With the support of the Erasmus+ Programme of the European Union

EULIoT

National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"

Міністерство освіти і науки України
Національний технічний університет України
«Київський політехнічний інститут
імені Ігоря Сікорського»
Факультет соціології і права

ЗБІРНИК МАТЕРІАЛІВ
конференції молодих вчених та студентів

ІНТЕРНЕТ РЕЧЕЙ: ТЕОРЕТИКО-ПРАВОВІ ТА ПРАКТИЧНІ АСПЕКТИ ВПРОВАДЖЕННЯ В УМОВАХ ЄВРОПЕЙСЬКОЇ ІНТЕГРАЦІЇ

02 листопада 2022 року

КИЇВ
2022

СКЛАД ОРГАНІЗАЦІЙНОГО КОМІТЕТУ:

Баранов О.А. - *доктор юридичних наук, професор, Керівник наукового центру цифрової трансформації і права Державної наукової установи «Інститут інформації, безпеки і права Національної академії правових наук України». Академічний лідер проекту «Європейська інтеграція: законодавство та Інтернет речей».*

Головко О.М. - *кандидат юридичних наук,, старший викладач кафедри інтелектуальної власності та приватного права, КПІ ім. Ігоря Сікорського. Координатор проекту «Європейська інтеграція: законодавство та Інтернет речей».*

Дубняк М.В. - *кандидат юридичних наук, старший викладач кафедри інформаційного, господарського та адміністративного права, КПІ ім. Ігоря Сікорського. Менеджер проекту «Європейська інтеграція: законодавство та Інтернет речей».*

Видання рекомендоване до друку рішенням
Вченої ради факультету соціології і права
Національного технічного університету України
«Київський політехнічний інститут імені Ігоря Сікорського»

Інтернет речей: теоретико-правові та практичні аспекти впровадження в умовах Європейської інтеграції: зб.матеріалів науково-практичної конференції молодих вчених та студентів (02.11.2022, м. Київ) : ел. збірник / Упоряд.: Баранов О.А., ГоловкоО.М., Дубняк М.В. – Київ : КПІ ім. Ігоря Сікорського, 2022. – 114 с.

У конференції взяли участь студенти КПІ ім.Ігоря Сікорського та курсанти Луганського державного університету внутрішніх справ ім. Е.О. Дідоренка

Рекомендується студентам та аспірантам, а також усім, хто цікавиться проблемами правового регулювання суспільних відносин у сфері застосування штучного інтелекту, робототехніки, криптовалют, технологій блокчейн, хмарних технологій, великих даних та інших складових Інтернету речей (IoT), правовим забезпеченням цифрової трансформації, дослідженням національного законодавства та законодавства Європейського Союзу з питань забезпечення кібербезпеки, вільного обігу даних, захисту персональних даних.

Матеріали подано в авторській редакції.

Конференцію проведено в рамках реалізації міжнародного проекту у сфері освіти «Європейська інтеграція: законодавство та Інтернет речей» у межах напряму Жан Моне «Модуль» програми «Erasmus+» №620017-EPP-1-2020-1-UA-EPPJMO-MODULE (спільний проект КПІ ім. Ігоря Сікорського, Еразмус+ Жан Моне Фонду та Виконавчого агентства з питань освіти, аудіовізуальної діяльності та культури за підтримки ЄС)».

Зміст

БРЕЦКО Валерія
студентка ФСП, КПІ ім. Ігоря Сікорського

СВОБОДА ІНТЕРНЕТУ В КОНТЕКСТІ СУЧАСНИХ МІЖНАРОДНИХ ВІДНОСИН

Сучасний світ невіддільний від інформаційно-комунікаційних технологій (далі ІКТ), які не тільки змінюють принципи та форми збору, обробки та передачі інформації, але й починають потужно впливати на культуру, економіку та політику , військово-стратегічні аспекти суспільного життя. ІКТ стали одним із головних факторів забезпечення та підтримки стабільного розвитку. Кількість, технічний рівень та доступність інформаційних ресурсів визначають рівень розвитку країни та її статус у міжнародному співтоваристві.

Визначення інформаційно-комунікаційних технологій часто є синонімом інформаційних технологій (ІТ), хоча ІКТ є більш загальним терміномДідоренка, який підкреслює роль об’єднуючих технологій та інтегрованого забезпечення телекомунікацій, комп’ютерів, програмного забезпечення, яка дозволяє користувачам створювати, отримувати, одержувати доступ, зберігати, передавати та змінювати інформацію. Іншими словами, ІКТ

складається з ІТ, а також телекомунікацій, медіа-трансляцій, усіх видів аудіо і відео обробки, передачі, мережевих функцій управління та моніторингу.

Соціальна інформатизація є перспективним шляхом економічного, соціального та освітнього розвитку, а міжнародна інформатизація спрямована на формування та розвиток інтелектуального потенціалу країни [8, с.72].

Міжнародна інформація визначається як сукупність відомостей, що характеризують структуру, загальні властивості та питання, пов'язані з їх пошуком, аналізом і поширенням у системі міжнародних відносин. Простір міжнародної інформації визначається конституційними нормами окремих країн, міжнародними угодами та технічним забезпеченням інформаційних процесів. Технологічна революція в системі масової комунікації, по-перше, сприяла вирівнюванню інформаційних та управлінських можливостей державних і недержавних структур, а по-друге, наразила інформаційну індустрію на нові небезпеки, пов'язані зі злочинністю.

Міжнародне право накладає на держави позитивні зобов'язання щодо обмеження (заборони) незаконної інформації. Пропаганда війни та розпалювання насильства на ґрунті етнічної, расової чи релігійної ненависті, пряме та публічне підбурювання до

геноциду, терористична пропаганда та дитяча порнографія обмежені та вимагають ухвалення відповідних заборон на національному рівні та кримінального переслідування згідно з національним законодавством.

Концепція свободи Інтернету перебуває на стадії формування, маючи переважно міжнародно-політичний зміст та потребує розвитку у вимірі позитивного міжнародного права, що є завданням на найближчу перспективу в порядку денному Ради Європи.

Проблема визначення змісту поняття свободи Інтернету є міжнародно- правовим питанням у сфері Інтернету, якій все більше приділяють увагу різні міжнародно-правові наукові та академічні спільноти.

Першою такою спільнотою, яка спробувала розкрити зміст цього поняття стала група експертів ЮНЕСКО. Вони визначили основні принципи, які стали основою змісту поняття свобод Інтернету, серед яких:

1) принцип відкритості, глобальності і публічності для здійснення свободи думок і вираження (свобода вираження он-лайн);

2) онлайнового контенту (свободи від фільтрації / цензури);

3) соціальних медіа і соціальних мереж (свобода медіа он-лайн).

На відкритті міжнародної конференції в Гаазі «Свобода он-лайн» у грудні 2011 р. державний секретар США Г.Р. Клінтон повідомила про створення міжурядової «Коаліції Онлайнової Свободи» (англ. Freedom Online Coalition), до складу якої увійшло 14 держав, та закликала держави працювати разом, щоб поліпшити дипломатичні зусилля, заохочувати більшу увагу до прав людини з боку корпорацій та посилити підтримку кіберактивістів і блогерів, які перебувають під загрозою. У заключній декларації конференції держави підтвердили, що свобода вираження он- лайн має так само захищатися як оффлайн [6, с.56].

Міжнародний союз електрозв'язку (далі – «МСЕ») як спеціалізована установа ООН, що здійснює координацію дій стосовно розбудови глобального інформаційного суспільства доклав зусиль для формування власного переліку питань державної політики, що потребують регулювання. У Резолюції Ради МСЕ No 1305 налічується дванадцять пунктів:

1) багатомовність Інтернету, в тому числі багатомовність найменувань доменів;
2) міжнародні інтернет-з'єднання;
3) безпека, безперервність, відмовостійкість і надійність Інтернету;
4) боротьба з кіберзлочинністю;
5) вжиття ефективних заходів щодо спаму;

6) питання, що стосуються використання та неправомірного використання Інтернету;
7) наявність, доступність, надійність і якість обслуговування, особливо в країнах, що розвиваються;
8) сприяння нарощуванню потенціалу в галузі управління Інтернетом у країнах, що розвиваються;
9) повага до приватного життя та захист персональних даних;
10) захист дітей та молоді від експлуатації [4, с.112];

Фактично цей перелік містить проблемні питання сучасного Інтернету, які можна назвати «проблемами росту», з якими не можна впоратися без участі держав, лише засобами саморегулювання.

Що ж до питань, які постають у зв'язку з особливостями суспільних відносин в Інтернеті, до яких не адаптоване ані національне, ані міжнародне право, то Робоча група Комісії з науки і техніки в цілях розвитку ЮНКТАД (Конференція ООН з торгівлі та розвитку) лише констатувала прогалини, не запропонувавши проектів рішень. Причинами нерозвиненості цього напрямку міжнародного співробітництва визнано наступні:
-недостатній інституційний потенціал та/або брак ресурсів для вирішення суспільних питань у сфері Інтернету, таких як кіберзлочинність, захист прав споживачів, юрисдикція;

-відсутність міжсекторальної взаємодії для вирішення комплексних питань, таких як захист приватності і персональних даних з позицій прав людини, міжнародної торгівлі, стандартизації і безпеки;

- розрив у знаннях і дослідження з міжнародно-правових питань державної політики у сфері Інтернету.

Міжнародно-правове забезпечення вирішення питань національної політики на глобальній Інтернет-арені є першочерговим завданням на найближчу перспективу, оскільки регуляторні ініціативи на регіональному рівні та нормативно-правові акти, прийняті окремими країнами, не можуть охопити глобальний масштаб інформаційних комунікацій. Дослідивши нормативні документи міжнародних та регіональних організацій у сфері правового регулювання ІКТ у міжнародних відносинах, можна зробити висновок, що єдиної основи та методики розуміння проблематики свободи Інтернету ще не сформовано. Враховуючи масштаби та транснаціональний характер такого поняття, жодна країна світу не може поодинці протистояти загрозам які несе в собі складова поняття свободи Інтернету.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Брижко В . М., Радянська А. І., Швець М. Я., Порівняльно-правове дослідження відповідності законодавства України законодавству ЄС у сфері персональних даних. Київ: Тріумф 2006. 256 с.

2. Додатковий протокол до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних щодо органів нагляду та транскордонних потоків даних URL: https://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=994_363#Text (Дата звернення 07.09.2022)
3. Казакова Н., Давиденко І., Штукаленко А. Інформатизація глобального економічного розвитку та місце України в інформаційному просторі. Вісник Харківського національного університету імені В. Н. Каразіна. 2019. 18-26. URL: https://periodicals.karazin.ua/irtb/article/view/14447 (дата звернення 02.10.2022)
4. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних: міжнародний договір України від 28 січня 1981 р. URL: https://zakon.rada.gov.ua/laws/show/994_326#Text (Дата звернення 07.09.2022)
5. Лєонов С. В., Рубанов П. М., Богданова К. А. Інноваційні фінансові технології та їх вплив на економічну безпеку держави. Управління інноваційною складовою економічної безпеки: монографія / за ред. О. В. Прокопенко, В. Ю. Школи, В. О. Щербаченко. Суми: ТОВ «Триторія», 2017. Т. ІІІ. С. 56–70 (0,67 друк. арк.).
6. Про Доктрину інформаційної безпеки України : Указ Президента України від 08.07.09 р. No 514/2009 //

Офіційний вісник України. – 2009. – No 52. –Ст. 1783. 7. Панова І.В. Тенденції розвитку системи інформаційного права України на сучасному етапі // Форум права. – 2011. – No 2. – С. 694-699. – Режим доступу : http://www.nbuv.gov.ua/ejournals/FP/2011-2/11pivnce.pdf
8. Хорошко В., Козел Т., Ярошенко О. ОСОБЛИВОСТІ ЗАСТОСУВАННЯ СУЧАСНОЇ ІНФОРМАЦІЙНОЇ ЗБРОЇ : Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 1 (29), 2015 р (дата звернення: 30.10.2022).

ВОДОЛАГА М.О.
Курсант Луганського державного університету
внутрішніх справ ім. Е.О. Дідоренка

ПРОБЛЕМИ РОЗВИТКУ ІНТЕРНЕТ РЕЧЕЙ У СУЧАСНОСТІ

У наш час Інтернет невіддільний від життя більшості людей. Ще в 1990-х роках в Україні ніхто не замислювався над питанням: «Що таке Інтернет?». Істотно відрізняється нинішня ситуація - кількість користувачів мережі зростає з кожним днем. З його допомогою протягом доби відкривається багато нових

напрямків економіки та суспільне життя людини. Одним із них є Інтернет речей.

IoT – це дротова або бездротова мережа, яка підключає пристрої з автономною підтримкою управляються розумною системою з передовою операційною системою, автономно підключені до Інтернету, можуть виконувати власні або хмарні програми та аналізувати зібрані дані. Крім того, вони мають можливість отримувати, аналізувати та передавати дані з інших систем.

Термін «Інтернет речей» вперше ввів Кевін Ештон у 1999 році під час роботи в Procter & Gamble для опису системи, яка може підключати фізичні об’єкти до датчиків та Інтернету. Ештон ввів цей термін, щоб проілюструвати потенціал радіочастотної ідентифікації (RFID), яка використовується в системах поставок підприємств для підрахунку та відстеження товарів без втручання людини. Сьогодні «Інтернет речей» став популярним терміном, який використовується для опису сценарію, у якому підключення до Інтернету та обчислювальна потужність розширюються до безлічі об’єктів, пристроїв, датчиків і побутових предметів.[3. с.1]

Багато Експертівв та спеціалістів стверджують, що Інтернет речей є однією з найпопулярнішою та найперспективніших технологій останніх років, що вже

сьогодні фактично створює сотні нових продуктів і призводить до появи нових компаній на ринку, які диктують свої умови IT-гігантам. Ви можете не помічати, але Ви самі, ваші друзі чи колеги вже не перший рік користуються такими пристроями кожен день. Більше того, у чималій кількості українських домівок вже встановлені системи "розумного будинку", в які інтегровані десятки датчиків.

Переваги IoT, які вже доступні,та ще знаходяться в розробці можна краще продемонструвати на прикладах, особливо сфер існує багато застосувань цієї технології.

IoT здатна оптимізувати діяльність працівників органів досудового розслідування, а одним із таких прикладів є впровадження технологій 3D сканування. Досвід застосування цієї інновації у діяльності польських, американських та інших поліцейських служб дає підстави для оптимізму та очікування активного застосування і українськими фахівцями, зокрема при розслідуванні ДТП.

Натомість застосування 3D технології при огляді місця події дозволяє: − збільшити інформативність зібраних даних про ДТП, їх точність; − зафіксувати найдрібніші сліди, деталі деформацій транспортних засобів, пошкоджень дорожньої інфраструктури, у тому числі в умовах темної пори доби, що не впливає на

результати; − візуалізувати дані, створити віртуальну модель місця події з високою ілюстративною якістю, що дозволяє «повернутися на місце події» не виходячи з кабінету слідчого, експерта, прокурора чи залу судових засідань; − оптимізувати вимірювання параметрів, необхідних для визначення механізму та причиннонаслідкових зв’язків події; − виготовити за наявності спеціального програмного забезпечення 2 D схеми до протоколів процесуальних дій; − скоротити час процесуальних дій, що не потребує тривалого перекриття смуг руху; − посилити безпеку осіб, залучених до процесуальних дій при ДТП.[4. с.97]

Українські споживачі знайомі з пристроями в концепції IoT. Головним чином завдяки пристрою, який носять на тілі. Це фітнес –браслети, розумні годинники, «розумні окуляри» та інше. Для багатьох ці гаджети стали, як рідними. Навіть зараз вже є такі застосунки, які слідкують за етапами нашого сна і активність протягом дня, ці застосунки можуть стежити за частотою серцевих скорочень, своїм нормування. Крім того, усі дані синхронізуються з власним додатком на смартфоні, та ідеально працюють зі сторонніми програмами.

У Інтернет речей є також негативні, небезпечні наслідки, а проникнення високих технологій в повсякденність приносить нові загрози. Якщо

нещодавно активність зловмисників в мережі була аспектом інформаційної безпеки, то тепер під загрозою можуть перебувати життя і здоров'я людей. Поки це лише тривожні припущення, однак реальність вже зараз дає привід турбуватися про фізичну безпеку при взаємодії з такими пристроями.

Актуальним прикладом є «розумний» автомобіль. Багато років тому, Безпілотні автомобілі є темою для письменників-фантастів, але вже Сьогодні безпілотні автомобілі їздять вулицями Києва, Дніпра та практично у кожній країні. І ці безпілотні автомобілі іноді попадають у нещасні випадки: Наприклад, широко обговорювалися випадки зі смертельними наслідками викликаною несправністю автопілота Tesla. Хто в цих випадках повинен відповідати, власник автомобіля або виробник пристрою - невідомо. Навіть без урахування системи автопілот, сучасний автомобіль насправді напханий різними високотехнологічними модулями, датчиками та контрольним обладнанням, яким можна дистанційно керувати, в тому числі через інтернет. Частіше є новини про проблеми, не пов'язані безпосередньо з автомобілем та механікою машини, безпеку програмного забезпечення та ситуація з домашніми IoT-пристроями залишає бажати кращого. І це питання стосується багатьох різних виробників. Так, у 2014 році автомобільна компанія General Motors,

змушена була відкликати більше 3 мільйонів автомобілів через програмну помилку.

Наступна велика проблема – конфіденційність користувачів. Питання в тому, що оскільки «розумні» пристрої збирають багато інформації про їх «господарів». Контролювати, що вони точно знають про власника пристрою та його виробника, ну це майже неможливо. В неприємному, але тим не менше все ще оптимістичному сценарії, ця інформація може продаватися рекламодавцям.. Інша справа, що ця інформація колись може стати доступною для злочинців. Дані, отримані з таких пристроїв, можуть надавати найбільш повний і детальний портрет користувача.[1]

Таким чином, Інтернет речей є технологією, що швидко розвивається, Має здатність фундаментально змінити світ у найближчому майбутньому. З розвитком в Україні 4G мережі, кількість продуктів IoT буде збільшуватися. Потенціал для збільшення цього поля справді вражаючий, але завжди є позитивні та негативні наслідкі.[2. с. 6]

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Дейв Еванс (Dave Evans) Інтернет речей: як зміниться все наша життя на черговому етапі розвитку мережі http://www.cisco.com/web/RU/news/releases/txt/2011/062711d.html

2. Леонід Черняк. Платформа Інтернету речей. Відкриті системи. СУБД, №7, 2012.

3. Інтернет речей (Матеріал з Вікіпедії) – Режим доступу: URL-адреса: wikipedia.org/wiki

Інформаційні технології в освіті та практиці : матеріали Всеукраїнської науковопрактичної конференції (Львів, 17 грудня 2021) / упорядник: Т. В. Магеровська. Львів : ЛьвДУВС, 2021. 97 с.

ГРАЧОВА Олександра
студентка ФСП, КПІ імені Ігоря Сікорського
Науковий керівник:
ШУМАК Ігор
к.ю.н, доцент, КПІ імені Ігоря Сікорського

ПРАВО ОСОБИ НА ПРИВАТНІСТЬ ДАНИХ В МЕРЕЖІ ІНТЕРНЕТ

В умовах постійної глобалізації та розвитку інформаційних технологій, кожна особа має вільний доступ до Інтернету. Незважаючи на наявність великої кількості переваг у технологічному прогресі, який проявляється через здатність людини миттєво знаходити цікаву їй інформацію, формування

інформаційного середовища спричиняє й загрози для втручання у приватне життя індивіда без його відома.

Таким чином, у сьогоденні, актуальним є висвітлення ризиків щодо порушення меж приватності в інформаційному суспільстві, зокрема в мережі Інтернет. Важливим є вироблення етапів контролю за рухом персональних даних в Інтернеті на нормативному та інституційному рівнях.

Мета даної роботи полягає у аналізі особливостей права особи на приватність в мережі Інтернет.

Загалом, поява інформаційних технологій запровадила зміни щодо питання захисту приватності. Відповідно, онлайн формат надав можливість відстежити інформаційну активність користувачів. Крім того, доступність даних, розміщених в Інтернеті для практично необмеженого кола осіб, робить їх надзвичайно вразливими, ставлячи під сумнів існування мережевої приватності як такої [1,с.55].

Такі дії обумовили дослідження щодо основних ризиків, які може отримати особа в мережі Інтернету. Однією із найвагомішою загрозою є аспекти збирання та використання персоналізованої інформації користувачів Інтернет за допомогою cookie-файлів. Адже застосування таких записів здійснює відстежування персональної інформацію (вік особи, її стать, країну походження, місце перебування, назва

пристрою з якого здійснюється пошук),що в деяких випадках дає змогу до детальної ідентифікації особи. Основною ціллю застосування cookie є аутентифікація, збір, збереження персональної інформації для формування відповідної характеристики споживача і надалі використання в своїх інтересах певної реклами. Наприклад, зауважимо, що відома компанія Google з метою формування рекламних акцій встановлює не лише закономірність дій особи в Інтернеті, наприклад пошук, покупки в Інтернеті, а відслідковує та має доступ до інформації в електронних листах, які знаходяться на платформі Gmail.

Зазначимо, що Google офіційно визнає про вчинення ним таких діянь і на сайті наявне роз’яснення щодо можливості здійснення[2]. Представники корпорації зазначають, що вищезгадана процедура є законною, адже безпосереднє втручання у життя особи не відбувається. Проте вважаємо ,що така технологія порушує конфіденційність в мережі Інтернет ,оскільки, здійснюється доступ до повідомлень. Тому, таке діяння Google є втручанням у приватне життя.

Зауважимо, що сприяння безпечного доступу особи до мережі Інтернет є важливою охороною функцією кожної демократичної країни. Так, у 2016 році було запроваджено Рекомендацію Рекомендації CM / Rec (2016) 5 (1) Комітету Міністрів держав-членів

щодо Інтернет-свободи (надалі – Рекомендація) [3]. Відповідно до Рекомендації на держави- члени Ради Європи покладаються позитивні, так і негативні зобов'язання щодо захисту права особи на приватність. Норми вищесказаного юридичного акту зазначають, що будь-яке втручання держави в здійснення прав людини і основних свобод в Інтернеті має відповідати вимогам Конвенції. Зокрема, країна-учасниця має своєчасно і належним чином надавати громадськості інформацію про обмеження, які безпосередньо стосуються можливостей поширення конфіденційної інформації, з урахуванням відповідної правової бази, яка має безпосереднє до цього відношення. Закони мають гарантувати, що всі особисті дані є захищеними відповідно до статті 8 Конвенції [3].

Держава обов'язково має здійснювати контроль за використанням персональних даних у мережі Інтернет. Практика Європейського Суду з прав людини зазначає, важливим є обов'язок володільця та розпорядника не допускати розголошення персональних даних, які стали йому відомі у зв'язку з виконанням професійних чи службових або трудових обов'язків. Зауважимо, що втручання держави право на приватність в Інтернеті вимагає дотриманню вимог законності, легітимності і пропорційності відповідно до статті 8 Конвенції, у вигляді використання так званого

забезпечення такого втручання в обмеження прав, яке було б виправданим у конкретних умовах. Зокрема, на міжнародному рівні зберігається певна свобода розсуду щодо виявлення балансу між громадськими та приватними інтересами в контексті захисту права на приватність в мережі Інтернет у сьогоденні[3].

Отже, враховуючи вищенаведене, можемо зауважити, що механізм захисту права користувача на приватність в мережі Інтернет є найбільш важливим під час постійної модернізації. Адже особа має почувати себе захищеною у вільному пошуку інформації, листуванні. Вважаємо, що на міжнародному рівні мають бути запроваджені нормативно-правові акти, що належним чином дають роз'яснення щодо неможливості втручання у особисте життя індивіда в онлайн секторі та у разі його порушення аспекти подання скарги до відповідного органу. Адже забезпечення конфіденційності особи є основоположним її правом.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1.Explanatory Memorandum – K. Recommendation CM/Rec(2014)6 of the Committee of Ministers to member States on a guide to human rights for Internet users. Інжиніринг. 2015. 56-58.

2.Політика конфіденційності Google. Конфіденційність умови. Google: офіц.веб-сайт:

URL:https://policies.google.com/privacy/archive/20200828?hl=uk(дата звернення:27.10.2022)
3.Recommendation CM/Rec(2016)5 of the Committee of Ministers to member States on Internet freedom.Council of European Portal: офіц. веб-сайт URL: https://www.coe.int/en/web/freedom-expression/committee-of-ministers-adopted-texts/-/asset_publisher/aDXmrol0vvsU/content/recommendation-cm-rec-2016-5-of-the-committee-of-ministers-to-member-states-on-internet-freedom?_101_INSTANCE_aDXmrol0vvsU_viewMode=view/. (дата звернення:27.10.2022)

ДЕМЧЕНКО Аліса
студентка 1 року магістратури
Інституту права Київського національного
університету ім. Т.Г. Шевченка

ВИКОРИСТАННЯ КРИПТОВАЛЮТИ У ПРОТИЗАКОННИХ ЦІЛЯХ

За останнє десятиріччя криптовалюти неабияк вплинули на суспільство та стали унікальною та невід’ємною платіжною системою сучасного світу. Із стрімким обертом популярності віртуальні валюти та

цифрові методи оплати все частіше використовуються злочинцями у протизаконних цілях. Наразі, неабияку частку від кримінальних злочинів становлять саме протизаконні дії, пов’язані із віртуальними активами, із тим становлячись все більш актуальною і складнішою проблемою для правоохоронних органів та національних регуляторів у всьому світі. На жаль, швидкий розвиток та поширення технологічних змін, таких як блокчейн, який слугує основою біткоїна, продовжує випереджати здатність законодавства негайно реагувати та створювати відповідні нормативно-правову та регулюторну бази. Ця стаття має на меті дослідити проблему існуючих злочинів, у яких задіяні криптовалюта.

Уже зараз можна побачити конкретні випадки і ризики скоєння різних правопорушень із задіянням криптоактивів. У злочинних цілях криптовалюта також використовується в реальному світі або в Даркнеті[1] для торгівлі, наприклад, наркотиками, нелегальною порнографією, торгівлі зброєю та іншою незаконною продукцією (в Україні вже були випадки, коли у справах про викрадення злочинці вимагали викупи у вигляді

1**"темний інтернет" (з англ. Darknet):** повністю анонімна, нерегульована і нікому не підконтрольна частина інтернету. Наразі є найпопулярнішою частиною всевітньої павутини для продажу заборонених товарів (насамперед персональних даних, зброї, наркотиків), дитячої порнографії, та реалізації ріних кримінальних послуг тощо.

віртуальних валют [1]). Стрімкий розвиток криптовалют, анонімність та обмеженість відстеження операцій роблять їх привабливими для злочинців або злочинних організацій. Так, за оцінками одного з досліджень, незаконна діяльність, пов'язана з біткоїном, складає близько 76 мільярдів доларів США на рік (або 46% загальної кількості транзакцій з криптовалютою [2]).

Спершу, важливо навести визначення поняттю криптовалюта та блокчейн. Отже, криптовалюта – це вид цифрової валюти, яка використовує криптографію для захисту транзакцій, які записуються в цифровому вигляді в розподіленому реєстрі, який називається блокчейн. Одиниці криптовалюти зазвичай називаються коїнами (від англ. Coin – «монета»). Криптовалютна система працює за допомогою блокчейну – технології зберігання та обміну закодованими даним. По суті, це реєстр обмінів коїнами всередині мережі блокчейну, без залучення центрального контролюючого органу. Блокчейн можна приватизувати, обмеживши доступ до мережі кільком конкретним суб’єктам. За умови реєстрації та дотримання правил, визначених віртуальною спільнотою, його користувачі можуть здійснювати торгівлю коїнами без необхідності розкривати свою особу. Так ми доходимо до висновку, що не всі користувачі криптовалюти та блокчейну

можуть бути ідентифіковані. Попри те, що концепція публічного блокчейну прагне забезпечити прозорість транзакцій всередині системи, можливість встановити особу-користувача досить обмежена.

Криптовалюта, як і інші нематеріальні активи, характеризується вартістю активів, тому із нею можуть бути пов’язані такі злочини у сфері кримінального законодавства, як:

(1) шахрайство (ст. 190 КК України),

(2) крадіжка (ст. 185 КК України),

(3) легалізація (відмивання) доходів, отриманих злочинним шляхом (ст. 209 КК України),

(4) фінансування тероризму (ст. 285-5 прим.1 КК України)

Іноді підозрілі транзакції здійснюються з криптовалютних сервісних платформ, які не зареєстровані у країнах, де проводяться транзакції. Також, непоодинокими є і випадки, коли злочинці розраховувалися на платформі Даркнету криптовалютою за покупку наркотиків, зброї, замовлення вбивств або скоєння інших злочинів (нагальність проблеми висвітлює і рішення Інтерполу створити окрему робочу групу з питань Даркнету та криптовалюти для дослідження злочинів у цій сфері та розробки можливостей їх запобігання [7]).

(5) сприяння учасникам злочинних організацій та укриття їх злочинної діяльності (ст. 256 КК України). Яскравим прикладом може бути закриття ФБР у жовтні 2013 року «Шовкового шляху» – чорного ринку Даркнету та подальший арешт його засновника Росса Ульбріхта. На цьому сайті транзакції частково оплачувалися біткоїнами, ФБР було вилучено, а згодом знищено 26 000 біткоїнів (станом на тоді, близько 30млн дол.США) [3].

(6) Окрім цього, одним із найпопулярніших злочинів, пов’язаних із криптовалютами, є також незаконний «майнінг» або «криптоджекінг» – це використання потужностей комп'ютерів або смартфонів третіх осіб, заражених шкідливим програмним забезпеченням (так званих бот-мереж), тобто несанкціоноване використання гаджетів інших людей для отримання криптовалюти [4]. Так, злочинними особами без відома власника на ноутбук або інший гаджет останнього запускаються спеціальні коди для здійснення майнінгу (виробництва) криптовалют через браузери. У лютому 2018 року ФСБ заарештувала науковців з російського Федерального ядерного центру в Сарові, коли вони збиралися підключити комп'ютерну систему центру, яка є однією з найпотужніших у світі, до Інтернету для проведення операцій з майнінгу біткоїнів [6].

Наразі відповідно до українського законодавства криптоджекінг, у залежності від обставин правопорушення, можна кваліфікувати як:

- Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж (ст. 361 КК України) або;
- Створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут (ст. 361-1 КК України) або;
- 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. 361-2 КК України).

Висновок

Наразі, серед існуючих об'єктів правового регулювання неможливо знайти аналогів криптовалюті. Вона є самобутньою та унікальною, і притаманні їй властивості мають бути покладені в основу її правового статусу та правового регулювання відносин з її

використанням. На жаль, криптовалютні технології є одним з найпоширеніших і найефективніших способів здійснення онлайн-злочинів. Особливості функціонування системи криптовалюти є серйозною перешкодою для кримінального переслідування, а її особливості (такі як анонімність, складність переслідування і встановлення суб’єктів операцій та волативність) тільки створює сприятливі умови для використання криптовалют злочинцями, завдаючи незворотної шкоди потерпілим сторонам. Держави, які зрозуміли невідворотність існування криптовалюти та усвідомили ірраціональність її законодавчої заборони, повинні також визнати, що новий об'єкт правового регулювання певною мірою вплине на всі існуючі суспільні відносини. Саме тому наразі існує нагальна потреба визначення правової природи та правового статусу криптовалюти, а також розробки нормативно-правової бази її використання (правових норм щодо контролю за її обігом, оподаткування, ліцензування діяльності учасників відносин, можливих кримінальних правопорушень та відповідальності за них тощо).

На мою думку, також нагальним є питання розробки міжнародного регіонального або універсального документу, який був би контрено присвячений регулюванню криптовалют та їх суб’єктів. Це дозволило б уніфікувати регулювання у цьому

секторі щодо валютних активів і спростило процес контролю за їх використанням у різних державах та на міжнародному рівні.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Стаття Національної поліції України «Поліція впроваджує нові методи розслідування викрадень людей та їх повернення за криптовалюту» [Електронний ресурс]: https://mvs.gov.ua/uk/press-center/news/Policiya_vprovadzhu_novi_metodi_rozsliduvannya_vikraden_lyudey_ta_ih_povernennya_za_kriptovalyutu_FOTO_11863.

2. Стаття авторів Сеан Фолі, Джонатана Карлсена та Таліса Путнінса (ориг.) «Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies?») [Електронний ресурс]: https://deliverypdf.ssrn.com/delivery.php?

3. Стаття «Шовковий шлях: жорстокий удар по війні з наркотиками» (ориг. «SILK ROAD: A VICIOUS BLOW TO THE WAR ON DRUGS») [Електронний ресурс]:https://bxroberts.org/2012/01/silk-road-a-vicious-blow-to-the-war-on-drugs/.

4. Стаття «Як не стати жертвою прихованого майнінгу. Визначення криптоджекінгу» [Електронний ресурс]: http://bitcoin-crypto-portal.com/yak-ne-stati-zhertvoyu-prixovanogo-majningu/.

5. Стаття BBC (ориг.) «Russian nuclear scientists arrested for 'Bitcoin mining plot’») [Електронний ресурс]: https://www.bbc.com/news/world-europe-43003740.
6. Стаття «Інтерпол провів першу робочу групу з питань DarkNet та криптовалют» [Електронний ресурс]: https://www.interpol.int/fr/Actualites-et-evenements/Actualites/2018/INTERPOL-holds-first-DarkNet-and-Cryptocurrencies-Working-Group.
8. Кримінальний кодекс України, Закон від 05.04.2001 № 2341-III, ред. від 19.08.2022.
9. Закон України «Про віртуальні активи» від 17.02.2022 № 2074-IX.

КАРЕЛІ Софія
студентка ФСП, КПІ ім. Ігоря Сікорського

ЮРИДИЧНИЙ АСПЕКТ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ПІД ЧАС ВПРОВАДЖЕННЯ ІНТЕРНЕТУ РЕЧЕЙ

Тема Інтернет-речей вже давно перестала бути новою, але попри це вона не перестає бути устарілою, а навпаки продовжує розвиватися з великою швидкістю. Це в свою чергу спричиняє актуалізацію теми законодавчого забезпечення розвитку Інтернет-речей

зокрема забезпечення приватності. Всі впроваджені нововведення додають серйозних проблем, що пов'язані з інформаційною безпекою. Інтернет-речі – це мережа фізичних об’єктів, які мають вбудовані технології, яка включає в себе можливість здійснювати взаємодію з зовнішнім середовищем, передаючи відомості про свій стан і приймати дані ззовні. Сучасний Інтернет складається з тисяч корпоративних, наукових, урядових та домашніх комп’ютерних мереж. Мережі різних архітектур і топологій з’єднуються через протокол IP.

Кожному учаснику Мережі (або групі учасників) присвоюється свій унікальний ідентифікатор IP-адреса. Безпека IoT стала одним з найважливіших аспектів нових технологій. Експерти вважають, що «в даний час безпечної екосистеми Інтернет-речей не існує». Згідно даним з 2020 року вже понад 50 мільярдів пристроїв підключені до Інтернету. Відповідно з таким темпом зростання критично постає питання безпеки пристроїв у разі відсутності процесів, які дають змогу забезпечувати цілісність і шифрування даних. Вся інформація, що зберігається IoT-пристроями, користується великим попитом, оскільки відображає повну картину щоденних дій і звичок користувачів. І наявність таких контентних баз корисна для різних компаній, які можуть спрямовувати свої ресурси на виробництво товарів і послуг, орієнтованих на звички

та переваги мас. Що допоможе мінімізувати проблеми, так це шифрування та спеціальні системи захисту для завантаження та зберігання даних у хмарі.

Право на приватність встановлене Загальною декларацією прав людини, там визначено, що «ніхто не може зазнавати безпідставного втручання у його особисте і сімейне життя, безпідставного посягання на недоторканність його житла, тайну його кореспонденції або на його честь і репутацію. Кожна людина має право на захист закону від такого втручання або таких посягань» [1].

Конфіденційність є основним правом людини, яке лежить в основі свободи асоціацій, думки та вираження поглядів, а також свободи від дискримінації. Різні країни пропонують різні погляди на конфіденційність. Загалом конфіденційність включає право: бути вільним від втручання; вільно спілкуватися з ким хочеш; мати можливість контролювати, хто може бачити або використовувати інформацію про вас [2].

Можна виділити наступні законодавчі принципи впровадження Інтернет-речей, які дозволять уникнути проблем і бар'єрів, пов'язаних з забезпеченням приватності [3]:

принцип законності – дані, які підлягають збору та обробці мають бути чітко визначеними, потрібно чітко визначати осіб, відповідальних за збереження

цілісності, доступності та конфіденційності даних. Як правило, дані, допустимі для збору та обробки є генеральними, тобто в різних державах їх перелік відповідає стандарту, але можуть виникнути і ситуації, коли регулювання доступності в різних країнах відбувається по-різному, що може ускладнити та спричинити виникнення проблем, пов’язаних з забезпеченням приватності. Також важливим для реалізації технологій Інтернету-речей є законодавче закріплення процедур отримання згоди суб’єкта на обробку даних;

- принцип цілеспрямованості – персональні дані повинні оброблятися для певних цілей, які є визначеними законодавчо;
- принцип відповідності – обробка персональних даних має бути актуальною, обмеженою та відповідати зазначеним цілям;
- принцип збереженості даних – дані мають зберігатися впродовж визначеного терміну, який є адекватним відповідно до встановленої мети збору персональних даних;
- принцип актуальності – персональні дані повинні бути актуальними та точними, у разі необхідності варто проводити процедуру актуалізації даних, яка також повинна відповідати встановленим вимогам законодавства;

- принцип конфіденційності – персональні дані повинні оброблятися з дотриманням вимог конфіденційності;
- принцип забезпечення безпеки – повинні бути реалізовані запобіжні заходи та процедури для захисту безпека персональних даних, у тому числі від несанкціонованих або випадкового отримання доступу, пошкодження, втрата чи інші ризики, пов’язані з даними обробки.
- принцип прозорості – обробка персональних даних повинна здійснюватися прозоро. Це має включати, наприклад, надання інформації про обробку персональних даних, а також інформацію про те, як це отримати доступ, перевірку, тощо;
- принцип безпечної передачі – оскільки Інтернет-речей передбачає передачу даних, вона має здійснюватися без випадкового отримання доступу третіх осіб, запобігання безцільової передачі даних.

Отже як ми знаємо інформаційною безпекою є стан захищеності систем передачі, обробки та зберігання даних, при якому забезпечується конфіденційність, доступність і цілісність даних. Інформаційна безпека включає комплекс заходів, які мають забезпечити захист даних від несанкціонованого доступу, використання, розголошення, зміни чи знищення.

Забезпечення безпеки, надійності та стабільності Інтернет-додатків і послуг має вирішальне значення для довіри та використання Інтернету. Зі збільшенням кількості пристроїв, підключених до Інтернету, відповідно з’являються нові потенційні слабкі місця, які через свою неналежну захищеність можуть бути точками доступу для кібератак, що дає змогу зловмисникам перепрограмувати пристрій або викликати його несправність. Недосконало розроблені пристрої можуть поставити дані користувачів під загрозу крадіжки через неналежний захист потоків даних. В свою чергу збір та обробка IoT-даних про особу створює ризик вторгнення в конфіденційність. З кожним днем цей ризик посилюється масштабами та більшою видимістю персональних даних, зібраних в Інтернеті речей. Пристрої IoT можуть збирати дані про людей із великою точністю, що створює можливість призвести до ситуацій, які загрожують здоров’ю, добробуту, фінансам чи репутації людини. Тобто йде мова про порушення приватності людини.

Обмін повідомленнями за допомогою Інтернету принципово відрізняється від передачі інформації за допомогою звичайних засобів зв'язку. Електронна передача інформації рухаючись мережею, проходить велику кількість операторів, які в свою чергу можуть

дізнатися більше ніж просто зміст даної переданої інформації.

Для вирішення питання захисту приватності користувачів Інтернет речей перш за все пропонується створити міжнародний наглядовий механізм для моніторингу приватності користувачів Інтернету в рамках існуючої системи регулювання Інтернету.

Також важливу роль у забезпеченні приватності в Інтернеті повинні відігравати міжнародні інструменти. Основні принципи захисту права на приватність, передбачені чинними міжнародно-правовими актами, потребують адаптації для використання в Інтернеті. Для цього вчені пропонують розширити коло прав людини. Серед «нових» прав можна назвати:

1. право не бути ідентифікованим (внесеним до списків);
2. право на ефективне шифрування персональної інформації;
3. право на справедливе поводження з людиною у сфері використання системи шифрування «відкритим ключем»;
4. право на розкриття інформації особі, яка може бути використана для створення її профілю користувача.

Тобто, забезпечення безпеки передачі даних потребує застосування комплексних заходів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Загальна декларація прав людини. Міжнародні договори України. Неофіційний переклад. URL: https://zakon.rada.gov.ua/laws/show/995_015#Text (дата звернення: 31.10.2022).
2. What is privacy? *OAIC*. URL: https://www.oaic.gov.au/privacy/your-privacy-rights/what-is-privacy (дата звернення: 31.10.2022).
3. Personal data protection and privacy principles. *The UN System Chief Executives Board for Coordination (CEB).* URL:https://unsceb.org/sites/default/files/imported_files/UN-Principles-on-Personal-Data-Protection-Privacy-2018_0.pdf (дата звернення: 31.10.2022).

КІСІЛЬ Анастасія
студентка ФСП, КПІ ім. Ігоря Сікорського

ОСОБЛИВОСТІ ЗАХИСТУ ПРАВА НА ПРАЙВЕСІ В УМОВАХ ВІЙНИ

Впровадження на території України воєнного стану значно вплинуло на розвиток суспільних відносин, а також захист прав громадян. Звісно, обмеження доткнулися й до сфери захисту персональних даних

українців. Саме тому, можна стверджувати, що право на прайвесі в умовах війни зазнало деяких змін, в тому числі законодавчих. Задля встановлення їх ефективності та доцільності варто розглянути нормативні положення, які стосуються процесу обробки персональних даних в Україні.

Таким чином, органи державної влади було забезпечено правом розміщувати інформацію, публічні реєстри, а також їх резервні копії на хмарних середовищах. Окрім цього, вони отримали змогу зберігати та обробляти дані в центрах обробки даних, що географічно знаходяться за межами України. Важливим кроком для захисту цілісності даних було обмеження, а також повне закриття доступу до більшості державних реєстрів (наприклад Єдиного реєстру судових рішень). Також зміни були внесені до діяльності банків, оскільки в їх базах даних вони також міститься конфіденційна інформація про громадян. Відповідно, у постанові Національного банку України «Про використання банками хмарних послуг в умовах воєнного стану в Україні» від 08.03.2022 року було доручено банкам обов’язок щодо використання хмарних ресурсів, що знаходяться за межами України, в тому числі з метою обробки персональних даних клієнтів [1].

Окрім цього, увагу необхідно звернути на законодавчі зміни, пов’язані з геномною інформацією про особу. Отож, 14 квітня 2022 року було прийнято за основу проєкт Закону України «Про державну реєстрацію геномної інформації людини» [2]. Важливо відзначити, що він був розробленим ще у жовтні 2022 року, тому на мою думку, його прийняття обумовлене виникненням гострої необхідності ідентифікації людей за рахунок молекулярно-генетичної експертизи. На жаль, з початком воєнний дій кількість жертв як серед військових, так і цивільних громадян сягала високих цифр, при чому велику частину з них було вкрай важко опізнати. Такий крок законодавця має пришвидшити цей процес, а також зробити його більш достовірним. Таким чином, положення наведеного вище закону стосуються деталізації правил обробки, а також обов’язкової державної реєстрації геномної інформації для ідентифікації визначеної категорії осіб. До останніх належать ті, які вчинили кримінальне правопорушення; що зникли безвісти; невпізнаних трупів людей, їхніх останків та частин тіла людини.

Окрім цього, законодавець визначає порядок відбору біологічного матеріалу у військовослужбовців, який є також охороняється правом на прайвесі. Таким чином, отримана геномна інформація буде зберігатися в окремій базі даних. При чому, обов’язок здійснювати

функціонування та адміністрування останньої покладається на Міністерство внутрішніх справ.

Не зважаючи на переваги такого законопроєкту, слід зауважити, що він має суттєві недоліки, особливо в контексті захисту права на прайвесі. Таким чином, запропоновані положення потребують удосконалення, а саме встановлення порядку псевдонімізації інформації, її захисту від несанкціонованої передачі третім особам. Окрім цього, деякі норми в наведеному нормативно-правовому актів стосуються регулювання частини відносин відповідно до кримінально-процесуальних норм. При цьому, законодавець не передбачає внесення відповідних змін до Кримінального процесуального кодексу (далі- КПК), що в результаті може спровокувати утворення колізій у національному законодавстві.

Що стосується правил огляду закріплених в ст. 237 КПК, то вони також зазнали змін [3]. Таким чином 15 березня 2022 року було регламентовано можливість проведення огляду комп’ютерних даних. Суб’єктами, що мають право на його реалізацію є прокурор або слідчий, які зобов’язані зафіксувати огляд у будь-який зручний спосіб. При цьому, неврегульованим залишився аспект, який стосується алгоритму фіксування персональних даних, а також приватного спілкування в ході проведення огляду комп’ютерних даних. Ці засади є надзвичайно важливими, оскільки

стосуються приватного життя особи і в результаті їх порушення мають бути захищеними і відновленими. На мою думку, вирішення цього питання можливе шляхом впровадження законодавчих змін. Отже, важливо закріпити положення про те, що огляд комп'ютерних даних має проводитися на підставі ухвали слідчого судді. Така позиція обумовлена тим, що усі слідчі дії, які передбачають втручання в приватне спілкування і життя людини, мають реалізовуватися лише за наявності ухвали слідчого судді.

При цьому, законодавцем було впроваджені зміни, які дозволили здійснювати обшук без попередньої ухвали суду. Таким чином, прокурори та слідчі отримали право шукати, виявляти та копіювати дані, що містяться на електронних пристроях, навіть за умови відсутності ухвали суду. Дана можливість обмежена випадками, в яких її можна реалізовувати. Таким чином, перелічені вище суб'єкти можуть здійснювати обшук даних, що містяться на електронних пристроях за умови, якщо у них є достатні підстави для того, щоб вважати, що ця інформація є важливою для кримінального провадження. При цьому, описані права можуть бути реалізованими лише на місці обшуку особи.

На мою думку, такий обсяг прав гарантують прокурору або слідчому надмірні повноваження до

доступу інформації, що є приватною та охоплюється правом на прайвесі. Це виражається у тому, що законодавець не конкретизує межі дискреції, а відтак не визначає вичерпний перелік підстав для доступу названих вище осіб до даних на пристроях, які не визначені в ухвалі суду. Окрім цього, на належному рівні не визначено який обсяг інформації може бути скопійованим, за умови доступу до нього у прокурора або слідчого. Безумовно, що об’єктивно визначити дані, які дійсно будуть необхідними для кримінального провадження є неможливо. Саме через це можливо стверджувати, що особа цілком можливо може зазнати порушення її права на прайвесі, а саме стосовно збереження конфіденційності інформації про себе чи приватного спілкування [4, с. 193].

Виходячи з сказаного вище можна зауважити, що в сучасних суспільних умовах право на прайвесі зазнає особливих змін, в тому числі з боку державних органів. Таким чином, втручання держави в приватне життя особи значно підвищилося, з цілей національної безпеки та захисту держави. Проаналізовані зміни у законодавстві демонструють, що вирішення питань, які різко набули актуальності на початку війни, було здійснено з ігноруванням таких принципів, як системності, логічності, виваженості. Саме через це, в роботі було запропоновано деякі зміни, які допоможуть

уникнути утворенню колізій у національному законодавстві, а також вільного доступу третіх осіб, в тому числі правоохоронців, до конфіденційної інформації про особу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Про використання банками хмарних послуг в умовах воєнного стану в Україні : Постанова Національного банку України від 08.03.2022 р. № 42. URL: https://zakon.rada.gov.ua/laws/show/v0042500-22/card4#Future (дата звернення: 30.10.2022).
2. Про прийняття за основу проекту Закону України про державну реєстрацію геномної інформації людини : Постанова Верховної Ради України від 14.04.2022 р. № 2202-IX. URL: https://zakon.rada.gov.ua/laws/show/2202-20#Text (дата звернення: 30.10.2022).
3. Кримінальний процесуальний кодекс : Закон України від 13.04.2012 р. № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення: 30.10.2022).
Крижна В., Кушнір І. Щодо обмежень прав людини та правових підстав для обробки персональних даних державними органами в умовах воєнного стану. *Регулювання приватно-правових відносин в умовах воєнного стану в Україні*: матеріали міжвуз. наук.-практ. конф., м. Київ, 29 вер. 2022 р. Київ, 2022. С. 191-193.

КРАСНОПЬОР Дар’я
Курсант Луганського державного університету
внутрішніх справ ім. Е.О. Дідоренка

ПРОБЛЕМИ ВДОСКОНАЛЕННЯ ЗАКОНОДАВСТВА З ПИТАНЬ ІНФОРМАТИЗАЦІЇ, ТЕЛЕКОМУНІКАЦІЙ, ВИКОРИСТАННЯ РАДІОЧАСТОТНОГО РЕСУРСУ.

На сучасному етапі розвитку суспільства відбувається черговий вибух технологічної і соціальної революції – становлення інформаційного суспільства. Сьогодні у зв’язку із процесом інформатизації суспільства інформація має важливе значення в житті кожної людини. Про виникнення інформаційних правовідносин у всіх сферах життя і діяльності суспільства, а також держави, свідчать різноманітні дії, пов’язані з одержанням, використанням, поширенням та зберіганням інформації. В результаті майже кожна особа є залежною від інформації. Результатом цього є виникнення інформаційних прав та обов’язків. Зміни, що відбуваються в суспільстві, в тому числі щодо процесів, пов’язаних з реалізацією права на

інформацію, мають значний вплив і в сфері законотворчості.

Тематика інформаційного суспільства, розвитку світового ринку телекомунікацій, Інтернету не сходить зі сторінок провідних ділових вітчизняних і зарубіжних журналів. Колосальні обсяги інформації, присвячені цій тематиці, доступні зараз й Інтернету. Особливо це стосується висвітлення діяльності міжнародних і національних організацій з розробки і реалізації стратегій інформаційного розвитку.

Сучасна ситуація, що склалася у світі, характеризується такими рисами: - Становлення інформаційного суспільства в різних країнах є передумовою для еволюційного переходу до наступної стадії розвитку людства, технологічною основою якої є індустрія створення, обробки і передачі інформації.

- Інформаційна взаємодія держави, суспільства і особистості найбільш оптимальна при використанні інформаційних і телекомунікаційних технологій з метою підвищення ефективності діяльності державного механізму, створення інформаційно відкритого суспільства, розвитку інститутів демократії [5].

Інформаційне суспільство – це суспільство, в якому діяльність людей здійснюється на основі використання послуг, що надаються за допомогою інформаційних технологій та технологій зв’язку.

Інформаційне суспільство, що є результатом впливу і проникнення інформації у всі сфери людського життя, має певні основи свого існування: економічні; правові; технологічні.

Правовими основами інформаційного суспільства є закони і нормативні акти, що регламентують права людини на доступ до інформаційних ресурсів, технологій, телекомунікацій, захист інтелектуальної власності, недоторканість особистого життя, свободу слова, інформаційну безпеку.

Серед позитивних здобутків сучасної інформаційної цивілізації можна визначити такі:

- зростання можливості швидко здійснювати інформаційні зв’язки на великих відстанях, у тому числі між континентами;
- зростання можливості швидко, у великому обсязі сприймати та обробляти, зберігати інформацію на компактних (малогабаритних) технічних засобах;
- об’єднання різних технологій комунікації: теле-, радіо- та обчислювальної техніки.

Водночас ці позитивні соціальні явища супроводжуються негативними, які активно використовуються в сучасних умовах воєнного стану, створюючи загрозу інформаційному суверенітету, інформаційній безпеці окремої держави, групи держав, регіонів, а також безпечному існуванню окремих людей:

- зростання можливості швидкого перехоплення, витоку, перекручення, знищення інформації;
- використання технічних засобів і технологій інформації в антисоціальній діяльності: воєнній; політичній; економічній [6].

Стрімкий розвиток високих технологій, інформатизації та телекомунікації, поряд із безсумнівними перевагами розширення можливостей для міжнародного співробітництва, створюють водночас передумови для виникнення принципово нової, інформаційної, конфронтації на міжнародній арені. Ця проблема висувалася на Саміті «великої вісімки» на Окінаві, де поряд з іншими документами була прийнята 22 липня 2000 р.

Відповідно до Окінавської Хартії, ІК технології є одним з найбільш важливих факторів, котрі впливають на формування суспільства XXI сторіччя. Їх революційний вплив стосується способу життя людей, їх освіти й роботи, а також взаємодії уряду та громадянського суспільства. ІТ швидко стають життєво важливим стимулом розвитку світової економіки.

У 2014 році Україна підписала Угоду про асоціацію з Європейським Союзом, Євроатомом і їхніми державами-членами. Пунктом 5 Угоди були визначені вимоги щодо телекомунікаційних послуг. У зв’язку з цим українське законодавство мало бути

приведено у відповідність до актуального законодавства ЄС, зокрема у сфері цифрової економіки [7].

Однак на цьому шляху виникла велика кількість проблем:

- відсутність стандартів та технічних регламентів, гармонізованих зі стандартами ЄС;
- недосконалість законодавства у сфері цифрового підпису;
- недосконалість законодавчої бази з інформатизації та телекомунікацій [6].

На сьогодні в Україні створені та діють розгалужена система державних органів з питань розвитку інформаційного суспільства. Це Комітети Верховної Ради України, відповідальні за інформатизацію та е-урядування: Комітет ВРУ з питань транспорту та зв'язку; Комітет з питань інформатизації та інформаційних технологій; Комітет з питань свободи слова та інформатизації; Комітет ВРУ з питань науки та освіти; Комітет ВРУ з питань національної безпеки та оборони; Консультаційна рада з питань інформатизації при ВРУ [6].

Останніми роками прийнято ряд Законів у сфері інформатизації та інформаційних технологій.

Закон України «Про основні засади забезпечення кібербезпеки України», що визначає правові та організаційні основи забезпечення захисту життєво

важливих інтересів громадян, держави, національних інтересів у кіберпросторі, основи державної політики у сфері кібербезпеки, повноваження державних органів та засади координації їхньої діяльності із забезпечення кібербезпеки [3].

Закон України «Про Національну комісію, що здійснює державне регулювання у сферах електронних комунікацій, радіочастотного спектра та надання послуг поштового зв'язку». Визначає правовий статус Національної комісії, її завдання, функції, повноваження та порядок їх здійснення [2].

Закон України «Про електронні комунікації». Визначає організаційні та правові основи державної політики у сферах електронних комунікацій та радіо частотного спектра, права, обов’язки та відповідальність фізичних і юридичних осіб, які користуються електронними комунікаційними послугами [1].

Основними напрямами вдосконалення законодавства мають стати:

1. Проведення інвентаризації існуючих механізмів державного управління сферою, забезпечення їх взаємоузгодженості та адаптація до відповідних європейських механізмів.
2. Розробка та прийняття законопроєктів щодо електронних адміністративних послуг та

інформаційних ресурсів; Інформаційного кодексу України; засад державного регулювання у сфері інформатизації; внесення змін до Законів України "Про радіочастотний ресурс України“ та "Про телекомунікації"

3. Здійснення заходів щодо оптимізації структури, завдань та функцій органів влади, що здійснюють управління та регулювання сферою з метою усунення дублювання, підвищення рівня їх координованості, ефективності, відкритості та прозорості, якості адміністративних надання послуг.

4. Вдосконалення системи моніторингу та аналізу розвитку сфери [6].

Висновок. Отже, сучасний стан вдосконалення законодавства у сфері інформатизації потребує невідкладного вирішення наступних питань: підвищення рівня об’єктивізації законодавчого забезпечення та обґрунтованості нормативно-правових актів; інвентаризація механізмів державного управління сферою, забезпечення їх узгодженості з європейськими механізмами; лібералізація ринку телекомунікацій; забезпечення гармонізованих умов доступності та ефективності використання радіочастотного ресурсу; унормування державного регулювання в сфері інформатизації; підвищення рівня інформаційної безпеки ІК інфраструктури, насамперед забезпечення

захисту систем управління мережами; впровадження новітніх радіо технологій 3G, 4G; створення умов для розвитку інфраструктури телекомунікаційних мереж та ефективного її використання операторами, провайдерами телекомунікацій; вдосконалення тарифної політики в сфері телекомунікацій; вдосконалення механізмів стимулювання та збереження конкуренції на ринку електронних комунікацій.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Закон України «Про електронні комунікації». від 14.09.2022, https://zakon.rada.gov.ua/laws/show/1089-20#Text

2. Закон України «Про Національну комісію, що здійснює державне регулювання у сферах електронних комунікацій, радіочастотного спектра та надання послуг поштового зв'язку» від 16.12.2021 // Електронний ресурс. – Режим доступу: https://zakon.rada.gov.ua/laws/show/1971-IX#Text

3. Закон України «Про основні засади забезпечення кібербезпеки України». Відомості Верховної Ради, 2017, № 45, ст.403 // Електронний ресурс. – Режим доступу: https://zakon.rada.gov.ua/laws/show/1089-20#Text

4. Закон України «Про радіочастотний ресурс України» від 1 червня 2000 року N 1770 - III. // Електронний ресурс. – Режим доступу: https://www.rrt.ua/govsupport/index/lawsone/lang/uk?id=95

5. Процайло М. Бути чи не бути? Як і коли запрацює закон про електронні комунікації // Електронний ресурс. – Режим

доступу: https://mind.ua/openmind/20217890-buti-chi-ne-buti-yak-i-koli-zapracyue-zakon-pro-elektronni-komunikaciyi
6. Семенченко А.І. Організаційно-правові аспекти розвитку сфери зв'язку та інформатизації // Електронний ресурс. – Режим доступу:
7. Чота Ілона. 10 положень нового Закону «Про електронні комунікації» для споживачів // Електронний ресурс. – Режим доступу: https://nkrzi.gov.ua/ images/ news/11/583/090368fdd6884fd0fff92b0f6c09c56b.pdf

ЛЯЩЕНКО Дар`я
Курсант Луганського державного університету
внутрішніх справ ім. Е.О. Дідоренка

ІНТЕРНЕТ РЕЧЕЙ: ПРОБЛЕМИ ПРАВОВОГО РЕГУЛЮВАННЯ ТА ВПРОВАДЖЕННЯ

На сьогодні технологічне середовище IoT неоднорідне, оскільки використовує різноманітні радіотехнології передачі даних, платформи IoT, ідентифікатори, універсальні ідентифікаційні системи та механізми ідентифікації, переважно застосовуючи нормативно-правові акти технічного характеру. Розгляд проблеми рпавового регулювання та впровадження

Інтернету речей та штучного інтелекту є вкрай актуальною.

Серед проблем, пов'язаних з Інтернетом речей, можна виділити такі, як правовий режим інформації, персональні дані й приватне життя, інформаційна безпека, розроблення понятійного апарату, проблема ідентифікації осіб, відповідальність учасників цих відносин, проблема збору доказів тощо. Деякі з проблем, що виникають у сфері Інтернету речей, зокрема проблема відповідальності за шкоду, заподіяну пристроями, що входять до системи от, уже розглядалися нами раніше.

Одним чи не найважливішим проблемним питанням у сфері Інтернету речей є питання захисту персональних даних. Із метою забезпечення захисту персональних даних у Європейському Союзі було розроблено нові правила оброблення персональних даних і прийнято Загальний регламент із захисту даних (Регламент ЄС 2016/679 від 27 квітня 2016 р. або GDPR - General Data Protection Regulation), який набув чинності в травні 2018 року, після чого компанії, що порушують правила щодо оброблення персональних даних, ризикують бути притягнутими до відповідальності з накладенням штрафів до 20 мільйонів євро, або 4% річного доходу компанії.

Основні принципи оброблення персональних даних за GDPR такі:

1) законність, справедливість і прозорість: персональні дані повинні оброблятися законно, справедливо й прозоро. Будь-яку інформацію про цілі, методи й обсяги опрацювання персональних даних слід висловлювати максимально доступно
й просто;

2) обмеження мети: дані повинні збиратися й використовуватися виключно в тих цілях, які заявлені компанією (онлайн-сервісом):

3) мінімізація даних: не можна збирати особисті дані в більшому обсязі, ніж це необхідно для цілей оброблення: дальших розвідок у цьому напрямі.

Дослідники наголошують на доцільності створення комплексного законодавства у сфері управління ідентифікаційними даними в тому числі IoT та ШІ, яке забезпечить якісне регулювання суспільних відносин у сфері управління ідентифікаційними даними та інформації, що застосовуються для ідентифікації суб’єктів та об’єктів у державних реєстрах, базах даних та інформаційно-комунікаційних системах

Ще одним недоліком розвитку Інтернету речей є вразливість людини до загроз інформаційній безпеці та зростання ризиків, пов’язаних з конфіденційністю. Адже не кожен користувач сервісів IoT володіє

компетентностями протистояти вказаним вище загрозам. Трансформація системи освіти, на наш погляд, повинна здійснюватися таким чином, щоб забезпечити в майбутньому можливість формування діалектично мислячих людей, які, користуючись усіма перевагами IoT, зможуть протистояти загрозам, що пов’язані з його розвитком.

ВИСНОВОК. У підсумку хотілося зазначити, що оскільки Інтернет речей є складним і багатогранним поняттям, правові проблеми, що виникають у цій сфері, є досить різноманітними.

До таких відносять проблеми захисту персональних даних і забезпечення невтручання у приватне життя, проблеми інформаційної безпеки, проблеми ідентифікації осіб, відповідальності учасників цих відносин, проблеми збору доказів тощо.

На вирішення проблеми захисту персональних даних у сфері Інтернету речей спрямовані, 30-крема, норми GDPR шляхом закріплення дружніх для інновацій правил, відповідно до яких гаранти захисту даних у продуктах і послугах, що розробляються, повинні бути забезпечені на найбільш ранніх стадіях розвитку, тобто ще на стадії проектування.

Проблему забезпечення інформаційної безпеки сьогодні пропонують вирішувати шляхом саморегуляції у сфері Інтернету речей і введенням стандартизації й

обов'язкової сертифікації об'єктів. що входять до системи Інтернету речей. Остання позиція видається доцільною, хоча й піддається критиці, оскільки надмірна регуляція може завадити розвитку технологій у сфері loT.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Бортник К.Я., Ольшевський О.В., Пащук В.Ю. Інтернет речей та як він змінить наше життя у майбутньому. Комп’ютерно-інтегровані технології: освіта, наука, вир-во. 2018. № 30/31. С. 14–18
2. Каткова Т.Г. Штучний інтелект в Україні: правові аспекти. Право і суспільство. 2020. № 6. С. 46–55.
3. Харитонов Є.О., Харитонова О.І. До проблеми цивільної правосуб’єктності роботів. Інтернет речей: проблеми правового регулювання та впровадження: матеріали II наук.-практ. конф., м. Київ, 29 листопада 2018 р., Київ, 2018. 168 с.
4. Становлення і розвиток правових основ та системи захисту персональних даних в Україні : монографія / В.Г. Пилипчук та ін. ; за ред.: В.М. Брижка, В.Г. Пилипчука. Київ : Нац. акад. прав. наук України, «АртЕк», 2017. 226 с

МАКСИМЕНКО Каріна
Студентка ФСП, КПІ ім. Ігоря Сікорського

ВИКОРИСТАННЯ СМАРТ КОНТРАКТІВ У ПРИВАТНОПРАВОВИХ ВІДНОСИНАХ: МІЖНАРОДНО-ПРАВОВИЙ АСПЕКТ

Стрімкий розвиток технологій, глобалізація та міжнаціональний характер економічних відносин сприяли появі та поширенню в міжнародному приватному полі смарт контрактів.

Ряд держав вже почали реформувати своє законодавство з метою регулювання нового виду договорів. Регулювання вже наявне в деяких штатах Сполучених Штатів Америки, зокрема в Арізоні та Тенесі. Спробу врегулювати дану сферу здійснили й наші ворожі сусіди - Білоруси. Питання смарт контрактів та їх регулювання класичним договірним правом жваво обговорюється серед науковців Франції, Німеччини, Італії та інших європейських країн. Наведена інформація свідчить про високий рівень зацікавленості світового співтовариства до даної тематики.

Смарт контракт реалізуються у вигляді програмного коду на базі платформи Blockchain, яка забезпечує автономність та самовиконання договору.

Через те, що смарт контракти реалізуються на базі серверів та інтернет з'єднання, залежно від предмету договору, поширюються випадки, коли контрагенти перебувають в різних країнах. Як наслідок, постає питання визначення правової системи, якою буде врегульовано такі відносини.

Контракти засновані на системі Blockchain мають ряд особливостей, які не завжди узгоджуються з характерними для міжнародного приватного права колізійними прив'язками, що ускладнює вибір правової системи. Так, метою даної роботи є дослідження узгодженості наявних колізійних прив'язок з природою смарт контрактів.

Концепція смарт контракту була запропонована Ніком Сабо, ще в 1996 році. Він припустив можливість формування «високорозвиненої практики» договірного права. Основна відмінність від класичних договорів – цифрова форма та зобов'язання у формі алгоритму [6].

Значного поширення концепція набула після появи у 2008 році платформи Blockchain. Перекладається як «ланцюжок блоків». Blockchain це цифрова технологія яка підтримує перевірку, виконання та запис транзакцій між різними сторонами [7].

Засновані на цифровій технології смарт контракти мають багато відмінностей від класичних договорів. Так, смарт контракти мають електронну форму та

виражаються у вигляді програмного коду. Будь-які зміни вносяться в режимі теперішнього часу з повідомленням всіх учасників домовленості. Доступ до коду мають лише сторони договору. Виконання здійснюється автоматично без участі третіх осіб, проте з можливим використанням програми-оракула. Оплата здійснюється виключно в криптовалюті.

Через перелічені відмінності, в науці існує декілька думок щодо правової природи смарт контрактів. Їх визначають самостійним договором, несамостійною договірною конструкцією [3], договором з особливим (автоматизованим) способом виконання або способом виконання зобов'язання [4], формою договору [2] та навіть доказом, який підтверджує факт укладення договору в усній формі [5].

Ми ж підтримуємо думку Баранова О.А. та в межах цієї роботи визначаємо смарт контракт як інноваційну форму самостійного договору, укладення, виконання та припинення яких відбувається з використанням мережевих комп'ютерних програмних та/або програмно-апаратних засобів, що мають взаємозв'язок з фізичними або цифровими об'єктами, за участю або без участі людини [1].

У класичних договірних відносинах з іноземним елементом застосовуються різні способи вибору правової системи.

Смарт контрактам не властиві більшість характерних для договірного права колізійних прив’язок. Ми не можемо використати такі прив’язки як «місце виконання договору» та «місце укладання контракту». Це пов’язано з тим, що укладання та виконання договору відбувається в кіберпросторі. В свою чергу кіберпростір не перебуває в повному правовому контролі жодної з держав.

Також ми не можемо використати прив’язку до закону, із яким найбільш тісно пов’язані правочини. За загальним правилом, правочин більш тісно пов’язаний з правом держави, у якій перебуває або проживає сторона, що повинна здійснити його виконання. Питання виконання правочинів в смарт контрактах є досить спірним. Воно здійснюється платформою автоматично, без прямої участі сторін. Звичайно, ми можемо виділити виконавця зі змісту договору, проте ця дія потребуватиме розшифрування коду та додаткового адаптаційного тлумачення судами суті самих правовідносин.

Загалом, існують технічні та теоретичні способи за допомогою яких можна пов’язати укладений смарт контракт з певною правовою системою. Питання в тому, чи має така правова система належне правове регулювання такого типу відносин та чи зможе обрана національна судово система забезпечити права осіб, які

до неї звернулися. Вважаємо такий спосіб вибору правового регулювання неефективним.

В науці виділяють й інші способів вибору правової системи для регулювання правовідносин з іноземним елементом заснованих на смарт контрактах. Найбільш поширений - вибір на основі принципу автономії волі (lex voluntatis). Так, контрагенти, в межах договору, самостійно вирішують яку правову систему застосовувати. Через особливий спосіб побудови та вираження умов смарт-контракту, виникають питання щодо можливості закріплення умови про вибір юрисдикції в алгоритмізованій системі Blockchain. Така умова має суб'єктивний характер, як наслідок система не зможе виконати її автоматично, а отже запис такої умови за допомогою програмного коду не має практичного застосування.

З іншого боку, учасники таких правовідносин можуть скористатися принципом автономії волі шляхом проведення додаткових переговорів та закріплення рішення щодо вибору юрисдикції в рамках звичайної, класичної додаткової угоди.

Одним з новітніх підходів до вирішення проблеми є використання інших комп'ютерних мереж. Вибір правової системи здійснюється спеціальною програмою на основі IP адреси сторін договору. IP адреса це унікальна адреса пристрою та мережі. Ідея в тому, що

програма проаналізує та обере найбільш повне правове регулювання ситуації. Це звучить утопічно, проте можливо.

Також в українських та зарубіжних правових колах обговорюється варіант створення єдиної онлайн-платформи смарт контрактів. В ній будуть діяти встановлені міжнародним співтовариством правила створені з врахуванням особливостей смарт контрактів та наявні правила торгівлі, в тому числі міжнародні уніфіковані правила. Вважаємо цей напрямок найбільш перспективним варіантом подальшого регулювання смарт контрактів в міжнародному секторі.

Отже, на даний момент найбільш реалістичним та ефективним способом вибору правової системи для врегулювання відносин з іноземним елементом заснованих на смарт контрактах вважаємо вибір юрисдикції на основі автономії волі сторін. Поширення використання цього принципу спричинить збільшення кількості звернень до держав, які мають розвинене законодавство. Що в свою чергу до розвитку та зацікавленості інших держав а темі регулювання смарт договорів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Баранов О.А Інтернет речей (IoT): правові проблеми застосування розумних контрактів. Інформація і право. 2017. № 4 (23). С. 26-40. URL:

http://ippi.org.ua/sites/default/files/5_7.pdf (дата звернення: 25.10.2022).
2. Богданова Е.Е. Проблемы применения смарт-контрактов в сделках с виртуальным имуществом. Lex russica. 2019. № 7 (152). С. 108–118.
3. Савельев А.И. Договорное право 2.0: «умные контракты» как начало конца классического договорного права. Вестник гражданского права. 2016. № 3. С. 32–60.
4. Сомова Е.В. Смарт-контракт в договорном праве. Журнал зарубежного законодательства и сравнительного правоведения. 2019. № 2. С. 79–86.
5. Тюльканов А.Л. Смарт-контракты – договоры или технические средства? URL: https://zakon.ru/blog/2017/4/7/smartkontrakty__dogovory_ili_tehnicheski_sredstva (дата звернення: 25.10.2022).
6. Szabo, Nick. Formalizing and securing relationships on public net-works. First Monday. 1997. URL: https://firstmonday.org/ojs/index.php/fm/article/view/548/469publisher=First (дата звернення: 25.10.2022).
7. Nakamoto, Satoshi. Bitcoin: A peer-to-peer electronic cash system. 2008. URL:https://www.google.com.ua/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&ved=2ahUKEwiGgqKW2qXmAhULMawKHV2UCEgQFjACegQIAhAC&url=https%3A%2F%2Fbitcoin.org%2Fbitcoin.pdf&usg=AOvVaw054mYD7EyyKjwcHh8i0Vw (дата звернення: 25.10.2022).

МАКСИМЕНКО Каріна
Студентка ФСП, КПІ ім. Ігоря Сікорського

МОЖЛИВІСТЬ ПРОВЕДЕННЯ ОНЛАЙН-МЕДІАЦІЇ В НОРМАХ ЗАКОНУ УКРАЇНИ «ПРО МЕДІАЦІЮ»

Складність та нестабільність теперішньої ситуації в країні потребує швидкої системи вирішення спорів. Перебування сторони конфлікту на окупованій території, його переїзд з постійного місця проживання або за кордон створюють додаткові перешкоди для здійснення юрисдикційної форми вирішення спорів, дають підґрунтя для розвитку нетрадиційних методів, зокрема вирішення спору за допомогою онлайн-медіації.

Онлайн-медіація це переговорний процес за участю сторін та медіатора, що проходить в реальному часі з використанням Інтернет платформи (програми) комунікації, спрямований на врегулювання конфлікту [2].

Правові засади та порядок проведення медіації, принципи медіації та інші питання, пов’язані з цією процедурою регулюються Законом України «Про медіацію» (Далі - Закон).

В Законі поняття медіації визначається як позасудова добровільна, конфіденційна, структурована процедура, під час якої сторони за допомогою медіатора (медіаторів) намагаються запобігти виникненню або врегулювати конфліктів (спорів) шляхом переговорів [1].

Медіація проведена відповідно до вимог Закону, має свої юридичні наслідки. Один з яких - угоди підписання на основі досягнутих під час медіації домовленостей. В угоді прописуються узгоджені сторонами зобов’язання, строки їхнього виконання та насідки невиконання. За умови неналежного проведення процедури медіації, таку угоду буде легко оскаржити в судовому порядку та уникнути юридичної відповідальності за її невиконання.

Так, мета даної роботи: розглянути чи передбачає нещодавно прийнятий Закон можливість проведення онлайн-медіації.

Відповідно до Закону медіація має декілька стадій: стадія підготовк, стадія проведення та припинення медіації.

Підготовка до медіації це здійснення підготовчих заходів із сторонами наявного або можливого конфлікту (спору) для з’ясування можливості проведення медіації з метою запобігання виникненню або врегулювання конфлікту (спору), зокрема зустрічі, збирання та обмін

інформацією, документами, необхідними для прийняття рішення сторонами конфлікту (спору) та рішення медіатора про участь в медіації, а також інші заходи, узгоджені між сторонами конфлікту (спору) та медіатором або суб'єктом, що забезпечує проведення медіації [1].

На етапі підготовки, онлайн-медіатор має дотриматись передбачених Законом вимог, а також здійснити додаткові заходи пов'язані з належним функціонуванням онлайн режиму. Так, медіатору потрібно: проговорити зі сторонами аспекти, пов'язані зі специфікою онлайн медіації, вирішити організаційні питання (оцінити реалістичність онлайн медіації, обрати зручну платформу для онлайн зустрічей, здійснити технічну підтримку сторін з завантаженням та користуванням онлайн платформою (у разі необхідності), організувати візуалізацію тощо), провести попередні технічні зустрічі зі сторонами для тестування якості зв'язку, тримати в фокусі більше питань (зокрема, щодо забезпечення технічного та психологічного комфорту сторін медіації) [3].

Медіатор зобов'язаний здійснювати підготовку до медіації та її проведення відповідно до ЗУ «Про медіацію», правил проведення медіації та кодексу професійної етики медіатора.

На етапі підготовки підписується договір про проведення медіації. В договорі має бути передбачено строк та місце проведення медіації, умови конфіденційності інформації, наслідки її розголошення учасниками медіації, а також порядок та підстави припинення медіації.

В Законі відсутні вимоги та обмеження щодо місця проведення медіації. Як наслідок, вважаємо, що до місця проведення медіації можна відносити й кіберпростір, зокрема спеціалізовані ресурси для проведення медіації та застосунки для здійснення онлайн комунікації.

Закон також згадує про правила проведення медіації. Правила проведення медіації – це порядок та методика проведення медіації, права та обов’язки учасників медіації, які визначаються договором про проведення медіації або затверджуються суб’єктом, що забезпечує проведення медіації [1].

З наведеного визначення випливає, що учасники медіації можуть самі визначити правила проведення медіації в договорі про проведення медіації. Єдина вимога до таких правил – не суперечити вимогам Закону. На наш погляд, таких законодавчо закріплених вимог недостатньо для повноцінного регулювання медіації. З іншого боку, саме такий спосіб регулювання

дозволяє проводити онлайн-медіацію без порушення вимог законодавства.

Проведення медіації регулюється статтею 17 Закону, проте дана стаття робить відсилку на ті ж вимоги договору про проведення медіації, правила проведення медіації та норми професійної етики. Вважаємо, що дана норма й постійна відсилка до непрописаних законодавцем правил є головним недоліком ЗУ «Про медіацію».

Медіатор зобов'язаний безпосередньо керувати процедурою проведення медіації. Можливість безпосереднього керування процедурою онлайн-медіації залежить від навичок медіатора, обраної ним програми дистанційного спілкування, його досвіду користування та ознайомленості з функціональними можливостями застосунку.

Найбільшою проблемою з якою стикаються онлайн-медіатори є забезпечення конфіденційності. Так, медіатор та інші учасники медіації, а також суб'єкт, що забезпечує проведення медіації, не мають права розголошувати конфіденційну інформацію, якщо інше не встановлено Законом або якщо всі сторони медіації не домовилися у письмовій формі про інше [1].

Під час проведення онлайн медіації, медіатор не може бути впевнений, що поряд зі стороною не перебувають особи, які не є учасниками медіації. На

наш погляд ця проблема вирішується правильно сформованими та роз'ясненими сторонам положеннями договору. Інший проблемний момент – здійснення необговореного звуко- чи відеозапису або трансляція зустрічі постороннім особам.

Таких ситуацій можна уникнути шляхом встановлення додаткових засобів технічного захисту. Так, є програми, які забороняють здійснювати фіксацію під час зустрічей, використовують захищені посилання, або дають доступ лише особам, які мають засоби входу: ключі, логіни, коди тощо. Медіатор, під час здійснення підготовки до медіації має прорахувати всі можливі загрози, знаходити та втілювати способи їхнього знешкодження.

Онлайн-медіація повинна також враховувати особливості укладання сторонами угоди за результатами медіації. Ця угода є однією з підстав припинення медіації. В Законі відсутні вимоги або обмеження щодо форми такої угоди та підпису сторін. Керуючись принципом свободи договору, вважаємо, що така угода може укладатися в письмовій формі з використанням інформаційно-комунікаційних технологій та застосуванням електронного цифрового підпису.

Отже, Закон України «Про медіацію» не містить обмежень щодо проведення онлайн медіації. Даний акт

передбачає лише вимоги до самої процедури незалежно від її форми проведення. Проведення онлайн-медіації має свої виклики, більшість з яких можна врегулювати за допомогою договору про проведення медіації. Цей договір дає можливість передбачити ключові проблемні моменти, такі як питання конфіденційності, присутності учасників та форми укладання угоди. Як наслідок, за умови дотримання передбачених в Законі моментів, онлайн медіація буде цілком правомірною.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Про медіацію: Закон від 16.11.2021 № 1875-IX. База даних: «Законодавство України»/ВР України. URL: https://zakon.rada.gov.ua/laws/show/1875-20#Text (дата звернення: 28.10.2022).

2. Галупова Л. І. Онлайн-медіація як спосіб захисту прав інтелектуальної власності в цифровому середовищі. Рекодифікація цивільного законодавства і системи права України у контексті євроінтеграційних процесів: матер. Всеукр. науково-практичн. конфер. (Одеса, 8–9 листопада 2019 року). За заг. ред. д.ю.н., проф. Є. О. Харитонова. Одеса: Фенікс, 2019. С. 236–239.

3. Романадзе Л.Д. Онлайн медіація між суб’єктами господарювання: додаткові виклики для сторін та медіатора. Правове життя сучасної України: матеріали Міжнар. наук.-практ. конф. (м. Одеса, 15 трав. 2020 р.). Одеса: Гельветика, 2020. Т. 2. С. 282-284.

МЕЛЬНИК Дарина
студентка ФБМІ, КПІ ім. Ігоря Сікорського

РИЗИКИ ПОРУШЕННЯ ПРАВ ЛЮДИНИ ЗА ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ

Використання штучного інтелекту набирає обертів щодня. Визначається безліч шляхів використання штучного інтелекту в різних сферах життя людини. Для аналізу ризику порушень прав людини за використання штучного інтелекту слід розглянути документи, що широко використовуються в Європі та несуть в собі великий спектр прав людини. Серед них Загальна декларація прав людини 1948 р., Міжнародний пакт про громадянські і політичні права 1966 р., Міжнародний пакт про економічні, соціальні та культурні права 1966 р. та Хартія основних прав ЄС. Проаналізувавши ці документи, серед ризиків порушень прав людини можна виділити: порушення права на життя, права на недоторканість приватного життя, обмеження свободи слова та думки, порушення права на справедливий судовий розгляд та презумпцію невинності, права на рівні можливості і недискримінанцію, права на працю тощо.

Поняття «штучний інтелект» є багатогранним і використовується як наратив, за допомогою якого

описуються інтелектуальні можливості комп ютерів під час прийняття ними рішень [2]. Вперше формулювання поняття «штучний інтелект» запропоноване Дж. Маккарті у 1956 році у роботі Дартмутської конференції, і звучав він так: «штучний інтелект – це наука й техніка створення інтелектуальних машин, особливо інтелектуальних комп`ютерних програм» [1].

Штучний інтелект працює шляхом систематизації і автоматизації інтелектуальних завдань будь-якої сфери інтелектуальної діяльності людини, стає універсальною науковою областю. Швидкий розвиток технології штучного інтелекту вимагає пильного контролю питань безпеки, надійності, ясності, справедливості, етики та рівності. Ці питання несуть ризик для основних прав людини, особливо за неможливості передбачення наслідків застосування даної технології. Безліч проблем порушень прав, що виникають, не є новими, але за рахунок масштабу, поширення і впливу – вони погіршуються. Через це, використання штучного інтелекту може одночасно і допомагати і шкодити людству в рівній мірі. Розглянемо 3 основні права людини, які може порушити штучний інтелект.

Право на працю та достойність життя. Статті 23, 25 Загальної декларації прав людини (ЗДПЛ) та ст.ст. 6,7,11 Міжнародного пакту про економічні, соціальні та культурні права (МПЕСКП) проголошують,

що абсолютно кожна людина має право на працю, вільний вибір роботи, справедливі і сприятливі умови праці та захист від безробіття. Усі робочі мають право на задовільну, і головне, справедливу оплату праці, що забезпечить гідне існування людини та її сім`ї [5,6,7].

Штучний інтелект відіграє значну роль у автоматизації робочих місць і несе потенційну загрозу праву на працю, а саме може стати перепоною для людей у зебезпеченні місця на ринку праці. Слід зазначити, що вже сьогодні автоматизація деяких робочих процесів суттєво вплинила на скорочення робочих місць у певних галузях, і багато науковців констатує, що ця тенденція зростатиме. Штучний інтелект вже поступово заміщує працівників, і наділений можливістю виконувати певну роботу чи надавати послугу. Безліч роботів, що наділені цим штучним інтелектом, надають продукт, послугу чи виконують роботу на підприємствах та приватних організаціях. Наприклад, збирають та сортують товари на складах, перевозять конкретні вантажі, у більш науково обізнаних країнах – осблуговують клієнтів у продуктових магазинах, реєструють відвідувачів у готелях, формують замовлення в ресторанах. Звісно, вдосконалення штучного інтелекту також сприяє полегшенню роботи людини. Науковці вважають, що штучний інтелект знищить близько 75 млн. робочих

місць, але вони запевняють одночасну появу близько 130 млн нових робочих місць, що будуть пов`язані з новим поділом праці між людиною і штучним інтелектом [3]. Серед професій, які знаходяться перед загрозою зникнення внаслідок впровадження штучного інтелекту виділяють: бухгалтери, продавці, страховики, касири, адміністратори, офісні працівники, працівники промислових та виробничих підприємств тощо. Звідси можемо зробити висновок, що з часом штучний інтелект повністю візьме на себе виконання усіх видів рутинної роботи будь-якої складності [4].

Також, слід зазначити проблему особистого кар`єрного росту працівника, що стає ускладненим, за використання штучного інтелекту в питаннях найму на роботу та моніторингу роботи персоналу чи проведення внутрішнього рейтингу працівників. Штучний інтелект суттєво вплине на суспільство шляхом збільшення безробіття, порушенням в оплаті праці, що призведе до великої нерівності. Проте, слід зазначити, разом з цими викликами, для працівників відкриються нові можливості, а саме в креативних індустріях, інноваційних сферах діяльності, де не знайдеться місця для штучного інтелекту.

Отже, впровадження штучного інтелекту в ринок праці суттєво його змінить, та значна кількість людей не зможе знайти роботу, в зв`язку з чим люди не

зможуть забезпечувати свої сім`ї, як наслідок, порушиться право на достатній рівень життя.

Право на життя. Стаття 3 ЗДПЛ, ст. 6 Міжнародного пакту про громадянські і політичні права (МПГПП), ст. 2 Хартії основних прав ЄС проголошують, що право на життя є невід`ємним правом кожної людини. Це право охороняється законом, ніхто не може бути свавільно позбавлений життя [5,6,7].

Штучний інтелект є цінним для людини помічником. За його допомогою можна виявити онко-захворювання, психологічні порушення, виявляти та попереджати тяжкі та смертельні захворювання на ранніх стадіях. Використання штучного інтелекту полегшує роботу лікарів у сфері аналізу анамнезу, зміни самопочуття пацієнта протягом лікування та дає змогу виконувати це віддалено. З`явилась можливість виконання надскладних операцій або операцій у важкодоступних місцях. Проте, незважаючи на надзвичайний прорив та користь для здоров`я, штучний інтелект здатний завдати шкоди життю людини. Світ переходить на новий вид війни, в основі якої лежить штучний інтелект. Зброя стає швидшою, більш точною, і відповідно, ефективнішою. На жаль, сьогодні ми це спостерігаємо в реаліях, у боротьбі України проти російської агресії. Щодня тисячі невинних цивільних українців гинуть внаслідок використання дронів

розвідки, безпілотників тощо. В їх основі лежить штучний інтелект. Слід зазначити, що загроза життю штучним інтелектом лежить не лише у військовій сфері. Наука медицини дозволяє використання штучного інтелекту у ДНК- та генетичних тестуваннях. Будь-яка похибка може вартувати життя.

Право на недоторканність приватного життя та захист даних. У ст. 12 ЗДПЛ, ст. 17 МПГПП, ст.7, 8 Хартії основних прав ЄС озвучено: ніхто не може безпідставно втручатись у особисте чи сімейне життя. Кожна людина має право на захист особистих даних щодо своєї особи. Ця інформація повинна використовуватися відповідно до встановлених правил в певних цілях чи інших правомірних підставах, фіксованих законом [5,6,7].

Системи штучного інтелекту в рази полегшують та пришвидшують процес збору, обробки та класифікації особистої інформації людства. Практика програм штучного інтелекту часто проводиться на готових базах даних. Одна похибка може сприяти розкриттю приватних даних, що може загрожувати особистому чи сімейному життю. Науковці розробили програму для ШІ, що допомагає аналізувати стать, вік, спеціальність, сімейний стан, місцезнаходження тощо. Це також особиста інформація, тому, з нею потрібно поводитись так само, як з конфіденційною, з метою захисту прав

людини. Через це, вже зовсім скоро, можна буде аналізувати всю історію життя людини, керуючись цими даними. Такі дані нині широко застосовуються для таргетованої реклами, задля чого відстежується «цільова» аудиторія за віком, статтю, інтересами чи іншими характеристиками, що вказує замовник. Саме розвиток ШІ дозволяє глибоко і детально відслідкувати ці процеси. Проте нерегульовані можливості ШІ можуть покласти край анонімності та особистого захисту в просторах Інтернету, а страх бути «відстеженим» може призвести до серйозних призвести до серйозних психологічних порушень, тим самим одночасно порушити права на здоров`я та недоторканості даних [8].

Висновок: неможливість точної регуляції можливостей ШІ може призвести до серйозних порушень прав людини, внаслідок популяризації його використання у різних сферах.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Баранов О. А. Інтернет речей і штучний інтелект: витоки проблеми правового регулювання. ІТ-право: проблеми та перспективи розвитку в Україні : зб. матеріалів II Міжнар. наук.-практ. конф. (Львів, 17 листоп. 2017 р.). Львів : Львів. політехніка, 2017. С. 18–42

2. Сидорчук Ю. М. Філософсько-правові проблеми використання штучного інтелекту. Право і суспільство. 2017.№ 3. Ч. 2. С. 16–19.
3. Томас Г., Вімм.Н. Штучний інтелект, робочі місця, нерівність і продуктивність: Чи має значення сукупний попит?, Робочі документи MERIT 2018-047, Університет ООН – Маастрихтський інститут економічних і соціальних досліджень з інновацій і технологій (MERIT), с. 3-7
4. Азьмук Н.А. Штучний інтелект у процесі праці у цифровій економіці: нові виклики та можливості., 2019. С. 137-145
5. Загальна декларація прав людини. URL: https://zakon.rada.gov.ua/laws/show/995_015#Text (дата звернення 30.10.2022)
6. Хартія основних прав ЄС. URL: URL: https://zakon.rada.gov.ua/laws/show/994_524#Text (дата звернення: 30.10.2022).
7. Міжнародний пакт про громадянські і політичні права. URL: https://zakon.rada.gov.ua/laws/show/995_043#Text (дата звернення 30.10.2022)
8. Гур’єва М. Штучний інтелект та «нова дискримінація»: як технології впливають на права та життя людини, Inspiered, 2019 р.

ПЕТРОВ Данило
Курсант Луганського державного університету
внутрішніх справ ім. Е.О. Дідоренка

ПОШИРЕНІ ЗАГРОЗИ КІБЕРБЕЗПЕКИ ТА СПОСОБИ БОРОТЬБИ З НИМИ

Ми досліджуємо типи кібератак і те, як ви можете залишатися в безпеці, використовуючи IT-обладнання та системи.

Стрімкий світ цифрових технологій означає, що ми робимо швидкий прогрес, долаючи багато кордонів. Однак із таким прогресом зростає масштаб і складність кіберзагроз. Ми досліджуємо деякі з найпоширеніших загроз кібербезпеці та те, як протистояти їм прямо.

Окрім того, що ми оновимо деякі основи кібербезпеки, ми розглянемо деякі кроки, які слід виконати, щоб захистити свої IT-системи. Насамкінець ми розглянемо деякі найкращі практики кібербезпеки та розглянемо, де можна пройти навчання.

Що таке кібербезпека? Ми використовуємо цей термін для позначення набору різних методів, які може використовувати особа чи організація для захисту цілісності різних мереж, програм і даних від будь-яких атак або неавторизованого доступу. У сфері

кібербезпеки існує багато різних методів і сфер, і вони відображають складність і різноманітність кібератак.

На індивідуальному, організаційному чи навіть національному рівні кібербезпека допомагає захиститися від таких проблем, як розкриття інформації та крадіжка чи пошкодження апаратного забезпечення, програмного забезпечення чи електронних даних.

Використовувані методи також допомагають гарантувати, що IT-сервіси можуть функціонувати без збоїв або неправильного спрямування. Розуміючи, наскільки важливою є ця галузь, не дивно, що це один із секторів IT, який найшвидше розвивається.

Часто існують неправильні припущення щодо того, хто відповідає за кібербезпеку. Дехто може сказати, що менеджер з інформаційної безпеки або аналітик з кібербезпеки – це той, хто бере на себе відповідальність в організації. Хоча вони певною мірою винні, кожна особа повинна взяти на себе відповідальність за власну кібербезпеку.

Хоча існують політики та засоби захисту, які гарантують безпеку окремого обладнання з технічної точки зору, кінцевий користувач також має бути навченим і усвідомлювати існуючі потенційні кіберризики.

Частиною цієї відповідальності є розуміння наявних кіберзагроз і вразливостей і прийняття

обґрунтованих рішень щодо того, як ви взаємодієте зі своїм ІТ-обладнанням. І, звичайно, якщо це ваша домашня мережа та апаратне забезпечення, потреба в цих знаннях є настільки ж необхідною.

Отже, хоча існують вакансії з кібербезпеки, які зосереджені на запобіганні витоку даних, збоях у роботі сервісів та інших ІТ-загрозах, кожна особа має бути уважною до потенційних небезпек. Не тільки це, але ви також повинні знати, що робити, щоб захистити себе від них.

Нижче ми вибрали деякі з найпоширеніших загроз кібербезпеці та описали, як з ними боротися. Це лише деякі з методів, які використовують хакери та інші зловмисники для компрометації ІТ-систем. Щоб дізнатися більше, ви можете переглянути наші мікрореєстраційні дані про операції з кібербезпеки.

«Фішинг». Це термін, який використовується для опису процесу спроби отримати приватну інформацію, видаючи себе за законного запитувача. Зловмисна особа чи організація може «ловити» інформацію, використовуючи підроблені повідомлення, наприклад електронні листи, щоб спробувати отримати облікові дані для входу чи іншу конфіденційну інформацію.

Фішинг – це усталена практика, яка з роками ускладнилася. Таким чином, ці шахрайства може бути важко помітити навіть тим, хто має гострий погляд.

Зловмисники можуть підробляти адреси електронної пошти, маскуватися під законні особи по телефону та створювати фіктивні веб-сайти, здатні перехоплювати конфіденційні дані.

Як боротися з фішингом? Є кілька способів виявити та уникнути фішингових атак. Ось кілька основних порад:

- Переконайтеся, що ваше IT-обладнання оновлено та встановлено необхідне програмне забезпечення безпеки.
- Ставтеся з підозрою до електронних листів і дзвінків, які здаються надто тривожними або трохи дивними. Наприклад, електронний лист може попереджати вас про зламаний пароль, але в ньому можуть бути орфографічні помилки, незвична адреса електронної пошти або непрофесійний макет. Не натискайте на посилання, якщо ви не впевнені в автентичності повідомлення.
- Якщо ви не впевнені, чи дзвінок чи електронний лист є законними, зв’яжіться з компанією, перш ніж відповісти. Вони зможуть перевірити, правда це чи ні.
- Якщо ви стали жертвою фішингу, зверніться до відповідних органів. Наприклад, у Великобританії ви можете повідомити про це NCSC
- Ви часто побачите, що зловмисне програмне забезпечення та фішинг йдуть рука об руку. Цей термін використовується для опису шкідливого програмного

забезпечення, призначеного для здійснення атаки на пристрій або сервер, який завантажує або запускає його. Атаки зловмисного програмного забезпечення можуть спричинити пошкодження даних або навіть вивести з ладу всю систему.

Як і у випадку з фішингом, зловмисне програмне забезпечення намагається обманом змусити користувача натиснути посилання або завантажити/ встановити програму. Потім такі програми можуть самовідтворюватися, відстежувати натискання клавіш, захоплювати системні ресурси, блокувати доступ та інші подібні компрометуючі дії.

Як боротися зі шкідливим програмним забезпеченням? Знову ж таки, ви можете зробити кілька кроків, щоб запобігти потенційним кіберзагрозам зловмисного програмного забезпечення та боротися з ними. Нижче ми вибрали кілька важливих порад:

• Переконайтеся, що на вашому пристрої встановлено та оновлено програмне забезпечення для захисту від шкідливих програм.

• Зробіть резервну копію своїх даних, особливо важливих файлів, і переконайтеся, що ви можете зберігати їх в автономному місці.

• Відкривайте лише ті файли та програмне забезпечення, які, як вам відомо, походять із надійного джерела.

• Перевірте вміст і листування, щоб виявити будь-які елементи, які здаються непотрібними (як у випадку з фішингом).

• Розробіть план протидії потенційній атаці зловмисного програмного забезпечення. Дізнайтеся більше про це в нашому ExpertTrack з основ кібербезпеки.

Програмне забезпечення-вимагач – це тип зловмисного програмного забезпечення, яке фактично блокує файли жертви, шифруючи їх, щоб до них не було доступу. Зазвичай зловмисник вимагатиме плату (часто сплачується анонімно через криптовалюту) за розшифровку даних. Це, мабуть, найбільша загроза кібербезпеці в поточному ландшафті.

Знову ж таки, типовою відправною точкою атаки програм-вимагачів є спроба фішингу. Зловмисник спробує змусити жертву встановити шкідливе програмне забезпечення, яке потім блокує систему.

Жертви атак програм-вимагачів часто можуть почуватися безпорадними, залишившись без доступу до своїх файлів. Як і з багатьма загрозами кібербезпеці в цьому списку, запобігання часто є найкращим способом боротьби з ними.

- Переконайтеся, що у вас встановлено та оновлено антивірусне програмне забезпечення. Те саме стосується ваших IT-пристроїв.

- Налаштуйте свої пристрої так, щоб на них могли працювати лише авторизоване програмне забезпечення та програми. Уникайте відкриття програм і файлів із невідомих джерел.
- Якщо ви стали жертвою атаки програм-вимагачів, негайно повідомте про це свою групу IT-безпеки (якщо на роботі). Відключіть уражену машину від мережі.
- Повідомте органи влади про порушення. Не платіть викуп, але переконайтеся, що відповідні організації поінформовані – вони можуть порадити вам більше.

Атака «людина посередині» (MITM) — це коли зловмисник встановлює позицію між відправником повідомлення чи інформації та одержувачем, що дозволяє їм перехоплювати будь-яку кореспонденцію. Зловмисник MITM міг навіть змінити вміст повідомлення без відома ні відправника, ні одержувача. Ці типи атак може бути важко виявити, тому знову ж таки запобігання є набагато простішим методом боротьби з атаками MITM:

- Переконайтеся, що точки доступу безпечні. Мережі Wi-Fi часто особливо вразливі до атак типу "людина посередині", тому важливо переконатися, що паролі надійні та безпечні.
- Використовуйте VPN для конфіденційної інформації. Віртуальна приватна мережа (VPN) може створити

безпечне середовище, яке можна використовувати під час обробки цінних даних.

- Переконайтеся, що ваші веб-браузери регулярно оновлюються – часто випускаються патчі, щоб закрити будь-які вразливості безпеки.

Троянські віруси — ще одна форма шкідливого програмного забезпечення. Однак, як випливає з назви, вони вторгнуться у вашу систему шляхом маскування. Часто вони виглядатимуть як звичайний файл або програма, намагаючись обманом змусити вас запустити або встановити їх.

Щойно троян отримав доступ до вашої системи, він може вимкнути антивірус, завантажити більше шкідливих програм або зробити його частиною DDoS-атаки (докладніше про це нижче).

Ретельне розуміння загроз кібербезпеці – найкращий спосіб запобігти проникненню троянів у вашу систему:

- Уникайте завантаження програмного забезпечення з джерел, яким ви не довіряєте або не авторизовані.
- Переконайтеся, що ваша операційна система, браузери та антивірусне програмне забезпечення оновлені.
- Ніколи не запускайте програми та не відкривайте вкладення з невідомих джерел.
- Якщо у вас є троян, потужна антивірусна програма повинна впоратися з ним. Якщо ви не впевнені, зверніться до свого IT-відділу або до спеціаліста.

Відмова в обслуговуванні/розподілена атака на відмову в обслуговуванні (DDoS) виникає, коли хакер використовує кілька пристроїв (часто тисячі) і використовує їх для перевантаження цільових систем. Зазвичай зловмисники націлюються на веб-сайти, які зазвичай можуть впоратися з певною кількістю користувачів одночасно. Це робить веб-сайт (і пов'язані служби) непридатним для використання на деякий час.

Значна частина запобігання та боротьби з DDoS-атаками виконується IT-фахівцями, які мають доступ до серверів і мереж. Вони часто гарантують наявність рішень кібербезпеки. Однак звичайні користувачі можуть допомогти, дотримуючись подібних процедур і запобіжних заходів, як і для захисту від зловмисного програмного забезпечення.

Кібербезпека є важливою умовою в нашому сучасному цифровому світі. Оскільки велика кількість нашої особистої інформації доступна одним натисканням кнопки, завжди є кіберризики, яких варто остерігатися. Однак, знаючи про загрози кібербезпеці та способи боротьби з ними, ви можете дати собі найкращі шанси зберегти свої дані в безпеці.

Майже кожен може отримати користь від базового навчання з кібербезпеки, а завдяки нашому асортименту мікрокредитів, курсів і ExpertTacks ви незабаром зможете почати оволодівати цією важливою навичкою.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1.Жарков Я.М. Кібербезпека особистості, суспільства, держави : підручник / Я.М. Жарков, М.Т. Дзюба, І.В. Замаруєва та ін. — К. : Видавничо-поліграфічний цента Київський університет», 2008. — 256 с.

2.Кібербезпека держави: підручник / [В.М. Петрик, М.М. Присяжнюк, Д.С. Мельник та ін.]; в 2 т. — Т. 2. / за заг. ред. В.В. Остроухова. — К. : ДНУ «Книжкова палата України», 2016. — 328 с.

3.Кормич Б.А. Організаційно-правові засади політики кібербезпеки України : монографія / Б.А. Кормич. — О. : Юридична література, 2003. — 472 с

4.Ліпкан В.А. Кібербезпека як складова національної безпеки України / В.А. Ліпкан // Інформаційні технології в економіці, менеджменті і бізнесі : Проблеми науки, практики і освіти : Зб. наук. праць VIII Міжнар. наук.- 256 практ. конф. — Ч. 2. — К. : Вид-во Європ. ун-ту, 2003. — С. 443–453.

5.Ліпкан В.А., Ю.Є. Максименко, В.М. Желіховський. Кібербезпека України в умовах євроінтеграції : Навчальний посібник. — К. : КНТ, 2006. — 280 с.

6.Максименко Ю.Є. Теоретико-правові засади забезпечення кібербезпеки України : дис.… канд. юрид. наук : 12.00.01 / Ю.Є. Максименко. — К., 2007. — 186 с.

7. Марущак А.І. Кібербезпека як об’єкт дослідження правової науки / А.І. Марущак // Актуальні проблеми управління кібербезпекою держави : зб. матер. наук.- прак.

конф., 17 березня 2010 року м. Київ. — К. : Наук. вид. відділ НА СБ України, 2010. — С. 36−41.
8. Медвідь Ф.М. Доносо В.Д.Х., Доносо В.С.Ф. Кібербезпека України в системі національної безпеки / Ф.М. Медвідь, В.Д.Х. Доносо, В.С.Ф. Доносо // Проблеми модернізації України : [зб. наук. пр.]. Вип. 1: Матеріали Всеукр. наук.- практ. конф. «Модернізація України: проблеми та технології успішності (питання економіки, права, соціології, освіти і культури)», 12 листопада 2015 р. / редкол. : А.М. Подоляка (голова) [та ін.] — Київ : ДП «Видавничий дім «Персонал», 2015. — С. 194–199.

ПИЛИПЕНКО Володимир
Студент ПБФ, КПІ ім. Ігоря Сікорського

ІННОВАЦІЙНЕ ВИКОРИСТАННЯ ІКТ У ЮРИДИЧНІЙ ДІЯЛЬНОСТІ

1.Застосування ІКТ безпосередньо сприяє юристам в розробці і впровадженні інноваційних підходів до надання правової допомоги, а також до пошуку і залучення клієнтів.

На сьогодні, завдяки стрімкому впровадженню інформаційних технологій в життя суспільства, з’явилась велика кількість каналів для розвитку особистого бренду, вибудовування сильної репутації, і,

як наслідок, для залучення клієнтів і лояльної аудиторії, що є важливим елементом діяльності адвоката.

Це дає можливість охопити більш широкий сегмент на ринку юридичних послуг, можливість удосконалити і посилити ефективність власних робочих процесів, а також можливість забезпечити собі суттєву конкурентну перевагу в професійному середовищі.

2.Впровадження продуктів і рішень сфери legal IT суттєво знижує витрати клієнтів, забезпечуючи повсякчасну доступність юридичних послуг, що повною мірою відповідає інтересам клієнтів.

Правові системи пошуку і аналізу інформації, програмне забезпечення для автоматизації бізнес-задач і робочих процесів, багатий інструментарій, що дозволяє моментально знаходити вірне рішення і максимально швидко виконувати операції різної складності – усе це надає можливість делегувати більшість рутинних процесів і завдань «розумним» технологіями, можливість максимально оптимізувати діяльність представників юридичного бізнесу аж до організації віртуальних юридичних офісів.

3. Вплив інформаційних технологій на діяльність адвокатів зокрема, багато в чому обумовлений спрямованістю державного управління та сучасної політики більшості країн, в тому числі і України, на діджиталізацію різних сфер життєдіяльності

суспільства. В правовій сфері це проявляється, головним чином, в створенні та впровадженні урядом держави електронного суду.

Електронний суд дозволяє подавати учасникам судового процесу до суду документи в електронному вигляді, а також надсилати таким учасникам процесуальних документів в електронному вигляді, паралельно з документами у паперовому вигляді відповідно до процесуального законодавства.

До суду користувачі можуть надіслати в електронному вигляді будь-які документи і матеріали, передбачені процесуальним законодавством. Права доступу до електронних документів, які надійшли на адресу суду надаються суддям, у провадженні яких перебувають відповідні судові справи. Суд після виготовлення та підписання процесуального документа, надсилає електронні копії процесуального документа, скріплені електронним цифровим підписом судді електронною поштою на поштову скриньку учасника судового процесу, якщо такий учасник зареєстрований в системі. Після отримання електронного підтвердження доставки електронного листа в поштову скриньку користувача відповідальний працівник суду роздруковує таке повідомлення та долучає його до матеріалів справи.

4. Можливість переходу адвокатів до віддаленого формату роботи зокрема через використання таких

інструментів, як Go To Meeting, Zoom, Skype, Slack, Google-продукти та сервіси, різних видів месенджерів тощо.

5. Можливість міжнародній юридичній комунікації. Адвокати та судді можуть ділитись досвідом формувати особистий імідж на міжнародній арені.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1.Ракитянська К. 2020 р. “інформаційні технології як запорука інноваційного розвитку адвокатської діяльності” URL: Rakytianska15.pdf (apir.org.ua)

2. Урядовий портал URL: Електронний суд — подання заяв до суду онлайн | Кабінет Міністрів України (kmu.gov.ua)

СОКИРКО Катерина

Курсант Луганського державного університету внутрішніх справ ім. Е.О. Дідоренка

ПРИНЦИПИ ЗАСТОСУВАННЯ ІНТЕРНЕТУ РЕЧЕЙ В ОСВІТІ

Інернет речей – це глобальна мережа підключених до інтернету пристроїв, оснащених сенсорами, датчиками, засобами передавання сигналів.

Ці цифрові пристрої можуть зчитувати за допомогою датчиків різноманітні сигнали з навколишнього світу, вступати у взаємодію з іншими пристроями, обмінюватися даними для віддаленого моніторингу за станом об’єктів, аналізу зібраних даних і прийняття на їх основі рішень. Завдяки впровадженню інтернету речей активно розвиваються такі сфери діяльності людини як медицина, освіта, лінгвістика, екологія, агрономія, маркетинг, сфера правових відносин, сфера безпеки, виробництво, страхування і кредитування, транспорт, туризм і розваги. Інтернет речей дає змогу людині по-новому контролювати своє персональне середовище.

Впровадження технологій IoT в освітній процес сприятиме підвищенню
рівня мотивації та пізнавальної активності учнів, формуванню їх готовності
використовувати свої знання в реальних життєвих ситуаціях. Інтернет речей дасть змогу змінити спосіб взаємодії між школярами і педагогами в процесі навчання та виховання.

Впровадження ІО в освіту відіграло важливу роль. Інтернет речей (сильно вплинув на навчальний заклад. Навчальні заклади вибирають екосистему IoT та використовують різні методи, починаючи від розширеної реальності до хмарних обчислень. Завдяки

інтеграції технології IoT фізичні середовища стають розумнішими та взаємопов'язанішими, ніж будь-коли.

Обговорюючи IoT в освіті, можна уявити собі такі речі, як розширений розумний клас, цифрова дошка та голосова система команд. Однак IoT прогресував значно далі, і його можна використовувати для того, щоб постійно оновлювати батьків щодо підбору та падіння дітей, розумних камер безпеки в приміщенні школи, автоматизованого відстеження відвідування учнів та багато іншого можна досягти в екосистемі IoT.

З розвитком технологій наше наступне покоління вже захоплюється Інтернетом та інформацією на вимогу. Основне питання виникає, чи матиме IOT в системі освіти позитивний чи негативний вплив на учнів. Наразі вивчається багато проблем, таких як конфіденційність та додаткова вартість технологій на освіту. Багато навчальних закладів все ще неохоче приймають IoT і знаходять кращу придатність для цього в системі. IoT в освіті може бути широко класифікований на перспективи студентів та працівників.

З точки зору персоналу, IoT має потенціал для управління відвідуванням класом учнів та наявністю необхідного навчального обладнання. Встановлення датчиків IoT у декількох місцях у системі освіти, таких

як бібліотека, кафетерія та вхід, допомагає відстежувати та контролювати діяльність учнів у різних місцях.

Завдяки IoT, включеному в аудиторії, викладачі можуть дистанційно керувати аудиторіями за допомогою голосових чи жестових команд, встановлювати зв’язок зі студентами з віддалених місць, збирати цінний відгук учнів з певного предмету та надавати допомогу студентам з особливими можливостями. Інші сценарії включають використання датчиків шуму для спілкування із сусідніми аудиторіями та поради щодо зменшення рівня шуму.

Під час експертизи вбудований РК-екран із IoT може виявити надмірний шум у певному класі та відображати попереджувальні повідомлення. Такі події, як реєстрація щоденного дня або спортивного дня, можна легко керувати за допомогою екосисIoIoT.

IoT може допомогти студентам спілкуватися з однокласниками локально чи віддалено, обмінюватися інформацією про проект, аналізувати та коментувати навчальний матеріал у режимі реального часу та віддалено отримувати доступ до навчальних засобів, таких як віддалені лабораторії. Особливо враховуючі сьогоднішу ситуацію в країні це дуже полегшить навчання.

Системи IoT полегшують навчальні заклади збирати велику кількість даних із сенсорів та носячих

пристроїв та здійснювати практичні дії на основі таких даних. Використовуючи вбудовані датчики, QR-коди та інші технології, ці системи дозволяють студентам в будь-який час досліджувати та отримувати доступ до навчальних матеріалів та іншої інформації.

Для підвищення рівня викладання та навчання вчителі також можуть користуватися носячими пристроями та смартфонами у класах. Розумний клас можна описати як розумне середовище з різними типами програмних та апаратних модулів. Відеопроектори, датчики та алгоритми розпізнавання обличчя - кілька прикладів екосистеми, вбудованої в IoT.

Застосування IOT в освітньому секторі відіграє важливу роль у трансформації традиційної системи освіти. У навчальному секторі існує широкий спектр застосувань IoT. Давайте подивимось декілька областей в освітній галузі, де можна застосувати IoT.

Однією з основних проблем освітньої системи, яка створює безпечну та безпечну атмосферу для студентів, можна досягти, вибравши екосистему IoT. Вбудовані технології, такі як NFC, можуть бути використані для управління студентами та їх доступу до різних частин кампусу, таких як лабораторії та інші місця в навчальному інституті.

Механізм контролю в класі в режимі реального часу може бути розроблений за допомогою NFC, який може доставляти інформацію про реєстрацію в класі та відображати стан класу на РК-панелях. Крім того, відвідуваність студента може бути записана за допомогою тегів RFID, вбудованих у посвідчення особи кожного студента.

Також навчальні програми полегшують налаштування та дозволяють учням вирішувати свою дію у спосіб передачі знань з предмету. Від домашніх комп'ютерів до телевізорів студенти можуть отримувати доступ до навчального контенту на декількох каналах у відпустці. Певні програми можуть бути використані для створення 3D графічного підручника, який містить відеовміст разом із приміткаами. Робити нотатки більше не записується на аркуші паперу, при просуванні в Інтернеті студенти можуть читати голосно і на основі голосу додаток перетворює мовлення в текст і зберігає їх у цифровому зошиті.

ВИСНОВОК. У цій публікації ми розглянули застосування Інтернет речей в галузі освіти та обговорювали різні переваги студентів, а викладачі виходять із вбудованої екосистеми IoT. Інтегруючи датчики та мобільні пристрої в будівлю, IoT має потенціал для перетворення аудиторій.

IoT створив унікальну можливість для посиленої співпраці студентів, викладання та навчання. Найближчим часом Інтернет речей буде включений у більшу частину системи освіти.

Деякі школи можуть використовувати його для підготовки своїх учнів до високотехнологічної грамотності, а інші можуть використовувати її для використання інформації, заощадження грошей та інших конкретних потреб. Якщо ми хочемо інтегрувати IoT в освіту, наше розуміння освіти має перейти на більшу перспективу

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Бортник К.Я., Ольшевський О.В., Пащук В.Ю. Інтернет речей та як він змінить наше життя у майбутньому. Комп’ютерно-інтегровані технології: освіта, наука, вир-во. 2018. № 30/31. С. 14–18

2. Олещенко Л. М. Програмування пристроїв Інтернету речей: лабораторний практикум [Електронний ресурс] : навчальний посібник для студентів спеціальності 121 «Інженерія програмного забезпечення» (освітня програма «Програмне забезпечення комп’ютерних та інформаційно-пошукових систем») / КПІ ім. Ігоря Сікорського ; уклад.: Л. М. Олещенко, Я. В. Хіцко. Електронні текстові дані (1 файл: 2,64 Мбайт). Київ : КПІ ім. Ігоря Сікорського, 2019. 47 с

ЧМИР Кирило
Курсант Луганського державного університету
внутрішніх справ ім. Е.О. Дідоренка

КІБЕРПРОСТІР ЯК НОВІТНІЙ ВИМІР БЕЗПЕКИ І ОБОРОНИ УКРАЇНИ

Людство завжди прагнуло я кнайповніше опанувати всі доступні йому простори. Об’єктивно це пов’язано з бажанням використати їх для цивілізаційного зростання, посилення економічних і політичних позицій держав, що з необхідністю призводило до виникнення протиріч. У результаті всі простори рано чи пізно перетворювалися на «території» запеклих протистоянь і конкурентної боротьби у сфері внутрішніх і зовнішніх відносин.

Щойно людина завдяки авіаційним і ракетним технологіям опанувала повітря й космос (третій і четвертий простори), розпочалася їх мілітаризація та внутрішня боротьба за гегемонію. Проте якщо з повітряними кордонами держав усе було більш-менш зрозуміло, то в космосі відсутні державні кордони, тому його мілітаризацію було заборонено відповідними міжнародними угодами. Разом з тим фактично мілітаризація й гонка космічних озброєнь мали двох основних акторів – головних суперників часів

«холодної війни» – СРСР і США. Згодом до клубу космічних гравців долучилася КНР, яка нині намагається стати країною, що першою створить постійну базу на Місяці.

Відсутність принципів існування та використання кіберпростору, пріоритет практичних міркувань над правилами співіснування людей характеризують політику використання кіберпростору як своєрідну realpolitik, яку часто намагаються поєднати з радикальними ліберальними теоріями, створюючи химери уявного світу, який нібито регулюється загальноприйнятими нормами на кшталт Вестфальського миру та міжнародним законодавством. Попри всі публічні заклики до мирного використання кіберпростору в інтересах усіх людей і держав, уряди тих самих країн, які до цього закликають, активно долучилися до гонки кіберозброєнь, відтворюючи класичну «дилему безпеки» на якісно новій основі. А це означає, що на тлі розгортання складних і суперечливих глобальних процесів політичного, економічного та соціального розвитку кіберпростір перетворюється на простір виникнення «холодної війни v2.0.», тобто основу нового протистояння ключових геополітичних суб’єктів, яке відбуватиметься переважно в кіберпросторі. Оскільки політична й геополітична змагальність у кіберпросторі є

віртуальною і, швидше, вторинною щодо інших просторів, для її адекватної оцінки доречно скористатися алегорією Платона про печеру: на віртуальній «стіні» «печери» кіберпростору можна бачити «тіні» реального протиборства держав (у найближчій перспективі й недержавних суб'єктів). Не залишається осторонь цих питань і Європейський Союз, інтеграцію до якого проголошено зовнішньополітичним пріоритетом України. Причому наразі ЄС фундаментально переосмислює кібербезпекову дійсність і переходить від розуміння кіберзагроз виключно як кіберзлочинів до військових і геополітичних трактувань цього явища.

Отже, держави загалом мають принципово переосмислити пріоритети національних інтересів і саморозуміння, зважаючи на те, що захист інтересів держави та нації в інформаційному суспільстві якісно вирізняється від традиційного розуміння безпеки як «стану захищеності». Оскільки світ перманентно перебуватиме під впливом різноманітних криз, то й про жодну «захищеність» у цьому світі не можна ставити питання. Ітиметься, вочевидь, лише про послаблення загроз та зниження вразливості до прийнятного рівня. Хоча цифрові кордони держав дедалі менше збігаються з їх географічними кордонами, захист цих кордонів і

цифрового суверенітету стає проблемою дедалі актуальнішою.

Україна інтегрована у світовий цифровий простір і відповідно зазнає різних загроз і негативних впливів, пов'язаних з розвитком кіберпростору (зокрема від наслідків суперництва США та КНР), що гостро актуалізує проблеми кібербезпеки на загальнодержавному рівні. Йдеться про необхідність концептуально зрозуміти нову безпекову (кібербезпекову) реальність та вирішити суто практичні питання впорядкування внутрішнього нормативно-правового поля, зон відповідальності відомств, задіяних у забезпеченні кібербезпеки держави, загалом весь комплекс проблем, пов'язаних з розбудовою ефективної національної системи кібербезпеки. Надто вже зараз Україна потерпає не лише від «традиційних» кіберзлочинів, а й від складніших кібератак. Україна має не просто сформулювати на загальнодержавному рівні власне бачення глобальних процесів, пов'язаних з розвитком кіберпростору, вона мусить віднайти себе в цих процесах. В іншому разі питанням стають перспективи державного буття Української держави в умовах «нового цифрового порядку» з його агресивно-гегемоністською компонентою «холодної війни v2.0.». На тлі формування нового простору людського буття – кіберпростору – геополітика як наукова та практична

сфера пояснення глобальних міждержавних процесів набуває якісно іншого виміру. Класичні геополітичні підходи багато в чому можуть бути застосовані до кіберпростору, але за умови їх певного корегування. Дедалі більше дослідників вважають за необхідне зосередити наукові дослідження на проблемі кібермогутності держав як здатності втілювати їх волю та забезпечувати національні інтереси в кіберпросторі. Проблема наукового осмислення та практичного використання кіберпростору супроводжується суттєвими термінологічними та нормативно-правовими питаннями. Нормативно-правові проблеми є природним наслідком термінологічних, однак виводять їх із суто наукового обговорення до сфери практичних міждержавних відносин. При цьому досі відсутні системні міжнародні нормативно-правові документи, які б чітко надавали визначення кіберпростору та всім похідним від нього поняттям сфери безпеки, принципово не визначено правовий статус кіберпростору (існує щодо всіх інших просторів), відсутній будь-який міжнародний далекосяжний консенсус щодо правил поведінки в кіберпросторі та загальноприйняті методики оцінювання наслідків кібератак та їх «прив’язування» до міжнародних норм і правил. Спроби впорядкувати ці проблеми в межах нормативно-правового поля можна вважати лише

частково успішними. Єдиним реальним документом кібербезпекового характеру є Конвенція про кіберзлочинність, однак вона, по-перше, присвячена доволі вузькому сегменту кіберзагроз (кіберзлочинам у сфері комп'ютерної інформації), а подруге є, по-суті, регіональним документом, що до того ж не сприймається значною кількістю геополітичних гравців. При цьому, найшвидше, без змін Статуту ООН і закріпленого в ньому поняття агресія такі спроби і надалі перебуватимуть поза міжнародним нормативно-правовим полем. І це незважаючи на особливу актуальність проблеми, спричинену реальною мілітаризацією кіберпростору, активним нарощуванням значною кількістю держав їхніх військових кіберпотенціалів попри численні публічні заклики до «мирного кіберпростору». Дедалі більше країн чи не офіційно починають займатися розробленням кіберозброєнь, вкладають мільярдні кошти в кібербезпековий сектор (лише США в 2013 році вклали в кіберсферу 14 млрд дол.), що спричинює нову гонку озброєнь і збільшення взаємної недовіри між геополітичними гравцями. За таких реалій дві найпотужніші держави сьогодення – КНР і США – вступають у довготривале суперництво, яке має глобальний характер і виявляється майже на всіх рівнях. Зокрема – в кіберпросторі. За таких умов

кіберпростір стає одним з важливих просторів протиборства, в т.ч. через його нормативно-правову невизначеність. Це формування створює умови для розгортання «холодної війни v2.0.» з усіма ознаками «класичної» «холодної війни»: високим рівнем латентних загострень на міжнародній арені, непрямими методами боротьби (передусім активізацією розвідувальної діяльності з обох сторін), винесенням конфліктів на територію третіх країн (наприклад у формі протистоянь за сфери впливу) та гонкою озброєнь. Фактично майже будь-яке програмне забезпечення, як, власне, й всі IT-технології, є технологіями подвійного призначення, а отже, потребують або тотального контролю, або принципово іншого підходу, ніж сучасне ставлення до «традиційних» подвійних технологій.

Маємо визнати, що міжнародні організації наразі, вочевидь, недостатньо готові до діяльності в умовах нової кіберпросторової реальності. Такі міжнародні інститути, як ООН, G7 та інші, поки що не змогл и посісти ту однозначну позицію щодо процесів у кіберпросторі, на яку очікує міжнародна спільнота. Багато в чому це пояснюється відносною ефективністю та нереформованістю цих структур на теперішньому етапі їх розвитку, однак і нинішні свої потенційні можливості й доступні механізми впливу на ситуацію

вони використовують недостатньо повно. Меншою мірою це стосується діяльності Міжнародного союзу електрозв'язку, який на практичному рівні задіяний у пошуку відповідей на глобальні кібервиклики, однак, як засвідчують події в Дубаї 2012 року, навіть у цієї організації виникають суттєві проблеми із пошуком балансу інтересів.

Доцільно розглянути питання комплексного огляду вітчизняного сектору кібербезпеки (у форматі Зеленої книги), забезпечити прийняття Стратегії забезпечення кібернетичної безпеки України та Закону України «Про кібернетичну безпеку України». Важливо сформувати загальнонаціональні міжвідомчі координаційні структури, спроможні узгоджувати та координувати діяльність різних силових відомств на час розслідування злочинів у кіберпросторі, та створити ефективну систему захисту вітчизняного кіберпростору (зокрема у військовій сфері). Сам кібербезпековий сектор має бути на якісно новому рівні забезпечений ресурсами (фінансовими, кадровими, технічними), в тому числі через створення національної операційної системи та «антивірусу», а також через відновлення вітчизняних потужностей з виробництва матеріально-технічної телекомунікаційної бази. З огляду на те, що значна кількість об'єктів критичної інфраструктури наразі є у приватній власності, конче важливим є

посилення взаємодії органів державної влади з приватним сектором, а також неурядовими організаціями та громадянським суспільством у цілому.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Дубов Д. В. Кіберпростір як новий вимір геополітичного суперництва : монографія / Д. В. Дубов. – К. : НІСД, 2014. – 328 с.

Післямова

Актуальність проекту «Європейська інтеграція: законодавство та Інтернет речей»у межах напряму Жан Моне «Модуль» програми «Erasmus+» №620017-EPP-1-2020-1-UA-EPPJMO-MODULE для України пов’язана з процесами європейської інтеграції у сфері цифрової трансформації, здебільшого, щодо процесу впровадження сучасних технологій Інтернету речей (IoT).

Йдеться про дослідження ролі ЄС у глобалізованому світі, зокрема, законодавства ЄС, яке стосується сфери інформаційних цифрових технологій в епоху розвитку досягнень четвертої технологічної революції.

Для реалізації цієї мети ми запропонували запровадити нову дисципліну - “Євроінтеграція: законодавство та Інтернет речей”. Вона призначена для залучення широкого кола студентів, науковців, представників зацікавлених державних органів і громадських та неурядових організацій, практикуючих юристів, ІТ-спеціалістів.

Залучені учасники проекту можуть набути та вдосконалити свої професійні навички з:

1) правових питань впровадження IoT;

2) законодавства ЄС у галузі інформаційних технологій;

3) порівняльно-правового аналізу національного законодавства та законодавства ЄС у сфері IoT.

Це передбачає вивчення змісту, складу, особливостей, системних ризиків та бар'єрів використання IoT, а також роз'яснення політики ЄС щодо його розвитку.

Центральними темами курсу є юридичні питання забезпечення кібербезпеки, пов'язаної з IoT, в контексті захисту критичної інформаційної інфраструктури персональних даних та ідентифікації суб'єктів та об'єктів, що стосуються технологій
IoT, використання роботів та штучного інтелекту, технологій хмарних обчислень та блокчейну.

Проект базується на інноваційних формах навчання. Це сприяє набуттю навичок самостійного пошуку, виявлення та вирішення юридичних проблем, пов'язаних із використанням IoT. У цьому проекті також впроваджений інноваційний мультидисциплінарний підхід. Це дозволяє поєднувати знання з технічних та правових аспектів IoT. Це стає можливим завдяки унікальному поєднанню професіоналів з політехнічних та юридичних дисциплін Національного технічного університету України «Київський політехнічний інститут Ігоря Сікорського».

Наукове видання

ЗБІРНИК МАТЕРІАЛІВ
конференції молодих вчених та студентів

ІНТЕРНЕТ РЕЧЕЙ: ТЕОРЕТИКО-ПРАВОВІ ТА ПРАКТИЧНІ АСПЕКТИ ВПРОВАДЖЕННЯ В УМОВАХ ЄВРОПЕЙСЬКОЇ ІНТЕГРАЦІЇ

02 листопада 2022 року

КИЇВ
2022