 на права, свободи і безпеку людини в інформаційній сфері.....	27
Білоконь Б. С., Вплив пандемії коронавірусу COVID-19 на права, свободи і безпеку людини в інформаційній сфері.....	29
Вареня М., Актуальні питання захисту прав і безпеки людини в інформаційній сфері в умовах карантинно-обмежувальних та інших режимних заходів.....	34
Марцинюк В., Вплив карантинного та пост карантинного періодів на роль та місце інформаційної безпеки в системі забезпечення конституційних прав і свободи людини в інформаційній сфері.....	37
Мазуренко П. В., Забезпечення інформаційної безпеки особи та безпечного доступу до інформації в умовах карантину.....	40
Крицун Т. Р., Апробація змін в інформаційній культурі ЗМІ спричинені пандемією коронавірусу COVID-19.....	44
Лобода Р. І., Вплив карантинного та пост карантинного періодів на додержання інформаційної культури і морально-етичних норм в соціальних мережах та ЗМІ.....	48
Коваль С. Д., Дослідження рівня інформаційної культури та інформаційної етичності студентів та аспірантів фізико-математичних та фізико-	

технічних спеціальностей в умовах пандемії COVID-19.....	52
Головатюк О. А.,	
Вплив карантинного періоду на соціальні мережі та ЗМІ.....	58
Мазур Є.,	
Фейкові новин стосовно COVID-19 в інформаційному просторі та їх вплив на населення.....	62
Румянцева К.,	
Проблема фальсифікації даних під час пандемії.....	65
Коваленко В. В.,	
Протидія фейкам про COVID-19 як складова інформаційної безпеки держави.....	67
Кучеренко В. С.,	
Дослідження впливу пандемії COVID-19 на дистанційне навчання студентів і аспірантів фізико-технічних спеціальностей та роль інформаційної безпеки.....	71
Завальнюк Ю. Ю.,	
Правове регулювання відносин у мережі Інтернет в Україні.....	77
Герега Б. Д.,	
Права і безпека дитини в кіберпросторі.....	80
Челепіс А.,	
Кібербезпека та COVID-19.....	83
Зозуля В. О.,	
Кібербезпека в умовах пандемії коронавірусу COVID-19.....	86
Собко І.О., Морква С.О.,	
Проблеми та перспективи розвитку кібербезпеки України в умовах карантинного та посткарантинного періоду.....	88
Хиленко В. В.,	
Інтернет-шахрайство та його види.....	93
Пивовар П. Є.,	
Е-резидент: досвід Естонії та перспективи запровадження в Україні...	96
Пономарьов К. С.,	
Практичні ризики при реформуванні національних органів контролю захисту персональних даних відповідно до положень загального регламенту захисту персональних даних європейського союзу (gdpr).	100
Александрова А.,	
Проблеми захисту інформаційної приватності та персональних даних	112
Жакулін Н. В.,	
Правове регулювання захисту персональних даних за законодавством України, ЄС та США: порівняльний аналіз.....	115
Завальнюк Ю. Ю.,	
Проблема збирання та обробки персональних даних у мережі Інтернет.....	120

Правосуд Р. О.,	
Вплив карантинного та посткарантинного періодів на захист персональних даних фізичних осіб в Україні.....	125
Зух Ю. О.,	
Вплив заходів в ІТ-сфері, спрямованих на боротьбу з пандемією COVID-19, на захист персональних даних.....	128
Пивовар П. Є., Пашнієва О. М.,	
Правові аспекти захисту персональних даних від кібератак.....	134
Купрієнко С. П.,	
Проблеми охорони та захисту авторських прав в мережі Інтернет.....	140
Чумакова А. В.,	
Сучасні електронні інформаційні системи як привід до вчинення кіберзлочинів.....	146
Коваленко М. Д.,	
Проблемні питання правового регулювання ІТ-підприємництва в Україні.....	151
Пастушок О. О.,	
Оподаткування послуг в ІТ-сфері в Україні: проблеми та перспективи розвитку.....	156
Філіпов М. В.,	
Правовий статус хмарних сервісів та проблеми їх використання.....	160
Кустарёва Е. М.,	
Существенный рост актуальности ИТ профессии в связи с изменением социальных взаимоотношений.....	167
Жук В. А.,	
Кібербезпека та захист персональних даних в Україні в умовах пандемії COVID-19	171
Зарічний Я. С.,	
Правове регулювання організації коворкінгу в ІТ-сфері в Україні	176
Купрієнко С. П.,	
Соціальні мережі як об'єкт правового регулювання	182
Чинник П. А.,	
Правове регулювання інформаційної приватності	186
Морозов Р. Д.,	
Концептуальні напрямки правового регулювання криптовалют в Україні	190

Горошко О. А.,

студентка факультету соціології і права
КПІ ім. Ігоря Сікорського

Науковий керівник: Солончук І. В.,

ст. викладач кафедри інформаційного права та
права інтелектуальної власності КПІ ім. Ігоря
Сікорського

ГАРАНТІЇ ПРАВ І СВОБОД ЛЮДИНИ В СФЕРІ ІНФОРМАЦІЇ

Гарантії прав і свобод людини в інформаційній сфері є найголовнішою засадою формування правової держави та демократичного суспільства. Забезпечення захисту прав і свобод людини в інформаційній сфері можна вважати найважливішою метою інформаційної безпеки. У той час людина - найголовніший об'єкт даної сфери.

У наш час набули великого розвитку технології у сфері інформації та комунікації. Водночас, загострюється проблема інформаційної безпеки громадян. При цьому, у державі зростає роль техніко-юридичних гарантій прав людини. Забезпечення прав людини у даній сфері є необхідною складовою забезпечення інформаційної безпеки. Тому, ефективність застосування даного права забезпечується у тандемі з правовими гарантіями прав людини. Це вказує на те, що принцип недоторканості приватного життя у праві Європейського Союзу відображається в правових актах. Захист прав – це використання передбачених законом можливостей для поновлення свого порушеного, визнання невизнаного чи присудження оспорюваного права. Загалом, правовий захист інформаційних прав громадян в Україні регулюють такі нормативно правові акти, як Закон України "Про інформацію" , а також Цивільний кодекс України.

Гарантії прав і свобод людини у інформаційній сфері є найголовнішим пунктом у формуванні громадського суспільства та держави. Саме такі права характеризують демократичне суспільство та є дієвим механізмом державного

управління. Вищезазначені ствердження вказують на те, що однією з найважливіших цілей інформаційної безпеки є забезпечення захисту прав і свобод людини безпосередньо в інформаційній сфері.

У сучасному світі важливу роль у житті людини грає саме інформаційна безпека. Також, необхідно зазначити, що право на свободу інформації, думки та слова є одними із головних громадянських та політичних прав особи. Саме ці права є невід'ємною частиною людської особистості. Права і свободи громадянина у сфері інформації – це важливий елемент для існування людини та визначає політичний устрій будь-якої держави. Даний інститут є основним для вільного суспільства, а також для демократичної держави. Деякі дослідники, у тому числі і Д. Р. Дуцик, у свої працях прирівнюють право на інформацію до свобод масової інформації [2]. Тобто, дане твердження можна пояснити тим, що інформаційне право, перш за все, реалізовує певну інформаційну свободу, яка, у свою чергу, поширюється за допомогою засобів масової інформації. Глобальний виклад та підтвердження всього зазначеного вище, можна знайти у Конвенції про захист прав та основоположних свобод людини 1950 р., а саме у статті 10, яка вказує на свободу вираження поглядів: "Кожен має право на свободу вираження поглядів. Це право включає свободу дотримуватися своїх поглядів, одержувати і передавати інформацію та ідеї без втручання органів державної влади і незалежно від кордонів" [5].

Але не тільки міжнародні акти, проголошують дане право як одне з невід'ємних для людини та громадянина. На загальнодержавному рівні його закріплює Конституція України. Конституційні засади прав і свобод людини закріплюють, що життя, здоров'я, честь та гідність, недоторканість та безпека визнаються в Україні найвищою соціальною цінністю [1]. Щодо прав і свобод людини у сфері інформації, то дане визначення викладено у нормах статей 34 і 32 Конституції України. Розглядаючи вказані норми, а саме у статті 34, яка визначає право на свободу слова та право на інформацію, закріплено: "кожному

гарантується право на свободу думки і слова, на вільне вираження своїх поглядів і переконань" [1]. Також, згідно з положеннями цієї статті, кожен має право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб - на свій вибір [1]. Отже, аналізуючи все, що було викладено вище, та звертаючись до наукових робіт, можемо дійти висновку, що інформаційна свобода є сукупністю певних можливостей інформаційних прав, а сама інформаційна свобода - це основне питання у сучасному світі [8].

Однак, у кожному правилі є свої виключення. Тому існують підстави та випадки, коли обмеження прав людини у сфері інформації все ж таки можливе. Дана інформація міститься у такому нормативно-правовому акті, як Загальна декларація прав людини. Але вона не містить повного викладу обмежень використання та реалізації людиною свого права на інформацію. Саме стаття 29 Декларації є загальною нормою, яка вказує на те, що при здійсненні своїх прав і свобод кожна людина може зазнавати тільки обмежень, установлених законом виключно з метою забезпечення належного визнання і поваги прав і свобод інших та забезпечення справедливих вимог моралі, громадського порядку і загального добробуту в демократичному суспільстві, а також зазначено, що здійснення відповідних прав і свобод в жодному разі не повинне суперечити цілям і принципам Організації Об'єднаних Націй [4]. Виходячи із даних фактів, визначено три основні риси, які, у сукупності, можуть стати підставами для обмеження прав і свобод людини:

- забезпечення прав і свобод третіх осіб або моралі, громадського порядку і загального добробуту, причому, що важливо, лише в тому розумінні, яке існує в рамках демократичного суспільства;
- забезпечення дотримання цілей і принципів ООН та наявність прямих правових приписів, що регламентують застосування подібних обмежень.

Також, згідно з Конвенцією про захист прав і основоположних свобод людини, у статті 8 вказується на те, що органи державної влади не можуть втручатися у здійснення права на повагу до приватного і сімейного життя "інакше ніж згідно із законом і коли це необхідно в демократичному суспільстві в інтересах національної і громадської безпеки або економічного добробуту країни, з метою запобігання заворушенням чи злочинам, для захисту здоров'я чи моралі або з метою захисту прав і свобод інших осіб" [5]. Саме цією Конвенцією визначено певні випадки та ряд причин, коли обмеження інформаційних прав людини ділиться на кілька груп. До першої групи, умовно, відносяться дії, які необхідні для захисту безпеки держави, а саме охорона і захист: громадського порядку; громадської безпеки; національної безпеки; територіальної цілісності.

До другої групи підпадають такі завдання, що потребують вирішення загальносуспільних питань: здоров'я; моральних засад.

Третя група включає певні заходи захисту прав та інтересів третіх осіб: прав і свобод інших людей; конфіденційності особистого життя: репутації інших людей; інтересів малолітніх осіб.

Четверта група поєднує завдання, які вирішуються за допомогою правоохоронної діяльності: запобігання заворушенням або злочинам; забезпечення інтересів правосуддя; підтримання авторитету і неупередженості правосуддя; запобігання розголошенню інформації, одержаної конфіденційно [5].

Проаналізувавши дану тему, розділяючи її на ряд підпунктів, можемо зробити висновок, що у світі новітніх технологій та інформаційних наук у суспільстві аналізується інформаційні права і свободи людини. Також, хочеться зазначити про співвідношення інформаційних прав та інформаційної свободи людини, адже це є головним правом у сучасному світі. Також інформаційна свобода та інформаційне право мають бути захищені державою належним

чином, а досліджені питання мають вивчатися і далі науковцями та правознавцями.

Список використаної літератури:

1. Конституція України: Закон України від 28 червня 1996 р. № 254к/96-ВР. *Відомості Верховної Ради України*. 1996. № 30. Ст. 141.
2. Дуцик Д. Р. Роль засобів масової інформації у забезпеченні політичних прав та свобод громадян у демократичному суспільстві : автореф. Київ: КНУ , 2004. С. 19.
3. Свобода інформації в Україні та світі. теорія та практика: посібник / упоряд. О. М. Павліченко, Р. І. Стадник. Харків: Права людини, 2015. 215 с.
4. Загальна декларація прав людини від 10 грудня 1948 року. URL: https://zakon.rada.gov.ua/laws/show/995_015 (дата звернення 20.05.2020).
5. Європейська конвенція про захист прав людини та основоположних свобод від 3 вересня 1953 року. URL: https://www.echr.coe.int/Documents/Convention_UKR.pdf (дата звернення 20.05.2020).

Семененко М.,

студент факультету соціології і права
КПІ ім. Ігоря Сікорського

Науковий керівник: Солончук І. В.,

ст. викладач кафедри інформаційного
права та права інтелектуальної власності
КПІ імені Ігоря Сікорського

АДАПТАЦІЯ ЗАКОНОДАВСТВА УКРАЇНИ З ПИТАНЬ ЗАХИСТУ ПРАВ І БЕЗПЕКИ ЛЮДИНИ В ІНФОРМАЦІЙНІЙ СФЕРІ ДО ЗАКОНОДАВСТВА ЄВРОПЕЙСЬКОГО СОЮЗУ

Сучасне інформаційне законодавство України майже відповідає європейським та світовим стандартам. Стаття 10 Конвенції про захист прав та основних свобод людини проголошує, що кожна людина має право на свободу виявлення поглядів. Це право включає свободу дотримуватися поглядів, одержувати і поширювати інформацію та ідеї без втручання з боку державних установ та незалежно від кордонів. Однак, наше законодавство не є ідеальним, а тому потребує деяких уточнень та доопрацювань. Так сам термін "інформація"

у наш час є недостатньо чітким і потребує суттєвих уточнень. Крім того, потребує значного скорочення термін розгляду запитів на інформацію. Також доцільно встановити ефективний механізм реалізації права на доступ до інформації, зокрема, офіційної.

Саме тому, хоч і можемо сказати, що наше законодавство знаходиться на значному рівні, проте, все одно "не дотягує" до європейських стандартів і потребує як не значних, так і, в деяких випадках, значних змін і доопрацювань.

На нашу думку, недосконалість українського законодавства в інформаційній сфері порівняно із законодавством ЄС є проблемою наукового обговорення з метою розроблення шляхів вирішення для покращення вітчизняного законодавства.

На даний час законодавство України у сфері інформації знаходиться на достатньому рівні, проте потребує постійного вдосконалення. У ратифікованій Україною Конвенції про захист прав і свобод людини було встановлено, що кожна людина має свободу поглядів та вільне вираження своїх думок. Крім того, вільне розповсюдження інформації гарантується Конституцією України, Законом України "Про інформацію", "Про друковані засоби масової інформації (пресу) в Україні", "Про телебачення і радіомовлення" та багато інших, що дозволяє вільно збирати, використовувати та розповсюджувати інформацію, крім випадків передбачених законом, наприклад державна таємниця, збирання та розповсюдження м якої заборонено на законодавчому рівні. Проте, більшість цих законів не завжди можуть адекватно та справедливо вирішити інформаційні проблеми сьогодення, оскільки більшість із них є старими і не відповідають достатньому рівню розвитку в інформаційній сфері. Навіть розглянувши саме поняття "інформація", що визначене у законі, можемо зробити висновок про недосконалість законодавства, адже дане визначення не є настільки широким як повинно бути у наш час.

Частиною інформації володіють державні органи, що у певних випадках ускладнює отримання інформації. У деяких випадках саме державні органи відмовляють у доступі до інформації, що є порушенням закону і про що свідчать скарги громадян. Саме тому потрібно створити механізм, який буде відповідати за реалізацію права на вільний доступ до інформації. Є потреба створити спеціальну інстанцію, яка буде контролювати надання інформації громадянам та законність усіх цих дій. Адже у багатьох випадках недоступність інформації громадянам відбувається не через випадкову помилку державних діячів, а через халатність або перевищення своїх повноважень. Саме такі дії і порушують права і свободи громадян у доступі до публічної інформації.

Український курс до ЄС має на меті не просто привести своє законодавство до рівня законодавства країн Європейського Союзу, а покращити свої нормативні положення для полегшення процедури діяльності з інформацією та дотриманням законності у даній сфері.

Рекомендація Ради Європи "Про право доступу до інформації, яка перебуває в розпорядженні органів державної влади" охоплює низку принципів, які мають бути реалізовані при удосконаленні інформаційного законодавства в частині доступу до інформації, якою володіють органи державної влади та органи місцевого самоврядування, а саме:

- необов'язковість вказування причини запиту;
- формальність вимог повинна бути мінімальною ;
- запити повинні розглядатись тими органами до чиєї юрисдикції входять ці документи;
- кожен запит повинен розглядатися однаково незалежно від соціального рівня особи;
- запити повинні розглядатись швидко;

- доступ має надаватись шляхом надання змоги переглянути оригінали документів або копії, беручи, в розумних межах, огляд на побажання запитувача;

- якщо лише частина документа є конфіденційною, до нього має бути наданий частковий доступ;

- доступ до оригіналів документів в стінах органів влади повинен бути безкоштовним, при цьому за виготовлення копій може братись плата, виходячи з собівартості;

- у разі відмови повинна надаватись можливість подати заяву до суду або іншого незалежного і безпосереднього органу влади, встановленого законом [1].

Серед пріоритетних напрямків в інформаційній сфері цим Планом заходів передбачено забезпечення необхідних юридичних умов для реалізації права на свободу вираження поглядів та доступ до інформації, для чого Кабінетом Міністрів України має бути підготовлений відповідно до стандартів Ради Європи та поданий в установленому порядку законопроект про нову редакцію Закону України "Про інформацію". З метою покращення даного закону застосовують і пропозиції звичайних громадян, адже на офіційному сайті Міністерства юстиції кожен може залишити свою пропозиції для покращення даного закону.

Отже, незважаючи на те, що наше законодавство знаходиться не на останньому місці у світовому рейтингу, воно є не досконалим і потребує значних змін. З метою покращення його потрібно оновити, тобто: вдосконалити саме поняття "інформація", змінити структуру доступу до інформації, запровадити контроль за цим доступом для законності та дотримання прав і свобод громадян України та інших осіб, що знаходяться на території нашої держави. Саму тому потрібно брати курс на країни ЄС та запозичити у них практику вирішення таких проблем, або, хоча б, взяти до уваги їх законодавство. Все це потрібно для правильної та швидкої адаптації

вітчизняного законодавства до законодавства країн Європейського союзу. Рухаючись таким курсом, ми зможемо не тільки бути на рівні з іншими розвинутими країнами, а й "обігнати" їх у розвитку законодавства та регулюванні даних важливих питань.

Список використаної літератури:

1. Про право доступу до інформації, яка перебуває в розпорядженні органів державної влади: Рекомендація Ради Європи № К (81) 19 1981 р. URL: <https://cedem.org.ua/library/rekomendatsiya-r-81-19-pro-dostup-do-informat-siyi-shho-znahodytsya-u-rozporyadzhenni-derzhavnyh-organiv/> (дата звернення: 20.05.2020).

2. Конституція України: Закон України від 28 червня 1996 р. №254к/96-ВР. *Відомості Верховної Ради України*. 1996. № 30. Ст. 141.

3. Про інформацію: Закон України від 2 жовтня 1992 р. № 2657-XII. *Відомості Верховної Ради України*. 1992. № 48. Ст.650.

4. Рудой К. М. Адаптація адміністративного законодавства України у сфері охорони особистих прав громадян до норм Європейського Союзу : автореф. дис... на здобуття наук. ступеня канд. юрид. наук: 12.00.07 "Теорія управління; адміністративне право і процес; фінансове право; інформаційне право". Нац. Університет внутрішніх справ. Харків, 2004. 20 с.

5. Про Концепцію Загальнодержавної програми адаптації законодавства України до законодавства Європейського Союзу : Закон України від 21 листопада 2002 р. URL: http://search.ligazakon.ua/l_doc2.nsf/link1/T020228.html (дата звернення: 20.05.2020).

6. Калюжний Р. Питання концепції реформування інформаційного законодавства України. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*: науково-технічний збірник. 2000. № 1. С. 17-21.

Правосуд Р. О.,

Студент 3-го курсу ІПСА КПІ ім. Ігоря
Сікорського

Науковий керівник: Іщенко В.В., викладач
кафедри публічного права КПІ ім. Ігоря
Сікорського

ВПЛИВ КАРАНТИННОГО ТА ПОСТКАРАНТИННОГО ПЕРІОДІВ НА ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ ФІЗИЧНИХ ОСІБ В УКРАЇНІ

В умовах всесвітньої пандемії коронавірусної хвороби (COVID-19) відповідно до постанови Кабінету Міністрів України від 11 березня 2020 р. № 211 з 12 березня 2020 р. на території України було запроваджено карантин [1]. В цей період набуло важливого значення питання захисту та використання персональних даних фізичних осіб, які можуть бути задіяні з метою протистояння розповсюдженню хвороби.

Інформаційне законодавство України регулює права громадян на збирання, одержання, використання та поширення інформації. Крім того, інформаційне законодавство, встановлює вимоги до обробки персональних даних. Згідно ст. 7 Закону України «Про захист персональних даних» забороняється обробка персональних даних про стан здоров'я особи без її на те згоди [2]. Проте, у разі надзвичайних ситуацій, зокрема, при пандемії COVID-19, уряд може ухвалити рішення, щодо змін у законодавстві, як це і сталося під час карантинного періоду.

13 квітня 2020 р. було прийнято Закон України «Про внесення змін до Закону України «Про захист населення від інфекційних хвороб» щодо запобігання поширенню коронавірусної хвороби (COVID-19)» № 555-IX [3], яким було, зокрема, дозволено обробку персональних даних без згоди особи. Дії влади було спрямовано на отримання щонайбільшої кількості даних про хворих на COVID-19, аби, маючи цю інформацію, якомога найефективніше впроваджувати заходи, що стримають розповсюдження цієї хвороби. Зокрема,

це стосувалося даних про стан здоров'я, місце госпіталізації, місце проживання та роботи особи – даних про місця, в яких хворий проводив багато часу до госпіталізації. Таким чином, можна ефективно вживати профілактичні заходи, наприклад, проводячи тестування на COVID-19 серед відвідувачів місць частого перебування хворого до госпіталізації. Найчастіше це співмешканці, сусіди та колеги, але іноді і люди, з якими хворий пов'язаний не так явно, наприклад клієнти фірми або співробітники охорони та обслуговування житлових будинків, які більш зв'язані з хворим географічними місцями перебування, ніж прямим знайомством і можуть бути заражені через посередників між ними. Таким чином, можна виявити більшу кількість заражених, ізолювати їх і стримати розповсюдження хвороби. В такому разі, введення нового закону, який, з одного боку, дещо порушує права громадян на конфіденційність персональних даних, з іншого є досить виправданим під час карантинного періоду.

У той же час, можна піти далі і зобов'язати юридичних осіб надавати персональні дані працівників у межах потреби боротьби з епідемією. Крім того, корисними можуть виявитися не лише персональні дані працівників, але і дані про закупівлі чи переміщення певних товарів, які, не так явно як персональні дані про кожну особу, показуються зв'язок між певними географічними місцями. Наприклад, коли мова йде про переміщення товарів між містами. Звісно, все це має бути дозволеним лише під час надзвичайних ситуацій для запобігання зловживання персональною інформацією громадян [4].

Держава має гарантувати, що отримані нею дані не будуть використані третіми особами для будь-яких цілей, окрім боротьби з епідемією. Бажано, щоб, після подолання всесередовищної пандемії вся отримана таким шляхом інформація була знищена, окрім, можливо, даних, які стануть корисними у випадку аналогічної надзвичайної ситуації. У такому разі, дані мають бути ретельно захищеними від доступу до них третіх осіб.

Згідно абз. 2 підп. 1 п. 2 розділу II «Прикінцеві та перехідні положення» Закону України «Про внесення змін до Закону України «Про захист населення від інфекційних хвороб» від 13.04.2020 р. № 555-IX передбачено, що протягом 30 днів після закінчення карантину всі зібрані таким чином дані будуть знеособлені або знищені, що є досить вдалим рішенням [3]. Хоча, на нашу думку, слід розглянути варіант збереження подібної інформації, у випадку невтрата її актуальності з часом, на випадок виникнення подібної ситуації знову. Окрім того, накопичена інформація є цінним матеріалом для аналізу, результати якого можуть підказати певні закономірності та шляхи більш ефективного розв'язання аналогічних проблем в майбутньому.

Виникнення надзвичайної ситуації – пандемії COVID-19 – було непередбаченим. Але тепер можна зробити певні висновки, та використати отриманий досвід у майбутньому. Було б доцільно розробити на рівні інформаційного законодавства України зміни до прав та обов'язків громадян стосовно збереження та надання особами своїх персональних даних, надання даних юридичними особами на період боротьби з надзвичайними ситуаціями. Зокрема, регламентувати процедуру отримання, зберігання, використання та захисту від доступу з боку третіх осіб, даних фізичних та юридичних осіб, зібраних в період надзвичайної ситуації. Також, описати відповідну процедуру ліквідації чи зберігання, отриманих під час карантину, даних. Дані зміни до інформаційного законодавства України дозволять органам влади більш оперативно реагувати на виникнення подібних надзвичайних ситуацій та ефективніше впроваджувати відповідні заходи.

Список використаної літератури:

1. Про запобігання поширенню на території України гострої респіраторної хвороби COVID-19, спричиненої коронавірусом SARS-CoV-2: Постанова Кабінету Міністрів України від 11.03.2020 р. № 211. URL: <https://zakon.rada.gov.ua/laws/show/211-2020-п> (дата звернення: 11.05.2020)

2. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI. URL: <https://zakon.rada.gov.ua/laws/show/2297-17>(дата звернення: 11.05.2020)

3. Про внесення змін до Закону України «Про захист населення від інфекційних хвороб» щодо запобігання поширенню коронавірусної хвороби (COVID-19): Закон України від 13.04.2020 № 555-IX. URL: <https://zakon.rada.gov.ua/laws/show/555-20> (дата звернення: 11.05.2020)

4. Якуша В. Голова комітету НААУ з медичного права Ірина Сенюта: «Коронавірус яскраво ілюструє роль медицини і те, хто має бути найвищою цінністю для держави». Закон і Бізнес. № 16 (1470). 25.04–01.05.2020. URL: <https://zib.com.ua/ua/142409-koronavirus-yaskravo-ilyustrue-rol-medicini-i-te-hto-mae-but.html> (дата звернення: 11.05.2020)

Звичайна А. О.,
Фізико-технічний інститут
Науковий керівник: Фурашев В. М.,
к.т.н., с.н.с., доцент

ПРАВО НА ІНФОРМАЦІЮ В УМОВАХ КАРАНТИНУ

Актуальність. Постановка завдання. Сьогоднішні реалії свідчать про те, що інформаційна війна на фоні пандемії вже почалася. Фальшиві новини, підробки і паніка поширюються в рази швидше, ніж сам вірус. Теорії змови ллються в інформаційний простір як з рогу достатку, а потім обростають численними варіаціями і тлумаченнями.

Основна частина. В сучасних умовах перш ніж починати розглядати будь-яку тему треба визначитися із поняттям «карантин». Відповідно до ст.1 Закону України «Про захист населення від інфекційних хвороб» карантин це - адміністративні та медико-санітарні заходи, що застосовуються для запобігання поширенню особливо небезпечних інфекційних хвороб. Порядок встановлення карантинних обмежень закріплений ст.29 вище згаданого закону та ст.40 Закону України «Про забезпечення санітарного та епідемічного благополуччя населення». Карантин встановлюється та відміняється Кабінетом Міністрів

України. Питання про встановлення карантину порушує перед Кабінетом Міністрів України центральний орган виконавчої влади, що забезпечує формування державної політики у сфері охорони здоров'я (Міністерство охорони здоров'я України), за поданням головного державного санітарного лікаря України. У рішенні про встановлення карантину зазначаються обставини, що призвели до цього, визначаються межі території карантину, затверджуються необхідні профілактичні, протиепідемічні та інші заходи, їх виконавці та терміни проведення, встановлюються тимчасові обмеження прав фізичних і юридичних осіб. Карантин встановлюється на період, необхідний для ліквідації епідемії чи спалаху особливо небезпечної інфекційної хвороби. На цей період можуть змінюватися режими роботи підприємств, установ, організацій, вноситися інші необхідні зміни щодо умов їх виробничої та іншої діяльності [1].

Якщо уважно прочитати постанову Кабінету Міністрів України «Про запобігання поширенню на території України гострої респіраторної хвороби COVID-19, спричиненої коронавірусом SARS-CoV-2» можна зробити висновок: обмеження прав і свобод людини, які запроваджені, не стосуються прав, свобод і безпеки людини в інформаційній сфері [2]. У нашому законодавстві навпаки містяться норми, які гарантують громадянам доступ до відомостей про події, їхній розвиток, кількісні та якісні показники, плани влади тощо. Надзвичайна суспільна значущість коронавірусу надає громадянам можливість вимагати оперативного, повного, точного надання інформації від органів влади, органів місцевого самоврядування. Заборона залишається тільки в частині персональних даних та лікарської таємниці конкретних хворих.

На початку квітня деякі електронні ЗМІ оприлюднили адреси будинків в Києві (без квартир), де на той момент зареєстрували Covid-19. Пізніше на аналогічний шлях пішла і влада Києва. У Дніпрі на будинках, де живуть госпіталізовані з підозрою на коронавірус, з'явилися відповідні оголошення. На мою думку, у цій ситуації відсутнє будь-яке порушення законодавства.

Опублікована стаття не розкриває нічийх персональних даних і не відноситься до інформації з обмеженим доступом. Навпаки, вона може служити застереженням для тих, хто знаходиться поруч, щоб вони не заразилися.

Відповідно до ст.1 Закону України «Про доступ до публічної інформації» будь-яка задокументована будь-якими засобами та на будь-яких носіях інформація стосовно епідемії, яка є у володінні розпорядників, вважається публічною. Єдине питання, яке може виникнути: чи вона з обмеженим доступом чи відкрита. Але у законі чітко сказано: публічна інформація є відкритою, крім випадків, встановлених законом. Частиною 1 статті 6, цього ж закону, до інформації з обмеженим доступом відноситься: конфіденційна інформація, таємна інформація, службова інформація [3]. Враховуючи загрозу поширення епідемії такі обмеження можуть бути, наприклад, в частині лікарської таємниці конкретних людей та їх же персональних/конфіденційних даних (адреса проживання, прізвище, ім'я та по-батькові, дата народження, майновий стан тощо). Більше нічого не може потрапити в статус «обмеженої», з огляду на рівень суспільної значимості теми.

Згідно із ст.17 Закону України «Про захист населення від інфекційних хвороб» Громадяни та їх об'єднання мають право на отримання достовірної інформації щодо епідемічної ситуації в Україні. Органи виконавчої влади та органи місцевого самоврядування, органи державної санітарно-епідеміологічної служби та заклади охорони здоров'я зобов'язані періодично повідомляти через засоби масової інформації про епідемічну ситуацію та здійснювані протиепідемічні заходи [1].

Отже, майже вся, інформація, якою володіють державні або місцеві органи влади стосовно епідемії, розвитку подій, заходів, є публічною інформацією з відкритим доступом (це і кількість апаратів штучного дихання, і кількість і наявність тих чи інших препаратів наявних для лікування, кількість бюджетних коштів, які витрачено і заплановано витратити і на що саме, і хто є

постачальником, і плани реагування, і ті чи інші параметри щодо стану системи охорони здоров'я на будь-якому рівні, і кількість хворих, і кількість підозр на захворювання, і інформація про ціни на препарати, маски і т.д.).

Стосовно статистичної інформації у нашій державі. Вона існує у двох видах: державна та інформація, яка не належить до діяльності державної служби статистики. Правовий режим державної статистичної інформації визначається Законом України «Про державну статистику» та ст.18 Закону України «Про інформацію»: офіційна державна статистична інформація підлягає систематичному оприлюдненню. Держава гарантує відкритий доступ до офіційної державної статистичної інформації, за винятком інформації, доступ до якої обмежений згідно із законом [4].

Проте на практиці все виглядає чомусь зовсім по-іншому. Ще на початку пандемії в Україні проект StateWatch запустив моніторинг забезпечення українських лікарень засобами індивідуального захисту. Суть полягала в тому, що представники цього проекту надсилали запити на інформацію з однаковими питаннями до всіх облдержадміністрацій. Вони просили надати інформацію про кількість засобів індивідуального захисту для медперсоналу (костюми біозахисту, нітрилові рукавички, одноразові халати тощо) в опорних лікарнях на початок карантину і розрахунок кількості таких засобів, необхідний на весь час карантину. Результати їх експерименту виявилися дуже «цікавими та показовими». Понад третина областей не надали даних. Це Волинська, Дніпропетровська, Донецька, Житомирська, Закарпатська, Київська, Луганська, Одеська, Чернігівська облдержадміністрації. Хтось із розпорядників узяв 20 днів на розгляд додатково, хтось надав лише частину інформації, а Закарпатська облдержадміністрація на запит про забезпечення засобами індивідуального захисту повідомила про підготовку 100 ліжко-місць в області [5]. Що це означає? – Місцева влада намагалась приховати інформацію: лікарні, які

визначено для госпіталізації хворих з вірусом, на початок карантину були забезпечені на рівні 1–7% потреб.

Єдиний державний веб-портал відкритих даних підходить для вирішення проблеми ефективного та оперативного обміну інформацією про вірус і його наслідки, швидко реагувати на виклики, які виникають перед державою. Доступ до порталу мають усі держоргани та органи місцевого самоврядування, він має відкриту можливість отримувати дані через інтерфейс прикладного програмування, підтримує роботу з популярними форматами даних, забезпечує можливість оновлення наборів у режимі реального часу. Проте, навіть там з кількох тисяч розпорядників лише 10 оприлюднили набори про медобладнання [6].

Повне та своєчасне оприлюднення інформації, відкритих даних про Covid-19, супутні теми, такі як безробіття, ціни тощо, може стати поворотним моментом, як для боротьби з коронавірусом, так і для зростання рівня довіри до влади.

Висновки. Не зважаючи на поширення інформації стосовно Covid-19, ЗМІ не завжди відображають реальне становище справ, а навпаки нагнітають ситуацію. Хотілося б, щоб у нашому суспільстві люди дотримувалися не тільки санітарно-гігієнічних заходів, знаходячись на карантині, а й поширювали правдиву інформацію, яка б відповідала реальному стану подій у нашій країні. В кінцевому підсумку все зводиться до елементарної інформаційної гігієни, яка, як і регулярне миття рук, знижує ризик захворювання або, хоча б, допомагає запобігти психозу на індивідуальному рівні.

Список використаної літератури:

1. <https://zakon.rada.gov.ua/laws/show/1645-14>
2. <https://zakon.rada.gov.ua/laws/show/211-2020-%D0%BF#n3>
3. <https://zakon.rada.gov.ua/laws/show/2939-17>
4. <https://zakon.rada.gov.ua/laws/show/2657-12>
5. <https://statewatch.org.ua/publications/rezul-taty-monitorynhu-pro-hotovnist-likaren-ukrainy-do-shpytalizatsii-khvorykh-na-covid-19/>

6. https://data.gov.ua/global_search?q=%D0%B4%D0%B0%D0%BD%D1%96+%D0%BF%D1%80%D0%BE+%D0%BC%D0%B5%D0%B4%D0%B8%D1%87%D0%BD%D0%B5+%D0%BE%D0%B1

Балінська В. О., Ярош І. С.,
2 курс, Факультет соціології і права КПП ім.
Ігоря Сікорського
Науковий керівник: Бежвець А. М.,
старший викладач кафедри інформаційного
права та права інтелектуальної власності

НЕПРИПУСТИМІСТЬ ПОРУШЕННЯ ПРИНЦИПІВ ІНФОРМАЦІЙНИХ ВІДНОСИН ПІД ЧАС КАРАНТИНУ У ДІЯЛЬНОСТІ ЗМІ

Ситуація, що склалася в країні сьогодні, пов'язана з введенням карантину по всій території України, кидає виклик усьому суспільству. Суспільство перебуває під враженням низки подій, які висвітлюють офіційні джерела влади та засоби масової інформації (далі – ЗМІ). Свідомість кожної особи наразі перебуває в критичному стані внаслідок того потоку інформації, що сприймає населення щодня, незалежно від того, чи є дана інформація достовірною. Відтак, усе це змушує людей сприймати події з абсолютно іншого ракурсу.

ЗМІ є основними носіями і поширювачами інформації серед населення. Їх соціальна роль і значення для суспільства є неоціненними. Одним з основних завдань ЗМІ є одержання й доведення інформації до широкого кола осіб. Вони слугують своєрідним мостом між джерелами інформації й населенням, а тому на них покладено відповідальність за повноту і достовірність інформації. На практиці ж досить часто журналісти в погоні за сенсацією припускаються правових помилок, рідко посилаються на використані джерела інформації. Нерідко трапляються випадки, коли випущені публікації або сказана в ефірі інформація містить неперевірені дані, що сприяє викривленню (спотворенню) сприйняття тих чи інших явищ в свідомості людей.

Для того, щоб проаналізувати рівень впливу ЗМІ на населення, пропонуємо звернутись до статистичних даних. У 2019 році українці стали набагато менше довіряти ЗМІ – як показує дослідження USAID-Internews «Споживання медіа», довіра до всіх традиційних медіа впала в середньому на 11%, в порівнянні з 2018 р. Довіра коливається між 19% до загальнонаціональної преси, 22% до місцевого радіо та 49% до загальнонаціональних телеканалів – в той час як загальнонаціональним інтернет медіа довіряють 51% респондентів – найбільший показник цього року [1]. Отримані дані сформувались внаслідок великої кількості джерел, що публікують недостовірну інформацію, або ж замовні матеріали, також відомі як «джинса». Відтак, існує нагальна необхідність у підвищенні рівня довіри населення до засобів масової інформації.

Наразі ЗМІ почали шукати нові способи подачі інформації для населення. Висвітлення подій, пов'язаних з карантином, перебуває під пильним поглядом усього світу, тому багато хто намагається знайти сенсацію в сучасних подіях, час від часу викривлюючи інформацію про карантин та його наслідки, замінюючи основні наголоси на другорядні. Наслідком цього є поширення паніки серед населення, що робить його вразливим до дезінформації, а інформаційні відносини в державі таким чином розвиваються в неправильному напрямі. Саме тому актуальним стає питання непорушності принципів інформаційних відносин під час карантину як основи, на яку має спиратися кожен, хто бере участь в інформуванні суспільства.

Стаття 2 Закону України «Про інформацію» вказує на такі принципи інформаційних відносин як: гарантованість права на інформацію; відкритість, доступність інформації, свобода обміну інформацією; достовірність і повнота інформації; свобода вираження поглядів і переконань; правомірність одержання, використання, поширення, зберігання та захисту інформації; захищеність особи від втручання в її особисте та сімейне життя [2].

Серед принципів, про які слід наголошувати, в першу чергу в контексті обраної теми, варто виділяти принципи доступності інформації та достовірності і повноти інформації. Саме ці принципи, на нашу думку, перебувають в зоні ризику на час введення на території України карантину.

Так, принцип доступності інформації здебільшого стосується діяльності владних органів, які повинні забезпечувати суспільство усією необхідною інформацією, в тому числі такою, що стосується стану, перебігу та наслідків карантину. ЗМІ, в такому випадку, виступають гарантами цього принципу. Оскільки уся інформація, пов'язана з карантинном, складає суспільний інтерес, ЗМІ можуть вимагати надати доступ в органів влади до такої інформації, таким чином забезпечуючи непорушність принципу доступності інформації.

З іншого боку, дізнавшись, отримавши чи відшукавши необхідну інформацію і не знайшовши у ній «цікавинку», що була б вигідною для підвищення рівня зацікавленості населення їх джерелом, ЗМІ часом можуть оприлюднити неповну та змінену інформацію, що хоч і не містить правдивих фактів, але становить об'єкт зацікавлення для споживачів. Таким чином, відбувається порушення принципу достовірності та повноти інформації.

Звичайно, кожен має право вільно поширювати інформацію. Однак під час карантинного періоду існує підвищена загроза паніки суспільства. Тому будь-яке порушення принципу достовірності інформації є нехтуванням не лише моральних, але й суспільних і державних цінностей та інтересів.

На сьогодні за поширення неправдивих чуток, що можуть викликати паніку серед населення або порушення громадського порядку, законодавцем введено адміністративну відповідальність, передбачену статтею 173-1 Кодексу України про адміністративні правопорушення [3]. Однак цю статтю важко застосувати до ЗМІ, особливо якщо враховувати те, що висвітлена ними інформація може спиратися на дані органів влади, але бути поданою не в повному вигляді. Наприклад, у Луцьку до магазинів утворилися великі черги

через те, що місцеві ЗМІ написали, як про достовірний факт, про закриття всіх магазинів і аптек, спираючись на рекомендаційне повідомлення місцевої влади [4].

Разом з тим, активна інформаційна кампанія влади за допомогою ЗМІ вказує на беззаперечні наміри повноцінного забезпечення принципу гарантованості права на інформацію. Активна співпраця телеканалів та офіційних комунікаційних ресурсів влади дозволяє ЗМІ виступати посередником у забезпеченні права на інформацію кожної людини щодо усіх процесів, про які інформує влада стосовно карантинної ситуації.

Немає сумніву, що діяльність ЗМІ для принципів інформаційних відносин має як позитивні фактори, так і негативні, особливо в карантинний період. На жаль, порушення принципу достовірності та повноти інформації є дуже помітним в умовах карантину. Часто саме недостовірна інформація має найбільший вплив на свідомість особистості, що може призвести до паніки і невизначеності ситуації як для кожної конкретної особи, так і для держави загалом.

Висновки та пропозиції. Карантинний період лише підкреслив проблеми порушення принципів інформаційних відносин. Непорушність принципів цих відносин веде до стабільного функціонування усієї інформаційної системи, однак постійні порушення, особливо під час карантинного періоду, підривають довіру до держави, впливають на суспільну свідомість. Це вказує на недоліки законодавства у сфері інформації. В цьому контексті період після карантину має сприяти усвідомленню законодавця щодо удосконалення нормативної бази у сфері інформації.

Список використаної літератури:

1. Опитування Usaid-Internews «Ставлення населення до ЗМІ та споживання різних типів медіа у 2019 р.». 2019. URL : <https://internews.in.ua/uk/news/onlajn-media-ta-sotsialni-merezhi-pereho-pyly-liderstvo-u-telebachennya-za-populyarnistyu-v-ukrajini-nove-opytuvannya-usaid-internews-schodo-spozhyvannya-zmi/>.

2. Про інформацію: Закон України від 02.10.1992 р. № 2657-XII. / Верховна Рада України. 1992. № 48. Ст. 650. URL : <https://zakon.rada.gov.ua/laws/show/2657-12>.

3. Кодекс України про адміністративні правопорушення від 07.12.1984 р. / Верховна Рада УРСР. – 1984. – додаток до № 51. Ст. 1123. URL : <https://zakon.rada.gov.ua/laws/show/80731-10>.

4. Волинські новини. Перше інформаційне агентство. – 2020. URL : https://www.volynnews.com/ua/news/all/_pislia-nepravdyvoho-povidomlennia-pro-zakryttia-mahazyniv-u-lutsku-dov/.

Мухамедзянов А. І.,
фізико-технічний інститут
Науковий керівник: Фурашев В. М.,
к.т.н., с.н.с., доцент

ВПЛИВ ПАНДЕМІЇ КОРОНАВІРУСУ COVID-19 НА ПРАВА, СВОБОДИ І БЕЗПЕКУ ЛЮДИНИ В ІНФОРМАЦІЙНІЙ СФЕРІ

Сучасний світ змінюється, COVID-19 це подія номер один в новинах, явище яке впливає на життя кожного, змінивши буденність та звичайне життя на новини про кількість хворих, і ми це сміливо називаємо епідемія яка характеризується найбільшим поширенням інфекційного захворювання на території усіх країн світу і континентах. Характеризується відсутністю колективного імунітету в людства, і, зазвичай, ефективних засобів профілактики (вакцини) й лікування. Це явище яке впливає на все в сучасному світі, на роботу, навчання, відпочинок, і звісно це впливає на свободи звичайних людей. Карантинний та посткарантинний періоди мають великий вплив на додержання інформаційної етики і морально-етичних норм в соціальних мережах та ЗМІ. Людям необхідно знати саме справжню інформацію про теперішню ситуацію пандемії в світі, і особливо в себе на батьківщині. Наразі повсюди в Інтернеті є фейки, які розповсюджують неправдиву інформацію щодо коронавірусу чи карантину, переслідуючи свої цілі. Держава вкладає кошти та зусилля на те, щоб громадяни країни отримували правдиву інформацію з різних джерел,

включаючи і соціальні мережі. Всім добре відомо, що епідемія пішла з Китаю, а якщо точно то з провінції Ухань. Ми всі могли уникнути такого розвитку подій як зараз, якщо Китай інформував би людей, та весь світ, що гряде буря. Із початку кризової ситуації багато статей піддалися цензурі, а також і повідомлення провідних ЗМІ. Людей, які намагалися поділитися інформацією в соціальних мережах про коронавірус почали переслідувати та залякувати розправою або строком в тюрмі. Після початку розповсюдження на інші країни, почали інформувати про стан хворих та головне їх кількість, це призвело до великої кількості дезінформації. Для того, щоб забезпечити своєчасне і точне керівництво в галузі охорони здоров'я, уряд повинен запобігати дезінформації. Але не можна обмежувати свободу вираження думок, вони повинні бути законними, пропорційними й дійсно необхідними.

Одна з самих великих загроз це витік персональних даних суб'єктів, які перебувають на лікуванні, карантині або самоізоляції. Хакери та інші країни намагаються в цей важкий час здобути бонуси в гонці країн. І цим самим ставлять під загрозу права громадян. Разом з тим варто відзначити, що деякі хакерські угруповання дотримуються негласного кодексу не атакувати поліклініки та госпіталі. Держава повинна забезпечувати конфіденційність персональних даних пацієнтів.

Міжнародні норми про права людини гарантують кожному право на найвищий рівень здоров'я і зобов'язують держави вживати заходів для запобігання шкоди здоров'ю населенню і надання медичної допомоги тим, хто її потребує. Міжнародні стандарти в області прав людини також передбачають, що в ситуаціях серйозних загроз для здоров'я населення і надзвичайних станів, що несуть небезпеку життю нації, допустимі обмеження певних прав і свобод. Такі обмеження повинні бути науково обґрунтовані та вводитися в законному порядку. Якщо їх застосування не є довільним або дискримінаційним і

обмежене за часом, та при цьому дотримується людська гідність, то такі обмеження ведуть до досягнення мети.

Є закон який встановив, що дані про здоров'я відносяться до особливо чутливих. Публікація інформації онлайн має великий ризик для осіб, до яких вона відноситься, особливо для тих, хто й так належить до вразливих груп. Використання і обіг персональних даних про здоров'я повинно юридично регламентуватися гарантіями, заснованими на правах людини.

Влада повинна забезпечувати достовірність і оперативність інформування суспільства про коронавірус відповідно до принципів прав людини. Це важливо для недопущення поширення неправдивої та некоректної інформації. Також уряд повинен забезпечувати наявність і доступність всієї інформації про COVID-19 на багатьох мовах, у форматі, доступному для розуміння неписьменних або малограмотних людей

Список використаної літератури:

1. Як коронавірус впливає на права людини. URL : <https://www.amnesty.org.ua/koronavirus-i-prava-lyudyny/> (Дата звернення 25.05.20200

Білоконь Б. С.,
Фізико-технічний інститут
Науковий керівник: Фурашев В.М.,
к.т.н., с.н.с., доцент

ВПЛИВ ПАНДЕМІЇ КОРОНАВІРУСУ COVID-19 НА ПРАВА, СВОБОДИ І БЕЗПЕКУ ЛЮДИНИ В ІНФОРМАЦІЙНІЙ СФЕРІ

Ми всі говоримо про пандемію коронавірусу COVID-19, але давайте розберемося з цим визначенням. «Пандемія» - це епідемія, що характеризується найбільшим поширенням інфекційного захворювання на території усіх країн світу і континентах. Характеризується відсутністю колективного імунітету в людства, і, зазвичай, ефективних засобів профілактики (вакцини) й лікування.

Оскільки пандемія коронавірусу COVID-19 є надзвичайною ситуацією міжнародного значення, то вона впливає майже на все, включаючи й права і свободу людей. Карантинний та посткарантинний періоди мають великий вплив на додержання інформаційної культури і морально-етичних норм в соціальних мережах та ЗМІ. Людям необхідно знати саме правдиву інформацію про теперішню ситуацію пандемії в світі, і особливо в їхній країні. Наразі повсюди в Інтернеті є дезінформатори, які розповсюджують неправдиву інформацію щодо коронавірусу чи карантину. Держава вкладає кошти та зусилля на те, щоб громадяни країни отримували правдиву інформацію з різних джерел, включаючи і соціальні мережі.

Після початку спалаху коронавірусу в Китаї, китайська влада наполегливо прагнула стримувати потік інформації і контролювати правдиву інформацію про вірус. Із початку кризової ситуації багато статей піддалися цензурі, а також і повідомлення провідних ЗМІ. «Той факт, що частина цієї інформації доступна не всім, збільшує ризик шкоди від коронавірусу і затримує ефективне реагування», – наголошує Ніколас Бекелін.

Людей, які намагалися поділитися інформацією в соціальних мережах про коронавірус почали переслідувати та залякувати. Люди боялися говорити правду, тому що за це їх могли цькувати. «Хоча спростування фейків про вірус має вирішальне значення, закриття законного контенту у ЗМІ та соцмережах на цю тему не піде на користь громадському здоров'ю», – сказав Ніколас Бекелін.

Після того як вірус поширився з Китаю в сусідні країни Південно-Східної Азії, у В'єтнамі, Таїланді та Малайзії штрафували або заарештовували людей за розповсюдження правдивої інформації про спалах хвороби COVID-19. Для того, щоб забезпечити своєчасне і точне керівництво в галузі охорони здоров'я, уряд повинен запобігати дезінформації. Але не можна обмежувати свободу вираження думок, вони повинні бути законними, пропорційними й дійсно необхідними.

Є багато прикладів дискримінації людей, які були в Китаї чи в інших країнах, де прогресує коронавірус. Навіть якщо в них немає симптомів, людей замикають в їхніх квартирах, піддають цькуванню і приниженню іншими людьми. Це стається саме тому, що в людей немає вірної інформації щодо цього вірусу. Уряд повинен вживати заходів для захисту людей від дискримінації. Також керівництво країн усього світу повинно проявляти абсолютну нетерпимість до расистських нападів на людей азіатського походження. Солідарність й співпраця між країнами - це єдиний спосіб, яким світ може боротися з спалахом пандемії.

Держава повинна ефективно вживати заходів, щоб захистити від нападів і цькувань окремих осіб і груп людей, які можуть вважатися «винуватцями» пандемії, ретельно розслідувати всі повідомлення про такі факти і притягати винних до кримінальної відповідальності.

Ще однією загрозою, пов'язаною з карантинними заходами є витік персональних даних суб'єктів, які перебувають на лікуванні, карантині або самоізоляції. Відзначається зростання кібератак на організації охорони здоров'я та медико-біологічні НДІ. Найбільш цитований випадок в новинах – зараження в середині березня чеської поліклініки комп'ютерним вірусом-вимагачем. Разом з тим варто відзначити, що деякі хакерські угруповання дотримуються негласного кодексу не атакувати поліклініки та госпіталі. Відносно новим об'єктом кібератак по компрометації персональних даних називають системи телемедицини, популярні на Заході при домашньому лікуванні. Окреслена загроза зумовлює потребу в забезпеченні безпеки віддаленого доступу до ресурсів інформаційних систем і стійкості інфраструктури. У ході реалізації заходів щодо виявлення потенційних носіїв вірусу, держава повинна забезпечувати конфіденційність персональних даних пацієнтів.

Міжнародні норми про права людини гарантують кожному право на найвищий рівень здоров'я і зобов'язують держави вживати заходів для

запобігання шкоди здоров'ю населенню і надання медичної допомоги тим, хто її потребує. Міжнародні стандарти в області прав людини також передбачають, що в ситуаціях серйозних загроз для здоров'я населення і надзвичайних станів, що несуть небезпеку життю нації, допустимі обмеження певних прав і свобод. Такі обмеження повинні бути науково обґрунтовані та вводитися в законному порядку. Якщо їх застосування не є довільним або дискримінаційним і обмежене за часом, та при цьому дотримується людська гідність, то такі обмеження ведуть до досягнення мети.

Міжнародні норми про права людини зобов'язують державу забезпечувати гарантії свободи вираження думок, включаючи право шукати, отримувати і поширювати інформацію будь-якого роду незалежно від кордонів. Держава зобов'язана надавати інформацію, необхідну для заохочення і захисту прав людини, включаючи право на здоров'я. Комітет з економічних, соціальних і культурних прав відносить до «пріоритетних зобов'язань» забезпечення доступу до інформації, що стосується основних медичних проблем в громаді, включаючи інформацію про методи запобігання таких проблем і боротьби з ними. Права людини передбачають надання всьому населенню достовірної та актуальної інформації про сам вірус, про доступ до послуг або припинення надання послуг та інші аспекти реагування влади на епідемію.

Влада повинна забезпечувати достовірність і оперативність інформування суспільства про коронавірус відповідно до принципів прав людини. Це важливо для недопущення поширення неправдивої та некоректної інформації. Також уряд повинен забезпечувати наявність і доступність всієї інформації про COVID-19 на багатьох мовах, у форматі, доступному для розуміння неписьменних або малограмотних людей. Це повинно включати дублювання телевізійних оголошень (як в Тайвані); сайти, доступні для сприйняття людьми з інвалідністю, в тому числі з порушенням зору, слуху і когнітивних функцій, як наприклад сайт МОЗ, який має режим для перегляду

людям з порушенням зору. Телефонне сповіщення текстовими повідомленнями людей з вадами слуху. Для максимальної дохідливості слід використовувати гранично прості формулювання. Дітям інформація повинна подаватися у доступній для їхнього віку формі, щоб допомогти їм захиститися від вірусу.

Дані про здоров'я відносяться до особливо чутливих. Публікація інформації онлайн має великий ризик для осіб, до яких вона відноситься, особливо для тих, хто й так належить до вразливих груп. Використання і обіг персональних даних про здоров'я повинно юридично регламентуватися гарантіями, заснованими на правах людини.

Підкреслюючи критично важливу роль Інтернету в часи пандемії, експерти з прав людини закликають уряди не блокувати Інтернет, а, навпаки, негайно забезпечити якомога ширший доступ до Всесвітньої павутини. В умовах надзвичайної ситуації, коли інформація має життєво важливе значення, широкі обмеження на доступ до інтернету не можуть бути виправдані міркуваннями громадського порядку або національної безпеки. Необхідно підтримувати безперебійний і безперешкодний доступ до Інтернету, вживаючи заходів для того, щоб він був доступним малозабезпеченим громадянам.

Список використаної літератури:

1. ©2020 Amnesty International Ukraine «Як коронавірус впливає на права людини». URL: www.amnesty.org.ua/koronavirus-i-prava-lyudyny/ (дата звернення 04.05.2020 р.)
2. © 2020 Human Rights Watch «COVID-19 и права человека».
3. URL: www.hrw.org/ru/news/2020/04/01/340211 (дата звернення 05.05.2020 р.)

Вареня М.,

студент факультету соціології і права КПІ
ім. Ігоря Сікорського

Науковий керівник: Солончук І. В.,

ст. викладач кафедри інформаційного права
та права інтелектуальної власності КПІ ім.
Ігоря Сікорського

АКТУАЛЬНІ ПИТАННЯ ЗАХИСТУ ПРАВ І БЕЗПЕКИ ЛЮДИНИ В ІНФОРМАЦІЙНІЙ СФЕРІ В УМОВАХ КАРАНТИННО- ОБМЕЖУВАЛЬНИХ ТА ІНШИХ РЕЖИМНИХ ЗАХОДІВ

З розвитком інформаційних технологій у кожного з'являється більше можливостей для застосування своїх прав та свобод, а також ризиків для їх порушення. Існують найбільш актуальні в сучасних умовах системні проблеми захисту прав, свобод і безпеки людини в інформаційній сфері, до яких, зокрема, відносять:

- проблеми збору, зберігання та використання біометричних даних громадян;
- проблеми захисту персональних даних;
- проблеми додержання прав людини при формуванні єдиних державних електронних реєстрів;
- проблеми поширення інформаційної агресії і насильства в національному та глобальному інформаційному просторі;
- проблеми правової культури та моральності в інформаційній сфері
- проблеми доступу громадян до публічної інформації [1 с.6].

Сьогодні питання щодо захисту прав і безпеки людини в інформаційній сфері в умовах карантинно-обмежувальних та інших режимних заходів є актуальними як ніколи раніше. Із введенням карантину спостерігається збільшення випадків кіберзлочинності, шахрайства, крадіжок і підробок. Злочинці використовують в своїх цілях високий попит на певні товари, зниження мобільності громадян, перебування великої частини людей вдома та

їх віддалену роботу, обмеження суспільного життя, а також зростання тривоги і страхів на тлі пандемії [2].

За умов пандемії, введення карантину, зокрема, обмежень на відвідання публічних місць, актуальним є питання комплексного вирішення вказаних вище проблем та спільного пошуку шляхів їх подолання.

За даними Європейського поліцейського агенства (Європол), в результаті поліцейської операції, яка проходила по всьому світу в березні 2020 р., було вилучено близько 34 тисяч підроблених хірургічних масок. Також часто фальсифікуються противірусні та вітамінні препарати, а також ліки проти малярії «Хлорохін» [2].

Європол також попереджає про високі ризики, пов'язані з кіберзлочинністю за часів пандемії. Наразі багато хто працює у віддаленому режимі з дому, підключаючи менш захищені особисті комп'ютери до мереж фірм і організацій, що становить серйозну загрозу для безпеки.

Окрім того, експерти вказують на ймовірне подальше збільшення випадків шахрайства, адже аферисти надзвичайно швидко підлаштовують свої схеми під актуальну ситуацію й використовують в своїх цілях страхи та побоювання людей в кризові часи [2].

INTERPOL виділяє такі види шахрайства:

1. Телефонне шахрайство - злочинці називають себе працівниками поліклініки чи лікарні, які стверджують, що родич жертви захворів на вірус і вимагає оплати за медичне лікування;
2. Фішинг - електронні листи, які, нібито, надходять від національних чи глобальних органів охорони здоров'я, з метою обману жертв, щоб ті надали особисті дані, платіжні дані або ж відкрити додаток, що містить зловмисне програмне забезпечення [3].

Приклад поширеного шахрайства в умовах карантинно-обмежувальних та інших режимних заходів: шахраї направляють потерпілому електронний лист або

"розсилку" по викраденій базі від імені медичної установи чи установи державного управління про зміну графіку роботи або порядку звернення до організації. Коли потерпіла особа перейде по посиланню або завантажить файл для ознайомлення з інформацією, це призведе до завантаження вірусу. Також існує можливість, що особу попросять ввести свої персональні данні. Під кінець такої афери предметом шахрайства стають гроші, які вилучені з банківської картки.

Інша схема, поширена серед шахраїв, полягає в тому, що нібито був створений вірус, щоб зменшити чисельність людей та полегшити урядам контроль за ними. Жертву повідомляють про те, що в них є готова вакцина і щоб її отримати особа повинна перейти за посиланням і ввести свої дані (ПІБ, адреса, телефон тощо), а вже після цього данні отримують шахраї.

Підсумовуючи викладене, можемо стверджувати те, що аналіз динаміки інформаційного законодавства останніх років свідчить про його активізацію в напрямку регулювання інформаційної безпеки, як провідної інституції інформаційного права. Обумовлено це загостренням негативного інформаційного впливу та відповідних загроз національній безпеці країни в інформаційному секторі та розповсюдження глобальної пандемії вірусу COVID-19. Зокрема мова йде про низку законодавчих та підзаконних актів, таких як Постанова КМУ від 20 травня 2020 року №392 тощо, спрямованих на встановлення й регулювання протиепідемічних заходів.

Встановлені чинним законодавством на період карантину обмеження призвели до того, що рівень спілкування людей та продажів товарів (робіт, послуг) через мережу Інтернет виріс в рази. На цьому фоні значно активізувалися кіберзлочинці, про що INTERPOL був вимушений повідомити на офіційному сайті ще 18 березня 2020 р. У таких складних умовах люди потребують посиленого захисту своїх прав і безпеки в інформаційній сфері.

Держава має подбати про удосконалення відповідного законодавства, що регулює дані правовідносини.

Список використаної літератури:

1. Проблеми захисту прав людини в інформаційному суспільстві : матеріали наук.-практ. конф. / 1 квітня 2016 р., м. Київ / Упорядн.: В. М. Фурашев, С. Ю. Петряєв. Київ: НДІП НАПрН України, Національний інститут стратегічних досліджень, Секретаріат Уповноваженого Верховної Ради України з прав людини, НТУУ «КПІ» Вид-во «Політехніка», 2016. 150 с.

2. Новини України та світу. URL: <https://nv.ua/ukr/world/geopolitics/koronavirus-vidi-shahraystva-pid-chas-pandemiji-ostanni-novini-50078304.html> (дата звернення: 20.05.2020).

3. INTERPOL. URL: <https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-warns-of-financial-fraud-linked-to-COVID-19> (дата звернення: 20.05.2020).

Марцинюк В.,

студентка факультету соціології і права
КПІ ім. Ігоря Сікорського

Науковий керівник: Бежевець А. М. ,

старший викладач ФСП КПІ ім. Ігоря
Сікорського

ВПЛИВ КАРАНТИННОГО ТА ПОСТ КАРАНТИННОГО ПЕРІОДІВ НА РОЛЬ ТА МІСЦЕ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В СИСТЕМІ ЗАБЕЗПЕЧЕННЯ КОНСТИТУЦІЙНИХ ПРАВ І СВОБОДИ ЛЮДИНИ В ІНФОРМАЦІЙНІЙ СФЕРІ

Екстрені ситуації вимагають рішучих дій та виняткових заходів. Зіткнувшись із великими масштабами ризику для здоров'я, спричиненими пандемією коронавірусу, органам влади довелося швидко прийняти рішення стосовно подальшого життя всієї країни для того, щоб стримувати поширення хвороби. Запровадження карантину безумовно спричиняє певні порушення прав людини, проте це виправдовується станом необхідності захисту всього населення. Тимчасово обмежуються такі права та свободи людини, як: свобода пересування, свобода зібрань та свобода підприємницької діяльності.

Проте, чи можуть бути обмежені інформаційні права людини? Інформаційні права людей - це гарантовані державою можливості людини задовольняти її потреби в отриманні, використанні, поширенні, охороні і захисті необхідного для життєдіяльності обсягу інформації. Гарантоване Конституцією України право на інформацію стає все більш важливим для існування демократичного суспільства. Специфіка інформаційної безпеки людини, на відміну від державної безпеки, полягає в тому, що вона базується, передусім, на чітких та дієвих гарантіях прав і свобод людини в сфері інформації. Слід зазначити, що права на свободу інформації, свободу думки і слова належать до так званих прав "першого покоління" - громадянських та політичних прав, які початково вважалися і вважаються невід'ємною частиною людської особистості. Реалізація прав на інформацію, свободу слова є найважливішим механізмом захисту прав людини.

Зіткнувшись з пандемією, яка становить загрозу для мільйонів людей, влада впевнено використовує новітні технології масового спостереження. Зокрема, Китай використовує безпілотники, камери розпізнавання обличчя та технологію коду швидкого реагування для контролю за місцем проживання своїх громадян [1]. Мобільні оператори в Європейському союзі обмінюються даними з органами охорони здоров'я в Італії, Німеччині й Австрії, щоб допомогти контролювати, як люди дотримуються соціального дистанціювання, повідомляє агентство Reuters. Південна Корея, Сінгапур та Ізраїль дістають дані з мереж мобільних телефонів, даних кредитних карток та відеозображень для моніторингу дій людей. Ці країни здійснюють "нав'язливу" політику, де за кожним рухом громадян можна спостерігати, перевіряти та контролювати кожного [1]. У Росії захисники конфіденційності переживають, що система розпізнавання облич, використання якої не було обмежено чіткими правилами, нині може дозволити державі ще більше контролювати своїх громадян і після того, як епідемія закінчиться. Хоча таке спостереження на відстані є

ефективним у боротьбі з COVID-19, проте мало відомо про те, як ці дані будуть зберігатися надалі і чи припиняться це спостереження у посткарантинний період? Є припущення, що епідемія може призвести до зменшення прав людини не тільки у період карантину, але й у пост карантинний період, зокрема право кожного на інформаційну безпеку (право одержувати і передавати інформацію без втручання органів державної влади) знаходиться під загрозою. Оскільки, свобода пересування та свобода зібрань обмежені, більшість осіб працює онлайн, використовуючи соціальні мережі та різні Інтернет ресурси, то, відповідно, збільшилась роль інформації та інформаційних технологій. На жаль, кількість кібератак, випадків поширення недостовірної інформації зростає та трапляється дуже часто протягом карантинного періоду.

Законодавство України, зокрема Закон України “Про захист персональних даних” гарантує захист персональних даних, зокрема право на невтручання в особисте життя, у зв’язку з обробкою персональних даних (ст.1). Тому, після закінчення пандемії Covid-19, усі права та свободи людини і громадянина мають бути відновлені, адже згідно з демократичними принципами, політика посиленого нагляду з боку державних органів та порушення права на інформаційну безпеку є неприпустимими у сучасній державі, якщо надзвичайна ситуація (пандемія) відсутня. Адже, на думку Томаша Флідра, (координатор кібербезпеки) : “Обмежувати права людини на визначений період можна, якщо це працює для боротьби з епідемією. Але час повинен бути чітко обмеженим” [2].

Список використаних джерел:

1. Nay O. Can a virus undermine human rights? [Електронний ресурс] / Olivier Nay. 2020. URL: [https://www.thelancet.com/pdfs/journals/lanpub/PIIS2468-2667\(20\)30092-X.pdf](https://www.thelancet.com/pdfs/journals/lanpub/PIIS2468-2667(20)30092-X.pdf).
2. Хто буде стежити за тими, хто стежить за громадянами? Цифрові права в епоху корона вірусу. 2020. URL : <https://www.radiosvoboda.org/a/digitalni-prava-u-sviti/30520457.html>.

Мазуренко П. В. ,

студентка факультету соціології і права
КПІ ім. Ігоря Сікорського

Науковий керівник: Солончук І. В.,

ст. викладач кафедри інформаційного
права та права інтелектуальної власності
КПІ імені Ігоря Сікорського

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОСОБИ ТА БЕЗПЕЧНОГО ДОСТУПУ ДО ІНФОРМАЦІЇ В УМОВАХ КАРАНТИНУ

Безперечно, питання інформаційної безпеки на сьогоднішній день являє собою невід’ємний аспект багатьох сфер людської діяльності. Відповідно до статті 17 Конституції України, забезпечення інформаційної безпеки є однією з найважливіших функцій держави [1]. Фактично, неможливо знайти сферу, не суміжну з використанням інформаційних технологій, адже інформація нині - це ключовий фактор взаємодії у соціальному середовищі. Завдяки технологічним інноваціям ми маємо змогу значно полегшити процес виконання щоденних задач, проте у сьогоднішніх реаліях, зумовлених карантинно-обмежувальними заходами безпеки, особливо важливим та потребуючим уваги питанням, є захист від шахраїв, які прагнуть до створення, поширення або використання недостовірної інформації в цілях негативного інформаційно-психологічного впливу, або ж заволодіння та використання ними персональних даних, отриманими шляхом свідомої дезінформації та маніпуляції свідомістю громадян, що не мають достатнього рівня обізнаності у даній сфері.

Відповідно до Закону України "Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки", інформаційна безпека – це стан захищеності життєво важливих інтересів людини і громадянина, суспільства і держави, при якому запобігається завдання шкоди через неповноту, несвоєчасність і 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 [2].

Сьогодні питання незахищеності інформації набирає дедалі більшої актуальності, адже у зв'язку із поширенням пандемії COVID-19 значно збільшилася кількість розповсюджуваної недостовірної інформації, яка може ввести в оману суспільство та призвести до неправильного сприйняття та, у результаті, створити низку наступних проблем, які протиставляються до національних інтересів України в інформаційній сфері згідно Доктрини інформаційної безпеки України:

1. зростання випадків правопорушень в інформаційній сфері;
2. неможливість у повному обсязі забезпечити розвиток та захист інформаційної інфраструктури;
3. ненадійність захисту від руйнівних інформаційно-психологічних впливів [3].

У сучасному інформаційному просторі ключовими учасниками подій є користувачі соціальних мереж, адже саме у глобальній мережі Інтернет зосереджена основна кількість розповсюджуваних *фейкових* новин, які зловмисники створюють з метою розповсюдження паніки серед членів нашого суспільства. Нині боротьба з фейковими новинами має пряму дотичність до захисту права громадянина на інформацію, що гарантовано йому Законом України "Про інформацію", у якому одним з основоположних принципів є її достовірність та повнота [4]. Проте, водночас, не менш важливу роль відіграє наше суб'єктивне сприйняття ситуації та наявність критичного мислення, за допомогою якого ми можемо вберегти себе від згубного інформаційного впливу.

З боку влади України, а саме Міністерством культури, молоді та спорту України, було представлено на розгляд законопроект про дезінформацію, у якому розглянуті запобіжні міри щодо боротьби з неправдивими відомостями

про осіб, факти, події, явища, яких не існувало взагалі або які існували, але відомості про них неповні або перекручені [5]. Авторами проекту було запропоновано введення суворого контролю над соціальними мережами, що передбачає покарання журналістів за розповсюдження недостовірної інформації, а також представлена ініціатива щодо створення спеціального контролюючого органу – уповноваженого з питань інформації. Також проектом передбачалося введення штрафів, а у певних випадках - навіть можливість тюремного покарання. Проте даний законопроект зазнав критики, зокрема про свою несхвальну позицію висловилися Моніторингова місія ООН з прав людини, представники якої закликали українську владу утриматися від встановлення відповідних обмежень, адже поточний проект закону не відповідає міжнародним стандартам щодо прав людини [6].

На фоні пандемії помітно збільшився обсяг використання інформаційних технологій, які й до того були невід’ємною частиною сучасного життя. Стан захисту державних електронних інформаційних ресурсів, реєстрів, баз даних та інших інформаційних масивів залишається незадовільним, проте саме нинішня ситуація повинна слугувати державі важливим поштовхом до удосконалення вітчизняної нормативно-правової бази та її адаптації до міжнародних вимог та стандартів, що стане підґрунтям до розвитку стабільного інформаційного суспільства.

Найкраще, що може зробити держава для забезпечення інформаційної безпеки громадян, - створення сприятливих умов для розвитку інститутів громадського суспільства, а також засобів масової інформації. Щоб задовільнити всі умови, слід з більшою увагою поставитися до пошуку балансу між забезпеченням права на інформацію та підтриманням моральної і духовної стабільності серед суспільства, що дасть змогу не тільки надати захист інтересам громадян, а також сприятиме наданню їм доступу до якісної інформації.

Потрібно звернути увагу на те, що контролюючи ЗМІ та будь-яким чином обмежуючи доступ до мережі Інтернет, неможливо досягти бажаного результату та в повній мірі забезпечити національні інтереси як самої держави, так і її громадян. Тому найбільш оптимальний підхід – це позитивне сприяння шляхом створення якісного інформаційного сектору, який забезпечить становлення самобутнього та захищеного від несприятливих інформаційних впливів суспільства.

Список використаної літератури:

1. Конституція України: Закон України від 28 червня 1996 р. №254к/96-ВР. *Відомості Верховної Ради України*. 1996. № 30. Ст. 141.

2. Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки: Закон України від 9 січня 2007 р. №537-V. URL: <https://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=537-16> (дата звернення: 20.05.2020).

3. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»: Указ Президента України; Доктрина від 25.02.2017 № 47/2017. URL: <https://zakon.rada.gov.ua/laws/show/47/2017> (дата звернення: 20.05.2020).

4. Про інформацію: Закон України від 2 жовтня 1992 р. № 2657-XII. URL: <https://zakon.rada.gov.ua/laws/show/2657-12> (дата звернення: 20.05.2020).

5. Про внесення змін до деяких законодавчих актів України щодо протидії загрозам національній безпеці в інформаційній сфері: Проект Закону від 12 липня 2017 р. №6688. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=62236 (дата звернення: 20.05.2020).

6. Моніторингова місія ООН з прав людини: запис у Facebook. URL: <https://www.facebook.com/UNHumanRightsUkraine/posts/1501446583354713> (дата звернення: 20.05.2020).

Крицун Т. Р.,
факультет соціології і права
Науковий керівник Баранов О. А., д.
ю. н., с.н.с.

АПРОБАЦІЯ ЗМІН В ІНФОРМАЦІЙНІЙ КУЛЬТУРІ ЗМІ СПРИЧИНЕНІ ПАНДЕМІЄЮ КОРОНОВІРУСУ COVID-19

Практично все населення країни та світу зараз вимушено залишається вдома у зв'язку з карантином. Інформаційна сфера, як і будь-яка інша, зазнала значних змін під впливом пандемії та карантинних заходів, що з нею пов'язані. Це, в свою чергу, покладає обов'язок на ЗМІ та держави в цілому надавати актуальну, важливу, достовірну інформацію задля уникнення панічних настроїв у суспільстві.

Оскільки, людство вперше стикнулось з такою глобальною небезпекою, інформування про поширення коронавірусу COVID-19, загрози, що ним супроводжуються, етап на якому зараз знаходиться розробка вакцини, відомості про методи (способи) захисту та профілактики є найважливішим завданням ЗМІ на сьогодні.

Через актуальність та попит на таку інформацію ЗМІ переповнилися статистичними даними, підрахунками хворих, даними про медикаменти та засоби захисту, що стало причиною одноманітності ЗМІ.

Однією із проблем спричинених введенням карантинних заходів стала неможливість школярами відвідувати навчальні заклади. Органи державної влади вирішили використати ЗМІ в досить неординарному руслі задля подолання цієї проблеми.

21 березня під час зустрічі з керівництвом українських телеканалів Володимир Зеленський запропонував запустити загальнонаціональний освітній телевізійний проект, у межах якого «найкращі педагоги України проводитимуть відеоуроки з різних предметів шкільної програми для 5-11 класів, а найбільші

українські телеканали показуватимуть їх у своїх ефірах у найбільш зручний для дітей час” [1].

Така пропозиція досить швидко знайшла своє практичне відображення. Станом на сьогодні близько 12 найбільших телевізійних каналів України почали транслювати телеуроки. Хоч канали звісно отримують певну вигоду від цього, та все ж те, що ЗМІ відійшли від розважальної тематики, цілодобових новин і почали займатись навчанням дітей шкільного віку, заставляє замислитись над тим, що інформаційна культура ЗМІ не деградувала із запровадженням карантинних обмежень, а навпаки розвинулась та видозмінилась, ефективно підлаштувавшись під виклики сьогодення.

Прогалини в навчальній сфері, що не були передбачені МОН України, зокрема, мова йде про відсутність механізмів проведення дистанційного навчання та платформ, через які можлива взаємодія між вчителями та учнями, між викладачами та студентами, а також ефективних методів викладання на такій формі навчання. Такі прогалини почали заповнюватись завдяки співпраці провідних спеціалістів з різних сфер, через створення нових освітніх платформ, розробку професійних рекомендацій, надання власних напрацювань і розміщення їх на різних ресурсах. Такими ресурсами стали: соціальні мережі, різноманітні веб-сайти та ЗМІ. Студенти, учні, вчителі та викладачі почали підлаштовуватись до навчання в режимі online.

Такі зміни дозволяють зробити далекоглядні припущення про те, що Україна в подальшому зможе використовувати ЗМІ, як один із осовних освітніх ресурсів, шляхом накладання зобов'язань, що можуть бути прописані на законодавчому рівні.

"Масова комунікація" – це процес передачі та поширення інформації на велику аудиторію, з використанням ЗМІ. Якщо вести мову про це, то інтенсивність інформаційного потоку зараз (у період карантину) збільшилась в рази, завдяки мережі Інтернет, які доступні практично усім верствам населення.

Це дає можливість комплексно проводити навчальні заходи незалежно від напрямку чи предмету, який вивчається в усіх його аспектах (соціальних, моральних, психологічних, художніх, інтелектуальних). Ще у 1967 році на зустрічі соціологів у м. Кяеріку, на якій обговорювались проблеми масової комунікації, була зроблена спроба прийняти спільне рішення - розуміти під масовою комунікацією процес передачі інформації у суспільстві засобами преси, радіо, телебачення тощо [2].

Навряд чи хтось зможе заперечувати факт, що суспільство зазнає значних змін, трансформується та підлаштовується під новий стиль життя в період карантину. Так чи інакше пандемії настане кінець і усі держави будуть чи уже починають проходити пост карантинний період. У такий час роль засобів масової інформації значно посилюється. Саме в такі періоди зростає потреба громадян точно та об'єктивно оцінювати суспільні явища і події, в іншому випадку, коли в суспільстві все гаразд, коли жодних загроз життю немає потреба включати ЗМІ кожні дві години відпадає сама собою.

Згадаємо кілька фактів з історії людства: 11 вересня 2001 року (теракт в США), 11 березня 2011 року (великий тохокусський землетрус та аварія на АЕС Фукусіма-1 в Японії), 26 грудня 2004 року (цунамі в Індійському океані). Усі ці події, хоч і відбувались на території не багатьох країн, та все ж суспільний інтерес (цікавість) до подробиць та наслідків був неймовірно великим. Це дає підстави для того, щоб стверджувати, що коли у світі стається подія, яка стосується життів великої кількості людей, то це одразу є предметом широкого розголосу в ЗМІ цілої планети.

Ситуація, що відбувається зараз показує те, як усі люди залежать від кількості та якості інформації. Тільки стикнувшись із проблемою відсутності перевірених (достовірних) альтернативних джерел інформації, відбувається усвідомлення важливості ЗМІ в житті кожного.

Інформаційна культура – це той рівень інформаційного спілкування людей, що досягнутий у процесі його розвитку, а також характеристика інформаційної сфери життєдіяльності людей, в якій ми можемо відмітити ступінь досягнутого, кількість і якість створеного, тенденції розвитку, ступінь прогнозування майбутнього[3], саме у цьому слід відслідковувати зміни та робити певні підсумки.

Те, як карантинні заходи реорганізували повсякденне життя людей, значною мірою пришвидшило вивчення новітніх тенденцій взаємозв'язку ЗМІ і користувача інформації. Сучасні мас-медіа надають можливість людині встановлювати та підтримувати зв'язок із широким соціальним середовищем, кордони якого розміщені далеко за межами їх безпосереднього оточення [4].

Отже, з усього вище викладеного, можна зробити висновок, що рівень інформаційної культури ЗМІ та соціуму зростає в умовах певних катаклізмів та потрясінь, що створюють певні загрози життю людей.

Список використаної літератури:

1. Телеуроки — Детектор медіа: веб-сайт. URL: <https://detector.media/production/article/175969/2020-03-30-teleuroki-translyuvatimut-11-kanaliv/> (дата звернення 29.04.2020)
2. Лазарева Л.М. Медіакультура та її функції — Наукова бібліотека України веб-сайт. URL: <http://www.info-library.com.ua/libs/stattya/318-mediakultura-ta-yiyi-funktsiyi.html> (дата звернення: 30.04.2020)
3. Костюк М. А. Місце і роль засобів масової інформації у формуванні інформаційної культури суспільства УДК 070.23 (477) (043) — Кафедра культурології та інформаційної діяльності: веб-сайт. URL: https://mdgu-kid.at.ua/publ/misce_i_rol_zasobiv_masovoji_informaciji_u_formuvanni_informacijnoji_kulturi_suspilstva/1-1-0-29 (дата звернення: 30.04.2020)
4. Лапл Дж. Мас-медіа, комунікація, культура. Глобальний підхід. — Київ: К.І.С., 2002. – 264 с.

Лобода Р. І.

інститут Телекомунікаційних Систем,
Науковий консультант

Радзієвська О. Г., к. ю. н., провідний
науковий співробітник НДІ інформатики і
права НАПрН України

ВПЛИВ КАРАНТИННОГО ТА ПОСТ КАРАНТИННОГО ПЕРІОДІВ НА ДОДЕРЖАННЯ ІНФОРМАЦІЙНОЇ КУЛЬТУРИ І МОРАЛЬНО-ЕТИЧНИХ НОРМ В СОЦІАЛЬНИХ МЕРЕЖАХ ТА ЗМІ

Починаючи з 2019 року коронавірусна інфекція принесла значні зміни у різні сфери життя людини. До сьогодні людство ще не стикалось з пандемією в глобалізованому світі в умовах надзвичайно швидкого поширення інформації. Використовуючи різні технічні засоби, можна дізнатися, що відбувається на другому кінці світу. Відеозаписи лікарів, звернення науковців, політиків, ЗМІ, відеоблогерів дуже швидко стають доступними мільярдам людей. Інформації з кожним днем, з кожною годиною стає все більше і більше. Досвід попередніх років чітко показує, що все, навіть ретельно приховане, стане відомим усьому загалу. Можна пригадати вибори у США, збиття літака над Іраном, спроби Китаю спочатку не поширювати інформацію про спалах інфекційного захворювання. Тому потрібно розуміти, що приховати інформацію у сучасному світі вже не вдасться.

Актуальність цієї теми полягає, перш за все, в тому, що сьогодні людство опинилося в нових реаліях, де інформація відіграє значну роль у формуванні будь-яких системних заходів безпеки, а також може нести в собі таку ж токсичність для суспільства, як і сам вірус.

Метою даної роботи є бажання дослідити поведінку людей у соціальних мережах та ЗМІ під час карантинного та пост карантинного періодів.

Оскільки приховати інформацію в сучасному глобалізованому світі неможливо, залишається тільки перекручувати факти, створювати фейки, маніпулювати твердженнями. Створений фейк породжує невдоволення, гнів,

паніку, радість, будь-яку потрібну емоцію, якою з легкістю можна управляти. Так само як недостатність інформації призводить до культивування вимислів, які знову ж таки породжують певні почуття у населення. У цьому баченні хотілося б звернути увагу на дві проблеми, які становлять загрозу уже сьогодні. З одного боку – це бажання де-яких держав під виглядом боротьби з COVID-19 взяти інформацію під управління і контроль, тим самим звужуючи права та свободи своїх громадян. З іншого боку – це використання недостовірної, фейкової інформації в інформаційному протистоянні та проведенні спеціальних інформаційних операцій проти окремих груп чи держав.

Павло Ковтонюк, заступник міністра охорони здоров'я у 2016-2019 роках в своєму інтерв'ю зазначив, що в час популізму та постправди пандемія COVID-19 показала світові цілком реальні, а не віртуальні загрози. Очільник Міністерства охорони здоров'я зазначив, що «можна маніпулювати інформацією до тих пір, доки не захворіли або не вмерли цілком конкретні люди» [1]. Він також звертає увагу на те, що «популістичні уряди не здатні адекватно відповідати на загрозу. Вони діють або занадто пасивно, або занадто істерично – і завжди без чіткого плану. Цей урок дуже знадобиться і перед іншими світовими викликами: кліматичними змінами та міграцією» [1]. Можна помітити, що питання маніпуляції, пропаганди стоять досить гостро у сьогоднішніх реаліях. Звинувачення політиків, світової еліти у неспроможності протидіяти інформаційному впливу не є безпідставними.

«Ми не просто боремося з епідемією, ми боремося з інфодемією»,— заявив генеральний директор Всесвітньої організації охорони здоров'я (ВООЗ) Тедрос Аданом Гебреїсус, легітимізувавши новий термін, що описує нашу реальність. Інфодемія — це лавина дезінформації, нагнітання й залякування у бажанні масмедій підняти власні рейтинги, псевдонаукових порад та інтерпретацій, що накриває світ і серйозно ускладнює боротьбу з реальною проблематикою зупинення та подолання хвороби [2].

Суспільство давно зіткнулося з викликом інформаційних підробок, неправдивих новин і провокацій, емоційне поширення яких у соціальних мережах та ЗМІ призводить до трагічних подій у суспільстві. Українському соціуму це явище добре відоме за хвилями фейсбучних «зрад» та «перемог» часів Майдану, як і прагнення гасити ці шкідливі роздмухування емоцій. Нині ж бачимо, як це працює на глобальному рівні, дезорієнтуючи, сіючи паніку. Інфодемія — виклик світовому співтовариству, як зазначає Т.А. Гебреїсус [2].

11 березня 2020 року ВООЗ оголосила пандемію у зв'язку з поширенням коронавірусу в світі. В Україні, як і в багатьох інших країнах, ввели карантин. Такі заходи передбачувано викликали першу хвилю паніки — люди скуповують продукти в магазинах, захисні маски та антисептичні засоби в аптеках. Завдяки впливу соціальних мереж та швидкому поширенню інформації було створено значний ажіотаж, що призвело до значної кількості конфліктних ситуацій. Люди в прямому сенсі билися за товари першої необхідності.

Опрацьовуючи дану тему, було проаналізовано реакцію людей як на офіційно підтверджену, так і на офіційно не підтверджену інформацію.

Проаналізувавши коментарі людей на різних форумах з приводу поширення та наслідків інфекції, можна сказати, що лише незначна кількість людей не вдається до панічних висловів. При появі будь-якої нової інформації, не важливо вона офіційна чи ні, виникає велика кількість невдоволених, розгніваних коментарів. Відчуваючи свою безпомічність у ситуації, люди намагаються поділитися з іншими своїми думками. І далеко не завжди це добре, оскільки веде до поширення неперевіреної та суб'єктивної інформації. Не всі аналізують, перевіряють інформацію, що призводить до важких наслідків, у тому числі, до культивування негативних емоцій у спільноті, що може провокувати панічні настрої та невдоволення у суспільстві.

Висновки. Світ розвивається, інформації з кожним днем стає все більше. Обробляти її все важче. А спілкування онлайн дозволяє створювати, збирати, зберігати, опрацьовувати, подавати і використовувати інформацію, що забезпечує цілісне бачення світу. Світ став взаємопроникним. І це створює не тільки дивовижні можливості, а й великі ризики. Коронавірусна інфекція яскравий приклад. Невміння користуватися інформацією сьогодні, створює велику небезпеку завтра.

Наслідки епідемії можуть призвести до зміни формату роботи великої кількості людей. Що раніше було дивним, незрозумілим, стає реальністю. Віддалена робота, навчання використовуючи онлайн ресурси, перегляд фільмів вдома, спілкування з друзями усе це у більшій мірі переходить в онлайн режим. Тому досить важливим у пост карантинний період є наступні дії: не піддаватись паніці, уточнювати інформацію з різних джерел, знайомитись з новими методами виконання типових завдань.

Уміння людини брати інформацію з надійних джерел, порівнювати, аналізувати, критично осмислювати, приводити аргументовані докази, не піддаватись на провокації – усе це демонструє інформаційну культуру. Інформаційна культура формується завдяки інформаційній грамотності кожного. Вміння сприймати, аналізувати та поширювати інформацію створює безпечне інформаційне середовище.

Приходить на думку вислів: «Інформація – рятує , дезінформація – убиває».

Список використаних джерел:

1. Штогрін І. Пандемія коронавірусу: уроки для людства та України // Радіо Свобода, 21.03.2020 р. URL: <https://www.radiosvoboda.org/a/pandemiya-koronaviruskarantyn-vysnovky/30500165.html>

2. Дорошенко К. Світові інтелектуали про наслідки пандемії коронавірусу для людства. // ПАТ «НСТУ», 19.03.2020 р. URL: <https://suspilne.media/20654-svitovi-intelektuali-pro-naslidki-pandemii-koronavirusu-dla-ludstva/>

*Коваль С. Д.,
фізико-технічний інститут
Науковий керівник: Фурашев В.М.,
к.т.н, с.н.с.,доцент*

ДОСЛІДЖЕННЯ РІВНЯ ІНФОРМАЦІЙНОЇ КУЛЬТУРИ ТА ІНФОРМАЦІЙНОЇ ЕТИЧНОСТІ СТУДЕНТІВ ТА АСПРАНТІВ ФІЗИКО-МАТЕМАТИЧНИХ ТА ФІЗИКО-ТЕХНІЧНИХ СПЕЦІАЛЬНОСТЕЙ В УМОВАХ ПАНДЕМІЇ COVID-19

Пандемія COVID-19 внесла значні зміни у життя людства. Такі терміни як самоізоляція, карантинні заходи, пандемія, коронавіруси, ПЛР-тести увійшли у повсякденний словник звичайних громадян. Попри ці терміни, багато хто у спілкуванні у соціальних мережах, висловлюючи своє особисте ставлення до ситуації, яка склалась у світі, використовує некоректні образливі терміни, тим самим порушуючи як інформаційний етикет так і загальноприйняті морально-етичні норми.

Наприклад, вживання словосполучення «вірус з Уханю», «китайський вірус», «азіатська хвороба», замість затвердженого терміну COVID-19 (Co – означає “corona”, Vi– “virus” – вірус, D – “disease” – хвороба, 19 – рік спалаху). Або називати людей, які захворіли на коронавірус «жертвами коронавірусу», «постраждалими від COVID-19», або апогей клеймування – «випадки захворювання на COVID-19» - який дегуманізує громадян, хто вже захворів на коронавірусну інфекцію. Це визначення фігурує у державному стандарті медичної допомоги «Коронавірусна хвороба», додаток 2 [1], затверджене наказом МОЗ України від 28.03.2020 №722 «Організація надання медичної допомоги хворим на коронавірусну хворобу (COVID-19)» [2].

Із використанням цих термінів ми зустрічаємось кожен день, навіть при перегляді новин та брифінгів державних посадовців.

Вживання даних термінів неприпустимо у інформаційному середовищі, бо це створює враження, що хворі самі винні у своїй хворобі – що поводитись не правильно, не вберегли себе, а тому – гірші за нас. Це призводить до стигматизації хворих, в результаті якої пацієнти почнуть уникати тестування, госпіталізації або самоізоляції, що в свою чергу приведе до значного розповсюдження інфекції.

Протидія паніці – першочергове завдання влади, а кожне невдале формулювання може лише загострити ситуацію.

В рамках дослідження рівня додержання інформаційної культури і морально-етичних норм студентів та аспірантів фізико-математичних та фізико-технічних спеціальностей, було проведено соціологічне опитування студентів та аспірантів цих спеціальностей, спрямоване на виявлення використання клеймованих, образливих фраз, та настроїв, які сприяють поширенню паніки у суспільстві. Опитування проводилось за допомогою сервісу google Google Forms. Всього було опитано 255 осіб.

Опитування складалось із семи питань із різними типами варіантів відповідей. Тест наведений нижче:

1. Чи вживаєте Ви наступні словосполучення у повсякденному спілкуванні? (можна обрати декілька варіантів)

- a. «вірус з Уханю»
- b. «китайський вірус»
- c. «азіатська інфекція»
- d. Інше

2. Чи часто Ви чуєте з новин термін «випадок захворювання на коронавірус»? (один можливий варіант відповіді)

- a. Так, часто
- b. Так, але рідко
- c. Ні, жодного разу не чув

d. Не слідкую за новинами

e. Інше

3. Чи вживаєте Ви наступні речення для опису людей, які захворіли на COVID-19? (можна обрати декілька варіантів відповіді)

a. Люди поширюють вірус

b. Вони заражають інших

c. Вони переносять COVID-19

4. Чи називаєте Ви людей, які хворі на коронавірус, постраждливими від COVID-19? (один можливий варіант)

a. Так

b. Ні

c. Інше

5. Чи називаєте Ви людей, які хворі на коронавірус, жертвами COVID-19? (один можливий варіант)

a. Так

b. Ні

c. Інше

6. Чи вважаєте Ви спалах COVID-19 чумою 21-го сторіччя? (один можливий варіант)

a. Так

b. Ні

c. Інше

7. Чи вважаєте Ви, що COVID-19 це апокаліпсис? (один можливий варіант)

a. Так

b. Ні

c. Інше

Результат опитування та аналіз

Результати опитування подаються у графічному вигляді на наступній сторінці, у відповідності з нумерацією питань. Аналіз буде проводитись по кожному питанню, а загальний висновок – в кінці.

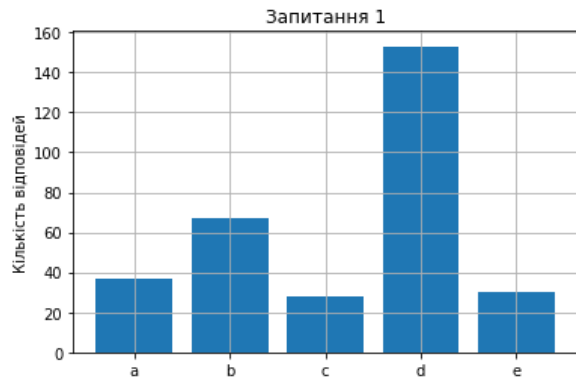


Рисунок 1 Відповіді на пит.1



Рисунок 2 Відповіді на пит.2



*Рисунок 3 Відповіді на пит.3
пит 4*

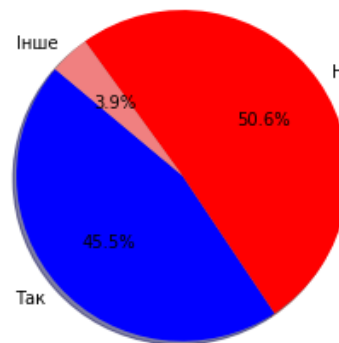
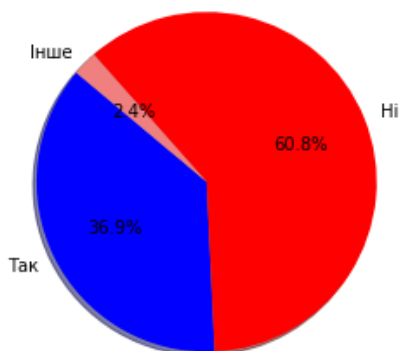


Рисунок 4 Відповіді на



*Рисунок 5 Відповіді на пит.5
пит.6*

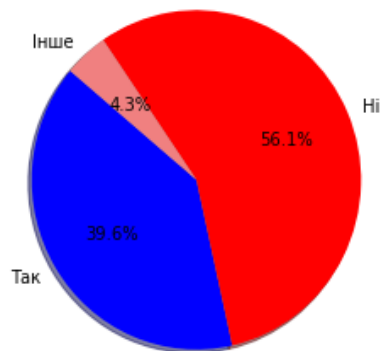


Рисунок 6 Відповіді на

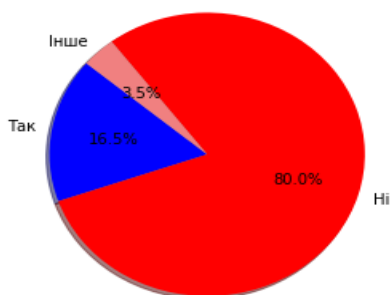


Рисунок 7 Відповіді на пит.7

1. На рис. 1 подаються розподіл відповідей на пит.1. Більшість відповідей на перше запитання (150 осіб) це варіант d) COVID-19, що є етично сприйнятливим. Потім йдуть відповіді b) «китайський вірус», а) «вірус з Уханю», е) інше, с) «азіатська інфекція». Вживання а), b), с) є неетичним

2. Згідно до рис. 2 більшість відповідей (56.1%) на друге запитання – варіант а) Так, часто. Використання клеймування «Випадок захворювання на COVID-19» є неетичним та несприйнятливим, хоча і використовується у всіх ЗМІ

4. На рис.3 показано, що більшість (120 осіб) респондентів обрали відповідь с) «Вони переносять коронавірус», що є етичним, у порівнянні із двома попередніми пунктами.

4. На рис.4 показано, що приблизно половина (50.6%) учасників опитування не вважають хворих на коронавірус постраждалими

5. Згідно до рис. 5 більшість студентів (60.8%) не вважають людей, хворих на коронавірус, жертвами COVID-19

6. Згідно до рис. 6 більшість (56.1%) студентів не вважють COVID-19 чумою 21-го сторіччя.

7. На рис. 7 показано, що переважна більшість (80%) респондентів не вважають COVID-19 апокаліпсисом.

Запитання 1-5 спрямовані на оцінку етичності студентів та аспірантів. Запитання 6-7 спрямовані на виявлення настроїв, які призводять до поширення паніки у суспільстві.

Необхідно відмітити, що переважна кількість студентів та аспірантів не піддалися панічним настроям. Але, відсоток тих, хто вважає COVID-19 чумою 21 сторіччя є, і його необхідно зменшувати.

Загалом, можна сказати, що ситуація цілком задовільна. Переважна кількість респондентів користуються етичними термінам. Але, все одно, ситуацію не можна випускати з-під контролю, бо відсоток людей, які користуються неправильною термінологією є, і він суттєвий. Пандемія не повинна переростати в інфодемію.

Ситуація з використанням терміну «Випадок захворювання на коронавірус» - вкрай несприйнятлива, причому з офіційних ЗМІ та законів України. Громадяни України – це не випадки, це живі люди. Тому, замість терміну «Випадки захворювання на коронавірус» пропоную застосовувати «Кількість осіб, які захворіли на COVID-19»

При використанні будь-яких термінів, пов'язаних з пандемією коронавірусу, потрібно підкреслювати необхідність запобіжних заходів та своєчасного лікування, фокусуватися на позитиві, підкреслювати ефективність раннього тестування за наявності симптомів захворювання.

1. Стандарти медичної допомоги «Коронавірусна хвороба (COVID-19)»// додаток 2: додаток до наказу МОЗ України від 28.03.2020 №722 «Організація надання медичної допомоги хворим на коронавірусну хворобу (COVID-19)», пункт 2

2. Організація надання медичної допомоги хворим на коронавірусну хворобу (COVID-19): наказ МОЗ України від 28.03.2020 №722

Головатюк О. А.,

студент 2-го курсу, ФСП, КПІ ім. Ігоря Сікорського

Науковий керівник: Бежжевець А. М., ст.
викладач, ФСП, КПІ ім. Ігоря Сікорського

ВПЛИВ КАРАНТИННОГО ПЕРІОДУ НА СОЦІАЛЬНІ МЕРЕЖІ ТА ЗМІ

Соціальні мережі та ЗМІ є особливими засобами донесення та отримання інформації. Інформація як об'єкт правовідносин може мати цінність, купуватися чи продаватися, відчужуватися в інший спосіб. Як абстрактне судження, інформація є у сучасному світі засобом впливу та аналізу подій, які відбулися, відбувалися та можливо будуть відбуватися. Інформація завжди займає значне місце в житті кожної людини, адже аналізуючи ті чи інші явища, людина вибудовує свою поведінку. Проте, інформація може відображати як істинний, так і неправдивий зміст подій.

Засоби масової інформації здійснюють загальний аналіз, синтез і висновки вмісту інформації, подій, які є актуальними у суспільстві, та подій,

які відбуваються чи можуть відбутися. Інколи, ЗМІ використовує для підсилення інформації думки, свідчення та висновки очевидців, експертів, псевдоекспертів, політичних діячів та інших осіб. Окрім того, ЗМІ користуються популярністю у великої кількості населення планети. За статистикою особи вікової категорії 16-78 років хоч раз використовували інформацію засобів масової інформації. Більшість із них продовжують користуватися актуальними джерелами отримування інформації, як свідчать дані опитування Research & Branding Group. Соціологи зазначають, українці віддають перевагу: телебаченню (53 %) та інтернету (42 %) [1]. Газети та радіо користуються популярністю серед старших вікових груп, і стають дедалі не популярними серед молоді та середньої вікової групи населення.

Враховуючи значний вплив на свідомість людей, головною метою ЗМІ повинно бути об'єктивне та неупереджене підняття актуальних проблем, висвітлення дійсності в проєктах, у випусках новин тощо. Проте, сьогодні можна неозброєним оком спостерігати різну політичну спрямованість ЗМІ через належність найбільших медіа-груп України (близько 76,25% аудиторії) певним олігархам [2], які заради власних амбіцій можуть здійснювати лобіювання політичних, суспільних чи приватних інтересів на власних телеканалах заради особистих прибутків, рейтингу чи впливу на процеси в країні.

Карантин і карантинний період, який триває в Україні із 12 березня 2020 року, вплинув на ЗМІ і змінив формат сюжетів новин на онлайн режим спілкування, телефонних дзвінків та відеоконференцій. Засоби масової інформації почали активно висвітлювати проблеми у медичній та політичній сфері протягом періоду карантину. В основному складається враження, що увага кожного глядача повинна зосереджуватися тільки на цих двох проблемах. Про вірус COVID-19 знає кожен. Вся увага деталізується на його подоланні, на кількості захворюваних та вилікуваних.

Але інші проблеми, серед яких знецінення гривні, збільшення цін на товари першої необхідності, воєнні дії на сході України, зображуються вже не так деталізовано як до карантинного періоду. Активно у засобах масової інформації почали використовуватися такі поняття, як пандемія, апарати ШВЛ, протівірусні маски, таблетки від вірусу Covid-19. Постійне дослідження, повторення та висвітлення цих проблем має психологічний вплив на кожну людину. Політичні діячі, зокрема, опозиція до влади, такими методами впливу намагаються використати недоліки медичної системи для того, щоб показати кожному, що влада не досить досвідчена та неактивна в діях. При цьому, на певних каналах активно висвітлюється, як відомі бізнесмени-філантропи (які, як правило, є власниками цих каналів або наближеними до них особами), надають допомогу малозабезпеченим медикам, лікарням, хворим під гаслом «Допомога тому, хто її потребує».

Карантинний період продовжується надалі [3]. І кожен повинен досліджувати та аналізувати отриману інформацію, виділяти основну та другорядну, правдиву та неправдиву інформацію серед наявного її масиву.

Соціальні мережі у період карантину здійснюють активну комунікативну функцію. Використання соціальних мереж та месенджерів набуває все більшої популярності серед людей, які потребують активного спілкування. Окрім того, користувачі, які зареєстровані у соціальних мережах, обговорюють актуальні події, інформацію та політику в нашій країні та світі. Карантин став основною темою для багатьох. При цьому більшість населення не розуміє, що інформація, яку поширює той чи інший користувач, може містити у собі авторську думку та особистий аналіз, а, відповідно, може бути необґрунтованою та містити неперевірені факти. Проте, на перший погляд вона здається правдивою та переконливою.

На сьогодні соціальні мережі нараховують близько 200 млн активних користувачів, тобто аудиторія поширення інформації надзвичайно велика та

неоднорідна. Соціальні мережі – це спосіб здійснення між людьми аналізу поданої інформації у ЗМІ, інтернет-ресурсах, та інформації, яка отримана у міжособистісних комунікативних суперечках. Будь-яка отримана інформація може бути тлумачена та використана для поширення її серед рідних, друзів та знайомих. Активні користувачі соціальних мереж своїми діями можуть мати прибуток із викладеної інформації чи проведеної реклами, використовуючи пандемію на власну користь. Зокрема, в соціальних мережах здійснюється активний продаж масок, пігулок від вірусу, захисні костюми, та засоби для дезінфекції рук, поверхонь та інших предметів. Проте, у соціальних мережах залишаються ризики виокремлення достовірної інформації серед недостовірної.

Пандемія Covid-19 змінила погляд на події в цілому. Загалом вся увага суспільства зосереджена на карантинних заходах та на наслідках, які неминуче настануть для кожного. Цьому, зокрема, сприяла діяльність ЗМІ та соціальних мереж. Завдання кожного - зосереджуватися на актуальній та дійсній інформації.

Список використаної літератури:

1. Карантин в Україні. Що варто знати? 2020. URL : <https://petropavlivka.city/read/card/69856/karantin-v-ukraini-scho-var-to-znati>.
2. Українські журналісти в період карантину: аналітичний звіт за результатами опитування. 2020. URL : <https://imi.org.ua/monitorings/ukrayinski-zhurnalisty-v-period-karantynu-analitychnyj-zvit-za-rezultatamy-opytuvannya-i32608>
3. Кабмін установив в Україні адаптивний карантин с 22 мая по 22 июня. 2020. URL : <https://delo.ua/economyandpoliticsinukraine/kabmin-ustanovil-v-ukraine-adaptivnyj-karantin-s-368695/>

Мазур Є.,
фізико Технічний Інститут КПІ ім. Ігоря
Сікорського
Науковий керівник: Фурашев В.М.,
к.т.н., с.н.с., доцент

ФЕЙКОВІ НОВИН СТОСОВНО COVID-19 В ІНФОРМАЦІЙНОМУ ПРОСТОРІ ТА ЇХ ВПЛИВ НА НАСЕЛЕННЯ

Реалії сучасного життя такі, що відлучившись з інформаційного простору хоча б на декілька днів, з'являється ризик заплутатися в останніх подіях, що в свою чергу загрожує потраплянням під інформаційний вплив та подальшою маніпуляцією. Це пов'язано з ростом відсотку інформації отриманої безпосередньо з мережі Інтернет та телебачення, та зменшенням «живого» спілкування. Також значно виросла зацікавленість населення в новинах через новизну такої ситуації та невідомість до неї.

Дійсно, сьогоднішній карантин є унікальною подією в історії людства, адже за останні 20 років, не було жодного випадку такого масового карантину. На згадку приходить тільки куриний (пташиний) грип, пік якого припав на 2005 рік. Пташиний грип - це інфекційне захворювання птиці, яке викликане вірусами грипу А. Вірус H5N1 - це підтип вірусу грипу А, який буває в основному у птахів, дуже заразний у птахів і може бути причиною їхньої смерті. [1] Але через його особливості, він не був настільки ж небезпечним для людей. Хоча засоби масової інформації не переставали обговорювати H5N1, проте жодного карантину не було. Необхідно додати, що інформаційний простір також відрізнявся. Відповідно до інформації Світового банку [2] лише 3,7% населення України мали доступ до глобальної мережі станом на 2005 рік, в той час як зараз близько 22,9 мільйонів українців користуються Інтернетом.

Саме тому проблема ненадійності джерел інформації та «фейкових» новин ще ніколи не була настільки актуальною. Ми пропонуємо розділити всі

фальшиві новини на категорії, дати короткий опис кожної з них, пояснити причину їх виникнення та навести приклад, обговорити можливі наслідки.

Роздмухування паніки.

Даний тип новин є одним з найнебезпечніших, адже паніка не дозволяє людям мислити об'єктивно. Це може призвести до необдуманих вчинків серед населення, прийняття невірних рішень, громадського тиску на владу, виникнення безпорядків та невиконання рекомендацій, щодо поведінки під час карантину.

Яскравим прикладом може бути фраза народного депутата Олександра Дубінського: «Якщо в Україну потрапить хоча б один випадок захворювання, то ми будемо всі хворіти. У нас тут буде епідемія іспанського грипу з тисячами жертв». [3]

І хоча ми не звинувачуємо нікого, але таке вискакування могло негативно вплинути на загальний стан занепокоєності громадян України.

Применшення загрози.

Іншою крайністю є навпаки – применшення загрози. Давня приказка «ніколи не недооцінюй свого супротивника», ще ніколи не була настільки актуальною. Дійсно, під час карантину загальний рівень безпеки залежить від кожного з нас, а небрежне ставлення частини суспільства негативно відобразиться на усьому населенні України. Так, згідно офіційної статистики Міністерства охорони здоров'я України, кількість захворювань на COVID-19 під час травневих свят значно виросло.

Я особисто знаю людей, що йшли до церкви під час Пасхи, мотивуючи це тим, що у Швеції відмовились від карантину. Ця інформація була досить поширеною, але як виявилось, була підставною, більше того її розповсюджували саме російські СМІ, з чого можна зробити висновок: це всього лиш інформаційна атака.

Пошук панацеї.

Страх захворіти, змушує людей шукати шляхи лікування. Саме через це стають популярними різні непідтверджені теорії. Одна з них говорила, що «перед тим як коронавірус потрапить до легень, він 4 дні перебуває в горлі. Якщо пити багато води, полоскати теплою чи окисленою водою, то це знищить вірус». Хоча одночасно з цим МОЗ повідомляло про відсутність чітких методів боротьби з захворюванням.

Необхідно пам'ятати, що самолікування шкідливо для вашого здоров'я, а експерти в Інтернеті досить часто не мають навіть профільної освіти.

Крім цього такі новини можуть мати комерційний інтерес. Так, досить поширеною була новина про те, що препарат «Декасан» має профілактичний ефект.

Антинауковість.

До цієї категорії можна віднести кожен з попередніх новин, адже вони не мали під собою жодного наукового обґрунтування. Важливо розуміти, що науковий діяльність це процес не швидкий, який вимагає досить ретельну перевірку отриманих результатів.

Тому досить дико виглядають звинувачення від українського інфекціоніста, доктора медичних наук, професора, Ольги Голобувської звинувачення США в розробці COVID-19 на підставі інформації взятої з російського сайту [4], який в 2017 був звинувачений НАТО у веденні інформаційної війни на користь Росії і поширенні проросійської пропаганди.

Нісенітниця.

Сюди сміливо можна віднести всі самі безглузді новини, які здаються смішними навіть при їх прочитанні. Чого варта теорія про те, що 5G вежі розповсюджують коронавірус. Для мене, студента технічного інституту, це виглядає як просто невдалим жартом, який при цьому став досить популярним.

Такі новини є скоріше інформаційним шумом, основна небезпека якого полягає в засміченні інформаційного простору, привертанні до себе надлишкової уваги та маскуванні справді важливих подій.

Під час нестандартних ситуацій, а саме такою є нинішній карантин, необхідно бути особливо уважними: перевіряти джерела інформації, довіряти тільки офіційним порталам та головне – мислити критично. При нинішніх умовах населення є особливо вразливим до інформаційних небезпек, тому обов'язком держави є спостереження за інформаційним простором, його очищення від фейкових новин та своєчасне оприлюднення достовірної інформації.

Список використаної літератури:

1. Офіційний сайт Державної служби України з надзвичайних ситуацій.
URL : <https://www.dsns.gov.ua/ua/Ptashiniy-grip.html>
2. Статистика Світового Банку <https://data.worldbank.org/indicator/IT.NET.USER.P2>
3. Інтерв'ю Олександра Дубінського на ток-шоу "Народ проти" від 13.02.2020. URL :
<https://www.youtube.com/watch?v=sDGIGzwcc4E&feature=youtu.be &t=1830>
4. Офіційний аккаунт в Facebook Ольги Голубовської. URL :
<https://www.facebook.com/ogolubovska>

Румянцева К.,
фізико-технічний інститут
Науковий керівник: Фурашев В. М.,
к.т.н., с.н.с., доцент

ПРОБЛЕМА ФАЛЬСИФІКАЦІЇ ДАНИХ ПІД ЧАС ПАНДЕМІЇ

Після першого спалаху коронавірусної хвороби 2019 року, серед населення та в інформаційному просторі поширилася дезінформація та конспірологічні побудови стосовно походження, поширення та інших різних аспектів щодо захворювання та вірусу, що його збуджує, дій урядів і приватних компаній. Ці чутки містять найрізноманітніші твердження,

зокрема щодо антропогенного походження вірусу: від розробок біологічної зброї до схем «контролю чисельності населення. Вони ширяться попри надійно встановлений факт походження вірусу SARS-CoV-2 від популяцій диких ссавців та його неконтрольованого поширення, що наносить шкоду економіці, здоров'ю та психічному стану населення усіх країн світу, а також відсутність, станом на березень 2020 року, вакцин.

У зв'язку з тим, що наразі інфопростір займає велике місце у нашому житті і його вплив та вага збільшуються з кожним роком, у лютому 2020 року світ зіткнувся з поняттям «масової інфодемії». Про це оголосила ВООЗ, посилаючись на надмірну кількість відомостей, точних та неправдивих, про вірус, які заважають людям отримувати адекватну оцінку подій у світі. ВООЗ заявила, що високий попит на своєчасну та вірогідну інформацію сприяв створенню прямої цілодобової гарячої лінії ВООЗ, де її співробітники та групи в соціальних медіа, здійснюватимуть моніторинг і реагування на дезінформацію через кіберпростір.

Такі впливові компанії, як Facebook, Twitter та Google заявили, що співпрацюють зі Всесвітньою організацією охорони здоров'я для вирішення питань з «дезінформацією». У дописі на власному блозі, Facebook заявив, що видалятиме вміст, позначений провідними світовими організаціями охорони здоров'я та місцевими органами влади, який порушує його політику стосовно вмісту щодо дезінформації, котра призводить до «фізичної шкоди».

У соцмережах розповсюджувалися різні неправдиві відомості про негативний вплив 5G на людей та природу. Це призвело до того, що кілька вишок 5G було знищено у Великій Британії. За однією з версій, випромінювання від антен нового стандарту пригнічує імунітет і таким чином коронавірус інфікує людей. Насправді ж, нові мережі ще не розгорнуті у повну силу в жодній країні, натомість коронавірус є в країнах, де немає мереж 5G. Інша ще безглуздіша версія припускає, що сам вірус можна якось

передавати за допомогою технології 5G. Було пошкоджені також вишки 3G і 4G. YouTube та Facebook видалили матеріали, що закликають знищувати вишки і розповсюджують фейки, пов'язані із 5G. Люди не просто псують та трошать майно приватних компаній, а й заражаються самі та розповсюджують вірус на мітингах та зустрічах.

Але боротися з фальсифікацією даних не завжди можливо. Багато країн приховують реальні статистичні цифри стосовно захворювання. Щоб на світовій політичній арені не загубити своє впливове місце та зберегти спокій серед населення. Державні СМІ проводять масштабну дезінформацію, через це населення халатно та безвідповідально відноситься до дотримання вимог карантину. Зараз проводиться інформаційна війна на цю тему. Кожна держава намагається викрити іншу у приховуванні даних.

Через умови карантину, кіберпростір проник у всіх сфери нашого життя: навчання, робота, спілкування, торгівля. Ми, як ніколи, вразливі до дезінформації, через обсяг тієї інформації, яку отримуємо кожен день. Це час, коли кіберзлочинці активізували всі свої сили та спроможності. І людям потрібен захист зі сторони влади та правоохоронних органів.

Коваленко В. В.,

факультет інформатики та обчислювальної
техніки

Науковий керівник: Фурашев В. М.,

к.т.н., с.н.с.

ПРОТИДІЯ ФЕЙКАМ ПРО COVID-19 ЯК СКЛАДОВА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

Пандемія коронавірусної інфекції COVID-19 в інформаційному просторі багатьох країн супроводжувалася поширенням фейків, пов'язаних з коронавірусом. Під фейками розуміється будь-який інформаційний контент

(текстові повідомлення, зображення, аудіо- та відео інформація), що розповсюджується різними каналами (наприклад, засобами масової інформації) з метою введення в оману окремих суспільних груп та здійснення цілеспрямованого впливу на громадську думку.

Розповсюдження фейків про коронавірус вже призвело до низки негативних наслідків: від активізації протестної поведінки та ігнорування карантинних заходів до пошкодження важливих інфраструктурних об'єктів. Так, 6 квітня 2020 року агенція BBC повідомила про підпал 5G-веж мобільного зв'язку [1]. Серед причин називалася версія, заснована на розповсюдженні недостовірної інформації про зв'язок технології 5G з поширенням коронавірусної інфекції. Також зустрічалися фейки про те, що: «карантин штучно вигаданий, тому треба виходити на вулиці та продовжувати звичайне життя»; «COVID-19 – легка хвороба, яку можна лікувати засобами народної медицини»; «вакцина проти коронавірусу буде містити чіпи, які при вакцинації будуть імплантовані в людину». Такі фейки поширювалися для підвищення недовіри громадян до урядів та ставили під сумнів заходи, що запроваджувалися для протидії поширення COVID-19. Активізація дезінформаційної діяльності у ЗМІ актуалізує потребу посилення боротьби з фейками в контексті забезпечення інформаційної безпеки держави.

Проблемам протидії фейкам та поширенню дезінформації присвячено багато напрацювань зарубіжних та вітчизняних науковців та експертів. Серед них потрібно відзначити Дубова Д., Ожевана О., Баровську А., Траммелла Т., Гобла П., Ренди А. та ін. У зазначених працях досліджується широкий спектр науково-прикладних проблем: визначення фейкової інформації, механізми (канали та інструменти) її поширення, негативні наслідки та мета розповсюдження відповідної інформації та ін.

Інституціями багатьох країн вживаються заходи з протидії поширенню дезінформації та фейків стосовно COVID-19. Так, Єврокомісія співпрацює з

різноманітними засобами масової інформації з метою стримування неправдивої інформації та підтримки авторитетних джерел інформації про COVID-19 [2]. На інформаційному ресурсі Європолу «COVID-19 Fake News» зазначається, що «злочинці швидко адаптували свої методи, щоб використовувати наші страхи навколо пандемії COVID-19, основна їх мета – отримання прибутку будь-якими необхідними засобами» [3] та пропонуються засоби протидії відповідним явищам.

Дослідження ініціатив та зусиль ЄС з протидії поширенню фейків в цілому дозволило відзначити високий рівень інституціоналізації, а також оперативності реагування на загрози інформаційній безпеці. Серед документів слід відзначити План дій проти дезінформації [4], розроблений спільними зусиллями Європейського Парламенту, Європейської Ради, Європейського економічного та соціального комітету та Комітету регіонів, а також Кодекс практики проти дезінформації [5], яким представники інтернет-платформ, провідні соціальні мережі, рекламодавці та рекламна індустрія домовилися про кодекс практичної діяльності зі здатністю до саморегуляції, щоб вирішити питання поширення дезінформації в інтернеті.

Інформаційна підтримка протидії поширенню фейків про COVID-19 в Україні значною мірою забезпечується зусиллями Міністерства охорони здоров'я (МОЗ) України. Для цього використовуються спеціальні інформаційні ресурси із щоденною інформацією про кількість нових випадків захворювання, одужання, смертельних випадків, а також поради щодо поведінки в умовах карантину та його послаблення, що довели свою ефективність. Надаються також спростування інформації, що носить неправдивий характер. Заради кращої поінформованості громадян МОЗ України публікує цю інформацію не лише на офіційних сайтах, а й на спеціально створених каналах у таких сервісах обміну повідомленнями, як Telegram та Viber.

Вагомий внесок у протидії фейкам про COVID-19 здійснюють приватні міжнародні компанії. Так, на пошукові запити про COVID-19 пошуковим сервісом Google надається відповідь про поради, що довели свою ефективність, інформацію про симптоми хвороби, посилання на органи влади багатьох країн (Міністерство охорони здоров'я у випадку України) та актуальні статистичні дані про перебіг епідемії. Аналогічним чином Facebook запустив кампанію з інформування користувачів під назвою «Центр інформації про коронавірус» [6], де також публікуються останні новини та поточні дані про перебіг епідемії.

Серед іншого, на державному рівні в багатьох країнах здійснюються широкомасштабні заходи з підвищення інформаційної грамотності громадян. Це включає програми з підвищення медіагігієни (вивчення джерел інформації, перевірки публікацій на достовірність, співставлення різних джерел інформації). Такі навички суттєво підвищує рівень інформаційної безпеки громадян та держави в цілому.

Невизначеність перебігу пандемічної ситуації та очікування другої хвилі захворювань неминуче призведуть до збільшення кількості фейків про COVID-19. В Україні доцільно здійснити превентивну роботу з протидії поширенню дезінформації про COVID-19. В рамках цієї роботи доцільно рекомендувати органам державної влади удосконалити нормативно-правове поле з протидії поширенню дезінформації на основі адаптації кращих практик ЄС. Підвищенню ефективності протидії фейкам про COVID-19 сприятиме кодифікація етичних норм. Для цього доцільно розробити та ухвалити Кодекс практики проти дезінформації на кшталт аналогічного кодексу ЄС. Рекомендувати розробити та імплементувати план заходів з протидії фейкам про COVID-19, які зокрема включали б: відслідковування неправдивої інформації та блокування відповідних інформаційних комунікацій; збільшення кількості інформаційних платформ, які у доступній для громадян формі інформують про перебіг пандемії COVID-19 в Україні та світі; навчання з підвищення інформаційної грамотності

громадян на основі роз'яснення негативних наслідків впливу фейків, формування критичного ставлення до інформації. Вжиття таких заходів дозволить зміцнити інформаційну безпеку України в період до появи ефективних засобів подолання коронавірусу.

Список використаної літератури:

1. BBC. Коронавірус: у Британії підпалюють 5G-вежі мобільного зв'язку. URL : <https://www.bbc.com/ukrainian/news-52188271>
2. The Mayor. The European Commission's Fight Against Coronavirus Disinformation. URL : <https://www.themayor.eu/en/the-european-commissions-fight-against-coronavirus-disinformation>
3. Europol. Staying Safe During COVID-19: What You Need To Know. URL : <https://www.europol.europa.eu/staying-safe-during-covid-19-what-you-need-to-know> за станом на 6 травня 2020р.
4. Action Plan against Disinformation. Joint Communication To The European Parliament, The European Council, The Council, The European Economic And Social Committee And The Committee Of The Regions. Brussels, 5.12.2018. URL : https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=56166
5. Code of Practice on Disinformation. European Commission. URL : <https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation>
6. Facebook. Coronavirus (COVID-19) Information Centre. URL : https://www.facebook.com/coronavirus_info

Кучеренко В. С.,
фізико-технічний інститут
Науковий керівник: Фурашев В. М.,
к.т.н., с.н.с., доцент

ДОСЛІДЖЕННЯ ВПЛИВУ ПАНДЕМІЇ COVID-19 НА ДИСТАНЦІЙНЕ НАВЧАННЯ СТУДЕНТІВ І АСПІРАНТІВ ФІЗИКО-ТЕХНІЧНИХ СПЕЦІАЛЬНОСТЕЙ ТА РОЛЬ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Очевидно, що пандемія COVID-19 значно вплинула повсякденне життя людства. Неможливо повністю досягнути яким флуктуаціям була підвернута глобальна економіка, система охорони здоров'я. Вже другий місяць у більшості країн Європи та Заходу введені карантинні заходи, що значним чином вплинуло на повсякденне життя громадян. Паралельно до переходу від звичайного

графіку роботи до дистанційного, школярі, гімназисти, студенти та аспіранти також через домашню ізоляцію повинні отримувати освіту.

Трафік даних мав неймовірний приріст під час перших днів карантину, через що навіть такі відеосервіси як “YouTube” та “Netflix” серйозно обмежували якість контенту^[1]. Усі освітні заняття перейшли у відео формат, що стало можливим завдяки таким сервісам як “Discord”, “Zoom”, “Skype”. Однак через шалену кількість користувачів почало все більше спливати новин у інфополі на тему хакерських атак: витік персональних даних, продаж активних аккаунтів^[2]. Останнє найстрашніше – хакери мають такий самий доступ до аккаунту, як і користувач, і можуть дивитися персональні відео зустрічі, чати тощо. “Zoom” вже активно впроваджує нові методи кібербезпеки у своїй компанії, проте це стосується не тільки цього сервісу.

Не заважаючи на таку неприємну новину, новітні технології забезпечили нам плавний перехід та можливості дистанційного навчання. Завдяки соціальним мережам та онлайн-платформам, на яких люди роблять тести викладачі мають усі можливості підтримувати навчальний процес та контролювати усвідомленість студентів.

Для того, щоб більш чітко вивчити питання дистанційного навчання було проведено дослідження щодо найбільш актуальних проблем. Було цікаво, як на карантин відреагувала локальна система освіти (ФТІ) та як це вплинуло на повсякденне життя студентів та аспірантів.

Опитування та аналіз результатів

Перш за все, за результатами опитування, стало зрозуміло, що студенти відреагували на карантин не зовсім однозначно. Згідно з діаграми, що на рис. 1, навчання до та після введення

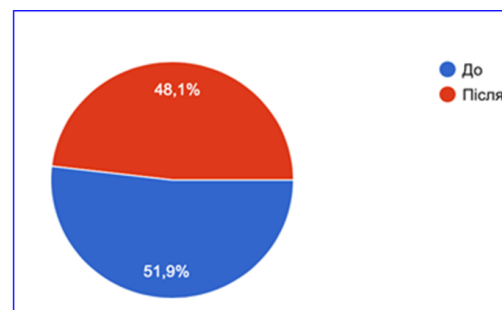


Рис. 1. Навчання до чи після пандемії Вам подобається більше?

карантину подобається студентам приблизно 50/50.

Щоб більш детально поглибитися в питання, треба зрозуміти що стало основними причинами першого чи другого вибору.

Питаючи скільки часу витрачалося до пандемії на лекції, семінари, домашнє завдання та самостійну обробку матеріалу у звичайний навчальний день та скільки часу витрачається так само на схожі речі тепер, були сформовані діаграми 2-3.

Аналізуючи, можна побачити, що частина студентів, котра займалася 7-8 або ж 3-4 години не змінилася. Проте група, що займалася 5-6 годин стала займатися менше – (**35.7** → **10.7**) %, (**3.6** → **25**)%.

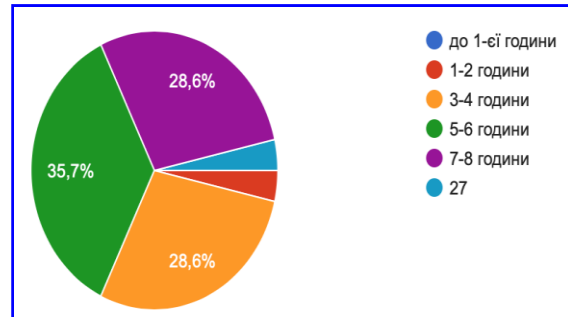


Рис.2. Час навчання ДО пандемії

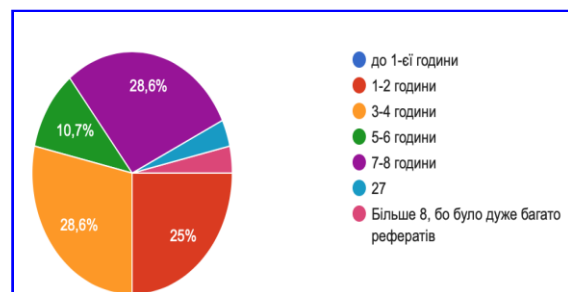


Рис.3. Час навчання ПІСЛЯ пандемії

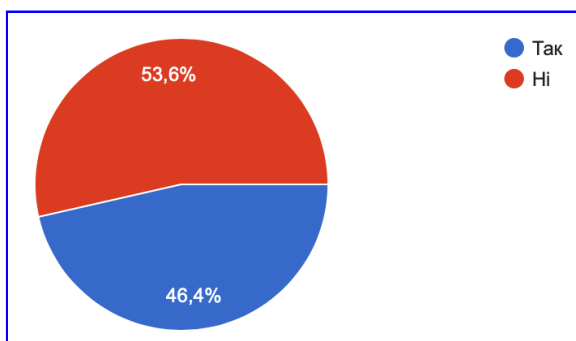


Рис. 4. Чи стало дистанційне навчання для Вас більш свідомим?

Цей результат може бути аргументований двома протилежними варіантами: спостерігається регрес в процесі навчання, студенти витрачають менше часу на обробку матеріалу.

Згідно з результатом наступного питання про те, чи стало для Вас навчання вдома більш усвідомленим, можна зрозуміти що обидва варіанти мають місце. Сидячи вдома, студенти не відчувають психологічний тиск з боку викладача і можуть вільно та самостійно формувати свій графік, проте також це може призвести до сприйняття

карантину як “канікул”. Наступне свідчить про халатне відношення до своєї освіти і безумовний регрес.

Грають роль безумовно і такі фактори, чи є в студента можливість взагалі навчатися вдома, маючи вільний час, робочий простір, техніку (мікрофон, ноутбук, камера тощо). На щастя, більшість студентів відповіли, що мають такі можливості, див. рис. 5.

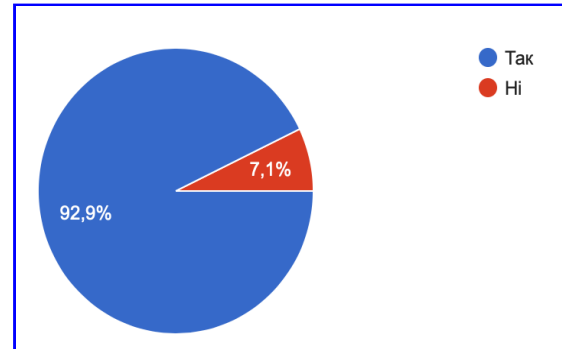


Рис. 5. Чи маєте ви можливість навчатися вдома?

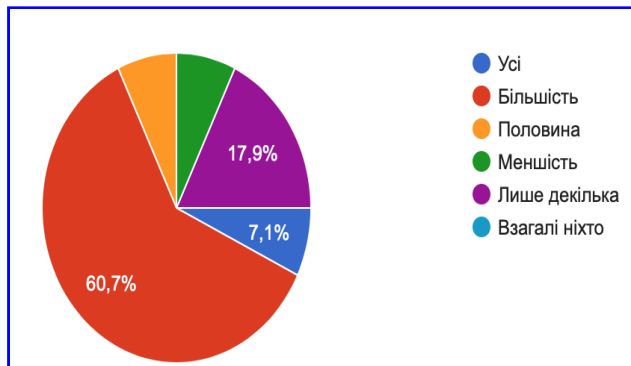


Рис. 6. Скільки викладачі швидко адаптувалися до дистанційного навчання?

Також грає роль рівень комунікації з викладачами. Пропонуючи різні альтернативні та цікаві методи навчання, викладач заохочує студентів до опанування матеріалу. Питаючи думку студентів, яка частина викладачів змогла швидко адаптуватися та встановити контакт

зі студентами, 60 процентів опитуваних відповіли – більшість. Інші результати представлені на рис. 6.

Повертаючись до теми інформаційної безпеки, найбільш вразливим місцем

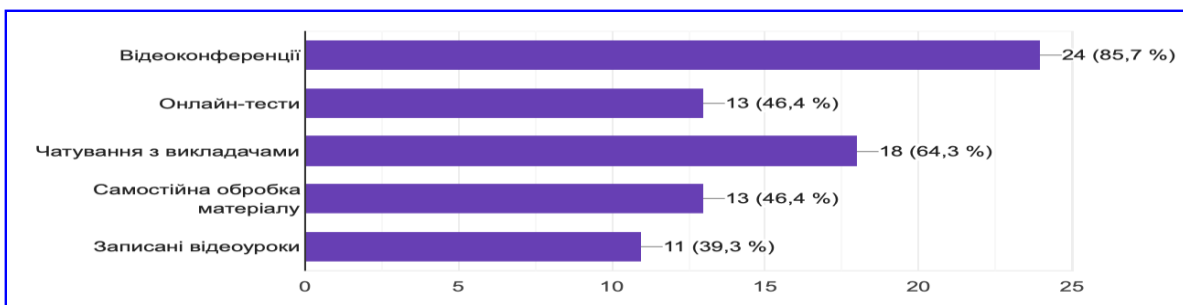


Рис. 7. Які методи навчання є, за думкою студентів, найбільш ефективними?

для процесу навчання залишаються відеоконференції, а саме сервіси, де вони проводяться. За думкою студентів, відеоконференції дійсно є найбільш ефективним методом навчання, проте не єдиним. Згідно з рис.7 видно, що пряма комунікація з викладачем також є найефективнішим методом навчання. Таким чином, роблячи процес більш дискретним, пропонуючи різні методи навчання, це допоможе уникнути витоку персональних даних студентів.

Звертаючи увагу на психологічне здоров'я студентів, критичним залишається те, що графік сну збився приблизно в 60 відсотків студентів. Беручи до уваги цей факт, викладачам та студентам потрібно формувати оптимальний графік.

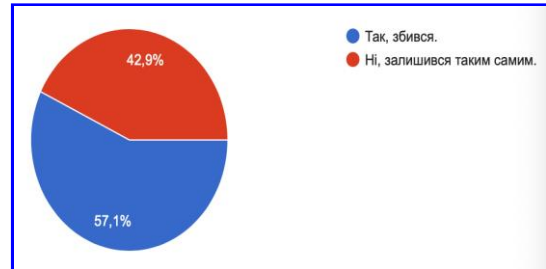


Рис. 8. Чи збився Ваш графік сну під час карантину?

Як не дивно, через масштабний карантин, з'являється багато можливостей

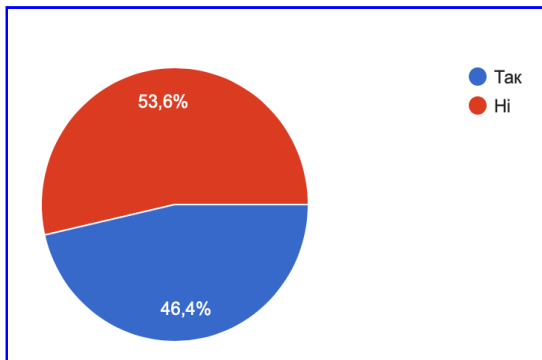


Рис. 9. Чи використали Ви можливість пройти безкоштовні курси?

отримати нові знання та професійні здібності. Глобальні освітні портали такі, як “Coursera” та “GeekBrains” відкрили багато платних курсів, щоб заохотити людей розумно витратити час вдома. Для студентів КПІ взагалі було виділено 5000 сертифікатів на будь-які курси гуманітарного або технічного

спрямування^[3]. На жаль, дивлячись на результат опитування “Чи використали Ви можливість безкоштовно представлені курси?” більше половини відповіли негативно.

До недавнього часу, невирішеним питання залишалася сесія цього семестру. Лише 9-го травня^[4] був остаточно виданий наказ про проведення дистанційної сесії. На думку студентів, дистанційна сесія та підготовка до неї буде легше, аніж звичайна. Остається це тільки перевірити

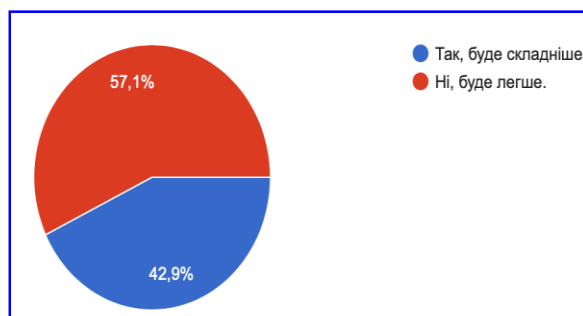


Рис. 10. Чи вважаєте Ви, що дистанційна сесія буде складніше?

Висновки

Був проведений аналіз дистанційного навчання та його адаптація серед студентів. Також, порівнюючи світові тенденції із витоком персональних даних у відео сервісах, стає зрозуміло, що серед методів навчання студентів це є не єдиний варіант, а отже і загроза мінімізована. Насамперед, проводячи опитування серед студентів, було зроблено багато цікавих висновків щодо сприйняття, графіку та методів дистанційного навчання.

Список використаної літератури:

1. <https://www.bbc.com/news/technology-52560602>
2. <https://edition.cnn.com/2020/03/19/tech/netflix-internet-overload-eu/index.html>
3. <https://kpi.ua/index.php/2020-04-coursera>
4. <https://drive.google.com/file/d/1zUxqVP2QUs7VQXXKIYvG4QFJuA3qqpYz/edit>

Завальнюк Ю. Ю.,

Студентка 3-го курсу ІПСА КПП ім. Ігоря
Сікорського, yulyzavalnuk@gmail.com

Науковий керівник: Іщенко В. В., викладач
кафедри публічного права КПП ім. Ігоря
Сікорського

ПРАВОВЕ РЕГУЛЮВАННЯ ВІДНОСИН У МЕРЕЖІ ІНТЕРНЕТ В УКРАЇНІ

У сучасному інформаційному суспільстві Інтернет – це особливий інформаційний простір, в якому класичні форми взаємодії замінюються електронними, проникаючи в діяльність держави, суспільства та громадян у всіх сферах. Близько 4,1 мільярда людей у світі користувалися Інтернетом у 2019 р. [1], а кількість інтернет-користувачів в Україні становить 22,9 мільйони [2]. У зв'язку з цим виникає необхідність правового регулювання роботи Інтернету та відносин, що виникають з його допомогою. Проте, не існує єдності у питанні, що саме підлягає правовому регулюванню щодо Інтернету (технічна складова Інтернету чи суспільні відносини, які розвиваються з його допомогою) та в якій мірі.

Згідно зі ст. 1 Закону України “Про телекомунікації”, Інтернетом є всесвітня інформаційна система загального доступу, яка логічно пов'язана глобальним адресним простором та базується на інтернет-протоколі, визначеному міжнародними стандартами [3].

Відповідно до ст. 20 Закону України “Про інформацію” порядок створення та керування засобами масової інформації визначаються законодавчими актами про ці засоби [4], а саме Законами України “Про друковані засоби масової інформації (пресу) в Україні” та “Про телебачення і радіомовлення”. Інформація в Інтернеті також регулюється і цими законами.

Інтернет-відносини – це особливі суспільні відносини, які виникають у результаті впливу норм інформаційного, комп'ютерного, міжнародного та

інших галузей права, міжнародних договорів на поведінку суб'єктів цих відносин. Це не лише правові, фактичні, етичні відносини, це складні соціальні зв'язки особливої правової, інформаційної та технічної природи [5, с. 50]. Поширення інформації в Інтернеті має таку саму природу, як і чутки в соціальному середовищі. Якщо до інформації є великий інтерес, вона швидко поширюється широкому колу осіб, немає інтересу – немає розповсюдження.

На даний момент не існує ефективного закону щодо регулювання багатьох методів поширення інформації в Інтернеті. Для прикладу поширення інформації в мережі Інтернет так званими блогерами (журналістами чи пересічними громадянами). На сьогодні блогерська діяльність в законодавстві України не врегульована ні у сфері реклами, ні у сфері інформації. Хоча ці люди мають великий вплив на суспільну думку та можуть нею маніпулювати.

Особливо важливе таке регулювання під час пандемії COVID-19. Так, СБУ притягає до відповідальності осіб, які поширюють в Інтернеті неправдиву інформацію щодо ситуації в Україні через поширення коронавірусу COVID-19: кількість жертв, методи лікування та ін. [6]. На порушників складають протокол про адміністративне правопорушення за ознаками ст. 173-1 “Поширювання неправдивих чуток” Кодексу України про адміністративні правопорушення. Також під час пандемії COVID-19 виникла проблема кібератак на дослідницькі інститути, що займаються знаходженням вакцини. Так, британські спецслужби стверджують, що мали місце спроби зламати сервери та пошту науково-дослідницьких центрів, які працюють у напрямку протидії коронавірусу [7].

Проте, надмірний контроль за достовірністю інформації в мережі Інтернет може призвести до порушення права на свободу слова, гарантованого ст. 34 Конституції України [8]. Тому необхідно збалансувати свободу та безпеку всіх учасників інтернет-відносин. Управління мережею Інтернет має відбуватися за принципом розподілу відповідних повноважень між державними органами та

громадськими організаціями. Це дозволить уникнути монополізації технічних ресурсів мережі, надмірної цензури вмісту, доступу до баз даних.

Таим чином, мережа Інтернет, стала надбанням усього людства, має багато як корисних так і шкідливих властивостей, що використовуються зацікавленими особами. На цей момент в Україні не існує законодавства, що охоплювало би всі сфери та методи поширення інформації чи спілкування. Державне регулювання мережі Інтернет має здійснюватися з урахуванням інтересів усіх зацікавлених сторін у правових відносинах. Також потрібно чітко окреслити в законодавстві поняття та критерії маніпулювання суспільною думкою, а також ввести адміністративну та кримінальну відповідальність за такі маніпуляції, за замовлення, замовчування та здійснення такого маніпулювання.

Список використаної літератури:

1. Лесишин І. Скільки людей у світі користуються інтернетом – ООН. URL: <https://www.the-village.com.ua/village/city/city-news/290933-skilki-lyudey-u-sviti-koristuyutsya-internetom-oon> (дата звернення 11.05.2020)
2. Лесишин І. Скільки українців користуються інтернетом – дослідження. URL: <https://www.the-village.com.ua/village/city/city-news/290161-skilki-ukrayintsiv-koristuyutsya-internetom-doslidzhennya> (дата звернення 11.05.2020)
3. Про телекомунікації: Закон України від 18.11.2003 № 1280-IV. URL: <https://zakon.rada.gov.ua/laws/show/1280-15> (дата звернення 11.05.2020)
4. Про інформацію: Закон України від 02.10.1992 № 2657-XII. URL: <https://zakon.rada.gov.ua/laws/show/2657-12> (дата звернення 11.05.2020)
5. Рассолов И. М. Интернет – право. Москва: Юнити, 2004. 143с.
6. СБУ притягає до відповідальності осіб, які поширюють фейки про коронавірус. URL: <https://ssu.gov.ua/ua/news/1/category/2/view/7300#.RO0g2Yt8.dpbs> (дата звернення 11.05.2020)
7. Ковач О. Спецслужби Британії: російські хакери намагаються викрасти інформацію щодо протидії COVID-19. URL: <https://www.radiosvoboda.org/a/30592588.html> (дата звернення 11.05.2020)
8. Конституція України від 28.06.1996 № 254к/96-ВР. URL: <https://zakon.rada.gov.ua/laws/show/254к/96-вр> (дата звернення 11.05.2020)
9. Красноступ Г. Правове регулювання суспільних відносин, пов'язаних з поширенням інформації за допомогою мережі Інтернет. URL: https://minjust.gov.ua/m/str_28845 (дата звернення 11.05.2020)

Герега Б. Д.,

Студент ФІОТ КПІ ім. Ігоря
Сікорського

Науковий керівник: Золотар О. О.,

д.ю.н., с.н.с., професор КПІ ім. Ігоря
Сікорського

ПРАВА І БЕЗПЕКА ДИТИНИ В КІБЕРПРОСТОРІ

Небажаний контент. Інтернет-хижаки. небезпечні віруси і шкідливі програми. Це лише мала частина небезпек з якими може зіштовхнутись дитина.

Безпека в кіберпросторі ставиться на перше місце, коли мова заходить про знайомство дітей з цифровими пристроями: смартфонами, планшетами та комп'ютерами.

Поряд з тим, що інтернет надає дітям швидкий і зручний доступ до корисної інформації, а також до розважальних матеріалів, все ж користування інтернетом пов'язане з величезними ризиками. Нижче представлені деякі з небезпек, які підстерігають дітей онлайн [1]:

1. Інтернет-залежність;
2. кібербулінг;
3. кіберпереслідування;
4. дитяча порнографія;
5. обман та шахрайство;
6. крадіжка особистої інформації.

В статті 16 Конвенції про права дитини ООН гарантовано, що кожна дитина буде захищена від незаконного втручання в здійснення її права на особисте і сімейне життя, недоторканність житла, таємницю кореспонденції або незаконного посягання на її честь і гідність; дитина має право на захист закону від такого втручання або посягання. В статті 13 зазначено, що дитина має право

вільно висловлювати свої думки; це право включає свободу шукати, одержувати і передавати інформацію та ідеї будь-якого роду незалежно від кордонів в усній, письмовій чи друкованій формі, у формі творів мистецтва чи за допомогою інших засобів на вибір дитини [2]. Проте в кіберпросторі присутні багаточисленні зловживання правами дітей. Наведу конкретний приклад взаємозв'язку прав дитини і небезпеки на які наражається дитина при їх реалізації:

- право на свободу пошуку інформації наражає дітей на вільний доступ до джерел, де йде мова про пропаганду насильства, суїциду, наркотиків, психотропних речовин, рекламу тютюну й алкоголю, нецензурні тексти;
- право на поширення інформації може призвести до крадіжки особистої інформації кіберзлочинцями, кіберпереслідувань, онлайн-шахрайств, збирання та розголошення приватної інформації ;
- право на відпочинок у нашому контексті може зіграти злий жарт, тобто при тривалому використанні девайсів діти наражаються на проблеми із зайвою вагою, із зором, з шийним відділом хребта, порушення нервового стану та розлади сну.

В рамках ініціативи ООН Child Online Protection Захист дитини в онлайн-овому середовищі (COP) були підготовлені спеціальні рекомендації, мета яких створити основу безпечного і захищеного кіберсвіту для майбутніх поколінь [3].

Боротьба за кібербезпеку і, в першу чергу, за безпеку дітей в Інтернеті сьогодні стає одним з основних трендів у розвитку глобального мережевого простору, і Україна тут не виняток. Вплив на інтернет-ринок в нашій країні виявляється переважно за рахунок правового регулювання галузі. В останні роки був прийнятий цілий ряд нових законів, що накладають обмеження на поширення інформації в мережі.

По-перше, в Україні блокуються сайти, що містять дитячу порнографію та інформацію про неповнолітніх, які постраждали в результаті злочинів.

По-друге, закривається доступ до ресурсів, здатним спровокувати небезпечне для життя і здоров'я поведінки дітей, сайти, де є заклики до самогубства, заворушень, екстремізму, участі в масових публічних заходах [4].

По-третє, законодавство захищає юних експериментаторів від будь-якої інформації в Інтернет, що розповідає про виробництво і поширення наркотиків.

Практика показує, що найбільш безпечним для дітей Інтернет став саме в тих країнах, де сильні були традиції громадського діалогу і, як наслідок, саморегулювання медіаринку - в Канаді, США, Великобританії та ряді інших держав Євросоюзу. Позитивний досвід цих країн поступово розповсюджується всесвітньою мережею, в тому числі за рахунок реалізації різних глобальних програм і ініціатив.

Важливу роль при цьому відіграє нова європейська стратегія економічного розвитку на найближчі 10 років, прийнята в 2010 році, - «Європа 2020» (Europe 2020). Розроблена як відповідь на кризу 2008 року стратегія покликана створити умови для сталого та всеохоплюючого економічного зростання і розвитку Євросоюзу. При цьому першою з семи провідних ініціатив стратегії є реалізація Цифрового Порядку денного для Європи (Digital Agenda for Europe) [5, с. 11].

Для забезпечення безпеки дітей в інтернеті існує безліч різноманітних інструментів: антивірусне програмне забезпечення, VPNs (віртуальні приватні мережі) і додатки для реалізації батьківського контролю. Завдяки цим інструментам можна отримати можливість контролювати діяльність дітей в мережі, що забезпечує розумне використання інтернету дитиною.

Список використаної літератури:

1. Діти в Інтернеті: реальні загрози віртуального світу – 2018. – URL: <https://learning.ua/blog/201811/dity-v-interneti-realni-zahrozy-virtualnoho-svitu/> .

2. Конвенція про права дитини // Законодавство України. – 1989. – URL: https://zakon.rada.gov.ua/laws/show/995_021 .
3. Child Online Protection // Committed to connecting the world – URL: <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/COP.aspx> .
4. Рекомендації щодо вікової класифікації інформаційної продукції // Законодавство України. – 2013. – URL: <https://zakon.rada.gov.ua/rada/show/ru/vr060623-13/conv> .
5. EUROPE 2020 // European Commission. - 2010 – URL ресурсу: <https://ec.europa.eu/eu2020/pdf/COMPLET%20EN%20BARROSO%20%20%20007%20-%20Europe%202020%20-%20EN%20version.pdf>

Челеніс А.,
фізико-технічний інститут
Науковий керівник: Фурашев В.М., к.т.н.,
с.н.с., доцент

КІБЕРБЕЗПЕКА ТА COVID-19

Сьогоднішня ситуація з COVID-19 нагадує схожість між двома, на перший погляд зовсім не схожими галузями, епідеміологією та кібербезпекою. Ми можемо взяти кілька уроків з вірусу реального світу та застосувати їх для безпеки в інтернеті.

Для цього порівнюємо поширення інформації по комп'ютерних мережах з хворобою. Ця схожість починається ще на найнижчому(базовому рівні), коли ви тільки підключаєтесь до інтернету, то запускається маршрутизація, при якій, якщо один маршрутизатор дізнається, що ви зайшли в систему, то повідомляє відразу інших. Цей процес є хвилеподібним і поширює інформацію як хворобу.

Отже, давайте з'ясуємо чого може навчити нас епідемія щодо безпеки в Інтернеті?

По-перше, нам потрібно розуміти те, що захворювання поширюються між людьми, коли ми з'єднуємось між собою, тобто спілкуємось. Однак, так як людські мережі є глобальними та взаємопов'язаними, хвороба розповсюдилась по всьому світу, навіть дійшла до невеликих віддалених острівних громад. В

інтернеті зловмисникам найпростіше спочатку порушити цілі «низького» значення, а потім поширюватись далі. Це відбувається тому, що ми не можемо захистити всі наші мережі до кожної кінцевої точки. Саме тому, кожна атака, починається з пошуку одного порушеного місця і звідти вже можна дістатись до іншого. Ця система схожа на авіаперельоти, що також є чудовим засобом для перенесення вірусу. Для того, щоб вірус не поширювався, більшість країн ввели карантин. Аналогічно, цифровим захисникам потрібно розбити схеми руху інформації за допомогою сегментації, яка перегороджує дані на різні ділянки. Це запобігає переходу «інфекції» в нові сегменти.

По-друге, важливим є знання де знаходиться інфекція. У боротьбі з хворобою вже стало зрозумілим, що різниця між країнами в яких більше випадків захворювання і в яких менше в тому, що хто може більше перевірити людей.

Тобто можна побачити, де знаходиться хвороба і запобігти її ускладненню: коли ми дізнаємось про носія, то тестуємо контактні лиця і поміщаємо під самоізоляцію. Цифрова безпека є схожою. Спеціалісти намагаються дізнатись, де знаходиться інфекція і потім «наздоганяють» те, що вже почало поширюватись. Однак, все ж таки, цифрова версія набагато складніше, оскільки комп'ютери «спілкуються» через мережу в різних напрямках, які змінюються. В умовах кризи в інтернеті немає простої відповіді на питання «як ця інфекція потрапила сюди і куди піде далі?». Для того, щоб знайти відповідь командам безпеки потрібно зрозуміти всі шляхи доступу та потоки інформації.

По-третє, так званий метод уповільнення. Глобальні зусилля залишитися вдома та «згладити криву» щодо поширення хвороби - це чудовий крок для зменшення напруги нашої медичної системи. Так само уповільнення онлайн-атаки приносить потужні переваги. Ми знаємо, що ви не зможете зупинити кожного зловмисників, але сповільнюючи їх, ви купуєте час, коли ваші датчики

можуть виявити цифрових зловмисників, щоб ви змогли б відреагувати на блокування чи карантин.

Нарешті, «гігієна» критично важлива. Найважливіші та повторювані поради щодо нинішньої ситуації COVID-19 завжди однакові: Вимийте руки. Це наша перша і найкраща лінія захисту. В інтернеті все те саме: основні засоби гігієни. У цифровій царині гігієна мережі включає в себе знання того, що є у вашій мережі, що ваші пристрої надійно налаштовані, що ваша мережа налаштована за призначенням, і що будь-які зміни не впливають на вашу безпеку.

Однією з основних проблем сьогоденної ситуації є те, що зловмисники пристосовують свої методи до пандемічної реальності. Протягом останніх місяців були проведені дослідження, які виявили зміну тактики зловмисників, які використовують підвищений інтерес до COVID-19. Згідно з повідомленнями різних організацій, зловмисники продовжують використовувати тему пандемії коронавірусу для створення більш переконливих приманок. Тема COVID-19 також продовжує використовуватися у спам-повідомленнях. За перші 100 днів спалаху кількість спам-повідомлень, що використовують «коронавірусні теми», збільшилася на 26%, а кількість тематичних атак, які видають себе як COVID-19 підскочила на 30%, повідомляє одна з охоронних фірм. Оскільки зараз велика частка працівників працює з дому, де кіберзахист не є хорошим, зловмисники мають великий успіх. Кількість URL-адрес, які були заблоковані після натискання користувача, за цей період зросла на 56%.

Від підроблених електронних листів команд Microsoft до масової реєстрації доменів, пов'язаних із COVID-19, кіберзлочинці та шахраї роблять ставку на те, що віддалені працівники з більшою ймовірністю натискатимуть на тему коронавірусу. На початку квітня Microsoft зазначила, що зловмисники використовували страх перед вірусом, щоб спокусити користувачів переходити

на посилення та розлучатися з конфіденційною інформацією, такою як дані для входу.

Отже, в умовах сьогодення нам потрібно звернути більше уваги на інформаційну безпеку та кібербезпеку, покращити систему захисту.

Зозуля В. О.,

Фізико-технічний інститут

Науковий керівник: Фурашев В. М., к.т.н.,

с.н.с., доцент

КІБЕРБЕЗПЕКА В УМОВАХ ПАНДЕМІЇ КОРОНОВІРУСУ COVID-19

На даний момент часу пандемія коронавірусу COVID-19 торкнулася всіх сфер нашого життя, включаючи інформаційну частину. Тисячами повідомлень щодня приходить інформація від різних джерел, повідомляючи нову кількість заражених, небезпеку самого вірусу і застереження у вигляді самоізоляції.

Найскладнішим є визначити, яка інформація є правдивою та якому джерелу можна довіритися. Тому що інтернет, телебачення, ЗМІ майже всю інформацію повідомляють у переробленому вигляді : пандемію коронавірусу перетворили на інформаційну зброю.

І така інформаційна пелена стала прикриттям для багатьох хакерських атак. Департамент кіберполіції Нацполіції України повідомив про те, що кіберзлочинці скористалися пандемією коронавірусу, щоб замаскувати свої атаки з використанням злочинного програмного забезпечення, під повідомлення про COVID-19 [1].

Метою хакерів є отримання персональних даних користувачів від різних інтернет ресурсів (соціальні мережі, електронна пошта, банківські реквізити) [2].

Для введення в оману кіберзлочинці використовують у своїх повідомленнях

(розсилках) посилання на слово «Corona». Також, вони поширюють шкідливе програмне забезпечення шляхом копіювання інформаційних панелей організацій, що надають актуальну інформацію про COVID-19 [3].

За інформацією Департаменту кіберполіції Нацполіції України в Інтернеті виявлено близько 170 фейкових інформаційних ресурсів з приводу пандемії COVID-19 [4].

Вперше повідомлення про кібератаки було прийнято у ВООЗ на початку розростання пандемії коронавірусу в Україні (середина березня). Інтернет-ресурс імітував внутрішню поштову систему деякої організації. На той момент часу кількість хакерських атак збільшилася вдвічі, порівнюючи з результатами до виявлення вірусу [4].

Результати опитування близько 400 спеціалістів по інформаційним технологіям і інформаційній безпеці у світі виявили, що близько 70% спеціалістів повідомили про збільшення числа атак чи загроз з початку спалаху короновірусної інфекції.

Щоб не стати жертвою кіберзлочинців Департамент кіберполіції Нацполіції України порадив ряд застережних правил в умовах пандемії коронавірусу :

1. Користування інформацією тільки з офіційних джерел : МОЗ, МВС, КМУ.
2. Використання ліцензійного програмного забезпечення та ліцензійних антивірусних програм.
3. Не переходити за сумнівними посиланнями.
4. Не завантажувати підозрілі файли з листів електронної пошти.
5. Постійно оновлювати операційну систему [2].

А найголовніше правило це не піддаватися паніці та мати серйозне та відповідальне відношення до своєї безпеки як у реальному світі, так і в інформаційному.

Список використаної літератури:

- 1.<https://ua.news/ru/kyberpolytsyya-predupredyla-o-fyshyng-rassylkah-pod-prykrytyem-covid-19/> - Інтернет-ресурс
- 2.https://lb.ua/society/2020/04/06/454652_kiberpolitsiya_predupredila.html - Інтернет-ресурс
- 3.<https://korrespondent.net/ukraine/4214062-khakery-staly-maskyrovat-ataky-pod-soobscheniya-o-koronavyruse> - Інтернет-ресурс
- 4.<https://korrespondent.net/world/4208759-v-voz-zaiavyly-o-tysiachakh-khakerskykh-atak-v-den> - Інтернет-ресурс

Собко І. О., Морква С. О.,
студенти 3-го курсу ІПСА КПІ ім.
Ігоря Сікорського
Науковий керівник: Іщенко В. В.,
викладач кафедри публічного права
КПІ ім. Ігоря Сікорського

ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ РОЗВИТКУ КІБЕРБЕЗПЕКИ УКРАЇНИ В УМОВАХ КАРАНТИННОГО ТА ПОСТКАРАНТИННОГО ПЕРІОДУ

Відкриття Всесвітньої мережі є одним з найбільших досягнень людства, яке назавжди змінило світ, подарувавши можливості миттєвого доступу до інформації. Проте через стрімке поширення інформаційно-комунікаційних технологій світова спільнота отримала не лише численні переваги, а й цілу низку проблем, зумовлених дедалі більшою вразливістю інфосфери щодо шкідливого впливу. На сьогоднішній день кібератаки – це вид злочинності, що найбільш стрімко розвивається, як в Україні, так і по всьому світу. За даними, опублікованими Cybersecurity Ventures, у 2019 р. злочини у сфері використання електронно-обчислювальних машин, систем та комп'ютерних мереж і мереж електрозв'язку по всьому світу в середньому відбувалися кожні 14 секунд, що майже у 3 рази частіше у порівнянні з 2016 роком [1]. Актуальність цієї проблеми не варто недооцінювати, адже враховуючи швидкість поширення, постійне вдосконалення злочинних методів та масову інформатизацію подібний

вид атак за досить незначний період часу може викликати глобальну катастрофу. Особливо гостро питання кібербезпеки постає саме зараз, в умовах карантину, що був викликаний пандемією COVID-19. Постановою Кабінету Міністрів України від 11 березня 2020 р. № 211 на території України було запроваджено карантин на період з 12 березня 2020 р. до 22 травня 2020 р. [2] та встановлено цілу низку обмежень, серед яких й обмеження підприємницької діяльності. У зв'язку з цим компанії вимушені масово використовувати інструменти для віддаленої роботи і переходити в онлайн, що за умови відсутності належного захисту робить їх уразливими для хакерів. Під прицілом знаходиться персонал фінансових установ, телекомунікаційних операторів і IT-компаній, а метою кібератак найчастіше стає крадіжка грошей або персональних даних. За статистикою експертів компанії ESET, у першому кварталі 2020 р. кількість шахрайських сайтів зросла на 21% у порівнянні з четвертим кварталом минулого року [3].

Враховуючи усю критичність та екстреність кібербезпеки, що насувається на Україну, надзвичайно важливо, щоб українське законодавство виявилось готовим до запобігання та у найгіршому випадку подолання наслідків подібної ситуації. Проте, через новизну самого терміну «кіберзахист», недостатнє розуміння можливих руйнівних наслідків кібератак та технічну складність, дане питання дуже слабо врегульовано у законодавствах більшості країн світу (в т.ч. і України). Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 р. №2163-VIII [4] лише окреслив контури законодавчої бази, що регламентує відносини у сфері кібербезпеки України. Каталізатором таких змін у законодавстві став вірус Petya [5], котрий показав яких масштабів можуть набувати кіберзлочини, атакувавши десятки українських банків, медіа ресурсів, держустанов та приватних підприємств. Безперечно ця комп'ютерна надзвичайна ситуація показала українським законотворцям, що нехтувати кібербезпекою не можна ні в якому разі, тож на

сьогоднішній день питання кібербезпеки регулюються Законом України «Про основні засади здійснення кібербезпеки України», Стратегією кібербезпеки України, Конвенцією про кіберзлочинність, Кримінальним кодексом України та іншими нормативно-правовими актами.

Проте, кіберзлочинність не стоїть на місці, тож питання чи відповідає українське законодавство сьогоденним реаліям та чи будемо ми готові до можливих небезпек все ще потребує детального аналізу. У процесі дослідження серед здобутків вже прийнятих нормативно-правових актів можна виділити наступні: вперше були окреслені такі поняття, як кібербезпека, кіберзагроза, кіберпростір, кіберінцидент, кібершпигунство, кібертероризм; визначено об'єкти критичної інфраструктури й що найголовніше цей перелік віднесено до інформації з обмеженим доступом, що означає, що ця інформація є закритою для пересічного громадянина, що правильно з точки зору безпеки; передбачено створення Національної системи кібербезпеки, а також урядової команди реагування на комп'ютерні надзвичайні події CERT-UA. Також важливим здобутком є відсутність цензури у зазначеному вище законі, адже даний нормативно-правовий акт не поширюється на соціальні мережі та блог-платформи. Це дуже важливий виняток, адже межа між кіберзахистом населення та зазіханням на свободу слова громадян дуже тонка. Проте експерти наголошують, що законодавство України все ще потребує правок і доповнень, адже наразі притягнення до відповідальності через кіберзлочини майже неможливе [5]. Хоч і встановлено, що за порушення у сфері кібербезпеки особи несуть відповідальність передбачену цивільним, адміністративним та кримінальним законодавством, в кодексах України відсутні будь-які згадки поняття «кіберпростір», що може здійснювати складнощі в притягненні до відповідальності.

Для того, щоб зрозуміти які аспекти законодавства потребують модернізації, необхідно взяти до уваги досвід інших країн. Протидія

кіберзлочинності в загальному розумінні включає в себе загальнодержавні заходи економічного, політичного, виховного та іншого характеру, а також комплекс спеціальних заходів, спрямованих на безпосереднє подолання злочинності. Враховуючи міжнародний характер кіберзлочинності, у боротьбі з нею життєво необхідне значення має гармонізація національних законодавств. Проте, гармонізація повинна враховувати регіональні вимоги і можливості. Велике значення регіональних аспектів в здійсненні стратегій боротьби з кіберзлочинністю підкреслює той факт, що багато правових і технічних стандартів було погоджено між країнами світу. Глобальна програма кібербезпеки заснована на п'яти основних принципах: правові заходи; технічні й процедурні заходи; організаційні структури; створення потенціалу; міжнародна співпраця [6, с. 68-69]. Україна намагається притримуватись цих принципів. Так, розпорядженням Кабінету Міністрів України «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури» від 19 червня 2019 р. № 518 було затверджено заходи, які визначають організаційно-методологічні, технічні та технологічні умови кіберзахисту об'єктів критичної інфраструктури. Зазначені вимоги розроблені на базі сучасного досвіду провідних країн світу і є усталеною практикою як в ЄС, так і в США, та гармонізовані з вимогами міжнародних стандартів ЄС, НАТО та NIST з питань забезпечення кіберзахисту [7].

Тож можемо підсумувати, що Закон України «Про основні засади здійснення кібербезпеки України» є хорошим початком у боротьбі України за безпечний кіберпростір, проте для ефективної протидії кіберзлочинності лише відомчих ініціатив вже недостатньо. Потрібна централізована координація зусиль для забезпечення злагодженої взаємодії усіх зацікавлених суб'єктів. Можна визначити основні пріоритети розвитку державних структур по боротьбі з кіберзлочинністю такі як: реорганізація та удосконалення законодавчої і нормативно-правової бази; створення єдиного інформаційного простору в

загальній та організація і удосконалення динамічної взаємодії із зарубіжними законодавчими та державними органами. Задля забезпечення безпеки підприємств в умовах карантину та підвищеної шахрайської діяльності можна пропонувати такі заходи: організовувати навчання працівників і клієнтів на тему базової кібербезпеки; перемістити критичну інфраструктуру до хмарних операторів, які пропонують високий рівень безпеки даних; проводити внутрішнє тестування IT-інфраструктури на предмет захисту від хакерів. Отже, тільки доклавши максимальних зусиль, та приділивши увагу усім вищеписаним аспектам можна сподіватись на подальший розвиток законодавства України у сфері кібербезпеки та забезпечення інформаційного захисту громадян та бізнесу.

Список використаної літератури:

1. Morgan S. Global Cybercrime Damages Predicted To Reach \$6 Trillion Annually By 2021. URL: <https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/> (Last accessed: 11.05.2020)
2. Про внесення змін до деяких законодавчих актів України, спрямованих на запобігання виникненню і поширенню коронавірусної хвороби (COVID-19): Закон України від 17 березня 2020 р. № 530-IX. URL: <https://zakon.rada.gov.ua/laws/show/530-20> (дата звернення: 11.05.2020)
3. Тенденції поширення Інтернет-загроз: як змінилася динаміка під час пандемії. [Київ, 30 квітня 2020 р.] URL: <https://eset.ua/ua/news/view/789/tendentsii-rasprostraneniya-internet-ugroz-kak-izmenilas-dinamika-vo-vremya-pandemii> (дата звернення: 11.05.2020)
4. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 р. № 2163-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2163-19> (дата звернення: 11.05.2020)
5. Литвин А. Що дасть Україні новий закон про кібербезпеку URL: https://biz.censor.net.ua/columns/3069149/scho_dast_ukran_noviyi_zakon_pro_kberbezpeku (дата звернення: 11.05.2020)
6. Швець Д. В. Державні механізми боротьби з кіберзлочинністю. Актуальні питання протидії кіберзлочинності та торгівлі людьми: зб. матеріалів Всеукраїнської наук.-практ. конф. (15 листоп. 2017 р., м. Харків). Харків: ХНУВС, 2017. С. 68–70. URL: http://univd.edu.ua/general/publishing/konf/15_11_2017/pdf/22.pdf (дата звернення: 11.05.2020)
7. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури: Постанова Кабінету Міністрів України від 19 червня 2019 р. №

518. URL: <https://www.kmu.gov.ua/npas/pro-zatverdzhennya-zagalnih-vimog-do-kiberzahistu-obyektiv-kritichnoyi-infrastrukturi-i190619> (дата звернення: 11.05.2020)

Хиленко В. В.,

студентка 3-го курсу ІПСА КПІ ім. Ігоря
Сікорського, l.khylenko@gmail.com

Науковий керівник: Іщенко В. В., викладач
кафедри публічного права КПІ ім. Ігоря
Сікорського

ІНТЕРНЕТ-ШАХРАЙСТВО ТА ЙОГО ВИДИ

В сучасну епоху практично кожна людина користується послугами в Інтернеті. На жаль, розвиток інформаційних технологій призводить до збільшення випадків шахрайства через Інтернет. За результатами дослідження 2018 р., до п'ятірки найбільш поширених видів економічних злочинів та шахрайства входять: незаконне привласнення майна, шахрайство у сфері закупівель, шахрайство у сфері управління персоналом та кіберзлочини, серед яких доля кіберзлочинності та інтернет-шахрайства становить 31% [1]. Через карантин на 15% зріс рівень шахрайства в Інтернеті [2]. Зокрема, онлайн-шахраї намагаються організувати фальшивий продаж ліків від COVID-19, засобів захисту та інші.

До поняття «інтернет-шахрайство» відноситься будь-який тип шахрайства, який використовує електронну пошту, веб-сайти, чати або дошки оголошень для проведення шахрайських операцій або для передачі доходів від шахраїв фінансовим установам пов'язаних зі схемою. Інтернет-шахрайство може включати шпигунське програмне забезпечення, крадіжку особистих даних, фішинг або шахрайство в сфері Інтернет-банкінгу [3]. Інтернет-шахрайство є підвидом звичайного шахрайства, визначення якого є в ч. 1 ст. 190

Кримінального Кодексу України, а саме «заволодіння чужим майном за допомогою введення в оману або зловживання довірою іншої людини» [4].

Шпигунське програмне забезпечення, як правило, вважається програмне забезпечення, яке таємно встановлюється на комп'ютер і виконує певні дії без дозволу користувача. Шпигунське програмне забезпечення може знаходити та забирати особисту інформацію та таємно передавати її комусь іншому. Крім того, зловмисники також можуть дізнатись, які персональні веб-сайти відвідуються, та інші конфіденційні дані (такі, як номер кредитної карти, PIN-коди та ін.). Шпигунське програмне забезпечення дуже сильно знижує продуктивність комп'ютера.

Значна частина злочинів в Інтернеті зараз зосереджена на крадіжках особистих даних, що є частиною крадіжки ідентифікації особистості, і стосується крадіжки та використання особистих ідентифікаційних даних фактичної особи, на відміну від використання фіктивного посвідчення особи. Сюди можна віднести крадіжку та використання особистих даних людей, що живуть чи померли. Ця проблема стає з кожним роком все більш і більш актуальною. Так, наприклад, згідно зі звітом Identity Theft Resource Center, кількість крадіжок в США, виявлених у 2019 р., збільшилася на 17 відсотків від загальної кількості порушень у 2018 р. [5].

Фішинг – це найпопулярніший метод шахрайства в Інтернет-просторі, який використовується для злому паролів і крадіжки конфіденційної інформації, таких як платіжні дані кредитної картки, банківські ім'я користувача і пароль, дані з особистих сторінок користувача, доступ до банківських рахунків, фінансова інформація і т.д. З метою заволодіння вашою інформацією шахраї йдуть на різні хитрощі: виконують масову розсилку електронних листів (спам), а також іменних повідомлень від фінансових і державних установ, соціальних мереж, створюють фішингові сайти, завантажувальні сторінки, спливаючі вікна і т.д.

Шахрайство у сфері інтернет-банкінгу – це шахрайство або крадіжка, вчинених за допомогою онлайн-технології з ціллю незаконного вилучення грошей з банківського рахунку та/або перерахування грошей на рахунок в іншому банку. Шахрайство у сфері інтернет-банкінгу – це форма крадіжки особистих даних, яка зазвичай стає можливою завдяки таким методам, як фішинг. За 2019 р. сума збитків від незаконних дій із платіжними картками становила 0,0042% від загального обсягу всіх операцій із платіжними картками. Найбільша кількість незаконних дій із платіжними картками в 2019 році відбувалась у мережі Інтернет – 41,4 тис. випадків (58% від загальної кількості) [6].

Інтернет-шахрайство тягне в Україні за собою кримінальне покарання. Так, згідно ч. 3 ст. 190 Кримінального кодексу України шахрайство, вчинене шляхом незаконних операцій з використанням електронно-обчислювальної техніки, карається позбавленням волі на строк від трьох до восьми років [4]. Якщо гроші були переведені шахраєві через платіжну онлайнсистему, то варто звернутися в службу підтримки банку чи цієї платіжної системи. Є ймовірність, що після цього рахунок шахрая заблокують.

Так як проблема інтернет-шахрайства поширюється з кожним роком все більше і більше, Україні необхідно замислитись про подальші перспективи розвитку належного рівня безпеки та протидії інтернет-шахрайству. Так, в Україні з 2015 р. вже існує Кіберполіція, завданням якої є виявлення злочинів в Інтернет-просторі, серед яких інтернет-шахрайство. Враховуючи швидкий розвиток інформаційних технологій, також необхідно ставити перед розробниками програмного забезпечення, службами, які займаються інформаційною безпекою, і іншими структурами питання про запобігання можливостей для шахрайських дій в Інтернеті.

Список використаної літератури:

1. Всесвітнє дослідження економічних злочинів та шахрайства 2018 року: результати опитування українських організацій. URL: <https://www.pwc.com/ua/uk/survey/2018/pwc-gecs-2018-ukr.pdf> (дата звернення: 11.05.2020).
2. Продовження та пом'якшення карантину обговорили на нараді в Офісі Президента. URL: <https://www.president.gov.ua/news/prodovzhennya-ta-pomyaks-hennya-karantinu-obgovorili-na-narad-60757> (дата звернення: 11.05.2020).
3. Internet fraud. URL: <https://police.act.gov.au/sites/default/files/PDF/bizsafe-internet-fraud-factsheet.pdf> (Last accessed: 11.05.2020)
4. Кримінальний кодекс України від 5 квітня 2001 р. № 2341-III. URL: <https://zakon.rada.gov.ua/laws/show/2341-14> (дата звернення: 11.05.2020).
5. 2019 Data Breaches. URL: <https://www.idtheftcenter.org/2019-data-breaches/> (Last accessed: 11.05.2020)
6. Збитки від незаконних дій із платіжними картками зменшилися більше ніж удвічі. URL: <https://bank.gov.ua/news/all/zbitki-vid-nezakonnih-diy-iz-platijnimi-kartkami-zmenshilisya-bilshe-nij-udvichi> (дата звернення: 11.05.2020).

Пивовар П. Є.,

студент 3-го курсу ПІСА КПІ ім.
Ігоря Сікорського

Науковий керівник: Іщенко В. В.,

викладач кафедри публічного права
КПІ ім. Ігоря Сікорського

Е-РЕЗИДЕНТ: ДОСВІД ЕСТОНІЇ ТА ПЕРСПЕКТИВИ ЗАПРОВАДЖЕННЯ В УКРАЇНІ

Сьогодні, в умовах пандемії COVID-19 в світі різко зросла потреба у впровадженні дистанційної роботи. На період карантину аеропорти закриті, громадський транспорт не працює, навіть пересування між містами обмежене. Проте, ділове життя будь-якої з держав світу на цьому не закінчується. Суб'єкти підприємницької діяльності (далі – СПД) продовжують управляти своїм бізнесом, проте не так, як раніше. Онлайн-управління за допомогою електронних пристроїв та сервісів у мережі Інтернет стає чи не єдиним способом тримати свій бізнес на плаву. Варто пам'ятати, що бізнес – це не лише

управління командою, збір прибутків та створення бізнес-моделі, але й велика кількість правових аспектів (державна реєстрація, отримання ліцензій та дозволів, сплата податків, судові процеси тощо). Тож під час карантину постає проблема того, як здійснювати СПД свої обов'язки перед державою повністю електронно.

Чудовим прикладом реалізації даної ідеї є концепція е-резидента (електронного резидента) в Естонії. За офіційним визначенням на державному порталі Естонії е-резидентом є іноземець, якому на підставі ідентичності держави громадянської належності Естонія надала можливість створення електронно-цифрової ідентичності й видала електронно-цифрове посвідчення особи – діджитал-ID (з англ. digital ID) е-резидента [1]. У такий спосіб, громадяни іноземної держави отримують захищений доступ до електронних послуг Естонії. З діджитал картою е-резидента можна підписувати документи цифровим підписом і входити у всі портали та інфосистеми, які признають ID карту Естонії. Е-резидент може через інтернет засновувати в Естонії комерційне об'єднання і брати активну участь у його управлінні, проживаючи при цьому в іншій державі. Е-резидентство спрощує діловодство також для СПД, що вже інвестували в Естонію і створили тут підприємство. У СПД, зареєстрованих за межами Європейського союзу, завдяки е-резидентству з'являється зручна можливість заснувати в Естонії підприємство й таким чином організувати діловодство в Європейському союзі [1].

За словами керівника зі зв'язків із громадськістю програми e-Residency Арно Касьяна: «У грудні 2017 року Deloitte опублікувала звіт, згідно з яким за три роки програма принесла Естонії 14,5 млн євро у вигляді прямих і непрямих податків. З цієї суми 1,5 млн євро — це прямі податки. Решта 13 млн євро – це непрямі податки, зібрані державою в результаті зростлого попиту на послуги у сфері податкових і юридичних консультацій, додаткових послуг, пов'язаних із веденням бізнесу. Deloitte прогнозує, що до 2025 року загальні доходи Естонії

від діяльності учасників програми складуть до 1,5 млрд євро. Тому в Естонії головним завданням вважають створення зв'язків між бізнесом, створеним «електронними резидентами», й естонським бізнесом» [2].

Як можна побачити на офіційному порталі програми е-резидентства Естонії Україна посідає третє місце за кількістю учасників програми поступаючись лише РФ та Фінляндії, а щодо кількості зареєстрованих компаній – Україна посідає перше місце в цьому списку. Постає природне питання: «Чому українські СПД створюють бізнес в Естонії?»[3].

На думку керівника із розвитку зовнішніх ринків програми естонського уряду e-Residency Олексія Воронкова: «Українці приєднуються до програми, оскільки вона спрощує вихід компаній на міжнародний ринок. Реєстрація бізнесу займає 15 хвилин, пройти її можна зі смартфона, з нього ж вдасться вести бізнес і далі» [4]. Арно Касьян з цього приводу додає: «Однак у першу чергу вони (українці) використовують електронне резидентство Естонії, щоби полегшити свої відносини з ринками європейських країн, спростити бюрократичні процедури та розширити бізнес.» [2].

Отже, з досвіду е-резидентства в Естонії, можна констатувати наступне.

По-перше, українські СПД потребують спрощення процедури створення та управління бізнесом на території України.

По-друге, запровадження подібної програми в Україні може мати позитивний ефект на економіку держави. Наразі, варто дізнатись чи були запропоновані подібні ініціативи урядом України.

14 січня 2020 р. Міністерство цифрової трансформації (Мінцифра) України анонсувало про план створення е-резидентства в Україні. Як зазначено на офіційному сайті міністерства, попередньо первинною цільовою аудиторією українського е-резидентства визначили п'ять країн, що є основними постачальниками ІТ-послуг на аутсорсі: Індія, Бангладеш, Пакистан, Китай та

Філіппіни. Серед того, що Україна може запропонувати іноземцям Мінцифра перераховує:

- Привабливі податки та уникнення подвійного оподаткування;
- Відсутність бюрократичної тяганини;
- Просту і зручну платформу для провадження бізнесу з доступом до всіх необхідних послуг та можливістю здійснення правочинів онлайн із застосуванням безпечного ключа електронного підпису, сертифікованого в Україні;
- Персональну консультаційну підтримку;
- Англomовний сервіс підтримки;

Перевагами для України мають бути наповнення державного бюджету внаслідок оподаткування е-резидентів і оплати послуги щодо надання статусу е-резидентства та можливість покращити національний імідж на міжнародному ринку ІТ [5].

Важливою передумовою до створення будь-якої з е-послуг в Естонії було створення надійної системи кіберзахисту держави. Відповідно до Національного індексу кібербезпеки (NSCI) наразі Естонія посідає третє місце, Україна ж посідає двадцять дев'яте місце. Як видно Естонія є одним із лідерів у кібербезпеці. Персональні дані, які надають громадяни для користування е-послугами є скарбом для кіберзлочинців, тому захист інформації є обов'язковим. [6]

Таким чином, з прикладу Естонії видно, що напрям е-резидентства є перспективним та може сприяти економічному розвитку держави. Проте, варто зауважити, що для України наразі необхідно створити міцну законодавчу базу, що чітко та ефективно і водночас без зайвої бюрократії, регулювала відносини е-резидента з державою, таким чином забезпечити сприятливі умови для іноземних інвесторів. Водночас Україні слід підняти вище у рейтингу NSCI для того, щоб діджиталізація не супроводжувала кібер-криміналізацію.

Нарешті, слід зауважити, що сприятливі умови повинні бути створені не тільки для іноземців, а і для українських СПД, для того, щоби їм не потрібно було ставати е-резидентами інших держав.

Список використаної літератури:

1. Э-резидентство. URL: <https://www.eesti.ee/ru/predprinimatel/erezidentstvo/> (дата звернення: 14.05.2020).

2. Некрасов В. В погоне за PayPal: почему тысячи украинцев стали «электронными гражданами» Эстонии. URL: <https://www.epravda.com.ua/rus/publications/2018/10/3/641242> (дата звернення: 14.05.2020).

3. Total number of e-residents. URL: <https://e-resident.gov.ee/dashboard/> (дата звернення: 14.05.2020).

4. Скільки компаній українці відкрили в Естонії. URL: <https://nv.ua/ukr/biz/economics/chomu-ukrajinci-vidkrivayut-noviy-biznes-v-estoniji-50031168.html> (дата звернення: 14.05.2020).

5. Українське е-резидентство: навіщо це нам та світу. URL: <https://thedigital.gov.ua/news/ukrainske-e-rezidenstvo-navishcho-tse-nam-ta-svitu> (дата звернення: 14.05.2020).

6. National Cyber Security Index. URL: <https://ncsi.ega.ee/ncsi-index/> (дата звернення: 14.05.2020).

Пономарьов К. С.,

студент факультету соціології і права, КПП
ім. Ігоря Сікорського

Науковий керівник: Солончук І. В., ст.

викладач кафедри інформаційного права та
права інтелектуальної власності КПП ім.

Ігоря Сікорського

**ПРАКТИЧНІ РИЗИКИ ПРИ РЕФОРМУВАННІ НАЦІОНАЛЬНИХ
ОРГАНІВ КОНТРОЛЮ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ
ВІДПОВІДНО ДО ПОЛОЖЕНЬ ЗАГАЛЬНОГО РЕГЛАМЕНТУ ЗАХИСТУ
ПЕРСОНАЛЬНИХ ДАНИХ ЄВРОПЕЙСЬКОГО СОЮЗУ (GDPR)**

GDPR або Загальний регламент захисту персональних даних – найважливіший законодавчий документ ЄС у сфері інформаційного права, який суттєво підвищує рівень захисту персональних даних в ЄС та за його межами.

Навіть до початку дії регламенту у травні 2018 року, його правові положення та правила їх імплементації стали однією з найгостріших правових тем, навколо якої ведуться спори як в юридичних колах, так і серед представників сфер бізнесу, пов'язаних зі збиранням та обробкою персональних даних.

Не дивлячись на неймовірну актуальність проблем щодо захисту конфіденційності та негайну потребу в прозорості та підзвітності для процесів збирання та обробки персональних даних, регламент GDPR, який від самого початку позиціонувався як ясний і зрозумілий звіт правил та послідовно розроблений та чіткий механізм регулювання, виявився набагато більш проблемним та складним у реалізації, ніж передбачає його амбітна концепція.

Розширюючи поняття “персональні дані” в контексті можливих ідентифікаторів та інформації, встановлюючи нові всеосяжні рамки для таких понять, як процесор інформації, контролер інформації, суб'єкт даних, обробка, профілювання, портативність даних, система подачі даних, транскордонна обробка, вводячи такі концепції прав як "право бути забутим", "право на мобільність даних", "право на зрозумілу та доступну інформацію", "право заборони використання автоматизованих рішень, заснованих на профілюванні щодо себе", "право отримувати інформацію про порушення правил безпеки зберігання даних", та, найголовніше, розроблюючи реальні та дієві важелі впливу на контролерів та процесорів інформації, тобто тих, хто збирає та застосовує персональну інформацію користувачів у своїй діяльності, GDPR створює нові напрямки діяльності в індустрії захисту персональних даних. В умовах сучасної економіки та переорієнтації великої кількості економічних та соціальних процесів в онлайн сферу, а також всеосяжного проникнення інформаційних технологій обробки та збирання даних в ці сфери, тема відповідності положенням GDPR стає неабияк актуальною для контролерів та процесорів персональних даних в Україні, які є резидентами України та орієнтуються на ринок Європейського Союзу.

Але паралельно з розвитком нової сфери застосування законодавства виникає не тільки потреба у відповідності певним нормам законодавства, але й необхідність в ефективному контролі дотримання нових нормативно-правових положень. Особливо дана проблема важлива у контексті послідовної Євроінтеграції України та адаптації українського законодавства щодо захисту персональних даних до законодавства ЄС та відповідного регламенту GDPR. І якщо на даному етапі Україна лише починає рухатися у напрямку гармонізації законодавства та робить перші кроки на шляху створення нових та зміни існуючих механізмів, країни-члени ЄС пройшли цей шлях та реформували відповідні національні органи контролю. Тут варто згадати, що GDPR представляє з себе регламент, а не директиву ЄС, що означає, що він не вимагає гармонізації законодавства та прийняття відповідних законів від національних урядів країн-членів, та має пряму та безпосередню дію на бізнес.

Важливим в цих умовах є звернення уваги українських законотворців та юристів на ті проблеми, з якими стикаються Європейські країни під час здійснення контролю за дотриманням положень GDPR, а не тільки на проблеми гармонізації вітчизняного законодавства та регламенту GDPR. Використовуючи результати досліджень та наукові роботи Європейських та вітчизняних правників та спеціалістів у сфері захисту персональних даних, можна ефективно прослідити та окреслити ті ризики, які виникають під час здійснення контролю.

В першу чергу, при окресленні організаційних ризиків державного регулювання, необхідним буде дати відповідь на питання щодо тих основних положень GDPR, які регламентують правові аспекти організації наглядових органів моніторингу та контролю. Також, задля формування конкретних практичних порад щодо запобігання виявлених ризиків у процесі регуляції, важливим є характеристика вже існуючих публічних органів в Україні, спрямованих на захист персональних даних.

GDPR загалом є масивним документом, який складається з 173 пунктів Преамбули та 99 статей, які поділяються на 11 глав та секції всередині цих глав. Основні положення GDPR, що стосуються організації роботи державних регуляторів, викладені у главі 6, яка регламентує положення щодо незалежного статусу публічного контролюючого органу (Supervisory Authority), загальні умови заснування та функціонування таких органів, їх компетенцію, завдання, повноваження, а також зобов'язання щорічного звітування національних органів перед національним парламентом, урядом, та іншими законодавчо обумовленими органами. Виходячи з положень Секції 1 глави 6 кожна держава-учасник зобов'язується створити незалежний контролюючий орган, на якого покладалася б відповідальність слідкувати за дотриманням положень, закріплених GDPR, приймати скарги від громадян щодо порушення їх прав, та застосовувати санкції проти порушників регламенту [1]. Загалом, кожна країна ЄС має власний державний регулятор, який повинен відповідати вищевикладеним принципам GDPR. Такі органи мають загальну назву Уповноважених органів контролю захисту персональних даних (*Data Protection Authority*, або *DPA*), та грають вирішальну роль як контролюючі органи, мета яких полягає у безперервному контролі дотримання контролерами та процесорами застосованих до них положень регламенту в межах кордонів відповідних країн. Також статтею 51 глави 6 GDPR визначається можливість створення регіональних органів контролю захисту персональних даних (*Regional Supervisory Authority*) [2]. Дана можливість була створена для тих країн членів, які мають федеративний устрій та складаються з відповідних автономних регіонів, кожний з яких має свій власний орган, відповідальний за захист персональних даних, задля можливості представлення сукупності цих органів в Європейській Раді з захисту даних. Єдиною країною ЄС, що створила такий регіональний орган, є Німеччина [3].

Кожний Уповноважений національний та регіональний орган контролю має звітувати перед Європейською Радою з захисту даних (*European Data Protection Board*), яка є новоствореним наддержавним органом ЄС, завданням якого є нагляд за забезпеченням застосування регламенту GDPR у рівній мірі серед усіх країн-членів та координування діяльності національних та регіональних органів контролю. Європейська Рада з захисту даних замінила Робочу групу із захисту персональних даних 29 (*Article 29 Working Party*) як основний незалежний консультуючий та наглядовий орган ЄС, який розглядає запити та заперечення національних органів контролю, видає настанови і рекомендації щодо належної імплементації положень GDPR, зокрема щодо належного обміну інформацією та практичного досвіду, та заохочує ефективну співпрацю між відповідними органами. Європейська Рада складається з представників або голів відповідних національних наглядових органів та Європейського інспектора із захисту даних (*European Data Protection Supervisor*, або *EDPS*), який представляє собою незалежний наглядовий орган ЄС, створений 2001 року в рамках Договору про заснування Європейської Спільноти, який має забезпечувати дотримання прав на приватність та захист персональних даних громадян ЄС у межах роботи установ та інституцій ЄС.

Принципи співпраці між національними агенціями на Європейською Радою з захисту даних регламентовані статтями, викладеними у главі 7 регламенту GDPR. Також Секцією 3 цієї глави встановлено структуру, основні принципи функціонування, повноваження та завдання Європейської ради з захисту даних [2].

Головною законодавчою інституцією, яка пропонує та створює закони, що стосуються захисту персональних даних у рамках ЄС, є Європейська комісія – вищий орган виконавчої влади Європейського Союзу, який є відповідальним за загальну законодавчу політику ЄС, розроблення загальних для країн учасниць законодавчих правил та положень, та має законодавчу ініціативу у межах ЄС.

Описавши організаційну структуру органів, які призначені слідкувати за дотриманням правил GDPR у межах ЄС та Європейської економічної зони, для кращого розуміння перспектив реформування вітчизняних органів та тих ризиків, які стоять за цим процесом, важливим буде також визначення вже існуючої організаційної структури відповідних органів в Україні.

Основним законом, який регламентує структуру державних наглядових органів з захисту персональних даних в Україні, є Закон України "Про захист персональних даних", який, крім того, є головним актом національного законодавства у сфері захисту персональних даних. Згідно цього закону, основні повноваження за здійсненням контролю дотримання законодавства України про захист персональних даних покладено на Уповноваженого Верховної Ради України з прав людини [4]. Для забезпечення виконання Уповноваженим своїх функцій у структурі секретаріату був створений та функціонує Департамент у сфері захисту персональних даних. Цей окремий структурний підрозділ, у свою чергу, підрозділяється на менші структурні підрозділи, а саме – чотири відділи (Відділ нормативно-правового забезпечення; Відділ розгляду звернень; Відділ перевірок; Відділ взаємодії із суб'єктами обробки персональних даних) та Сектор упровадження міжнародних стандартів у сфері захисту персональних даних [5]. Основні функції Департаменту у сфері захисту персональних даних - здійснення контролю та моніторингу за виконанням законодавства у сфері захисту персональних даних, здійснення перевірок власників персональних даних, прийняття скарг від громадян, чий права були порушені, та проведення заходів щодо поновлення їх порушених прав. Також у компетенцію даного департаменту входить забезпечення виконання міжнародних зобов'язань України щодо імплементації міжнародних правових норм та стандартів, зокрема законодавства Європейського Союзу, у сфері захисту персональних даних, а також здійснення нормативно-правового забезпечення у сфері захисту персональних даних, у тому числі організації

проектування нормативно-правових актів, їх опрацюванні, та проведенні юридичної експертизи. Основні положення про Департамент захисту персональних даних затверджуються Уповноваженим Верховної Ради України з прав людини, та визначають загальні положення функціонування департаменту, його основні завдання, функції та права [5]. Щодо самого Уповноваженого, його повноваження регламентуються статтею 23 ЗУ "Про захист персональних даних" [4].

Також, окрім Уповноваженого, контроль за дотриманням законодавства про захист персональних даних здійснюють суди України, що визначається статтею 22 ЗУ "Про захист персональних даних" [4]. Відповідно до пунктів 8 та 9 частини другої статті 8 ЗУ "Про захист персональних даних", суб'єкт персональних даних має право використовувати відповідні засоби правового захисту та звертатися до суду в разі порушення їх прав про захист персональних даних [4].

Розібравшись з організаційними структурами органів захисту персональних даних України та Європейського Союзу, важливим кроком буде дослідження тих проблем, які виникають у національних та європейських регуляторів у процесі контролю за захистом персональних даних. Звернення уваги на ті ризики, які несуть у собі реформи існуючих механізмів контролю, має велике значення при окресленні того шляху, яким буде рухатися Україна при гармонізації власного законодавства та організації органів контролю у процесі Євроінтеграції. Дана необхідність була досліджена в наукових працях таких вітчизняних правників, як О. В. Гронь, А. К. Погорелко, Я. О. Овчаренко, В. Г. Пилипчук, В. М. Брижко, та інших.

Загалом, серед основних та невідкладних практичних кроків реформування органів контролю можна визначити декілька найбільш важливих.

По перше, це необхідність розмежування та розподілу функцій, які в даний час належать Уповноваженому Уповноваженим Верховної Ради України з прав

людини. Пропонується створити нові органи контролю у межах Міністерства Юстиції та перекласти на них ту частину завдань Уповноваженого, яка торкається сфер здійснення контролю та моніторингу за виконанням законодавства у сфері захисту персональних даних, здійснення перевірок власників персональних даних, прийняття скарг від громадян, та проведення заходів щодо поновлення їх порушених прав. Уповноваженому при цьому пропонується залишити функції здійснення нормативно-правового забезпечення, проектування, опрацювання та експертної оцінки нормативно-правових актів, а також функції взаємодії з уповноваженими органами ЄС у сфері захисту персональних даних, у тому числі щодо питань виконання міжнародних зобов'язань України щодо імплементації міжнародних правових норм та стандартів [6, с.238; 7, с. 18].

Також пропонується віднесення правопорушень, які стосуються захисту персональних даних громадян, до компетенції ДБР, для більш якісного запобігання та розслідування даної категорії правопорушень, а також покладання на Національну поліцію України функції сприяння у проведенні перевірок та розслідування правопорушень у цій сфері [6, с.238; 7, с. 18].

Головним питанням, яке постає при аналізі потреби України у впровадженні викладених дій при розробці ефективного механізму захисту персональних даних, є визначення тих ризиків, які так чи інакше впливали б на ефективність та державного регулювання. На даний час ця проблема слабо окреслена у вітчизняних наукових дослідженнях. Більшою мірою увага приділяється нормативно-правовим ризикам та можливим шляхам реформування законодавчої бази. Між тим, останні дослідження показують наявність широкого кола проблем у національних та регіональних органів контролю серед країн ЄС та Європейської економічної зони [3]. Дані, отримані у процесі дослідження, сигналізують неспроможність національних регуляторів ефективно контролювати дотримання регламенту GDPR, через причини, які

беззаперечно будуть проявлятися пізніше і в українських реаліях, якщо не буде вчасно вжито дієвих превентивних заходів.

Основним відкриттям дослідження стало те, що навіть після двох років з моменту прийняття регламенту країни-члени не мають можливості задовольнити ті вимоги GDPR, які торкаються створення та функціонування національних наглядових органів. Автори дослідження наголошують на неефективності роботи цих органів та відсутності штрафів для компаній-технологічних гігантів (*Big Tech companies*), таких як Google LLC та Facebook Corp., незважаючи на велику кількість скарг на ці компанії. Показовим є приклад Ірландії, де національний регулятор "Irish Data Protection Commission", який несе основну відповідальність за дотримання цими компаніями положень GDPR з причини масової реєстрації технологічних гігантів у цій країні, не виграв жодного судового провадження проти цих компаній [3]. Дослідження, проаналізувавши великий масив даних, які було взято з опублікованих національними наглядовими органами та Європейською Радою з захисту даних звітів, знаходить дві основні причини неефективності національних агенцій, які є результатом недотримання урядами країн-членів вимог GDPR, викладених у статті 52 глави 6 регламенту - забезпечення наглядового органу людськими та фінансовими ресурсами.

Незабезпеченість регуляторів фінансовими ресурсами має неабияке значення для фінансових регуляторів не тільки у світі забезпечення їх діяльності та інфраструктури, але, що набагато головніше, у світі необхідності витратити ресурси на судові баталії з гігантами індустрії, через наявність в останніх майже необмежених фінансових та людських ресурсів. У той час, як дохід компаній-технологічних гігантів перевищує сотні мільярдів доларів на рік, загальний річний бюджет усіх 45 європейських органів контролю захисту персональних даних у приватному секторі не перевищує третини мільярда Євро (€325,896,343), при тому що більше ніж половина регуляторів має річні

бюджети менше, ніж 5 мільйонів Євро, а три країни мають бюджети менше ніж 1 мільйон Євро[3]. Важливо при цьому звернути увагу на те, що, не дивлячись на об'єктивну необхідність багатократного збільшення бюджетів регуляторів, у 2020 загальний бюджет для всіх європейських регуляторів підвищиться лише на 15%, на противагу збільшенню у 24% у 2019. Варто додати, що збільшення бюджетів не відбувається у всіх країнах, а у деяких, таких як Португалія та Естонія, навіть зменшується. Відносний приріст бюджетів в першу чергу відбувається за рахунок підвищення фінансування національного органу контролю Великої Британії (*Information Commissioner's Office*, або *ICO*), та німецьких федеральних органів контролю, на противагу незначному підвищенню річних бюджетів більшості країн-членів.

Ще однією проблемою, яка висвітлюється дослідженням, є те, що в європейських наглядових органах рішуче не вистачає технічних фахівців. Недостатня кількість фахівців такого профілю є наріжною проблемою через те, що такі фахівці вкрай необхідні для того, щоб проводити глибокі розслідування, на підставі яких можна будувати сильні і обґрунтовані судові прецеденти без страху того, що їх апелюють і ресурси будуть витрачені даремно[3].

Дослідження проблеми виявило, що майже усі країни, за винятком Німеччини, відчувають істотну нестачу в технічних спеціалістах. Загальна кількість технічних спеціалістів, працевлаштованих у національних органах контролю ЄС, сягає планки у 305 працівника, але при цьому майже третина (29%), або 101 спеціаліст (з урахування вільних вакансій), приходяться на федеральні та регіональні органи контролю. На фоні досягнень Німеччини рівно половина усіх національних агенцій має у своїй команді менше ніж 5 технічних спеціалістів показує, при цьому 7 країн ЄС мають у команді менше двох технічних спеціалістів [3]. Дана статистика показує, що, не зважаючи на крайню необхідність проведення технічних розслідувань проти процесорів та контролерів даних, їх працевлаштування не є пріоритетом для більшості

національних регуляторів. Апелюючи до проаналізованих даних, дослідники роблять висновок щодо необхідності збільшення фінансування таких регуляторів, для створення нових можливостей ефективного контролю дотримання регламенту GDPR. Допоки цього не буде зроблено можна зробити висновок про неспроможність країн-членів забезпечити свої контролюючі органи необхідними фінансовими та людськими ресурсами, що сигналізує про порушення більшою частиною країн-членів своїх зобов'язань, визначених у статті 52 глави 6 регламенту GDPR.

На основі вищевикладених даних, важливим є взяття до уваги тих проблем, з якими стикнулися національні та регіональні європейські контролюючі органи. Превентивні заходи, які допоможуть зробити ефективним механізм здійснення контролю, допоможуть українському уряду в імplementації зобов'язань з захисту приватності та персональних даних громадян, взятих на себе при підписанні Угоди про асоціацію України з ЄС та інших міжнародних договорів. Особливо важливим вирішення цієї проблеми є у світі нестачі не тільки технічних спеціалістів, але й взагалі працівників в Департаменті захисту персональних даних Уповноваженого Верховної Ради України з прав людини. На липень 2018 року, за кілька місяців після вступу у силу регламенту GDPR, загальна кількість працівників Департаменту сягала лише 39 осіб [8]. У найближчих по кількості населення до України Європейських країни, Іспанії та Польщі, на 2019 рік кількість працівників у відповідних органах контролю сягала 155 и 224 відповідно, що значно більше, ніж в Україні [3]. Загалом, важливим також є подальше вивчення тих організаційних ризиків, з якими стикнулися європейські національні органи контролю за час своєї діяльності. Крім того, важливим є подальше висвітлення тих практичних кроків урядів країн-членів, які будуть направлені на збільшення ефективності моніторингу та контролю контролерів та процесорів даних суб'єктів ЄС. Слід враховувати, що перспективність нових стратегій розбудови ефективного та дієвого

національного механізму захисту персональних даних громадян України залежить від здатності вчитися на помилках інших, що зумовлює необхідність всебічного аналізу європейської практики вітчизняними правниками.

Список використаної літератури:

1. D. Savic, M. Veinovic. Challenges of General Data Protection Regulation (GDPR), in *Sinteza 2018/ International Scientific Conference on Information Technology and Data Related Research*, Belgrade, Singidunum University, Serbia, 2018, pp. 23-30. Sinteza-2018-23-30 / p. 25.

2. EU General Data Protection Regulation (GDPR). URL: <http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf>. (дата звернення: 20.05.2020).

3. Dr. Johnny Ryan. Europe's governments are failing the GDPR: Brave report on the enforcement capacity of data protection authorities to enforce against tech infringements of the GDPR. *Brave Insights, Policy, Press, Research*. 2020. URL: <https://brave.com/wp-content/uploads/2020/04/Brave-2020-DPA-Report.pdf> (дата звернення 20.05.2020).

4. Про захист персональних даних: Закон України від 1 червня 2010 року №2297-VI (зі змінами та доповненнями). URL: <http://zakon3.rada.gov.ua/laws/show/2297-17> (дата звернення: 20.05.2020).

5. Уповноважений Верховної Ради з прав людини. URL: <http://www.ombudsman.gov.ua/ua/page/zpd/info/> (дата звернення : 20.05.2020).

6. Овчаренко Я. О. Регламент захисту персональних даних Європейського Союзу (GDPR) та можливості його застосування на території України. *Юридичний науковий електронний журнал*. 2018. №3. С. 236-239.

7. Пилипчук В. Г. Брижко В. М. Реформування і розвиток системи захисту персональних даних в Україні. *Інформація і право*. 2018. № 3(22). С. 5 - 21.

8. Структура Секретаріату Уповноваженого Верховної Ради України з прав людини: Додаток до наказу уповноваженого з прав людини від 3 липня 2018 № 355/к. URL: <https://dostup.pravda.com.ua/request/39114/response/85610/attach/3/03.07.18.pdf> (дата звернення: 20.05.2020).

Александрова А.,
студентка факультету соціології і права, КПП
ім. Ігоря Сікорського
Науковий керівник: Солончук І. В.,
ст. викладач кафедри інформаційного права
та права інтелектуальної власності КПП імені
Ігоря Сікорського

ПРОБЛЕМИ ЗАХИСТУ ІНФОРМАЦІЙНОЇ ПРИВАТНОСТІ ТА ПЕРСОНАЛЬНИХ ДАНИХ

Проблема захисту інформаційної приватності та персональних даних громадян набула розповсюдження з того часу, коли стрімко почали розвиватися інформаційні технології. Якщо раніше доступ до інформації могли отримати виключно юридичні особи, спеціалізовані організації, то сьогодні це може зробити майже кожна людина.

Актуальність даної теми полягає у тому, що на сьогоднішній день розвиток інформаційних технологій є досить швидким, а механізми захисту інформаційної приватності та персональних даних громадян значно відстають. Інтернет став універсальним способом і засобом зберігання інформації. Процес обміну даними став набагато простішим, швидшим та, в багатьох випадках, безкоштовним. Але чи є він настільки безпечним? Наразі, кожна особа, чий дані є в глобальній мережі, може бути під загрозою різноманітних махінацій через використання тих же технологій.

Зі сказаного вище, можемо зробити висновок, що на даному етапі не тільки в Україні, а й в усьому світі постає питання - які заходи потрібно вжити для надання максимального захисту персональних даних.

Статтею 32 Конституції України проголошено право людини на невтручання в її особисте життя. Крім того, не допускається збирання, зберігання, використання поширення конфіденційної інформації про особу без її

згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини [1].

На сьогодні, як зазначається в багатьох наукових дослідженнях, сучасна система захисту прав і безпеки людини в інформаційній сфері є дуже далекою від ідеальної, і залишається дуже хиткою. Саме тому вона потребує максимальної трансформації.

Для початку вважаємо доцільним вазначити, що саме являють собою персональні дані громадян. В українському законодавстві немає чітко визначеного переліку, але у статті 2 Закону України “Про захист персональних даних” зазначено, що персональні дані - це відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована [2]. Цей закон регулює правові відносини, пов’язані із захистом і обробкою персональних даних, і спрямований на захист основоположних прав і свобод людини і громадянина, зокрема права на невтручання в особисте життя у зв’язку з обробкою персональних даних.

Вся інформація про особу поділяється за режимом доступу до неї на наступні види:

- відкрита інформація: таку інформацію ще називають загальнодоступною.

Водночас, особа має право за певних умов обмежувати доступ до такої відкритої інформації за власним бажанням (право на забуття). Ця інформація, незважаючи на її існування, формально не вписується у термінологію на рівні визначень у відповідних профільних інформаційних законах. Саме тому вона має бути офіційно вказана. Для цього потрібно змінити формулювання Законів України «Про інформацію» та «Про доступ до публічної інформації», а також переформулювати норму Закону України «Про захист персональних даних» щодо обробки будь-яких персональних даних на підставі закону або згоди

особи. Такі підстави мають стосуватися лише конфіденційної інформації, а не будь-яких персональних даних (зокрема, відкритої інформації) [4];

- інформація, обмежена у доступі:

а) таємна або службова (відповідно до спеціальних законодавчих актів, що встановлюють правовий режим таємниці і службової інформації);

б) конфіденційна, яка, у свою чергу, поділяється на інформацію, що визначається конфіденційною самою особою (яка не віднесена законом ані до відкритої, ані до чутливої/вразливої. Обробка такої інформації можлива за згоди особи) та вразливу (чутливу) інформацію, щодо якої законодавець може встановлювати обмеження або пряму заборону на її обробку (що не забороняє самій особі добровільно її поширювати) або дозволяти, за умови прямої згоди на обробку з боку особи (проте, за таких умов, визначається особливий підвищений порядок її обробки). Законодавство може встановлювати спеціальні правила обробки чутливої інформації, спрямовані на гарантування конфіденційності або на заборону збирання /обробки певних видів особливо чутливої інформації.

Сміливо можемо стверджувати, що сьогодні інформація - це основа всього, що є довкола нас. І в першу чергу потрібно пам'ятати, що найважливішою інформацією є саме персональна. Щодо цього, звернено багато уваги до випадку з онлайн-кампанією британської консалтингової фірми "Cambridge Analytica", за допомогою якої кандидат у Президенти США Дональд Трамп переміг у виборах у 2016 році. В основі методів роботи фірми був несанкціонований доступ до персональних даних 50 мільйонів користувачів соціальної мережі "Facebook" для визначення політичних симпатій виборців з метою впливу на них через відповідну рекламу та публікації у стрічці новин, які дискредитували Хіларі Клінтон. І випадки, на зразок цього, зустрічаються доволі часто, але ми можемо навіть не помічати цього. Як зазначали Гронь О. В. та Погореленко А. К., дуже важливим в цьому є, з одного боку, узгоджена

робота фахівців із безпеки, до компетенції яких безпосередньо відноситься це питання, а також ІТ-фахівців, які розробляють відповідне програмне забезпечення, обов'язкова опція якого – неможливість попадання персональних даних до сторонніх осіб [5].

Список використаної літератури:

1. Конституція України: Закон України від 28 червня 1996 р. №254к/96-ВР. *Відомості Верховної Ради України*. 1996. № 30. Ст. 141.
2. Про захист персональних даних: Закон України від 1 червня 2010 р. № 2297-VI. *Відомості Верховної Ради України*. 2010. № 34. Ст. 481.
3. Про інформацію: Закон України від 2 жовтня 1992 р. № 2657-XII. *Відомості Верховної Ради України*. 1992. № 48. Ст.650.
4. Кардаш А. В. Конституційно-правовий захист інформації про особу: порівняльно-правовий аспект. Харків, 2019. 228 с.
5. Гронь О. В. Проблеми захисту персональних даних у контексті сучасної комунікації. *Науковий вісник Ужгородського національного університету*. 2018. №19. С. 102–108.

Жакулін Н. В.,

студент 3-го курсу ІПСА КПП ім. Ігоря
Сікорського

Науковий керівник: Іщенко В. В., викладач
кафедри публічного права КПП ім. Ігоря
Сікорського

ПРАВОВЕ РЕГУЛЮВАННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ЗА ЗАКОНОДАВСТВОМ УКРАЇНИ, ЄС ТА США (ПОРІВНЯЛЬНИЙ АНАЛІЗ)

В сучасному світі ми стикаємося з різними видами інформації, зокрема з інформацією, що зберігається в електронному вигляді. Майже в кожного з нас є електронні документи, що можуть представляти деяку цінність, і ми можемо навіть не замислюватися про це. Наприклад, персональні дані, файли з логінами та паролями, робочі файли. Проходячи процедуру реєстрації на сайті, користуючись соціальною мережею чи роблячи покупки в інтернет-магазині, ми змушені передавати інформацію про себе третім особам, що не

завжди приділяють належну увагу захисту даних. За відсутності належного захисту персональних даних, ми ризикуємо тим, що ці дані можуть бути викрадені та протиправно використані. Згідно з даними Harris Poll лише в США у 2017 р. постраждало приблизно 60 мільйонів людей від крадіжки персональних даних[4]. Реальну ж ситуацію в світі оцінити дуже важко.

США є першою в світі державою, що почала контролювати захист персональних даних. 31 грудня 1974 р. був прийнятий «Закон про конфіденційність» (Privacy Act). Цей закон встановлює Кодекс добросовісної інформаційної практики, що регулює збір, технічне обслуговування, використання і поширення особистої інформації про приватних осіб, які підтримуються в системах запису федеральних агентств [3]. Всі установи зобов'язані повідомити публічним повідомленням про свої бази даних і зареєструватися в Федеральному реєстрі; розголошення інформації з баз даних за відсутності письмової згоди суб'єкта інформації є забороненим, окрім одного з дванадцяти статутних винятків. Введений після терористичних актів 11 вересня 2001 р. «Патріотичний акт» (USA Patriot Act) дозволяв передавати владі США дані сервісів, що належать американським компаніям, без повідомлення самих користувачів. Цей акт дозволив американським правоохоронним органам отримати доступ до будь-якої особистої інформації клієнтів американських електронних компаній без повідомлення користувачів [2]. 1 червня 2015 р. термін дії «Патріотичного акту» закінчився. Його змінив «Акт про свободу США» (USA Freedom Act), що забороняє спецслужбам США вести за американськими громадянами електронне стеження [5]. В липні 2003 р. в штаті Каліфорнія було прийнято «Закон про захист персональних даних штату Каліфорнія» (California Online Privacy Protection Act, CalOPPA), а в червні 2018 р. – «Каліфорнійський закон про конфіденційність споживачів» (California Consumer Privacy Act, CCPA). CalOPPA був першим законом про конфіденційність даних у США, який

вимагав, щоб усі комерційні веб-сайти, що збирали особисті дані про жителів Каліфорнії, мали політику конфіденційності. ССРА, що є найсуворішим законодавством про конфіденційність даних, прийнятим у США на сьогоднішній день, був прийнятий, щоб дати жителям Каліфорнії більше контролю над своїми персональними даними та відстеженням в Інтернеті [6].

Європа, наслідуючи приклад США, також розробила низку законів про захист персональних даних. Наприкінці 70-х років XX ст. в актах Ради Європи захист персональних даних виділився в самостійний вид діяльності. Комітетом експертів Ради Європи з питань захисту персональних даних були сформульовані принципи захисту від неправомірного збору, обробки, зберігання і розповсюдження даних фізичних осіб і 28 січня 1981 р. ці принципи отримали офіційне закріплення в Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних (ETS No. 108) [3]. Ця Конвенція дає гарантії стосовно збору та обробки персональних даних і забороняє, якщо національне право не забезпечує належних гарантій, обробку «чутливих» даних (sensitive data) щодо расової приналежності особи, його політичних поглядів, здоров'я, релігії, сексуальної життя, кримінального минулого тощо. Конвенція також дає особі право знати, що дані про нього зібрані, і, в разі потреби, мати можливість їх виправити. Обмеження викладених у Конвенції прав можливі тільки в разі, коли під загрозою опиняється безпека держави або інтереси оборони [7]. Принципи, що містяться в Конвенції, уточнюються і розвиваються в Директиві про обробку персональних даних та про вільне переміщення таких даних від 24 жовтня 1995 р. (Директива 95/46/ЄС) та в Директиві про обробку персональних даних і захисту права на невтручання в приватне життя в телекомунікаційному секторі від 15 грудня 1997 р. (Директива 97/66/ЄС) [3]. Наприклад, відтепер громадянам Союзу гарантують право на отримання в організаціях та компаніях копій документів, що містять персональні дані про них [2]. У

травні 2018 р. Директива 95/46/ЄС була замінена на Загальний регламент захисту даних (General Data Protection Regulation, GDPR). Новий регламент надає резидентам ЄС інструменти для повного контролю над своїми персональними даними. Разом з цим посилюється відповідальність за порушення правил обробки персональних даних, штрафи сягають 20 мільйонів євро, або 4% річного глобального доходу компанії [8].

Директива 95/46/ЄС стала основою для Закону України «Про захист персональних даних» від 1 червня 2010 р. № 2297-VI (далі – Закон № 2297-VI) [9]. Проте, між Директивою та Законом № 2297-VI в деяких аспектах правового регулювання є серйозні відмінності. Наприклад, Закон № 2297-VI, на відміну від Директиви, включає не тільки автоматизовану обробку і каталогізацію, а й всі можливі випадки і способи обробки персональних даних. Також Закон № 2297-VI не містить прямої заборони на об'єднання декількох баз персональних даних, зібраних для різних цілей, в одну, що може привести до порушення прав людини. Однак під об'єднанням баз даних можна мати на увазі й звичайну синхронізацію двох аккаунтів, що є звичайною справою. Особливістю Директиви 95/46/ЄС є створення робочої групи із захисту індивідумів щодо обробки їх персональних даних, що має статус консультативного органу і діє як незалежна структури. Таким чином, крім органу нагляду існує незалежна група експертів, яка регулює нормативно-правові відносини всіх суб'єктів відносин, пов'язаних з базами даних. Також, як вже було сказано вище, Директива виділяє «чутливі» дані (sensitive data) в окрему групу і забороняє їх обробку, якщо тільки людина не дала дозвіл на це. Аналогічне положення закріплено і в ст. 7 Закону № 2297-VI. Проте, Законом № 2297-VI і так передбачені високі вимоги до обробки персональної інформації, яка не є «чутливою», тому в виділенні даних в таку групу не є необхідності [1].

На сьогоднішній день ЄС і США активно співпрацюють між собою і хочуть створити єдину, уніфіковану угоду. США, на відміну від багатьох інших юрисдикцій, не мають загального закону про конфіденційність та захист даних. Там є закони, що на різних рівнях контролюють захист персональних даних. Це пов'язано з тим, що захист персональних даних в США почав розвиватися ще в 70-х роках минулого сторіччя і при постійному розвитку в ІТ-секторі треба модифікувати старі чи створювати нові закони. Штат Каліфорнія виступає в авангарді регулювання конфіденційності в Інтернеті в США, бо у Каліфорнії на сьогодні наявний найвищий рівень економіки у порівнянні з будь-яким іншим штатом. ССРА, що є найсуворішим законодавством про конфіденційність даних коли-небудь прийнятим у Сполучених Штатах, є схожим на GDPR, прийняття якого сильно вплинуло на підприємців з усього світу. Закон № 2297-VI ще є відносно молодим і, в свою чергу, є схожим на Директиву 95/46/ЄС, хоча й зі своїми відмінностями. Підприємцям з України, що працюють з США чи країнами ЄС треба бути дуже уважними в питаннях законодавства про захист персональних даних, постійно слідкувати за змінами і адаптувати свою роботу у випадку прийняття нових законів.

Список використаної літератури:

1. Про захист персональних даних: Закон України від 01.06.2010 р. № 2297-VI. URL: <https://zakon.rada.gov.ua/laws/show/2297-17> (дата звернення: 15.05.2020)
2. Бирюков М. М. Актуальные аспекты правовой защиты персональных данных в Европейском союзе, США и России. *Московский журнал международного права*. 2015. № 3. С. 197–208. URL: <https://www.mjil.ru/jour/article/viewFile/102/27> (дата звернення: 15.05.2020)
3. Евсеев С. П., Линд Э. А., Король О. Г., Носик О. М. Защита персональных данных. *Системы обработки информации*. 2012. № 4. С. 108–117. URL: http://www.hups.mil.gov.ua/periodic-app/article/9738/soi_2012_4_27.pdf (дата звернення: 15.05.2020)
4. Статистика кражи персональных данных. URL: <https://www.securitylab.ru/blog/company/PandaSecurityRus/344032.php> (дата звернення: 15.05.2020).

5. USA FREEDOM Act of 2015 H.R.2048 from 06/02/2015. URL: <https://www.congress.gov/bill/114th-congress/house-bill/2048/text> (Last accessed: 15.05.2020)

6. Complying with California's privacy protection laws: CalOPPA and CCPA. URL: <https://preyproject.com/blog/en/complying-with-californias-privacy-protection-laws-caloppa-and-ccpa/> (Last accessed: 15.05.2020).

7. Details of Treaty No.108. URL: <https://www.coe.int/ru/web/conventions/full-list/-/conventions/treaty/108> (Last accessed: 15.05.2020).

8. GDPR – новые правила обработки персональных данных в Европе для международного IT-рынка. URL: <https://habr.com/ru/company/digitalrightscenter/blog/344064/> (дата звернення: 15.05.2020).

9. Галаган Д. Защита персональных данных и ЕС. Юридическая практика. 2010. 7 декабря. № 49 (676). URL: <https://pravo.ua/articles/zashhita-personalnyh-dannyh-i-es/> (дата звернення: 15.05.2020).

Завальнюк Ю. Ю.,

Студентка 3-го курсу ІПСА КПІ ім. Ігоря

Сікорського, yulyzavalnuk@gmail.com

Науковий керівник: Іщенко В. В., викладач
кафедри публічного права КПІ ім. Ігоря
Сікорського

ПРОБЛЕМА ЗБИРАННЯ ТА ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ У МЕРЕЖІ ІНТЕРНЕТ

Ми живемо у надзвичайний час, коли для того, щоб зв'язатися з будь-ким у світі достатньо просто зайти в Інтернет та ввести повідомлення. Близько 4,1 мільярда людей у світі користувалися Інтернетом у 2019 р. [1], а кількість інтернет-користувачів в Україні становить 22,9 мільйона людей [2]. Ми залишаємо гігабайти інформації про себе у мережі щодня. Знаючи лише декілька фактів про людину алгоритми можуть передбачити вашу реакцію на таргетовану рекламу, вашу поведінку в мережі чи фільм, який ви захотіли б переглянути краще ніж ваші родичі чи друзі.

Пошукова мережа Google, якою ви скоріше за все сьогодні користувались, збирає приголомшливу кількість особистої інформації про своїх користувачів.

Google запам'ятовує кожен ваш пошук та кожне відео, яке ви переглядаєте YouTube. Google Maps записує журнали скрізь, куди ви їдете, маршрут, який ви проїдете, щоб дістатися туди, і як довго ви будете там залишатися, навіть якщо ви не відкриваєте додаток. Що ще гірше: щоразу, коли ви вносите зміни, які якимось чином обмежують Google, вас попереджають, що служби не працюватимуть без безперебійного доступу до даних. Незважаючи на всі зусилля Google щодо підвищення прозорості, нещодавно виявилось, що він таємно обмінювався приватними даними користувачів із сторонніми рекламодавцями, що не викликають довіри громадськості, в т.ч. даними з розумної лінії Google Nest, що передбачає встановлення динаміків, мікрофонів та камер у вашому будинку [3]. Між корпораціями, політиками та маркетологами ведеться боротьба за вашу увагу, і у цій боротьбі вони шукають будь-які дані, що дізнатись про вас більше.

Так у 2016 р. близько 300 тисяч американців пройшли онлайн-опитування про їх повсякденне життя в соціальній мережі Facebook. В результаті маніпуляцій з цими даними дані більш ніж 50 мільйонів користувачів були використані в президентській кампанії Дональда Трампа. Вважається, що саме ця кампанія принесла йому перемогу на виборах [4].

На території України діють декілька актів, що покликані захищати приватність громадян в Інтернеті: Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних [5], Закони України «Про інформацію» [6] та «Про захист персональних даних» [7]. В ЄС вказані питання регулюють Директива 95/46/ЄС Європейського Парламенту і Ради «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» [8] та Загальне положення про захист даних [9]. Проте, на даний момент відсутнє визначення, які дані є вразливими, тобто повинні регулюватись з більшою обережністю. Наприклад, расове походження, політичні, світоглядні та релігійні уподобання, здоров'я, біометричні та генетичні дані та інші. Причин,

чому немає регулювання цих даних називають багато, від банальних прогалин в законодавстві до теорій змови правління держав. Та все ж регулювання здійснюється. Згідно зі ст. 8 Закону України «Про захист персональних даних» суб'єкт персональних даних має право: знати про джерела збирання даних, мету їх обробки, на доступ до своїх персональних даних; а також отримувати зміст таких даних, пред'являти вмотивовану вимогу щодо зміни або знищення своїх персональних даних та знати механізм автоматичної обробки персональних даних [7]. Тобто підставою для обробки ваших даних є ваша проінформована згода. Проте, згідно зі ст. 17 цього ж Закону відстрочення доступу суб'єкта персональних даних до своїх персональних даних не допускається. Дійсно при відвідуванні багатьох веб-сторінок, ви повинні спершу дати свою згоду на обробку персональних даних [7]. Але, якщо заповнити спеціальну форму заяву у своєму обліковому записі Google, то через якийсь час ви отримаєте на свою пошту архів (іноді більше декількох терабайт), де буде вся інформація, яку ви дозволили збирати, навіть не усвідомлюючи цього. Інколи навіть аудіозаписи, що їх ваш телефон робить без вашого відома.

Потрібно пам'ятати, що згідно з ч. 4 ст. 18 Закону України «Про електронні довірчі послуги» кваліфікований електронний підпис в Україні має таку саму юридичну силу, як і власноручний підпис, та має презумпцію його відповідності власноручному підпису [10]. Тобто у разі якщо суб'єкт даних підписав щось онлайн, він фактично дав свою згоду на обробку та зберігання даних. Отже у разі боротьби за свої права у суді суб'єкт може виявити, що ніякого закону офіційно не було порушено.

Нині, під час всесвітньої пандемії COVID-19, коли серед інших протиепідеміологічних заходів деякі держави пропонують ввести цілодобове спостереження за місцем перебування людей через смартфони з метою детальнішого відстеження шляхів поширення вірусу. Так, в Україні було розроблено програму «Дій Вдома» для контролю людей, які мають пройти

обсервацію [11]. На думку юриста А. Шульгіна, інсталиючи мобільний додаток, громадянин (або ж користувач), по-перше, вступає у добровільні цивільні відносини, тобто у рівні відносини між міністерством як виробником мобільного додатку та користувачем, а по-друге... «Добровільно дає згоду на обробку своїх персональних даних, що є співрозмірним із положеннями частини 2 статті 11 Закону України «Про інформацію» та статті 21 Конституції України, де передбачено, що тільки за вашою згодою є можливим збирання, зберігання, використання, інформації про ваше місцеперебування, стан здоров'я, тощо» [11]. Аналогічні додатки було створено в Гонконзі, Ізраїлі, Китаї, Польщі, Сингапурі [11; 12]. Прем'єр-міністр Росії доручив за чотири дні створити систему відстеження громадян, які перебувають в контакті з хворими на корона вірус. Система, яка повинна сповіщати людей про можливі контактах із зараженими, буде працювати на підставі «відомостей про геолокації стільникового телефону» [12]. Дані мобільних операторів щодо геолокації з аналогічною метою використовують також в Ірані, Італії, Тайвані. Американські ІТ-гіганти Facebook і Google також обговорюють з владою можливість використання даних про місцезнаходження телефонів для боротьби з поширенням. Нині COVID-19 слугує виправданню та легітимізації таких заходів контролю і регулювання, які були б раніше немислимі в західних демократичних суспільствах [12].

Таким чином, базовою метою захисту персональних даних повинно бути забезпечення ключових прав та свобод людини. IBM оцінює, що ми щодня генеруємо квінтільйони байт даних (число з 30 нулями) [13]. Час, в якому ми живемо, так звана «Big Data Era», характеризується обробкою величезної кількості різноманітних даних. Інформація про користувачів, їх діяльність та поведінку в Інтернеті використовується для сотень різних цілей, про які в більшості користувач і не здогадується. Хоча законодавством в передбачені правила та заходи щодо захисту персональних даних користувачів, найперше,

що користувач може зробити для цього сам, це не залишати свої справжні особисті дані на ресурсах, що не викликають довіри, знати свої права, та розуміти обов'язки власників веб-сервісів та за потреби притягувати їх до відповідальності за неправомірні дії. Дехто вважає, що боротьба за безпеку даних у мережі Інтернет вже програна. Проте, грамотне правове урегулювання цього питання та обізнаність населення могли б значно покращити теперішній стан речей.

Список використаної літератури:

1. Лесишин І. Скільки людей у світі користуються інтернетом – ООН. URL: <https://www.the-village.com.ua/village/city/city-news/290933-skilki-lyudey-u-sviti-koristuyutsya-internetom-oon> (дата звернення: 15.05.2020)
2. Лесишин І. Скільки українців користуються інтернетом – дослідження. URL: <https://www.the-village.com.ua/village/city/city-news/290161-skilki-ukrayintsiv-koristuyutsya-internetom-doslidzhennya> (дата звернення: 15.05.2020)
3. Smith D. Google keeps a frightening amount of data on you. URL: <https://www.cnet.com/how-to/google-keeps-a-frightening-amount-of-data-on-you-heres-how-to-find-and-delete-it/> (Last accessed: 15.05.2020)
4. Agence France-Presse. How Facebook data helped Trump win over voters. URL: <https://www.straitstimes.com/world/united-states/how-facebook-data-helped-trump-win-over-voters> (Last accessed: 15.05.2020)
5. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних від 28.01.1981. URL: https://zakon.rada.gov.ua/laws/show/994_326 (дата звернення 15.05.2020)
6. Про інформацію: Закон України від 02.10.1992 № 2657-XII. URL: <https://zakon.rada.gov.ua/laws/show/2657-12> (дата звернення 15.05.2020)
7. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI. URL: <https://zakon.rada.gov.ua/laws/show/2297-17> (дата звернення 15.05.2020)
8. Директива 95/46/ЄС Європейського Парламенту і Ради «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» від 24.10.1995 № 95/46/ЄС. URL: https://zakon.rada.gov.ua/laws/show/994_242 (дата звернення 15.05.2020)
9. Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 р. про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних (Загальний регламент про захист даних). URL: <https://zakon.rada.gov.ua/laws/file/text/63/f474904n8.pdf> (дата звернення 15.05.2020)

10. Про електронні довірчі послуги. Закон України від 05.10.2017 № 2155-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2155-19> (дата звернення 15.05.2020)

11. Ліскович М. Додаток «Дій Вдома» буде за вами стежити. Звісно, якщо ви погодитесь. URL: <https://www.ukrinform.ua/rubric-society/3001538-dodatok-dij-vdoma-bude-za-vami-steziti-ale-zvisno-akso-vi-pogodites.html> (дата звернення 15.05.2020)

12. Бородихин А. Геолокация, дроны и пандемия. Большой Брат против коронавируса. URL: <https://zona.media/article/2020/03/24/surveillance-covid-19> (дата звернення 15.05.2020)

13. 90% Of Today's Data Created In Two Years URL: <https://www.mediapost.com/publications/article/291358/90-of-todays-data-created-in-two-years.html> (Last accessed: 15.05.2020)

Правосуд Р. О.,

Студент 3-го курсу ІІСА КПП ім. Ігоря Сікорського

Науковий керівник: Іщенко В. В.,

викладач кафедри публічного права КПП ім. Ігоря Сікорського

ВПЛИВ КАРАНТИННОГО ТА ПОСТКАРАНТИННОГО ПЕРІОДІВ НА ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ ФІЗИЧНИХ ОСІБ В УКРАЇНІ

В умовах всесвітньої пандемії коронавірусної хвороби (COVID-19) відповідно до постанови Кабінету Міністрів України від 11 березня 2020 р. № 211 з 12 березня 2020 р. на території України було запроваджено карантин [1]. В цей період набуло важливого значення питання захисту та використання персональних даних фізичних осіб, які можуть бути задіяні з метою протистояння розповсюдженню хвороби.

Інформаційне законодавство України регулює права громадян на збирання, одержання, використання та поширення інформації. Крім того, інформаційне законодавство, встановлює вимоги до обробки персональних даних. Згідно ст. 7 Закону України «Про захист персональних даних»

забороняється обробка персональних даних про стан здоров'я особи без її на те згоди [2]. Проте, у разі надзвичайних ситуацій, зокрема, при пандемії COVID-19, уряд може ухвалити рішення, щодо змін у законодавстві, як це і сталося під час карантинного періоду.

13 квітня 2020 р. було прийнято Закон України «Про внесення змін до Закону України «Про захист населення від інфекційних хвороб» щодо запобігання поширенню коронавірусної хвороби (COVID-19)» № 555-IX [3], яким було, зокрема, дозволено обробку персональних даних без згоди особи. Дії влади було спрямовано на отримання щонайбільшої кількості даних про хворих на COVID-19, аби, маючи цю інформацію, якомога найефективніше впроваджувати заходи, що стримають розповсюдження цієї хвороби. Зокрема, це стосувалося даних про стан здоров'я, місце госпіталізації, місце проживання та роботи особи – даних про місця, в яких хворий проводив багато часу до госпіталізації. Таким чином, можна ефективно вживати профілактичні заходи, наприклад, проводячи тестування на COVID-19 серед відвідувачів місць частого перебування хворого до госпіталізації. Найчастіше це співмешканці, сусіди та колеги, але іноді і люди, з якими хворий пов'язаний не так явно, наприклад клієнти фірми або співробітники охорони та обслуговування житлових будинків, які більш зв'язані з хворим географічними місцями перебування, ніж прямим знайомством і можуть бути заражені через посередників між ними. Таким чином, можна виявити більшу кількість заражених, ізолювати їх і стримати розповсюдження хвороби. В такому разі, введення нового закону, який, з одного боку, дещо порушує права громадян на конфіденційність персональних даних, з іншого є досить виправданим під час карантинного періоду.

У той же час, можна піти далі і зобов'язати юридичних осіб надавати персональні дані працівників у межах потреби боротьби з епідемією. Крім того, корисними можуть виявитися не лише персональні дані працівників, але і дані

про закупівлі чи переміщення певних товарів, які, не так явно як персональні дані про кожну особу, показуються зв'язок між певними географічними місцями. Наприклад, коли мова йде про переміщення товарів між містами. Звісно, все це має бути дозволеним лише під час надзвичайних ситуацій для запобігання зловживання персональною інформацією громадян [4].

Держава має гарантувати, що отримані нею дані не будуть використані третіми особами для будь-яких цілей, окрім боротьби з епідемією. Бажано, щоб, після подолання всесередовищної пандемії вся отримана таким шляхом інформація була знищена, окрім, можливо, даних, які стануть корисними у випадку аналогічної надзвичайної ситуації. У такому разі, дані мають бути ретельно захищеними від доступу до них третіх осіб.

Згідно абз. 2 підп. 1 п. 2 розділу II «Прикінцеві та перехідні положення» Закону України «Про внесення змін до Закону України «Про захист населення від інфекційних хвороб» від 13.04.2020 р. № 555-IX передбачено, що протягом 30 днів після закінчення карантину всі зібрані таким чином дані будуть знеособлені або знищені, що є досить вдалим рішенням [3]. Хоча, на нашу думку, слід розглянути варіант збереження подібної інформації, у випадку невтрата її актуальності з часом, на випадок виникнення подібної ситуації знову. Окрім того, накопичена інформація є цінним матеріалом для аналізу, результати якого можуть підказати певні закономірності та шляхи більш ефективного розв'язання аналогічних проблем в майбутньому.

Виникнення надзвичайної ситуації – пандемії COVID-19 – було непередбаченим. Але тепер можна зробити певні висновки, та використати отриманий досвід у майбутньому. Було б доцільно розробити на рівні інформаційного законодавства України зміни до прав та обов'язків громадян стосовно збереження та надання особами своїх персональних даних, надання даних юридичними особами на період боротьби з надзвичайними ситуаціями. Зокрема, регламентувати процедуру отримання, зберігання, використання та

захисту від доступу з боку третіх осіб, даних фізичних та юридичних осіб, зібраних в період надзвичайної ситуації. Також, описати відповідну процедуру ліквідації чи зберігання, отриманих під час карантину, даних. Дані зміни до інформаційного законодавства України дозволять органам влади більш оперативно реагувати на виникнення подібних надзвичайних ситуацій та ефективніше впроваджувати відповідні заходи.

Список використаних джерел:

1. Про запобігання поширенню на території України гострої респіраторної хвороби COVID-19, спричиненої коронавірусом SARS-CoV-2: Постанова Кабінету Міністрів України від 11.03.2020 р. № 211. URL: <https://zakon.rada.gov.ua/laws/show/211-2020-п> (дата звернення: 11.05.2020)

2. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI. URL: <https://zakon.rada.gov.ua/laws/show/2297-17> (дата звернення: 11.05.2020)

3. Про внесення змін до Закону України «Про захист населення від інфекційних хвороб» щодо запобігання поширенню коронавірусної хвороби (COVID-19): Закон України від 13.04.2020 № 555-IX. URL: <https://zakon.rada.gov.ua/laws/show/555-20> (дата звернення: 11.05.2020)

4. Якуша В. Голова комітету НААУ з медичного права Ірина Сенюта: «Коронавірус яскраво ілюструє роль медицини і те, хто має бути найвищою цінністю для держави». Закон і Бізнес. № 16 (1470). 25.04–01.05.2020. URL: <https://zib.com.ua/ua/142409-koronavirus-yaskravo-ilyustrue-rol-medicini-i-te-hto-mae-but.html> (дата звернення: 11.05.2020)

Зух Ю. О.,

Факультет соціології та права

Науковий керівник: Бежвець А.М.,

старший викладач кафедри

інформаційного права та права

інтелектуальної власності

ВПЛИВ ЗАХОДІВ В ІТ-СФЕРІ, СПРЯМОВАНИХ НА БОРотьБУ З ПАНДЕМІЄЮ COVID-19, НА ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ

Спалах COVID-19 призвів до безпрецедентного впровадження нових ІТ-технологій для контролю поширення хвороби. Від спостереження за станом

здоров'я до координації волонтерів, дані використовуються як в державному, так і в приватному секторах, щоб спробувати взяти під контроль COVID-19 та зменшити його вплив.

Цифрові технології, зокрема мобільні та біометричні програми, впроваджуються інноваційними способами для підвищення ефективності боротьби з вірусом. Розкриття особистої інформації може дозволити громадськості краще ідентифікувати потенційні спалахи COVID-19 та відстежувати його поширення у часі. Питання полягає в тому, чи не порушують такі заходи інформаційні права людини?

Насамперед, збираються дані про геолокацію, щоб допомогти владі контролювати та стримувати поширення вірусу. Ця інформація може надаватися постачальниками послуг телекомунікацій під час телефонних дзвінків або інших операцій з телекомунікацій, які дають цінну інформацію про переміщення осіб. Оскільки оператори мережі обслуговують значну частину населення в різних країнах, переміщення мільйонів людей за чіткими просторовими та часовими масштабами можна виміряти майже в реальному часі. Провайдери телекомунікацій у ряді країн почали надавати дані про геолокацію. Наприклад, німецький провайдер телекомунікацій «Deutsche Telekom» надає анонімізовані дані про "потoki руху" своїх користувачів Інституту Роберта-Коха, науково-дослідному інституту та державному агентству, відповідальному за контроль та профілактику захворювань[7].

Наразі Європейська Комісія підтримує зв'язок з вісьмома європейськими операторами зв'язку, щоб отримати від них анонімізовані сукупні дані про геолокацію. Для вирішення проблем конфіденційності дані будуть видалені, коли криза закінчиться [6].

Мобільні додатки вже є важливою частиною заходів для боротьби з вірусом та виявились ефективними в цілях профілактики, ранньої діагностики хвороби (наприклад, перевірки симптомів) та для підключення користувачів до

місцевих служб охорони здоров'я та служб швидкої допомоги. Зараз з'являються нові програми, спрямовані на відстеження COVID-19. Ці програми є продуктом партнерства технологічних компаній, наукових кадрів, та державних органів влади, які в кінцевому рахунку відповідають за їх фінансування, подальший розвиток та впровадження.

Виділимо найцікавіші з них. Додаток «TraceTogether» розроблений Урядовим агентством з технологій Сінгапуру (GovTech) у співпраці з Міністерством охорони здоров'я. Використовуючи Bluetooth, цей додаток відстежує людей, які заразилися коронавірусом. Ця інформація використовується для ідентифікації тісних контактів та тривалості зустрічі двох користувачів. Потім він попереджає тих користувачів, хто контактує з тими, у яких підтвердився позитивний результат тесту на вірус або які можуть переносити інфекцію. Дані збираються на основі заповнення самими користувачами інформації про себе. Якщо особа підозрює, що заражена або її хвороба була підтверджена, вона може вирішити дозволити лікарням, Міністерству охорони здоров'я та третім сторонам отримати доступ до даних у додатку, щоб допомогти встановити контакти з іншими людьми. Сінгапур планує скласти базовий протокол збереження конфіденційності для обміну даними у цій програмі [8].

Понад 130 вчених, технологів та експертів з восьми європейських країн, включаючи Францію, Німеччину та Італію, взяли участь в розробленні додатку з відкритим кодом, який аналізує сигнали Bluetooth між мобільними телефонами для виявлення користувачів, які були в безпосередній близькості один від одного. Додаток тимчасово зберігає зашифровані дані локально, і якщо пізніше користувачі перевірятимуть позитивність на COVID-19, він може попередити всіх, хто був поруч із зараженою людиною в попередні дні, не відкриваючи особистість користувачів[7].

Проте ці заходи можуть недостатньо захищати персональні дані. Як зазначалось раніше, багато країн вже прийняли рішення для аналізу даних з мобільних мереж, щоб простежити рух громадян. Однак виявляється, що компетентні органи захисту даних не завжди були належним чином залучені до цього питання. Італійський орган захисту даних заявляє, що не був проінформований про таку ініціативу, і тому вони не в змозі робити будь-яку подальшу оцінку з цього питання[9].

У будь-якому випадку, відстеження руху громадян за допомогою мобільної мережі виявилось недостатньою мірою для стримування вірусу. Тому Італія проводить оцінку впровадження «цифрового відстеження контактів» з метою відображення осіб, які перебували у фізичному контакті з особами, зараженими вірусом. Також було запропоновано залучити великі компанії з передачею даних, зокрема, Google та Facebook, для збору відповідної інформації щодо поширення вірусу. Німеччина та Польща розглядають можливість втілення подібних рішень. У Норвегії в даний час Норвезький інститут громадського здоров'я оцінює реалізацію програми, здатної простежити рух громадян. Загальна мета - автоматизувати та прискорити контроль над випадками зараження [9].

Вищезгадані заходи викликають кілька проблем щодо конфіденційності. Хто є контролером даних для оброблених персональних даних? Які особисті дані можна обробляти і на який термін? Як буде забезпечено захист персональних даних? Відповіді на ці питання, очевидно, залежатимуть від прийнятих рішень та часових обмежень. Демократичним країнам складно скопіювати китайську модель, де тоталітарні рішення влади значно зменшили права на конфіденційність. Та чи відповідають вищезгадані рішення принципам демократії та чи не порушують вони права у сфері захисту персональних даних?

Конфіденційність вважається одним з основних прав людини відповідно до Європейської конвенції з прав людини (Стаття 8) та Хартії основних прав

Європейського Союзу (Стаття 7), але це право можна обмежити, якщо виконуються певні вимоги (Стаття 52 Хартії)[1,4].

Можливість обмеження прав на конфіденційність також впливає із Загального регламенту щодо захисту даних. Стаття 6 визначає, що обробка персональних даних є законною, коли обробка необхідна з міркувань, що становлять суспільний інтерес, тоді як стаття 9 дозволяє обробляти спеціальні категорії даних (тобто дані про здоров'я), коли обробка необхідна з міркувань, що становлять суспільний інтерес, за умови, що обробка базується на законодавстві Союзу чи країн-членів. Це також підтверджує Європейська рада захисту даних, яка 16 березня 2020 року випустила заяву, в якій заявила, що "правила захисту даних не перешкоджають заходам, вжитим у боротьбі з пандемією коронавірусу"[3]. Що стосується відстеження геолокації за допомогою мобільної мережі та відстеження цифрових контактів, стаття 15 Директиви 2002/58 стосовно обробки персональних даних та захисту права на недоторканість особистого життя в сфері електронних засобів зв'язку від 25 листопада 2009 року дозволяє державам-членам вводити законодавчі заходи щодо обробки даних про місцезнаходження без згоди осіб та в неанонімізованій формі, при здійсненні національної та громадської безпеки[2].

Зважаючи на вищезазначене, права на конфіденційність можуть бути обмежені лише за допомогою законодавчих заходів. Наприклад, в Італії, Закон від 25 березня 2020 р. №19 дозволяє особам, які надають національні послуги в галузі охорони здоров'я, та тих, що гарантують виконання запобіжних заходів, обробляти персональні дані, включаючи спеціальні категорії даних, для цілей національної безпеки та охорони здоров'я. Захід обмежений поточним надзвичайним періодом і служить правовою основою для обробки персональних даних. Однак, наразі тривають суперечки, чи застосовуватиметься акт також до приватних компаній і чи будуть прийняті нові постанови для регулювання можливого здійснення цифрового відстеження контактів.

Італійський орган з захисту даних рекомендує, посилаючись на цифрове відстеження контактів, щоб збір даних був якнайменш інвазивним. Наприклад, слід віддавати перевагу анонімізованій обробці даних мобільним оператором, тим самим залишаючи державним органам повноваження аналізувати особисті дані щодо осіб, де це необхідно[5].

Отже, звуження права на конфіденційність може відбуватися на законодавчому рівні, шляхом прийняття відповідних актів центральними та кваліфікованими органами влади, таким чином забезпечуючи рівномірність у застосуванні вжитих заходів. Обмеження прав на конфіденційність повинні бути пропорційними актуальним потребам суспільства.

Таким чином, слід ретельно продумати спосіб впровадження нових ІТ-технологій в боротьбі проти вірусу. Наприклад, регламент про можливе залучення таких великих компаній, як Google та Facebook, повинен не допустити масового збору персональних даних цими транснаціональними корпораціями. Важливо знайти правильний баланс між захистом суспільних інтересів та обмеженням прав на конфіденційність. Якщо країнам вдасться досягти успіху в цьому, технології можуть стати вирішальним фактором у боротьбі з вірусом. ІТ-технології, які вже доступні на ринку, продемонстрували свою ефективність у цьому плані.

Список використаної літератури:

1. Конвенція про захист прав людини і основоположних свобод : з поправками, внесен. відповідно до положень Протоколів №№ 11 та 14 з Протоколами №№ 1, 4, 6, 7, 12 та 13) // Право України. – 2010. – № 10. – С. 215–233;
2. Директива № 2002/58/ЄС Європейського Парламенту і Ради ЄС стосовно обробки персональних даних та захисту права на недоторканість особистого життя в сфері електронних засобів зв'язку від 25 листопада 2009 року[Електронний ресурс]. – https://zakon.rada.gov.ua/laws/show/994_b34
3. Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 р. про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 96/46/ЄС

(Загальний регламент про захист даних) / Європейський Союз. Цит. 24.11.2014 р. URL - <https://www.kmu.gov.ua/storage/app/media/uploaded-files/es-2016679.pdf>

4. Хартія основних прав Європейського Союзу. – 712. – URL: https://zakon.rada.gov.ua/laws/show/994_524.

Закон Італії від 25 березня 2020 р. №19 - DEGREE-LAW of 25 March 2020, No. 19// OFFICIAL GAZETTE OF THE REPUBLIC OF ITALY. – 2020. – №79. – С. 1–4.

5. Зайонц А. Влада ЄС буде відстежувати розповсюдження коронавірусу через мобільні телефони / Артур Зайонц // НВ. – 2020. – URL: <https://nv.ua/ukr/techno/it-industry/v-yes-operatori-zv-yazku-budut-dilitisya-z-vladoyu-danimi-pro-misceznahodzhennya-koristuvachiv-50078153.html>

6. Кочкодан О. Війна за персональні дані під час пандемії / О. Кочкодан // Економічна правда. – 2020. – URL: <https://www.epravda.com.ua/columns/2020/04/30/660040/>.

7. Офіційний сайт додатку "TraceTogether" // A Singapore Government Agency Website. – 2020. – URL: <https://www.tracetgether.gov.sg/>.

8. Olaussen H. B. COVID-19 and new IT solutions: Privacy in quarantine? / H. B. Olaussen, G. Hvidsten, D. Leonio // Wikborg Rein. – 2020. – URL: <https://www.wr.no/en/news/covid-19-and-new-it-solutions-privacy-in-quarantine/>.

Пивовар П. Є., Пашиєва О. М.,

Студенти 3-го курсу ІПСА КІП ім.

Ігоря Сікорського

Науковий керівник: Іщенко В. В.,

викладач кафедри публічного права

КІП ім. Ігоря Сікорського

ПРАВОВІ АСПЕКТИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ВІД КІБЕРАТАК

Пандемія COVID-19 вимусила багатьох людей проводити свою професійну та повсякденну діяльність онлайн. Все більше людей залишають у мережі Інтернет свої персональні дані — об'єкт нападу зловмисників, які організовують кібератаки. Динаміка кількості кіберзлочинів зростає рік за роком. Так, якщо у 2014 р. в Україні було зареєстровано 443 злочинів у сфері використання комп'ютерів, систем та комп'ютерних мереж і мереж електрозв'язку, то у 2015 р. – 598, у 2016 р. – 865, у 2017 р. – 2573, а тільки за

січень-серпень 2018 р. – 1885 злочинів. У структурі кіберзлочинності в Україні переважає несанкціоноване втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ст. 361 КК України). На нього припадає понад 69,8 % злочинів, які вчиняються (реєструються) на території України [1, с. 161]. Враховуючи цю статистику, стає зрозуміло, що потрібна особлива увага до питання захисту персональних даних від кібератак.

Як зазначено у п. 2 ст. 11 Закону України “Про інформацію” не допускаються збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та захисту прав людини [2]. Отже, постає потреба у захисті прав громадян, а саме права на конфіденційність персональні дані від атак хакерів. В Україні велика кількість державних сервісів та сервісів приватного сектору надаються з використанням мережі Інтернет. Для користування онлайн-сервісами користувачам необхідно надати свої персональні дані. До конфіденційної інформації про фізичну особу належать, зокрема, дані про її національність, освіту, сімейний стан, релігійні переконання, стан здоров'я, а також адреса, дата і місце народження. Слід зазначити, що до конфіденційної може відноситись також інформація про юридичну особу, наприклад, комерційна таємниця. Відповідно до ст. 505 Цивільного кодексу України це можуть бути відомості технічного, організаційного, комерційного, виробничого та іншого характеру (за винятком тих, які відповідно до закону не можуть бути віднесені до комерційної таємниці) і щодо яких ця юридична особа вжила заходи щодо збереження секретності [3]. До конфіденційної юридичною особою може бути віднесена й інша інформація. Таким чином, з однієї сторони в умовах карантину, коли будь-яка професійна комунікація відбувається за допомогою електронних сервісів, постає проблема забезпечення захисту комерційної таємниці. З іншої сторони,

існує задача захисту персональних даних громадяни, що користуються інтернет-послугами.

Закон України «Про захист персональних даних» регулює правові відносини, пов'язані із захистом і обробкою персональних даних, і спрямований на захист основоположних прав і свобод людини та громадянина, зокрема права на невтручання в особисте життя у зв'язку з обробкою персональних даних (ст. 1) [4]. Таким чином, якщо СПД для ведення своєї господарської діяльності потребує зберігання персональних даних громадян, він або вона зобов'язані їх захистити. Вказаний закон встановлює обмеження СПД на обробку, зберігання та розповсюдження та у випадку порушення обмежень накладаються адміністративні штрафи. Так, відповідно до ст. 188-39 Кодексу України про адміністративні правопорушення передбачено адміністративну відповідальність у формі штрафу за неповідомлення або несвоєчасне повідомлення Уповноваженого Верховної Ради України з прав людини про обробку персональних даних або про зміну відомостей, які підлягають повідомленню згідно із законом, повідомлення неповних чи недостовірних відомостей, а також за недодержання встановленого законодавством про захист персональних даних порядку захисту персональних даних, що призвело до незаконного доступу до них або порушення прав суб'єкта персональних даних [5].

Крім цього, в ст. 361, 362 та 363 Кримінального кодексу України передбачена кримінальна відповідальність за несанкціоновані дії з інформацією, яка обробляється на комп'ютерах та за порушення правил експлуатації комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них обробляється; за несанкціоноване втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, що призвело до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її

маршрутизації; за несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається на комп'ютерах, автоматизованих системах, комп'ютерних мережах або на носіях такої інформації; за несанкціоновані перехоплення або копіювання інформації, яка обробляється на комп'ютерах, автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, якщо це призвело до її витоку, вчинені особою, яка має право доступу до такої інформації; за несанкціоновану зміну, знищення або блокування інформації, яка оброблюється на комп'ютерах, автоматизованих системах чи комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї [6].

В якості прикладу порушення порядку захисту персональних даних можна навести нещодавні події, пов'язані з платформою Zoom. Відеоконференції набули великого значення в умовах соціального дистанціювання. Онлайнзустрічі на платформі Zoom проводять не лише звичайні громадяни, а й представники бізнесу та навіть державні структури [7]. Проте, нещодавно стало відомо, що персональні дані понад 500000 користувачів Zoom, серед яких і суб'єкти підприємницької діяльності (далі – СПД), були злиті у так звану “темну мережу” [8].

Варто також зазначити, що СПД, які мають користувачів за кордоном, зокрема у країнах Європейського Союзу, зобов'язані дотримуватися вимог Загального регламенту про захист даних (GDPR) [9]. На організації чи компанії, які порушують положення GDPR, можуть накладатися штрафи у розмірі від 2% від річного валового обороту до 20 млн. євро.

У багатьох випадках для малого та середнього бізнесу, що намагається провадити свої сервіси через Інтернет, штрафні санкції є завеликими та можуть призвести до їх банкрутства, тим більше зараз, коли через епідемію COVID-19 попит на електронні послуги зростає, але бізнесу все тяжче триматися на плаву, зважаючи на складнощі роботи під час карантину. Встановити обладнання,

запровадити процеси та найняти спеціалістів можна самостійно чи скористатися послугами з кібербезпеки у спеціалізованих компаній. Проте, варто врахувати, що для малого та середнього бізнесу розробка власної системи, що могла б повністю забезпечувати безпеку даних користувачів від кібератак або оплата послуг спеціалізованих компаній вимагає чималих ресурсів. Тому забезпечити надійність даних користувачів можуть лише представники великого бізнесу.

Можливі два шляхи розв'язання проблеми.

Перший полягає у зменшенні розміру штрафних санкцій для СПД. Такий підхід має недолік, адже зменшення штрафів може призвести до нехтування СПД правами користувачів або порушення процедури безпечного зберігання конфіденційних даних. Інший підхід полягає у наданні державою послуг у сфері кібербезпеки для малого та середнього бізнесу або наданні фінансової допомоги для боротьби з кібератаками.

Прикладом другого підходу є ініціатива Національного центру з кібербезпеки Великої Британії (NCSC) – Кібер Акселератор (Cyber Accelerator). Проєкт полягає у підтримці стартапів, що спеціалізуються на розробці технологій у сфері кібербезпеки. В межах програми підприємцям надається допомога спеціалістів з NCSC, грант у розмірі 25000 фунтів стерлінгів, доступ до інвесторів та зв'язки з такими технологічними гігантами як бренди Telefónica [10].

Гуйван П. Д. слушно констатує невизначеність чинного українського законодавства в площині запровадження негативних наслідків для порушника прав особи на повагу її особистої інформації. Він закликає розпочати нормотворчу роботу з метою конкретизації загальних положень Закон України “Про захист персональних даних” та деталізації відповідних механізмів правозастосування. Слід додати, що така невизначеність дає підстави для перевищення повноважень органами влади, які відповідають за накладання санкцій, що може призвести до несправедливого покарання СПД. Цю проблему

необхідно вирішити шляхом внесення змін до існуючих нормативно-правових актів [11, с. 90].

Оскільки частота та важкість наслідків кібератак збільшуються, особливо зараз, під час епідемії COVID-19, коли найбільша кількість людей в історії працюють, проводять ділові та особисті зустрічі у мережі Інтернет, то стає неможливим ігнорування питання захисту персональних даних. СПД, що збирають дані про користувачів для ведення своєї господарської діяльності зобов'язані забезпечувати захист персональних даних від кібератак, що вимагає чималих фінансових ресурсів. Крім того, штрафи часто несправедливі - суми є значними для малого та середнього бізнесу, великий же бізнес навіть не зверне на них уваги та не постарается виправити становище. Тому необхідна допомога держави бізнесу у сфері кібербезпеки. У роботі розглянуто декілька варіантів розв'язання проблеми. Найкраща альтернатива, на нашу думку, це взяти за приклад ініціативу NCSC, адже в Україні вже існують державні проекти підтримки стартапів і приділити більше уваги саме кібербезпеці не потребує значного виділення коштів або часу на реалізацію.

Список використаних джерел:

1. Кравцова М. О. Сучасний стан і напрями протидії кіберзлочинності в Україні. Вісник кримінологічної асоціації України. 2018. № 2 (19). С. 155–166. URL: <http://dspace.univd.edu.ua/xmlui/handle/123456789/3848> (дата звернення: 10.05.2020)
2. Про інформацію: Закон України від 02.10.1992 № 2657-XII. URL: <https://zakon.rada.gov.ua/go/2657-12> (дата звернення: 11.05.2020)
3. Цивільний кодекс України від 16.01.2003 № 435-IV. URL: <https://zakon.rada.gov.ua/go/435-15> (дата звернення: 10.05.2020)
4. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI. URL: <https://zakon.rada.gov.ua/go/2297-17> (дата звернення: 28.04.2020)
5. Кодекс України про адміністративні правопорушення від 07.12.1984 № 8073-X. URL: <https://zakon.rada.gov.ua/go/80731-10> (дата звернення: 10.05.2020)
6. Кримінальний кодекс України від 05.04.2001 № 2341-III. URL: <https://zakon.rada.gov.ua/go/2341-14> (дата звернення: 29.04.2020)
7. Corera G. UK government defends PM's use of Zoom. BBC. 2020. URL: <https://www.bbc.com/news/technology-52126534> (Last accessed: 11.05.2020)

8. Abrams L. Over 500000 Zoom accounts sold on hacker forums, the dark web. BleepingComputer. 2020. URL: <https://www.bleepingcomputer.com/news/security/over-500-000-zoom-accounts-sold-on-hacker-forums-the-dark-web/> (Last accessed: 11.05.2020)

9. Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних) від 27.04.2016 № 2016/679. URL: https://zakon.rada.gov.ua/go/984_008-16

10. Next-gen start-ups to partner with National Cyber Security Centre: // URL: <https://www.ncsc.gov.uk/news/next-gen-start-ups-to-partner-with-national-cyber-security-centre> (Last accessed: 11.05.2020)

11. Гуйван П. Д. Правові засади захисту персональних даних. Науковий вісник Ужгородського національного університету. Серія ПРАВО. 2018. Випуск 51. Том 1. С. 87–91. URL: http://www.visnyk-juris.uzhnu.uz.ua/file/No.51/part_1/20.pdf (дата звернення 11.05.2020)

Купрієнко С. П.,

Студентка 3-го курсу ФБМІ КПІ ім. Ігоря
Сікорського

Науковий керівник: Іщенко В. В., викладач
кафедри публічного права КПІ ім. Ігоря
Сікорського

ПРОБЛЕМИ ОХОРОНИ ТА ЗАХИСТУ АВТОРСЬКИХ ПРАВ В МЕРЕЖІ ІНТЕРНЕТ

В останні десятиріччя спостерігається стрімкий розвиток інформаційних технологій. Цей розвиток супроводжується проблемою захисту авторських прав. Це зумовлено в першу чергу простотою та швидкістю розміщення інформації у всесвітній мережі і, відповідно простотою її отриманням. Проблема захисту авторського права як об'єкта інтернет-відносин постала давно. Основним джерелом її виникнення є питання анонімності автора контенту в мережі Інтернет, тобто головна проблема, яка унеможливає врегулювання інтернет-відносин – труднощі при ідентифікації користувача.

Науковці виділяють наступні правові проблеми захисту авторського права, викликані розвитком інформаційних технологій:

1. Відсутність нормативно-правових актів, які б регулювали дану сферу відносин.
2. Правова невизначеність багатьох ключових понять або недостатнє їх відпрацювання.
3. Транскордонний характер використання об'єктів авторського права через мережу Інтернет.
4. Проблема слідкування за тим чи буде використовуватися даний об'єкт з урахуванням авторських прав.
5. Велика кількість (з тенденцією до збільшення) порушень авторського права, оскільки дієві механізми захисту авторського права відсутні [1, с. 164].

Розглянемо ці проблеми детальніше. На сьогодні жодна країна світу не має повного та кодифікованого законодавства, яке б регулювало відносини в мережі Інтернет. Ця проблема напряду пов'язана з наступною – невизначеністю правових понять. Наприклад, немає єдиного визначення мережі Інтернет в міжнародних актах. Оскільки основним джерелом виникнення проблем захисту авторського права в Інтернеті є ідентифікація користувача, то транскордонний характер робить цю проблему ще гострішою. Більшість соціальних мереж та деякі веб-сайти мають прив'язку до іноземного інтернет-сегменту. Для автора твору чи аудіовізуального контенту дана особливість відкриває нові можливості – його матеріали можуть використовувати майже у всьому світі, але водночас це унеможлиблює регулювання його авторських прав. Слід враховувати, що на території, де використовуються матеріали автора, відповідні норми права можуть не мати юридичної сили. Після розміщення об'єкта в Інтернеті виникає проблема щодо можливості простеження, ким і як буде використовуватися даний об'єкт авторського права. На даний фактор впливає масштабність –

доступ до контенту автора відкривається для мільйонів користувачів по всьому світу.

На думку М. Мельникова, законодавець повинен підвищити рівень покарань за порушення у вказаній сфері залежно від рівня суспільної небезпеки. Уряд активними діями повинен довести суспільству, що він не потуратиме порушенням авторських прав у сфері інформаційних технологій і за їх допомогою. Також широкого поширення набули факти незаконного розповсюдження творів у мережі Інтернет, їх публічне сповіщення у громадських місцях, закладах торгівлі, харчування тощо [2, с. 87].

Особливої уваги заслуговує також таке порушення авторського права як плагіат. Однією з найважливіших передумов поширення плагіату на сьогодні є розвиток Інтернету, велика кількість користувачів в мережі, необізнаність громадян, що спричиняє оббіг інформації без врахування авторських прав.

Плагіатом вважається публікація повністю або частково чужого твору під іменем особи, яка не є автором цього твору. Плагіат вирізняється саме присвоєнням чужого авторства, порушенням майнових та особистісних немайнових прав, тобто відбувається розповсюдження матеріалу автора з прихованим або з чужим іменем [3].

Вирішенням проблем захисту авторських прав в Інтернеті повинне стати, по-перше, спеціалізоване законодавче регулювання інтернет-відносин першочергово у кожній державі. Тоді б автори не боялись таких негативних явищ, як плагіат, піратство, а електронні бібліотеки могли б повноправно працювати, не ставлячи під загрозу права автора. В такому випадку користувачі зможуть знаходити необхідну їм інформацію в зручний для них спосіб, не порушуючи закон, а автори будуть у спокої за свої авторські права.

Але необхідно розробляти шляхи вирішення проблем захисту авторських прав в Інтернеті не тільки на внутрішньодержавному рівні, але і на міждержавному з залучення якомога більшої кількості держав. Це повинно

стосуватися і держав «третього світу», яким необхідно створювати сприятливі умови для входження до світового співтовариства.

Є декілька варіантів вирішення існуючих проблем при захисті авторських прав в мережі Інтернет, зокрема, в соціальних мережах.

- Використання електронних цифрових підписів.
- Використання цифрових марок.
- Обмеження доступу до матеріалів, що розміщені в мережі Інтернет. Наприклад, бази даних комерційних сайтів і деяких електронних бібліотек та архівів доступні тільки за попередню плату.
- Створення веб-депозитаріїв. Цей метод заснований на реєструванні творів автора в певне сховище, в якому зберігається текст твору, його короткий опис, дата подання. Автору надають свідоцтво, про те що об'єкт прийнятий на зберігання в певну дату. Саме ця дата буде вирішальною при встановленні прав авторства у конфліктній ситуації.
- Підхід обмеженої функціональності. За такого підходу, власник авторського права надає користувачеві примірник твору, який має функціональні обмеження.
- «Годинникова бомба». Аналогічно до прийому з функціональними обмеженнями, за цього підходу власник авторських прав розповсюджує функціонально повноцінний об'єкт інтелектуальної власності, але встановлює дату, після якої доступ до нього буде неможливим. Один з варіантів такого підходу передбачає закриття продавцем доступу до твору після певної кількості користувань [4, с.93].

Обґрунтуємо ці способи.

Зараз є поширена практика використання електронних цифрових підписів (далі – ЕЦП). ЕЦП – електронний підпис, що отриманий при криптографічному перетворенні набору електронних даних. В основному, ЕЦП використовують для аутентифікації особи, в нашому випадку – автора контенту. Завдяки ЕЦП

можна однозначно визначити походження інформації, та розмежовувати відповідальність за діяльність в мережі. (наприклад відповідальність за дезінформування).

Можна також використовувати цифрові марки. Найпростіша цифрова марка – цифровий водяний знак – це мітка, яка встановлюється у тексти чи аудіовізуальний контент. Її особливість полягає в тому, що при звичайному розгляді її непомітно. Це може бути знак копірайта, ім'я автора або його псевдонім, видавництво, логотип і т.д. Встановлення цифрового водяного знаку може використовуватися для відстеження розповсюдження копій документів. Це спростить механізм ідентифікації правопорушника.

Також популярним способом є спосіб обмеженої функціональності та «годинникова бомба». Вони мають схожий підхід за тієї відмінності, що при обмеженій функціональності автор надає користувачеві примірник твору з обмеженою функціональністю, а за підходу «годинникова бомба» автор розповсюджує функціонально повний об'єкт але на певний термін. Такі підхід є одним із шляхів впровадження в життя таких бізнес-моделей як «спробуй перед тим, як купити» та «продавай поліпшені версії».

Наведені вище способи запобігання порушенням у сфері охорони та авторських прав в Інтернеті є перспективними, але вони не можуть бути повністю застосовані до усіх об'єктів авторського права, а тому необхідно докласти максимум зусиль для ліквідації прогалин у законодавстві задля поліпшення регулювання сфери охорони й захисту інтелектуальної власності.

Обмін інформацією з використанням об'єктів авторських прав в соціальних мережах, відрізняється тим, що інформація поширюється серед тих груп людей, які потенційно в ній зацікавлені; інформація поширюється з метою популяризації і така популяризація є безкоштовною.

Усі ці особливості забезпечують можливість ознайомлення з об'єктом авторського права в Інтернеті не будь-якого невизначеного кола осіб, а певної

соціальної групи, що потенційно зацікавлена в отриманні саме такої інформації. Зв'язок, що виникає між об'єктом авторського права і адресатом використовується як для популяризації об'єкта, що саме по собі не має майнового характеру, так і для подальшого спонукання придбати певний товар, що містить об'єкт інтелектуальної власності. Така особливість може спричинити порушення майнових і немайнових прав інтелектуальної власності. Сформульовані особливості дають можливість серед використання об'єктів інтелектуальної власності в Інтернеті виділити в окремий вид використання об'єктів інтелектуальної власності у соціальній мережі.

Аналізуючи актуальні проблеми у сфері охорони та захисту авторських прав в Інтернеті, приходимо до висновку щодо необхідності, передусім, вдосконалення як внутрішньодержавного законодавства, так і міжнародного права у даній сфері. По-друге, потрібно провести належне впровадження таких договорів усіма без винятку державами, що полегшить міжнародно-правове регулювання сфери охорони авторських прав в Інтернеті та сприятиме більш швидкому вирішенню існуючих в проблем даної сфери.

Список використаної літератури:

1. Харитонova О. І., Ульянова Г. О., Кирилюк А. В., Симонян Ю. Ю., Бааджи Н. П., Позова Д. Д., Григор'янц Г. І., Бурова Л. І., Мартинюк І. В. Проблемні питання визначення правової природи і структури правовідносин інтелектуальної власності, що виникають у мережі Інтернет. Наукові праці Національного університету «Одеська юридична академія». Т. XVII. Одеса: Юридична література, 2015. С. 159–200. URL: <http://www.naukovipraci.nuoua.od.ua/arhiv/tom17/7.pdf> (дата звернення 18.05.2020).
2. Мельников М. Піратство як злочин у галузі авторського права та суміжних прав: погляд на проблему. Право України. 2003. №4. С. 83–87.
3. Правдиченко А. Що таке плагіат і чи законна праця «найманих авторів»? URL: <https://detector.media/rinok/article/142335/2018-11-06-shcho-take-plagiat-i-chi-zakonna-pratsya-naimanikh-avtoriv/> (дата звернення 18.05.2020).
4. Пастухов О. М. Авторське право в Інтернеті. Київ: Школа, 2004. 144 с. URL: <http://programming.in.ua/other-files/internet/251-copyright-in-internet-pastuhov-book.html> (дата звернення 18.05.2020).

Чумакова А. В.,

студентка факультету соціології і права, КПП
ім. Ігоря Сікорського

Науковий керівник: Солончук І. В., ст.

викладач кафедри інформаційного права та
права інтелектуальної власності КПП імені
Ігоря Сікорського

СУЧАСНІ ЕЛЕКТРОННІ ІНФОРМАЦІЙНІ СИСТЕМИ ЯК ПРИВІД ДО ВЧИНЕННЯ КІБЕРЗЛОЧИНІВ

Із динамічним розвитком сучасних електронних систем та технологій на перший план виходить питання інформаційної безпеки та захисту прав людини в глобальній мережі. Поява та розвиток нових інтернет-технологій зумовили створення як нових можливостей для передачі інформації, так і стрімке зростання правопорушень та злочинів у сфері інформаційних та комп'ютерних мереж.

На жаль, розвиток сучасних інформаційних технологій став приводом для здійснення правопорушень у цій сфері, та в багатьох випадках має ознаки злочинів, які свідомо та навмисно порушують права людини, найчастіше - з корисливих спонукань та мотивів.

Конституція України визначає право на захист персональних даних як основоположне право людини, та такі права набувають особливої актуальності з поширенням й розвитком інформаційних технологій. На сьогодні, при використанні мережі Інтернет або мобільних телефонів, значні обсяги персональних даних часто зберігаються та передаються без нашої явної згоди чи, навіть, обізнаності про їх обробку. Наслідком такого явища може бути і кіберзлочин [1, с.141].

Існує величезна кількість потенційних зловживань за допомогою оволодіння нашими даними, які можуть варіюватися від прямого визначення змісту нашої інформації за допомогою цільової реклами аж до свідомої та зловмисної діяльності [2, с. 256].

Забезпечення прав людини у сфері новітніх технологій стає найбільш проблемною сферою захисту, адже нормативно-правове регулювання значно відстає від реалій сьогодення. Тому, забезпечення недоторканності персональних даних особи в кіберпросторі потребує абсолютно нового підходу до його розуміння, ефективного контролю збору таких даних, обробки, знищення та виправлення.

З огляду на конституційність даного права, особа має право знати, хто і де обробляє її персональні дані, надавати або не надавати дозвіл на їх передачу або зберігання. В реаліях сьогодення захист персональних даних кожного індивіда повинен трактуватися як один з аспектів, що є основою існування демократичного суспільства. Технології досягли такого прогресу, що, здається, неможливо почуватися захищеним у кіберпросторі.

Із стрімким розвитком даної сфери зростає й кількість злочинів в електронних системах, а тому з впевненістю можна стверджувати, що саме "кіберзлочини" у двадцять першому столітті будуть одними з найчисельніших.

Щороку у всьому світі вчиняються десятки тисяч злочинів з використанням програмних, інформаційно-комунікаційних технологій, інших технічних й технологічних засобів та апаратів. Кожен день звичайні люди, компанії, корпорації потерпають від викрадення персональних даних, що вміщують конфіденційну та комерційну інформацію, від викрадення коштів з рахунків тощо.

На нашу думку, легкий доступ та шлях до вчинення таких злочинів є однією з головних проблем в цій сфері. Наприклад, звичайна пропозиція заповнити анкету при реєстрації на сайті стала приводом до вчинення злочину і отримання конфіденційної інформації. В травні 2020 року співробітники Департаменту кіберполіції спільно із Головним слідчим управлінням НПУ викрили мешканця Київської області у розповсюдженні персональних даних громадян України. Виявилося, що фігурант організував діяльність веб-ресурсу,

через який здійснював розповсюдження персональних даних громадян України. Для доступу до зазначеної інформації користувачу необхідно було зареєструватись на веб-ресурсі з використанням месенджера. Задля наповнення бази, зловмисник створив відповідну форму, яку заповнювали користувачі веб-ресурсу. Після чого він несанкціоновано отримував доступ до персональних даних користувачів [6].

За останні кілька років державні установи неодноразово були атаковані з кіберпростору. Однією з таких атак був запуск різновиду вірусу *Petya*, який спричинив порушення роботи українських державних підприємств, установ, банків, медіа та інших. Внаслідок атаки була заблокована діяльність таких підприємств як аеропорт «Бориспіль», ЧАЕС, «Укртелеком», «Укрпошта», «Ощадбанк», «Укрзалізниця» та багатьох інших великих підприємств. Також були заражені інформаційні системи Міністерства інфраструктури, Кабінету Міністрів України, сайти Львівської міської ради, Київської міської державної адміністрації, кіберполіції та служби спецв'язку України [5, с.16].

Однак, порівнюючи з кількістю подібних правопорушень, успішність запобігання таким злочинам, їх викриття та притягнення винних осіб до відповідальності наразі є достатньо рідкісним явищем.

Як бачимо, одним із найпоширеніших злочинів у цій сфері є злочини, які стосуються розголошення конфіденційної інформації, що становить державну та іншу, передбачену законом, таємницю, а також конфіденційну інформацію, що є власністю держави або спрямована на забезпечення потреб і національних інтересів суспільства й держави, за допомогою різного роду сучасних інформаційних систем та технологій. Як вже наголошувалося, у світі останнім часом з'являється багато нових систем, вдосконалюються вже існуючі електронні інформаційні системи, що постійно стають об'єктами вчинення злочинів [3, с.113].

Стан законодавчої і нормативної бази у сфері кібернетичної злочинності, в цілому, можна охарактеризувати як недосконалий через наявну безсистемність і відсутність термінологічної визначеності в базових поняттях. Це призводить до низької розкриваності кіберзлочинів з огляду на відсутність нормативної визначеності таких дій в законодавстві. Логічним вбачається висновок про те, що динамічний розвиток електронних систем та відсутність нового законодавчого закріплення, у зв'язку із прогресивністю останніх, найчастіше призводить до порушення прав людини та неможливості притягнення особи до юридичної відповідальності.

Україні необхідно враховувати досвід іноземних держав, а саме Європейського Союзу, де вже давно розробляються принципи, кодекси й декларації з метою встановлення нормативної бази та спеціальних правил і кодексів поведінки для врегулювання всіх аспектів, пов'язаних з розвитком та глобалізацією інформаційного суспільства. Сучасне право ЄС містить декілька нормативно-правових актів, призначенням яких є забезпечення належного рівня захисту персональних даних осіб у всіх країнах ЄС. Одним з основних аспектів, врегульованих у законодавстві ЄС, є "право бути забутим". Це означає, що кожна особа у будь-який момент має право вимагати видалення її персональних даних з мережі [4, с. 25].

Отже, прогрес у науково-технічній діяльності та створення глобальних кібертехнологій стали підґрунтям для виникнення кіберзлочинності, яка постійно зростає. На сьогодні кіберзлочини завдають шкоди як фізичним та юридичним особам, так і державі. Боротьба з кіберзлочинністю та кібербезпека є одними з найбільш головних питань, які потребують якісного аналізу та розробок з метою запобігання та викриття кіберзлочинів в даній сфері. Можна стверджувати, що із розвитком сучасних інформаційних технологій виникають як позитивні, так і негативні наслідки, зокрема, у вигляді кіберзлочинів.

Досить "легкодоступний" спосіб вчинення даних злочинів робить шлях їх вчинення досить простим, а відсутність їх нормативного регулювання зумовлює складність їх запобігання та протидії. Можна зробити висновок про те, що стан захищеності прав і свобод людини під час здійснення кримінального провадження кіберзлочинів не є задовільним та потребує більш рішучих заходів зі сторони правоохоронних органів, а недосконалість існуючої законодавчої і нормативно-правової бази призводить до зростання кіберзлочинів, що вчиняються за допомогою електронних інформаційних систем, з огляду на низьку вірогідність покарання.

Список використаної літератури:

1. Конституція України: Закон України від 28 червня 1996 р. №254к/96-ВР. *Відомості Верховної Ради України*. 1996. № 30. Ст. 141.
2. Манжай О. В., Осятинська І. А. Актуальні питання розслідування кіберзлочинів. Харків, 2013. URL : <http://www.science-community.org/ru/node/16132> (дата звернення: 20.05.2020).
3. Яцик Т. П. Кіберзлочинність: зміст та методи боротьби. *Міжнародний юридичний вісник: актуальні проблеми сучасності (теорія та практика)*. Вип. 1 (5) 2017 с.113. URL : http://archive.nbuv.gov.ua/portal/soc_gum/tppe/2009_19/Zb19_48.pdf.\ (дата звернення: 20.05.2020).
4. Fieldeman A. K Project 2020 Scenarios for the Future of Cybercrime – White Paper for Decision Makers . – 25 p.URL : https://www.europol.europa.eu/sites/default/files/publications/2020_white_paper.pdf. (дата звернення 20.05.2020).
5. Арістова І. В., Запара С. І. Органи місцевого самоврядування як суб'єкти реалізації національної політики розвитку інформаційного суспільства в Україні *Науковий вісник Ужгородського національного університету*, 2017 №.7. URL : http://www.visnyk-juris.uzhnu.uz.ua/file/No.59/part_2/30.pdf (дата звернення: 20.05.2020).
6. Офіційний сайт кіберполіції в Україні: Департамент кіберполіції Національної поліції України\Новини: Кіберполіція викрила чоловіка у розповсюдженні конфіденційної інформації громадян 21 травня 2020 р. 17:36 URL: <https://cyberpolice.gov.ua/news/kiberpolicziya-vykryla-cholovika-u-rozprovsyudzheni-konfidencijnoyi-informacziyi-gromadyan-2300/> (дата звернення: 20.05.2020).

Коваленко М. Д.,

студентка 3-го курсу ІПСА КПІ ім.
Ігоря Сікорського

Науковий керівник: Іщенко В. В.,

викладач кафедри публічного права
КПІ ім. Ігоря Сікорського

ПРОБЛЕМНІ ПИТАННЯ ПРАВОВОГО РЕГУЛЮВАННЯ ІТ-ПІДПРИЄМНИЦТВА В УКРАЇНІ

На сьогодні застосування інформаційних технологій на ринку України є невід’ємною частиною ведення будь-якої підприємницької діяльності. Різні види інформаційних ресурсів все більше перетворюються на предмет майнових відносин. ІТ-технології стрімко розвиваються, а тому виникає низка проблемних питань, пов’язаних із правовим регулюванням ІТ-підприємництва, з якими стикаються підприємці цієї галузі на ринку. Саме тому обрана тема є надзвичайно актуальною для України на сьогоднішній день, адже вирішення цих питань сприятиме розвитку ринку ІТ-технологій в Україні, залученню іноземних інвестицій, і, як наслідок, розвитку економіки в державі.

Сучасні проблеми правового забезпечення підприємницького потенціалу ІТ-сфери стосуються, насамперед, порядку державної реєстрації, нормативно-правового забезпечення захисту авторських прав розробників, системи оподаткування та багато інших, зокрема дотримання гарантій щодо іноземних інвестицій в ІТ-секторі (розділ 2 Закону України «Про режим іноземного інвестування») [1]. За даними Міністерства юстиції України на 2019 р. в Україні зареєстровано близько 173 тисяч фізичних осіб-підприємців (далі – ФОП) в ІТ-сфері [2]. При цьому основним видом діяльності ФОП в ІТ-сфері залишається «Комп’ютерне програмування» (близько 102 тис. спеціалістів). Проте, справжні цифри можуть бути дещо іншими. Це пов’язано, в першу чергу, із наявністю так званих “фрілансерів” – працівників, які виконують роботу віддалено. Найчастіше вони працюють “у тіні” або на іноземні компанії, не оформлюючи

трудові відносини належним чином. Таким чином, у ІТ-спеціалістів виникають проблеми у відносинах з органами державної податкової служби, Пенсійного фонду України, з банками тощо.

Питання легалізації роботи фріланс-працівників залишається актуальною проблемою для законодавства України, адже подібні правовідносини фактично не врегульовані нормативно-правовими актами. В той же час, на міжнародному рівні вже прийнято Конвенцію Міжнародної організації праці про надомну працю № 177 від 20.06.1996 р. [3] та Конвенцію Міжнародної організації праці про гідну працю домашніх працівників (фрілансерів) № 189 від 16.06.2011 р. [4]. Щоправда, Україна досі не тала їх учасницею.

Для вирішення питання співпраці фріланс-працівників з іноземними компаніями існує кілька варіантів. Якщо іноземна компанія не має свого представництва на території України, то фріланс-працівників, які є громадянами України, можна оформити як фізичних осіб-підприємців платників податків 3-ої або 2-ої групи. Альтернативним варіантом є державна реєстрацію нової юридичної особи (наприклад, у формі ТОВ). Наразі, найпоширенішим варіантом, який використовують іноземні компанії для співпраці з українськими спеціалістами, є реєстрація працівників компанії як ФОП, а не укладення з ними трудових договорів. Оформлення працівників компанії як ФОП дозволяє уникнути сплати великих податків, що є вигідним як для працівників, так і для самої компанії. ФОП сплачує лише сплачують 3% від доходу для платників ПДВ або 5% від доходу для неплатників ПДВ (ст. 293 Податкового кодексу України) [5] та 22% від мінімальної заробітної плати (ст. 8 Закону України “Про збір та облік єдиного внеску на загальнообов'язкове державне соціальне страхування”) [6].

Однак, таке “розбиття” компанії на велику кількість ФОП істотно зменшує навантаження на фонд оплати праці, що має наслідком істотне зменшення надходження податків та зборів до бюджетів та державних цільових

фондів. Тому лише за останні два роки було зареєстровано декілька законопроектів щодо зміни оподаткування ІТ-сфери. Наприклад, проектом Закону України № 10094 пропонувалося створити окрему п'яту групу ФОП, спеціально для спеціалістів, що провадять діяльність винятково у сфері інформаційних технологій та поступово збільшити ставку єдиного податку для цієї групи до 10% [7].

Окремої уваги потребують й інші питання, зокрема належна охорона прав інтелектуальної власності на ІТ-продукти. Проте, як в Україні (ст. 8 Закону України «Про авторське право та суміжні права» [8], так і у всьому світі, готові програмні продукти охороняються як літературні твори (зокрема у ст. 4 Договору ВОІВ про авторське право вказано, що комп'ютерні програми охороняються як літературні твори у розумінні ст. 2 Бернської конвенції незалежно від способу або форми їх вираження) [9]. При цьому, самі алгоритми, що лежать в основі створення програмного продукту, захистити як об'єкти прав інтелектуальної власності практично неможливо. Розв'язком цієї проблеми може стати захист алгоритму за допомогою патенту. Якщо алгоритм вже пройшов перевірку на патентоздатність, автор може подати заяву на винахід, і отримати на нього патент. Ще одним способом захистити програмний продукт є охорона його назви шляхом реєстрації торгової марки, назви сайту чи його доменного імені тощо.

Серед розповсюджених проблем в ІТ-сфері можна виділити порушення порядку оплати послуг за договором, наприклад, коли замовника не задовольняють результати виконаної розробником роботи, і він замовник виплачувати кошти, вимагаючи переробити замовлення. У цьому випадку клієнт аргументує свою поведінку тим, що він особисто має права на всі напрацювання розробника і може навіть розірвати договір з ним, так і не виплативши йому кошти. Причиною таких ситуацій є те, що комп'ютерні програми пишуть програмісти, а володіють майновими правами на них

роботодавці або замовники, і останні часто не приділяють належної уваги правильному оформленню майнових прав на програмні продукти. Оскільки проблеми захисту програмних продуктів в Україні так і залишаються невирішеними, в таких ситуаціях слід приділяти особливу увагу умовам договору між замовником та виконавцем.

Важливим також є питання захисту конфіденційної інформації підприємців в ІТ-сфері. Законодавство кожної держави встановлює свої власні, але незмінно жорсткі та конкретні зобов'язання щодо захисту конфіденційної інформації і персональних даних. До такої інформації у компанії можна віднести дані про заробітні плати працівників, клієнтські бази, проекти та алгоритми тощо. Одним зі способів захисту цієї інформації на підприємстві є укладення та підписання угоди про нерозголошення конфіденційної інформації (NDA) з кожним із співробітників, клієнтів, інвесторів, постачальників, підрядників, контрагентів і т.д. Ще одним документальним видом захисту конфіденційної інформації може бути затвердження в організації Положення про захист конфіденційності. Вимога до наявності такого документа найчастіше встановлюється законодавством для компаній, які працюють зі співробітниками за трудовими договорами. З кожного співробітника має бути взято письмове зобов'язання, в якому співробітник вказує, що ознайомився з текстом Положення і зобов'язується не порушувати його норми.

Підсумовуючи наведене вище, можна зробити висновок, що законодавство України не встигає за стрімкими змінами у сфері ІТ-технологій. Це виражається, зокрема, у регулюванні роботи так званих “фрілансерів” (спеціалістів, які працюють дистанційно, а також на зарубіжні компанії). Найпоширенішим варіантом легалізації їх діяльності в Україні на даний час є державна реєстрація цих працівників як ФОП з використанням спрощеної системи оподаткування, обліку та звітності 3-ої або 2-ої групи. Серед інших проблем правового регулювання ІТ-підприємництва можна виділити наступні:

порядок оформлення трудових та договірних відносин ІТ-спеціалістів, правове забезпечення захисту авторських прав розробників, захист конфіденційної інформації. Проблемними питаннями залишаються захист авторських прав на програмні продукти, вирішення яких можливе шляхом внесення відповідних змін до законодавства. На сьогоднішній день, в Україні лише розробляються зміни та деякі доповнення до нормативно-правових документів з цих питань. Подібне доповнення до нормативної бази значно покращить розуміння того, яким чином особи можуть захистити свої права та інтереси при виникненні спірних правовідносин.

Список використаної літератури:

1. Про режим іноземного інвестування: Закон України від 19 березня 1996 р. № 93/96-ВР. URL: <https://zakon.rada.gov.ua/laws/show/93/96-ВР> (дата звернення: 15.05.2020)
2. Скільки податків сплачують українські айтішники URL: https://biz.censor.net.ua/resonance/3176639/sklki_podatkv_splachuyut_ukransk_ayits_hniki (дата звернення: 15.05.2020)
3. Конвенція про надомну працю № 177 від 20 червня 1996 р. URL: https://zakon.rada.gov.ua/laws/show/993_327 (дата звернення: 15.05.2020)
4. Конвенция о достойном труде домашних работников (Конвенция № 189) от 16 июня 2011 р. URL: https://zakon.rada.gov.ua/laws/show/993_530 (дата звернення: 15.05.2020)
5. Податковий кодекс України від 2 грудня 2010 р. № 2755-VI. URL: <https://zakon.rada.gov.ua/laws/show/2755-17> (дата звернення: 15.05.2020)
6. Про збір та облік єдиного внеску на загальнообов'язкове державне соціальне страхування: Закон України від 8 липня 2010 р. № 2464-VI. URL: <https://zakon.rada.gov.ua/laws/show/2464-17> (дата звернення: 15.05.2020)
7. Про внесення змін до Податкового кодексу України (щодо розвитку креативних індустрій в Україні): Проект Закону України від 26 лютого 2019 р. № 10094. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=65564 (дата звернення: 15.05.2020)
8. Про авторське право і суміжні права: Закон України від 23 грудня 1993 р. № 3792-XII. URL: <http://zakon2.rada.gov.ua/laws/show/3792-12/> (дата звернення: 15.05.2020)
9. Договір Всесвітньої організації інтелектуальної власності про авторське право, прийнятий Дипломатичною конференцією 20 грудня 1996 року та положення Бернської конвенції (1971 р.), на які містяться посилання у

Пастушок О. О.,

студентка 3-го курсу ІПСА КПП ім. Ігоря Сікорського

Науковий керівник: Іщенко В. В.,

викладач кафедри публічного права КПП ім. Ігоря Сікорського

ОПОДАТКУВАННЯ ПОСЛУГ В ІТ-СФЕРІ В УКРАЇНІ: ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ РОЗВИТКУ

У сучасних умовах складної економічної ситуації не лише в Україні, а й у всьому світі, на фоні пандемії, спричиненої COVID-19 все актуальнішими стають проблеми оподаткування ІТ-сфери, адже більшість людей, які працюють вдома, за допомогою дистанційної роботи в технологічній сфері, хочуть підвищити свій місячний заробіток, адже витрати значно збільшилися. Сьогодні фріланс доволі популярний, але не варто забувати, про податки.

У сучасному світі інформаційні технології набирають все більшої популярності та охоплюють практично всі сфери бізнесу та життєдіяльності людини. Для України ІТ-сфера – відносно молода галузь, що стрімко розвивається, яка має особливе значення, адже на фоні складних економічних та політичних подій, що відбуваються на теренах України, вона здатна продемонструвати стрімкий розвиток та допомогти в цьому суміжним галузям. Тому сьогодні гостро постає питання оподаткування ІТ, що з однієї сторони збільшить надходження до державного та місцевих бюджетів, а з іншої – загрожує відтоком спеціалістів цієї конкурентоспроможної галузі за кордон.

У галузі нових інформаційних технологій лідирують США, Японія, Канада, Південна Корея, Австралія та ін. Уряди цих країн вважають, що у світі необхідно встановити режим невтручання держави до електронного сегмента

економіки та запровадити мораторій на оподаткування суб'єктів електронної комерції. Незважаючи на те, що сьогодні країни Латинської Америки, включаючи Мексику і Чилі, а також Азії, включаючи Південну Корею і Індію, розглядають можливість введення нових податків на діяльність глобальних високотехнологічних гігантів – таких, як Google і Facebook, відмова від оподаткування електронної комерції у США була головним фактором зростання електронного ринку на етапі її становлення [1, с. 224].

На 2019 р. за даними Міністерства юстиції України в Україні зареєстровано близько 173 тисяч фізичних осіб-підприємців в ІТ-сфері (далі – ФОПів-айтішників) [2]. За даними ДФС України обсяг задекларованих ФОПів-айтішниками доходів за 2019 р. становить лише 5% від загального доходу, який офіційно «засвітили» всі ФОПи України – 12,5 млрд грн [3]. Якщо розглядати ФОПів-айтішників у розрізі КВЕДів, то у з них головну групу, а саме 66% складає «Комп'ютерне програмування», у 17% – «Консультування з питань інформатизації», у 12% – «Оброблення даних» [2].

Нині більшість ФОПів-айтішників використовують спрощену систему оподаткування на умовах 2-ої (якщо річний обсяг доходу не перевищує 1500000 грн., кількість працівників не перевищує 10 осіб) або 3-ї групи (якщо річний обсяг доходу не перевищує 5000000 грн., кількість працівників не обмежено) платників єдиного податку. Платники 2-ої групи сплачують до 20% мінімальної зарплати у розрахунку на календарний місяць Платники 3-ої групи сплачують 3% від доходу для платників ПДВ або 5% від доходу для неплатників ПДВ [4, ст. 399]. У 2020 р. розмір податків для ФОПів підвищився: для I групи платників до 10 % розміру прожиткового мінімуму (210,20 грн. (2102 грн. *10%)), для II групи до 20 % розміру мінімальної заробітної платні (944,60 грн. (4723 грн. * 20%)). Для решти ж груп ставки залишилися не змінними [4].

Однак, були ще інші законопроекти.

Так, проектом Закону України «Про внесення змін до Податкового кодексу України (щодо розвитку креативних індустрій в Україні)» (реєстр. № 10094 від 26.02.2019 р.) пропонувалося створити окрему групу оподаткування – п'яту (за умови отримання доходу до 7500000 грн.) для якої ставка єдиного податку зростатиме щороку на 1% до досягнення 10% від доходу, а єдиний соціальний внесок пропонують збільшити у 2 рази починаючи з 2020 р. – до 22%» від двох мінімальних зарплат [2; 5]. Такі пропозиції викликали невдоволення в ІТ-підприємців [5] і 29.08.2019 р. цей законопроект було відкликано.

Оскільки внесення змін до податкового законодавства не дало ніякого результату, то Кабінет Міністрів України обґрунтовував дані зміни наступним позитивним ефектом для ІТ:

1. забезпечення безпеки ІТ-підприємців від звинувачення їх представниками податкових органів в ухиленні від сплати податків шляхом неправомірного переходу на спрощену систему оподаткування;

2. можливість ІТ-підприємцям і надалі користуватися спрощеною системою оподаткування, що збереже привабливість цього виду бізнесу в Україні для зарубіжних інвесторів [5].

Згідно законопроекту Мінсоцполітики від 6 лютого 2019 р. усі ФОПи повинні закладати з роботодавцями трудовий договір, в якому повинно чітко бути прописано усі умови, від податків до заробітної платні, інакше їх буде притягнуто до кримінальної або адміністративної відповідальності [6].

У ІТ-спеціалістів на це є інше бачення, адже перш за все це означає зменшення їхнього доходу, що несе загрозу суттєвого зменшення фінансового росту індустрії та скоротити обсяги валютної виручки, оскільки близько 45% ІТ-послуг експортуються [5]. У випадку збільшення оподаткування частина ІТ-спеціалістів може втратити бажання працювати в Україні та переїхати до більш

розвинених країн, що спровокує зменшення кількості робочих місць у галузі. Внаслідок такої ситуації економіка України може навпаки постраждати.

На даний час весь світ страждає через пандемію COVID-19 і у зв'язку з цим було послаблено деякі закони, це зачепило також і оподаткування, так відповідно Закону України «Про внесення змін до деяких законодавчих актів України, спрямованих на запобігання виникненню і поширенню коронавірусної хвороби (COVID-19)» від 17 березня 2020 р. № 530-IX було внесено наступні корективи:

За порушення податкового законодавства штрафні санкції не застосовуються.

Встановлено мораторій на проведення документальних та фактичних перевірок.

Річна декларація про майновий стан і доходи за 2019 р. подається до 01 липня 2020 р.

Фізичні особи – підприємці, особи, які провадять незалежну професійну діяльність, та члени фермерського господарства тимчасово звільняються від нарахування та сплати єдиного внеску на загальнообов'язкове державне соціальне страхування

Платникам єдиного внеску не нараховується пеня, а нарахована пеня за ці періоди підлягає списанню [7].

Таким чином, враховуючи дану ситуацію, при збільшенні оподаткування ІТ-технологій на даному етапі його розвитку може негативно вплинути на економіку України та дану галузь в цілому. На нашу думку, українській владі варто перейняти досвід зарубіжних країн на етапі розвитку та становлення ІТ-сфери і підтримати її, а не обтяжувати її податками. В майбутньому, коли Україна вийде з кризи та пандемії, оподаткування цієї галузі зможе принести значно більше доходу та не нести такі загрози, як сьогодні, коли в Україні немає ніяких чинників, щоб стримати вплив спеціалістів за кордон.

Список використаної літератури:

1. Тедеев А. А. Электронная коммерция: правовое регулирование и налогообложение. Москва: Приор-издат, 2002. 224 с.
2. Скільки податків сплачують українські айтишники URL: https://biz.censor.net.ua/resonance/3176639/sklki_podatkv_splachuyut_ukransk_ayits_hniki (дата звернення: 15.05.2020)
3. Віннічук Ю. Скільки айтишників в Україні працює в тіні. URL: https://biz.censor.net.ua/resonance/3114051/sklki_ayitshnikv_v_ukran_pratsyu_v_tn. (дата звернення: 15.05.2020)
4. Про внесення змін до Податкового кодексу України та деяких інших законодавчих актів України щодо покращення адміністрування та перегляду ставок окремих податків і зборів. URL: <https://zakon.rada.gov.ua/laws/show/2628-19> (дата звернення: 15.05.2020)
5. Вінокуров Я. Депутати пропонують підвищити податки для ФОПів, що працюють в ІТ, у 2 рази за 5 років. URL: <https://hromadske.ua/posts/deputati-proponuyut-pidvishiti-podatki-dlya-fopiv-sho-pracyuyut-v-it-u-2-razi-za-5-rokiv>. (дата звернення: 15.05.2020)
6. Про внесення змін до деяких законодавчих актів України щодо посилення захисту прав працівників та протидії застосуванню незадекларованої праці. URL: <https://www.msp.gov.ua/projects/401/> (дата звернення: 15.05.2020)
7. Пільги в оподаткуванні під час карантину (COVID-19). URL: <http://vektor.if.ua/articles/2011-10-18-14-34-15/502-povyny> (дата звернення: 15.05.2020)

Філіпов М. В. ,

студент факультету соціології і права, КПП
ім. Ігоря Сікорського

Науковий керівник: Солончук І. В.,

ст. викладач кафедри інформаційного
права та права інтелектуальної власності
КПП імені Ігоря Сікорського

ПРАВОВИЙ СТАТУС ХМАРНИХ СЕРВІСІВ ТА ПРОБЛЕМИ ЇХ ВИКОРИСТАННЯ

У сучасному світі технології розвиваються з надзвичайною швидкістю. Дедалі частіше трапляються ситуації, коли люди опановують, поступово звикають до певної технології чи програми тоді, коли ця технологія вже стає

неефективною, застарілою, несумісною з іншими технічними рішеннями (засобами). Крім того, такий стрімкий розвиток технологій не дає можливості українському законодавцю врегулювати, узагальнити, визначити на законодавчому рівні правовий статус та особливості тих чи інших технологій. Одним зі способів припинення цих "перегонів" є хмарні обчислення. Однак, на сьогодні, чинним законодавством України не визначено конкретно, що таке - хмарні технології, хмарні сервіси та хмарні обчислення. Це породжує цілу низку доволі очевидних проблемних питань:

Що таке - хмарний сервіс, технологія, обчислення?

Яке законодавство маємо застосовувати до правовідносин, що виникають у зв'язку з використанням хмарних сервісів?

Суб'єкти і об'єкти цих правовідносин? Що вважати, власне, предметом послуги хмарного сервісу?

Які гарантії безпеки хмарних технологій? Як захистити свої права у разі втрати особистої інформації чи її протиправного поширення?

Проблематику використання хмарних технологій та сервісів, їх технічну захищеність та системний аналіз переваг і недоліків даної технології у своїх наукових працях досліджували, зокрема, Брижко В. М., Фурашев В. М., Юдін О. К., Аулов І. Ф., Горбенко І. Д., Гладківська О. В. та інші вчені. Міжнародна спільнота також не оминає таку проблематику. Згідно зі щорічним рейтингом BSA Global Cloud Computing Scorecard за 2018 рік, 24 провідні країни, відповідно до своїх стратегій розвитку хмарних технологій, визначають такі основні завдання у цій галузі: забезпечення всієї території країни високошвидкісним інтернетом, надання доступу і реальної можливості для всіх громадян користуватися цим інтернетом, приватність даних, захист даних у хмарі від протиправних втручань, вільний ринок хмарних послуг, захист права інтелектуальної власності [1] . У дослідженнях визначають основні ризики та

переваги використання хмарних технологій у бізнес-сфері [2]. Визначається юридичний аспект використання хмарних сервісів у Європейському Союзі [3].

Метою дослідження є з'ясування змісту поняття "хмарні сервіси", їх основні ознаки, суб'єктний склад правовідносин пов'язаних з наданням хмарних послуг та визначення проблем, що існують у зв'язку з відсутністю законодавчого закріплення правового статусу цих сервісів.

Хмарні обчислення(англ. *Cloud Computing*) - модель забезпечення повсюдного та зручного доступу на вимогу через мережу до спільного пулу обчислювальних ресурсів, що підлягають налаштуванню (наприклад, до комунікаційних мереж, серверів, засобів збереження даних, прикладних програм та сервісів), і які можуть бути оперативно надані та звільнені з мінімальними управлінськими затратами та зверненнями до провайдера [4].

Хмарний сервіс – це, власне, послуга, яка полягає у наданні доступу до обчислювальних ресурсів через мережу інтернет на певних, визначених суб'єктом надання таких послуг умовах, з обов'язковою платою або ж без такої. Найпопулярнішими прикладами хмарних сервісів є "Google Disk", "Dropbox" "OneDrive" та "iCloud". Основною функцією даних сервісів є збереження інформації, яку завантажив користувач на своїх серверах та надання доступу до неї користувачу з будь-якого пристрою, що має доступ в інтернет: планшет, ноутбук, персональний комп'ютер, смартфон, навіть можна використати комп'ютер в бібліотеці. Якщо спробувати дати загальну характеристику хмарним сервісам то серед їх основних ознак можна виділити:

це послуга оренди: користувач лише орендує певні обчислювальні потужності на певний час;

користувач не повинен турбуватися про саме оснащення, яке надає обчислювальні потужності; користувач навіть не знає де воно знаходиться і як працює;

єдиною умовою доступу до хмарних сервісів є наявність інтернет-з'єднання. Плата часто не є обов'язковою, так наприклад, "Google Disk" надає своїм користувачам 15 Гб хмарного сховища абсолютно безкоштовно і платити потрібно лише за наступні розширення цього обсягу сховища;

хмарні сервіси є надзвичайно гнучкою і доступною технологією, ви можете користуватися ними хоч з смартфона, хоч з ноутбуку або навіть з комп'ютера який знаходиться у громадському просторі (бібліотека);

хмарні сервіси гарантують збереженість ваших даних і захист прав інтелектуальної власності.

У законодавстві України на сьогодні відсутні спеціальні норми, які б регулювали суспільні відносини пов'язані з використанням хмарних сервісів, проте така робота ведеться. Так, проектом Закону від 23 березня 2016 р. група народних депутатів запропонувала внести зміни у ЗУ "Про захист інформації в інформаційно-телекомунікаційних системах"[5]. Цей проект якраз і був покликаний врегулювати правовідносини у сфері надання хмарних послуг. Зокрема, вносилися наступні пропозиції:

порядок доступу до інформації, яка обробляється в системі хмарних обчислень, визначається у договорі, укладеному між надавачем хмарних послуг та володільцем інформації або власником системи;

надавач хмарних послуг забезпечує захист інформації в системі хмарних обчислень, а також надання володільцю інформації або власнику системи відомостей щодо захисту інформації в системі хмарних обчислень від внутрішніх та зовнішніх загроз, кібератак, в порядку та на умовах, визначених цим Законом та договором щодо надання хмарних послуг;

надавач хмарних послуг надає користувачеві відомості про правила і режим роботи системи хмарних обчислень та забезпечує йому відповідно до визначеного договором порядку доступ до інформації в цій системі;

вперше визначалися такі поняття як: надавач хмарних послуг; користувач хмарних послуг; захист інформації в системі чи системі хмарних обчислень; доступ до інформації в системі чи системі хмарних обчислень; несанкціоновані дії щодо інформації в системі чи системі хмарних обчислень;

інформація, у тому числі інформація з обмеженим доступом (крім інформації, яка в установленому порядку віднесена до державної таємниці), може оброблятися в системі хмарних обчислень на підставі договору, укладеного між надавачем хмарних послуг та володільцем інформації або власником системи. Визначені істотні умови такого договору.

На нашу думку зміни, які запропоновані даним проектом, є цілком виправданими і можуть бути основною для подальшої розробки законодавства у цій галузі. Завдяки таким змінам можна буде однозначно визначити, що відносини, пов'язані з наданням послуг хмарного сервісу, є цивільними, здійснюються на підставі договору. Визначено, що суб'єктами цих відносин є як фізичні, так і юридичні особи, причому надавачем може бути і нерезидент України. Також встановлено обов'язки надавача і користувача. Гарантується безпека і передбачена відповідальність надавача послуг за втрату інформації. Відповідальність за порушення умов договору чи за завдану шкоду буде відшкодовуватися в порядку цивільного судочинства. Завдяки таким змінам з'явиться і судова практика, яка буде гарантувати захист прав людини у цій сфері. На даний час проект очікує на друге читання.

Висновки. Проаналізувавши поняття і загальні ознаки хмарних сервісів, недоліки і переваги можемо зробити висновок, що, незважаючи на явні переваги цієї технології, залишається відкритим питання захисту даних користувача. Національне законодавство щодо регулювання таких відносин і стратегія впровадження таких технологій в Україні потребують доопрацювання. На нашу думку, технологія має більше переваг, ніж недоліків, і тому необхідно

розробити національні стандарти, стратегію, положення про розвиток хмарних технологій в Україні.

Хмарні технології мають цілу низку особливостей, які якісно відрізняють їх від інших інформаційних систем, зокрема це їх доступність, легкість у використанні, цілковита незалежність від оснащення користувача, спосіб оплати таких послуг (підписка). Проте є і явні недоліки: залежність від якісного інтернет-з'єднання; можливість витоку чи втрати даних з сервера; неможливість користувача визначити особливі умови користування, модель поширення передбачає одного надавача і багатьох користувачів, які обирають лише з певного переліку заздалегідь визначених умов (тарифів).

Відсутність законодавчої бази значно ускладнює захист прав і свобод людини, порушення яких пов'язане з використанням хмарних сервісів. На сьогодні у суді можливо посилатися лише на норми договору про надання хмарних послуг і на загальні норми цивільного права, що не є цілком достатнім для таких правовідносин.

Без законодавчої бази неможливе широке впровадження хмарних технологій у сферу державного управління, освіти, медицини, тощо. А враховуючи те, що хмарні технології не потребують значних коштів та модернізації матеріально-технічної бази, таке впровадження, на нашу думку, було б цілком доцільним. До речі, перехід держави одразу на масове використання хмарних технологій зможе зекономити значні кошти, адже на момент такого переходу ми запозичимо одразу останню версію цієї технології, якісну, усталену, напрацьовану і покращену технологію, яку ми зможемо впровадити в Україні. Не потрібно витрачати ресурси на усунення недоліків цієї технології, не потрібно буде розробляти систему "з нуля", а лише потрібно адаптувати її.

Список використаної літератури:

1. BSA Global Cloud Computing Scorecard, 2018 рік, веб-сайт. URL: <https://cloudscorecard.bsa.org/2018/> (дата звернення: 20.05.2020).
2. Sai Gadia, «How to manage five key cloud computer risks», KPMG LLP, 2018. URL: <https://assets.kpmg/content/dam/kpmg/ca/pdf/2018/03/cloud-computing-risks-canada.pdf> (дата звернення: 20.05.2020).
3. Patrick Van Eecke Partner, DLA Piper Brussels, 2013, Cloud computing legal issues. URL: https://www.isaca.org/Groups/Professional-English/cloud-computing/GroupDocuments/DLA_Cloud%20computing%20legal%20issues.pdf (дата звернення: 20.05.2020).
4. The NIST Definition of Cloud Computing, NIST Special Publication 800-145, 2011. URL: <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf> (дата звернення: 20.05.2020).
5. Про внесення змін до деяких законодавчих актів України щодо обробки інформації в системах хмарних обчислень: Проект Закону від 24 березня 2016 р. № 4302. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_2?pf3516=4302&skl=9 (дата звернення: 20.05.2020).
6. Юдін О. К., Зюбіна Р. В. Нормативно-правові аспекти використання хмарних технологій. *НАУ: Наукоємні технології*, 2014. № 3 (23). URL: <http://jrn1.nau.edu.ua/index.php/SBT/article/view/7405/8440> (дата звернення: 20.05.2020).
7. Аулов І. Ф., Горбенко І. Д. Хмарні обчислення та аналіз питань інформаційної безпеки в хмарі. *Прикладная радиоэлектроника*. 2013. Т. 12, № 2. С. 194 - 201. URL: http://nbuv.gov.ua/UJRN/Prre_2013_12_2_5. (дата звернення: 20.05.2020).
8. Гладківська О .В. Вплив хмарних технологій на стан інформаційної безпеки: правовий аспект. *Інформація і право*. № 3(12)/2014. URL: <http://ippi.org.ua/sites/default/files/14govbpa.pdf> (дата звернення: 20.05.2020).

Кустарёва Е. М.,

студентка 3-го курса ФТИ КПИ им. Игоря
Сикорского

Научный руководитель : Фурашев В. М., к.

т. н., КПИ им. Игоря Сикорского

СУЩЕСТВЕННЫЙ РОСТ АКТУАЛЬНОСТИ ИТ ПРОФЕССИИ В СВЯЗИ С ИЗМЕНЕНИЕМ СОЦИАЛЬНЫХ ВЗАИМООТНОШЕНИЙ

История развития информационных войн – это история развития человечества, история борьбы цивилизаций. Немало примеров побед и поражений в конкретных сражениях, когда ситуация резко изменялась благодаря какой-нибудь военной хитрости, целенаправленно распространенной дезинформации. Доведение информации до определенного лица или группы лиц и получение от этого выигрыша – информационная операция, являющаяся элементом информационной войны в которой на данный момент, как никогда раньше, участвует Украина.

Информационная война - процесс противоборства человеческих общностей, направленный на достижение политических, экономических, военных или иных целей стратегического уровня, путём воздействия на гражданское население, власти и (или) вооружённые силы противостоящей стороны, посредством распространения специально отобранной и подготовленной информации, информационных материалов, и, противодействия таким воздействиям на собственную сторону. Современная информационная война обретает все более самостоятельный характер, нанося все больший вред психологическому и моральному состоянию людей.

Однако, именно современные реалии дают мощный толчок развитиям современной ИТ индустрии, которая и так прочно вошла во все сферы деятельности : от мелкого бизнеса до гигантов современной промышленности, политики, медицины.

Виртуальный мир небезопасен, потому как люди самостоятельно сливают туда тонну личной информации, пропаганды, именно поэтому специальности кибербезопасность и *криптография* как никогда актуальны в данное время.

Защита информации – мера предосторожности, способ избежать утечки важной информации, что в свою очередь помогает предотвращать массовую дезинформацию.

Брюс Шнайер -специалист, который построил карьеру на способах защиты информации, считается лучшим криптографом в данной сфере, часто отмечает успехи Украины в своих работах.

Зачатки данных специализаций были заложены на момент Великой Отечественной войны. На сегодня функции и потенциал технологий стремительно прогрессируют и буквально кишат уязвимостями. Хакеры или взломщики торгуют информацией, и, профессионал в области информационной безопасности по сути тот же хакер, действующий в рамках закона. Белые хакеры востребованы на рынке труда, что подчеркивает нехватку перспективных на практике профессионалов.

Защита систем, сетей и программных приложений от цифровых атак становится все более актуальной и сложной задачей. С каждым днем хакеры совершенствуют свою стратегию и тактику, генерируют новые виды угроз, придумывают более изощренные лазейки, чтобы достучаться «до клиента».

По данным исследования McAfee и CSIS, мировой ущерб от хакерских атак уже достигает \$600 млрд в год.

Цифровой мир проник почти в каждый аспект нашей жизни.

Теперь преступления стали более прибыльными, менее рискованными и никогда не были настолько легкими.

«В отместку» мир вооружается против хакеров. Недавно стало известно, что девять стран ЕС намерены создать группы быстрого реагирования для противодействия кибератакам в рамках нового пакта об обороне Евросоюза.

По словам соучредителя платформы Hacken, CEO Information Security Group Егора Аушева, новый толчок для развития кибербезопасности даст недавно вступивший в силу Общий регламент о защите персональных данных (GDPR).

Теперь все компании в мире, в том числе и в Украине, обязаны должным образом сохранять персональные данные граждан и компаний ЕС. Штрафы в случае утечки информации достигают миллионов евро.

«К сожалению, в большинстве случаев наш бизнес начинает совершенствоваться после болезненных пинков: успешные атаки хакеров побуждают компании задумываться о защите. К счастью, в Украине уже есть зрелые компании, которые внедряют подходы

риск-менеджмента и управляют киберрисками, не только приобретая программное и аппаратное обеспечение, а и выстраивая планы по киберустойчивости бизнеса», – рассказывает операционный директор компании 10Guards Виталий Якушев.

Самое главное, по его мнению – не потратить бюджет на приобретение продуктов и услуг, а эффективно инвестировать в безопасность, чтобы каждая вложенная копейка работала.

Украинские предприятия стали увеличивать бюджет на кибербезопасность после свершившихся инцидентов. Они послужили катализатором. Компании прочувствовали значение

«утечки информации» и «кибератаки», которые ранее были в области теории. Три масштабные кибератаки 2017 года очень хорошо продемонстрировали бизнесу, какие могут быть последствия. И после них рынок начал стремительно расти.

Уже в 2020 году мировой ущерб от киберпреступлений может достигнуть \$2 трлн, а затраты компаний на защиту от хакеров – \$100 млрд. С каждым годом мы оцифровываем все больше сфер жизни и бизнеса, повсеместное используем интернет вещей. И всем этим цифровым «помощникам» нужна будет защита от несанкционированного доступа. Помимо битв человеческого интеллекта, будут бои так называемых искусственных интеллектов, как со стороны кибербезопасников, так и со стороны киберпреступников.

Наступающая эра интернета вещей несет новые риски и вызовы.

В поле киберугроз будет попадать все больше «персоналий». Мы станем наблюдать атаки, направленные не только против машин или информации, а и на подмену значений.

С каждым годом число проблем будет возрастать, появятся новые протоколы, стандарты, увеличится объем кода.

«Не существует универсальных технических средств, которые бы решали данные проблемы, потому востребованными будут оставаться правильно организованная система управления информационной безопасностью и технические компетенции», – отмечает менеджер по защите информации ДТЭК.

«Пинком» для роста отрасли в Украине становятся и законодательные нормативы. «В нашей стране только недавно – в 2017 году – был принят первый в истории независимости закон «Об основах кибербезопасности». В дальнейшем станут появляться и новые законы, и регулирования, которые будут привлекать к ответственности лиц за халатное отношение к кибербезопасности. Это приведет к росту затрат компаний на эту сферу и увеличению спроса на сотрудников».

Команды DCUA из ФТИ КПИ чемпионами мира 2016 года на соревнованиях CTF, где соревнуются лучшие в мире «белые» хакеры.

Спрос и уровень обучения криптографии растёт с каждым годом.

Уровень дохода таких специалистов в разы отличается от многих профессий в нашей стране. Так как рынок испытывает дефицит качественных специалистов, оплата услуг растет. Конечно, она зависит от технических знаний и опыта, наличия международных сертификатов и т.д. Однако, абсолютно неоспоримый факт, что именно профессия IT-специалиста актуальна как никогда и остается профессией будущего для многих поколений.

Список используемой литературы :

1. Международный журнал прикладных и фундаментальных исследований.
2. <https://applied-research.ru/ru/article/view?id=10880>
3. Егор Аушев. "Хакнуть" мозг легче, чем взломать сайт ЦИК. https://zn.ua/interview/egor-aushev-haknut-mozg-legche-chem-vzlomat-sayt-cik-337812_.html
4. Эксперт по кибербезопасности: По 10-балльной шкале Украина защищена максимум на 3,5–4 балла. <https://gordonua.com/tags/vitalij-jakushev.html>
5. Основные принципы обеспечения кибербезопасности Украины. <https://uteka.ua/publication/news-14-delovye-novosti-36-osnovnye-obespecheniya-kiberbezopasnosti-ukrainy>

Жук В. А.,

студентка 3-го курсу ІІСА КІІ ім. Ігоря Сікорського

Науковий керівник: Іщенко В. В.,

викладач кафедри публічного права КІІ ім. Ігоря Сікорського

**КІБЕРБЕЗПЕКА ТА ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ
В УКРАЇНІ В УМОВАХ ПАНДЕМІЇ COVID-19**

Світова пандемія COVID-19 серед інших загострила питання кібербезпеки, адже кризові ситуації традиційно викликають активізацію різноманітних хакерських атак. У вітчизняній та зарубіжній юридичній науці досі триває пошук оптимальної моделі правового механізму регулювання відносин з використання персоніфікованої інформації, захисту персональних

даних, яка узгоджувалася б з міжнародно-правовими стандартами та гарантувала б ефективний захист прав і свобод людини та громадянина.

Кібербезпека – це поняття, під яким розуміється захист цілісності комп’ютерних систем, апаратного забезпечення, програмного забезпечення та даних, в тому числі персональних, від комп’ютерних атак та інших загроз, які можуть виникнути в процесі ведення бізнесу. Кібербезпека покликана захистити дані на етапі їх обміну та збереження. До таких заходів безпеки входять контроль доступу, навчання, аудит та оцінка ризиків, тестування, управління та безпека авторизації [1].

Згідно ст. 2 Закону України «Про захист персональних даних»: «Персональні дані – це відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована» [2]. Об’єктом правового захисту в даному випадку є персональні дані. Під персональними даними, на нашу думку, слід розуміти інформація, яка стосується фізичної особи, що була ідентифікована або може бути ідентифікована. До цих даних належать, наприклад, прізвище, ім’я, поштова та електронна адреси, номер телефону, а також інформація, яка обов’язково формується при відвіданні веб-сторінки (наприклад, початок та завершення відвідування, обсяг переглянутих даних тощо).

Д. Дубов виділяє 4 ключові кібербезпекові тренди, які можуть призвести до зростання кіберзагроз, на фоні розгортання пандемії COVID-19:

- збільшення кількості людей, які працюють віддалено (використовуючи ІТ, але не маючи належних знань та досвіду);
- збільшення електронних платежів (що збільшує увагу шахраїв);
- збільшення кількості випадків фішингових атак;
- потенційна можливість для інформаційних та кібератак з метою дестабілізації ситуації [3].

Кіберзлочинність постійно вдосконалюється і йде в ногу з технологіями.

Це ускладнює виявлення та протидію зазначеним протиправним діям. Тому варто усвідомити, що проблема кібербезпеки – це проблема не лише загальнодержавного рівня, а й кожної окремо взятої юридичної особи [4].

Міністерство цифрової трансформації України опрацьовує можливість проведення додаткових роз'яснювальних заходів з питань кіберграмотності (кібергігієни) та особистої кібербезпеки для громадян вікових груп 45+, які внаслідок вжиття карантинних заходів можуть перейти на віддалений режим роботи з використанням цифрових засобів, а також інформує всі вікові категорії про базові правила безпеки використання електронних засобів розрахунків в мережі Інтернет [5].

7 квітня 2020 р. було презентовано ноу-хау в Україні у сфері обробки персональних даних в умовах пандемії COVID-19 – додаток «Дій вдома». В його основу було покладено зарубіжний досвід країн, які використовують цифрові інструменти для забезпечення безпеки громадян в період пандемії COVID-19. Мета додатку «Дій вдома» – моніторинг дотримання процесу самоізоляції тими, хто наразі повернувся з-за кордону або хто лікується вдома чи хто має підозру на коронавірус, а також мав близькі контакти з хворими. Додаток надає переваги на час самоізоляції, але його встановлення є добровільним [6].

Функціонал додатку «Дій вдома»:

- підтвердження місця проходження самоізоляції з визначенням геолокації;
- фотопідтвердження перебування за місцем проходження самоізоляції;
- екстрений виклик на гарячу лінію МОЗ України;
- запланований функціонал для моніторингу розвитку симптомів [7].

Законом України «Про внесення змін до Закону України «Про захист населення від інфекційних хвороб» щодо запобігання поширенню коронавірусної хвороби (COVID-19)» від 13 квітня 2020 р. № 555-IX було дозволено обробку персональних даних без згоди особи, зокрема, даних про

стан здоров'я, місце госпіталізації, місце проживання та роботи особи – даних про місця, в яких хворий проводив багато часу до госпіталізації, дотримання особою зобов'язання про перебування в карантині (самоізоляції) [8].

На думку Д. Дубова, пандемія COVID-19 загострила ще декілька питань, які можуть мати довгостроковий вимір:

По-перше, кіберпостереження та права людини. Уряд шукає можливостей збільшення точності відслідковування як вже заражених людей, так і тих, з ким вони мали контакти. В тому числі – з використанням сучасних технологій. Однак найбільші можливості для такого виявлення можуть входити в конфлікт із правами людини.

По-друге, система охорони здоров'я (включаючи елементи поставок в ній) набуває нового значення як критична інфраструктура. Хоча і раніше елементи системи охорони здоров'я відносили до критичної інфраструктури, однак зараз фокус такого віднесення зміщується: від розуміння критичності як місця циркуляції чутливих персональних даних пацієнтів до об'єктів, від яких залежить життя значних мас людей. При цьому рівень кіберзахисту таких об'єктів часто є незадовільним. Слід визнати, що за оцінками незалежних експертів ІТ української системи охорони здоров'я також не мають належного рівня захисту (водночас рівень залученості ІТ-систем до критичних процесів в українських реаліях менша ніж у розвинених країнах) [3].

На даний момент ворожа кіберактивність, яка може бути класифікована як така, що здійснюється іншими державами, повною мірою не підтверджується, хоча занепокоєння мають певну фактичну основу [4].

Підсумовуючи наведену вище інформацію, можна вказати наступне:

По-перше, експерти виділяють 4 ключові кібербезпекові тренди, які можуть призвести до зростання кіберзагроз, на фоні розгортання пандемії COVID-19:

- збільшення кількості людей, які працюють віддалено (використовуючи ІТ,

але не маючи належних знань та досвіду);

- збільшення електронних платежів, що привертає увагу шахраїв;
- збільшення кількості випадків фішингових атак;
- потенційна можливість для інформаційних та кібератак з метою дестабілізації ситуації.

По-друге, очікувано зростає фішингова діяльність хакерських угруповань. Водночас найбільш небезпечні групи, які є операторами вірусів-вимагачів, намагаються дистанціюватись від такої діяльності на даному етапі (вочевидь, не бажаючи привертати надмірну увагу правоохоронних органів та спецслужб).

По-третє, найбільшу потенційну небезпеку може становити стрімке збільшення кількості працівників, які працюють віддалено і використовують для цього ІТ, оскільки часто такі люди не мають відповідних навичок кібербезпеки, а ступінь кіберзахисту домашніх пристроїв не є надто високим. Це призводить до потенційного зростання кількості кіберінцидентів.

На нашу думку, потрібно ініціювати підготовку рекомендацій щодо посилення кіберзахисту об'єктів медичної інфраструктури (з урахуванням реальної епідеміологічної ситуації), а також проводити додаткові роз'яснювальні заходи з питань кіберграмотності (кібергігієни) та особистої кібербезпеки для громадян.

Список використаної літератури:

1. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 р. № 2163-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2163-19> (дата звернення: 12.05.2020)
2. Про захист персональних даних: Закон України від 1 червня 2010р. № 2297-VI. URL: <https://zakon.rada.gov.ua/laws/show/2297-17> (дата звернення: 12.05.2020).
3. Дубов Д. COVID-19: ключові кібербезпекові тренди. URL: <https://niss.gov.ua/doslidzhennya/informaciyna-politika/covid-19-klyuchovi-kiberbezpekovi-trendi> (дата звернення: 12.05.2020).

4. Співробітництво Україна – ЄС – НАТО з протидії гібридним загрозам у кіберсфері. Київ, 2019. 28 с. URL: <https://geostrategy.org.ua/ua/analitika/item/1565-cooperation-ukraine-nato> (дата звернення: 12.05.2020).

5. Комітет з питань цифрової трансформації позитивно оцінив роботу Міністерства цифрової трансформації. URL: <https://rada.gov.ua/news/Novyny/189264.html> (дата звернення: 12.05.2020).

6. Додаток «Дій вдома». URL: <https://play.google.com/store/apps/details?id=ua.gov.diia.quarantine&hl=ru> (дата звернення: 12.05.2020).

7. Як працює застосунок «Дій вдома». URL: <https://www.kmu.gov.ua/news/yak-pracyuye-zastosunok-dij-vdoma> (дата звернення: 12.05.2020).

8. Про внесення змін до Закону України «Про захист населення від інфекційних хвороб» щодо запобігання поширенню коронавірусної хвороби (COVID-19): Закон України від 13.04.2020 № 555-IX. URL: <https://zakon.rada.gov.ua/laws/show/555-20> (дата звернення: 12.05.2020)

Зарічний Я. С.,

студент 3-го курсу ІПСА КПІ ім. Ігоря Сікорського

Науковий керівник: Іщенко В. В.,

викладач кафедри публічного права КПІ ім. Ігоря Сікорського

ПРАВОВЕ РЕГУЛЮВАННЯ ОРГАНІЗАЦІЇ КОВОРКІНГУ В ІТ-СФЕРІ В УКРАЇНІ

Коворкінг (англ. Co-working – «спільна робота») – це модель організації роботи людей з різним типом зайнятості в єдиному робочому просторі. Основна суть коворкінгу – територіальне об'єднання та організація спільноти для більш ефективної роботи учасників [1]. Коворкінг сприяє розвитку стартап-культури (культура, яка будується або на основі нових інноваційних ідей або технологій, що щойно з'явилися), надаючи не тільки всю необхідну інфраструктуру для розвитку нового проекту і створюючи певну творчу атмосферу, а й формуючи креативне співтовариство, члени якого можуть увійти в новий стартап-проект.

Коворкінг-центр є новим робочим простором для представників сучасних креативних та інноваційних професій, зокрема, інтернет-працівники, які включають велику кількість різних сфер: програмування, дизайн тощо [2, с. 118]. Модель коворкінгу якнайкраще підходить для людей, які займаються творчою діяльністю. Компанія-організатор коворкінгу отримує чимало переваг:

1. Відхід від сфери регулювання трудового права, оскільки особи, які здійснюють певну діяльність для суб'єкта господарювання, укладають цивільно-правові чи господарські договори.
2. Податкове навантаження на фахівців у статусі підприємця значно нижче, ніж найманих за трудовим договором працівників.
3. Обмежена матеріальна відповідальність.
4. Повна відповідальність виконавця за зобов'язання, наприклад, за розголошення комерційної таємниці – демонстрацію креслень, схем.
5. Свобода діяльності, що якнайкраще підходить для представників творчих професій.
6. Партнерські відносини сторін господарського договору чи договору цивільно-правового характеру.

Модель коворкінгу найкраще підходить для бізнесу з високою часткою інтелектуальної та творчої праці:

1. ІТ-фахівці, які прагнуть перейти на новий рівень, об'єднатися із суміжними фахівцями для виконання великих проектів, зекономити на організаційних витратах.
2. ІТ-компанії, що створюють певний програмний продукт та реалізують його як власники майнових прав, надають ліцензії.
3. Інноваційно-технологічні компанії – стартапи, проектні, експериментальні, дослідницькі команди, конструкторські або технологічні бюро, що тестують, створюють, удосконалюють матеріальні та нематеріальні продукти.

4. IT-аутсорсинг – компанії, які розробляють програмне забезпечення на замовлення, підтримують його, чи надають інші схожі послуги.

5. Сервіси з інтелектуальною та творчою складовою – дизайн, маркетинг, пошук та навчання персоналу, зв'язки з громадськістю, управлінський консалтинг, аудиторські та юридичні сервіси.

6. Девелопери – учасники ринку нерухомості [3].

Коворкінг – це фактично «оренда» робочих місць (офісів та/або офісного обладнання). Строки такої «оренди» можуть коливатися у діапазоні від кількох годин до кількох років залежно від потреби конкретного «орендаря». «Орендодавці» (коворк-центри) – це власники коворк-офісів, які надають коворкерам робочі місця на певний строк і за плату. «Орендарі» (коворкери) – це фізичні або юридичні особи, які орендують коворк-офіси, аби виконувати в них свою роботу. Така форма організації праці дозволяє коворкерам оптимізувати свої витрати. Адже все частіше зустрічаються працівники (найчастіше фрілансери), які працюють дві-три години на день, тому утримувати власні офіси для них недоцільно. Також є працівники (і компанії) із сезонним характером діяльності, які не хочуть утримувати власний офіс цілий рік. Послуга коворкінгу задовольняє потребу цих «вільних художників» у наявності робочого місця рівно на стільки часу, на скільки це потрібно.

Юридична особа, яка вирішила зайнятися коворкінгом, перш за все постає перед необхідністю врегулювати питання цієї діяльності у правовій площині. Чинне законодавство не містить визначення терміна «коворкінг». Але це не становить суттєвої проблеми. Адже неважливо, як називається діяльність, важливо те, що за своєю суттю вона передбачає надання в оренду об'єктів нерухомого та/або рухомого майна. Відтак загальні принципи, якими керується підприємство, яке вирішило зайнятися коворкінгом, цілком можна взяти із гл. 58 «Найм (оренда)» Цивільного кодексу України (далі – ЦК України) [4]. За договором оренди орендодавець (у нашому випадку – коворк-центр) передає

або зобов'язується передати орендарю (у нашому випадку – коворкеру) майно у користування за плату на певний строк (ч. 1 ст. 759 ЦК України) [4]. Тож оренду робочих місць цілком можна оформляти за допомогою договору оренди. Адже предметом договору оренди може бути річ, яка визначена індивідуальними ознаками і яка зберігає свій первісний вигляд при неодноразовому використанні (ч. 1 ст. 760 ЦК України) [4]. Крім того, надання коворкерам офісного обладнання, можна розглядати як договір прокату (ч. 1 ст. 787 ЦК України) [4]. Тобто як надання у користування рухомих речей для задоволення потреб коворкерів (ст. 788 ЦК України) [4]. Здебільшого коворк-центри (колективні офіси) на практиці обмежуються прокатом чи орендою винятково офісного обладнання (комп'ютер, стіл, стілець тощо). Якщо укладено договір прокату обладнання – письмової форми він не потребує. Адже договір прокату – це публічний договір, який є договором приєднання (ст. 787 ЦК України) [4].

У випадку оренди обладнання письмовий договір оренди обов'язково укладати тільки тоді, коли коворкер – юридична особа (ч. 1 ст. 208 ЦК України) [4]. Якщо ж коворкер – фізособа і він згоден на усну форму договору, то надавати в оренду йому офісне обладнання, в принципі, можна і без письмового договору оренди. При цьому бажано, аби він сплачував за оренду безпосередньо перед тим, як стати до роботи на орендованому ним робочому місці. Це дасть підстави вважати, що правочин повністю виконано в момент вчинення (ч. 1 ст. 206 ЦК України) [4]. Усна форма правочину підійде здебільшого для короткострокової оренди робочих місць (наприклад, оренда комп'ютера на одну-дві години). А коли коворкер орендує (а не бере у прокат) ваше офісне обладнання більше ніж на один день, рекомендується все-таки укласти договір у письмовій формі.

Іноді трапляються випадки, коли коворкер орендує для роботи саме приміщення (або його частину), але привозить на робоче місце своє обладнання.

Прикладами таких коворкерів можуть бути перукар, стоматолог, косметолог, масажист та інші подібні працівники. Їм для роботи потрібен «дах над головою», а обладнання у них або своє, або його взагалі немає. У такому випадку без письмового договору оренди не обійтися. Адже договір оренди будівлі або іншої капітальної споруди (чи їх окремої частини) обов'язково укладається у письмовій формі (ч. 1 ст. 793 ЦК України) [4]. У випадку, якщо одночасно надаються в оренду коворкеру як приміщення, так і приладдя для роботи, можна укласти із ним змішаний договір (ч. 2 ст. 628 ЦК України) [4], аби не укладати окремо договори на оренду приміщення та обладнання, яке потрібне коворкеру для виконання роботи.

Зі змісту ст. 759 ЦК України випливає, що істотними умовами договору оренди є строк і ціна [4]. Строк оренди робочого місця, як правило, визначається побажанням коворкера (орендаря), залежно від його потреби, хоча орендодавець (коворк-центр) може встановити мінімальний строк оренди (одна година, один день тощо). Ціна послуги з коворкінгу визначається орендодавцем (коворк-центром) залежно від тих же факторів, що й при будь-якій іншій оренді [1].

Таким чином, організація коворкінгу надає чимало переваг усім сторонам. Для суб'єктів господарювання головна із них – зменшення податкового тиску на їх бізнес. Замовник послуг чи робіт підписує з підрядниками договори цивільно-правового характеру чи господарські договори. Він отримує бажаний результат, підтверджений актами наданих послуг чи виконаних робіт, та проводить оплату. Замовник не несе серйозної відповідальності за виконавців, як це було б, якби працівники виконували роботу за трудовим договором. Він також не сплачує податки та збори за виконавця, оскільки останній як ФОП сплачує їх самостійно. Популярність коворкінгів зростає у всьому світі, зокрема і в Україні. Одна з причин цього – зростання ціни на оренду комерційних приміщень [3].

Отже, виходячи із сказаного вище, до переваг коворкінгу слід віднести співтовариство та нетворкінг. На нашу думку, спільний офіс сприяє пошуку нових бізнес-контактів, постійному обміну ідеями і досвідом, професійному розвитку. Зібрати команду під потужний проект, знайти менторську допомогу в такому офісі значно легше, ніж робити це самостійно. Цьому, на нашу думку, сприяють настрій на позитивне вирішення необхідного завдання, відсутність контролю зверху, згуртоване за інтересами співтовариство створюють сприятливе середовище для роботи. До недоліків коворкінгу можна віднести час і кошти, потрібні на дорогу до коворкінг-центру і у зворотному напрямку, необхідність дотримання особистої безпеки, шум і відволікаючі події, характерні для громадського місця. Таким чином, коворкінг може виступати не тільки як форма організації праці індивідуальних самозайнятих працівників, а й як робочий простір для юридичних осіб, які хочуть одночасно поліпшити умови праці та створити ділову обстановку для роботи і навчання з мінімальними витратами.

Список використаної літератури:

1. Нестеренко М. Коворкінг (оренда робочих місць): облік. Податки & бухоблік. 2018. № 33. Квітень. URL: <https://i.factor.ua/ukr/journals/nibu/2018/april/issue-33/article-35972.html> (дата звернення: 12.05.2020).
2. Снігур Х. Коворкінг: переваги та недоліки в організації робочих місць. Вісник Тернопільського національного економічного університету. 2017. № 4. С. 117–124. URL: <http://visnykj.tneu.edu.ua/index.php/htneu/article/viewFile/974/1081> (дата звернення: 12.05.2020).
3. Яновський О. Особливості, вигоди та моделі організації коворкінгу в ІТ-галузі, між ФОПами або самозайнятими людьми. URL: <https://zkg.ua/osoblyvosti-vyhody-ta-modeli-orhanizatsiji-kovorkinhu-iz-samozajnyatymy-lyudmy/> (дата звернення: 12.05.2020).
4. Цивільний кодекс України від 16 січня 2003 р. № 435-IV. URL: <https://zakon.rada.gov.ua/laws/show/435-15> (дата звернення: 12.05.2020).

Купрієнко С. П.,

студентка 3-го курсу ФБМІ КПІ ім.

Ігоря Сікорського

Науковий керівник: Іщенко В. В.,

викладач кафедри публічного права КПІ

ім. Ігоря Сікорського

СОЦІАЛЬНІ МЕРЕЖІ ЯК ОБ'ЄКТ ПРАВОВОГО РЕГУЛЮВАННЯ

У 2020 р. комунікаційне агентство Plusone надало інформацію про кількість користувачів найпопулярніших соціальних мереж в Україні, а саме “Facebook” та “Instagram”. Кількість користувачів соціальної мережі “Facebook” в Україні склала 14 мільйонів. Наступною за чисельністю користувачів в Україні є «Instagram» – 11,5 мільйонів [1]. Якщо взяти світову статистику, то Facebook переглядають більше двох мільярдів користувачів щомісяця [2].

Соціальна мережа – це онлайн платформа, яка об'єднує людей для спілкування, обміну інформацією та ідеями. Необхідно лише зазначити, що Інтернет-мережа – це більше соціальне, а не технічне явище, і відразу постає питання необхідності та доцільності регулювання відносин, що виникають на веб-сайтах та в соціальних мережах.

На думку К.В. Єфремової: «Інтернет-відносини – це новий тип суспільних відносин, що виникають та змінюються у кіберпросторі. Це не правові і не фактичні відносини в чистому вигляді. Це соціальні зв'язки особливої правової, інформаційної та технічної природи» [3, с. 8]. Тому можна зробити висновок, що соціальні мережі – це масштабні платформи, які об'єднують велику кількість людей, між якими виникають певні відносини. Ці відносини називають інтернет-відносинами. Вони потребують особливої уваги і вироблення нових підходів до їх врегулювання.

Інтернет-відносини – це відносини, що пов'язані з правовим регулюванням інформаційного віртуального простору. Основні правовідносини,

які виникають при функціональному використанні соціальних мереж повинні регулювати такі питання:

- 1) регулювання змісту (тобто відбір контенту).
- 2) попередження кіберзлочинності.
- 3) захист персональних даних, конфіденційної інформації, інтелектуальної власності.
- 4) врегулювання прав при здійсненні електронної комерції (тобто торгівлі).
- 5) захист прав споживачів.
- 6) захист прав людини [4, с. 7].

Правове регулювання соціальних мереж фактично відсутнє. Це так звана “сіра зона” з точки зору законодавства. На сьогодні світова спільнота не може дійти єдиного висновку в питанні регулювання правовідносин в Інтернеті: одні наполягають на правовому регулюванні, яке б здійснювали відповідні державні органи, інші – дотримуються думки, що Інтернет – це остання зона свободи людства, тому вона повинна залишатися саморегульованою, і держава не повинна туди втручатися.

На сьогодні жодна країна світу не має повного та кодифікованого законодавства, яке регулює правовідносини в Інтернеті. В основному існують лише нормативні акти, які регулюють такі питання, як інформаційна безпека, зміст інформації, захист авторського права та ін. Наприклад, в Україні Закони України «Про інформацію», «Про телебачення і радіомовлення», «Про друковані засоби масової інформації в Україні» – це ті законодавчі акти, що визначають порядок створення та організації діяльності друкованих та аудіовізуальних засобів масової інформації. Протягом 2016-2017 рр. в Україні активно розроблялася нормативно-правова база, яка мала на меті врегулювання правовідносин в інформаційній мережі. Було прийнято Закони України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 р. та «Про електронні довірчі послуги» від 05.10.2017 р. Проте, ці та ряд інших законів не

здатні регулювати правовідносини в соціальних мережах.

Регулювання соціальних мереж здійснюється також на європейському рівні. Так, у 2004 р. було створено Європейське агентство інформаційної мережевої безпеки ENISA. У 2013 р. сформовано Європейський центр боротьби з кіберзлочинністю. В Європі діють Конвенція про кіберзлочинність від 23 листопада 2001 р. та Директива ЄС щодо мережевої та інформаційної безпеки 2016 р.

Розглянемо найпоширенішу проблему, з якою зустрічаються в соціальних мережах – порушення інтелектуальної власності. Відповідно до п. 9 ч. 3 ст. 15 Закону України «Про авторське право і суміжні права» право на дозвіл чи заборону використання твору іншими особами шляхом подання своїх творів до загального відома публіки таким чином, що її представники можуть здійснити доступ до творів з будь-якого місця і у будь-який час за їх власним вибором, є виключним правом автора (чи іншої особи, яка має авторське право) [5]. Якщо порушення буде зареєстровано через окремий веб-сайт, то в судовому порядку можна буде отримати дані правопорушника, але якщо порушення буде зареєстровано в соціальній мережі, то це є організаційно складним завданням. Враховуючи прив'язку найпопулярніших в Україні соціальних мереж до іноземного Інтернет-сегменту, знайти інформацію про правопорушника майже неможливо. Звичайно, соціальні мережі розробляють певні алгоритми перевірки опублікованої інформації, але вони не дають гарантії врегулювання інтернет-відносин відповідно до державних норм.

Але все ж правовідносини в соціальних мережах повинні бути врегульовані. Лише виникає питання: «В якому випадку держава через норми права має втручатись у сферу свободи Інтернету?». Оскільки право – це гарантована законом міра свободи людини, а при цьому права особи закінчуються там, де вони починають порушувати права іншого індивіда [6, с. 3], очевидно, що держава має регулювати діяльність соціальних мереж тільки в

тому випадку, коли надходять скарги від громадян про порушення їх прав.

Предметом адміністративно-правових правовідносин є різноманітні матеріальні та особисті нематеріальні блага, які становлять публічну цінність [7, с. 32]. Суб'єктами публічного управління в цій сфері є публічна адміністрація, яка здійснює адміністративно-правове регулювання соціальних Інтернет-мереж. Об'єктами публічного управління є засновники, автори аудіовізуального контенту, їх посередники [8, с. 34] та користувачі таких мереж. Якщо звернутися до законодавства, щоб з'ясувати, які блага суб'єктів адміністративного права у сфері адміністративно-правового регулювання соціальних Інтернет-мереж, на думку законодавця, потребують захисту нормами адміністративного права, то відповіді на ці питання ми в ньому не знайдемо.

Таким чином, можна зробити висновок, що Інтернет – це одночасно технічна і соціальна система, яка об'єднує велику кількість людей, в результаті чого виникають інтернет-відносини. Тому регулювати правові відносини, зокрема в соціальних мережах, повинні як розробники соціальної мережі (за допомогою технічної бази розробляти певні алгоритми, які б регулювали зміст, забезпечували захист персональних даних, прав інтелектуальної власності), так і держава. На сьогодні певні норми щодо регулювання соціальних мереж містяться в різних галузях права, зокрема в цивільному, адміністративному та кримінальному законодавстві. Проте, цих норм не достатньо для врегулювання правових відносин в соціальних мережах. Правове регулювання соціальних мереж має здійснюватися з урахуванням інтересів усіх зацікавлених учасників правових відносин. Також держава повинна розробити судові та позасудові механізми, які б регулювали захист прав та свобод людини в соціальних мережах.

Список використаної літератури:

1. Facebook та Instagram в Україні. URL: <https://plusone.com.ua>

/research/Facebook%20та%20Instagram%20в%20Україні%20(січень%202020)_U
A.pdf (дата звернення 11.05.2020).

2. Найпопулярніші соціальні мережі світу (2019) та рейтинг України.
URL: <https://futurenow.com.ua/21-najpopulyarnishyh-sotsialnyh-merezh-svitu-ta-rejtyng-ukrayiny/> (дата звернення 11.05.2020).

3. Єфремова К. В. До перспектив правового регулювання інтернет-правовідносин: господарсько-правовий аспект. Право та інноваційне суспільство. 2014. № 1 (2). С. 5–11. URL: <http://apir.org.ua/wp-content/uploads/2014/11/Yefremova.pdf> (дата звернення 11.05.2020)

4. Бабкин С. А. Право, применяемое к отношениям, возникающим при использовании сети Интернет. Москва: АО Центр ЮрИнфор, 2003. 68 с.

5. Про авторське право і суміжні права: Закон України від 23 грудня 1993 р. № 3792-XII. URL: <https://zakon.rada.gov.ua/laws/show/3792-12> (дата звернення 11.05.2020)

6. Основні права людини: навч. посіб. / Ю. М. Бисага, М. М. Палінчак, Д. М. Белов, М. М. Данканич. Ужгород, 2003. 66 с.

7. Середа В. В., Кісіль З. Р., Кісіль Р.-В. В. Адміністративне право: навч. посіб. Львів: ЛьвДУВС, 2014 [2015]. 520 с. URL: <http://dspace.lvduvs.edu.ua/handle/1234567890/241> (дата звернення 11.05.2020)

8. Іншин М. І. Сучасний стан та шляхи удосконалення взаємовідносин органів державної влади і засобів масової інформації. Матеріали Міжнародної науково-практичної конференції “Інформаційне суспільство в Україні: інформаційно–правова культура, освіта, наука”, присвяченої Всеукраїнському Дню інформаційного суспільства (16-17 травня 2008 р., м. Суми, Україна), Суми: Видавництво “Довкілля”, 2008. С. 33–38.

Чинник П. А.,

студент 3-го курсу ІПСА КПП ім. Ігоря
Сікорського

Науковий керівник: Іщенко В. В., викладач
кафедри публічного права КПП ім. Ігоря
Сікорського

ПРАВОВЕ РЕГУЛЮВАННЯ ІНФОРМАЦІЙНОЇ ПРИВАТНОСТІ

З моменту появи у 1981 р. персонального комп'ютера захист інформаційної приватності та персональних даних потребує нових законів та їх постійного вдосконалення, тому що інформаційні технології не стоять на місці, а весь час

розвиваються дуже швидкими темпами.

Приватність – це одна із фундаментальних категорій прав людини, які визнані у всьому світі, закріплена в ст. 12 Загальної декларація прав людини ООН від 10 грудня 1948 р. [1] та ст. 17 Міжнародного пакту про громадянські і політичні права від 19 жовтня 1973 р. [2]. Приватність тісно пов'язана з людською гідністю, свободою слова, свободою асоціацій тощо.

Інформаційна приватність – це приватність, що включає в себе встановлення правил збору та обігу персональних даних, таких як інформація кредитних установ та медичні записи [3].

Зростання інтересу до інформаційної приватності почалося у 60-70 рр. ХХ ст. з появою більш компактних комп'ютерів та автоматизованих систем. Через це з'явилися потенційні можливості для стеження з допомогою потужних комп'ютерних систем, а тому потрібно було ставити на перший план вимоги встановлення спеціальних правил щодо збору та обігу інформації особистого характеру. Першим законодавчим документом у світі у цій сфері був Закон про захист даних, який було введено в дію на землі Гессен в Німеччині в 1970 р.

На міжнародному рівні було прийнято два надзвичайно важливих документи, які почали регулювати інформаційну приватність: Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних від 28 січня 1981 р. [4] та Правила забезпечення захисту приватності у зв'язку із транскордонним переміщенням інформації про особу, встановлені Організацією Економічного Співробітництва та Розвитку (ОЕСР) від 24 жовтня 1995 р. [5], якими визначено спеціальні вимоги стосовно обігу електронних даних. Важливу роль відіграє також Регламент Європейського Парламенту і Ради (ЄС) 2016/679 про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних) (англ. General Data Protection Regulation, GDPR) від 27 квітня 2016 р. [6], що набрав чинності 25 травня 2018 р. Цей нормативний

акт детально визначає фактичну сферу його застосування, територіальну дію, основні принципи, пов'язані з обробкою персональних даних, його мету, термін набрання чинності тощо. Регламент є обов'язковим у повному обсязі та підлягає прямому застосуванню у державах-членах ЄС.

В Україні забезпечення конфіденційності персональних даних регулюють Конституція України, Закони України “Про захист персональних даних”, “Про інформацію”, рішення Конституційного Суду України тощо. Основна роль у формування механізму правового захисту персональних даних людини й громадянина розкривається через конституційні засади, що містяться у ст. 3, 28, 30, 31, 32, 34, 35, 41, 54, 55, 64 Конституції України. Відсутність у тексті Конституції України спеціально визначеного права на захист персональних даних не є перешкодою для визнання цього права предметом конституційного захисту, оскільки такий захист передбачений комплексом положень конституційних норм Розділу II Основного Закону [7]. Відповідно до рішень Конституційного Суду України у справі щодо офіційного тлумачення ст. 3, 23, 31, 47, 48 Закону України “Про інформацію” та статті 12 Закону України “Про прокуратуру” (справі К. Г. Устименка) від 30 жовтня 1997 р. № 5-зп та у справі за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України від 20 січня 2012 р. № 2-рп/2012: “...забороняється не лише збирання, але й зберігання, використання та поширення конфіденційної інформації про особу без її попередньої згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту, прав та свобод людини” [9; 10].

В Україні основним нормативно-правовим актом, який регулює правила поводження з персональними даними є Закон України “Про захист персональних даних”, відповідно до ст. 2 якого: «персональні дані – це відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути

конкретно ідентифікована» [8]. Таке визначення, на нашу думку, є недосконалим, оскільки в ньому на концептуальному рівні відсутні критерії, за якими можна відрізнити персональні дані від будь-якої іншої інформації (наприклад, конфіденційної інформації про особу).

Таким чином, Україні потрібно приводити своє законодавство у відповідність до норм законодавства Європейського Союзу, оскільки останнє більш чітко врегульовує процедуру зберігання та доступ до персональних даних людини. Також необхідно дати більш чітке визначення персональних даних в Законі України “Про захист персональних даних”. На нашу думку, в Україні є необхідність у прийнятті окремого закону, який би регулював приватність людини в Інтернеті, щоб компанії не зловживали збором персональних даних користувачів і не заробляли гроші на цьому без їх дозволу.

Список використаної літератури:

1. Загальна декларація прав людини: Прийнята і проголошена резолюцією 217 А (III) Генеральної Асамблеї ООН від 10 грудня 1948 р. URL: https://zakon.rada.gov.ua/laws/show/995_015 (дата звернення: 12.05.2020).
2. Міжнародний пакт про громадянські і політичні права від 19 жовтня 1973 р. URL: https://zakon.rada.gov.ua/laws/show/995_043 (дата звернення: 18.05.2020)
3. Приватність і права людини / підгот. Д. Банісар, С. Девіс. URL: <http://library.khpg.org/index.php?id=928437562> (дата звернення: 12.05.2020).
4. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних від 28 січня 1981 р. URL: https://zakon.rada.gov.ua/laws/show/994_326 (дата звернення: 12.05.2020).
5. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31995L0046> (Last accessed: 12.05.2020).
6. Регламент Європейського Парламенту і Ради (ЄС) 2016/679 про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний

регламент про захист даних) від 27 квітня 2016 р. URL: https://zakon.rada.gov.ua/laws/show/984_008-16 (дата звернення: 12.05.2020).

7. Головченко В. Правові основи захисту персональних даних. Юридична газета. 2018. 5 вересня. № 36 (638). URL: <https://yur-gazeta.com/publications/practice/inshe/pravovi-osnovi-zahistu-personalnih-danih.html> (дата звернення: 12.05.2020).

8. Про захист персональних даних: Закон України від 1 червня 2010 р. № 2297-VI. URL: <https://zakon.rada.gov.ua/laws/show/2297-17> (дата звернення: 12.05.2020).

9. Рішення Конституційного Суду України у справі щодо офіційного тлумачення статей 3, 23, 31, 47, 48 Закону “Про інформацію” та статті 12 Закону України “Про прокуратуру” (справа К. Г. Устименка) від 30 жовтня 1997 р. № 5-зп (справа № 18/203-97). URL: <https://zakon.rada.gov.ua/laws/show/v005p710-97> (дата звернення: 12.05.2020).

10. Рішення Конституційного Суду України у справі за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України від 20 січня 2012 р. № 2-рп/2012. URL: <https://zakon.rada.gov.ua/laws/show/v002p710-12> (дата звернення: 12.05.2020).

Морозов Р. Д.,

студент 3-го курсу ІПСА КПП ім. Ігоря Сікорського

Науковий керівник: Іщенко В. В.,

викладач кафедри публічного права КПП ім. Ігоря Сікорського

КОНЦЕПТУАЛЬНІ НАПРЯМКИ ПРАВОВОГО РЕГУЛЮВАННЯ КРИПТОВАЛЮТ В УКРАЇНІ

Криптовалют (тобто цифрових валют, що функціонують завдяки механізму асиметричного шифрування) у світі налічується декілька тисяч, але найвідомішою є Bitcoin (біткойн). В Україні останнім часом підвищилася увага до Bitcoin через стрімке зростання їхніх цін. Кількість криптовалют, доступних в Інтернеті станом на 10 березня 2020 р., становить більше 2,3 тис. і їх кількість

росте [1]. У Міністерстві фінансів України зазначають, що точної статистики щодо криптовалют в Україні немає, однак там вважають, що, за експертними оцінками, обсяги операцій з криптовалютами в Україні є достатньо високими. У 2017 році Україна входила в ТОП-10 країн світу за кількістю користувачів віртуальних валют. За експертними оцінками, розмір сегмента Майнінг в Україні перевищує 100 млн. доларів США на рік. Обсяг проведення ICO / ІТО компаній з українським походженням або розміщенням команд розробників в 2017-2018 рр. близько 100 млн. доларів [2].

На сьогодні в Україні відсутнє правове регулювання діяльності, пов'язаної з криптовалютами, зокрема, не врегульовано їх правовий статус, оподаткування операцій з ними, можливості укладення смарт-контрактів (контракт, що укладається за допомогою спеціального комп'ютерного алгоритму і виконання якого здійснюється в автоматичному режимі) . Як наслідок, ринок криптовалют в Україні значною мірою розвивається “в тіні”.

У Міністерстві фінансів України вважають, що легалізація операцій з криптовалютами може принести додаткові можливості для розвитку української економіки. Водночас ризиків того, що криптовалюти використовуватимуть для відмивання коштів, менше. На думку колишнього міністра фінансів України О.С. Маркарової: “Наші злочинці і корупціонери досить консервативні і досі тримають кошти здебільшого у готівці. Тому у легалізації криптовалют я бачу можливості для розвитку цієї галузі у нашій країні, а не загрозу” [3]. У свою чергу у 2018 р. Мінекономрозвитку ініціювало ухвалення Концепції державної політики у сфері віртуальних активів, метою якої є створення зрозумілих умов для ведення діяльності у сфері віртуальних активів та віртуальних валют (криптовалют) [4]. Департамент кіберполіції Національної поліції України з посиланням на керівника департаменту кіберполіції С. Демедюка теж підтримує ідею легалізації криптовалюти і повідомляє, що де-факто криптовалюта за всіма ознаками може ставитися до електронних грошей [5].

Офіційна позиція Національного банку України за операціями з Bitcoin абсолютно категорична. Так, в роз'ясненні “Щодо правомірності використання в Україні “віртуальної валюти/криптовалюти” Bitcoin” від 10.11.2014 НБУ вказує: “Відповідно до Конституції України (ст. 99), Цивільного кодексу України (ст. 192), Закону України “Про платіжні системи та переказ коштів в Україні” (ст. 3), гривня, як грошова одиниця України, є єдиним законним платіжним засобом на території України. Тільки гривня приймається всіма фізичними та юридичними особами без будь-яких обмежень на всій території країни для здійснення будь-яких переказів і розрахунків” [6]. Згідно ч. 2 ст. 32 Закону України “Про Національний банк України” випуск та обіг інших грошових одиниць і використання грошових сурогатів, як одного із способів платежів забороняється [7]. Тому НБУ офіційно розглядає “віртуальну валюту/криптовалюту” як грошовий сурогат, який не має забезпечення реальної вартості. Звідси неможливість використання зазначеної одиниці фізичними та юридичними особами на території України як засобу платежу. НБУ акцентує увагу і на те, що всі ризики по використанню в розрахунках “віртуальної валюти/криптовалюти” Bitcoin несе тільки учасник розрахунків по ним. У той же час з себе, як регулятора ринку фінансових послуг в країні, Нацбанк знімає відповідальність за можливі ризики і втрати, пов'язані з використанням такої системи платежів [6].

Позицію НБУ повністю підтверджує висновок експерта Bitcoin Foundation Г. Андерсена, який радить звичайним людям поки триматися подалі від Bitcoin. Дослідник говорить про фінансові труднощі, пов'язані з використанням Bitcoin, а також порівнює цифрову валюту з раннім Інтернетом і нарікає на незахищеність комп'ютерів і даних, що зберігаються на них, від шахрайських дій в процесі здійснення операцій. Експерт стверджує, що такий порядок речей тимчасовий, однак його слід перечекати [8].

Незважаючи на чітку позицію Національного банку України та багато

негативних відгуків про роботу системи, заперечувати світовий досвід і розвиток Bitcoin в практиці міжнародних валютних розрахунків нерозумно. Відмовлятися від використання електронних грошей через їх потенційну небезпеку та схильності до шахрайських дій також не розумно. Єдиним вирішенням такої проблеми є створення ефективної системи контролю над переміщенням Bitcoin. Природно, це процес не швидкий і дуже клопіткий. Однак для цього можна використовувати вже працюючу практику іноземних держав. Так, наприклад, в США була запущена перша в світі ліцензована криптовалютна біржа [9], яка зібрала чимало інвестицій. Багато експертів покладають великі надії на її діяльність і розраховують на те, що саме вона зможе принести біткоїну першу офіційну легітимність.

Виходячи з вищезазначеного, встановлення чітких правил роботи ринку криптовалют в Україні має усунути проблеми «криптовиків» в роботі з банками. Створення зрозумілих правил гри стане благом як для користувачів, так і для держави в цілому. Учасники ринку мають проблему з відкриттям банківських рахунків. Банкам важливо перестати боятися криптобізнесу, для чого потрібні зрозумілі правила від державного регулятора. Як тільки регулятор дозволить, у криптобізнесу відразу з'явиться можливість відкривати банківські рахунки. Правила потрібні, щоб учасники ринку могли нормально працювати з банківською системою, щоб не треба було вигадувати цілі платежів, які маскують реальну діяльність, і простий громадянин міг через банк зайти на біржу, відправити гроші за купівлю або продаж криптовалюти.

Офіс ефективного регулювання спільно з Міністерством цифрової трансформації та ключовими блокчейн-асоціаціями розробляють законодавчу базу щодо легалізації криптовалюти в Україні [10], в результаті чого криптовалюти нарешті зможуть бути легалізовані в Україні. Такі активи б'ють рекорди популярності у світі та мають величезний потенціал для економічного зростання. Передові держави вже розробили законодавство для blockchain-

сфери, яка тепер працює на їхню економіку, за зрозумілими і прозорими правилами. Нарешті й Україна має шанс забезпечити законодавчу базу для розвитку ринку.

Список використаної літератури:

1. Цит. за: Список криптовалют. URL: https://uk.wikipedia.org/wiki/Список_криптовалют#cite_note-1 (дата звернення: 12.05.2020).
2. Пальчевский И. Як працює ринок криптовалют в Україні. URL: <https://finclub.net/ua/analytics/yak-pratsiuie-rynok-kryptovaliut-v-ukraini.html> ((дата звернення: 12.05.2020).
3. Болотова К. Перевірятимуть менше, але каратимуть жорсткіше: міністр фінансів Оксана Маркарова про оновлений фінмоніторинг. URL: <https://mc.today/pereviryatimut-menshe-ale-karatimut-zhorstkishe-ministr-finansiv> - oksana-makarova-pro-onovlenij-finmonitoring/ (дата звернення: 12.05.2020).
4. Мінекономрозвитку ініціює легалізацію криптовалют в Україні. URL: <https://www.me.gov.ua/News/Detail?id=2cc04fa0-3577-49c7-a465-bd0fc3f61bed> (дата звернення: 12.05.2020).
5. Киберполиция поддерживает идею легализации криптовалюты. URL: <https://interfax.com.ua/news/economic/480819.html> (дата звернення: 12.05.2020).
6. Щодо правомірності використання в Україні “віртуальної валюти/криптовалюти” Bitcoin: Роз’яснення Національного банку України від 10.11.2014. URL: <https://zakon.rada.gov.ua/laws/show/n0435500-14> (дата звернення: 12.05.2020).
7. Про Національний банк України: Закон України від 23.05.2020 № 679-XIV. URL: <https://zakon.rada.gov.ua/laws/show/679-14> (дата звернення: 12.05.2020).
8. Сяміна Д. 5 ризиків операцій з криптовалютами – до якого суду звертатися, якщо зіткнулися із шахраями? URL: https://yaadvokat.com/news/1/5_rizikiv_operacij_z_kriptovalyutami-_do_yakogo_sudu_zvertatisya_yakscho_zitknulisya_iz_shahrayami?.html (дата звернення: 12.05.2020).
9. Coinbase стал первой лицензированной торговой площадкой для криптовалюты в США. URL: <https://www.kommersant.ru/doc/2654872> (дата звернення: 12.05.2020).
10. У Мінцифри готують законопроекти щодо легалізації криптовалют. URL: <https://business.ua/news/7000-u-mintsifri-gotuyut-zakonoproekti-shchodo-legalizatsiji-kriptovalyuti> (дата звернення: 12.05.2020).
