

Міністерство освіти і науки України
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Навчально-науковий центр інформаційного права та правових питань
інформаційних технологій
Кафедра інформаційного права та права інтелектуальної власності
Науково-дослідний інститут інформатики і права
Національної академії правових наук України

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

Матеріали другої науково-практичної студентської конференції

18 листопада 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 другої наук.-практ. студ. конф., м. Київ, 18 листоп. 2020 р. / Упоряд. : В. М. Фурашев, С. Ю. Петраєв, О. А. Самчинська. – Київ : КПІ ім. Ігоря Сікорського», Вид-во «Політехніка», 2020. – 96 с.

ISBN 978-966-990-015-9

Матеріали другої конференції присвячені розгляду питань впливу пандемії коронавірусу COVID-19 на права, свободу і безпеку людини в інформаційній сфері через вісім місяців спроб її подолання.

Участь у конференції взяли виключно студенти, переважно Київського політехнічного інституту імені Ігоря Сікорського різних спеціальностей та спеціалізації.

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

Матеріали подано в авторській редакції.

Упорядники: В. М. Фурашев, С. Ю. Петраєв, О. А. Самчинська

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 № 5 від 24.11.2020 р.

Вченою радою Науково-дослідного інституту інформатики і права

Національної академії правових наук України.

Протокол № 11 від 03.12.2020

ISBN 978-966-990-015-9

© Національний технічний університет України
«Київський політехнічний інститут імені Ігоря
Сікорського», 2020

© Науково-дослідний інститут інформатики і права
НАПрН України, 2020

© Колектив авторів, 2020

Наукове видання

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

Матеріали другої науково-практичної студентської конференції

18 листопада 2020 р.

*За редакцією авторів
Надруковано з оригінал-макета замовника*

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Свідоцтво про державну реєстрацію: серія ДК № 5354 від 25.05.2017 р.
просп. Перемоги, 37, м. Київ, 03056

Підп. до друку 08.12.2020. Формат 60×84¹/₁₆. Папір офс. Гарнітура Times.
Спосіб друку – електрографічний. Ум. друк. арк. 5,58. Обл.-вид. арк. 8,12. Наклад 20 пр.
Поз. 20-3-3-007. Зам. № 20-107.

Видавництво «Політехніка» КПІ ім. Ігоря Сікорського,
вул. Політехнічна, 14, корп. 15.
м. Київ, 03056
Тел. (044) 204-81-78

ЗМІСТ

Ковтко Ю. А., Вплив карантинного та посткарантинного періодів на забезпечення конституційних прав і свобод людини в інформаційній сфері.....	5
Ланкін С. В., Вплив карантинного та посткарантинного періодів на роль та місце інформаційної безпеки в системі забезпечення конституційних прав і свобод людини в інформаційній сфері.....	8
Водько Ю. В., Забезпечення конституційних прав і свобод людини в інформаційній сфері в умовах карантину.....	12
Радзівська А. Є., COVID-19 – «смертоносний» вірус чи всепланетна паніка.....	16
Долматов І. О., Виклики інформаційній безпеці спричинені пандемією коронавірусу COVID-19.....	20
Шпак І. В., Кібербезпека під впливом пандемії та карантинного режиму.....	22
Тутов В. А., Перехід на дистанційне навчання та безпека веб-ресурсів.....	24
Огер А. К., Вплив карантинного режиму на освітянську сферу в Україні.....	28
Пастушак Д. В., Застосунок для комплексного пошуку злочинного контенту на веб-сайтах з використанням інструментів Big Data.....	30
Калиновська В. В., Інтелектуальні системи кіберзахисту мереж електропостачання та їх надійність.....	33
Дудка В.О., Проблема фейків під час пандемії коронавірусу.....	37
Нагорний М. Ю., Проблема фейків в соціальних мережах та ЗМІ в період карантину.....	39
Головатюк О. А., Вплив карантинного періоду на соціальні мережі та ЗМІ.....	43
Безпалько С. О., Інформаційна культура і морально-етичні норми в соціальних мережах та ЗМІ в період карантину.....	45
Морозов-Леонов О. С., Вплив пандемії коронавірусу на культуру спілкування у соціальних мережах.....	49

Воротинцев П. І., Інформаційна культура «нетрадиційних» засобів масової інформації в період карантину.....	51
Музика О. А., Проблематика приватності громадян в умовах пандемії коронавірусу COVID-19.....	55
Ніколюк А. В., Реалізація права подружжя на свободу та особисту недоторканість в умовах карантину.....	59
Шведа К. О., Вплив карантинного періоду на захист персональних даних в мережі Інтернет.....	63
Кісіль А. В. Ризики втрати персональних даних в умовах карантинного та посткарантинного режиму.....	65
Ярош І. С., Балінська В. О., Особливості використання мобільних додатків та механізми захисту персональних даних особи в умовах пандемії Covid-19.....	69
Куніцька З.Е., Конфіденційність персональних даних у мобільних додатках боротьби з Covid-19: особливості підходів у різних державах світу.....	73
Костенко А. Г., Наслідки впливу карантинного режиму на трансформаційні процеси суспільних відносин.....	77
Водько Ю. В., Обмеження права вільно збирати, зберігати, використовувати і поширювати інформацію в інтересах національної безпеки.....	79
Кухрівський Денис Наслідки впливу карантинного режиму на трансформаційні процеси суспільних відносин.....	82
Ткаченко О. О., Соціальна інженерія у період пандемії.....	86
Бурдело Є. В., Методика моніторингу чутливих даних об'єкта критичної інфраструктури на основі відкритих джерел.....	89
Соболь Н. О., Кіберзлочинність в умовах пандемії COVID-19.....	92

Ковтко Ю. А.,
факультет інформатики та
обчислювальної техніки.
Науковий керівник:
Самчинська О.А., викладач.

ВПЛИВ КАРАНТИННОГО ТА ПОСТКАРАНТИННОГО ПЕРІОДІВ НА ЗАБЕЗПЕЧЕННЯ КОНСТИТУЦІЙНИХ ПРАВ І СВОБОД ЛЮДИНИ В ІНФОРМАЦІЙНІЙ СФЕРІ

Права людини як броня – вони захищають нас;
вони як правила – говорять нам, як себе поводити;
і вони як арбітри – ми можемо до них звертатися.
Вони абстрактні – як емоції, і як емоції
вони належать всім й існують,
що б навколо не відбувалося [1].

Останні три місяці стали безпрецедентними в сучасній історії людства. Це неймовірно, але ще на початку 2020 року ніхто навіть уявити собі не міг з яким викликом зустрінеться кожна особа, громадянин, незважаючи від свого місця перебування. Вірус COVID-19 поширився на всіх континентах планети, окрім Антарктиди, вразивши 3,5 млн людей (станом на 04.05.2020). Кожна країна світу вирішувала конкретно для себе, які приймати міри для захисту населення від пандемії COVID-19, орієнтуючись на рекомендації Всесвітньої організації охорони здоров'я [2], які стосуються попередження по запобіганню розповсюдження вірусу. І, як не парадоксально, але виявилось, що для цього найкраще, що люди можуть зробити – це триматись подалі один від одного. Що і було впроваджено урядами багатьох країн (не всіх) у вигляді запровадження режиму самоізоляції, карантину, подекуди надзвичайно суворого (Італія, Іспанія), подекуди добровільного, самовідповідального, а подекуди – з введенням загальнонаціональної комендантської години (Шрі-Ланка, Турецька Республіка), надзвичайної ситуації (деякі області України, Австралія, деякі штати США), надзвичайного стану (Чехія, деякі штати США , Естонія) .

І тут людство постало перед новим викликом. Постала проблема забезпечення конституційних прав і свобод людини в даних умовах, зокрема і в інформаційній сфері. На важливість даної проблеми вказує і резолюція ПАРЄ «COVID-19 – ефективна відповідь із забезпеченням прав людини» від 01.04.2020 (Social Affairs, Health and Sustainable Development) [3] . Розглянемо що ж відбувається з даною проблематикою в Україні.

У нас ключовими для окреслення прав і свобод людини щодо інформаційної сфери є положення Конституції України [4] та документ, що вводить певні обмеження – це Постанова Кабінету Міністрів від 11.03.2020 р. № 211 Про запобігання поширенню на території України гострої респіраторної хвороби COVID-19, спричиненої коронавірусом SARS-CoV-2 [5] :

Конституція України	Постанова Кабінету Міністрів від 11.03.2020 р. № 211 Про запобігання поширенню на території України гострої респіраторної хвороби COVID-19
1	2
1. Стаття 23: Кожна людина має право на вільний розвиток своєї особистості.	Забороняється : – проведення всіх масових (культурних, розважальних, спортивних, соціальних, релігійних, рекламних та інших) заходів; – роботу суб’єктів господарювання, яка передбачає приймання відвідувачів, зокрема закладів громадського харчування (ресторанів, кафе тощо), торговельно-розважальних центрів, фітнес-центрів.
2. Стаття 31. Кожному гарантується таємниця листування, телефонних розмов, телеграфної та іншої кореспонденції.	Жодної додаткової заборони щодо даних прав немає.
3. Стаття 32. Ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України. Не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного	Відповідно до підпункту 1 пункту 2 розділу II “Прикінцеві та перехідні положення” Закону України від 13 квітня 2020 р. № 555-IX “Про внесення змін до Закону України “Про захист населення від інфекційних хвороб” щодо запобігання поширенню коронавірусної хвороби (COVID-19)” дозволяється здійснювати обробку (в тому числі обмін інформацією в порядку, визначеному цією постановою) персональних даних осіб, визначених цією постановою як таких, що підлягають самоізоляції або обсервації (ізоляції).

добробуту та прав людини.	
4. Стаття 34. Кожному гарантується право на свободу думки і слова, на вільне вираження своїх поглядів і переконань. Кожен має право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб на свій вибір.	Жодної додаткової заборони щодо даних прав немає.
5. Стаття 53. Кожен має право на освіту. Повна загальна середня освіта є обов'язковою.	Забороняється відвідування закладів освіти її здобувачами.

Якщо детальніше заглибитись у додаткові обмеження щоденного життя вищевказаною постановою, то варто зазначити, що міри, прийняті в Україні, не є унікальними в світовій практиці, навіть щодо держав, які є прикладами демократичних суспільств. Хоча одні скажуть, що впровадження даних заходів, в епоху потужного цифрового інформаційного середовища не повинні створювати критичних обмежень права та свобод. Інтернет-ресурси здатні покрити всі запити на розвиток особистості (онлайн-курси, різного роду блоги, статті), на здобуття освіти (впроваджене дистанційне навчання в школах та університетах, багато світових навчальних закладів відкрили безкоштовний доступ до своїх бібліотек), можливо насторожує більший контроль держави особистих даних щодо тих, хто підпадає під поняття «обсервований» чи «інфікований». Коли мета виправдовує заходи. З іншого боку, є небезпідставні думки щодо того, що ніякий наказ Кабінету Міністрів України не може відмінити основні положення Конституції. Проте, він чинний, доки не оскаржений у Конституційному суді. Чи про те, що варто було б запроваджувати режим надзвичайного стану, який передбачений у випадку пандемій, що повністю зняло б питання неконституційності, проте наклало ще більші обмеження на права і свободи громадян.

Рано чи пізно ми вийдемо із карантинного періоду. Більш ніж впевнений, що він накладе вагомий слід на всіх людей і кожного зокрема. Одні можуть продовжити такий спосіб життя, заради власної безпеки, інші ж повернуться до звичного допандемічного режиму. Але, найважливішим в цей момент буде винести всі уроки

такого досвіду, звернути увагу на кожну скаргу щодо обмеження конституційного права, в тому числі і в інформаційній сфері, зреагувати на нові виклики, щоб виробити нові правила. Адже інформаційні права людини – це фундаментальні можливості і потреби кожної людини в доступі, використанні, розповсюдженні та захисті необхідного для її життєдіяльності обсягу інформації, які повинні гарантуватись державою.

Список використаної літератури:

1. Офіційний сайт Ради Європи. КОМПАС:Посібник з освіти в області прав людини за участі молоді. Що таке права людини? URL: <https://www.coe.int/uk/web/compass/what-are-human-rights-> (дата звернення 03.05.2020).
2. Офіційний сайт Всесвітньої організації охорони здоров'я . Coronavirus disease (COVID-19) advice for the public. URL: <https://www.who.int/emergencies/diseases/novel-coronavirus-019/advice-for-public> (дата звернення 03.05.2020).
3. Офіційний сайт Парламентської Асамблеї Ради Європи. Social Affairs, Health and Sustainable Development. COVID-19: We must face the pandemic while respecting economic and social rights, says committee Chair. URL : <https://pace.coe.int/en/news/7836/we-must-face-the-covid-19-pandemic-while-respecting-economic-and-social-rights-says-committee-chair> (дата звернення 04.05.2020).
4. Конституція України. URL : <https://zakon.rada.gov.ua/laws/show/254к/96-вр> (дата звернення 04.05.2020).
5. Про запобігання поширенню на території України гострої респіраторної хвороби COVID-19, спричиненої коронавірусом SARS-CoV-2. Постанова Кабінету Міністрів від 11 березня 2020 р. № 211. Дата оновлення 05.05.2020. URL : <https://zakon.rada.gov.ua/laws/show/211-2020-п> (дата звернення 05.05.2020).

Ланкін С. В.,
факультет соціології і права.
Науковий керівник:
Бежвець А. М., старший викладач.

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

Стаття 34 Конституції України визначає право кожного вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб – на свій вибір [1], відповідно дане положення є основою прав і свобод людини в інформаційній сфері. Особливо актуальним це конституційне положення стає в

період однієї з найбільш масових викликів 21 століття – пандемії коронавірусу в Україні.

Для громадян України як ніколи стає необхідним доступ до публічної інформації для усвідомлення масштабів поширення хвороби та розуміння дій, які приймає держава для боротьби з ним. Відповідно до ст.3 Закону України «Про доступ до публічної інформації» серед основних гарантій права на доступ до публічної інформації визначають:

1. Обов'язок розпорядників інформації надавати і оприлюднювати інформацію, що чітко означає заборону приховування будь-якої інформації, що знаходиться у суб'єктів владних повноважень, і становить суспільний інтерес.

2. Доступ до засідань колегіальних суб'єктів владних повноважень.

Відтак, усі засідання вищих органів державної влади, як Кабінет Міністрів України чи Верховна рада України, транслюються як по відповідних телеканалах, так і в мережі Інтернет безпосередньо, таким чином кожен громадянин може сприймати будь-яку важливу інформацію з приводу рішень влади, прийнятих для боротьби з COVID-19. Також іншим важливим аспектом є своєчасне оприлюднення державою усіх рішень на сторінках відповідних органів в мережі Інтернет для можливості ознайомлення з ними усіх громадян України та їх виконання. Зважаючи на темпи поширення захворювання, саме трансляція дій держави через мережу Інтернет, на нашу думку, є найбільш дієвим способом вжиття заходів і рішень для боротьби з поширенням коронавірусу.

3. Юридична відповідальність за порушення закону та приховування необхідної для суспільства інформації є саме тим положенням, яке повинно застерігати суб'єктів владних повноважень при поширенні публічної інформації від її перекручування або заниження показників, а також неповної відповіді на запити громадян, або іншому поширенню публічної інформації [3].

Цікавим є положення ст.17 Конституції України, де визначаються засади забезпечення інформаційної безпеки, що є однією з найголовніших функцій держави в реалізації громадянами права на інформацію, передбаченого ст.34 Основного закону. Так, наприклад, навіть в абзаці другому ст.34 зазначається певне виключення із загального права на інформацію, а саме обмеження цього права задля дотримання інтересів національної безпеки, запобігання масовим заворушенням, охорони здоров'я населення або при поширенні конфіденційної інформації. Таким чином держава обмежує для себе певне коло інформації серед загального інформаційного простору, що не може бути поширене. Такі же виключення встановлюються в ст.6 Закону

України «Про доступ до публічної інформації». Але чи належить інформація про поширення коронавірусу до виключного переліку інформації, зазначеного в законі?

На нашу думку – звісно ні, оскільки даний тип інформації пов'язаний з певною надзвичайною ситуацією, що виникла на території нашої держави. Таким чином відповідно до ч. 2 та ч. 5 ст. 31 Кодексу цивільного захисту України органи державної влади зобов'язані надавати населенню через засоби масової інформації оперативну та достовірну інформацію про надзвичайні ситуації, що виникли, межі її поширення та її наслідки, а також способи захисту від неї [2]. Такі ж положення визначає ст.17 Закону України «Про захист населення від інфекційних хвороб» [4].

Виходячи з цього, можемо зазначити, що держава зобов'язана інформувати громадян через засоби масової інформації якщо не по годинно, то хоча б щодня про ситуацію в країні, та рішення уповноважених органів державної влади для протидії поширенню цієї хвороби, а найкраще буде підкріплення рішень конкретними діями, що також можна транслювати за допомогою сучасних технологій навіть в режимі реального часу.

Але чому важливо, щоб таку інформацію поширювала саме держава, а не інші поширювачі інформації, як наприклад блоггери або так звані «незалежні» ЗМІ? По-перше, у випадку відсутності інформації про хворобу створюється певний інформаційний вакуум, де кожен громадянин будучи наляканим або при відсутності потрібної освіти для повного аналізу питання вдається до сторонніх джерел інформації, що не завжди бувають правдивими, перевіреними. Відтак дуже легко поширювати паніку і занепокоєння серед суспільства, і населення починає вірити в такі речі як поширення коронавірусу через 5-G телевежі або примусове поширення хвороби для зачистки бідного прошарку громадян України [5]. Здавалося б, що в двадцять першому столітті такі речі неможливо вкласти в голову свідомому громадянину, але відсутність іншої надійної інформації і спростування подібних «фейків» створює цілком реальне підґрунтя для існування таких теорій змов.

По-друге, використання інформації з неперевірених джерел створює цілком реальні наслідки у формі масових заворушень, порушення роботи суспільно-необхідних підприємств, підвищення криміногенної ситуації в країні та інші негативні наслідки, обов'язком контролю яких лежить саме на державі. По-третє, інформація, що поширюється з офіційних джерел, повинна викликати довіру у громадян, це забезпечується підкріпленням дій держави різними показниками, роз'яснення іноді простих речей для сприйняття їх населенням, та заклику до порозуміння.

Ще одним важливим аспектом, що характерний саме для періоду надзвичайних ситуацій, є оперативний обмін інформацією про вірус різними державними

відомствами, для можливості швидкого реагування та виконання рішень найвищих органів влади на локальному рівні. Гарною перевагою в цьому є наявність сучасних інформаційно-комунікативних засобів, будь-то смартфон або комп'ютер, що дозволяє швидко обмінюватись даними. Особливо цікавим досвідом України є створення Єдиного порталу відкритих даних, що дозволяє усім державним органами, органам місцевого самоврядування або неурядовим організаціям мати доступ до усієї актуальної інформації, яка завантажується туди усіма розпорядниками публічної інформації в державі Україна [5].

Але, на жаль, іноді дана інформація оприлюднюється у неповному обсязі, що ставить питання щодо можливості їх нормального використання. Так, наприклад, з кількох тисяч розпорядників лише 10 оприлюднили кількість наборів медичного обладнання на відповідному порталі. Такі ухилення розпорядників від виконання обов'язків, гарантованих українському народові Конституцією України і відповідним Законом України «Про доступ до публічної інформації», потребують притягнення відповідних осіб, в першу чергу, до адміністративної відповідальності, а якщо така відсутність інформації спричинить тяжкі наслідки, то й до кримінальної відповідальності відповідно.

Список використаної літератури:

1. Конституція України // Відомості Верховної Ради. – 1996. URL : <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#n4269.н>
2. Кодекс цивільного захисту України // Відомості Верховної Ради. 2013. URL : <https://zakon.rada.gov.ua/laws/show/5403-17#n563>.
3. ЗАКОН УКРАЇНИ "Про доступ до публічної інформації" // Відомості Верховної Ради. 2011. URL : <https://zakon.rada.gov.ua/laws/show/2939-17>.
4. ЗАКОН УКРАЇНИ "Про захист населення від інфекційних хвороб" // Відомості Верховної Ради. 2000. URL : <https://zakon.rada.gov.ua/laws/show/1645-14#n163>.
5. Чи приховують правду про коронавірус: шість тез щодо права на інформацію під час пандемії // ZMINA. 2020. URL : <https://zmina.info/articles/chy-pryhovuyut-pravdu-pro-koronavirus-6-tez-pro-pravo-na-informacziyu-pid-chas-pandemiyi/>.

Водько Ю. В.,
факультет соціології і права.
Науковий керівник:
Бежвець А. М., старший викладач.

ЗАБЕЗПЕЧЕННЯ КОНСТИТУЦІЙНИХ ПРАВ І СВОБОД ЛЮДИНИ В ІНФОРМАЦІЙНІЙ СФЕРІ В УМОВАХ КАРАНТИНУ

Забезпечення прав людини у сфері інформації дедалі дужче набуває високого ступеню важливості. Карантинний період безумовно впливає на пришвидшення інформатизації всіх ланок суспільного життя. Раніше оголошена державою стратегія щодо цифровізації державних послуг та цифрова трансформація інформації стала не просто потребою, а необхідністю. Каталізаторами цього процесу є не лише інтенсивний розвиток інформаційних технологій, а й виникнення багатьох кризових ситуацій, як це особливо помітно через пандемію, в яких без швидкого реагування через інформаційні канали неможливе ефективне регулювання суспільних відносин як з боку держави, так і всередині самого суспільства.

Статтями 34 та 64 Конституції України закріплюються основоположні права людини у сфері інформації, зокрема «право вільно збирати, зберігати, використовувати й поширювати інформацію усно, письмово або в інший спосіб» [1]. Проте також у цих статтях передбачено, що це право може обмежуватися з певною метою та за певних обставин, вичерпно передбачених цими статтями – в умовах воєнного або надзвичайного стану із зазначенням строку їхньої дії, а також законом в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя. Важливо звернути увагу, що в Україні карантинні обмеження були введені разом з надзвичайною ситуацією відповідно до розпорядження Кабінету Міністрів України від 25 березня 2020 р. № 338-р «Про переведення єдиної державної системи цивільного захисту у режим надзвичайної ситуації» [7]. Тобто підстави для обмеження прав, що визначені статтею 64 Конституції України, відсутні.

Відповідно до Закону України «Про внесення змін до деяких законодавчих актів України, спрямованих на запобігання виникненню і поширенню коронавірусної хвороби (COVID-19)» важливість дотримання і гарантія безперешкодного здійснення прав людини в інформаційній сфері підкреслюється [3]. Оскільки своєчасне та повне інформування населення відіграє найбільшу роль для запобігання паніки, контролю

прозорості, ефективності з боку громадян за діями влади у боротьбі з коронавірусною хворобою, то обмеження прав і свобод людини не стосуються права на доступ до публічної інформації. Законодавство встановлює навіть спеціальні гарантії для отримання відомостей про події, їхній розвиток, кількісні та якісні показники, плани органів виконавчої влади та органів місцевого самоврядування тощо [8].

Відповідно до презумпції відкритості інформації, яку визначає ч. 2 ст. 1 Закону України «Про доступ до публічної інформації», інформація стосовно епідемії, яка є у віданні органів державної влади, вважається публічною, крім випадків, встановлених законом [4]. Стаття 17 Закону України «Про захист населення від інфекційних хвороб» передбачає права та обов'язки громадян та їх об'єднань у сфері захисту населення від інфекційних хвороб, зокрема, це право на отримання достовірної інформації щодо епідемічної ситуації в Україні. У свою чергу органи виконавчої влади та органи місцевого самоврядування, які зобов'язані періодично повідомляти через засоби масової інформації про епідемічну ситуацію та здійснювані протиепідемічні заходи несуть відповідальність згідно із законом за відмову у наданні інформації, умисне перекручення або приховування об'єктивних даних про захворювання населення на інфекційні хвороби [5].

На нашу думку, відбувається перетин права на недоторканність приватного життя і права на отримання правдивої інформації щодо епідемічної ситуації в Україні, тому головним розмежувачем залишається принцип: «права однієї людини закінчуються там, де починаються права іншої». Це право повинно забезпечуватися, не порушуючи право на анонімність і конфіденційність персональних даних, включно з конфіденційною інформацією щодо здоров'я людей. У випадку незаконного розголошення персональних даних (ПІБ, місця проживання, дані родичів) осіб, у яких була підозра на захворювання, стаття 182 Кримінального кодексу України передбачає кримінальну відповідальність за незаконне збирання, зберігання, використання, знищення, поширення конфіденційної інформації про особу [2].

До Верховної Ради України був поданий Проект Закону про внесення зміни до пункту 2 розділу II «Прикінцеві положення» Закону України «Про внесення змін до деяких законодавчих актів України, спрямованих на запобігання виникненню і поширенню коронавірусної хвороби (COVID-19)», яким пропонується тимчасово зупинити перебіг строків розгляду звернень громадян, запитів на публічну інформацію, адвокатських запитів, окрім звернень (запитів), що стосуються захисту життя чи свободи особи, щодо стану довкілля, якості харчових продуктів і предметів побуту, аварій, катастроф, небезпечних природних явищ та інших надзвичайних подій, що сталися або можуть статись і загрожують безпеці громадян. Від дня

припинення карантину перебіг цих строків продовжується з урахуванням часу, що минув до його зупинення [6]. Тимчасове зупинення хоч і не означає скасування розгляду запитів, проте обмежує своєчасну та ефективну реалізацію цього права. Згідно з пояснювальною запискою законопроект аргументується тим, що працівники органів державної влади та органів місцевого самоврядування не можуть в повній мірі давати відповіді на запити щодо отримання інформації через карантинні обмеження, які ускладнюють їхню роботу з надання відповідей [9].

Проте, ми вважаємо, що такі обмеження є очевидно неконституційними, оскільки створюють інші підстави для обмеження права на доступ до публічної інформації, окрім тих, які містяться у ст.34 та ст.64 Конституції України, що є неприпустимим [1].

Отже, вплив карантинних заходів безумовно справив величезний вплив на інформаційну сферу і на права людини у ній. Важливість їхньої швидкої та безперешкодної реалізації набула нового значення. Держави з недемократичними політичними режимами прикладають багато зусиль, щоб обмежити право людини на інформацію, оскільки вона є найголовнішою зброєю у політиці. Попри високий розвиток Китаю, у цій державі правозахисники з усього світу фіксують численні утиски свободи преси, що, як наслідок, призводить до порушення прав людини в інформаційній сфері. Під час пандемії, спричиненої хворобою COVID-19, ці утиски спричинили незворотні наслідки через приховування та перекручування інформації владою, які ми можемо спостерігати у вигляді надзвичайно масштабного поширення вірусу по всьому світу [11]. Ще більш безглуздо виглядає боротьба влади Туркменістану з правами людини у сфері інформації, яка заборонила навіть вживання слова «коронавірус», що аж ніяк не сприяє формуванню у населення повного та реального уявлення щодо ситуації у країні та світі з пандемією [10].

Україна, як держава з демократичним політичним режимом, повинна у повній мірі забезпечувати права людини у сфері інформації та рівнятися на інформаційну політику тих держав, які ефективно борються з коронавірусною хворобою. Карантинний період вже призвів до багатьох неправомірних обмежень та утисків прав людини у сфері інформації, тому слід переглянути та усунути фактори, що спричиняють це, щоб той період, що ще буде переживати країна у карантині та посткарантинний період якомога менше завдав негативного впливу на права людини загалом і у сфері інформації, зокрема.

Список використаної літератури:

1. Конституція України // Відомості Верховної Ради України (ВВР). 1996. № 30. с. 141. URL : <http://zakon5.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80>

2. Кримінальний кодекс України. // Відомості Верховної Ради України (ВВР). 2001. № 25-26. ст.131. URL : <https://zakon.rada.gov.ua/laws/show/2341-14>
3. Закон України «Про внесення змін до деяких законодавчих актів України, спрямованих на запобігання виникненню і поширенню коронавірусної хвороби (COVID-19)». // Відомості Верховної Ради України (ВВР). 2020. № 16. ст.100. URL : <https://zakon.rada.gov.ua/laws/show/530-IX>
4. Закон України «Про доступ до публічної інформації». // Відомості Верховної Ради України (ВВР). 2011. № 32. ст. 314. URL : <https://zakon.rada.gov.ua/laws/show/2939-17>
5. Закон України «Про захист населення від інфекційних хвороб». // Відомості Верховної Ради України (ВВР). 2000. № 29. ст. 228. URL : <https://zakon.rada.gov.ua/laws/show/1645-14>
6. Проект Закону про внесення зміни до пункту 2 розділу II "Прикінцеві положення" Закону України "Про внесення змін до деяких законодавчих актів України, спрямованих на запобігання виникненню і поширенню коронавірусної хвороби (COVID-19)". URL : http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=68503
7. Розпорядження Кабінету Міністрів України «Про переведення єдиної державної системи цивільного захисту у режим надзвичайної ситуації». // Урядовий портал. 25 березня 2020 р. № 338-р. URL : <https://www.kmu.gov.ua/npas/pro-perevedennya-yedinoi-derzhavnoyi-sistemi-civilnogo-zahistu-u-rezhim-nadzvichajnoyi-situaciyi-338250320>
8. Доступ до інформації під час карантину – гарантії чи обмеження? // Доступ до правди. 23 березня 2020. Олександр Бурмагін, медіа юрист ГО «Платформа Прав Людини». URL : <https://dostup.pravda.com.ua/news/publications/dostup-do-informatsii-pid-chas-karantynu-harantii-chy-obmezhennia>
9. Доступ і карантин: чому не потрібен закон про зупинку розгляду запитів. // Доступ до правди. 3 квітня 2020. Олександр Бурмагін, медіа юрист ГО «Платформа прав людини». URL : <https://dostup.pravda.com.ua/stories/publications/zapyty-i-karantyn-chomu-ne-potriben-zakon-pro-vidstrochku>
10. У Туркменістані заборонили слово "коронавірус". // Українська правда. 31 березня 2020. Репортери без кордонів. URL : <https://www.pravda.com.ua/news/2020/03/31/7245891/>
11. Як Китай практично зупинив поширення коронавірусу: від замовчування до тотального контролю. // Радіо Свобода. 19 березня 2020. Марія Щур. URL : <https://www.radiosvoboda.org/a/30495542.html>

Радзієвська А. Є.,
студентка НМУ ім. О.О.Богомольця.
Науковий керівник:
Фурашев В.М., к.т.н., с.н.с., доцент.

COVID-19 – «СМЕРТОНОСНИЙ» ВІРУС ЧИ ВСЕПЛАНЕТНА ПАНІКА

COVID-19. На сьогоднішній день найбільш вживаний термін на планеті. Вірус, що уразив величезну кількість людей. Перший вірус, який замкнув майже всю планету вдома. Чи дійсно він такий страшний? Чи його славу робить всесвітня паніка? У доповіді я спробую пояснити деякі аспекти та з'ясувати чи дійсно настільки страшний вовк, як його малюють.

30 січня 2020 року Всесвітня організація охорони здоров'я оголосила надзвичайну ситуацію у зв'язку з поширенням раніше невідомого виду коронавірусу за межами однієї країни. Виявили його 12 грудня 2019 року в китайському місті Ухань [1].

Інфікуватися COVID-19 можна при тісному й тривалому контакті з хворим на коронавірус, навіть під час інкубаційного періоду, який триває 7–14 днів. Тобто людина, яка не має жодних симптомів хвороби, здатна передати вірус іншим. В середньому інфікований коронавірусом може передати його 3 людям, тоді як інфікований кором може заразити в 6 разів більше осіб. Показники інфікування також значно вищі у разі захворювання на «свинку» (епідеміологічний паротит) та віспу у 7 разів, ВІЛ – у 5 разів [1].

На офіційному інформаційному порталі Кабінету Міністрів України можна знайти такі данні щодо пандемії: протестованих – 257890; хворих на коронавірус – 19706; тих, хто одужав – 6227; летальних випадків – 579. Показник летальності від коронавірусу відповідно до слів прем'єр-міністра Дениса Шмигала в Україні знаходиться у межах 2,7 – 2,9 % [2]. Для порівняння візьмемо дані ВООЗ про рівень смертності: від лихоманки Ебола – 40%, MERS – 35%, SARS – 10%, дифтерії – 5% .

Чи здається нам грип смертельно небезпечним захворюванням? Щороку під час карантинних заходів батьки все одно ведуть малечу до торгівельних і розважальних закладів, мало хто переймається медичними масками та вакцинаванням. Тоді як рівень смертності від грипу у світі – 6%. Зкладами охорони здоров'я регулярно виявляються ускладнення у хворих, які намагалися перенести запалення легень на ногах. Не від безвиході, а від «гарної репутації» хвороби. Мовляв, це просто ускладнення ГРВІ, всі цим хворіють, навіть немовлята. Утім, смертність від пневмонії становить 4%, а знайдений у Китаї штам коронавірусу дає найнижчі в цьому переліку

показники – в межах 2% [1]. Близько 80% заражених переносять хворобу легко, дехто навіть може і не здогадуватися, що у нього COVID-19. Як зазначено на сайті ВООЗ, більшості хворим не призначають спеціальне лікування [3]. Виникає запитання чому всі в такому нездоровому страху перед коронавірусом?

Вселюдська паніка приводить до абсурдних випадків. Наприклад, я не поведу свою дитину на прогулянку, бо там коронавірус, там небезпечно. Хоча всі лікарі як один кажуть, що один з найкращих способів запобігання зараженню вірусом – це підвищення імунітету, а що може підвищити імунітет краще за свіже повітря? Крім того, діти без проблем з респіраторною системою та інших вад здоров'я не знаходяться в зоні ризику. Звісно, перехворіти на таку хворобу – важке випробування для малечі. Але ж коронавіруси значно рідше вражають дітей. За цей час повідомили лише про 5 випадків інфікування новим штамом тих, кому немає 14 років. Частина з них не мали зовнішніх проявів хвороби. Що більший вік, то вищий ризик, запевняють лікарі. 80% померлих від коронавірусу – люди пенсійного віку. Три чверті мали ще й важкі хронічні проблеми зі здоров'ям (астма, діабет, серцево-судинні захворювання) [1].

Звідки взявся COVID-19? Дехто вважає, що коронавірус – це якась цілком нова хвороба, невідома людству. Але коронавіруси є в будь-якому медичному довіднику як банальні збудники ГРВІ. Чи серйозно ми ставимося до застуди? Вірусів, які спричиняють респіраторні захворювання близько 300, всі вони видаються нешкідливими, «дрібними». Кожен сьомий випадок ГРВІ – коронавіруси. Ще 20 років тому вважалося, що вони не можуть спричинити значної шкоди людині. Але в 2002 році один з них мутував і спричинив епідемію SARS, а інший десять років потому – MERS. Особливість цих двох варіантів, як і нинішньої мутації (штам 2019-nCoV), – ураження легень. Саме це головна небезпека. У багатьох інфікованих людей хвороба минає в легкій формі як банальна застуда. Хіба що значно частіше супроводжується кашлем [1].

Чи дійсно самоізоляція обов'язкова для всіх? До яких наслідків може призвести сам карантин і які лікарі знадобляться людям по його завершенню? Самоізоляція – це обмеження контактів з іншими людьми [3]. Тривалі обмеження соціальних контактів між людьми в період карантинних заходів провокує певні психологічні та психічні стани у населення, зокрема стан неспокою чи нервозності. Європейські дослідники привели статистику, що за час карантину в європейських родинах збільшився відсоток розлучень та конфліктів в сім'ї. Крім цього не слід забувати, що «людина є соціальною твариною» і довга відсутність соціальних контактів призведе до часткової втрати соціальних навичок поведінки та спілкування.

Через величезну кількість новин про пандемію вже зараз у багатьох людей фіксуються панічні атаки зі схожими до коронавірусу симптомами: задишка, відчуття здавлювання в грудях. Природно, що це збиває людей з пантелику, особливо, якщо панічна атака сталася вперше. Панічна атака – це незрозумілий, болісний напад тривоги і страху в поєднанні з соматичними симптомами. Цей невротичний розлад надзвичайно поширений, а його причини до кінця не вивчені. Дослідники вважають, що причиною панічних атак в більшості випадків є сильний стрес, хвороба або надмірні навантаження. Вважається, що до панічних атак найбільш схильні молоді люди у віці 20-30 років, а жінки хворіють частіше за чоловіків [4]. Але як відрізнити панічну атаку від справжніх симптомів COVID-19?

Пітливість, задишка, страх смерті – все це симптоми панічного атаки. Але під час пандемії COVID-19 люди, які вперше зіткнулися з панічною атакою навряд чи зможуть зрозуміти що з ними відбувається. Ситуацію ускладнює той факт, що одним із симптомів панічної атаки, як і у COVID-19, є тривога. Якщо панічна атака сталася вперше, то дослідники, як не дивно, радять зізнатися собі в тому, що вам страшно або ви відчули горе [4]. Якщо симптоми, такі як висока температура або кашель, зберігаються після того як ви заспокоїлися, негайно зверніться до лікаря. Це можуть бути симптоми COVID-19.

Щоб розрізнити коронавірус і панічну атаку слід проаналізувати основні симптоми: кашель, високу температуру, задишку, утруднене дихання, біль в горлі і навіть висип (рідше – нежить, фарингіт і діарея) на предмет належності до психологічних проблем.

Чи можна точно встановити чи ти хворий на коронавірус, звичайний грип чи може у тебе просто панічна атака? На сьогодні існують експрес тести на виявлення COVID-19. Крім того, ВООЗ розробила тест-систему, яка дозволяє виявляти хворих на COVID-19. Наразі така тест-система є в Україні і використовується виключно у випадках, що відповідають епідеміологічному і клінічному визначенню хвороби, зазначених в рекомендаціях ВООЗ. Тестування проводиться у вірусологічній референс-лабораторії Центру громадського здоров'я України. Для дослідження зразки направляються саме в цю лабораторію. До отримання результату проходить орієнтовно 5-6 годин. Тест-система ВООЗ дає більш точні результати у порівнянні з експрес-тестом, похибка якого за різними даними становить від 25 до 30% [5].

На жаль, через величезну кількість фейків немає змоги донести до людей дійсно корисну і правдиву інформацію про вірус. Наприклад, в інформаційному просторі активно тиражувалась ідея, що вплив низьких чи високих температур знешкоджує вірус COVID-19. Дуже хотілося би, але на жаль ні, коронавірусна інфекція є достатньо

стійкою до температурних режимів. COVID-19 можна захворіти незалежно від того, наскільки сонячною або жаркою є погода. Країни з жарким кліматом також повідомляють про випадки захворювання COVID-19. Деякі міфи про коронавірус є не тільки смішними, але і небезпечними, як наприклад: вживання алкоголю захищає від COVID-19. Часте або надмірне вживання алкоголю лише підвищує ризик виникнення проблем із здоров'ям.

Загальну паніку провокує той факт, що ліків, рекомендованих ВООЗ для боротьби з коронавірусом, не існує. З цього приводу також є безліч непідтверджених чуток. Як наприклад, COVID-19 лікується антибіотиками. Для лікування вірусних інфекцій, антибіотики не використовуються, це ж стосується нового захворювання COVID-19.

Отже, не слід впадати у паніку і наставляти на паніку інших. Не потрібно встановлювати свій діагноз самостійно, краще звернутися до фахівців, оскільки, одні і ті ж симптоми можуть описувати різні захворювання. Також слід розглядати і перевіряти факти, критично сприймати прочитане, побачене та почуте. Не варто вірити всьому в Інтернеті, бажано користуватися лише офіційними порталами, а також не слід тиражувати неперевірену інформацію через соціальні медіа. І можливо тоді ми побачимо справжню картину і зможемо скласти свідоме бачення проблеми чи є COVID-19 «смертоносним» вірусом чи це в більшій мірі всепланетна паніка.

Список використаної літератури:

1. Коронавірус: 9 головних міфів. URL: <https://osvitoria.media/experience/koronavirus-9-golovnyh-mifiv/>
2. Статистика щодо коронавірусу з офіційної сторінки Кабінету Міністрів України. URL: <https://covid19.gov.ua/>
3. Чим страшний коронавірус? URL: <https://rivnepost.rv.ua/news/chim-strashniy-koronavirus>
4. Сокови́кова Л. Пани́ческая ата́ка может имитировать симптомы COVID-19. Что с этим делать? URL: <https://hi-news.ru/eto-interesno/panicheskaya-ataka-mozhet-imitirovat-simptomy-covid-19-chto-s-etim-delat.html>
5. Топ запитань про коронавірус. URL: <https://www.ukrinform.ua/rubric-society/2884397-25-zapitan-pro-koronavirus.html>

Долматов І.О..,
факультет інформатики та
обчислювальної техніки.
Науковий керівник:
Самчинська О.А., викладач.

ВИКЛИКИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ СПРИЧИНЕНІ ПАНДЕМІЄЮ КОРОНАВІРУСУ COVID-19

Пандемія COVID-19 є однією з найбільших проблем сучасності. Хвороба проходить важко і, більш того, має наслідком летальні випадки. Заради запобігання поширенню хвороби влади країн всього світу були змушені вжити заходів, серед яких закриття кордонів і введення карантину в межах країн.

У зв'язку із ситуацією, що склалася, нагальною стала проблема обмеження прав людей, зокрема конституційних, заради забезпечення їх безпеки. Очевидно, що обмеження прав людини на пересування, яке є одним із обов'язкових положень карантину, суперечить доктрині про права людини [1]. Окрім цього, подібне обмеження, спонукає людей більше часу проводити в електронному форматі. Отримання та поширення інформації, покупки, робота, навчання, зустрічі з друзями та безліч інших справ, які ми зазвичай здійснювали без прямої залежності від мережі Інтернет, зараз повністю перейшли в режим онлайн. Як наслідок значно збільшилася кількість покупок в онлайн-магазинах, кількість публікацій та читачів та й взагалі кількість активних користувачів мережі. Це в свою чергу викликає низку проблем в аспекті забезпечення інформаційної безпеки в умовах карантину.

Перша проблема, на яку варто звернути увагу – це проблема захисту особистих даних, адже в період пандемії люди з усього світу починають активно використовувати незвичне для себе програмне забезпечення для роботи і дозвілля, навіть не замислюючись про те, наскільки це безпечно. Одним з найяскравіших прикладів цьому може слугувати загальновідома програма ZOOM, яка набула популярності саме в період ізоляції [2]. Але якщо ZOOM – продукт, який первинно не призначений для масового використання, тому не повинен був би бути привабливий для зловмисників, однак, вже є випадки його злому, то інші сервіси, в яких збільшилася кількість користувачів (соціальні мережі, інтернет-магазини, сайти для розваги, онлайн-бібліотеки та інші), які спочатку були розраховані на велику кількість користувачів, стали куди більш привабливі для злому, адже тепер зберігають куди більше особистої інформації більшої кількості людей. Усе тому, що всі перераховані ресурси та сервіси містять великий обсяг інформації про людину, її особисте життя,

інтереси, захоплення, матеріальний стан і т.п. А інформація, в умовах інформаційного суспільства, найцінніший та найдорожчий ресурс.

Друга проблема, яка особливо гостро постала в час карантину – це дезінформація. Вимушений перехід в онлайн-життя не зробив всіх людей миттєво більш перебірливими до інформації. Якщо раніше люди постійно обмінювалися новинами і пізнали їх від інших, то зараз багато хто шукає інформацію в Інтернеті, не думаючи про те, що вона може бути помилковою. З іншого боку цієї проблеми знаходяться ті, хто створює та поширює неправдиву інформацію на актуальні нині теми. Як результат подібної діяльності, ряд сервісів починають обмежувати поширення новин про COVID-19 [3].

Третя проблема, яку варто розглянути, це проблема, яка впливає в онлайн-життя - проблема реального життя. А саме те, що люди зараз змушені майже весь свій час проводити в межах свого місця проживання і не мають можливості побути на самоті або з друзями. Йдеться про вплив закритого простору на людину в цілому. У людей різко зростає бажання вийти, погуляти, виїхати, відпочити від свого ж будинку. Але про відпустку немає й мови, навіть на роботу зараз можуть вийти лише деякі люди. Як результат соціальні мережі починають боротися з поширенням новин про відпустки і всім, що з ним асоціюється [4].

Таким чином соціальні мережі намагаються зменшити кількість асоціацій, пов'язаних з відпочинком. Так само в соцмережах зараз з'явилося багато «лайфхаків» як проводити час «в 4 стінах», що знову ж таки є частиною дій в сторону дотримання карантину.

Отже, світ опинився в незвичній ситуації, до якої не був готовий. Жодна із країн не могла передбачити розвиток подій, що відбувається зараз, як в сфері прав людини в реальному, так і онлайн життя. Це в свою чергу поставило перед світовою спільнотою завдання щодо розроблення ефективного механізму протидії виникнення таким ситуаціям та плану дій у разі її настання.

Особливо варто звернути увагу на розвиток інформаційного суспільства та усіх елементів його прояву, адже, саме забезпечення ефективності механізмів та безпеки у цій сфері є першочерговим у сучасних умовах.

Список використаної літератури:

1. Ю. С. Разметаєва. Доктрина та практика захисту прав людини. URL: <https://nlu.edu.ua/wp-content/uploads/2019/08/PhD-1-%D0%94%D0%BE%D0%BA%D1%82%D1%80%D0%B8%D0%BD%D0%B0-%D1%82%D0%B0%D0%BF%D1%80%D0%B0%D0%BA%D1%82%D0%B8%D0%BA%D0%B0%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B>

%D0%B7%D0%B0%D1%85%D0%B8%D1%81%D1%82%D1%83%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D1%8E%D0%B4%D0%B8%D0%BD%D0%B8.pdf (дата звернення 10.05.2020).

2. Дарья Громова. В Сеть попали данные более 500 тысяч пользователей Zoom. Скорее обновите свой пароль. URL: <https://lifehacker.ru/zoom-sliv-500k-akkauntov/> (дата звернення 10.05.2020).

3. Елена Аракелян. Коронавирусный YouTube: в Genesis рассказали, что меняется в работе видеоплатформ. URL: <https://tech.liga.net/technology/article/koronavirusniy-youtube-v-genesis-rasskazali-cto-menyetsya-v-rabote-videoplatform> (дата звернення 10.05.2020)

4. Антон Курилов. Instagram скрыл хэштег #море. Пользователи соцсетей гадают, почему. URL: <https://rozetked.me/news/10975-instagram-skryl-heshteg-more-pol-zovateli-socseti-gadayut-pochemu> (дата звернення 10.05.2020).

Шнак І. В.,

факультет соціології та права.

Науковий керівник:

Фурашев В. М., к.т.н., с.н.с., доцент.

КІБЕРБЕЗПЕКА ПІД ВПЛИВОМ ПАНДЕМІЇ ТА КАРАНТИННОГО РЕЖИМУ

Нещодавно один з найавторитетніших британських словників Collins English Dictionary визнав слово «lockdown» (в перекладі з англійської – карантин, закриття) найпопулярнішим словом 2020 року. Цей термін вперше почав з'являтися в новинах у січні цього року, відтоді практично кожна велика країна запровадила певну форму блокування – з безпрецедентними соціальними обмеженнями, що мінімізують взаємодію людей і роблять 2020 рік несхожий на жодний за всю історію людства.

Як зазначає Джон Ольцік, старший головний аналітик та науковий співробітник ESG, пандемія мала широкий вплив на осіб, що працюють у службах безпеки. 84% фахівці з кібербезпеки працювали під час пандемії виключно вдома, і майже дві третини вважали, що їх організації будуть більш гнучкими, впроваджуючи розповсюджену політику «роботи з дому», ситуація особисто вплинула на спеціалістів з кібербезпеки, їхні робочі місця та їхнє життя.

У сфері кіберзахисту пандемія коронавірусу надала хакерам та інтернет-шахраям «найкращу у житті можливість», відповідно до нового звіту Асоціації захисту інформаційних систем (ISSA), спільноти міжнародних фахівців з кібербезпеки та незалежної фірми-аналітика. В рамках свого дослідження організація у квітні 2020

року провела опитування 364 фахівців з питань кібербезпеки та ІТ із глобального списку членів ISSA і виявили, що серед респондентів, 63% зіштовхнулися зі збільшення кібератак через пандемію.

У статті компанії Deloitte наводяться деякі можливі та цілком реальні способи впливу пандемії на інформаційну безпеку. По-перше, спостерігається значний ріст випадків фішингових атак (отримання цінних даних, які можуть бути продані або використані для зловмисних цілей) та атак-вимагачів (програми, які вимагають викуп, надають злочинцям можливість віддалено заблокувати доступ до комп'ютера) пов'язаних із COVID-19. Як результат, це призводить до збільшення кількості заражених персональних комп'ютерів. Але такі зловмисники націлюються не лише на великі бізнеси, а й на звичайних користувачів, які завантажують додатки та інформацію, що пов'язані з COVID-19.

Друга проблема, яка постає – підвищення ризику небезпеки під час віддаленої роботи та на дистанційному навчанні. Багато співробітників працюють з дому, а студенти навчаються віртуально, тому сервери корпоративної віртуальної приватної мережі (VPN) стали справжнім порятунком для компаній та навчальних закладів. Прагнучи встановити їх безпеку та доступність, доволі часто зустрічається невідповідність організацій, що цілком реально може привести до викриття та розповсюдження конфіденційної інформації, а також загрози для пристроїв у вигляді DoS-атак (атака на відмову в обслуговуванні комп'ютера). До того ж, деякі користувачі можуть використовувати особисті комп'ютери для виконання службових обов'язків, які також можуть представляти великий ризик для організацій.

Третя загроза для інформаційної безпеки спричинена пандемією — складність у виявленні потенційної кібератаки та її попередженні. Функціонування багатьох команд з безпеки могло бути порушеним як наслідок пандемії COVID-19, що, таким чином, в разі ускладнює викриття зловмисних дій та ефективну і дієву відповідь на них. Тому організації повинні оцінювати свої засоби захисту та дослідити використання спільних джерел із зовнішніми консультантами, особливо в тих областях, де ключові особи ризикують бути ідентифікованими.

То ж яким чином можна покращити інформаційну безпеку та захистити її від внутрішніх та зовнішніх загроз? Перш за все, всі організації повинні вживати всіх можливих ініціативних заходів, застерігаючи своїх співробітників та клієнтів бути обачнішими та обережнішими, особливо при відкритті посилань, електронних листів або документів, що стосуються теми COVID-19. Також організації мають бути впевненими, що їх можливості виявлення та попередження функціонують задовільно. Зрештою бажано обмежити проведення робочого часу в громадських приміщеннях, а

організація, в свою чергу, повинна використовувати технології, що забезпечують збереження конфіденційної інформації на пристроях у разі крадіжки або пошкодження.

Пандемічна криза COVID-19 вплинула на життя кожного і змінила багато щоденних процедур за досить короткий час. Коронавірусна інфекція поставила перед людьми найрізноманітніші технічні та організаційні завдання і проблеми, які потребують глибокого аналізу, розуміння та переоцінки всіх методів та інструментів у галузі кібербезпеки. Існує велика ймовірність того, що деякі з таких змін можуть бути безповоротними або продовжать з'являтися в інших формах в епоху після COVID-19. Тож варто подумати про можливості управління кризовими ситуаціями, про можливі швидкі рішення поточної ситуації та оцінити наслідки цього для кібербезпеки.

Список використаної літератури:

1. The Life and Times of Cybersecurity Professionals 2020. A Cooperative Research Project by ESG and ISSA / Дж. Ольцік 2020. URL : <https://www.issa.org/wp-content/uploads/2020/07/ESG-ISSA-Research-Report-Cybersecurity-Professionals-Jul-2020.pdf>

2. COVID-19's Impact on Cybersecurity. / Т. Аладенусі. URL : 2020.
<https://www2.deloitte.com/content/dam/Deloitte/ng/Documents/risk/ng-COVID-19-Impact-on-Cybersecurity-24032020.pdf>

Тутов В.А.,
фізико-технічний інститут.
Науковий керівник:
Стьопочкіна І. В., к.т.н., доцент.

ПЕРЕХІД НА ДИСТАЦІЙНЕ НАВЧАННЯ ТА БЕЗПЕКА ВЕБ-РЕСУРСІВ

У зв'язку із поширенням епідемії, особливої актуальності набувають засоби дистанційного навчання та комунікації. В тому числі, яскраво стають видні і недоліки проектування веб-ресурсів, особливо в сфері недоліків кібернетичної безпеки.

Через введення режиму самоізоляції традиційна освіта змушена була перейти в «онлайн» формат. Технологічна революція яка обіцяла в майбутньому перевести всі освітні комунікації та навчання в цифровий формат настала.

За підрахунками ЮНЕСКО, близько 1,5 млрд. школярів по всьому світу через пандемію COVID-19 були переведені в режим дистанційного навчання. В той же час на сьогодні в Україні і світі створені десятки сервісів для дистанційного навчання і їх кількість, у зв'язку з потребою, тільки збільшується.

Які платформи і сервіси взяли на себе основне навантаження в сегментах шкільного, вузівського, додаткового і корпоративного навчання під час пандемії і чи здатні вони замінити звичайні уроки?

iLearn – це безкоштовна гейміфікована платформа з навчальними онлайн – курсами, тестами і вебіарами для всіх, хто хоче вчитися і успішно скласти ЗНО (Зовнішнє Незалежне Оцінювання) [1].

Платформа масових відкритих онлайн-курсів Prometheus – перший та найбільший проект безкоштовної освіти для всіх та кожного в Україні [2].

КПІ ім. Ігоря Сікорського використовує «**Систему дистанційного навчання**», що побудована на платформі Moodle <https://do.ipokpi.ua/> [3]. У цій системі викладачі також реєструють свої дистанційні курси, створені в **G Suite for Education** [4].

Онлайн-школа «Альтернатива» – це дистанційна школа з отриманням повної загальної середньої освіти з 1 по 11 (12) клас і видачею документів державного зразка [5].

Крім сервісів, що надають базову освіту існує багато онлайн – курсів, що надані всесвітньо відомими університетами, такими як:

- 1. Six Sigma: Define and Measure, Мюнхенський технологічний університет**
- 2. Preparing to Manage Human Resources, Університет Міннесоти**
- 3. Marketing in a Digital World, Іллінойський університет в Урбана-Шампейн**
- 4. Marketing Digital: Content & Community Manager, Університет Галілео**
- 5. Introduction to Financial Accounting, Університет Пенсільванії**

Широко використовується в умовах дистанційного навчання як шкільними закладами, так і закладами вищої освіти також і сервіс **Google Classroom**, який був анонсований 6 травня 2014 року компанією Google. [6].

Забезпечення належної безпеки веб-застосунків - це дуже важлива, актуальна і не проста задача, з якою стикаються всі, хто займається розробкою відповідних продуктів. Питання безпеки веб-застосунків стали ще більш актуальними у зв'язку із масовим використанням онлайн ресурсів для дистанційного навчання. Тестування безпеки забезпечує зворотний зв'язок команди розробників про стан захищеності продукту. Згідно ISO/IEC 25010:2011 тестування безпеки є частиною функціонального тестування. SWEBOOK (Software Engineering Body of Knowledge), керівництво по розробці програмного забезпечення визначає тестування безпеки як перевірку того, що програмне забезпечення захищене від зовнішніх атак: зокрема, включає перевірки конфіденційності, цілісності та доступності систем і їх даних. Вирішити цю непросту задачу допомагають автоматизовані інструменти тестування, спрямовані на пошук уразливостей продукту.

Сьогодні існує велика кількість сканерів веб-безпеки, які допомагають спеціалістам з кібербезпеки та розробникам оцінювати безпеку продукту, а також шляхи усунення знайдених уразливостей. Розглянемо деякі з них:

w3af - це безкоштовний сканер безпеки веб-застосунків з відкритим кодом, що дозволяє проводити тестування як в ручному, так і автоматизованому режимах з використанням графічного інтерфейсу і інтерфейсу командного рядка. Сканер здатний ідентифікувати більше 200 уразливостей, в тому числі міжсайтовий скриптинг, SQL-ін'єкції.

SQLMap – безкоштовний сканер з відкритим вихідним кодом, головне завдання якого – автоматизований пошук та експлуатація SQL-ін'єкцій. Основною особливістю сканера є експлуатація знайденої уразливості.

Nikto – веб-сканер з відкритим вихідним кодом, який перевіряє веб-сервери на найчастіші помилки, що виникають через людський фактор. Перевіряє наявність неправильних конфігураційних файлів, файлів виконуваних сценаріїв, застарілого програмного забезпечення.

Burp Suite – це платна (безкоштовна містить обмежений функціонал) потужна платформа для тестування безпеки веб-додатків як в ручному, так і автоматизованому режимах з інтуїтивно зрозумілим інтерфейсом, включає інструменти зі створення карти веб-додатки, зміни запитів, фаззінга і т.д.

OWASP Zed Attack Proxy Project (ZAP) – один з найвідоміших інструментів для тестування безпеки веб-додатків.

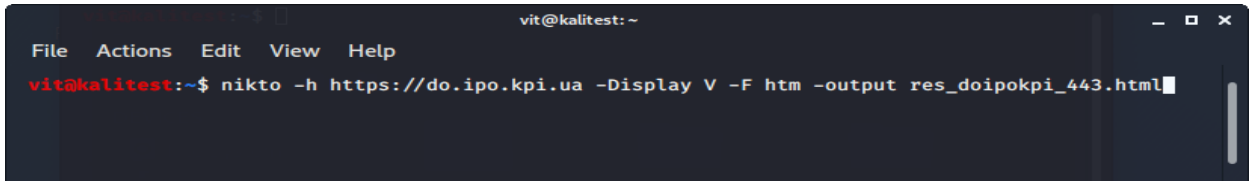
Netsparker - платний інструмент для пошуку уразливостей для всіх типів веб-додатків, таких як SQL Injection та Cross-Site Scripting (XSS). Також інструмент аналізує структуру веб-сайту на предмет розкриття службової інформації, такої як резервні копії даних, налагоджувальні веб-скрипти, приховані каталоги та інше.

Тестування безпеки в автоматизованому режимі має наступні основні переваги:

- економія і раціональне використання робочого часу, так як сканування може проводитися у фоновому режимі, і в будь-який час;
- виконання для кількох збірок або додатків в один і той же час;
- паралельний запуск декількох тестових сценаріїв для збільшення тестового покриття;
- велика кількість вбудованих різноманітних перевірок;
- згенерований звіт про результати тестування (може містити результати тестування, оцінку безпеки продукту, а також шляхи усунення знайдених уразливостей).

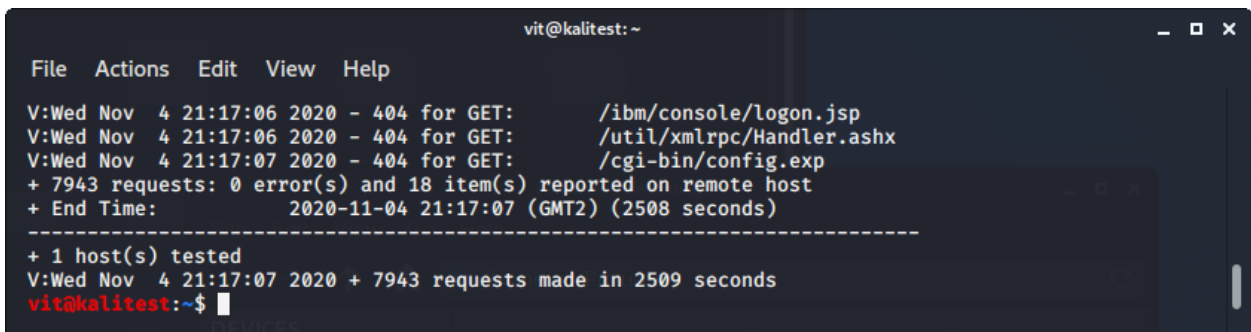
Важливим моментом є наступне: автоматизація не замінює людської участі в процесі, оскільки результати, отримані в результаті виконання автоматизованих тестів, необхідно оцінити з критичної точки зору і проаналізувати для прийняття подальших рішень.

У дослідницьких цілях спробуємо проаналізувати систему, яка використовується для дистанційного навчання КПІ ім. Ігоря Сікорського, для цього використаємо сканер веб-безпеки для пошуку уразливостей **Nikto** [7].

A screenshot of a terminal window with a dark background. The window title is "vit@kalitest: ~". The menu bar shows "File", "Actions", "Edit", "View", and "Help". The command prompt shows "vit@kalitest:~\$ nikto -h https://do.ipokpi.ua -Display V -F htm -output res_doipokpi_443.html".

```
File Actions Edit View Help
vit@kalitest:~$ nikto -h https://do.ipokpi.ua -Display V -F htm -output res_doipokpi_443.html
```

Рисунок 1 – Команда запуску сканеру Nikto.

A screenshot of a terminal window with a dark background. The window title is "vit@kalitest: ~". The menu bar shows "File", "Actions", "Edit", "View", and "Help". The output of the Nikto scan is displayed, showing three 404 errors for specific endpoints, a summary of 7943 requests, and the end time. A separator line is followed by the total number of hosts tested and the total time taken.

```
File Actions Edit View Help
V:Wed Nov 4 21:17:06 2020 - 404 for GET: /ibm/console/logon.jsp
V:Wed Nov 4 21:17:06 2020 - 404 for GET: /util/xmlrpc/Handler.ashx
V:Wed Nov 4 21:17:07 2020 - 404 for GET: /cgi-bin/config.exp
+ 7943 requests: 0 error(s) and 18 item(s) reported on remote host
+ End Time: 2020-11-04 21:17:07 (GMT2) (2508 seconds)
-----
+ 1 host(s) tested
V:Wed Nov 4 21:17:07 2020 + 7943 requests made in 2509 seconds
vit@kalitest:~$
```

Рисунок 2 – Результат роботи сканеру Nikto.

Як видно з Рисунку 2, сканер Nikto провів 7943 тести, критичних помилок не було виявлено, але сканер вказав на 18 зауважень.

Проаналізувавши файл звіту програмного сканера Nikto, ми дізналися IP адресу сайту <https://do.ipokpi.ua/>, HTTP Server який використовується, операційну систему, також дізналися яку платформу використовує система дистанційного навчання. Крім того, ми виявили, що не дивлячись на те, що в браузері сайт працює по захищеному протоколі https, деякі сторінки сайту доступні по незахищеному протоколі http.

Вказані в роботі інструменти можуть бути використані в подальшому для усунення недоліків в безпеці роботи веб-ресурсів дистанційної освіти та в коригуванні їх налаштувань.

Список використаної літератури:

1. iLearn – це безкоштовна платформа з навчальними онлайн-курсами. 2020. URL : <https://ilearn.org.ua/>
2. Prometheus – перший та найбільший проект безкоштовної освіти в Україні. 2020. URL : <https://prometheus.org.ua/>

3. Система дистанційного навчання КПІ ім. Ігоря. 2020. URL : <https://do.ipk.kpi.ua/>
4. G Suite for Education. 2020. URL : <https://edu.google.com/products/gsuite-for-education/>
5. Онлайн - школа «Альтернатива» – дистанційна школа з отриманням повної загальної середньої освіти. 2020. URL : <https://online-shkola.com.ua/>
6. Google. Google Classroom – веб-сервіс, розроблений для шкіл. 2020. URL : <https://classroom.google.com/>
7. Nikto is an Open Source (GPL) web server scanner. 2020. URL : <https://cirt.net/Nikto2>.

Озер А. К.,
факультет соціології і права.
Науковий керівник:
Фурашев В. М., к.т.н., с.н.с., доцент.

ВПЛИВ КАРАНТИННОГО РЕЖИМУ НА ОСВІТЯНСЬКУ СФЕРУ В УКРАЇНІ

Наслідки карантинних обмежень для боротьби з COVID-19 досить жорстко відобразилися на освітній сфері. За короткий час відбулася повна зміна повсякденних реалій педагогів, учнів та їх сімей. Однак, існують і більш масштабні та тривалі наслідки. Фізичне закриття вузів та шкіл пролило світло на деякі хронічні та системні проблеми, що стоять перед нашою системою освіти, надавши можливість звернути нашу увагу та зусилля на них. Крім того, воно створило умови для постановки питання про те що і як ми повинні змінити в освіті.

Нерівність, що існує в системі освіти нашої держави, не є чимось новим. Однак цей період дистанційної освіти показав глибокі диспропорції в доступі дітей до необхідної їм підтримки і можливостей. Це, мабуть, найбільш яскраво проявилось у відсутності у деяких учнів вдома доступу до комп'ютерів і Wi-Fi-підключення. Однак це лише один з аспектів величезного розмаїття ресурсів, потрібних вдома для підтримки навчання учнів, який також включає в себе наявність відповідного місця для занять, здатність батьків підтримувати навчання (в тому числі різні можливості для розвитку та інші форми соціального потенціалу), а також доступ до книг та інших матеріалів. До цього додаються здатність і готовність окремих учнів до самостійного навчання, а також необхідна основа, включаючи знання, навички самонавчання, соціальні та емоційні компетенції, необхідні для того, щоб вони могли робити це ефективно.

Найбільші проблеми фіксуються у викладанні природничо-наукових дисциплін і предметів, пов'язаних з відпрацюванням навичок: образотворче мистецтво, фізична культура, музика, технології. Природничі науки передбачають лабораторні роботи, досліди, експерименти, які неможливо проводити в домашніх умовах. Все викладання звелось до теорії. Найменша кількість проблем у викладанні гуманітарних наук. Велика кількість освітніх онлайн-платформ, розроблених, наприклад, для навчання іноземним мовам, дозволяють вчителю ефективно сформувати навчальний матеріал, зробивши уроки цікавими і пізнавальними.

У більшості повідомлень наголошується, що уроки перетворилися в самостійну роботу учнів: вчителі дають завдання, учні їх виконують і за допомогою електронної пошти відправляють на перевірку. Це призводить до великого навантаження на невідготовлених одержувачів освіти, які швидко втомлюються від дистанційного навчання: не вмикають комп'ютер, не з'являються на заняттях, не виконують завдання.

Останнім часом вчителям постійно давали поради, спрямовані на те, щоб скоротити кількість матеріалу, який необхідно охопити, і визначити основні пріоритети навчання. Слід зазначити, що було досить багато рекомендацій щодо того як підходити до дистанційного викладання та навчання. Цікаво те, що більша їх частина, мабуть, заснована на усталених принципах звичайного (очного) викладання.

В результаті карантинного режиму з'явився широкий спектр моделей і підходів до дистанційного навчання. Стає очевидним, що заклади освіти, які розробили чіткі системи і процеси, що лежать в основі їх переходу до дистанційного навчання, як правило, краще справляються з поставленим завданням. У міру того, як школи звертають свою увагу на розгляд того, яким буде життя, коли вони повністю відновлять свою роботу, є можливість подумати про засоби, механізми і культуру, які повинні бути закладені в основу їх діяльності.

Список використаної літератури:

1. Освітня сфера після карантину. URL: <https://www.pedrada.com.ua/article/2785-osvtnya-sfera-pslya-karantinu>
2. Відповіді на поширені запитання щодо організації освітнього процесу в умовах карантинних обмежень. URL: <https://mon.gov.ua/ua/osvita/zagalna-serednya-osvita/vidpovidi-na-poshireni-zapitannya-shodo-organizaciyi-osvitnogo-procesu-v-umovah-karantinnih-obmezhen>
3. Про підготовку закладів освіти до нового навчального року та опалювального сезону в умовах адаптивного карантину. URL: <https://osvita.ua/legislation/other/75378/>

Пастушак Д. В.,
фізико-технічний інститут.
Науковий керівник:
Коломицев М. В., к.т.н., доцент.

ЗАСТОСУНОК ДЛЯ КОМПЛЕКСНОГО ПОШУКУ ЗЛОЧИННОГО КОНТЕНТУ НА ВЕБ-САЙТАХ З ВИКОРИСТАННЯМ ІНСТРУМЕНТІВ BIG DATA

Люди відвідують веб-сайти щодня, але чи всі вони знають, наскільки сайти є безпечними? Насправді, яким би безпечним не виглядав сайт, є всі ризики, що він є зловмисним.

За підрахунками, до 18,5 мільйонів веб-сайтів заражені шкідливим вмістом. Це близько 1% від загальної кількості веб-сайтів в Інтернеті. [1] З першого погляду може здатися, що цей показник досить невисокий, але насправді це відсоток, який може створити значні проблеми як бізнесу, так і особистому життю. І основна проблема в тому, що більшість організацій та окремих людей недостатньо проінформовані. Наприклад, шкідливі електронні листи добре відомі завдяки лякаючим історіям, які заповнюють наші стрічки новин. Але ми менш проінформовані про шкідливі веб-сайти. І саме це робить їх небезпечними.

Пандемія COVID-19 змусила організації та фізичних осіб застосувати нові практики, такі як соціальне дистанціювання та віддалена робота. Уряди переглядають шляхи забезпечення стабільності своїх країн шляхом розробки та впровадження нових економічних планів. Тим не менш, хоча світ зосереджений на загрозах для здоров'я та економіки, спричинених COVID-19, кіберзлочинці у всьому світі, безсумнівно, виграють від цієї кризи. У березні було виявлено збільшення середньодобової кількості щойно зареєстрованих доменних імен на 569%, в порівнянні з лютим, та збільшення доменів високого ризику на 788% [1].

Шкідливий веб-сайт подібний до будь-якого іншого веб-сайту в Інтернеті: ви підключаєтесь до нього за допомогою браузера. Основною метою шкідливого веб-сайту є встановлення шкідливого програмного забезпечення на ваш персональний комп'ютер. У більшості випадків він навіть не запитує дозволу. Момент, коли ви потрапляєте на шкідливий веб-сайт, це момент, коли шкідливе програмне забезпечення починає завантажуватися.

Але чому шкідливий веб-сайт настільки оманливий? Зловмисники намагаються ввести користувачів Інтернету в оману. Ось чому вони розробляють такі веб-сайти, що виглядають як справжні. Люди, приймають швидкі рішення, базуючись на перших

враженнях, а шкідливі веб-сайти цим користуються в повній мірі. І фальшивий рівень довіри, який це породжує, незабаром може призвести до того, що буде натиснуто на посилання, яке може привести до негативних наслідків.

Дана робота являє собою розробку застосунку, для комплексного пошуку як і шкідливих посилань так і шкідливого коду на веб-сторінках використовуючи машинне навчання.

Постановка задачі та вибір інструментів для її вирішення

Щоб розробити даний застосунок потрібно просканувати значну кількість веб-сторінок, а потім обробити їхній зміст на предмет зловмисного контенту.

Для того щоб провести аналіз даних – потрібно спочатку їх отримати. Для цього буде використано Scrapy. Scrapy - це надійний веб-фреймворк для отримування даних з різних джерел [2].

Як файлове сховище використовуватиметься Amazon S3.

Для обробки великих об'ємів даних, що були витягнуті та збережені попередніми інструментами буде використано Apache Spark. Spark має власну бібліотеку для машинного навчання [3], що значно облегшує роботу.

Розробка методів комплексного пошуку зловмисного контенту

Оскільки даний застосунок буде використовуватись для комплексного пошуку зловмисного контенту, то і видів контенту повинно бути більше одного. В даний роботі запропоновано аналіз посилань, на які направляє витягнута веб-сторінка, та JavaScript коду на цих веб-сторінках.

Для реалізації першого виду пошуку потрібен набір даних з уже класифікованими посиланнями. Для цього нам підійдуть посилання на фішингові сторінки, сторінки, що розсилають спам, шкідливе ПЗ, а також потрібні і доброякісні сторінки. В інтернеті є реєстри різних посилань, як-от <http://www.joewein.de/sw/blacklist.htm>, що є реєстром спам-посилань.

Скомпільовавши набір даних з посиланнями, потрібно його також і промаркувати. Всі посилання, що надійшли з реєстрів шкідливих отримують марку шкідливості 1, ті, що взяті з <https://majestic.com/reports/majestic-million>, шкідливими не вважаються (марка - 0). Всього в наборі даних є 54955 шкідливих та 52384 нешкідливих посилань.

Використано 3 алгоритми машинного навчання (Naïve Bayes, SVM, Logistic Regression)[4], отримано такі результати ефективності:

Алгоритм	Accuracy	F-score	Recall	Precision
Naïve Bayes	86.453	86.746	82.910	88.91

	2	71	5	
Logistic Regression	3	92.342	93.595	90.761
SVM	6	97.010	97.031	94.241
				95.614
				99.990

З цього випливає, що найкращим алгоритмом для даної класифікації є SVM (Метод опорних векторів).

Для другого виду пошуку буде використано код веб-сторінок, а саме його JavaScript-сценарії. Використано сервіс PhishTank, а також GeeksOnSecurity для генерації тренувального набору даних. Було підібрано більше 40 ознак для тренування, які були видобуті з коду сторінок ще на етапі їхнього завантаження. Було розглянуто ті ж 3 алгоритми, що і в попередній класифікації і отримані такі результати:

Алгоритм	Accuracy	F-score	Recall	Precision
Naïve Bayes	88.257	88.746	85.831	90.36
Logistic Regression	95.693	95.886	92.48	97.795
SVM	96.489	97.01	93.86	98.91

Як і в минулому досліді найкраще себе показує SVM.

Порівняння з уже існуючими способами пошуку зловмисного контенту на веб-сайтах

Існує подібний сервіс для аналізу коду сторінок [5], проте в цьому проекті виконувався тільки статичний аналіз, без використання машинного навчання і найкращий показник точності становить 89.44%, де у даній роботі – 96.489%. У іншому проекті було реалізовано аналіз послідовностей системних викликів [6]. Точність такої класифікації 94%. Також у обох роботах відсутній аналіз посилань, на які може направляти аналізована сторінка, який присутній в даній роботі.

Подальші дослідження

Даний застосунок буде використано для сканування та обробки 10 млн. сторінок. Також буде розроблено веб-інтерфейс для зручності отримання з нього статистики.

Висновок

В даній роботі було показано застосунок для комплексного пошуку зловмисного контенту на веб-сторінках, який показав дуже надійні результати. Також

було проведено порівняльний аналіз зі вже існуючими застосунками, який доводить, що запропонований застосунок має новизну та є особливо актуальним в час пандемії COVID-19.

Список використаної літератури:

1. Palo Alto Networks Blog [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: <https://unit42.paloaltonetworks.com/how-cybercriminals-prey-on-the-covid-19-pandemic/>.
2. Learning Scrapy. [Текст] / Dimitrios Kouzis-Loukas. – 2016. – (Packt Publishing) – 481 с.
3. Jalaj Thanaki Python Natural Language Processing [Текст] / Jalaj Thanaki. – 2017. – (Packt Publishing) – 468 с.
4. Learning Spark, 2nd edition [Текст] / Jules S. Damji, Brooke Wenig, Tathagata Das, Denny Lee. – 2020. – (O'Reilly Media) – 399 с.
5. AMA: Static Code Analysis of Web Page for the Detection of Malicious Scripts [Електронний ресурс]. /Prabhu Seshagiria, Anu Vazhayilb, Padmamala Sriramb – 2018 – Режим доступу до ресурсу: <https://doi.org/10.1016/j.procs.2016.07.291>
6. Detection of Malicious Web Pages Using System Calls Sequences. [Електронний ресурс]./ Canfora G., Medvet E., Mercaldo F., Visaggio C.A. – 2018 – Режим доступу до ресурсу: https://doi.org/10.1007/978-3-319-10975-6_17.

Калиновська В. В.,
фізико-технічний інститут.
Науковий керівник:
Качинський А. Б., д.т.н., професор.

ІНТЕЛЕКТУАЛЬНІ СИСТЕМИ КІБЕРЗАХИСТУ МЕРЕЖ ЕЛЕКТРОПОСТАЧАННЯ ТА ЇХ НАДІЙНІСТЬ

Система електромереж фізично пов'язує виробництво електроенергії та споживачів електроенергії. Основною функцією електромережі є економічна доставка електроенергії з урахуванням обмежень потужності та надійності енергетичного обладнання та ліній електропередач.

Традиційно системи автоматизації електромереж були фізично ізольовані від корпоративної мережі, часто використовуючи власні протоколи та застаріле обладнання та програмне забезпечення. Нещодавнє відкриття того, що хакери вставили програмне забезпечення в електричну мережу США, що дозволило б в подальшому порушити роботу мережі з віддаленого місця, наочно демонструє той

факт, що комунальна інфраструктура досить вразлива і що її загальна місія обслуговування населення може бути серйозно скомпрометовано в результаті несподіваних техногенних або природних катастроф. Оскільки в інших галузях промисловості вже є досвід систем автоматизації озброєння сучасними ІТ-технологіями, електроенергетика також стикається з тенденцією інтеграції електричної інфраструктури з інформаційною інфраструктурою, яка є так званою «розумною мережею» [1].

У даній роботі розглядається підхід до розробки і використання систем кіберзахисту, заснований на виділенні інтелектуальної надбудови над традиційними механізмами захисту і побудові єдиного уніфікованого середовища для створення і підтримки функціонування систем захисту. В рамках вирішення завдання кіберзахисту досліджується комплекс формальних методів, моделей, алгоритмів і побудованих на їх основі програмних прототипів, що реалізують різні інтелектуальні механізми захисту.

Перспективним підходом до побудови інтелектуальних механізмів кіберзахисту є технологія інтелектуальних багатоагентних систем. В рамках цього підходу компонентами багатоагентної системи кіберзахисту є інтелектуальні автономні програми (агенти захисту). Вони дозволяють реалізувати комплексну надбудову над механізмами безпеки використовуваних мережевих програмних засобів, операційних систем і додатків, підвищуючи захищеність системи до необхідного рівня[2]. Ознайомимося з архітектурою типового агента (рис.1).

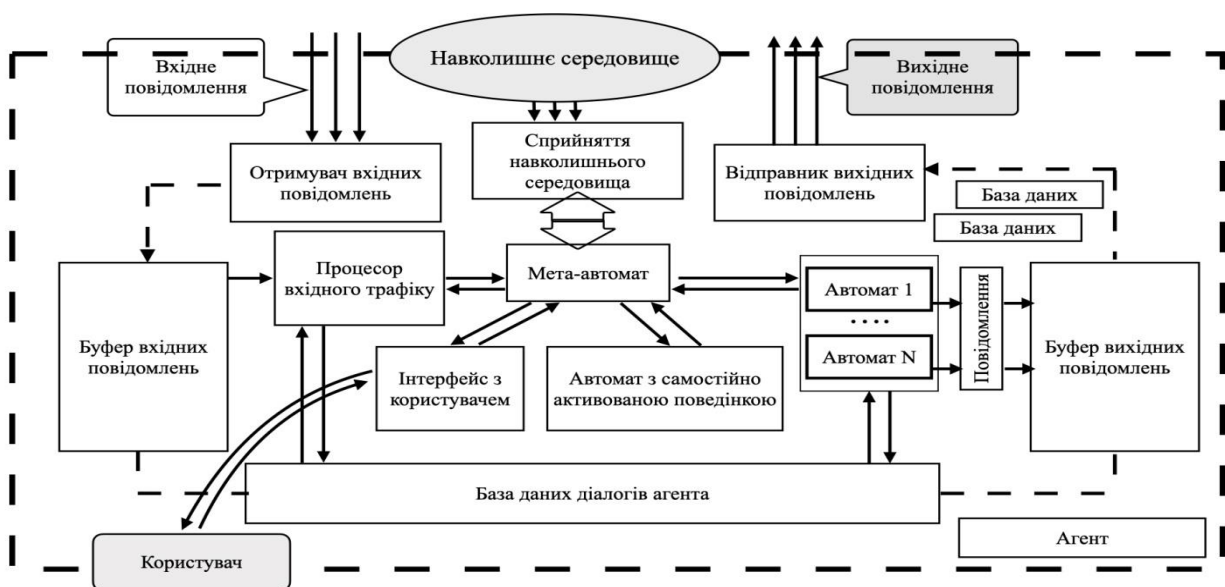


Рис.1. Архітектура типового агента

Нехай стан кожного із елементів структурної схеми позначається двома змінними: 1 (елемент справний), 0 (елемент в непрацездатному стані). В такому разі функціонування системи можна описати за допомогою функцій алгебри логіки (ФАЛ), використовуючи операції кон'юнкції, диз'юнкції та інверсії. Розглянемо процедуру побудови ФАЛ для нашої системи, що відповідає працездатній системі з послідовно-паралельними з'єднаннями елементів. Система є діючою за умови, що всі вони працездатні. Наприклад, нехай x_i - справний стан i -го елемента, $\bar{x}_i$ - несправний стан, $i = 1, 2, \dots, k$. Розглянемо таблицю (Табл.1), яка відображає відмовостійкість системи, що досліджується [3].

Таблиця 1. Відмовостійкість агента

№ п/п	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	x_9	x_{10}	x_{11}	y
1	1	1	1	1	1	1	1	1	1	1	1	1
2	1	1	1	0	0	0	0	0	0	1	1	1
3	1	1	1	1	0	0	0	0	0	1	1	1
4	1	1	0	0	0	0	0	0	0	1	1	0
5	1	1	1	1	1	0	0	0	0	1	1	1
6	1	1	1	1	1	1	0	0	0	1	1	1
7	1	1	1	1	1	1	1	0	0	1	1	1
8	1	1	1	1	1	1	1	1	0	1	1	1
9	1	1	0	0	1	1	1	1	1	1	1	0
10	1	1	1	1	1	0	1	1	1	1	1	1
11	1	1	1	1	1	0	0	1	1	1	1	1
12	1	1	1	1	1	1	1	0	1	1	1	1
13	1	1	0	1	1	1	1	1	1	1	1	1
14	1	1	0	1	0	1	1	1	1	1	1	0
15	1	1	0	1	1	0	0	1	1	1	1	1
16	1	1	0	1	1	1	0	0	1	1	1	1
17	1	1	0	1	1	1	0	0	1	1	1	1
18	1	1	0	1	1	1	1	0	1	1	1	1
19	1	0	1	1	1	1	1	0	1	1	1	0
20	1	1	0	0	1	1	0	0	0	0	1	0
21	1	1	1	1	1	1	0	0	1	1	1	1
22	1	1	1	1	1	1	0	1	0	1	1	1
23	1	1	1	1	1	0	0	0	1	1	1	1
24	1	1	1	1	1	0	0	1	0	1	1	1
25	1	1	1	1	1	0	1	0	0	1	1	1

Тоді наступна досконала диз'юнктивна нормальна форма буде функцією алгебри логіки, яка описує працездатний стан системи:

$$\begin{aligned}
y(X_1, X_2, X_3, X_4, X_5, X_6, X_7, X_8, X_9, X_{10}, X_{11}) = & X_1 X_2 X_3 X_4 X_5 X_6 X_7 X_8 X_9 X_{10} X_{11} \vee X_1 X_2 X_3 \bar{X}_4 \bar{X}_5 \bar{X}_6 \bar{X}_7 \bar{X}_8 \bar{X}_9 X_{10} X_{11} \vee \\
& X_1 X_2 X_3 X_4 \bar{X}_5 \bar{X}_6 \bar{X}_7 \bar{X}_8 \bar{X}_9 X_{10} X_{11} \vee X_1 X_2 X_3 X_4 X_5 \bar{X}_6 \bar{X}_7 \bar{X}_8 \bar{X}_9 X_{10} X_{11} \vee X_1 X_2 X_3 X_4 X_5 X_6 \bar{X}_7 \bar{X}_8 \bar{X}_9 X_{10} X_{11} \vee \\
& X_1 X_2 X_3 X_4 X_5 X_6 X_7 \bar{X}_8 \bar{X}_9 X_{10} X_{11} \vee X_1 X_2 X_3 X_4 X_5 X_6 X_7 X_8 \bar{X}_9 X_{10} X_{11} \vee X_1 X_2 X_3 X_4 X_5 \bar{X}_6 X_7 X_8 X_9 X_{10} X_{11} \vee \\
& X_1 X_2 X_3 X_4 X_5 \bar{X}_6 \bar{X}_7 X_8 X_9 X_{10} X_{11} \vee X_1 X_2 X_3 X_4 X_5 X_6 \bar{X}_7 X_8 X_9 X_{10} X_{11} \vee X_1 X_2 \bar{X}_3 X_4 X_5 X_6 X_7 X_8 X_9 X_{10} X_{11} \vee \\
& X_1 X_2 \bar{X}_3 X_4 X_5 \bar{X}_6 \bar{X}_7 X_8 X_9 X_{10} X_{11} \vee X_1 X_2 \bar{X}_3 X_4 X_5 X_6 \bar{X}_7 \bar{X}_8 X_9 X_{10} X_{11} \vee X_1 X_2 \bar{X}_3 X_4 X_5 X_6 X_7 \bar{X}_8 X_9 X_{10} X_{11} \vee \\
& X_1 X_2 X_3 X_4 X_5 X_6 \bar{X}_7 X_8 X_9 X_{10} X_{11} \vee X_1 X_2 X_3 X_4 X_5 X_6 \bar{X}_7 X_8 \bar{X}_9 X_{10} X_{11} \vee X_1 X_2 X_3 X_4 X_5 \bar{X}_6 \bar{X}_7 \bar{X}_8 X_9 X_{10} X_{11} \vee \\
& X_1 X_2 X_3 X_4 X_5 \bar{X}_6 \bar{X}_7 X_8 \bar{X}_9 X_{10} X_{11} \vee X_1 X_2 X_3 X_4 X_5 \bar{X}_6 X_7 \bar{X}_8 \bar{X}_9 X_{10} X_{11}
\end{aligned}$$

Функція алгебри логіки може бути математичною моделлю функціонування системи в сенсі її надійності.

Компоненти багатоагентної системи виявлення вторгнень – це взаємодіючі між собою агенти, що спільно вирішують загальну задачу виявлення вторгнень в комп'ютерну мережу. Архітектура багатоагентної системи виявлення вторгнень включає один або кілька примірників агентів різних типів, спеціалізованих для вирішення підзадачі виявлення вторгнень. Агенти розподілені по хостам мережі, що захищається, спеціалізовані за типами розв'язуваних завдань і взаємодіють один з одним з метою обміну інформацією та прийняття узгоджених рішень. У прийнятій архітектурі досліджуваного прототипу багатоагентної системи виявлення вторгнень в явному вигляді відсутній «центр управління» сімейством агентів – залежно від ситуації, що склалася головним може ставати будь-який з агентів, який ініціює та (або) реалізовує функції кооперації та управління. Передбачається, що архітектура багатоагентної системи виявлення вторгнень може адаптуватися до реконфігурації мережі, зміни трафіку і нових видів атак, використовуючи накопичений досвід.

Звісно ж, що найбільш дієвий шлях виявлення розподілених багатофазних атак, спрямованих на комп'ютерні мережі, полягає в кооперації безлічі агентів захисту, розподілених по хостам мережі. Тому основна перевага багатоагентної системи виявлення вторгнень полягає в можливості щодо «легких» компонентів системи співпрацювати і спільно вирішувати складну задачу виявлення таких атак.

Висновок. Були розглянуті інтелектуальні системи кіберзахисту мереж електропостачання та був проведений аналіз їх надійності. Підхід заснований на реалізації інтелектуальних механізмів управління захистом і побудові єдиного уніфікованого середовища для створення і підтримки функціонування систем захисту на всьому їхньому життєвому циклі, включаючи адаптивне управління політиками безпеки.

Список оригінальної літератури:

1. Котенко, И.В. Интеллектуальные механизмы управления кибербезопасностью / И.В. Котенко // Труды ИСА РАН. – 2009. – Т. 41. – С.74-103.

2. Половко А.М. Основы теории надежности / А.М. Половко, С.В. Гуров. -СПб.: БХВ-Петербург, 2006. — 702 с.

Дудка В. О.,
факультет інформатики та
обчислювальної техніки.
Науковий керівник:
Самчинська О.А., викладач.

ПРОБЛЕМА ФЕЙКІВ ПІД ЧАС ПАНДЕМІЇ КОРОНАВІРУСУ

Сьогодні, у зв'язку з поширенням хвороби COVID-19 в Україні, кожен громадянин має потребу в оперативній і перевірненій інформації. Однак, у зв'язку з популярністю даної хвороби, в мережі Інтернет, поряд з правдивою інформацією, з'являється багато фейків. Згідно з дослідженням соціальних мереж, проведеним українською консалтинговою компанією «Центр контент-аналізу», 37% новин є фейками, а ще 26% - неможливо визначити через відсутність доказів. Аналіз показав, що «панічні» новини містять неправдиві відомості в 64% випадків, а «заперечливі» - в 54% [1]. Ці дані свідчать про те, що більш ніж половина новин в соціальних мережах є або обманом, або не мають переконливих доказів.

Завдяки вебресурсу «По той бік пандемії» [2] можна отримати доступ до вже відомих фейків. Наприклад, існує інформація про «блокувальники вірусів» у вигляді бейджів [3]. Ці предмети, як запевняють продавці, захищають від будь-яких вірусів і алергії, проте ніяких реальних доказів їх користі немає. Ймовірний прототип цього пристрою, «Virus protector», розроблявся в Японії, але у 2013 році Агенство з питань захисту прав споживачів Японії винесло попередження людям негайно припинити використовувати продукти цієї торгової марки, бо деякі з користувачів цього пристосування отримали хімічні опіки.

Ще одним прикладом фейку є новина про штучне походження коронавірусу [4]. Цікаво, що розповсюджувачем цих чуток є нобелівський лауреат, вірусолог Люк Монтаньє. І все ж це твердження є безпідставним. Дослідження індійських біоматематиків, на яких посиляється професор, були опубліковані на сайті bioRxiv. Там дійсно розміщують наукові звіти. Але специфіка ресурсу така, що тексти не рецензуються. А тому їх не можна розглядати як переконливі або остаточно доведені. Через виникнувший ажітаж, і безліч критики від інших вчених автори власноруч вилучили свій текст.

Кабінет Міністрів України використовує доступні засоби для боротьби з розповсюдженням фейкової інформації. Так, наприклад, МВС України закликає громадян повідомляти Департамент кіберполіції Національної поліції України про її поширення [5]. Відповідно до статті 173-1 (Поширювання неправдивих чуток) Кодексу України про адміністративні правопорушення, поширення неправдивої інформації тягне за собою штраф від десяти до п'ятнадцяти неоподатковуваних мінімумів доходів громадян або виправні роботи на строк до одного місяця з відрахуванням двадцяти процентів заробітку [6]. Реальним прикладом застосування даної статті може послужити притягнення до відповідальності розповсюджувача недостовірної інформації про кількість в Україні випадків захворювання на COVID-19, у тому числі й з летальними наслідками [7]. Порушник був виявлений під час моніторингу мережі Інтернет співробітниками Глибоцького відділення поліції. Цей та інші подібні прецеденти дають можливість зробити висновок, що дії, вжиті урядом, дійсно працюють і допомагають протистояти потоку фейків в соціальних мережах і мережі Інтернет [8].

Однак, незважаючи на описані вище дії, на сьогоднішні існує безліч недостовірних джерел інформації, причому деякі з яких можуть заподіяти шкоду людям, викликати паніку серед населення або порушення громадського порядку. Через це важливим і актуальним є вміння протистояти таким фальсифікаціям. На вебресурсі Amnesty International розміщена стаття [9], в якій наводиться перелік сайтів з перевіреною інформацією, а також деякі поради, як ставитися до інформації про коронавірус. На мою думку, одним з найбільш ефективних способів перевірки новини, є аналіз її джерел. Як вбачається з прикладів, більшість фейків посилаються на невірогідні дані, або ж зовсім ні на що не посилаються. Використання цього та інших простих правил може допомогти уникнути більшості популярних хибних домислів і чуток.

Список використаної літератури:

1. Тривожний діагноз: комунікаційна криза в українських соцмережах під час карантину. URL: <https://ukrcontent.com/reports/trivozhnij-diagnoz-komunikacijna-kriza-v-ukrainskih-socmerezah-pid-chas-karantinu.html> (дата звернення: 07.05.2020).
2. По той бік пандемії. URL: <https://coronafakes.com/> (дата звернення: 07.05.2020).
3. Фейк про “блокувальники вірусів” у вигляді бейджів. URL: <https://coronafakes.com/fake/feyk-pro-blokuval-nyky-virusiv-u-vyhliadi-beydzhiv/> (дата звернення: 07.05.2020).

4. Фейк від нобелівського лауреата професора Монтаньє. URL: <https://coronafakes.com/fake/feyk-vid-nobelivs-koho-laureata-profesora-montan-ie/> (дата звернення: 07.05.2020).
5. МВС України. URL: <https://www.facebook.com/mvs.gov.ua/photos/a.737527876333906/2856564351096904/?type=3> (дата звернення: 08.05.2020).
6. Кодекс України про адміністративні правопорушення. URL: <https://zakon.rada.gov.ua/laws/show/80731-10#n1863> (дата звернення: 08.05.2020).
7. За поширення неправдивих чуток поліція склала на жителя Чернівецьчини адмінпротокол. URL: <https://www.npu.gov.ua/news/Informacziya/za-poshirennya-nepravdivix-chutok-policziya-sklala-na-zhitelya-chernivechchini-adminprotokol/> (дата звернення: 08.05.2020).
8. СБУ притягає до відповідальності осіб, які поширюють фейки про коронавірус. URL: <https://ssu.gov.ua/ua/news/1/category/21/view/7300#.09sE4XQP.dpbs> (дата звернення: 08.05.2020).
9. Інформаційна гігієна під час пандемії коронавірусу (гайд). URL: <https://www.amnesty.org.ua/media-literacy-covi19/> (дата звернення: 07.05.2020).

*Нагорний М. Ю.,
Факультет інформатики та
обчислювальної техніки.
Науковий керівник:
Самчинська О. А., викладач.*

ПРОБЛЕМА ФЕЙКІВ В СОЦІАЛЬНИХ МЕРЕЖАХ ТА ЗМІ В ПЕРІОД КАРАНТИНУ

2020 рік запам'ятається людству надовго, адже не залишилося жодної країни нашої Земної кулі, яка б не отримала виклик – COVID-19.

Першочергово уряду потрібно було вжити певних заходів задля безпеки громадян, захисту їх життя і здоров'я. Тож Україна вдалася до надзвичайних кроків безпеки: введення карантинного режиму. Адже карантин – це безпека.

У період ізоляції від зовнішнього світу люди позбавлені активного спілкування, але потреба в отриманні інформації навпаки значно зросла. Насамперед перед кожною свідомою людиною постало багато запитань: що таке коронавірус, як розпізнати захворювання, кількість захворілих, чим небезпечний COVID-19, як з ним боротися тощо. На всі ці питання у період пандемії ми маємо можливість отримати відповідь лише за допомогою засобів масової інформації та соціальних мереж.

А чи можемо ми стовідсотково довіряти тій інформації, яку чуємо і бачимо по телебаченню, отримуємо від друзів та знайомих із соціальних мереж? Чи вся інформація, яку ми читаємо або чуємо зі ЗМІ, правдива? Адже вже давно сучасний світ формується не лише за допомогою інформації, а й дезінформації.

Фейкові новини – це навмисне поширення брехні з метою змінення громадської думки або розділення людей на кілька ворогуючих таборів [1]. На створенні й розповсюдженні фейкової інформації, її автори заробляють великі гроші. Для цього використовують різні інструменти: вигадують історії, спеціальним чином монтують різноманітні фото та відеоматеріали. І все це, на жаль, робиться достатньо професійно.

Фейковий продукт створюється, як правило, або на інформації, що є частково правдивою, або є повністю неправдивою. На жаль, фейки можна зустріти не тільки в жовтій пресі, але й в популярних респектабельних засобах масової інформації. Фейкові новини створюються максимально схожими на справжні, інколи навіть досвідчені професіонали не завжди можуть відрізнити їх від підробки.

Саме фейки є причиною паніки, адже люди схильні довіряти будь-якій інформації. І навіть якщо до істини далеко, вони охоче повірять у брехню та ще й розповсюдять її. І чим більше її поширюють, тим правдивішою виглядає вона для інших [2].

Впродовж тримісячної пандемії захворювання обросло такою кількістю чуток і вигадок, що інколи ця інформація вражає своєю нелогічністю й абсурдністю. А деякі з цих пліток вже стали зброєю в інформаційних війнах не лише громадян, а й цілих країн. Чому виникає така ситуація? Від чого це залежить? Чого не вистачає сучасним користувачам медіа контенту? Наскільки наразі важливе питання додержання інформаційної культури і морально-етичних норм в соціальних мережах та ЗМІ? Навіщо сучасній людині потрібно бути медіаграмотним? На всі ці питання можна отримати відповідь, якщо розібратися в понятті інформаційної культури.

Інформаційна культура (від лат. information – роз’яснення, висловлення) – сукупність норм, правил і стереотипів поведінки та культури, що пов’язані з інформаційним обміном у суспільстві [6]. У широкому сенсі ІК є сукупністю принципів і механізмів, що забезпечують взаємодію етнічних і національних культур, їх включення в загальний досвід людства [3].

Критеріями нової інформаційної культури є вміння людини адекватно формулювати свою потребу в інформації, знаходити її, переробляти, відбирати, оцінювати і створювати якісно нову. Окрім цього, це вміння людини мати адекватну культуру поведінки в умовах комп’ютерно-мережевого середовища [4].

Все вище перераховане повинне базуватися на усвідомленні ролі інформації у суспільстві, знанні законів інформаційного середовища та розумінні свого місця в ньому, володінні новими інформаційними технологіями [5].

У зв'язку з прийняттям Постанови Кабінету Міністрів «Про запобігання поширенню на території України коронавірусу COVID-19» було організовано частково дистанційну роботу та освіту. На жаль, багато свого часу при виконанні роботи відділено громадяни почали витратити на так званих «пожирачів часу» – соціальні мережі, пусті балачки по телефону тощо. На даний час кожна соціальна мережа розміщує інформацію про COVID-19, моніторинг захворюваності у світі та кожній країні зокрема. Окремі «гумористи» розміщують на своїх сторінках різноманітні жарти, що стосуються ізоляції та захворювання в цілому тощо. Отриманий «вінегрет» із новин пересічні громадяни не можуть розділити на окремі інгредієнти, адже не всі українці можуть похвалитися високою медіаграмотністю. Люди «проковтнули» безліч фейків про коронавірус. Наприклад, що вірус кілька днів живе у горлі або про винахід ліків від COVID-2019. Перший фейк стверджує, що вірус перед тим, як вразити легені, живе в горлі до 4 днів. Тому так звані «спеціалісти» рекомендують пити гарячі напої або міцний алкоголь, що змиють вірус у шлунок, де його нібито знищить кислота. Другий – говорить про винахід ліків, що рятує від коронавірусу. Фейк стверджує, що в деяких країнах завдяки даному винаходу змогли врятувати навіть важкохворих. Насправді ж є інформація про експериментальні випробування деяких медикаментів від інших хвороб, котрі не впливають на вірус, проте можуть послабити наслідки, які він викликає в організмі людини [2].

І в першому, і в другому випадку коментарі надають ВООЗ і МОЗ України: такі методи лікування не підтверджують, а спеціалісти в галузі вірусології стверджують, що вакцини або медичного препарату від цієї хвороби на сьогодні не існує, а тому закликають людей не скуповувати ліки, котрі можуть завдати більше шкоди, аніж допомогти [2]. І взагалі медичні працівники не рекомендують займатися самолікуванням, а при перших симптомах захворювання звертатися за консультацією до лікаря.

Найжахливіше те, що подібні фейки розслабляють людей та змушують їх несерйозно ставитися до ситуації з пандемією. Неправдива інформація починає стрімко розповсюджуватися, коло людей, яке потрапляє під загрозу, стає ширшим. Багато людей просто ігнорують заклики влади дотримуватися карантинних заходів.

Чому українці не можуть відрізнити правдиві новини від фейку? Чому саме фейкова інформація є такою популярною в Україні і не тільки? Психологи пояснюють це тим, що люди за своєю природою схильні до ідей підозри та викриттів [2].

Економічний стан в країні викликає суспільне незадоволення з боку її громадян. Майже кожен українець невдоволений багатьма українськими системами: охороною здоров'я, освітою тощо. Люди настільки перестали довіряти державі, що будь-які дії з її боку ставлять під сумнів. Люди зневірилися, тому шукають і вірять всьому, що їм пропонують в ЗМІ та соціальних мережах.

І тут знову постає питання інформаційної культури. Якби люди були більш медіаграмотними, чи вплинуло б це на ситуацію з пандемією в Україні? Вважаю, що однозначно ситуація була б кращою. Кожен пересічний українець повинен усвідомити, що не вся інформація в соціальних мережах є правдивою. Перед тим як ділитися такою інформацією, варто її перевірити. Адже спеціалісти радять більше звертатися до офіційних джерел, так би мовити «фільтрувати» й перевіряти кожную інформацію у соціальних мережах.

Список використаної літератури:

1. Що таке фейк? URL: <https://artefact.live/?p=411> (дата звернення 03.05.2020).
2. Топ-10 фейків про коронавірус і чому люди довіряють чуткам та вигадкам. URL: <https://galychyna.if.ua/analytic/top-10-feykiv-pro-koronavirus-i-chomu-lyudi-doviryayut-chutkam-ta-vigadkam/> (дата звернення 03.05.2020)
3. Українська бібліотечна енциклопедія. URL: <http://ube.nlu.org.ua/article/%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B0%20%D0%BA%D1%83%D0%BB%D1%8C%D1%82%D1%83%D1%80%D0%B0> (дата звернення 03.05.2020).
4. Роль комп'ютерної етики в формуванні інформаційної культури користувачів комп'ютерно-мережевого середовища. Л.Я.Філіпова, доктор педагогічних наук, професор, професор кафедри інформаційних технологій Харківської державної академії культури. URL: <http://journals.urau.ua/bdi/article/download/187981/187182> (дата звернення 03.05.2020).
5. Інформаційна культура як основа загальної культури людини. URL: https://mdgu-kid.at.ua/publ/informacijna_kultura_jak_osnova_zagalnoji_kulturi_ljudini/1-1-0-68 (дата звернення 03.05.2020).
6. Герчанівська П.Е. Культурологія: термінологічний словник / П.Е. Герчанівська. – К. Національна Академія керівних кадрів культури і мистецтв, 2015. – 439 с., с.79. URL: https://nakkkim.edu.ua/images/vidannya/Monografii/Gerchanivska_Slovnyk_compressed.pdf (дата звернення 07.05.2020).

Головатюк О. А.,
факультет соціології і права.
Науковий керівник:
Бежвець А. М., старший викладач.

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, відбуваються 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 висновок 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 отримання 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, кількості захворівших та тих, хто вилікувався. 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, противірусні 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 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 [Електронний ресурс]. – 2020. URL: <https://delo.ua/economyandpoliticsinukraine/kabmin-ustanovil-v-ukraine-adaptivnyj-karantin-s-368695/>

Безпалько С. О.,
факультет інформатики та
обчислювальної техніки.
Науковий керівник:
Самчинська О. А., викладач.

ІНФОРМАЦІЙНА КУЛЬТУРА І МОРАЛЬНО-ЕТИЧНІ НОРМ В СОЦІАЛЬНИХ МЕРЕЖАХ ТА ЗМІ В ПЕРІОД КАРАНТИНУ

Вперше в сучасній історії людства, пандемія, що поширилася світом, змусила кожного пристосовуватися до незвичних правил, і перелаштувати повсякденність, щоб убезпечити себе і близьких від страшної небезпеки – коронавірусу COVID-19. Ще зовсім нещодавно, страшна епідемія лише починалась в Китаї, а зараз це вже пандемія і вона забрала тисячі людських життів у всьому світі. У зв'язку з введенням карантинного режиму, люди проводять більше часу у соціальних мережах та активно користуються ЗМІ. Хтось споживає вже готову інформацію, а хтось її поширює, в тому числі і про коронавірус COVID-19.

Та чи дотримуються інформаційної культури і морально-етичних норм в соціальних мережах та ЗМІ?

Як відомо, інформаційна культура – це оптимальні способи поводження з інформацією та подання її споживачу для вирішення теоретичних і практичних завдань; механізми вдосконалення технічних засобів виробництва, зберігання і передачі інформації; розвиток системи навчання, підготовки людини до ефективного використання інформаційних засобів та інформації [2].

Кожного дня ми вмикаємо телевізор чи гортаємо сторінки в соціальних мережах і бачимо страшну статистику та жахливі подробиці пандемії. Та не завжди інформація, яку нам пропонують - достовірна, є випадки оприлюднення неправдивої інформації, у якій перекручено факти або ж зведено наклеп чи завдано моральної образи людині.

8 квітня видання «Вести» опублікувало фейковий список домашніх адрес жителів міста Києва, хворих на COVID-19, що на деякий час посилило паніку серед населення та зумовило упереджене ставлення сусідів до мешканців зі списку.

Завдяки відкритим джерелам в інтернеті та ЗМІ, ширяться чутки, що приписують технологіям 5G не останню роль у поширенні коронавірусу. Це призвело до жахливих наслідків. Щонайменше 20 телекомунікаційних веж у різних частинах Великої Британії зазнали спалювання або інших актів вандалізму. Деякі напади були здійснені на телекомунікаційні вежі, які навіть не мають 5G, а натомість роздають мобільний зв'язок 3G та 4G.

Варто зазначити, що в соціальних мережах та через ЗМІ діють інтернет-провокатори. Користуючись ситуацією, певні особи провокують паніку і протестні настрої серед громадян, намагаються дискредитувати владу, закликають до порушення конституційного ладу. Крім того, СБУ зафіксувала появу великої кількості деструктивних спільнот на різних інформаційних майданчиках. Як відомо, панічні настрої, які поширюється через інформаційний простір, здатні фізично послаблювати людей, які відносяться до так званих «груп ризику». Серед них не лише люди зі слабким здоров'ям чи імунітетом, а й люди, схильні до навіювання.

Не може не викликати сумніви і інформація, що американський мільярдер Білл Гейтс придумав коронавірус як «якийсь диявольський план для скорочення чисельності населення, масової чипізації і навіть нанесення електронних штрих кодів» [1].

Соціальні мережі стали успішною платформою для продажі масок та антисептичних засобів. На даний момент, велика кількість інтернет-магазинів, які раніше не спеціалізувались на výroбах медичного призначення, виготовляють захисні

маски. Бувають випадки, коли продавці цих товарів вимагають передплату. Після отримання коштів вони видаляють свої оголошення та зникають. Саме тому, кіберполіція неодноразово закликала громадян купувати товар лише на перевірених ресурсах та без передоплати.

Велика кількість «лідерів думок» стали вести блоги про пандемію коронавірусу COVID-19, адже тема актуальна, вільного часу в умовах карантину вдосталь, а це до того ж непоганий заробіток. У соціальних мережах можна зустріти відео-інструкції щодо правильного використання медичних засобів індивідуального захисту, які створені людьми, які не мають медичної освіти та навіть не пройшли жодних навчальних курсів стосовно даного питання.

З початком пандемії, в додатку Instagram з'являлося безліч AR-фільтрів, присвячених захворюванню. Наприклад, був фільтр «What are you», який «опитує» користувачів, чи хворіють вони на коронавірус. На щастя, з додатку видалили всі ефекти доповненої реальності, які стверджують, що «діагностують» або «лікують» коронавірус.

В умовах карантину знову постало питання про право громадян на інформацію, її доступність у будь-який час і в будь-якому місці. Доступна інформація дає можливість отримувати якісніші медіаматеріали, аналітику даних, сервіси, продукти.

Право на інформацію гарантовано Конституцією України (ст. 34). Ситуація, що склалася у світі, спонукала експертів з питань доступу до інформації, антикорупції та відкритих даних простежити за реалізацією права на інформацію під час пандемії. Під час карантину доступ до публічної інформації – право гарантоване, влада зобов'язана інформувати про ситуацію з COVID-19 оперативно, адже відсутність інформації та даних про коронавірус сприяє поширенню фейків та дезінформації. За даними моніторингу Офісу Уповноваженого з прав людини, лише 76% розпорядників публічної інформації належно оприлюднюють на офіційних веб-сайтах інформацію щодо розпоряджень, спрямованих на протидію поширенню коронавірусної хвороби (COVID-19). А плани відповідних протиепідемічних заходів належним чином оприлюднює тільки половина розпорядників [3].

Під час карантинного періоду вживаються заходи для боротьби з фейковою інформацією стосовно пандемії коронавірусу COVID-19, що буде продовжено і в посткарантинний період.

На державному рівні кіберполіція блокує шахрайські посилання про COVID-19 та виявляє осіб, що розповсюджують неправдиву інформацію.

Керівництво соціальних платформ і мереж теж не залишаються осторонь питань інформаційної безпеки. З початку пандемії коронавірусу компанія Google, якій

належить YouTube, впровадила багато змін, які мають боротися з поширенням фейків про COVID-19. Із березня в результатах пошуку YouTube стали відображатися короткі прев'ю новин про коронавірус (посилання на сторінку ВООЗ про COVID-19). Стало неможливим монетизувати відео про фейкові способи діагностики й лікування або ті, які вводять в оману щодо COVID-19. Платформа водночас не блокує монетизацію відео про коронавірус, якщо вони не стосуються мови ненависті, домагань, шахрайства чи розпалювання ненависті.

Водночас, для того, щоб користувачі Facebook змогли отримувати інформацію про коронавірус з достовірних джерел, соцмережа дозволила ВООЗ розміщувати у себе безкоштовну рекламу.

До того ж, кожен має змогу перевіряти інформацію особисто. Для цього необхідно звертати увагу на першоджерело, хто поширив інформацію та чи є її підтвердження в офіційних джерелах.

Отже, під час пандемії в соціальних мережах та ЗМІ спостерігаються порушення інформаційної культури і морально-етичних норм. Недотримання норм провокує паніку серед населення, сприяє появі великої кількості неправдивої та спотвореної інформації, що в деяких випадках призводить до матеріальних збитків як окремим особам, так і в цілому державам.

На державному рівні правління багатьох країн, включаючи міжнародні організації, докладають зусиль у подоланні як самої пандемії, так і її наслідків – переосмислюються правові норми, застосовуються заходи по боротьбі з неправдивою інформацією, кіберполіція веде боротьбу із шахраями та провокаторами, і до цього процесу долучаються і великі корпорації, як Google і Facebook. Превентивні заходи дозволять у майбутньому зменшити фейковість і тим самим знизити панічні настрої, зберегти спокій людей. Ефективні комунікації без пропаганди дозволять донести людям необхідну інформацію вчасно, і це вже не буде посягати на морально-етичні і культурні норми, і, можливо багато життів буде врятовано ще до появи потенційних загроз.

Також, завдяки інформаційній полярності в Інтернеті і ЗМІ, люди самотужки змушені виокремлювати достовірні дані з поміж усіх інших, і це без сумніву, одна з позитивних змін для сучасного суспільства.

Список використаної літератури:

1. Thomas Ricker. Lies about Gates outpace 5G conspiracies. URL: <https://www.theverge.com/2020/4/17/21224728/bill-gates-coronavirus-lies-5g-covid-19> (дата звернення: 17.04.2020).
2. Філіпова Людмила Яківна. Роль комп'ютерної етики в формуванні інформаційної культури користувачів комп'ютерно-мережевого середовища (за

книгою американського етика Дебори Джонсон*) : дис. ... доктор педагогічних наук: 08.01.01 / Філіпова Людмила Яківна. – Харків: Харківська державна академія культури, 2019. – 5 с. – Бібліогр. : с. 2–3.

3. Надія Вірна. Чи приховують правду про коронавірус: шість тез щодо права на інформацію під час пандемії. URL: <https://zmina.info/articles/chy-pryhovuyut-pravdu-pro-koronavirus-6-tez-pro-pravo-na-informacziyu-pid-chas-pandemiyi/> (дата звернення: 21.04.2020).

Морозов-Леонов О. С.,
факультет інформатики та
обчислювальної техніки.
Науковий керівник:
Самчинська О. А., викладач.

ВПЛИВ ПАНДЕМІЇ КОРОНАВІРУСУ НА КУЛЬТУРУ СПІЛКУВАННЯ У СОЦІАЛЬНИХ МЕРЕЖАХ

Культура спілкування є тією властивістю взаємодії людей як в реальному житті, так і в Інтернеті, завдяки якій можливе саме існування понять «дискусія», «обговорення» та «аналіз». Завдяки їй думка кожної людини може бути врахована, і разом з тим не може неправомірно затьмарити собою іншу думку іншої людини. Саме завдяки дотримання культури спілкування і будується можливість колективного роз'яснення суті, походження і можливих наслідків тих чи інших ситуацій, подій або непорозумінь, число яких останнім часом високе як ніколи.

Останнім часом стрімко зросла залежність людей від новин у зв'язку з поширенням CoViD-19 як в Європі, так і по всьому світу. Доступ до актуальних новин, які можуть інформувати про темп і географію поширення хвороби, про реальні засоби і методи індивідуального захисту та загальнодержавні заходи щодо боротьби з поширенням вірусу на сьогоднішній день є куди більшою потребою, ніж раніше.

Певна ступінь дезінформації, панічності і неорганізованості укупі із збільшеною увагою населення до новин, призвело, серед усього іншого, до безладів в Нових Санжарах 20 лютого 2020 року [1], чому передувало повідомлення про виліт літака з евакуйованими громадянами України з вогнища поширення хвороби Ухань (Китай) [2]. Починаючи з 19 лютого, коли було оголошено про виліт літака в Україну, і аж до прибуття [3] Президента України в Нові Санжари 5 березня у зв'язку з закінченням 14-денного терміну обсервації евакуйованих, дані події масово обговорювалися в соціальних мережах і на форумах. Через неясність плану дій після

майбутньої посадки літака багато користувачів критично обговорювали події і сперечалися [4], що в кінцевому підсумку призвело до вищевказаних заворушень в Нових Санджарах.

Після підтвердження [5] випадку зараження коронавірусом в Україні ступінь панічності і імпульсивності в обговореннях збільшилася, деякі користувачі застосовували засоби провокації, поширювали чутки, пропонуючи «скинути на місто атомну бомбу» [6].

Також, збільшенню кількості гнівних і нецензурних обговорень в соціальних мережах і на форумах слугувала почасти цинічна заява [7] Міністра охорони здоров'я Іллі Ємця щодо його погляду на розвиток пандемії в Україні: за його словами, «помруть всі пенсіонери», що поза всяким сумнівом певною мірою підірвало довіру населення до державних медичних заходів, образило людську гідність всіх громадян похилого віку України і, як вирішили для себе багато користувачів Інтернету, показало справжнє ставлення влади до народу, що знову-таки призвело до гнівних відгуків про оголошення карантину по всій країні.

Загалом можна зробити висновок, що основними факторами, що вплинули на погіршення культури спілкування в соціальних мережах і на форумах, є дезінформація, фейки, тривожність, панічність і низький рівень медіакультури населення.

За умови більш повільного розвитку подій культура спілкування могла бути дотримана і приведена в норму засобами модерації, натомість через занадто різкий темп зміни ситуації, наявних засобів не вистачило, щоб її забезпечити.

На мою думку, лише за дотримання норм культури спілкування можливе неструктивне обговорення, що здатне призвести до конкретних позитивних рішень; увага уряду повинна бути зфокусована не лише на практичному вирішенні медичних проблем, що з'являються у зв'язку із пандемією, а також і приділяти увагу додержанню інформаційної культури у соціальних мережах. Вищезазначені випадки громадських безладів та реакція на сумнівні вислови представників уряду, що не були належним чином пояснені згодом, є наслідками нестачі такої уваги.

Список використаної літератури:

1. Беспорядки из-за коронавируса: как в Новых Санжарах встретили эвакуированных из Уханя. URL: <https://www.dw.com/ru/%D0%B1%D0%B5%D1%81%D0%BF%D0%BE%D1%80%D1%8F%D0%B4%D0%BA%D0%B8-%D0%B8%D0%B7-%D0%B7%D0%B0-%D0%BA%D0%BE%D1%80%D0%BE%D0%BD%D0%B0%D0%B2%D0%B8%D1%80%D1%83%D1%81%D0%B0-%D0%BA%D0%B0%D0%BA-%D0%B2->

%D0%BD%D0%BE%D0%B2%D1%8B%D1%85-%D1%81%D0%B0%D0%B (дата звернення 08.05.2020).

2. Літак для евакуації українців з Уханя вилетів – Гончарук. URL: <https://www.pravda.com.ua/news/2020/02/19/7240942/> (дата звернення 08.05.2020).

3. Кінець обсервації: людей з "Нових Санжар" випускали Зеленський з Аваковим. URL: <https://www.pravda.com.ua/news/2020/03/5/7242613/> (дата звернення 08.05.2020).

4. Самолет из Уханя с украинцами на борту летит в Борисполь. В Харькове воздушное судно не село из-за тумана. URL: <https://www.facebook.com/news112ua/photos/%D1%81%D0%B0%D0%BC%D0%BE%D0%BB%D0%B5%D1%82-%D0%B8%D0%B7-%D1%83%D1%85%D0%B0%D0%BD%D0%B8-%D1%81-%D1%83%D0%BA%D1%80%D0%B0%D0%B8%D0%BD%D1%86%D0%B0%D0%BC%D0%B8-%D0%BD%D0%B0-%D0%B1%D0%BE%D1%80%D1%82%D1%83-%D0%BB%D0%B5%D1> (дата звернення 08.05.2020).

5. В Україні зафіксовано перший випадок зараження коронавірусом SARS-CoV-2 – МОЗ. URL: <https://gordonua.com/ukr/news/society/-v-ukrajini-zafiksovanij-pershij-vipadok-zarazhennja-koronavirusom-sars-cov-2-moz-1489373.html> (дата звернення 08.05.2020).

6. Новосанжарський синдром та тотальний карантин. Що відбувається в Чернівцях після виявлення коронавірусу. URL: <https://tsn.ua/ukrayina/novosanzharskiy-sindrom-ta-totalniy-karantin-scho-vidbuvayetsya-v-chernivcyah-pislya-viyavlennya-koronavirusu-1504665.html> (дата звернення 08.05.2020).

7. "Умрут все пенсионеры". Глава Минздрава Емец сделал прогноз по коронавирусу. URL: <https://strana.ua/news/254796-koronavirus-ubet-pensionerov-ukrainy-emet.html> (дата звернення 08.05.2020).

Воротинцев П. І.,
факультет інформатики та
обчислювальної техніки.
Науковий керівник:
Самчинська О. А., викладач.

ІНФОРМАЦІЙНА КУЛЬТУРА «НЕТРАДИЦІЙНИХ» ЗАСОБІВ МАСОВОЇ ІНФОРМАЦІЇ В ПЕРІОД КАРАНТИНУ

Пандемія коронавірусу сколихнула свідомість громадян всіх країн, Україна не стала винятком та теж піддалась страху перед хворобою. Цей страх побудив багатьох українців до пасивного захисту (самоізоляції та пошуку інформації про те як уникнути захворювання). Реакція державних органів щодо інформування населення була

повільною, тому активізувалися інформаційні джерела, які ставили собі за мету збільшити прибутки внаслідок паразитування на бажанні громадян бути інформованими. Не потрібно говорити, що якість інформації таких джерел була надзвичайно низькою, але багато людей просто не помітили цього керуючись принципом «більше знаю - краще сплю».

Важливість діяльності засобів масової інформації, зокрема їх вплив на різні сфери життя і діяльності держави та суспільства, стала зрозуміла давно. Саме тому, в українському законодавстві прийнято ряд нормативно-правових актів, які регулюють їх діяльність, таких як Закон України «Про друковані засоби масової інформації (пресу) в Україні», Закон України «Про телебачення і радіомовлення», Закон України «Про інформаційні агентства», Закон України «Про Національну раду України з питань телебачення і радіомовлення», Закон України «Про порядок висвітлення діяльності органів державної влади та органів місцевого самоуправління в Україні засобами масової інформації» та інші.

Однак, онлайн-медіа, IPTV і OTT платформи та соціальні мережі, які на даний момент вже витіснили традиційні ЗМІ, не підпадають під поняття засобів масової інформації, визначених українським законодавством, а, отже, на них не поширюються норми, встановлені вище згаданими законами. Невизначеність поняття, вимог до контенту та механізмів регулювання діяльності «нетрадиційних» засобів масової інформації вже давно є проблемним питанням, зокрема, в аспекті дотримання останніми інформаційної культури.

Ситуацію міг змінити законопроект «Про медіа» від 27.12.2019 р. №2693 та його альтернативним проектом №2693-1. В пояснювальній записці до проекту зазначеного закону наголошувалося, що деякі форми існування медіа знаходяться поза правовим полем (не підпадають під дію вимог, заборон чи обмежень, які встановлені для таких самих медіа, що виходять в світ у іншій формі). Так, наприклад, законодавством передбачається регулювання «класичного» ТБ (ефір, супутник, кабель) при повній відсутності регулювання відносно "нових" способів поширення ТБ (IPTV, OTT), відео на замовлення і платформ спільного доступу до інформації[1][2]. Але обидва проекти, хоч і були названі системними та такими, що унормовують діяльність традиційних та новітніх медіа, повернули на доопрацювання авторам законопроекту.

Особливо гостро проблема діяльності як традиційних медіа, так і нових засобів поширення інформації постала в період карантину, зокрема, в аспекті дотримання морально-етичних норм та інформаційної культури. На жаль, ні для кого вже не секрет, що під час пандемії ЗМІ займаються не інформуванням населення та

доповіддю адекватної статистики, а фактично відмовляються від відповідальності за неповноцінне інформування та змінюють тему на пошук відповідальних за невдалі превентивні міри запобігання розповсюдженню вірусу COVID-19 та його штамів [3].

Під час карантину в соціальних мережах, зокрема Telegram, з'явився попит на актуальну інформацію про коронавірус в регіонах користувачів соціальних мереж. Це призвело до створення безлічі «каналів-клонів», які почали розповсюджувати неперевірену інформацію в неконтрольованих кількостях. Із збільшенням кількості підписників власники каналів почали продавати різноманітну рекламу, яка зовсім не пов'язана з інформуванням населення. Так, наприклад, канал з власними історіями дівчини про захворювання на вірус почав продавати ювелірні прикраси. Інформація, що поширюється за допомогою таких каналів складається переважно з переказу новин та показу фото з відкритих джерел та відсутністю реальних доказів захворювання у автора. Таким чином, зі збільшенням попиту людей на інформацію, ринок реклами таких каналів став приносити значні дивіденди їх власникам. Потрібно зауважити, що власник може і не бути автором новин та історій каналу, а лише керівником над маркетологом, який збільшує аудиторію каналу та автора історій[4].

Відносно достовірної інформації, більшість даних, які були донесені через ЗМІ відносились до локальних випадків та не були результатами проведення системного статистичного дослідження населення. Як наслідок, на основі цього більшість українців зробили поспішні висновки відносно небезпеки ситуації. До того ж, коли в Америці політики, які виступали з заявами про несерйозність розповсюдження вірусу, тепер забирають свої слова назад [5], в Україні інформування про вірус залишилось лише на рівні порад ВОЗ.

Варто зазначити, що вітчизняні ЗМІ не вдаються до безпідставних звинувачень в початку пандемії як медіа на непідконтрольних Україні територіях Донецької та Луганської областей. За їх інформацією саме Україна відповідальна за створення корона вірусу [6]. Нестачу інформування населення про загрозу вірусом можна побачити і по кількості людей, які не дотримуються правил поведінки під час карантину на вулиці. Адже, саме ЗМІ повинні були донести важливість превентивної тактики боротьби з корона вірусом.

Підсумовуючи, можна сказати, що морально-етичні норми та інформаційна культура соціальних мереж поступилась цінностями та обрала для себе за мету заробити на попиті інформації про корона вірус, ЗМІ своєю чергою виконують не достатню інформаційну компанію. Протистояти цьому можливо, якщо створити єдину, впорядковану та взаємоузгоджену систему правових норм, спрямованих на

регулювання правовідносин у сфері медіа та імплементацію норм європейського законодавства шляхом забезпечення реалізації права на свободу вираження поглядів, права на отримання різнобічної, перевіреної та оперативної інформації, вільного поширення інформації, на захист національних інтересів України та прав користувачів медіасервісів та регулювання діяльності у сфері медіа відповідно до принципів прозорості, справедливості та неупередженості, незалежності медіа.

Список використаної літератури:

1. Ткаченко О.В. Пояснювальна записка законопроекту №2693. URL: w1.c1.rada.gov.ua/pls/zweb2/webproc34?id=&pf3511=67812&pf35401=516435 (дата звернення: 03.05.2020)
2. Проект закону №2693. URL: w1.c1.rada.gov.ua/pls/zweb2/webproc34?id=&pf3511=67812&pf35401=516295 (дата звернення: 03.05.2020)
3. Роман Гриценко. Помпео пообещал найти виновного в пандемии коронавируса. URL: https://focus.ua/world/453715-rompeo_poobeshchal_naiti_vinovnogo_v_pandemii_koronavirusa (дата звернення: 03.05.2020)
4. Світлана Салий. Как хайпануть на коронакризисе в Телеграме. URL: <https://webpromoeexperts.net/blog/kak-haypanut-na-koronakrizise-v-telegrame/> (дата звернення: 03.05.2020)
5. Марія Фенг. New York Mayor Urges Support For Chinatowns Amid Racist Coronavirus Fears. URL: https://www.huffpost.com/entry/coronavirus-chinatown-businesses-decline_n_5e4599dbc5b603b067c89fb0 (дата звернення: 03.05.2020)
6. Марія Красненко. У «Л/ДНР» поширюють фейк, що коронавірус створили в лабораторіях України. URL: <https://nv.ua/ukraine/events/v-dnr-zayavili-hto-koronavirus-sozdala-ukraina-poslednie-novosti-50084550.html> (дата звернення: 03.05.2020).

Музика О. А.,
факультет інформатики та
обчислювальної техніки.
Науковий керівник:
Самчинська О. А., викладач.

ПРОБЛЕМАТИКА ПРИВАТНОСТІ ГРОМАДЯН В УМОВАХ ПАНДЕМІЇ КОРОНАВІРУСУ COVID-19

Пандемія коронавірусу COVID-19 стала кризою для сфери громадянського здоров'я, адже єдиним ефективним на даний момент шляхом протидії поширенню SARS-CoV-2 є введення карантинного режиму та обсервація потенційних та фактичних носіїв вірусу.

З початку введення карантину були відомі випадки порушення самоізоляції з боку громадян. Міністерство цифрової політики оприлюднило мапу випадків порушення самоізоляції [1], що демонструє необхідність контролю з боку держави проведення протиепідемічних заходів. Варто зазначити, що попри заяву міністра Михайла Федорова, що дані були отримані від операторів мобільного зв'язку в деперсоналізованому вигляді, правомірність такої передачі даних третім особам є сумнівною.

Стеження за громадянами для деяких країн є прийнятною практикою, наприклад в Китаї та Росії використовуються камери відеоспостереження з розпізнанням облич. Однак, в демократичному суспільстві таке порушення права на приватність, як і будь-яких інших прав громадян, є не недопустимим, окрім випадків крайньої потреби.

Враховуючи розвиток технологій, не дивно, що для контролю за самоізоляцією або дотриманням дистанції стали широко використовуватись мобільних додатки у багатьох країнах світу: в Норвегії в тестовому режимі запустили додаток, який надсилає рекомендацію піти на карантин, якщо особа контактувала з хворим на COVID-19, в Гонконзі видають електронні браслети усім, хто прибуває з-за кордону, Південна Корея надсилає попередження всім, хто міг перебувати поруч з місцями, де був зафіксований випадок зараження.

Відповідно до Постанови Кабінету Міністрів України № 211 [2] (далі – Постанова), особам, що потребують госпіталізації до обсерваторів, може бути запропоновано альтернативу – самоізоляція, за умови згоди на застосування мобільного додатку «Дій вдома» для контролю. Впродовж самоізоляції додаток надсилає пуш-повідомлення у випадковий проміжок часу, у відповідь на які громадяни мають протягом 15 хвилин надіслати фото свого обличчя.

Мобільний додаток отримав переважно негативні відгуки. Користувачі скаржились, на відсутність звукових сигналів, неточність геолокації та інші технічні проблеми. Також, алгоритми мобільного додатку не враховують багато інших об'єктивних причин, як-то відсутність стабільного інтернет-з'єднання.

Позитивним моментом є те, що у четвертому абзаці пункту 13 Порядку проведення протиепідемічних заходів, пов'язаних із самоізоляцією осіб, що додавався до Постанови, зазначено, що повідомлення не можуть бути підставою для притягнення осіб до адміністративної відповідальності. Однак, факт порушення, зафіксований додатком, є підставою для контролю дотримання умов самоізоляції з боку Національної поліції та Національної гвардії, що цілком ймовірно може бути невиправданим кроком.

Правозахисні організації застерігають про ймовірні зловживання з боку державних інституцій доступом до персональних даних. Зокрема, публічне звернення до урядів країн з проханням не допустити безпідставного стеження за громадянами, у питаннях протиепідемічних заходів діяти виключно прозоро та не допустити загрози цифровій безпеці підписало більш ніж сто організації [3].

Нагальним питанням стає відповідність чинному законодавству України факту захисту та обробки таких персональних даних, як ПІБ, стать, дата народження, місце самоізоляції, місцеперебування, зареєстроване місце проживання, контактна інформація, строк самоізоляції, контактні особи хворого (за наявності), місце роботи, навчання або дошкільний заклад, можливість самостійно піклуватися про себе та стан здоров'я.

По-перше, відповідно до Постанови, встановлення додатку є добровільною альтернативою проходження обсервації у спеціалізованих закладах. Відповідно до пункту 1 частини 1 статі 11 Закону України «Про захист персональних даних» [4], підставою для обробки персональних даних є згода суб'єкта. Також в Постанові передбачено, що згоду на проходження самоізоляції з використанням додатку «Дій вдома» та згоду на обробку персональних даних особа надає в момент авторизації у ньому.

По-друге, інформація про суб'єктів відносин (володільця, розпорядника, місце зберігання, третіх осіб), перелік даних, що обробляються, мету та права суб'єкта персональних даних, визначених статтею 8 Закону України «Про захист персональних даних», надається у політиці конфіденційності [5].

Хоча при встановленні додатка «Дій вдома» особа надає згоду на обробку персональних даних і в такому випадку особливих проблем правомірності їх обробки немає, дані в інформаційну систему Дії потрапляють і про осіб, які відповідного

додатку не встановлювали. Така інформація, окрім суб'єкта персональних даних, може вноситись до системи лікарями або працівниками держустанов МОЗ епідеміологічного профілю. В такому випадку постає питання про законні аспекти використання персональних даних, за умови відсутності це згоди суб'єкта.

Можливість обробки персональних даних без згоди особи передбачена Конституцією та Законом України «Про захист персональних даних». Через кризу громадського здоров'я, в Постанові було встановлено, що для обробки ПІБ, дати народження, місця самоізоляції, місця проживання, місця роботи (навчання), стану здоров'я згода особи не потрібна. Але стан здоров'я входить в особливий перелік даних, передбачених частиною 1 статі 7 Закону України «Про захист персональних даних», адже неправомірне поширення такої інформації несе за собою особливі наслідки для особи. Тобто, даною постановою було розширено перелік підстав для дозволу на обробку даних про стан здоров'я без згоди суб'єкта.

Прикметно, що лише в редакції Постанови від 22.04.2020 було конкретизовано, які відомства до обробки якої інформації мають доступ, вказано особливості обміну інформації між відомствами, наведено перелік критеріїв для самоізоляції осіб та процедуру внесення особи до системи. Подібна недосконалість закону призвела до неприпустимого інциденту: публікації переліку вулиць, на яких мешкають хворі на COVID-19, відділом охорони здоров'я виконавчого комітету Коростенської міської ради на їх фейсбук-сторінці [6]. Даний випадок ілюструє, що до захисту даних про здоров'я осіб треба підходити відповідально, а формулювання законів та підзаконних актів має унеможличувати вільного тлумачення та неправомірного використання даних.

Однак законодавством досі не передбачено механізму вилучення або деперсоналізації (для подальшого використання у наукових та статистичних цілях) інформації із системи про особу після закінчення строку самоізоляції. Відомо лише, що інформацію буде видалено або деперсоналізовано через 30-денний після завершення карантину.

Можна зробити висновок, що законодавство, яким регулювались карантинні заходи було доволі проблематичним, не відповідало принципам правової визначеності та мало шляхи для зловживання повноваженнями доступу до інформації відомствами, які причетні до запобігання поширенню коронавірусної інфекції SARS-CoV-2. Об'єктивних підстав вважати, що подібні неточності буди допущенні навмисно – немає. Більш ймовірною причиною постає необхідність екстреного реагування на пандемію при невідповідності нормативно-правової бази до таких випадків, адже

розповсюдження коронавірусу стало безпрецедентним випадком пандемії у цифрову епоху.

Важливо підкреслити, що основні недоліки законодавства було усунено, однак, досі є аспекти, які потребують доопрацювання. Загалом ця ситуація демонструє, що вся нормативно-правова база, що стосується надзвичайних ситуацій будь-якого характеру, потребує ретельного коригування, адже вона показала себе неспроможною відповідати на виклики нової технологічної епохи. Також, варто враховувати, що у будь-якій надзвичайній ситуації обмеження прав має бути виключно пропорційним ризикам, механізми та мета обробки персональної інформації мають бути прозорими, а усі заходи подолання кризи повинні мати елементи підзвітності.

Список використаної літератури:

1. MediaSapiens. Мінцифри зробило мапу випадків порушення самоізоляції. URL: <https://ms.detector.media/media-i-vlada/post/24472/2020-04-09-mintsifri-zrobilo-mapu-vipadkiv-porushennya-samoizolyatsii/> (дата звернення: 08.05.2020 р).
2. Про запобігання поширенню на території України гострої респіраторної хвороби COVID-19, спричиненої коронавірусом SARS-CoV-2: Постанова Кабінету Міністрів України № 211 від 11 березня 2020 р. Дата оновлення: 04.05.2020 р. URL: <https://zakon.rada.gov.ua/laws/show/211-2020-%D0%BF> (дата звернення: 08.05.2020 р).
3. JOINT STATEMENT: STATES USE OF DIGITAL SURVEILLANCE TECHNOLOGIES TO FIGHT PANDEMIC MUST RESPECT HUMAN RIGHTS. URL: <https://www.amnesty.org/en/documents/pol30/2081/2020/en/> (дата звернення: 08.05.2020 р).
4. Про захист персональних даних: Закон України від 01.06.2010 № № 2297-VI. Дата оновлення: 04.03.2020 р. URL: <https://zakon.rada.gov.ua/laws/show/2297-17> (дата звернення: 08.05.2020 р).
5. Повідомлення про обробку персональних даних. URL: https://diia.gov.ua/policy_covid (дата звернення: 08.05.2020 р).
6. MediaSapiens. Чумні квартали: Житомирська ОДА оприлюднила карту з позначками вулиць, де мешкають хворі на COVID-19. URL: <https://ms.detector.media/zakonodavstvo/post/24517/2020-04-16-chumni-kvartali-zhitomirska-oda-oprilyudnila-kartu-z-poznachkami-vulits-de-meshkayut-khvor-i-na-covid-19/> (дата звернення: 08.05.2020 р).

Ніколюк А. В.,

факультет соціології і права.

Науковий керівник:

Бежвець А. М., старший викладач.

РЕАЛІЗАЦІЯ ПРАВА ПОДРУЖЖЯ НА СВОБОДУ ТА ОСОБИСТУ НЕДОТОРКАНИСТЬ В УМОВАХ КАРАНТИНУ

Право особи на свободу та особисту недоторканість закріплюється і гарантується як нормами національного, так і міжнародного права. Національне законодавство, а саме Сімейний кодекс, окреслює ці права для членів подружжя. Статтею 56 Сімейного кодексу України передбачено: право на вибір місця свого проживання, право на вжиття заходів, які не заборонені законом і не суперечать моральним засадам суспільства щодо підтримання шлюбних відносин, право на припинення шлюбних відносин [3]. Та це право чоловіка і жінки не обмежується лише цими правами, оскільки інші аспекти права подружжя на свободу одержали своє регулювання у положеннях інших нормативних актів, які поширюються на всіх громадян України, незалежно від їх сімейного стану.

Увесь цей спектр прав набуває особливого значення в умовах карантину. Безпосередньо поняття «карантин» передбачено Законом України «Про захист населення від інфекційних хвороб»: карантин - адміністративні та медико-санітарні заходи, що застосовуються для запобігання поширенню особливо небезпечних інфекційних хвороб [5].

У подальшому, при розгляді прав, окреслених статтею 56 Сімейного кодексу, особливу увагу варто звернути саме на право подружжя на особисту недоторканість, оскільки саме це право, на нашу думку, є найбільш порушуваним в умовах карантину.

Порушення права чоловіка та дружини на свободу та особисту недоторканість включає у себе, зокрема, примушування до збереження чи припинення шлюбних відносин, примушування до статевого зв'язку за допомогою фізичного або психічного насильства. Проте в Україні існує національне законодавство, що передбачає захист членів родини від насильства, тобто охороняє право кожного з подружжя на особисту недоторканність, а саме Закон України «Про запобігання та протидію домашньому насильству» [4]. Окрім цього існує ряд міжнародних документів, які варто було б ратифікувати Україні, зокрема, доцільним є звернути увагу на Стамбульську конвенцію, яку наша держава досі не ратифікувала. Цей документ регулює питання запобігання насильству щодо жінок і домашньому насильству та боротьби з цими явищами [1]. Наразі створено петицію про ратифікацію цієї конвенції. Імплементация

цього документу в національне законодавство буде досить вагомим кроком у попередженні домашнього насильства.

Під домашнім насильством розуміють діяння фізичного, сексуального, психологічного або економічного насильства, що вчиняються в сім'ї чи в межах місця проживання або між родичами, або між колишнім чи теперішнім подружжям, або між іншими особами, які спільно проживають однією сім'єю, але не перебувають у родинних відносинах чи у шлюбі між собою, незалежно від того, чи проживає особа, яка вчинила домашнє насильство, у тому самому місці, що й постраждала особа, а також погрози вчинення таких діянь [4]. У світлі сучасних подій питання домашнього насилля постало досить гостро. За даними ГО «Ла Страда-Україна» станом на кінець квітня 2020 року кількість звернень на гарячі лінії з приводу насилля у сім'ї зросла майже вдвічі. За перший тиждень карантину кількість дзвінків перевищила позначку за попередній тиждень на 130 звернень. Серед основних причин таких подій експерти зазначають, зокрема, проблеми з роботою та транспортним сполученням, постійні конфлікти на фоні відсутності роботи та стрімке погіршення матеріального становища родин.

Проте подібний негативний досвід прослідковується не тільки в Україні, але і за кордоном. Прикладом може слугувати ряд країн з найбільш стрімким рівнем захворюваності, а відповідно найбільш жорсткими карантинними обмеженнями. Так у Китаї та Італії повідомляють про значне збільшення рівня домашнього насилля та розлучень [6].

Законом України «Про запобігання та протидію домашньому насильству» передбачена низка заходів з протидії домашньому насиллю. А статтею 173-2 Кодексу України про адміністративні правопорушення встановлюється відповідальність за насильство в сім'ї [2].

Законодавчі новели зробили більш ґрунтовною протидію даним порушенням прав кожного з подружжя, проте дієвість цих заходів, а тим більше в умовах карантину, залишається дискусійною. Цікавою тут є судова практика, яка і висвітлює недоліки нововведень у законодавстві. Зокрема, проблеми виникають тому, що строки розгляду справ за даною статтею обмежені однією добою, а також є обов'язковою явка особи, яка притягається до адміністративної відповідальності. Однак в 90% випадків правопорушники до зали суду не з'являються і відповідно затягуються строки розгляду справи. В даній ситуації частина суддів притримується такої думки, що у разі неявки правопорушника слід повернути адміністративний протокол правоохоронним органам на доопрацювання цим самим перервавши строк розгляду справи. Більш того, у зв'язку з тим, що законом чітко не описується, в чому конкретно

може проявлятися насильство, дуже мало протоколів у таких справах складаються правильно [7]. Також необізнаність правоохоронців під час складання протоколів тягне за собою подальше затягування розгляду справ. Крім того, в умовах карантину суди залишаються зачиненими, судові засідання не проводяться (переносяться на інший період), що також ускладнює процес захисту.

Найбільш актуальним засобом захисту права подружжя на свободу та особисту недоторканність в останній час стала можливість розірвання шлюбу. В разі використання розірвання шлюбу як засобу захисту прав подружжя, факт порушення особистого немайнового права подружжя буде слугувати підставою для його розірвання. Враховуючи досить довготривалу самоізоляцію населення та зростання рівня конфліктних ситуацій та домашнього насилля, стрімко зріс і показник розлучень у світі. Наприклад у Китаї в окремих провінціях кількість розірвань шлюбу значно зросла [6]. Не зважаючи на вагомий негативний вплив карантинних обмежень на працездатність державних установ, запровадження новітніх технологій та цифровізація державних послуг призвели до можливості звернення до РАЦСу в онлайн режимі. Та попри більш адаптовані умови для розірвання шлюбу та досить хиткий стан справ з дотриманням подружжям прав одне одного на карантині, в Україні не прослідковується світова тенденція розлучень. Принаймні за даними Міністерства юстиції за період самоізоляції органи РАЦСу розлучили трохи більше двох тисяч пар, що значно менше за звичайні показники [8].

Підводячи підсумки усього вище сказаного, можна зазначити, що пандемія COVID-19 істотно вплинула на можливість подружжя реалізовувати своє право на свободу та особисту недоторканність. Основні труднощі, з якими стикаються подружні пари, полягають у нестабільній ситуації в країні, проблемах транспортного зв'язку, відсутності роботи, але найголовніше – самоізоляції. Ці фактори призводять до стрімкого зростання рівня домашнього насилля у родинах. У свою чергу не до кінця врегульований процес застосування оновленого законодавства з цього питання гальмує можливість відновлення порушених прав і свобод подружжя. Вагомим недоліком законодавчого регулювання питання порушення права кожного члена сім'ї на особисту недоторканність можна вважати відсутність імплементації міжнародно-правових норм з цього питання.

На тлі активного зростання рівня побутового насилля досить неочікуваним є зниження кількості розлучень, хоча такий показник є актуальним лише для нашої країни. Закордонний досвід свідчить про збільшення випадків розірвання шлюбу за період карантину.

Таким чином подібні тенденції з порушення права подружжя на свободу та особисту недоторканність, на думку експертів, з продовженням карантину та по його завершенню буде лише зростати. У свою чергу державі залишається вдосконалювати реальні механізми захисту цього права та звертати увагу на міжнародний досвід нормативно-правового регулювання подібних питань.

Список використаної літератури:

1. Конвенція Ради Європи про запобігання насильству стосовно жінок і домашньому насильству та боротьбу із цими явищами. URL: <https://rm.coe.int/1680093d9e>
2. Кодекс України про адміністративні правопорушення//Офіційний веб-сайт Верховної Ради України. URL: <https://zakon.rada.gov.ua/laws/show/80731-10>
3. Сімейний кодекс України //Офіційний веб-сайт Верховної Ради України. URL: <https://zakon.rada.gov.ua/laws/show/2947-14#n283>
4. Закон України «Про запобігання та протидію домашньому насильству» //Офіційний веб-сайт Верховної Ради України. URL: <https://zakon.rada.gov.ua/laws/show/2229-19#n367>
5. Закон України «Про захист населення від інфекційних хвороб» //Офіційний веб-сайт Верховної Ради України. URL: <https://zakon.rada.gov.ua/laws/show/1645-14>
6. Ірина Крикуненко. Жорсткий карантин. За місяць самоізоляції в Україні вдвічі зросла кількість скарг на домашнє насильство / Журнал Новое время. URL: <https://nv.ua/ukr/ukraine/events/karantin-v-ukrajini-prinis-sumni-naslidki-vipadki-domashnogo-nasilstva-pochastishali-vdvichi-novini-ukrajini-50083885.html>
7. Протидія домашньому насильству: наскільки дієвими є останні законодавчі зміни. Аналітика / Українське право. URL: https://ukrainepravo.com/scientific-thought/legal_analyst/protydiya-domashnomu-nasylstvu-naskilky-diyevymy-ye-ostanni-zakonodavchi-zminy-/
8. Українці на карантині стали менше розлучатися / Укрінформ. Мультимедійна платформа іномовлення України. URL: <https://www.ukrinform.ua/rubric-culture/3006146-ukrainci-na-karantini-stali-mense-rozluatisa.html>

Шведа К. О.,
факультет соціології і права.
Науковий керівник:
Бежвець А. М., старший викладач.

ВПЛИВ КАРАНТИННОГО ПЕРІОДУ НА ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ В МЕРЕЖІ ІНТЕРНЕТ

Право на інформацію та забезпечення інформаційної безпеки як України, так і кожного громадянина України загалом є необхідними конституційними положеннями, потреба в яких виникла з розвитком нашого суспільства. На сьогодні неможливо уявити масштаби та швидкість поширення інформації, особливої уваги все більше набуває правове регулювання мережі Інтернет, зокрема, в частині захисту персональних даних.

Конституція України у ст. 17 поряд із захистом суверенітету та територіальної цілісності України встановлює забезпечення інформаційної безпеки України, що відноситься до безпосередніх функцій держави та є завданням всього українського народу [1].

Закріплюючи це положення в Основному законі, держава бере на себе зобов'язання захисту прав і свобод громадян в інформаційній сфері, що може проявлятися у встановленні контролю за інформацією, що розміщується як компетентними державними поширювачами інформації, так і іншими поширювачами інформації, що мають безпосередній вплив на думку народу. Відповідно, «найжорсткіше» держава піклується про персональні дані, визнаючи порушення недоторканності приватного життя злочинним, і передбачаючи за нього покарання у вигляді обмеження волі на строк до трьох років [3].

Таким чином держава захищає права кожного на невтручання в його особисте чи сімейне життя, встановлені ст.32 Конституцією України [1].

З'ясувавши основні положення закону, які захищають кожного з нас, постає критичне питання про його реалізацію в період інформатизації суспільства, та впливу ізольованості під час пандемії хвороби COVID-19.

Оскільки саме під час обмеженості пересування і соціальних контактів в період карантину для особи є важливим захист від поширення неправдивої інформації, що може призвести як до поширення паніки серед суспільства, так і до масових заворушень, що також визнаються злочинними.

Відповідно цікавими видаються рекомендації профільного державного органу, відповідального за інформаційну безпеку України, а саме Служби безпеки України.

Державне відомство розробило систему рекомендацій, що повинні виконуватись усіма свідомими інтернет-користувачами, а саме: по-перше, отримувати інформацію лише від офіційних представників та офіційних джерел. Така необхідність

пояснюється декількома факторами, що гарантують надійність інформації, поширеної державними посадовими особами. Це пов'язано, в першу чергу, з підвищеною відповідальністю посадових осіб за власні дії та інформацію, яка підлягає поширенню цими особами, відповідно до Закону України «Про доступ до публічної інформації» та їх посадових обов'язків. Таким чином за поширення недостовірної інформації передбачається як адміністративна, так і кримінальна відповідальність посадової особи. Зважаючи на сучасні реалії та досить обмежені джерела інформації, саме забезпечення суспільства перевіреною інформацією з надійних джерел є необхідністю. Така інформація повинна бути заснована на фактах та наукових дослідженнях, не повинна бути спортворена або подана в неповному вигляді, оскільки така посадова халатність може завдати реальної шкоди у вигляді недоотримання необхідної інформації про карантинні обмеження, відповідальність за порушення умов карантину, строки карантину, місця отримання першої медичної допомоги у разі захворювання тощо.

По - друге, заборона поширення громадянами недостовірної інформації про коронавірус. Кодекс України про адміністративні правопорушення встановлює відповідальність за поширювання неправдивих чуток, що можуть викликати паніку серед населення або порушення громадського порядку, у формі штрафу [2]. Саме таким чином держава намагається боротися зі спекуляціями на тему симптомів коронавірусу, джерел його поширення та статистики хворих. Саме зараз постає необхідність ефективної роботи правоохоронних органів в мережі Інтернет задля притягнення таких порушників до відповідальності, передбаченої законодавством України. Таке публічне покарання неправомірних дій повинно викликати у суспільства довіру до інформації, що поширює держава. Також, важливим є спростування державою такої «фейкової» інформації для того, щоб громадяни України могли бути обізнані в ситуації, що відбувається в країні.

По-третє, для власної безпеки та спокою рекомендується обмежити участь навіть в коментуванні такої недостовірної інформації. Звісно, що саме ваше спростування поширення коронавірусу через телекомунікаційні мережі заслуговує на увагу, але потрібно замислитися скільки ви віддаєте власних сил на боротьбу з невпинною злочинністю або з людиною, яка через власну неосвідченість скоріш за все не змінить власної думки, а лише більш агресивно буде поширювати недостовірну інформацію створюючи ще більше інформаційного «шуму» [4]. В даному випадку доцільно залишити цю ситуацію для правоохоронних органів, до повноважень яких входить боротьба з такими інформаційними злочинцями та притягнення їх до відповідальності.

По-четверте, не рекомендується використовувати службову електронну пошту та заборонені поштові сервіси для приватного листування. Тобто, необхідно користуватися безпечним програмним забезпеченням, щоб уникнути випадків доступу

до приватної інформації. Дана рекомендація відноситься більше до загальних, але саме в час поширення коронавірусу та обмеженості інших джерел інформації відкривається велике поле для правопорушень з персональними даними, які містяться у поштової скринці, уся інформація особистого листування тощо. Також варто пам'ятати про те, що Конституція встановлює таємницю листування, телефонних розмов або іншої кореспонденції, а втручання у приватну розмову карається кримінальним законодавством.

По-п'яте, держава, роз'яснюючи правила поведінки в мережі Інтернет, які були вироблені з часом, шляхом численних порушень прав громадян, рекомендує перш за все робити досить прості, але необхідні для захисту персональних даних речі, зокрема, встановлювати складні паролі, уникати отримання файлів від невідомих аккаунтів, уникати будь-якого оприлюднення особистих даних без прямої необхідності тощо.

Список використаної літератури:

1. Конституція України // Відомості Верховної Ради. – 1996. URL: <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#n4269.n>
2. Кодекс України про адміністративні правопорушення (статті 1 - 212-20) // Відомості Верховної Ради Української РСР (ВВР. – 1984. URL: <https://zakon.rada.gov.ua/laws/show/80731-10#Text>.
3. Кримінальний кодекс України // Відомості Верховної Ради. – 2001. URL: <https://zakon.rada.gov.ua/laws/show/2341-14#Text>.
4. Як подбати про онлайн-безпеку під час карантину – поради // УКРІНФОРМ. – 2020. URL: <https://www.ukrinform.ua/rubric-society/2903724-ak-podbati-pro-onlajnbezpeku-pid-cas-karantinu-poradi-sbu.html>.

Кісіль А. В.,
факультет соціології і права.
Науковий керівник:
Дубняк М. В., к.ю.н., ст. викладач.

РИЗИКИ ВТРАТИ ПЕРСОНАЛЬНИХ ДАНИХ В УМОВАХ КАРАНТИННОГО ТА ПОСТКАРАНТИННОГО РЕЖИМУ

На сьогоднішній день проблема використання персональних даних інтернет-користувачів є як ніколи актуальною, це безпосередньо зумовлено введенням карантинних обмежень через поширення гострої інфекційної хвороби COVID-19 та часткового локдауна в Україні. Саме в цьому році більшість українців залишили свої робочі офіси та опановували новий для більшості працівників дистанційний формат роботи, а деякі громадяни і навчання. Зрозуміло, що більшість вільного часу основна

маса суспільства проводила саме в режимі онлайн, що безперечно призвело до збільшення ризиків для користувачів щодо втрати контролю над своїми персональними даними, та все ж таки, обумовило в черговий раз розглянути проблеми, пов'язані із захистом таких даних.

Отже, метою дослідження є спроба розкрити актуальність проблеми ризиків втрати персональних даних під час загальнонаціонального карантину та посткарантинного режиму, виокремити основні засади правового захисту цих даних відповідно до законодавства України.

Для досягнення вказаної мети поставимо ряд завдань: встановити основні джерела небезпеки втрати персональних даних під час користування інтернет-ресурсами, розглянути основні нормативно-правові акти сучасного законодавства України, що безпосередньо стосуються персональних даних та їх захисту, охарактеризувати сучасний стан освіченості населення та виокремити методи його підвищення.

Найбільшою небезпекою для українських громадян в мережі є те, що про збирання цих даних дехто навіть не здогадується. Це відбувається багатьма способами, але один з найпростіших використання файлів під назвою cookie, які ми зустрічаємо на кожному веб-сайті, поштових сервісах та інших мережевих платформах. Файли cookie - це невеликі текстові файли, які використовуються для опису даних, отриманих від сайту шляхом дослідження та аналізу інформації, що зберігається в браузері Вашого комп'ютера або мобільного телефону, а також відправлення сформованих даних на той самий браузер ці показники, у випадку, якщо ви повторно відвідуєте веб-сайт [1].

Окрім додаткової зручності для користувача, яка полягає в тому, що збережені дані спрощують повторне використання веб-сайтом, це несе доволі високу небезпеку, тому що з такими примітивними даними може бути зібрана важлива, конфіденційна інформація, яка зберігається у вашому браузері.

Надзвичайно важливою для нас частиною всесвітньої павутини являються соціальні мережі, в яких ми на період самоізоляції можемо спілкуватися з друзями та рідними, замовляти товари, дізнаватися новини, тощо. На жаль, навіть в цьому процесі є високий відсоток ризику втрати персональних даних. Тим більше, люди самі вносять конфіденційну інформацію про себе назавжди в простори Інтернету і як правило видалити її звідти досить проблематично. Окрім цих відомостей, зазвичай відбувається збір наших вподобань і найчастіших запитів, результатом чого може стати надмірна кількість небажаних рекламних роликів або спаму.

Варто зауважити, що неодмінною складовою щоденного життя сучасного українця є мобільні додатки, якими користуються за допомогою смартфонів. Дійсно, дані програми є неодмінною складовою незворотнього процесу інформатизації, що поєднують в собі функціонування багатьох елементів та дозволяють спрощувати діяльність особи. Проте, вони також несуть за собою деякі загрози, що можуть потім виявитись у матеріальних збитках чи моральній шкоді. Одним з найпростіших та найактуальніших прикладів є популярна соціальна мережа Instagram, де дані використовуються таким чином: «Ми збираємо інформацію про людей, Сторінки, облікові записи, хештеги й групи, з якими ви зв'язуєтесь, і про те, яким чином ви взаємодієте з ними в наших Продуктах, наприклад, про людей, з якими ви спілкуєтесь найчастіше, або про групи, до складу яких ви входите. Ми також збираємо контактну інформацію, якщо ви завантажуєте, синхронізуєте або імпортуєте таку інформацію з пристрою (наприклад, адресну книгу, журнал викликів або SMS), яку ми використовуємо для того, щоб допомогти вам та іншим користувачам знайти людей, яких ви можете знати, і для інших цілей, описаних нижче» [2].

Окрім таких технічних загроз в об'єктивному розумінні існує і суб'єктивна сторона цієї проблеми. Вона виокремлюється безпосередньо в обізнаності громадян саме в інформаційній сфері. На жаль, українці досить часто потрапляють в неприємні ситуації пов'язані з отриманням їхніх даних і в подальшому шантажуванні чи будь яких протизаконних діях. Однією з найпоширеніших причин таких діянь серед громадськості є - безробіття, яке пов'язане з втратою роботи чи частковим її призупинення внаслідок епідеміологічної ситуації в країні. Шукаючи якийсь заробіток, люди не помічають, як залишаючи свої резюме на різних порталах вони віддають в безмежний простір Інтернету таку конфіденційну інформацію: місце проживання, контактний телефон, номер банківської карти, а деякі навіть паспортні дані, якими потім користуються шахраї [3].

Конституція України встановлює правовий захист персональних даних, це передбачено в статті 32: не допускається 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 прав людини [4].

Захист персональних даних в Україні передбачений Законом України «Про захист персональних даних». Відповідно цей нормативно - правовий акт 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.

Встановлено, що обробка персональних даних можлива виключно за згодою суб'єкта цих даних, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини [5]. При зборі інформації на веб-сторінках та інших платформах особа повинна бути обов'язково повідомлена і згодом надати згоду. Потрібно зауважити, що в електронному режимі надання дозволу користувачем може здійснюватися в різних формах: натискання відмітки «погоджуюсь» (активний); попередження про подальше зчитування даних, при користуванні ресурсом (пасивний); опис необхідних відомостей в окремих непримітних розділах.

Додатково до цих актів законодавством про захист персональних даних передбачені інші закони та підзаконні акти, міжнародні договори України, згода на обов'язковість яких надана Верховною Радою України. Щодо європейської системи законодавства про захист персональних даних, то до їхнього складу входять більше ніж 10 нормативно-правових актів. Інститут захисту персональних даних в ЄС ґрунтується на принципах законності, цільової визначеності, мінімальності, об'єктивності інформації, участі суб'єкта персональних даних у здійсненні контролю, обмеження розкриття персональних даних, інформаційної безпеки. Порівнюючи законодавство України про захист персональних даних та законодавства ЄС, слід зазначити, що для повного приведення національного законодавства у відповідність зі стандартами ЄС потрібні додаткові організаційно-правові заходи щодо вдосконалення контролю за виконанням законів і підзаконних актів у цій галузі та доповнення їх змісту за моделями Міжнародної та Європейської Конвенцій про захист персональних даних, ухвалених у новітній час Директив ЄС [6].

Підсумувавши вищенаведене, можна вказати, що ризики втрати контролю над персональними даними є досить високими в сучасних умовах карантинного режиму, що призводять до негативних наслідків для користувачів. Основними джерелами такого ризику є: файли cookie, соціальні мережі, мобільні додатки, але найголовнішим, на нашу думку, все ж таки є суб'єктивний фактор. Для підвищення обізнаності громадян України в інформаційній сфері можливе запровадження спеціальних освітніх програм та курсів, як в освітніх закладах, так і в підприємствах, установах, організаціях для підвищення рівня обізнаності працівників з ризиками втрати контролю як над персональними даними так і над комерційною таємницею. Щодо законодавчої бази слід зауважити, що кількість нормативно-правових актів в цій сфері є достатньою, але головним завданням залишається їхня гармонізація, узагальнення між собою та встановлення відповідності європейським стандартам.

Список використаної літератури:

1. Файли cookies. URL: <https://uk.wikipedia.org/wiki/файли-cookies> (дата звернення: 12.11.2020).
2. Політика використання даних Instagram. Режим доступу: <https://www.facebook.com/help/instagram/519522125107875>.
3. Правдиченко А. Громадський простір: Персональні дані онлайн: проблеми регулювання та перспективи захисту. URL: <https://www.prostir.ua/?library=personalni-dani-onlajn-problemy-rehulyuvannya-ta-perspektyvy-zahystu>. (дата звернення: 12.11.2020).
4. Конституція України URL: <http://zakon5.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80> (дата звернення: 12.11.2020).
5. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI. URL: <https://zakon.rada.gov.ua/laws/show/2297-17> (дата звернення: 12.11.2020).
6. Головченко В. Правові основи захисту персональних даних. URL: <https://yur-gazeta.com/publications/practice/inshe/pravovi-osnovi-zahistu-personalnihdanih.html> (дата звернення: 12.11.2020).

Ярош І. С., Балінська В. О.,
факультет соціології і права.
Науковий керівник:
Радзієвська О. Г., к.ю.н., провідний
науковий співробітник НДІ ІІ
НАПрН України.

ОСОБЛИВОСТІ ВИКОРИСТАННЯ МОБІЛЬНИХ ДОДАТКІВ ТА МЕХАНІЗМИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ОСОБИ В УМОВАХ ПАНДЕМІЇ COVID-19

Умови карантину змусили суспільство змінювати усталений порядок денний. Значна частина людства перейшла на віддалену роботу з використанням можливостей мережі Інтернет та інформаційно-комунікаційних технологій, а також почали користуватися більшою кількістю мобільних додатків та комп'ютерних програм. Це підвищило рівень загроз у кіберпросторі пов'язаних з цілісністю та недоторканністю інформації. Особливо небезпечними є загрози несанкціонованого поширення персональних даних людей. В таких умовах держава зобов'язана належним чином реагувати на інциденти, пов'язані із захистом інформації, що трапляються в інформаційній сфері, задля ефективного забезпечення індивідуальної та суспільної інформаційної безпеки.

Відповідно до Стратегії розвитку інформаційного суспільства в Україні, схваленої розпорядженням Кабінету Міністрів України від 15 травня 2013 р. № 386-р, пріоритетами діяльності в галузі забезпечення інформаційної безпеки є забезпечення цілісності, доступності та конфіденційності інформаційних ресурсів України, які створюють умови для розвитку особи, стійкого функціонування суспільства і держави, захисту персональних даних та інформації, що перебуває у володінні фізичних, юридичних осіб та держави, від зовнішніх і внутрішніх інформаційних загроз, зокрема шляхом протидії комп'ютерним злочинам [1].

Таким чином, можна зробити висновок, що держава взяла на себе зобов'язання захищати персональні дані та інформацію фізичних та юридичних осіб, ліквідовувати інформаційні загрози, протидіяти злочинам, скоєним за допомогою комп'ютерних технологій.

В умовах пандемії, коли основна частина операцій по обміну інформації здійснюється за допомогою смартфонів та комп'ютерів, виникає нагальна необхідність у підвищенні рівня захисту інформації, яку особа надає, завантажуючи ту чи іншу програму на свій гаджет. Відтак, розробники додатків, у першу чергу, повинні подбати не лише про багатофункціональність свого винаходу, але й про можливість належним чином забезпечити право особи на невтручання в особисте життя та таємницю листування.

Наразі мобільні додатки користуються особливою популярністю. Більшість з них містять особисті дані про користувача. До популярних мобільних додатків, що містять особисті дані користувача, можна віднести, зокрема, сервіси з доставки їжі, батьківський контроль, відстеження місцезнаходження, управління продуктивністю працівників. За даними компанії ESET вид кіберзлочинів, пов'язаний з втручанням в роботу цих додатків, зріс на третину [2].

Зловмисники користуються тим, що до карантину більшість людей не користувалися цими додатками або користувалися ними не так часто, через що люди не знають, яку небезпеку несуть ці програми, яка надійність їх використання, як їх налаштувати, щоб зменшити рівень загрози і т.п.

Звичайно, розробники усувають неполадки, а карантинні умови є саме тим механізмом, що допомагає їх виявляти. Проте зловмисники, яких заохотив карантин, намагаються знайти нові можливості для зловживань додатком і викрадення даних. Враховуючи це, перед тим, як завантажувати додаток, необхідно перевірити його на безпеку, почитати відгуки про нього, виявити позитивні та негативні аспекти його використання.

Крім того, зростання кількості крадіжок інформації пов'язана з тим, що віддалена робота змушує працівників різних компаній користуватися персональними комп'ютерами, зберігати дані на флешках та внутрішній пам'яті мобільного телефону. З них легше викрасти інформацію або навіть з якось корисливою метою навмисне змінити певні відомості, звіти чи дані. Як зазначає юрист-практик Борис С., існує поняття інформаційної гігієни, рівень якої із запровадженням роботи з дому катастрофічно впав. Саме тому збереження усіх даних на віддалених серверах і з достатнім рівнем шифрування є справді хорошим захистом вразливих місць компанії. Цього правила і до карантину мало хто дотримувався, а зараз інформація знаходиться на незахищених флешках і домашніх комп'ютерах працівників[3].

Сьогодні відбувається трансформація цих загроз, але водночас і переусвідомлення їхнього рівня бізнесом. Якщо на початку карантину небезпека була серйозною, то зараз, на нашу думку, завдяки карантинній практиці і порадам юристів, бізнес почав вживати запобіжних заходів, знижуючи рівень небезпеки.

Варто наголосити на тому, що влітку цього року в Україні фіксувалося 300 тис. нових кіберзагроз щодня, і відповідно зросла кількість звернень осіб за захистом своїх порушених прав у сфері інформаційної безпеки [4]. Відтак, треба дослідити, чи зросла кількість судових рішень, що стосувалися дій кіберзлочинців і захисту права особи на інформацію у зв'язку з такими діями.

У Кримінальному кодексі України передбачено відповідальність за несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку [5]. Проаналізувавши дані Єдиного державного реєстру судових рішень, можемо сказати, що за період карантину було винесено лише 10 вироків, що стосувались захисту прав особи на інформацію.

Можемо зробити висновок, що суди наразі не можуть повною мірою впоратись із тим навантаженням, що виникло через поширення пандемії коронавірусу. Держава в цілому не здатна забезпечити покарання для кіберзлочинців, притягнути їх до відповідальності, а отже протидіяти достатньою мірою кіберзлочинам.

Таким чином, кожна особа повинна зважати на те, що її інформаційна безпека може бути порушена, персональні дані можуть бути вкрадені, а захисту від держави може буде недостатньо для відновлення порушеного права. Тому кожен самостійно має дбати про інформаційну безпеку. Держава, у свою чергу, повинна не лише інформувати суспільство про наслідки пандемії, загрози для системи охорони здоров'я, а й повідомляти про інформаційні загрози, надавати рекомендації, як запобігати цим загрозам. На нашу думку, така інформаційна кампанія держави

допоможе вибудувати правильне уявлення громадян про механізми протидії інформаційним загрозам.

Нам необхідно розуміти, що інтереси особи в інформаційній сфері є національними інтересами України. В період карантину існує велика ймовірність порушення цих інтересів, зокрема, шляхом викрадення персональних даних фізичних та юридичних осіб. Тому швидке реагування на проблеми в цій сфері державою, реалізація зобов'язань в інформаційній сфері, вдосконалення системи з виявлення кіберзлочинців забезпечить належний і достатній захист права на інформацію з боку держави.

Висновки та пропозиції.

Підсумовуючи хочемо зазначити, що поширення пандемії COVID-19 на території України стало наслідком збільшення випадків порушення інформаційних прав особи та спричинило масове поширення випадків викрадення інформації за допомогою інформаційно-комунікаційних технологій. Оскільки в умовах карантину суспільство почало модернізувати свій спосіб життя, все більше пов'язуючи його із гаджетами, виникає нагальна необхідність у розробці нової системи захисту персональних даних особи з метою захисту законодавчо закріплених прав людини і громадянина.

Відтак, на нашу думку, слід розробити державні механізми захисту інформаційних прав особи з метою реалізації положень Стратегії розвитку інформаційного суспільства в Україні, підвищити кваліфікацію фахівців правоохоронних органів та судової системи, що здійснюють забезпечення права особи на інформацію, а також звернути увагу розробників мобільних додатків не лише на комфортність та швидкість використання їх програми, а й на належний рівень захисту особистих даних користувача.

Список використаної літератури:

1. Про схвалення Стратегії розвитку інформаційного суспільства в Україні : розпорядження Кабінету Міністрів України від 15.05.2013 р. № 386-р. URL: <https://zakon.rada.gov.ua/laws/show/386-2013-%D1%80#Text> .
2. Полицька І. Під час карантину кількість шкідливих сайтів істотно зросла: експерти. Телеканал новин «24»: офіц. веб-сайт. URL: https://techno.24tv.ua/pid_chas_karantinu_kilkist_shkidlivih_saytiv_istotno_zroslo_eksperti_n1336590 (дата звернення: 06.11.2020).
3. Борис С. Безпека бізнесу під час карантину: як уникнути рейдерської атаки. Ліга Закон: офіц. веб-сайт. URL: https://biz.ligazakon.net/ua/analitycs/194528_bezpeka-bznesu-pd-chas-karantinu-yak-uniknuti-reydersko-ataki (дата звернення: 06.11.2020).

4. Підсумки карантину: IT-фахівці розповіли про основні правила кібербезпеки, до яких привчила пандемія. Уніан. Інформаційне агентство: офіц. веб-сайт. URL: <https://www.unian.ua/science/pidsumki-karantinu-it-fahivci-rozpovili-pro-osnovni-pravila-kiberbezpeki-do-yakih-privchila-pandemiya-novini-11064098.html> (дата звернення: 06.11.2020).

5. Кримінальний кодекс України: Закон України від 05.05.2001 р. № 2341-III. Відомості Верховної Ради України. 2001. № 25-26. Ст.131. URL: <https://zakon.rada.gov.ua/laws/show/2341-14#Text>.

Куніцька З. Е.,
факультет соціології і права.
Науковий керівник:
Фурашев В. М., к.т.н., с.н.с., доцент.

КОНФІДЕНЦІЙНІСТЬ ПЕРСОНАЛЬНИХ ДАНИХ У МОБІЛЬНИХ ДОДАТКАХ БОРОТЬБИ З COVID-19: ОСОБЛИВОСТІ ПІДХОДІВ У РІЗНИХ ДЕРЖАВАХ СВІТУ

Прогресивне розповсюдження коронавірусу COVID-19 надало право урядам багатьох держав світу вимагати розширення доступу до персональних даних громадян. Необхідність такої потреби аргументувалась тим, що це допоможе контролювати та стримувати сам вірус. Буде доречним згадати Загальний регламент про захист даних (GDPR), який надає дозвіл обробляти персональні дані за умови, що це необхідно для захисту суспільних інтересів, а також життєво важливих інтересів будь-якої особи [1]. В Україні, наприклад, дане право було втілене в Законі України «Про внесення змін до Закону України «Про захист населення від інфекційних» хвороб щодо запобігання поширенню коронавірусної хвороби (COVID-19)» [2]. Цим законом було дозволене використання персональних даних українців без їхньої згоди на період карантину.

Наразі керівництво більшості держав вбачає головний свій інструмент боротьби з пандемією в розробці технологій, які б збирали, зберігали та обробляли великі обсяги даних, зокрема й персональні дані. Хоч і зрозуміло, що влада має використовувати різноманітні засоби, аби побороти хворобу, однак певні її дії викликають напругу в співвідношенні використання цих даних та права на приватність. Сьогодні у світі був застосований широкий спектр підходів та оголошена значна кількість заяв щодо прихильності урядів до конфіденційності персональних даних або ж, навпаки, щодо грубого нехтування нею. Тому можна сказати, що на

міжнародному рівні відношення до використання персональних даних значно різняться, а також, що способи такого використання в боротьбі з пандемією в різних державах мають свої особливості та наслідки.

Франція. Національна комісія з інформатизації та свобод Франції (CNIL) заявила, що дані повинні використовуватись лише з метою стримування вірусу. Ішлося, зокрема, про створення спеціальної мобільної програми StopCovid, яка б стежила за пересуванням хворих вірусом людей та за їхніми контактами з іншими. Використання цієї програми, за словами Національної комісії, є добровільним та не порушує права й свободи громадян [3].

Німеччина. У цій державі було спеціально оновлено національне законодавство у сфері конфіденційності задля офіційного дозволу використання персональних даних при природних, техногенних катастрофах або при епідеміях. Попри те, що Німеччина більше була схильна до зміцнення конфіденційності даних та те, що в березні 2020 року через громадську реакцію уряд мав відмовитись від відстеження даних про місцеперебування людини, вона все ж таки розглядала можливість розробки та впровадження специфічних програм, метою яких мало стати відстеження контактів інфікованої особи з іншими.

Південна Корея. Поступове зниження випадків захворювання на COVID-19 у цій державі пояснюється введенням програми SoGona 100m. Це центральна програма відстеження, що надає своїм користувачам загальнодоступну карту, де показуються випадки їх зустрічі з хворими на коронавірус. Дана програма викликала хвилювання в масах щодо обсягу тієї інформації, яка надається громадянам. Ця інформація, зокрема, включає наступні відомості: вік, стать, прізвище, маршрут подорожі хворих осіб.

Сінгапур. Тут була введена в користування програма TraceTogether. Вона використовує Bluetooth для ідентифікації людей, які знаходились від користувача в радіусі двох метрів, при цьому маючи підтверджений тест на COVID-19. Після надання дозволу програмі, починається ведення певного списку осіб, що також використовують програму та з якими користувач контактував. Якщо виявляється, що користувач тісно контактував з особою, хворою на COVID-19, тоді він може вирішити, чи ділитись цією інформацією, тобто даними про інших, з урядом країни чи ні.

Інші держави теж застосовували різноманітні підходи до цього питання, зокрема штат на південному заході Індії Карнатака ввів обов'язок для громадян, що перебувають на самоізоляції, завантажувати своє погодинне селфі в спеціальну програму. Польща також реалізувала подібний досвід [4].

Україна. Наша держава не відстає у впровадженні таких нововведень на своїй території. В Україні розроблена програма «Дій вдома», що ставить собі за мету контроль за дотриманням вимог самоізоляції тими, хто: нещодавно повернувся з-за кордону, проходить лікування вдома, перебуває в зоні ризику захворіти на коронавірус через контактування з уже хворими особами. Постанова Кабміну «Про запобігання поширенню на території України гострої респіраторної хвороби COVID-19, яку спричинив SARS-CoV-2» зазначає необхідність внесення відповідних даних до інформаційних систем та складення переліку осіб на самоізоляції [5]. Такі особи мають можливість вводити всю інформацію до мобільної програми Єдиного державного веб-порталу електронних послуг особисто, в іншому випадку за них це зроблять відповідальні за даний процес робітники. Тобто в будь-якому разі надання персональних даних особами, що несуть певний ризик для оточуючих через свою хворобу, є обов'язковим.

Так згідно з вищевикладеним матеріалом можна стверджувати про переважне використання персональних даних як інструмента подолання COVID-19 у багатьох державах світу, зокрема й в Україні. Попри те, що це аргументується намірами уряду забезпечити самих громадян, дані явища можуть спричинити виникнення ряду ризиків.

Зі створення нових баз для накопичення персональних даних зросла й кількість кібератак. Згідно з дослідженням, проведеним компанією Internet Security Sophos, обсяг шахрайських операцій з електронною поштою лише за один тиждень березня 2020 року майже потроївся [4]. Однак це не єдина проблема, що наразі наявна в багатьох державах. Також існує ще й несанкціонований доступ до даних, що обробляються у різноманітних додатках; порушення анонімності осіб, що через можливість хвороби чи самої хвороби являють небезпеку для оточуючих; необґрунтований контроль за пересуванням таких осіб; неправомірне використання персональної інформації не з тією метою, з якою вона була зібрана; втручання у роботу особистих пристроїв через мобільні додатки, що пов'язані з даною хворобою тощо.

Реальність ризиків, що можуть виникнути у зв'язку з надмірним використанням персональної інформації, підтвердилась і в Україні. У жовтні цього року в одному з медичних закладів Дніпра стався витік персональної інформації працівників та клієнтів. Зокрема, це ПІБ, номери телефонів, адреси проживання, e-mail, діагнози пацієнтів та дані їхніх медичних карт, серед яких і позитивні тести на COVID-19 [6]. Так виникла небезпека не лише викрадення персональної інформації, а й модифікації результатів аналізів, обстежень та ліків.

Отже, спалах COVID-19 у сучасних умовах спричинив безпрецедентний інтерес та зосередження уваги на значущості даних, які залучаються до розв'язку будь-яких питань як на національному, так і на міжнародному рівнях. Зокрема, можна говорити й про розв'язок питань щодо контролю та стримування COVID-19. Найефективнішим способом розв'язку таких питань наразі є створення мобільних додатків, які дозволяють урядам швидко збирати персональні дані громадян заради боротьби з пандемією. Але ні швидкість ні бажання подолати дану кризу в багатьох країнах не має слугувати виправданням у питаннях порушення конфіденційності особи. Органи влади в державі попри ті труднощі, що виникнули у світі на даний момент, зберігають свій обов'язок збереження інформаційної приватності громадян, а також мають керуватись цим обов'язком у визначенні своїх завдань та стратегії. В іншому випадку може виникнути ризик появи певних проблем у державі, на розв'язок яких їй необхідні будуть значні сили та ресурси.

Список використаної літератури:

1. Про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС: Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 р. URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text (дата звернення: 08.11.2020).
2. 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#Text> (дата звернення: 08.11.2020).
3. У Франції дозволили стежити за хворими на COVID-19 через мобільний додаток // Укрінформ : веб-сайт. URL: <https://www.ukrinform.ua/rubric-world/3033124-u-francii-dozvolili-slidkuvati-za-hvorimi-na-covid19-cerez-mobilnij-dodatok.html> (дата звернення: 11.11.2020).
4. COVID-19: people: how governments are using personal data to fight COVID-19 (UK) // Herbert Smith Freehills : веб-сайт. URL: <https://www.herbertsmithfreehills.com/latest-thinking/covid-19-people-how-governments-are-using-personal-data-to-fight-covid-19-uk> (дата звернення: 09.11.2020).
5. Про запобігання поширенню на території України гострої респіраторної хвороби COVID-19, спричиненої коронавірусом SARS-CoV-2: постанова Кабінету Міністрів України від 11 березня 2020 р. № 211. URL: <https://zakon.rada.gov.ua/laws/show/211-2020-%D0%BF#Text> (дата звернення: 08.11.2020).
6. В одній із клінік Дніпра стався витік медичних даних, зокрема результатів тестів на Covid-19 // 112 Україна : веб-сайт. URL: <https://ua.112.ua/suspilstvo/v-odnii-z->

Костенко А. Г.,
факультет соціології і права.
Науковий керівник:
Фурашев В. М., к.т.н., с.н.с., доцент.

НАСЛІДКИ ВПЛИВУ КАРАНТИННОГО РЕЖИМУ НА ТРАНСФОРМАЦІЙНІ ПРОЦЕСИ СУСПІЛЬНИХ ВІДНОСИН

Карантинні заходи та обмеження вносять свої корективи в усі сфери суспільного життя. Світ змінюється - змінюється людина в межу своїх можливостей. Подальше життя суспільства та його розвиток також змінює свою траєкторію еволюціонування. Тому варто розуміти, що карантинний режим безпосередньо впливає і на трансформаційні процеси суспільних відносин.

Якщо робити аналіз історичного підґрунтя трансформації людського роду, то можна сказати, що цей процес завжди був неперервний і зародився одночасно з появою людей на Землі. Будь - які зміни відбувалися у прив'язці до часового проміжку та історичних обставин.

На даному етапі розвитку суспільство стикнулося з такою ситуацією, як пандемія COVID – 19. Звичайно, епідемії і раніше були в історії людства, проте вони не несли таких глобальних наслідків на суспільне бачення організації подальшого функціонування міжособистісних відносин. Причиною цього, на мою думку, може бути те, що наразі країни досить міцно зв'язані між собою в економічному та політичному планах, а також не менш важливим є існування глобальної мережі Інтернет.

Саме Інтернет є ретранслятором трансформаційних притягів індивідуумів. Кожен із нас тепер має таку можливість, як висловлюватися на будь-яку тему у будь-якому ключі та форматі, розглядати будь-які питання у вибраній особисто площині. І, що є головним, тепер думки окремої і навіть маловідомої людини можуть не тільки почути мільйони інших людей, а й викликати певний резонанс у суспільстві та запустити механізм трансформації окремих процесів чи явищ. Саме це ми зараз можемо спостерігати. Виникає логічне питання: «Чому саме карантин став тою рушійною силою?» На мою, можливо суб'єктивну думку, причиною цього стало те, що більшість людей наразі знаходяться вдома і не мають можливостей не тільки

ходити в ресторани, активно відпочивати чи подорожувати, а їй не можуть банально вийти з помешкання. У людей з'явилося багато вільного часу, який вони не знають куди витратити. Тому багато хто починає замислюватися над своєю роллю у суспільстві і намагається вносити свої корективи у суспільні відносини, використовуючи при цьому свій аккаунт у певній соціальній мережі або власну веб-сторінку.

Ще одним чинником, який впливає на трансформаційні процеси і виник із початком карантину є те, що люди починають розуміти, що їх звичний спосіб життя може змінитися досить швидко і непрогнозовано для них самих. Це лякає, проте змушує пристосовуватися до обставин так, щоб зберегти хоча б найнеобхідніші ресурси для існування. Наприклад: люди старшого покоління починають опановувати комп'ютерні технології, а молодь вчиться вирішувати свої домашні справи (такі як ремонт, прибирання чи приготування їжі) самостійно. Тобто, люди набувають певні досі невідомі їм навички і звикають жити у новому суспільстві.

Також варто зазначити, що наразі усе, що можливо перенести в Інтернет і цим мінімізувати контакти людей вживу, інтегрують у глобальну мережу. Звичайно, набагато легше вчитися і працювати з дому, адже тут під рукою є все необхідне, проте втрачається такий важливий для людини момент, як живе спілкування. Це трансформує як суспільство в цілому, так і окремих людей. Хочу навести приклад мого знайомого. З самого початку карантину він не покидав свого дому, навіть не виходив у магазин. Ми з ним періодично спілкуємося у Zoom і мені досить помітною є зміна у поведінці та звичках цієї людини. Він став якимось закритим і відстороненим. Найгіршим є те, що тепер він вважає, що йому зовсім не потрібне живе спілкування і не буде потрібне у майбутньому. Мені дуже хотілося б вірити в те, що мій знайомий є винятком із правил, адже суспільство без живих комунікацій стане неспроможним для існування.

Отже, підсумовуючи, хочу сказати, що карантин – це не кінець світу, а ще одна точка неповернення, що має змінити суспільство. Людина здатна не тільки пристосуватися до тимчасових труднощів, а й знайти нові можливості та альтернативи, які неодмінно будуть використані у більш сприятливих умовах. Також важливим є те, що наразі суспільства досить різних держав об'єднуються для подолання карантинної кризи. У час, коли біда одна для всіх, люди тільки у кооперації зможуть її подолати. Тому, особисто для себе я намагаюсь бачити тільки сприятливий і позитивний вплив пандемічних обмежень на майбутнє людства.

Водько Ю. В.,
факультет соціології і права.
Науковий керівник:
Радзієвська О. Г., к.ю.н., провідний
науковий співробітник НДІ ІП
НАПрН України.

ОБМЕЖЕННЯ ПРАВА ВІЛЬНО ЗБИРАТИ, ЗБЕРІГАТИ, ВИКОРИСТОВУВАТИ І ПОШИРЮВАТИ ІНФОРМАЦІЮ В ІНТЕРЕСАХ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Основним нормативно-правовим актом, що гарантує права та свободи людини і громадянина в Україні є Конституція України. У ній зокрема передбачені права людини в інформаційній сфері, що закріплені у статті 34 [1]. Так як усі сфери суспільних відносин сьогодні тісно пов'язані з обміном інформацією, процес інформатизації стрімко розвивається, а світ неупинно глобалізується, то необхідність забезпечення права кожної людини на доступ до інформації, а також право вільно її збирати, зберігати, використовувати і поширювати стає чи не найбільш необхідним в реаліях сьогодення. Проте для того, щоб кожна людина могла реалізувати повною мірою свої права при одночасному забезпеченні захищеності від посягань на них, необхідне існування певних законодавчих обмежень, в яких можуть реалізовуватись дані права, а також для того, щоб охороняти права інших людей від посягань на них. Однією з вимог законодавства є те, що право вільно збирати, зберігати, використовувати і поширювати інформацію не повинно здійснюватися всупереч інтересів національної безпеки України. В разі недотримання такої вимоги, це право може бути правомірно обмежено.

В умовах російсько-української гібридної війни, головним засобом якої є масові інформаційні атаки зі сторони агресора, співвідношення права вільно збирати, зберігати, використовувати і поширювати інформацію та вимог національної безпеки, відповідно до яких і може обмежуватися це право, є вкрай важливим для визначення пріоритетності, стану їх забезпечення та охорони як одного, так і іншого.

Тітко Е. В. у своїй праці зазначає, що Європейський суд з прав людини, розглядаючи справи, пов'язані з обмеженням державою права на свободу вираження поглядів, що в тому числі включається до права на поширення інформації, визначає, що правомірне обмеження свободи вираження поглядів є необхідним в інтересах національної безпеки, яка захищає життєво важливі інтереси людини і громадянина, суспільства й держави, за якої забезпечуються сталий розвиток суспільства, своєчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз національним

інтересам. Оскільки об'єктами охорони національної безпеки є не лише безпосередньо державно-владні інтереси, а й права та свободи людини та громадянина, а також конституційний лад, який власне і гарантує їх реалізацію та охороняє їх від протиправних посягань, то саме правомірне обмеження прав людини в інтересах демократії є вагомим чинником та критерієм збереження безпеки держави та суспільства в цілому [3]. Таким чином пошук балансу між категоріями права людини в інформаційному просторі та поняття національної безпеки є метою нашого дослідження.

Також існує думка, яку висловлює у своєму дослідженні директор Архіву національної безпеки Сполучених Штатів Америки при університеті імені Джорджа Вашингтона Т. Блантон про те, що національна безпека сама по собі не є цінністю, а це є стан, який дає нації можливість захищати свої цінності [6].

Ще один науковець В. Бурк-Вайт вважає, що права і свободи людини та національна безпека насправді доповнюють одне одного і також зазначає, що з точною пропорційністю можна передбачити, що залежно від ступеню захисту прав і свобод своїх громадян залежить імовірність проявів порушень міжнародного права відносно інших держав, зокрема випадків міжнародної інтервенції, втручання у внутрішні справи інших держав тощо [4].

Забезпечення національної безпеки, на нашу думку, повинно здійснюватися спільно з активною участю та залученням різноманітних громадянських інститутів, оскільки абсолютно взаємопов'язаними є показники рівня життя громадян та ступеню захищеності національної безпеки держави. Протидія як внутрішнім так і зовнішнім дестабілізуючим чинникам, як показує практика, найефективніше здійснюється саме завдяки громадянській активності та високій правосвідомості громадян, що спонукає до створення різних волонтерських організацій, які часто показують значно кращі результати, ніж створені для виконання певних функцій державні структури.

Відображення подібної точки зору можна знайти і в праці професора В. Номоконова, який вказує на те, що в державах з демократичним режимом повинен існувати розумний баланс між правами й обов'язками, міжнародними інтересами особи, суспільства і держави. На його погляд, порушення цього балансу призводить до зловживання правами і свободами, появи негативних соціальних наслідків, ослаблення державних начал, порушення законності [7].

Таким чином, вирішення проблеми характеру обмежень конституційних прав і свобод людини і громадянина в інформаційній сфері в інтересах національної безпеки лежить у пошуку компромісу між забезпеченням першого та досягненням другого.

Слід також зауважити те, що в час глобалізації, яка найбільше проявляється в колообігу інформації величезну функцію виконують медіа, які водночас становлять неабияку небезпеку для інтересів держави та її національної безпеки, зокрема тоді, коли зумисно та свідомо поширюється неправдива, маніпулятивна, агресивна інформація або ж інформація, що містить персональні дані, заклики до насильства, засекречена інформація, що належить до державної таємниці тощо. Такі випадки відомі на практиці, наприклад, поширення інформації з персональними даними військовослужбовців Збройних сил України в соцмережах призводять до випадків агресії, нападів на учасників бойових дій на Сході України. В такому контексті питання національної безпеки виходить на перший план, отже таке поширювання інформації не може вважатися правомірним [5].

Цікавою думкою також вважаємо висвітлену у статті Фурашева В.М., якою описується тісно взаємопов'язане існування складових так званого трикутника – це забезпечення прав і свобод людини, прав суспільства і забезпечення функціональних обов'язків держави. І так як абсолютна свобода соціуму, суб'єктів суспільних відносин – людей, а також держави, яка це об'єднує неможлива за визначенням, тож кожен суб'єкт обирає та визначає свою поведінку та дії самостійно, свідомо їх обмежуючи задля комфортного співіснування та взаємодії, що, звичайно, забезпечується загальнообов'язковими правилами поведінки, що виражаються в нормативно-правових актах та у примусі державної влади [2].

Отже, дослідивши питання обмеження права вільно збирати, зберігати, використовувати і поширювати інформацію в інтересах національної безпеки, ми можемо зробити висновок, що дійсно, як забезпечення прав людини в інформаційній сфері, так і національної безпеки мають велике значення для функціонування та існування держави. Питання співвідношення повинно безперервно досліджуватися науковцями, адже саме збереження балансу між даними явищами допоможуть пануванню демократії у державі, непорушності її суверенітету та територіальної цілісності. Оскільки дедалі більше зростають масштаби інформаційних війн, маніпуляцій, а також інформаційного насильства, то пріоритетним завданням стає пошук шляхів досягнення найвищого рівня безпеки інформації для людини. Сьогодні небезпека від впливу інформації на свідомість людини та суспільства, а також суспільні відносини, пов'язані із забезпеченням національної безпеки держави навіть більша, аніж небезпечність впливу людини на інформацію. На нашу думку, правомірне обмеження прав людини в сфері інформації в інтересах національної безпеки є фундаментальним завданням для розбудови розвинутого громадянського суспільства та правової держави.

Список використаної літератури:

1. Конституція України // Відомості Верховної Ради України (ВВР). – 1996. – № 30. – с. 141. URL: <https://cutt.ly/Hg9yS3g>
2. Фурашев В.М. Основні стримуючі фактори правового забезпечення інформаційної безпеки / «Інформація і право», № 2(8)/2013// URL: <https://cutt.ly/tgMF01e>
3. Тітко Е. В. Правомірне обмеження свободи вираження поглядів в інтересах захисту національної безпеки / Науковий часопис НПУ імені М. П. Драгоманова. Серія 18 : Економіка і право.// URL: <https://cutt.ly/3g9yAQv>
4. Ірха Ю. Обмеження конституційних прав і свобод людини і громадянина в інтересах національної безпеки України в сучасних умовах // Вісник Конституційного Суду України. - 2015. - № 5. - С. 78-87 URL: <https://cutt.ly/5g9yOLP>
5. Сухраков , А. С. (2020). Сучасні виклики російсько-української інформаційної війни. // Науковий часопис НПУ імені М.П. Драгоманова. Серія 22. Політичні науки та методика викладання соціально-політичних дисциплін, 22(27), 83-88. // URL: <https://cutt.ly/Lg9yY86>
6. Blanton T.S. National Security and Open Government in the United States : Beyond the Balancing Test / T. S. Blanton // National security and open government : striking the right balance / Campbell Public Affairs Institute, The Maxwell School of Syracuse University. Syracuse, New York, 2003.— P. 33 URL: <https://cutt.ly/4g9ymMF>
7. Номоконов В. А. Права человека и национальная безопасность / В. А. Номоконов // Криминологический журнал Байкальского государственного университета экономики и права. Иркутск : Изд-во БГУЭП, 2008. № 2. С. 5–6. URL: <https://cutt.ly/Cg9yJzJ>

Кухрівський Денис,
факультет соціології і права.
Науковий керівник:
Фурашев В. М., к.т.н., с.н.с., доцент.

НАСЛІДКИ ВПЛИВУ КАРАНТИННОГО РЕЖИМУ НА ТРАНСФОРМАЦІЙНІ ПРОЦЕСИ СУСПІЛЬНИХ ВІДНОСИН

Ситуація, яка склалася сьогодні у світі справді є для нас незвичною. Її цілком можна називати кризовою. Тому що в нас є три масштабні проблеми – ситуація із самим коронавірусом, панікою через пандемію та соціально-економічні проблеми, адже бізнес зупиняється, можливо, деякий закритися. Люди природньо переживають чи матимуть роботу. Ситуація є емоційно складною, тому що є комплексною. Люди дезорієнтовані – не знають, що їм робити, їхній звичний режим змінився [1].

На сьогодні дослідження того, як психологічно позначається і позначиться в майбутньому пандемія та карантин на людське життя, тривають досі. Однак, вже

частково представлена низка цікавих даних з різних куточків світу, про те як саме реагує людство на COVID-19.

Так, наприклад, відповідно до результатів останніх досліджень психологічного впливу поширення COVID-19 у Туреччині (на вибірці 1130 осіб з 28 міст) показало, що 52,7% опитаних оцінили загальний психологічний вплив як помірний; 18,6% показали виражені депресивні симптоми; 26,5% – сильні симптоми тривоги; 7,9% - виражений рівні стресу. Дані, отримані зі Шрі Ланки, підтверджують, що жінки, хворі на COVID-19 та пацієнти з психіатричною історією мають вищий ризик появи психологічної симптоматики у зв'язку з пандемією.

Дослідна група з Індії засвідчує такі основні психологічні впливи пандемії COVID-19 :

- страх і стурбованість про власне здоров'я та здоров'я близьких;
- постійна стурбованість щодо зазнаних фінансових втрат;
- зміни в режимі сну або їжі;
- укладення концентрації та роздратування;
- побоювання та фактичне погіршення хронічних проблем зі здоров'ям;
- посилення вживання алкоголю, тютюну чи інших психоактивних речовин.

Щодо режиму карантину, то дослідницька група з Великобританії детально проаналізувала 24 дослідження із психологічного впливу карантину та підкреслила специфічні стресові фактори:

- тривалість карантину (більше 10 днів провокує значно вищий ризик розвитку симптоматики посттравматичного стресу);
- побоювання зараження, особливо у вагітних жінок та жінок з маленькими дітьми;
- розчарування, нудьга та відчуття ізоляції від решти світу;
- неадекватні запаси, що також викликало тривогу і гнів через 4-6 місяців;
- недостатня інформація, відсутність чітких вказівок.

Результати дослідження вітчизняних науковців також продемонстрували широкий спектр психологічних наслідків, до яких може призвести спалах COVID-19, серед яких поява нових психіатричних симптомів в осіб, які не мають психічних захворювань, а також погіршення стану тих, хто вже страждає на такі захворювання. Спалах коронавірусної хвороби спричиняє суспільні психологічні реакції, такі як напруга, тривога та страх, втрата орієнтирів і планів на майбутнє, також може призводити до посттравматичного стресового розладу, депресії, до загострення психопатологічної симптоматики та психологічних труднощів [2].

«На сьогодні ВООЗ почала говорити про все більшому ураження психіки, зростання випадків тривожних і стресових розладів, початок депресивних розладів і неврозів, алкоголізації, сімейну агресію, розлучення, агресію до дітей тощо», – повідомив Чабан [4].

Також пандемія вплинула і на феміністок. Чимало феміністок, поборників гендерної рівності та жіночих організацій напередодні своєї річниці відчували марність своїх зусиль у боротьбі з розпалом сексизму і мізогінії. Аж ось вибухнула пандемія Covid-19. Вона зробила їхню роботу з окреслення всебічних культурних та системних змін ще важливішою, не в останню чергу тому, що навіть нині занадто мало жінок можуть брати участь у прийнятті рішень на різних рівнях, на яких впроваджуватимуться термінові заходи реагування та окреслюватимуться довгострокові кроки з відновлення та бачення глобальних систем майбутнього. Втім, виживання багатьох феміністичних та жіночих правозахисних організацій знаходиться під загрозою, оскільки ресурси для їхньої подальшої діяльності, яка зараз потрібна як ніколи, будуть перенаправлені на інші цілі. Пандемія COVID-19 не є першопричиною нерівності, але вона посилює, нагнітає та погіршує дискримінаційність і несправедливість наших систем та громад, зокрема через пригнічення, використання та віктимізацію жінок та дівчат у багатьох сферах повсякденного життя.

Не менше пандемія COVID-19 вплинула і на наше спілкування. Адже навчання у вищих навчальних закладах так як і роботу перевели на дистанційний режим. Тому і спілкування відбувається у дистанційному режимі. Попри те, що чимало людей мають досвід онлайн-спілкування, досі ще практично ніхто не стикався з тотальним перенесенням усього спілкування, як з друзями, так і професійного у віртуальний формат. Така онлайн комунікація має багато недоліків у порівнянні з традиційним «живим» спілкуванням. Виникають суттєві викривлення, бо текст не передає міміки, емоцій та безлічі інших знаків, важливих у нашому спілкуванні й, відтак, не дозволяє зчитати жарт, іронію, натяк [5].

Але найбільше пандемія вразила економіку. Перш за все, через епідемію коронавірусу зменшується виробництво в різних країнах світу. Разом з ним, зменшуються і обсяги постачань та торговельних операцій. Через глобальний характер сучасної економіки, це веде до розриву ланцюжків постачання, і відповідно – впливає на виробництво не тільки у серйозно уражених вірусом країнах, а й в усіх, що ведуть з ними інтенсивну торгівлю. Економічна загроза викликана не стільки загрозою самого вірусу, як вимушеними обмеженнями, введеними для запобігання його поширенню.[7] Зміни на фондових ринках, де купують і продають акції

компаній, впливають не лише на самі компанії і трейдерів. Вони впливають на те, як у світі рухаються інвестиції, а також на пенсійні та інші заощадження у багатьох країнах, адже, наприклад, пенсійні фонди часто вкладають гроші клієнтів у цінні папери. Усі головні індекси провідних фондових бірж світу в Японії, Британії та США суттєво впали відтоді, як наприкінці минулого року хвороба почала поширюватися. Від початку нового року FTSE впав на 34,1%, Dow Jones Industrial Average – на 31,1%, а Nikkei – на 28,7%. Ці цифри означають: інвестори бояться, що поширення коронавірусу припинить зростання економіки, а дії урядів будуть недостатніми, аби запобігти поширенню хвороби. У відповідь на це центральні банки у багатьох країнах почали знижувати облікові ставки, щоб зробити гроші дешевшими, а позики – доступнішими. В теорії це також має підтримати споживчий попит.

Із тисячами скасованих рейсів, відряджень і відпусток, туристична галузь зазнала величезних втрат. Уряди по всьому світу запровадили заборони на подорожі, аби стримати поширення вірусу. У США наклали обмеження на авіасполучення із Європою. У Китаї, звідки коронавірус поширився світом, виробництво падає від початку року. Китай виробляє третину усіх товарів у світі та є найбільшим світовим експортером. Тому, зупинка виробництва вразила ланцюжки постачання низки світових гігантів [6].

Список використаної літератури:

1. Христина Гоголь. Як не впасти у депресію. Важлива розмова з психологом про карантин. URL: http://tvoemisto.tv/exclusive/vyyty_zi_shtormu_yak_pryborkaty_koronavirusnu_kryzu_107587.html .–
2. Кубай В.Г. Вплив пандемії COVID-19 та карантину на психологічний стан людини. URL: <https://gatne-rada.gov.ua/covid19-doslidzhennya-vplivu-15-43-44-23-07-2020/> .–
3. Лаура Маннінен. Карантин може бути небезпечніше коронавірусу. Як ізоляція впливає на психіку людей[Електронний ресурс]/ Лаура Маннінен. URL: <https://112.ua/mnenie/karantin-mozhet-byt-opasnee-koronavirusa-kak-izolyaciya-vliyaet-na-psihiku-lyudey-533649.html> –
4. Як коронавірус вплинув на психічне здоров'я людей? URL: <https://news.dtki.ua/society/community/64172> .–
5. Оксана Міхеєва. Українське суспільство та коронавірус: як пандемія змінює кожного з нас зсередини. URL: <https://www.radiosvoboda.org/a/30510549.html> .

6. Коронавірус в цифрах: як змінилася світова економіка? URL: <https://www.bbc.com/ukrainian/features-51994936> .–

7. Данило Герасимов. Коронавірус: як епідемія коронавірусу загрожує світовій економіці? URL: <https://rubryka.com/article/koronavirus-ekonomika/> .–

Ткаченко О. О.,
факультет інформатики та
обчислювальної техніки.
Науковий керівник:
Самчинська О. А., викладач.

СОЦІАЛЬНА ІНЖЕНЕРІЯ У ПЕРІОД ПАНДЕМІЇ

Наразі, під час пандемії, питання інформаційної безпеки стало одним із найбільш важливим. Люди потребують актуальну інформацію щодня, проте через свободу мережі Інтернет пандемія спонукала розвитку соціальної інженерії та фейків. Згідно зі статистикою, зараз приблизно 88% новин присвячені коронавірусу.

Соціальна інженерія є найбільш успішним тактичним методом, використаним у 98% кібератак. Найбільш розповсюдженим способом є фішинг. Прикладом фішинга є розсилка спам-листів, у яких жертву просять відвідати сайт за посиланням або скинути пароль. У результаті, конфіденційна інформація викрадається та використовується для злову акаунтів або отримання доступу до комп'ютера жертви.

Соціальна інженерія, перш за все, спрямована на найгучніші новини у світі, зокрема новини про пандемію COVID-19. Оскільки подібний досвід самоізоляції та дистанційної праці є новим для більшості населення України, не є дивним, що атаки соціальної інженерії мають таким успіх. За даними ресурсу Cynet [5] з початком карантину кількість фішингових атак в Італії зросла втричі. Наразі йдеться про те, що пандемія несе не лише біологічну загрозу, а й інформаційну.

Серед соціальних атак можна виокремити два рівня:

- кримінальний, що включає в себе фішинг та фінансові махінації;
- кібероперації, що стосуються політичної дезінформації, тролінгу та нові додатки для стеження за людьми.

Прикладом атак побутового рівня є розповсюдження електронних листів та СМС із посиланнями на різні сайти або програми, що містять віруси. Найчастіше відправники таких листів вказують назви державних установ, наприклад, Міністерство охорони здоров'я або благодійні компанії. За даними дослідження TrenMicro [2], близько 65% соціальних атак відбуваються через спам.

Іншим прикладом є фейкові новини, пов'язані із місцезнаходженням хворих. У квітні цього року було опубліковано список адрес хворих на коронавірус у Києві. Дана новина дуже швидко стала «вірусною», а через декілька днів після публікації у мережі з'явилося спростування правдивості даного списку, проте люди вже побачили його та багато хто повірив. Крім того, популярним типом фейків стали новини про всесвітні політичні змови.

Ще одним яскравим прикладом є реклама різних додатків, пов'язаних із темою пандемії. Наприклад, карти розповсюдження коронавірусу, які стали дуже популярними через природню тривогу людей. Проте, насправді такі додатки можуть встановлювати віруси до вашого девайсу або навіть викрадати особисту інформацію. У найгіршому випадку «карта» блокує телефон та вимагає гроші, погрожуючи видаленням всього, що зберігалось на гаджеті.

Наразі в українському законодавстві відсутнє визначення поняття «фішинг» та «соціальна інженерія». Проте, існує ряд статей Кримінального кодексу України, під поняття та склад злочину яких підпадають і діяння вчинені у кіберпросторі, серед яких:

- У розділі 4 (злочини проти власності):
 - Ст. 190 «Шахрайство»;
 - Ст. 192 «Заподіяння майнової шкоди шляхом обману або зловживання довірою»;
 - Ст. 194 «Умисне знищення або пошкодження майна»;
 - Ст. 195 «Погроза знищення майна»;
- У розділі 16 (Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку):
 - Ст 353 «Самовільне присвоєння владних повноважень або звання службової особи»;
- У розділі 16 (злочини у сфері використання електронно-обчислювальних машин (комп'ютерів):
 - Ст. 361 «Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку»;
 - Ст. 361¹ «Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут»;
 - Ст. 361² «Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних

машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації»;

- Ст. 362 «Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї» [6].

Наведена вище інформація демонструє загрози інформаційній безпеці, з якими будь-хто може зустрітися у будь-який час. Саме тому, у наш час людству необхідно почати більш серйозно ставитися до новин у мережі Інтернет та будь-якої інформації з неперевіраних джерел. Відповідальне ставлення до встановлення додатків та посилань допоможе запобігти серйозних проблем із технікою, а критичне мислення – не довіряти всіх новинам, що потрапляють у поле зору. Крім того, законодавчі органи України вживають дії для захисту населення від методів соціальної інженерії.

Список використаної літератури:

1. Human hacking a guide to social engineering. URL: <https://www.comtact.co.uk/blog/human-hacking-a-guide-to-social-engineering> (дата звернення: 10.05.2020).
2. Developing Story: COVID-19 Used in Malicious Campaigns. URL: <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names-and-malicious-domains> (дата звернення: 10.05.2020).
3. Список з адресами "хворих" на COVID-19: поліція перевіряє публікацію. URL: <https://www.ukrinform.ua/rubric-society/3002413-spisok-z-adresami-hvorih-covid19-policia-perevirae-publikaciju.html> (дата звернення 11.05.2020).
4. Coronavirus Cybersecurity: Scams To Watch Out For. URL: <https://securityboulevard.com/2020/03/coronavirus-cybersecurity-scams-to-watch-out-for/> (дата звернення: 10.05.2020).
5. The Coronavirus is Already Taking Effect on Cyber Security– This is How CISOs Should Prepare. URL: <https://threatpost.com/cynet-the-coronavirus-is-already-taking-effect-on-cyber-security-this-is-how-cisos-should-prepare/153758/> (дата звернення: 10.05.2020).
6. Кримінальний кодекс України. URL: <https://zakon.rada.gov.ua/laws/show/2341-14#Text> (дата звернення: 11.05.2020).

Бурдело Є. В.,
фізико-технічний інститут.
Науковий керівник:
Стьопочкіна І. В., к.т.н., доцент.

МЕТОДИКА МОНІТОРИНГУ ЧУТЛИВИХ ДАНИХ ОБ'ЄКТА КРИТИЧНОЇ ІНФРАСТРУКТУРИ НА ОСНОВІ ВІДКРИТИХ ДЖЕРЕЛ

На даний момент в Україні зроблено ряд кроків до покращення кіберзахисту важливих для країни промислових, енергетичних та інших об'єктів, зокрема затверджено Постанову Кабінету Міністрів України “Про затвердження загальних вимог до кіберзахисту об'єктів критичної інфраструктури”, ведуться роботи над проектами Закону України “Про критичну інфраструктуру та її захист”, Постанови Кабінету Міністрів України “Про затвердження Порядку віднесення об'єктів до об'єктів критичної інфраструктури”.

Кіберзахист об'єктів критичної інфраструктури є актуальним питанням, що пов'язано із тим, що інфраструктура таких об'єктів дедалі більше пов'язується із середовищем Інтернет. Наразі, коли на фоні всесвітньої пандемії, спричиненою COVID-19, весь світ переходить на віддалену роботу, проблема стає ще актуальнішою.

Зокрема в роботі розглянуто проблеми вразливості, що можуть спричинити атаки із використанням техніки Google dorking.

В рамках даної роботи зібрано типові види запитів, які варто використати для самоперевірки персоналом, відповідальним за кіберзахист об'єкту, запропоновано методику тестування на основі запитів Google dorking та надано рекомендації для попередження витоків та усуненню поширення чутливої інформації в мережі Інтернет.

Способи одержання чутливої інформації по відкритих даних

Наразі існує велика кількість атак, які можуть призвести до одержання зловмисником чутливої інформації. Однією із ефективних технологій, які дозволяють розшукати такі дані у мережі Інтернет, є Google Dorking.

Google Dorking або Google Hacking – це техніка для створення запитів в різних пошукових системах для виявлення прихованої інформації та вразливостей, які можна виявити на загальнодоступних серверах та пристроях.

Замість звичайного типу пошукового запиту, який фокусується на семантичному способі поставлення питань, безпосередньо шляхом написання цілого питання або вибраних ключових слів, GD базується на зворотному проектуванні того, як машини сканують та індексують веб-вміст.

Інформація, яка може бути знайдена із використанням Google Dorks

З допомогою Google Dorking можна знайти будь-яку інформацію у текстовому, файловому або графічному виді, яка є у публічному доступі. Список можливих даних для пошуку: логіни, паролі, сторінки логіну для адміністраторів веб-сайту, конфіденційні, державні або військові документи, державні або військові документи, адреси електронних скриньок, дані банківських рахунків, файли будь-яких форматів (pdf, excel, txt та інші), HTML заголовки, логи, властивості систем, номери телефонів, камери відеонагляду з вільним доступом, фотографії та інші види інформації.

Таблиця: “Основний синтаксис Google Dorking” [2].

inurl:	Пошук документів, що містять ключове слово після двокрапок у назві або адресі.
allinurl	Google обмежить результати лише тими, що містять усі слова запиту в URL-адресі.
intitle:	Якщо ви включите у свій запит [intitle:], Google обмежить результати сторінками, що містять це слово в заголовку.
site:	Результати лише тими веб-сайтами в даному домені
stocks:	Терміни запиту як символи біржі, і буде посилатися на сторінку, що показує біржову інформацію для цих символів.
define:	Визначення слів, які ви вводите після нього, зібрані з різних Інтернет-джерел.
info:	Інформацію про цю веб-сторінку, яку має Google.
related:	Веб-сторінки, які “схожі” на вказану веб-сторінку.
link:	Веб-сторінки, які мають посилання на вказану веб-сторінку

Методика пошуку чутливої інформації критичної інфраструктури

Одним із прикладів критичних інфраструктур в Україні є енергетична компанія ObjectCompanyName. Спробуємо знайти інформацію про організаційну структуру компанії, ПІБ співробітників, назви їх посад, корпоративних електронних мереж, телефонних номерів, типів та моделей обладнання, що використовується в системах управління технологічними процесами, системах захисту та інформації щодо наявного ПЗ та його версій.

З допомогою синтаксису GD шукаємо всю можливу інформацію про співробітників компанії у соціальних мережах та інших сервісах, які

використовуються у роботі та повсякденному житті працівників.[3] [site:trello.com site: www.facebook.com site: www.linkedin.com site: www.instagram.com intext: objectcompanyname].

Скористувавшись цими запитами, можна знайти особисті сторінки людей, де згадується назва objectcompanyname. Наприклад, сторінки LinkedIn, де вказані стеки технологій, номери телефонів, поштові адреси та іншу інформацію, яка може запустити ланцюг атаки на підприємство.

Використовуючи оператори “info” та “related”, знайдемо список схожих веб-сайтів та конкретну інформацію, представлену в заголовку сайта: [related:objectcompanyname.com, info:objectcompanyname.com].

Файл robots.txt або індексний файл - звичайний текстовий документ в кодуванні UTF-8, діє для протоколів http, https, а також FTP. Файл дає пошуковим роботам рекомендації: які сторінки / файли варто сканувати.

- site:objectcompanyname.com inurl:robots.txt;
- site:www.objectcompanyname-kem.com.ua inurl:robots.txt;
- site:www.objectcompanyname-dnem.com.ua inurl:robots.txt.

Даний оператор дозволяє отримати доступ до параметрів конфігурацій різних серверів. Після проведення запиту, переходимо в файл robots.txt, шукаємо шлях до «web.config» і перехід по заданому шляху файлу. Щоб отримати ім'я сервера, версію і інші параметри, робиться наступний запит:

- site:objectcompanyname.com intitle:index.of server.at;
- site:www.objectcompanyname-kem.com.ua intitle:index.of server.at;
- site:www.objectcompanyname-dnem.com.ua intitle:index.of server.at;
- site:gov.ua inurl:backup intitle:index.of inurl:admin;

Наведений нижче запит знайде усі файли вибраного формату, у яких міститься хоча б один адрес електронної пошти з доменом ObjectCompanyName (корпоративної пошти співробітників компанії)

- "@objectcompanyname.com" filetype:xls (csv/xlsx/xlsm/xlm/xlt).

З допомогою синтаксису GD можливо знайти інформацію про паролі. Список можливих комбінацій для пошуку паролів у відкритому доступі:

- "objectcompanyname" password filetype:xlsx OR password filetype:xml (docx/csv/pdf/xml/docx/csv/pdf).

Рекомендації для захисту

Наступні рекомендацій слід дотримуватися адміністраторам будь-яких веб-платформ і серверів, щоб уникнути загроз від GD:

- Систематичне оновлення операційних систем, сервісів і застосунків.

- Впровадження та обслуговування анти-хакерських систем.
- Поінформованість про роботу і різних процедурах пошукових систем, а також способи перевірки таких процесів.
- Видалення конфіденційного вмісту із загальнодоступних джерел.
- Поділ загальнодоступного контенту, приватного контенту и блокування доступу до контенту для користувачів загальна доступу.
- Проводити тестування на проникнення.

Висновок.

На прикладі компанії ObjectCompanyName з допомогою синтаксису GD у відкритому доступі було знайдено особисті сторінки співробітників у соціальних мережах, адреси електронних пошт, контракти, чутливу інформації про існуючі веб-сайти, інформацію про системи захисту, обладнання, бюджети та технології, які використовуються на підприємствах та у ІТ структурі компанії.

Список використаної літератури:

1. Cyber-Security in Critical Infrastructures / S.Rass, S. Schauer, S. König, S. Zhu., 2020. – 299 с.
2. Google Dorking или используем Гугл на максимум. – 2020. URL : <https://habr.com/ru/company/postuf/blog/510766/>.
3. 7,000 Dorks for hacking into various sites. – 2018. URL : <https://github.com/aliadhillon/7000-Google-Dork-List>.

Соболь Н. О.,

студентка ІПСА КПП ім. Ігоря Сікорського
Науковий керівник:

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

КІБЕРЗЛОЧИНІСТЬ В УМОВАХ ПАНДЕМІЇ COVID-19

На сьогодні інформаційні технології відіграють важливу роль у нашому житті. Вони значно спрощують його і допомагають здобути потрібну інформацію дуже швидко. Зараз важко знайти галузь, в якій ІТ не беруть участь. Більшість підприємств переходять на автоматизоване виробництво і для цього розробляються нове програмне забезпечення. Майже не залишилося шкіл, в яких немає комп'ютерного класу, адже діти починають вивчати інформатику ще з першого класу. У вільному доступі є чимала кількість бібліотек і вже не потрібно витрачати купу часу, щоб їхати на інший кінець міста, замовляти

книгу і ще й відшукувати щось у ній. Так, наше життя зараз дуже тісно пов'язане з новими технологіями, а в період карантину ми відчуваємо це, як ніколи. Адже за комунальні послуги можна платити в Інтернеті, отже не потрібно відстоювати великі черги і наражати себе та своїх близьких на небезпеку зараження. До того ж, це ще й економія вашого часу: у багатьох людей робота перейшла в режим онлайн, усі покупки, а також спілкування з друзями, рідними та знайомим теж відбуваються в Інтернеті й цим, на жаль, не забувають користуватися шахраї. Тільки в Україні кількість кіберзлочинів зросла у 2,5 рази за останні 5 років [1]. До того ж, на тлі пандемії коронавірусу поліцейська служба ЄС фіксує збільшення числа кіберзлочинів, шахрайств, крадіжок та підробок критичних товарів [2]. Це, звичайно, пов'язано з розвитком нових технологій, які проникають у всі сфери нашої діяльності.

Кіберзлочинність – це злочинність, пов'язана як з використанням комп'ютерів, так і з застосуванням інформаційних технологій і глобальних мереж. У той же час термін «computercrime» в основному відноситься до злочинів, скоюваних проти комп'ютерів або комп'ютерних даних [3].

В.О. Притула запропонував наступну модель сучасного кіберзлочину (рис. 1):

Рисунок 1. Модель сучасного кіберзлочину (за В.О. Притулою) [3].



Що ж відбувається у світі під час пандемії COVID-19 і як інтернет-шахраї користуються нашою необачністю (за даними проекту CyberEast):

- поширюють через веб-сайти шкідливі програми або документи, які виглядають справжніми і нібито надають інформацію або рекомендації про

COVID-19, але натомість використовуються для зараження комп'ютерів і вилучення облікових даних користувачів .

- створено програму-вимагач Ransomware – шкідливе програмне забезпечення, яке блокує медичні, наукові чи інші установи, пов'язані з медициною, де люди проходять тестування на COVID-19 або де розробляються вакцини, до тих пір, поки їм не буде сплачена певна грошова сума
- правопорушники отримують доступ до систем компаній або інших організацій, орієнтуючись на співробітників, які працюють вдома.
- створено нові схеми шахрайства, за допомогою яких людей обманюють, щоб вони купили такі товари як маски, дезінфікуючі засоби для рук, а також підроблені ліки, які, як стверджують шахраї, запобігають або виліковують SARS-CoV-2.
- дезінформація або фейкові новини поширюються троями і фальшивими обліковими записами в ЗМІ та соціальних мережах для створення паніки, соціальної нестабільності і недовіри до урядів або до заходів, які застосовуються їх органами охорони здоров'я [4].

В звіті поліцейської служби Європейського Союзу “Pandemic profiteering: How criminals exploit the COVID-19 crisis” констатується: “Кількість кібератак є значною і, як очікується, ще збільшиться. Кіберзлочинці продовжуватимуть впроваджувати інновації у розробці різних зловмисних програм та пакети з викупними програмами, розроблені на тему навколо пандемії COVID-19. Вони можуть розширити свою діяльність, щоб включити інші типи онлайн-атак” [5]. Яскравим свідченням діяльності кіберзлочинців стала хакерська атака на Університетську лікарню в Брно в Чеській Республіці, що змусило закрити всю ІТ-мережу цього закладу, відкласти термінові хірургічні операції та перенаправити пацієнтів в іншу лікарню [5].

Таким чином, у період пандемії COVID-19 люди у всьому світі стали ще більше користуватись мережею Інтернет та різними соціальними мережами, чим не могли не скористатись кіберзлочинці. Глобальна пандемія COVID-19 – це не лише серйозне питання охорони здоров'я, але й важлива проблема в кібербезпеці. Злочинці швидко скористалися розповсюдженням коронавірусу і зловживають попитом людей на інформацію та онлайн-доставки. Вони також використали COVID-19 для здійснення нападів із застосуванням соціальної інженерії, зокрема електронних листів через масовані спам-кампанії та більш цільових спроб. Регулярно фіксуються кібератаки з боку організацій та осіб, включаючи фішинг-компанії, які поширюють зловмисне програмне

забезпечення через шкідливі посилання та вкладені файли, виконують атаки зловмисних програм та програм-вимагачів, що спрямовані на отримання прибутку від світової системи охорони здоров'я. Інформація від правоохоронних органів свідчить про зростання активності в Інтернеті і з боку осіб, які шукають матеріали про насильство над дітьми. Вони очікують, що через ізоляцію діти є більш вразливими, знаходяться під меншим наглядом та більше часу проводять в Інтернеті.

Список використаної літератури:

1. Кількість кіберзлочинів в Україні зросла вдвічі за останні п'ять років – Opendatabot. URL: <https://mind.ua/news/20203511-kilkist-kiberzlochiniv-v-ukrayini-zroslo-vdvichi-za-ostanni-p-yat-rokiv-opendatabot>
2. Сааков В. Європол: Під час коронавірусної кризи активізуються кіберзлочинці та шахраї. URL: <https://www.dw.com/uk/європол-під-час-коронавірусної-кризи-активізуються-кіберзлочинці-та-шахраї/a-52935286>
3. Притула В. О. Кіберзлочинність. URL: https://ukrainepravo.com/legal_publications/essay-on-it-law/it_law_prytula_cybercrime/
4. Кіберзлочинність і коронавірус: попередження від проекту CyberEast. URL: <https://eufordigital.eu/uk/cybercrime-and-coronavirus-warning-from-cybereast-project/>
5. De Bolle C. Pandemic profiteering: How criminals exploit the COVID-19 crisis. URL: <https://www.europol.europa.eu/publications-documents/pandemic-profiteering-how-criminals-exploit-covid-19-crisis>