Міністерство інформаційної політики України

Секція правового забезпечення національної безпеки і оборони Національної академії правових наук України

Науково-дослідний інститут інформатики і права Національної академії правових наук України

Факультет соціології і права Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського»

ІНФОРМАЦІЙНА БЕЗПЕКА: СУЧАСНИЙ СТАН, ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ

МАТЕРІАЛИ І МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

20 вересня 2019 року

Київ-2019

УДК 34:004.056.5](062)
ISBN 978-966-622-971-0
І - 74

Інформаційна безпека: сучасний стан, проблеми та перспективи: Матеріали І науково-практичної конференції. 20 вересня 2019 р., м. Київ. / Упоряд. : В. М. Фурашев, С. Ю. Петряєв. – Київ : Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського» Вид-во «Політехніка». 2019. – 124 с.

Матеріали конференції присвячені розгляду теоретичних та практичних засад державної політики у сфері інформаційної безпеки, проблемам формування, оцінці стану та реалізації Доктрини інформаційної безпеки України.

Наведені матеріали можуть бути корисними для спеціалістів у сферах правотворення, правозастосування та правоохоронної діяльності, вчених, фахівців та експертів різних галузей права, науково-педагогічних працівників вищих навчальних закладів, а також усіх, хто цікавиться суспільно-правовими тенденціями сучасного науково-технічного прогресу в сфері забезпечення інформаційної безпеки.

Участь у конференції взяли провідні експерти і вчені наукових установ і навчальних закладів, представники державних органів та громадських організацій. Інформаційну підтримку у проведенні заходу надали: журнали «Інформація і право» та Вісник «КПІ ім. Ігоря Сікорського» «Політологія. Соціологія. Право»

Матеріали подано у авторській редакції.

Упорядники: Фурашев В. М., Петряєв С. Ю.

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

Рекомендовано до друку:
Вченою радою Науково-дослідного інституту інформатики і права Національної академії правових наук України. Протокол № 7 від 30.10.2019 р.

Вченою радою факультету соціології і права Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського». Протокол № 2 від 30.09.2019 р.

ISBN 34:004.056.5](062)

ЗМІСТ

ВСТУПНЕ СЛОВО

Державного секретаря
Міністерства інформаційної політики України
Біденка Артема Ігоровича

Цього року Міністерством інформаційної політики України та Факультетом соціології і права Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського» спільно з Секцією правового забезпечення національної безпеки і оборони Національної академії правових наук України та Науково-дослідним інститут інформатики і права Національної академії правових наук України започатковано традицію проведення Міжнародної науково-практичної конференції «Інформаційна безпека: сучасний стан, проблеми та перспективи».

Головна мета проведення заходу полягає в об'єднанні теоретичних та практичних засад державної політики у сфері інформаційної безпеки, а також створенні постійно діючої платформи для обміну досвідом між представниками органів державної влади, науковими установами та профільними громадськими організаціями спрямованої на налагодження ефективного співробітництва.

Запропоновані теми до обговорення особливо важливі саме в час коли проти України здійснюється гібридна агресія, яка впливає як на кожного громадянина, так і на країну в цілому.

Інформаційна сфера є ключовою та найбільш вразливою сферою з точки зору можливостей здійснення ворожих дій, адже у поширенні інформації відсутні кордони, а новітні технології дозволяють кінцевому користувачу отримати інформацію в будь-який час та в будь-якому місці.

Тому Україна продовжує вживати рішучих дій на напрямі протидії сьогоденним загрозам і формування національної системи інформаційної безпеки. Зокрема, у лютому 2017 року Президентом України підписано Указ «Про Доктрину інформаційної безпеки України», яким визначено актуальні загрози національним інтересам та національній безпеці України в інформаційній сфері, пріоритети державної політики, а також механізми реалізації.

Впевнений, що Міжнародна науково-практична конференція стане ефективним та дієвим механізмом у пошуку шляхів протидії інформаційній агресії проти України, а також спонукатиме до розвитку кооперацийних зв'язків між усіма учасниками.

Сподіваюсь, що дискусія буде конструктивною і сприятиме подальшому вдосконаленню державної політики у сфері забезпечення інформаційної безпеки України.

----------***----------

Макобрій О. О., Завідувач Сектору з питань впровадження Доктрини інформаційної безпеки Міністерства інформаційної політки України.

РЕАЛІЗАЦІЇ ДОКТРИНИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ. СТАН ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА СПРЯМОВАНІСТЬ ЙОГО ВДОСКОНАЛЕННЯ ДЛЯ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ

Конституцією України визначено, що одним із пріоритетів захисту суверенітету і територіальної цілісності нашої країни є забезпечення інформаційної безпеки. І це є найважливішою функцією держави та справою всього Українського народу.

Отже інформаційна безпека, ефективна протидія інформаційним загрозам є не тільки питанням діяльності органів державної влади, це питання об’єднання зусиль усіх сфер і напрямів: як органів державної влади, так і громадських об’єднань, наукових установ, медіа тощо.

Тому саме об’єднання зусиль є головною запорукою успіху у відсічі інформаційній агресії, яка здійснюються проти України.

На сьогодні проти Україною використовуються технології гібридної війни, що перетворило інформаційну сферу на ключову арену протистояння.

Досвід який ми вже маємо, показує, що інформація використовується як технологія ведення війни.

Фактично інформація є найважливішим компонентом агресії.

Апробуються найновіші технології впливу на свідомість громадян, спрямовані проти України.

Моніторинг медіапростору свідчить про те, що використовуються усі доступні ресурси для досягнення своєї мети – знищення України як держави.

Зокрема Росією використовуються як власні можливості у вигляді телеканалів, таких як Russia Today, Росія-24, Росія-1, Перший телеканал, так залучаються Мас-медіа багатьох інших країн.

Діє головний принцип коли демократичні механізми використовуються проти демократії.

Особливо ворожі наративи та дезінформація мають високу ефективність завдяки постійній повторюваності та мультиплікації в ЗМІ та соціальних мережах.

Саме соціальні мережі дали доступ до особистої та колективної підсвідомості. Маніпулювання, не в залежності від того де знаходяться сервери, відкривають дуже багато можливостей для «правильного» вибору дій, які необхідні агресору.

Водночас важливо розуміти, що у світі немає єдиної відповіді як боротися з дезінформацією, і також однозначно не можливо боротися з дезінформацією дзеркальними методами.

Іноді заборони та обмеження можуть бути досить ефективними у деяких випадках, проте вони завжди тягнуть за собою ризики порушення однієї із основоположних свобод – свободи слова.

Державний контроль також не є універсальним рішенням для боротьби з дезінформацією, а незалежність ЗМІ – це обов'язковий критерій для розвитку демократичного суспільства.

Разом з цим, Міністерством інформаційної політики України здійснюються заходи щодо протидії інформаційним загрозам.

Так у 2017 році Президентом України було затверджено Доктрину інформаційної безпеки.

Головна мета Доктрини полягає у виробленні єдиної державної політики щодо захисту інформаційного простору в умовах гібридної агресії.

Вперше в Доктрині обґрунтовуються такі поняття, як «стратегічні комунікації», «урядові комунікації», «кризові комунікації», «стратегічний наратив», а також визначаються національні інтереси в інформаційній сфері, актуальні загрози та механізми їх подолання.

До реалізації Доктрини активно залучено понад 30 органів державної влади, які опікуються питаннями національної безпеки в інформаційній сфері.

Виконання Доктрини пов'язане з багатьма напрямками інформаційного простору.

Саме Міністерство інформаційної політики України забезпечує координацію виконання Доктрини (це і звітування і відповідні координаційні дії щодо методологічного забезпечення).

Також на Міністерство покладено ряд завдань.

Здійснюється моніторинг ЗМІ та Інтернету з метою виявлення інформації, поширення якої заборонено в Україні.

З метою забезпечення проведення моніторингу інформаційного простору Міністерством розроблено Концепцію інтегрованої системи

оцінки та моніторингу інформаційних загроз та оперативного реагування на них.

Забезпечено розвиток урядових та кризових комунікацій.

Головна мета полягає у впровадженні власного наративу та побудові ефективної системи державних стратегічних комунікацій.

Міністерство докладає значних зусиль для створення такої системи, постійно працює з представниками органів державної влади для надання рекомендацій щодо ведення комунікаційної роботи, проводить семінари та тренінги для державних службовців.

Розроблено методичні рекомендації «Комунікаційний інструментарій для держслужбовців» та Методологію проведення комплексного моніторингу медіапростору органами виконавчої влади.

З метою реформування системи здійснення комунікацій органами виконавчої влади в умовах кризи (в т.ч. в докризовий та посткризові періоди) Міністерством підготовлено Стратегію розвитку спроможностей із кризових комунікацій в органах державної влади.

Стратегія спрямована на реформування усієї системи здійснення кризових комунікацій.

Важливим елементом інформаційної політики є медіаосвіта та медіаграмотність. Міністерство здійснює заходи спрямованих на вдосконалення здатності громадян самостійно виявляти фейки, опиратися маніпуляціям, бути готовими до змін інформаційного середовища, розвивати власне критичне сприйняття інформації.

Що правда неможливо лише медіаграмотністю зупинити розповсюдження неправдивої інформації – іноді це питання добросовісності медіа та дотримання журналістських стандартів. Тому окрема увага приділяється роботі із представниками медіа, постійно проводяться круглі столи, тренінги, семінари, навчальні курси та дискусії для журналістів.

Разом з цим, Міністерством підготовлено дослідження «Біла книга спеціальних інформаційних операцій проти України» в якій визначено та спростовано інформаційна агресія Російської Федерації. Це дослідження показує загальну концепції того, як працює російська система поширення інформації.

«Біла книга» не прописує універсального механізму боротьби проти російських фейків, проте чітко окреслює основні напрями.

Дослідження спрямоване допомогти експертам зрозуміти, які технології використовуються Росією.

Для боротьби з дезінформацією важливим є створення та провадження власного наративу.

Саме тому Міністерство активно працює, розширюючи систему іномовлення, просуває бренд «Ukraine Now», проводить за кордоном інформаційні кампанії, культурні заходи спрямовані на формування позитивного іміджу України.

Міністерством проводяться багато публічних заходів спрямованих на звільнення та реінтеграції тимчасово окупованих територій.

Розроблено та прийнято стратегії реєнтеграції Криму та Донбасу. Створюються відповідні міжвідомчі плани.

Окрема увага приділена роботі із місевим населенням Збройними Силами України, Національною гвардією України та Національною поліцією України.

З метою донесення достовірної інформації до іноземної аудиторії про події в Україні Міністерством закордонних справ забезпечено формування та реалізацію напрямків публічної та культурної дипломатії України.

Здійснюється двостороннє співробітництво з закордонними партнерами щодо протидії існуючим інформаційним загрозам.

Міністерством оборони України та Національною гвардією України забезпечено функціонування системи військово-цивільних зв'язків.

Постійно проводяться іміджеві заходи, спрямовані на інформування суспільства про завдання та службово-бойову діяльність.

Постійно підтримуються зв’язки з представниками українських та іноземних ЗМІ направлених на оперативне висвітлення ситуації у районі проведення ООС.

Здійснюються заходи щодо протидії спеціальним інформаційним операціям, спрямованим проти ЗС України.

Міністерство культури України приділяє увагу міжнаціональним відносинам та етнонаціональній політиці, популяризації державної мови, що є важливим елементом захисту інформаційного простору.

Державним агентством з питань кіно забезпечується популяризація українського кіно як в цілому в Україні так і в прифронтових містах Донецької та Луганської областей. Приділяється увага забороні відповідної кінопродукції яка шкодить національним інтересам держави.

Національна рада України з питань телебачення і радіомовлення проводить заходи які запобігають поширенню програм російських телевізійних мовників, наративи яких іноді використовують українські ЗМІ.

Окремо слід звернути увагу на потужну моніторингову діяльність, яку здійснює Національна рада.

Забезпечується обмеження доступу на український ринок друкованої продукції антиукраїнського змісту (Держкомтелерадіо).

Службою безпеки України організовано моніторинг вітчизняних та іноземних ЗМІ та Інтернету з метою виявлення загроз в інформаційній сфері. За результатом виділяються ресурси, які використовує Росія у гібридній агресії.

Реалізують та захищають національні інтереси України в інформаційній сфері за кордоном розвідувальні органи України. На постійній основі протидіють зовнішнім загрозам інформаційній безпеці держави.

Державною службою зв'язку та захисту інформації України забезпечено державна політика у сфері спеціального зв'язку, захисту інформації, телекомунікацій та користування радіочастотним ресурсом України.

Здійснюються заходи щодо законодавчого забезпечення захисту і розвитку інформаційного простору України.

Важливим напрямком є науково-експертне супроводження процесу державної інформаційної політики. На регулярній основі розповсюджуються дослідження від Національного інституту стратегічних досліджень.

Отже Органами державної влади та державними установами забезпечується виконання положень Доктрини інформаційної безпеки України.

Але слід зауважити, що існують проблеми в її реалізації, зокрема в контексті інституційної координації та загальної ідеї стратегічного бачення.

1. Тому нагальною потребою є правове закріплення міжвідомчої групи на рівні органів державної влади щодо виконання Доктрини, а також створення постійно діючих платформ для наукових установ та профільних громадських організацій.

2. Визначення подальших дій для забезпечення вдосконалення правового регулювання інформаційної сфери (зокрема щодо виконання Доктрини).

----------***----------

Сунгуровський М. В., директор військових програм Центру Разумкова, к. т. н., старший науковий співробітник.

ЧОГО БРАКУЄ ТА ЩО ПОТРІБНО ДЛЯ ПОБУДОВИ ЕФЕКТИВНОЇ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1. Бракує культури системного, технологічного мислення. Це стосується як окремих експертів,так і переважно управлінців при владі. Не вистачає

- розуміння, що поняття система не зводиться до охоплення великої кількості об'єктів, тем, аспектів, але передбачає наявність насамперед взаємозв'язків між ними;
- розуміння, що об'єктами управління є не ЗМІ, не силові структури, не підприємства оборонної промисловості, а відповідні процеси досягнення певних цілей;
- чіткого, одноманітного цілєполагання в державній політиці в термінах результатів як опису бажаного стану системи (від цього залежить, зокрема, сумісність заходів і потенційних результатів, що є складовими відповідних планів і програм);
- небажання бачити відмінності між необхідним і достатнім (робити те, що потрібно для досягнення результату, а не те, що можливо для покращення ситуації).

Без всього цього розмовляти про стратегічне планування, управління якістю та управління взагалі немає сенсу.

2. Висока турбулентність, хаотизація, невизначеність безпекового середовища та неповнота знань є одними з головних рис (гібридної) сучасності та викликами для системи забезпечення національної безпеки. Помилки та неповне охоплення всього діапазону загроз може зумовити відсутність потрібних захисних спроможностей і неефективність системи забезпечення національної безпеки (СЗНБ). ІБ як складова СЗНБ.

3. Одним із засобів боротьби з невизначеністю є структурування проблеми. Процес побудови та функціонування СЗНБ – це чітка, на рівні алгоритму, послідовність взаємопов'язаних заходів, переміщення результатів від проміжних до кінцевих. Аби побудувати такий алгоритм, потрібно дати відповіді на наступні питання:

- що захищаємо?
- від кого та від чого захищаємо?
- яким чином захищаємо?

- які спроможності потрібні для цього?
- що потрібно для набуття цих спроможностей?
- скільки це коштуватиме, які ресурси потрібні та з яких джерел?

4. Що є об'єктами захисту та в чому полягає особлива роль інформаційної безпеки.

До об'єктів впливу загроз та, відповідно, об'єктів захисту належать:

- ціннісні засади суспільства;
- національні інтереси (стратегічні цілі);
- носії цінностей та інтересів;
- процеси реалізації стратегічних цілей з усіма їх складовими (технологія, виконавці, ресурси).

У сучасних умовах інформація є одним із головних і найефективніших засобів реалізації загроз і, відповідно, чи не найважливішим об'єктом захисту.

5. Для повного опису загроз, крім об'єктів їх впливу, необхідно визначити:

- носія загрози, його мотив і мету;
- спосіб реалізації загрози, сили та засоби, що залучаються на різних етапах ескалації (виникнення протиріч, поява негативних чинників, загострення протиріч, кризова ситуація або конфлікт, наслідки кризи);
- сценарії реалізації і розв'язання кризових ситуацій.

6. Для того, щоб система захисту була ефективною, вона повинна реагувати не лише на загрози і кризові ситуації, що виникають, але й на процеси ескалації (сценарії) кризових ситуацій в усьому або в максимально широкому діапазоні. Аналіз процесу ескалації загроз і кризових ситуацій дає можливість сформулювати вимоги до потрібних властивостей (спроможностей) системи захисту. З урахуванням цих вимог формується перелік (каталог) спроможностей, що періодично коригується в залежності від змін зовнішніх і внутрішніх умов. Структура спроможності є стандартною:

- елемент(и) системи (органи, сили або їх сукупність) що реалізують спроможність;
- персонал з відповідними якостями;
- засоби (озброєння, військова та спеціальна техніка) з потрібними характеристиками;
- способи їх функціонування та види забезпечення (оперативне, логістичне);
- ресурси, потрібні для створення та реалізації спроможностей (нормативно-правові, фінансові, кадрові, інформаційні).

Потрібно розрізняти тісно взаємопов'язані процеси створення й розвитку системи та процеси її функціонування.

7. Сили та засоби СЗНБ, процеси їх застосування мають бути сумісними між собою у часовому, просторовому, технологічному та функціональному аспектах, сумісні як із силами, засобами, процесами, на базі яких вони створювалися та з якими взаємодіють зараз, так і з тими, що створюватимуться далі. Звідси випливає роль стратегування і планування.

8. Важливо зазначити, що нормативно-правове, фінансове, технічне, кадрове, інформаційне забезпечення процесів створення та функціонування системи захисту є їх проекціями у відповідну площину системи координат. Головне тут опис самих процесів, але ніяк не навпаки.

9. Найголовнішим для нової влади є навчитися як (упорядковано) мислити. Структурований опис проблеми і процесу її розв'язання є передумовою зрозумілості процесу управління як для самої влади, так і для виконавців, експертів і широкої громадськості. Лише за цих умов вміння нової влади пропонувати та застосовувати нестандартні підходи може вважатися конструктивним.

----------***----------

Дубов Д. В., Національний інститут стратегічних досліджень, завідувач відділу інформаційної безпеки та розвитку інформаційного суспільства, д. п. н., старший науковий співробітник.

ІНФОРМАЦІЙНА ПІДРИВНА ДІЯЛЬНІСТЬ: ПРОБЛЕМИ НОРМАТИВНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ПРОТИДІЇ

Захист українського інформаційного простору від деструктивної інформаційної ворожої діяльності залишається актуальним завданням, яке стоїть перед органами державної влади та сектором безпеки зокрема. Заходи протидії, які були вжиті Україною (в частин припинення трансляції російських телеканалів, мовного квотування, функціонування російських соціальних мереж тощо) вирішили лише частину питань в цій сфері. Істотною проблемою, що залишилась на порядку денному, є комплексна протидія деструктивній інформаційній діяльності, що здійснюється або за допомогою внутрішніх суб'єктів інформаційної діяльності, або через канали інформування, власники яких безпосередньо не є суб'єктами (резидентами)

України, але при цьому здійснюють тут свою діяльність (іноземні соціальні сервіси).

Хоча органи державної влади, зокрема контррозвідувальні та правоохоронні органи, здійснюють заходи з протидії ворожій інформаційній діяльності в межах своїх повноважень, але в багатьох випадках їх дії виявляються обмеженими через низку чинників. Одна з важливих причин браку ефективності - недосконаліть нормативно-правової бази, яка б регламентувала протидію інформаційній підривній діяльності проти української державності.

Основними статтями Кримінального Кодексу [] в яких, фактично, описуються види підривної інформаційної діяльності зосереджені в статтях ст.109 ч.2., ст.110, ст.111, ст.258-2, ст.258-5, ст.295, ст.436 та 436-1, ст.442 ч.2. Однак спроби їх застосування на практиці стикаються із проблемами надто широких формулювань, що майже унеможливлює доведення факту злочину. Крім того, в жодному законодавчому акті не визначено і сутність «підривної інформаційної діяльності» як окремого виду протиправної діяльності.

Водночас щодо останнього, то коментар до ст.111 «Державна зрада» Кримінального кодексу України вказує [2], що «*підривною*» є діяльність, що, зокрема, пов'язана:

- з втручанням у міжнародну політику України (наприклад, несанкціоноване відповідними органами державної влади України розірвання дипломатичних чи консульських стосунків з іншою державою, **зрив важливих міждержавних переговорів або глобальних міждержавних форумів**);
- з втручанням у внутрішню політику (організація міжконфесійних, міжетнічних та інших конфліктів, розпалювання сепаратистських настроїв серед населення окремих регіонів, фінансування, оснащення чи інше забезпечення незаконних збройних формувань на території України, організація інформаційної експансії з боку інших держав);
- зі спробою зміни території України (організація не передбачених Конституцією України референдумів тощо);
- зі спробою знизити обороноздатність України (організація і вчинення диверсій у формі дій, спрямованих на зруйнування об'єктів, які мають важливе оборонне значення, прийняття рішень про згортання наукових досліджень у галузі військової науки і техніки**, свідоме гальмування приведення мобілізаційних планів відповідно до сучасних умов**, винахід спеціальних вірусів чи внесення їх у комп'ютерні системи з

метою утруднення їхньої роботи або знищення накопиченої на магнітних носіях важливої для виконання завдань оборони інформації тощо);

- зі створенням умов для діяльності на території України іноземних розвідок (вербування агентури серед жителів України, підбір кандидатів для вербування та завчасний підкуп службових осіб, зокрема тих, що допущені до інформації «особливої важливості», підготовка явочних квартир, надання допомоги у придбанні документів прикриття для іноземних розвідників, влаштування їх на посади, пов'язані з можливістю доступу до конфіденційної інформації).

Частина з цих дій може бути віднесена до інформаційної діяльності або ж бути досягнута завдяки діями суб'єктів інформаційної діяльності, як в середині держави, так і ззовні. Більшість з перерахованих пунктів відповідають і тому, як учасники слухань з протидії фейкам у Комітеті з питань свободи слова та інформаційної політики ВРУ (28.02.2018 року) описували проблему дезінформації, з якою має боротись держава на центральному рівні [3].

Незважаючи на вище вказане, юристи звертають увагу [4], що до останнього часу Верховна Рада так і не визначила законодавчо сутність «підривної діяльності», фактично унеможливлюючи ефективне застосування цілої низки статей Кримінального Кодексу (і передусім - ст.111 «Державна зрада»), а також до певної міри ускладнюючи діяльність СБУ, до основних завдань якої віднесено «захист… законних інтересів держави та прав громадян від розвідувально-підривної діяльності іноземних спеціальних служб» [5].

Проблеми використання поняття «підривна діяльність» доводить і практика правозастосування ст.111 «Державна зрада» для випадків, коли звинувачення було висунуто саме за проведення підривної діяльності проти України (в сфері інформаційної діяльності). У переважній більшості випадків обвинуваченню не вдалось довести факт ведення «підривної діяльності», оскільки категорія продовжує залишатись розмитою.

Все це обумовлює необхідність уточнення статті 111 Кримінального кодексу України, зменшивши її варіативність і можливість подвійних трактувань. З цією метою диспозиція частини першої статті 111 має бути сегментована на кілька частин відповідно до форм, у яких може виявитись державна зрада, в т.ч. – у формі підривної інформаційної діяльності. Вочевидь це буде потребувати уточнення не лише того, що таке «підривна діяльність» та «підривна інформаційна діяльність», але і що таке «підривна організація», оскільки у більшості випадків доведення факту ведення підривної діяльності доцільніше здійснювати через факт доведення

співпраці із організаціями, що визнані Україною «підривними». При чому коло таких організацій не обмежена лише розвідувальними організаціями інших держав, але може включати в себе їх ЗМІ чи інші недержавні структури.

Список використаних джерел:

1. Кримінальний кодекс України. URL:https://zakon.rada.gov.ua/laws/show/2341-14 (дата звернення: 29.09.2019)

2. Коментар до статті 111. Державна зрада. URL: http://yurist-online.com/ukr/uslugi/yuristam/kodeks/024/109.php (дата звернення: 29.09.2019)

3. Протидія фейкам: на комітетських слуханнях експерти обговорили наболілу проблему та озвучили низку пропозицій щодо її врегулювання. URL: http://komsvobslova.rada.gov.ua/documents/sluhannja/73873.html (дата звернення: 29.09.2019)

4. Юрист-кримінолог: Депутати досі не пояснили в законодавстві, що таке підривна діяльність. URL: https://zik.ua/news/2018/05/18/yurystkryminolog_ deputaty_dosi_ne_poyasnyly_v_zakonodavstvi_shcho_take_1327537 (дата звернення: 29.09.2019)

5. Про Службу безпеки України. URL: https://zakon.rada.gov.ua/laws/show/2229-12 (дата звернення: 29.09.2019)

----------***----------

Мошко М. С., Служба безпеки України.
Прозоров А. Ю., к. ю. н., Національна академія Служби безпеки України.

АКТУАЛЬНІ АСПЕКТИ ДЕРЖАВНОЇ ПОЛІТИКИ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Аналіз суспільно-політичної ситуації в України на тлі нестабільної обстановки практично в усіх сферах життєдіяльності потребує посиленого регулювання державної політики у сфері інформаційної безпеки. У той же час, аналіз державного забезпечення ефективного функціонування такої політики як на законодавчому так і на виконавчому рівні потребує значного покращення, оскільки реакції на зовнішні інформаційні виклики та загрози як правило є не спланованими, неузгодженими, неорганізованими, повільними або бездіяльними та часом неадекватними.

Перелічені системні проблеми інформаційної безпеки України цілком можливо виправити шляхом законодавчих змін у підходах протидії викликам та загрозам, здійснення заходів для унеможливлення формування їх передумов, а також підвищення рівня компетентності та професіоналізму відповідальних за цю сферу чиновників чи інших осіб або їх заміни.

Оцінюючи проблематику законодавчої сфери регулювання інформаційної безпеки України, як і в цілому українського законодавства, є її неоднозначність і в кращому випадку, двозначність. Вказане призводить до різного тлумачення положень законодавчих актів і як наслідок, різного підходу до виконання тих чи інших процесів [1-5]. Щоправда, з одного боку різноманіття підходів є запорукою до удосконалення існуючих процедур, проте з іншого – при неправильному тлумаченні або нерозумінні кінцевої мети процесу виконання будь-якої процедури призводить до небажаних або непередбачуваних результатів.

У той же час, в аспекті забезпечення інформаційної політики держави існує великий дисбаланс: поряд з надмірними наглядом, плануванням, координацією та контролем в одних питаннях, існує повна їх відсутність в інших. Вказана проблема у державному секторі частково може бути вирішена шляхом введення громадського нагляду як за надмірно контрольованими процесами, так і за неконтрольованими. Як приклад, можна навести формування рад громадського контролю при новостворених антикорупційних інститутах за зразком демократичних країн Заходу. Водночас, такі ради в українських реаліях не завжди здатні ефективно контролювати процеси в державних органах, зокрема через корупцію або лобізм тих чи інших інтересів, в тому числі державних чиновників або бізнесу, що знову ж таки в українських реаліях, тісно переплетено. У зв’язку з цим, процедури їх формування також необхідно удосконалювати в аспектах прозорості та виборності, а не лише шляхом проведенням процедури формального конкурсу.

Для прикладу процесів з надмірним контролем та відсутністю зворотного контролю (наприклад з боку громадських рад) є функціонування органів, в яких циркулює інформація з обмеженим доступом [6]. З одного боку функція держави зі збереження такої інформації цілком виправдана, проте з іншого боку, відсутність зовнішнього контролю над визначенням тієї чи іншої інформації державною таємницею може призводити до суттєвих зловживань чиновниками.

Водночас, у даному аспекті спостерігається невелике, проте покращення, зокрема відповідно до статті 8 Закону України «Про інформацію» [7] органами СБ України було розсекречено великі масиви інформації про факти порушень прав і свобод людини і громадянина, а також оприлюднені результати техногенних катастроф за часів СРСР, які були засекречені ще КДБ СРСР. З іншого боку, спостерігається масове надання допуску та доступу до державної таємниці особам з подвійним громадянством, зокрема серед народних депутатів України, попри відповідні

законодавчі заборони, зокрема ст. 2 Закону України «Про громадянство України» [8].

Зазначені дилеми часто стають не лише в наведених прикладах, а й в ситуаціях, які потребують швидкого та оперативного реагування. На жаль, на сьогоднішній день, архаїчний бюрократичний державний механізм законодавчого регулювання інформаційної політики часто гальмує або взагалі блокує життєво необхідні реагування на сучасні виклики та загрози. У будь-якому випадку, рано чи пізно, питання створення балансу між неконтрольованими або надмірно контрольованими важелями впливу держави на процеси та прозорим громадським або іншим аудиторським наглядом над ними стане на порядку денному України. І в першу чергу це стосуватиметься регулювання державної політики у сфері інформаційної безпеки, оскільки її функціонування виключно за рахунок державних механізмів стане неможливим, або неефективним без залучення громадського сектору.

Список використаних джерел:

1. Меморандум про гарантії безпеки у зв'язку з приєднанням України до Договору про нерозповсюдження ядерної зброї від 05.12.1994 № 998_158. URL : http://zakon3.rada.gov.ua/laws/ show/998_158

2. Протокол за результатами консультацій тристоронньої контактної групи щодо спільних кроків, спрямованих на імплементацію мирного плану президента України Петра Порошенка та ініціатив президента Росії Володимира Путіна від 05.09.2014. URL : http://www.osce.org/ru/home/ 123258?download=true

3. Меморандум про виконання положень протоколу за результатами консультацій Тристоронньої контактної групи щодо спільних кроків, спрямованих на імплементацію мирного плану президента України Петра Порошенка та ініціатив президента Росії Володимира Путіна від 19.09.2014/ URL : http://www.osce.org/ru/home/ 123807?download=true

4. Комплекс заходів по виконанню Мінських домовленостей від 12.02.201/URL : http://www. osce.org/ru/cio/140221?download=true.

5. Рамкове рішення тристоронньої контактної групи про розведення сил і засобів від 20.09.2016/ URL : https://www. osce.org/ru/cio/266271?download=true.

6. Закон України «Про державну таємницю», редакція від 05.08.2018 № 3855-XII/ URL : https://zakon.rada. gov.ua/laws/show/3855-12

7. Закон України «Про інформацію», редакція від 16.07.2019 № 2657-XII. URL : https://zakon.rada.gov.ua/ laws/show/ 2657-12

8. Закон України «Про громадянство України», редакція від 25.08.2019 № 2235-III/ URL : https://zakon.rada.gov.ua/ laws/show/2235-14

----------***----------

Солончук І. В., старший викладач ФСП КПІ ім. Ігоря Сікорського.

ІНФОРМАЦІЙНЕ СУДОЧИНСТВО ЯК ЕЛЕМЕНТ ДЕРЖАВНОЇ ІНФОРМАЦІЙНОЇ ПОЛІТИКИ ТА ЇЇ СКЛАДОВОЇ – ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

«Інформаційне суспільство –
суспільство особливе,
яке ще не було відоме історії»
В. А. Копилов [1, с. 16].

Конституція України в статті 3 проголошує безпеку людини як одну із найвищих соціальних цінностей, поряд із життям людини, її здоров'ям, честю, гідністю та недоторканністю. В умовах сучасного суспільства, тобто суспільства інформаційного, поняття безпеки має багатогранний характер та включає розуміння інформаційної безпеки.

Також Конституція України закріплює, що права і свободи людини та їх гарантії визначають зміст і спрямованість діяльності держави [2]. Забезпечення інформаційної безпеки має стати пріоритетним напрямком правоохоронної діяльності в контексті національної безпеки України. Проте, незважаючи на сучасні виклики, методологічні та нормативні розробки даного питання, не задовольняють нагальних потреб. Вважаємо доцільним звернути увагу, що сьогодні не існує спеціального нормативно-правового акту, спрямованого на врегулювання суспільних відносин в сфері інформаційної безпеки. Таку прогалину нормативного регулювання маємо сміливість пояснити тим, що інформаційне право – порівняно молода галузь права, яка розвивається надшвидкими темпами.

Наукою інформаційного права поняття інформаційної безпеки розглядається неоднозначно: по-перше, як стан захищеності систем обробки і зберігання даних, при якому забезпечується конфіденційність, доступність та цілісність інформації; по-друге, як комплекс заходів, спрямованих на забезпечення захищеності інформації від несанкціонованого доступу, використання, оприлюднення, руйнування, внесення змін, ознайомлення, перевірки, запису або знищення [3]; по-третє, як стан захищеності інформаційного середовища суспільства, який забезпечує його формування, використання й розвиток в інтересах громадян, організацій, держави; по-четверте, як стан захищеності потреб в інформації особи, суспільства й держави, при якому забезпечується їхнє існування та

прогресивний розвиток незалежно від наявності внутрішніх і зовнішніх інформаційних загроз [4].

Зважаючи на неоднозначність наукової думки та відсутність конкретизованих та обґрунтованих визначень, вважаємо дану термінологію дискусійною. Правовий вакуум у регулюванні інформаційної безпеки є одним із внутрішньодержавних дестабілізуючих факторів, що породжує інформаційні загрози.

Водночас статтею 55 Конституції України проголошується, що в Україні права і свободи людини і громадянина захищає суд. Дане положення передбачає, що кожній особі держава гарантує право на оскарження в судовому порядку рішень, дій чи бездіяльності органів державної влади, органів місцевого самоврядування, посадових і службових осіб [2].

Але ж за даними Центру політико-правових реформ станом на червень 2019 р. за результатами опитування, проведеного соціологічною службою Центру Разумкова спільно з Фондом «Демократичні ініціативи» імені Ілька Кучеріва, українські суди загалом мають негативний баланс довіри-недовіри у суспільстві, зокрема: довіряє судам 14% населення, тоді як не довіряє 75% населення [5]. Зважаючи на такі негативні показники та постійні реформи судової влади, які тривають з часу утворення незалежної держави Україна, вважаємо за доцільне розглядати судочинство в новому аспекті, зокрема в контексті інформаційного суспільства, в якому були б враховані всі можливості новітніх інформаційних технологій.

Судочинство як самостійна галузь державної діяльності, має важливе та особливе значення. Адже виключно суди здійснюють правосуддя в Україні, а також, згідно ч. 1 ст. 124 Конституції України, не допускаються делегування функцій судів, а також привласнення цих функцій іншими органами чи посадовими особами [2]. Змістовне наповнення поняття судочинства в його широкому розумінні не обмежується лише реалізацією судами повноважень у процесуальній формі, а охоплює різноманітні питання, зокрема щодо організації судоустрою, суддівського самоврядування, взаємовідносин судів з органами законодавчої та виконавчої влади, правил добору суддів, поведінки, відповідальності, звільнення тощо. Всі ці елементи є частинами єдиного механізму, покликаного забезпечити життєдіяльність ефективної та доступної судової системи [6, с. 9]. Такий особливий конституційний статус судів та судової влади вимагає виважених підходів до реформування судочинства. Адже не завжди нововведення є ефективними, вчасними, дієвими та результативними.

Однією з ознак інформаційного суспільства є переведення максимальної кількості комунікацій звичайної життєдіяльності людини в електронну, інформаційну форму. Судочинство є однією з таких сфер [7, с. 4]. Але в інформаційному суспільстві судочинство вже не можливо сприймати в тому «класичному» вигляді, як це мало місце ще кілька років тому. Сучасний розвиток суспільних відносин вимагає нового судочинства – інформаційного судочинства. Не претендуючи на однозначність, вважаємо за доцільне розглядати поняття «*інформаційне судочинство*», що включає встановлений законом порядок здійснення правосуддя в справах, які виникають з інформаційних правовідносин. Інформаційне судочинство охоплює весь комплекс процесуальних дій, зокрема подання заяв, скарг, прийняття рішень учасниками процесуальних дій, оскарження, перегляд рішень, порядок виявлення, розслідування злочинів, передачі матеріалів кримінальних справ до суду тощо), пов'язаних з порядком розгляду та вирішення судом справ щодо спорів, які виникають з правовідносин, обумовлених процесами забезпечення обороту інформації. Таким чином, інформаційне судочинство слід розглядати як комплекс взаємопов'язаних заходів, що застосовуються з метою організації судоустрою та правосуддя в справах, які виникають з інформаційних правовідносин.

Підсумовуючи викладене вище, можемо стверджувати, що чинний Закон України «Про судоустрій і статус суддів» має містити положення щодо інформаційного судочинства, а тому потребує внесення деяких змін. На наш погляд відправлення інформаційного судочинства має належати до юрисдикції відповідного вищого спеціалізованого суду, зокрема Вищого суду з питань інтелектуальної власності, а також на основі спеціалізації місцевих загальних та апеляційних загальних судів. Безумовно, що ефективність інформаційного судочинства залежить не лише від системи судоустрою та спеціалізації судів, але і від системи законодавства в інформаційній сфері та його термінологічного апарату. Логічність структури, виключення дублювання, уникнення неоднозначності трактування нормативних положень є головною запорукою функціонування та ефективності інформаційного судочинства. Великі сподівання на покращення правового регулювання інформаційних правовідносин викликає новий етап правової реформи, започаткованої Указом Президента України № 584/2019 від 7 липня 2019 р., одним із напрямів якої є підготовка та узагальнення пропозицій стосовно змін до Конституції України, законодавства про організацію судової влади, здійснення правосуддя та статус суддів, законодавства про кримінальну відповідальність та

кримінального процесуального законодавства, а також стосовно розвитку юридичної освіти, реформування органів правопорядку [8].

Список використаних джерел:

1. Копилов В. А. Информационное право: учебник. Изд. 2-е, перераб. и доп. Москва: Юрист, 2002. 512 с.

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

3. Інформаційна безпека. *Інформаційна безпека особистості:* веб-сайт. URL: https://sites.google.com/site/infobezpekaosobu/informacijna-bezpeka (дата звернення: 20.09. 2019).

4. Інформаційна безпека. Вікіпедія - вільна енциклопедія. URL: https://uk.wikipedia.org/wiki/Інформаційна_безпека (дата звернення: 20.09. 2019).

5. Судова реформа очима громадян: що може позитивно вплинути на довіру до суду? *Центр політико-правових реформ*: веб-сайт. URL: http://www.pravo.org.ua/ua/news/20873806-sudova-reforma-ochima-gromadyan-scho-mogee-pozitivno-vplinuti-na-doviru-do-sudu (дата звернення: 19.09.2019).

6. Європейські та міжнародні стандарти у сфері судочинства: Збірка європейських та міжнародних стандартів у сфері судочинства / Проект Агентства США з міжнародного розвитку (USAID) «Справедливе правосуддя», Проект ЄС «Підтримка реформ у сфері юстиції в Україні»: Київ, 2015. 708 с.

7. Бринцев О. В. «Електронний суд» в Україні. Досвід та перспективи: монографія. Харків: Право, 2016. 72 с.

8. Питання Комісії з питань правової реформи: Указ Президента України від 7 липня 2019 №584/2019. URL: https://zakon.rada.gov.ua/laws/show/ 584/2019 (дата звернення: 20.09.2019).

----------***----------

Дранник В. А., викладач
кафедри філософії ФСП КПІ
ім. Ігоря Сікорського.

ЩОДО ПИТАННЯ ПРО ІНФОРМАЦІЙНУ БЕЗПЕКУ

З розвитком техніки та науки дедалі актуальним сьогодні є стан правового забезпечення інформаційної безпеки, а також вдосконалення та підвищення її ефективності.

Теоретичні та практичні засади державної політики у сфері інформаційної безпеки, безумовно, мають велике значення для всієї держави та для кожної людини зокрема. Зараз, в вік нових інформаційних технологій, гостро стоїть питання про інформаційну безпеку стосовно інформації, яку

людина отримує і стосовно тієї, яку вона сама надає. Складність полягає в тому, щоб забезпечити повну інформаційну безпеку для людини у вірі інформаційного океану. Дуже важливо її захистити від неякісної інформації та забезпечити повну конфіденційність персональних даних.

Вельми актуальним є формування та реалізація державної політики у сфері інформаційної безпеки. Повинна бути зацікавленість на вищих щаблях влади у застосуванні ефективної політики у сфері існуючих питань, щодо ефективної інформаційної безпеки. Ґрунтовна реалізація державної політики в інформаційній сфері - запорука інформаційної безпеки держави.

Постає проблема складності у розпізнаванні достовірної чи не достовірної інформації та її вплив на морально-етичний стан людини, а також правове регулювання та захист персональної інформації особи, яке потребує дієвого вирішення.

Подальші напрями розвитку цієї теми можуть бути направлені на вдосконалення стану правового забезпечення інформаційної безпеки та вдосконалення і підвищення ефективності інформаційної безпеки, а саме, підвищення рівня правової обізнаності населення з питань інформаційної безпеки, забезпечення контролю з питань отримання, обміну, розповсюдження, використання інформації. Треба звернути увагу на те, що підвищення правової культури кожної людини сьогодні - це складова її успішності в майбутньому.

----------***----------

Федорова І. І., к.ф.н. професор
ФСП КПІ ім. Ігоря Сікорського.

ПРАВОВІ ТА МОРАЛЬНІ ЗАСАДИ РЕГУЛЮВАННЯ МЕДІАПРОСТОРУ – ФАКТОР ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОЇ БЕЗПЕКИ ЛЮДИНИ.

За умов потужного розвитку телекомунікаційних систем, які забезпечують багатовимірні можливості медіа каналів комунікації, що породжують “інформаційний вибух”, як технологію функціонування інформаційного суспільства XXI століття. Феномен інформації стає визначальним мірилом вибудовування аксіосфери соціуму, але у її континуумі критерієм формування системи суспільних цінностей виступає аксіологійний релятивізм, який свідчить про “деаксіологізацію” культури. Оскільки під тиском лавиноподібного шквалу “інформаційного шуму” нехтують адекватністю змісту інформації і навіть людина, що здатна

критично аналізувати медіа-інформаційний месседж не завжди може орієнтуватися у потоках інформації та довіряти її достовірності.

Суспільство сьогодення гіпертрофуючи технології споживання інформації програмує людину, як стереотипного користувача інформаційного міксту, який поглинаючи інформаційний потік, не потребує його аналітичного осмислення і конструктивного використання. Значні об'єми спеціально створених (запрограмовано - спрямованих) смислів інформації, що транслюються політично-заангажованими каналами у медійному просторі ширяться і вкорінюються у свідомість людини, значно швидше, ніж смисли і орієнтири, які вона отримує із власного безпосереднього життєвого досвіду. Нагальною проблемою сучасності, є збереження психологічного потенціалу особистості від загроз культивування уніфікованих (часто завуальованих) різновидів інформаційної небезпеки, яка продукується пресингом неадекватних впливів медіа-інфосфери.

Медіа технології розглядають, як преферентну загроза інформаційній безпеці людини, яку можна експлікувати як "сукупність умов і факторів, що впливають на інформаційну сферу, здійснюють негативний (деструктивний) інформаційно-психологічний вплив або/та загрожують реалізації законних прав і свобод людини[1, 8], а відповідно і державі у якій вона живе, дестабілізуючи суспільні інститути в цілому.

Інформаційна безпека людини і суспільства в просторі домінування медіакомунікацій стає визначальним напрямом розвитку не тільки IT галузей, а й сучасної гуманістики. Інформаційна ера, попри усі здобутки технічного прогресу, продукує гуманітарний розрив між технологіями інформаційно-комунікаційного потенціалу і їх деструктивними впливами на людину. "Відбувається конвергенція технобуття з гіперпростором людської культури, яка свідчить про перехід на якісно новий рівень розвитку. У такий спосіб формуються гібридні середовища"[2,68]. У віртуальному і реальному просторах створюються нові панкомунікації, які загрожують інтелектуальному суверенітету особистості, її психологічному стану, формують нові орієнтири поведінки, ревалоризують моральні цінності і правові устої соціуму. Медіапростір (особливо Інтернет) відкриває значні можливості реалізації різноманіття видів інтер-активності людини, але містить скриту небезпеку – деформацію у структурі свідомості особистості, вона втрачає здатність адекватно сприймати реальність, свідомо обирати інформацію ролевантно своїм переконанням, опиратися і протистояти маніпулятивним технологіям інформаційного впливу.

Суспільство потребує нової філософії медіакультури, стратегії розвитку якої, мають ґрунтуватися на засадах комунікативної етики консенсусу та співіснування, що забезпечить “пріоритет духовно-практичного розуму над розумом техно-практичним” (І.Кант). Нагальним завданням є також, розробки і запровадження правових норм функціонування медіапростору, задля врегулювання соціальних суперечностей викликаних колом проблем, пов’язаних із інформаційною безпекою і небезпекою, як джерелом дестабілізації соціальних процесів сьогодення.

Список використаних джерел:

1.Архіпова Є.О. Інформаційна безпека: соціально-філософський вимір // Автореферат дисертації канд. філос. наук. // К: -2012.- С. 16.

2.Рижко Л.В. Розвиток новітніх технологій і трансформація онтологічних категорій // Наука і наукознавство. К:- №2.- 2015. – С. 66-72.

----------***----------

Верголяс О. О., аспірант НДІ Інституту інформатики і права НАПрН України виконавчий директор ІА “Петро і Мазепа медіа”.

СПЕЦІАЛЬНІ ІНФОРМАЦІЙНІ ОПЕРАЦІЇ У ВЕДЕННІ ІНФОРМАЦІЙНОЇ ВІЙНИ

Невпинний рух світової цивілізації в інформаційну епоху розвитку обумовлює актуальність проблеми інформаційного протиборства як у науці, так і в діяльності органів державного й військового управління щодо забезпечення інформаційної безпеки та національної безпеки в цілому. В сучасних умовах особливої актуальності та небезпечності набувають загрози інформаційній безпеці та, власне, інформаційні загрози.

Зважаючи на те, як Закон України «Про національну безпеку України» визначає загрози національній безпеці України [1], під загрозами інформаційній безпеці можемо розуміти явища, тенденції і чинники, що унеможливлюють чи ускладнюють або можуть унеможливити чи ускладнити реалізацію національних інтересів та збереження національних цінностей України, а також досягнення національних цілей України в інформаційній сфері. Таке визначення дозволяє припустити, що загрози інформаційній безпеці можуть мати досить різну природу, причому не завжди інформаційну. Тож варто виокремити суто інформаційні загрози із загального спектру загроз інформаційній безпеці - під інформаційними

загрозами можемо розуміти інформаційні впливи технічного або психологічного характеру, що унеможливлюють чи ускладнюють або можуть унеможливлювати чи ускладнювати збереження національних цінностей, реалізацію національних інтересів та досягнення національних цілей України. Особливістю інформаційних загроз є те, що впливаючи безпосередньо на інформаційну сферу, вони можуть нести негативні наслідки для будь-яких складових національної безпеки.

Сьогодні реалізація інформаційних загроз в ході інформаційного протиборства відбувається у формі війн нового покоління, які одержали назву інформаційних.

Інформаційна війна, з урахуванням існуючих точок зору на її природу, може бути визначена як сукупність цілеспрямованих інформаційних впливів, що здійснюються суб‘єктом впливу на інформаційні системи або соціальні процеси з використанням засобів інформаційних технологій, інформаційних ресурсів і комунікацій шляхом створення факторів гальмування сталого розвитку або трансформації стабільності держави, суспільства, людини з метою втримання (досягнення) панування, переваги, монополії в різних сегментах людського буття [2]. Специфічною ознакою інформаційної війні є застосування інформаційної зброї [3], під якою розуміють способи цілеспрямованого інформаційного впливу на супротивника, рефлексивного управління ним з метою зміни його задуму на проведення стратегічних або тактичних дій у потрібному напрямку[4-5].

Інформаційну зброю характеризує передусім її цільове призначення і адресний контекст, адже фіксованих форм та змісту вона не має. Так, інформація «стає» інформаційною зброєю в разі включення до цілеспрямованої програми впливу на інформаційну систему, здатної призвести до досягнення запланованих суб’єктом впливу результатів. Як інформаційна зброя можуть використовуватися й інформаційні технології - не лише як потенційно призначені для обробки, передачі та виконання інших запланованих дій з інформацією, а й у поєднанні з передачею адресатові інформації певного характеру, зокрема, задля впливу на інформацію, що циркулює в інформаційних системах, або її одержання. Застосування інформаційної зброї та настання в результаті запланованих наслідків опосередковуються належним сприйняттям змісту інформаційного впливу тією мішенню, проти якої інформаційну зброю було застосовано.

Нищівна здатність інформаційної зброї та її цільове призначення є контекстно залежними від якостей мішені, а також визначаються потенційною спроможністю ефективно викликати в стані, структурі або поведінці мішені інформаційного впливу наслідки, бажані для суб’єкта впливу.

Інформаційна зброя є засобом здійснення інформаційних операцій, які, у свою чергу, визначають організаційну форму ведення інформаційної війни. Під інформаційними операціями традиційно розуміють дії, що застосовуються для досягнення інформаційних переваг у забезпеченні воєнної стратегії шляхом впливу на інформацію, інформаційні системи та інформаційну інфраструктуру супротивника з одночасним посиленням забезпечення безпеки власної інформації, інформаційних систем та інформаційної інфраструктури [6] (мова йде не лише про інформаційне супроводження традиційних війн або інформаційну війну як інструмент геополітичних змін, але й про будь-які прояви інформаційної війни). Основні цілі інформаційних операцій, які ведуться у військовий та у мирний час, полягають у створенні в супротивника неадекватного сприйняття реальної обстановки й порушенні його можливостей з управління військами [7]. На відміну від суто пропагандистських заходів, вони мають обмежену у часі тривалість, підпорядковані конкретній меті та координуються єдиним центром – спеціальними службами [8]. Фактично, за наявності у інформаційних операцій такого координуючого центру, мова має йти про спеціальні інформаційні операції, під якими слід розуміти комплекс акцій з реалізації інформаційних загроз або відвернення чи нейтралізації таких загроз з боку супротивника з використанням інформаційної зброї [9-10], які можуть проводитись як в ході наступальної, так і в ході оборонної війни. Наступальна інформаційна війна припускає використання ініціатором різноманітних засобів і методів впливу на інформаційні системи супротивника з метою зниження ефективності функціонування його системи прийняття рішень, тоді як оборонна - передбачає проведення спеціальних інформаційних операцій з використанням засобів і методів протидії ефективному застосуванню інформаційної зброї супротивником [11-12]. Використання спеціальних інформаційних операцій в ході оборонної інформаційної війни дозволяє розглядати їх не лише як інструмент нападу, але й як засіб забезпечення національної безпеки. Також слід зауважити, що спеціальні інформаційні операції можуть носити як інформаційно-технічний, так і інформаційно-психологічний характер, охоплюючи всі напрямки ведення інформаційної війни.

В умовах сьогодення основа функціонування управлінського механізму забезпечення національної безпеки та його ефективність передусім залежить від ефективності функціонування підсистеми інформаційного забезпечення. Тож усвідомлення виняткової небезпеки й руйнівної (передусім на рівні системи державного управління, критичної інфраструктури та інформаційно-психологічної безпеки людини) сили

інформаційної війни вимагає більш глибокого дослідження цього феномена, й передусім – підстав, форм та методів проведення спеціальних інформаційних операцій, у контексті права, оскільки це явище перешкоджає не тільки розвитку інформаційного суспільства, але й торкається усіх сторін життєдіяльності людської цивілізації, як на рівні окремих держав, так і на глобальному рівні.

Список використаних джерел:

1. Закон України «Про національну безпеку України» від 21 червня 2018 року: URL : http://zakon0.rada.gov.ua/laws/ show/2469-19/ paran355#n355(дата звернення 16.07.2018).
2. Коцюбинская Л.В. Понятие «информационная война» в современной лингвистике: новые подходы: URL : https://cyberleninka.ru/article/n/ponyatie-informatsionnaya-voyna- v-sovremennoy-lingvistike-novye-podhody (дата звернення 13.11.2018);
3. Манойло А.В. Государственная информационная политика в особых условиях. -М.: МИФИ, 2003. - 388 с.
4. Манойло А.В., Петренко Л. И., Фролов Д. Б. Государственная информационная политика в условиях информационно-психологической войны. — М., 2003. - С. 208.
5. Ж. Мина, А. Яновська та О.Матвійчук. Інформаційна зброя як інструмент впливу на сучасне суспільство: URL : http://ena.lp.edu.ua/bitstream/ntb/33315/1/34-84-85.pdf (дата звернення 25.11.2018).
6. С. Макаренко. Информационное противоборство и радиоэлектронная борьба в сетецентрических войнах начала XXI века: URL: https://psyfactor.org/t/Makarenko_InfPro_2017.pdf (дата звернення 03.12.2018).
7. Деньщиков А. Л. Информационная стратегия США (анализ, стратегия, перспективы): дисс. ... канд. педаг. наук. - М, 2008. - 186 с.
8. Литвиненко О.В. Інформаційні впливи та операції / О.Литвиненко. – К.: ВКФ. Сатсанга, 2003. – 240 с.
9. Заруба О.Г. Планування спеціальних інформаційних операцій/ О.Заруба// Інформаційна безпека людини, суспільства, держави. – 2017. – № 1 (21). – С.140-154.
10. Петрик В.М. Сутність і особливості проведення спеціальних інформаційних операцій та акцій інформаційного впливу: URL : http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/sitsbo_2009_3_15.pdf. (дата звернення 23.12.2018).
11. Цымбал В.И. О концепции информационной войны// Информационный сборник «Безопасность». М., 1995. № 9. - С. 35-38/
12. Прохожев А.А., Турко Н.И. Основы информационной войны// Анализ систем на пороге XXI века: теория и практика. М, 1996. - С. 252-253.

----------***----------

Джердж С., к. політ. н.,
голова ГС «Всеукраїнська Громадська Ліга Україна-НАТО».

ІНФОРМАЦІЙНА ВІЙНА РОСІЇ ПРОТИ УКРАЇНИ. АСИМЕТРИЧНА ВІДПОВІДЬ

В терміні «інформаційна війна» – ключове слово інформація. Інформація розрахована на свідоме сприйняття. Проте лише 15% інформації ми сприймаємо свідомо, а 85% будь-якого інформаційного повідомлення ми сприймаємо в площині несвідомого. Слова формують образ. Образ викликає в нас емоцію, в якій немає місця раціональним міркуванням.

Емоції, що повторюються, формують стійку реакцію та запускають асоціативний ряд. Таким чином формуються стереотипи сприйняття.

В гібридну війну Україна занурилась без підготовки, в період коли держава була деморалізована. Проте росіянам не вдалося абсолютно перемогти на інформаційному фронті.

В попередні роки російські ЗМІ тисячі раз розповідали про звірства нацистів. А сьогодні, показуючи окремі кадри про українських солдат, російські телевізійні фокусники домальовують знаки СС на їхні каски, формуючи цілий ланцюг негативної реакції. Так працюють медійні технологи, які ведуть проти України інформаційну війну.

Дійшло до штучного створення новин про Україну за допомогою імітації та акторів. Потрібно детально розбиратись у впливі ЗМІ на особистість і на суспільство, щоб ефективно протидіяти інформаційному тероризму.

Технологія інформаційної війни – це сегментування аудиторії. Інформаційна або смислова війна спочатку перемагає розум і лише згодом територію.

Важливим є заборона пропагандистських каналів. Багато контраверсійного контенту мають і українські телеканали – це залежить від соціальної відповідальності бізнесу. Проте медіа власників необхідно спонукати до дотримання громадянської позиції.

Інформаційна війна та війна реальна поєднані. І не відомо ще яка частина відіграє головнішу роль. В Росії вся інформаційна стратегія підпорядкована одному задуму і одному центру прийняття рішень та діє в комплексі з іншими чинниками: військовою складовою, економічним тиском, енергетичним шантажем.

В демократизацію Росії вкладені величезні зусилля та кошти. Проте життя показало, що це не дало результату. Кремль вважає, що Інтернет є головним місцем прориву західної ідеології в Росію, бо все інше під контролем.

Майже вся риторика в російських ЗМІ антиукраїнська. Україна не подається як суб'єкт міжнародної політики. Пропагандист Олександр Дугін закликає до екстермінації (знищення) українців. І це показують російські телеканали. Їхні головні тези: всі пострадянські країни не здатні самостійно вижити, і не можуть жити без допомоги РФ.

Російська пропаганда є правонаступницею радянської пропаганди. Вона вдосконалювалась і сьогодні досягла свого максимуму.

Кремлівська дезінформація постійно підтримується і тиражується, а ми часто після першої реакції заспокоюємось. Росіяни в інформаційні війні йдуть на крок попереду нас. Наша альтернатива – це відкритість влади в країні як протидія корупції та реальні зміни. Україна має чимало викликів для розбрату всередині (релігія, мова, географія), але протидією може бути міцний зв'язок між суспільством і владою на підставі взаємної довіри. Один із напрямків російської пропаганди – відчужити громадян від держави. В Росії насправді проблеми ще більш глибші, якщо говорити про конфесійні, мовні, національні, економічні проблеми. Ми повинні інформувати, що відбувається в РФ.

Захід має труднощі із відповіддю Росії. Європа зайняла позицію умиротворення агресора. Затягується прийняття рішень. Всі думають, якби не вийшло щось на гірше. Проте в умовах війни важливо наскільки ми вчасно і правильно реагуємо. Путінська інформаційна система врізається в політичні інституції Заходу та несе небезпеку. Усвідомивши, що зараз відбувається в Україні, ми краще розуміємо, що відбулось в Грузії та Молдові.

Російська тактика інформаційної війни – це напад. Україна здійснює тактику захисту. Постійно обороняючись ми програємо. Необхідна ініціатива, контратаки. Потрібно викривати ті проблеми в Росії, які сприймаються як стереотипи. Всі думають, що правда – це завжди захист, а потрібно іноді нападати правдою. Війна це не лише захист і напад, це і війна на території противника.

Прийняття рішень в РФ швидше, ніж в Україні. Час ввести корективи в систему прийняття рішень для протидії російському тиску. Оперативність та терміновість комунікації надважлива, адже важливо хто сказав перший.

Існують міжнародні конвенції щодо заборони хімічної зброї, протипіхотних мін, тепер є необхідність прийняти міжнародний запобіжник для протидії інформаційній агресії.

Важливим є питання іномовлення на російськомовний інформаційний простір. Росія закривається від всіх. Але потрібно протидіяти. Частково цю функцію розпочав канал UA. Важливо взагалі транслювати загальноукраїнські канали на Східну Європу та колишні радянські республіки.

Треба більше креативних ідей від України. Потрібно самим більше себе показати позитивно. Більше уваги цікавим історіям, які базуються на фактах.

Збільшити потужність телеретрансляційних центрів на територіях, що межують із захопленими землями. Збільшити глибину поширення сигналу українських радіоканалів на захоплені території. Створити нові студії донецького та луганського телебачення, замість тих які були захоплені терористами.

Адже телебачення дає ефект одночасного виходу на масового глядача на відміну від Інтернету, і за рахунок візуалізації стає потужним засобом інформаційної війни.

Україна набуває досвіду і цей досвід починає принципово змінювати ситуацію.

Люди не хочуть інформацію сприймати лише читаючи та дивлячись, а хочуть спілкуватись, комунікувати. Є стереотипи сприйняття. Слухають те, що хочуть почути. Новини подаються як розвага. Розвага більше подобається ніж правда. Відбувається зміщення в сторону форми, а не змісту. Варто брати важливі факти і робити з них факти цікаві, які сприймаються значно легше.

Ефективно протидіяти інформаційній війні зможуть підрозділи психологічних операцій. Центр формує головний вектор, але виконання ефективне, коли воно децентралізоване. Комунікативна стратегія кожного повинна бути частиною загальної стратегії. Меседж який ми створюємо, треба повторювати багато разів. Різні історії, різні теми, які мають різні складові, повинні бути підпорядковані одній стратегії.

Головна стратегія - показати якою ми хочемо бачити нову Україну.

----------***----------

Петряев С. Ю., к.ю.н., доцент,
заведующий кафедры
информационного права и права
интеллектуальной собственности
КПИ им. Игоря Сикорского.
kipp_fsp_kpi@ukr/net

ВЛИЯНИЕ ИНФОРМАЦИОННОГО «МУСОРА» НА БУДУЩЕЕ ЧЕЛОВЕЧЕСТВА

Мы, человечество, никогда не задумываемся о многих своих поступках до момента, пока не сталкиваемся с проблемами, которые начинают нарушать нормальный ритм нашего существования, вплоть до угрозы физического выживания. Мы возвели себя в ранг богов и пытаемся создать свой новый мир, постоянно забывая, что мы всего лишь маленькая часть другого мира, гораздо большего. Мы строим заводы, чтобы облегчить себе жизнь и при этом выбрасываем в атмосферу тысячи тонн отравляющих веществ и углекислого газа; мы сбрасываем отходы производства в реки, озера, моря и океаны, а потом спохватываемся, что в мире не хватает питьевой воды, а запасы рыбы в мировом океане на грани исчезновения; мы добываем полезные ископаемые и нарушаем экосистемы земли, а потом начинаем бороться за выживание флоры и фауны, «латаем» озоновые дыры и ломаем головы как восстановить изменившиеся погодные условия. Лишь в условиях критического «удушья» мы начинаем заключать международные договоры, подписываем протоколы, меморандумы, рамочные конвенции по охране окружающей среды, о трансграничном загрязнении воздуха на большие расстояния, охране озонового слоя, стабилизации концентрации парниковых газов в атмосфере, охраны водных и живых ресурсов, экосистем и многие другие, призванные хоть как-то остановить процесс сползания цивилизации к глобальной катастрофе.

Информация всегда была для человечества важнейшим условием для выживания, как вода и воздух или окружающая среда, продовольствие и энергоносители. В условиях четвертой технической революции информация превратилась в ресурс, обеспечивающий жизнедеятельность современного общества и ее потоки, растут в геометрической прогрессии. Если в физическом плане ресурсный объем информации занимает все меньше места, т.к. емкость носителей увеличивается очень быстро, а их размеры остаются теми же, то в контентном плане уже сейчас происходит ее «захламление», так как формируется значительная часть невостребованной

информации. Таким образом, вопрос о том, что же делать с этой «мусоркой», все чаще становится темой для обсуждения.

Как нам кажется, если объемы хранения информации не имеют значения, то, следуя процессу развития гедонизма народных масс, «*пусть идет как идет*», право на информацию пока никто не отменял, народ имеет право на развлечение.

Другой, более важной проблемой виртуального информационного пространства является вопрос о достоверности контентного материала, который искажается как естественным путем повседневных общественных отношений, так и в условиях конкуренции в бизнесе, политике или информационных войнах, «где все методы хороши» для достижения хоть маленькой победы.

Исходя из этого, многие люди все чаще задаются риторическим вопросом, сколько же в виртуальном мире «лжи»? На наш взгляд, в виртуальном мире ровно столько лжи, сколько в реальном мире, ибо он (этот самый виртуальный мир) наше творение, человек пока на создал себе подобного.

На протяжении всей истории цивилизации ложь была способом социально-биологической защиты человека и выступала неотъемлемым условием его выживания. Некоторые считают, что люди начали врать друг другу, как только научились говорить, хотя, если посмотреть на данное явление более детально, то можно заметить, что речь для обмана не всегда нужна, ее корни лежат куда глубже: даже звери обманывают друг друга, чтобы выжить.

Мы лжем в школе из-за прогулов, а дома, чтобы не наказали, мы лжем о любви ради любви, мы лжем на работе, чтобы не уволили, меньшинство врет большинству ради власти. Правдивая информация может привести к обидам или к трагическим результатам; без лжи самооценка ребенка страдала бы с раннего детства, да и дети сами довольно рано узнают о социальной ценности лжи. Уже в возрасте трех-четырех лет они прекрасно осваивают искусство лжи, а повзрослев, начинают врать регулярно.

Таким образом, ложь является естественным продуктом выживания человека как социального и биологического существа.

Поэтому, бытовая ложь (если можно так выразиться), как продукт человеческой жизнедеятельности, всегда будет сопровождать информационный контент и особо не будет влиять на общественные отношения.

У каждой медали всегда имеется оборотная сторона, которая выражается в использовании ботовых программ – как элемента

искусственного интеллекта, для создания сетевых информационных атак на компьютеры, для генерирования ложной (фейковой) информации в политике, бизнесе, для навязывания информации различного рекламного содержания, для мошенничества в финансовых сферах и многих других негативных случаях.

Например, ложь, которая формируемся в информационной сети и средствах массовой информации, стала критерием уровня «правды», так как народу невозможно уже определить, где правда, а где ложь. Нужно быть достаточно образованным, информированным и, самое главное, мыслящим человеком, чтобы уметь отделять правду от лжи, а ложь от правды. Высшая форма проявления всеобщей лжи – составной элемент информационной войны, которая началась, конечно же, не вчера и не год назад, она вечна, проявляется в разных формах, в разных масштабах, с разной целью и для разных аудиторий. Информационная эпоха стала всего лишь благодатной почвой и расцветом информационных войн, в которых львиную долу фейков сегодня генерируют ботовые программы. По прогнозам Business Insider, уже к концу текущего года восемьдесят процентов компаний будет пользоваться чат-ботами [1].

Учитывая тот факт, что чат-ботовые программы, по сути, можно признать прообразами будущих элементов искусственного интеллекта, то возникает вопрос, как недостоверная информация может в будущем повлиять на формирование самого искусственного интеллекта и как в дальнейшем этот искусственный интеллект будет влиять на общественные отношения, если уже сегодня в информационное пространство запускаются боты, формирующие фейковые и деструктивные программы.

На данный вопрос хочется ответить старой шуткой – на каждую «*кузькину мать*» всегда найдется «*кузькин папа*», как это происходит в реальном мире, т.е. баланс сил добра и зла, лжи и правды всегда будет соблюдаться, такова закономерность нашего бытия.

Список использованных источников:

1. Исправьте это немедленно: 8 ошибок чат-ботов. URL: https://blog. ingate.ru/detail/ispravte-eto-nemedlenno-8-oshibok-chat-botov/ (дата доступа 10.10.2019).

----------*----------**

Ліненко Ю. О., студент ФСП КПІ ім. Ігоря Сікорського.
Науковий керівник: ***Фурашев В. М.,*** к.т.н., доцент, старший науковий співробітник КПІ ім. Ігоря Сікорського.

ЗАГАЛЬНІ ЗАСАДИ ЗАХИСТУ ІНФОРМАЦІЙНОГО СУВЕРЕНІТЕТУ УКРАЇНИ

Постановка проблеми: У статті досліджується питання захисту інформаційного суверенітету держави, його визначення, складових даного поняття, джерело потенційних загроз та шляхів здійснення захисту.

У законі України "Про національну програму інформатизації" **інформаційний суверенітет** визначається, як здатність держави контролювати і регулювати потоки інформації з-поза меж держави з метою додержання законів України, прав і свобод громадян, гарантування національної безпеки держави.

Даний термін включає в себе дві складові: технологічну й інформаційно-психологічну. Технологічна складова полягає у розробці комп'ютерів, програмного забезпечення, різного роду електронної продукції. Інформаційно-психологічна складова представляє з себе бачення інформаційного суверенітету, з точки зори конкретної людини з певними цінностями та особистістю[2;305].

Наявність у держави суверенітету передбачає те, що останній потрібно захищати від руйнівного впливу. На інформаційний суверенітет дане правило теж розповсюджується. Коли держава знаходиться в умовах інформаційної війни, з обох боків інтенсивно йде потужний вплив на свідомість громадян. Протидія даному впливу є одним з першочергових завдань держави[3;150]. Говорячи про захист інформаційного суверенітету неможливо ігнорувати ту роль, яку роль у сучасному світі грає інтернет. Серед усіх способів розповсюдження інформації інтернет є найшвидшим. Саме інтернет надає колосальні можливості для передачі різного роду особистих даних. Соціальні мережі у XXI столітті є не менш дієвою зброєю ніж танки, автомати чи винищувачі.

Державна політика у сфері захисту інформаційного суверенітету полягає у:

- створення умов для реалізації конституційного права громадян на вільне отримання та використання інформаційних ресурсів;

- формування за допомогою інформаційних ресурсів демократично орієнтованої свідомості;
- створення умов для включення національного інформаційного простору до міжнародного інформаційного простору таким чином, щоб не завдавати шкоди національному інформаційному суверенітету.

Захист **інформаційного суверенітету** держави може бути ефективним лише у разі дотримання певних вимог:

- об'єднання й кординація усіх дій щодо захисту інформаційного суверенітету з єдиного центру;
- чітке узгодження між собою меседжів та позицій державних відомств;
- здійснення централізованого моніторингу інформаційного простору;
- формування позитивного іміджу України у очах іноземних ЗМІ;
- розвиток інформаційних технологій на національному рівні.

В свою чергу захист інформаційного суверенітету, як самостійне поняття теж складається з певних компонентів:

- політична воля;
- медіа грамотність;
- відповідальність журналістів;
- критичне мислення;

Усе вищезазначене неможливо без **політичної волі** з боку осіб, що здійснюють керівництво державою та реалізацію державної політики.

Також дуже велике значення має рівень **медіаграмотності** у суспільстві.[4;4] Під медіаграмотністю розуміють здатність скептично відноситись до інформації з неперевірених джерел й не реагувати емоційно на будь-яку "гучну" новину.

Журналісти в свою чергу мають усвідомлювати **відповідальність за поширювану ними інформацію**, наслідків розповсюдження даної інформації потенційний її вплив інформації на аудиторію тощо.

У умовах сьогодення важливо розвивати у себе **критичне мислення** й проявляти поміркований скептицизм до інформації з телевізора, інтернету, вуст політиків тощо.

Таким чином захист інформаційного суверенітету є комплексним явищем, яке поєднує як діяльність державних органів, так і відповідальність конкретних громадян. Лише комплексний підхід дозволить гарантувати, що інформаційний простір конкретної держави не стане об'єктом впливу

зовнішніх сил. Лише за таких умов держава у XXI столітті може вважатись дійсно незалежною.

Список використаних джерел:

1. Закон України “Про національну програму інформатизації”// Відомості Верховної Ради України — 1998 - № 27-28

2. Кормич Б. Інформаційна безпека: організаційно-правові основи: Навчальний посібник/ Борис Кормич,. -К.: Кондор, 2005. -305 с.

3. Маракова І. Захист інформації: Підручник для вищих навчальних закладів/ Ірина Маракова, Анатолій Рибак, Юрій Ямпольский,; Мін-во освіти і науки України, Одеський держ. політехнічний ун-т, Ін-т радіоелектроніки і телекомунікацій . -Одеса, 2001. -150 с.

4. Гуцалюк М. Інформаційна безпека України: нові загрози // Бизнес и безопасность. - 2003. - № 5. - С. 4

----------***----------

Петров С. Г., к.ю.н.,
співробітник СБ України.

ДО ПИТАННЯ ПРО КЛАСИФІКАЦІЮ КІБЕРЗАГРОЗ

Закон України «Про основні засади забезпечення кібербезпеки України» (далі – Закон про кібербезпеку) передбачає, що функціонування національної системи кібербезпеки забезпечується, зокрема, шляхом впровадження єдиної (універсальної) системи індикаторів кіберзагроз з урахуванням міжнародних стандартів з питань кібербезпеки та кіберзахисту [1, ст. 8]. Особливо важливим є європейський досвід в інформаційній сфері [2].

Результати даного дослідження можуть бути враховані при впровадження єдиної (універсальної) системи індикаторів кіберзагроз, яка на жаль, поки не створена.

Стратегія кібербезпеки України, затверджена Указом Президента України від 15.03.2016 № 96/2016, визначає, що «переваги сучасного цифрового світу та розвиток інформаційних технологій обумовили виникнення нових загроз національній та міжнародній безпеці», і закріплює перелік таких загроз у розділі 2 Стратегії «Загрози кібербезпеці». Виокремлюється уразливість до кіберзагроз єдиної автоматизованої системи управління Збройних Сил України, економічної, науково-технічної, інформаційної сфери та інших сфер для розвідувально-підривної діяльності іноземних, насамперед російських, спецслужб у кіберпросторі, вказує на можливість порушення штатних режимів роботи автоматизованих систем

керування технологічними процесами на об'єктах критичної інфраструктури, а також на поширення політично вмотивованих атак на урядові та приватні веб-сайти тощо [3].

Крім того, Стратегія вказує на чинники, які актуалізують загрози кібербезпеці: невідповідність інфраструктури електронних комунікацій держави, рівня її розвитку та захищеності сучасним вимогам; недостатній рівень захищеності критичної інфраструктури, державних електронних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, від кіберзагроз тощо [3].

Видається, що з урахуванням розвитку в Україні концепції «Держава у смартфоні» і швидкоплинності змін відносин у сфері кіберпростору, є необхідність уточнення підходів до визначення кіберзагроз національним інтересам України. У цьому напрямі є потреба у пропозиціях дослідників юридичної науки, наприклад, у частині закріплення у наступній редакції Стратегії у систематизованому вигляді таких загроз.

Загальні вимоги до кіберзахисту об’єктів критичної інфраструктури ґрунтуються на несистематизованих посиланнях на окремі кіберзагрози, наприклад, «модифікація інформації», поширення «зловмисного коду, шкідливого програмного забезпечення та вірусів», «порушення конфіденційності, цілісності та доступності інформації, недоступності служб (функцій) об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури, порушення функціонування компонентів об’єкта», атаки типу «відмова в обслуговуванні», «несанкціонований доступ через Інтернет» тощо [4, п.п. 19, 24].

Поєднуючи зазначений нормативний підхід із позицією Д.С.Бірюкова та В.М.Бурлакова [5] щодо наслідків комп’ютерних нападів: несанкціонований доступ або перехоплення інформації (втрата конфіденційності); несанкціонована зміна інформації, програмного забезпечення, обладнання і т.д. (втрата цілісності); блокування транзакцій та/або відключення системи (втрата готовності), пропонуємо наступний критерій для класифікації кіберзагроз: характер реальних чи потенційних негативних наслідків. За цим критерієм важливо також врахувати позицію А.Пазюка про наслідки від дій кібератак, які співпадають із дефініціями «тероризму» відповідно до Міжнародній конвенції про боротьбу із фінансуванням тероризму [6]. Адже втручання в мережі атомних станцій, комунальних служб, держорганів чи військових об’єктів з метою залякування населення тощо може призвести до катастрофічних наслідків.

За цим критерієм поділяємо кіберзагрози на такі, що спричиняють:

- несанкціонований доступ або перехоплення інформації;

- несанкціоновану модифікацію інформації;
- несанкціоноване порушення доступності інформації;
- залякування населення чи примушення уряду чи міжнародної організації вчинити будь-яку дію або утриматись від неї.

Важливими є класифікації кіберзагроз, які ґрунтуються на характеристиках об'єкта і суб'єкта посягань.

За об'єктом посягань виокремлюємо загрози, спрямовані на:

- державні електронні інформаційні ресурси;
- інформаційну інфраструктуру, призначену для обробки інформації, вимога щодо захисту якої встановлена законом, зокрема і на критичну інформаційну інфраструктуру;
- свідомість людей, дії (бездіяльність) населення.

За суб'єктом посягань класифікуємо загрози на:

- атаки, не ініційовані державами, насамперед, кіберзлочинність;
- кібератаки розвідувальних органів іноземних держав, насамперед, РФ;
- інциденти, не пов'язані з умисними діями чи бездіяльністю.

Характеризуючи розбудову потенціалу кібербезпеки України, відзначимо, що 15 серпня поточного року в Апараті РНБО України відбулось засідання робочої групи з питань реформування сфери забезпечення кібербезпеки у системі національної безпеки України. За підсумками наради було ухвалене рішення зі створення цільових груп для подальшої роботи щодо правових аспектів забезпечення кібербезпеки та удосконалення державного управління; цифровізації та розвитку галузі електронних комунікацій; визначення перспективної організаційно-технічної моделі кіберзахисту та удосконалення освіти в сфері кібербезпеки [7].

Список використаних джерел:

1. Закон України від 05.10.2017 «Про основні засади забезпечення кібербезпеки України». Відомості Верховної Ради України, 10.11.2017, № 45, ст. 403.

2. Марущак А.І. Європейський досвід з питань боротьби з правопорушеннями в інформаційній сфері. Безпека інформації. 2019. Том 25. №1. С. 13-17. URL: http://jrnl.nau.edu.ua/index.php/Infosecurity/article/view/13665.

3. Указ Президента України від 15.03.2016 № 96/2016 «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» // Офіційний вісник України, 2016, № 23, ст. 899.

4. Постанова Кабінету Міністрів України від 19 червня 2019 р. № 518 «Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури». Офіційний вісник України. 2019. № 50. ст. 1697.
5. Бірюков Д. С. Вплив сучасних кіберзагроз на ефективність систем фізичного захисту критично важливих об'єктів та інфраструктури / Д. С. Бірюков, В. М. Бурлаков // Адапт. системи автомат. упр. - 2012. - Вип. 21. - С. 9-17.
6. https://uacs.kiev.ua/kiberataki-terrorizm/.
7. http://www.rnbo.gov.ua/news/3347.html.

----------***----------

Мисливий В. А., д.ю.н., професор,
професор КПІ ім. Ігоря Сікорського.

МІСЦЕ ВЧИНЕННЯ ЗЛОЧИНУ У КОСМІЧНОМУ ПРОСТОРІ

Кримінальне законодавство, регулюючи питання відповідальності щодо чинності кримінального закону у просторі, у ч. 2 ст. 6 Кримінального кодексу України (далі – КК) передбачає, що «злочин визнається вчиненим на території України, якщо його було почато, продовжено, закінчено або припинено на території України».

Хоча така загальна регламентація кримінальним законом даного питання в цілому задовольняє теорію та правозастосовну практику, проте не дає чіткої відповіді на деякі аспекти кримінально-правової характеристики місця вчинення злочину як однієї з ознак об’єктивної сторони складу злочину. Так, згадані вище терміні «почато», «продовжено» та «припинено», що вживаються законодавцем у наведеній нормі, не мають свого визначення у Загальній частині КК, вже не кажучи про відсутність самого поняття – «місце вчинення злочину».

Відтак тлумаченням поняття «місце вчинення злочину» займається доктрина кримінального права та судова практика. Зокрема, у Великій українській юридичній енциклопедії відзначається, що місце вчинення злочину – це певна територія або інші місце, де здійснюється суспільно небезпечне діяння (дія або бездіяльність) та настають його суспільно небезпечні наслідки [1, с. 522]. В інших відомих юридичних виданнях зазначається, що це визначена територія, яка описана у диспозиції кримінально-правової норми, на якій було вчинено суспільно небезпечне діяння чи настав злочинний результат [2, с. 434].

Неважко побачити, що вказані визначення, які претендують на взірець сучасної кримінально-правової думки, суттєво різняться між собою,

оскільки перше передбачає спорідненість суспільно небезпечного діяння та суспільно небезпечних наслідків, а друге – навпаки розмежовує їх. У зв'язку з цим вдається, що означені підходи не забезпечують чітких орієнтирів визначення місця вчинення злочину.

І хоча кримінальний закон пов'язує вчинення злочину з «територією України» або іншою територією «поза межами України» чи «за межами України» (статті 6-10 КК), слід визнати обґрунтованим, що у навчальній і науковій літературі цей підхід щодо дії кримінального закону усталено визначається більш широким визначенням – як чинність кримінального закону у просторі.

При цьому поняття «простір», обумовлене сучасним рівнем розвитку суспільства, вже тривалий час передбачає не лише земну планетарну реальність, але й навколоземний космічний простір, що знаходиться за межами атмосфери Землі. Слід визнати, що правовий режим вказаного простору визначений міжнародним космічним правом [3, с. 406-407], оскільки він є відкритим і вільним для дослідження та використання всіма державами, які здійснюють космічну діяльність [4].

Разом з цим, у процесі цієї діяльності виникають ситуації, що можуть мати ознаки кримінальних правопорушень, які вимагають встановлення місця їх вчинення, а відтак визначення відповідної кримінально-правової юрисдикції.

Зокрема, за повідомленнями засобів масової інформації, 30 серпня 2018 року екіпажом Міжнародної космічної станції (далі – МКС) в обшивці побутового відсіку російського корабля «Союз МС-09» було виявлено отвір діаметром близько двох міліметрів, який призвів до витоку повітря зі станції. У той день у Центрі управління польотом на Землі звернули увагу, що на МКС відбувається повільний витік повітря, швидкість якого відповідала зниженню тиску на станції близько 0,8 міліметра ртутного стовпчика на годину. За таких умов МКС залишилась би без повітря за 18 днів. Уникаючи такої загрози космонавти локалізували отвір спеціальним герметиком.

Створена комісія з розслідування цього інциденту визнала малоймовірною версію виробничого браку чи недбалості під час зборки корабля на землі до його запуску. Разом з цим не була відкинута «космічна версія» про те, що хтось просвердлив отвір вже на орбіті, із середини космічної станції, після притискування до неї корабля [5]. Обставини щодо кримінального походження цього випадку поки залишились до кінця не з'ясованими, проте очевидно, що у разі підтвердження останньої версії суспільна небезпека вчиненого виглядала б надто серйозною.

На іншій стороні планети, як повідомляє The New York Times, у США розслідують перший злочин у космосі, в якому обвинувачують американську астронавтку Енн Макклейн, яка раніше знаходилась в офіційному лесбі-шлюбі з американкою Саммер Уорден. Пара розлучилася, але продовжує разом виховувати дитину, біологічною матір'ю якої є Уорден.

При цьому Уорден заявила, що її колишня дружина, перебуваючи на борту МКС, незаконно увійшла в її банківський кабінет в інтернеті. Макклейн, яка нещодавно повернулася на Землю, зізналася, що дійсно, перебуваючи в космосі, входила в аккаунт, а також дала свідчення під присягою. Натомість вона стверджує, що завжди перевіряла банківський кабінет з дозволу Уорден, щоб переконатися, що фінанси сім'ї були в порядку, а відтак не зробила нічого незаконного, оскільки доступ до банку з космосу був спробою переконатися, що на рахунку Уорден достатньо коштів для оплати рахунків і догляду за їхньою дитиною [6].

Отже і в цьому випадку при доведеності кримінального характеру поведінки астронавтки виникає питання щодо місця вчинення протиправного діяння за умов, що воно було здійснено при знаходженні суб’єкта у космічному просторі. Стаття VIII «Договору про принципи діяльності держав по дослідженню і використанню космічного простору, включаючи Місяць та інші небесні тіла» визначає, що «держава-учасниця Договору, до реєстру якої занесено об'єкт, запущений у космічний простір, зберігає юрисдикцію і контроль над таким об'єктом і над будь-яким екіпажом цього об'єкта під час їх знаходження в космічному просторі, у тому числі і на небесному тілі» [7].

У сучасному вимірі проблема можливості вчинення протиправних дій знайшла свій прояв на такому космічному об’єкті, як МКС (International Space Station – ISS), створеною за співробітництва між Росією і США для реалізації у космосі наукової діяльності, в якій приймає участь 16 країн: Бельгія, Бразилія, Велика Британія, Данія, Іспанія, Італія, Канада, Нідерланди, Німеччина, Норвегія, Російська Федерація, США, Франція, Швейцарія, Швеція та Японія. При цьому за угодою кожному учаснику проекту належать його сегменти на МКС. Так, Росія володіє модулями «Звєзда» і «Пірс», Японія – модулем «Кібо», ЄКА – модулем Columbus, сонячні панелі, а також інші модулі належать NASA (США) тощо [8]. Таким чином, існують фактичні та правові передумови для визначення певної належності складових модулів станції, що можуть розглядатися за територіальною належністю тої чи іншої держави.

Залежно від цього має вирішуватися визначення такої кримінально-правової ознаки, як місце вчинення злочину. Очевидно, що поняття

«простір» і «територія» як взаємообумовлені та взаємопов'язані категорії слугуватимуть кримінально-правовому визначенню місця вчинення злочину. При цьому поняття простір слід розглядати як більш широке, а територію – як більш вузьке утворення, що визначає конкретну частину простору, в якому може відбуватися злочин. У рамках останньої повинно розглядатися місце вчинення злочину.

Таким чином, місце вчинення злочину в космічному просторі має розглядатися як певна визначена частина території у межах того чи іншого модуля, сегменту, сектору, частини, блоку космічного об'єкта з урахуванням поширення на нього національної кримінально-правової юрисдикції конкретного суб'єкта міжнародного співтовариства.

Враховуючи викладене, з огляду на загальновизнані світоглядові філософські категорії «простір» та «час» як форми існування матерії, та задля усунення доктринальних суперечностей, вважаємо, що чинне кримінальне законодавство поряд з положенням ч. 3 ст. 4 КК – «часом вчинення злочину визнається час вчинення особою передбаченої законом про кримінальну відповідальність дії або бездіяльності», має також передбачати в ст. 6 КК таке формулювання: «Місцем вчинення злочину визнається місце вчинення особою передбаченої законом про кримінальну відповідальність дії або бездіяльності».

Список використаних джерел:

1. Велика українська юридична енциклопедія. Х.: Право, 2015. 258с.
2. Энциклопедия уголовного права. Т. 4. Состав преступления. Издание профессора Малинина, СПб., 2005. 798 с.
3. Великий енциклопедичний юридичний словник / За ред. акад. НАН України Ю. С. Шемшученка. К.: ТОВ «Видаництво «Юридична думка». 2007. 992 с.
4. Про космічну діяльність : Закон України від 15 листопада 1996 р. № 502/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/502/96-%D0%B2%D1% 80/print] (дата звернення: 09.09.2019 р.).
5. «Дыры на МКС недопустимы». URL : https://news.rambler. ru/tech/42872187-dyry-na-mks-nedopustimy-nasa-zhdet-obyasneniy-ot-rogozina/?utm_source=head&utm_campaign=self_promo&utm_ medium=news& utm_content=news&h_sp=1 (дата звернення: 09.09.2019 р.).
6. В NASA расследуют первое преступление в космосе. URL : https://news.rambler.ru/tech/42714231-v-nasa-rassleduyut-pervoe-prestuplenie-v-kosmose/?utm_source=head&utm_campaign=self_promo&utm_medium=news& utm_content=news&h_sp=1 (дата звернення: 09.09.2019 р.).
7. Договір про принципи діяльності держав по дослідженню і використанню космічного простору, включаючи Місяць та інші небесні тіла.

Набуття чинності для України: 31 жовтня 1967 року.URL: https://zakon.rada.gov.ua/laws/show/995_480/print (дата звернення: 09.09.2019 р.).

8. Міжнародна космічна станція. URL : https://uk.wikipedia.org/wiki/%D0%9C%D1%96%D0%B6%D0%BD%D0%B0%D1%80%D0%BE%D0%B4%D0%BD%D0%B0_%D0%BA%D0%BE%D1%81%D0%BC%D1%96%D1%87%D0%BD%D0%B0_%D1%81%D1%82%D0%B0%D0%BD%D1%86%D1%96%D1%8F (дата звернення: 09.09.2019 р.).

----------***----------

Янчук Ю. В., головний спеціаліст
Сектору стратегічних комунікацій
Міністерства інформаційної політики
України.

ДО ПИТАННЯ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ У ЗВ'ЯЗКУ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЙ ІНТЕРНЕТУ РЕЧЕЙ

Сучасний розвиток інформаційних технологій та стрімка інформатизація усіх сфер людської діяльності трансформують світове суспільство, ведуть його до нової цифрової революції, що виявляється у використанні штучного інтелекту, Інтернету речей, досягнень робототехніки тощо. Оскільки функціонування таких технологій передбачає підключення до мереж не лише гаджетів та комп'ютерів різних конфігурацій, а й різноманітних речей матеріального світу, проблема забезпечення безпеки особи, суспільства та держави на сьогодні є ще гострішою.

Сучасний світ інформаційних технологій вимагає постійної взаємодії між своїми компонентами, причому концепція комунікації між пристроями передбачає виконання певних дій взагалі без втручання людини. Для цієї концепції у 1999 році було введено назву «Інтернет речей» (англ. Internet of Things). Під терміном «річ» у даному контексті розуміють фізичні пристрої, предмети, механізми, транспортні засоби (інша назва – «розумні» пристрої) або, навіть, будівлі, що оснащені апаратним та програмним забезпеченням, що уможливлює обмін даними між цими пристроями та комп'ютерними системами [1, с. 30].

Інтернет речей створює умови для появи синергетичного ефекту від поєднання можливостей штучного інтелекту, хмарних обчислень, безлічі сенсорів, математичних алгоритмів обробки великих даних (Big Data), роботизованих пристроїв різного призначення, систем передання даних (мережі Інтернет), що дозволяє надавати різноманітні послуги та проводити всілякі роботи за участю чи без участі людей [2, с. 68].

Тобто, Інтернет речей є системою функціональних елементів, що складається з об'єктів фізичного світу (пристроїв, сенсорів, мікропроцесорів), об'єднаних мережею Інтернет, що на основі програмного забезпечення реалізують виконання завдань чи надання послуг дистанційно або за участі суб'єктів.

Варто зазначити, що багато країн вже обрали стратегію розвитку, побудовану на повсюдному використанні технологій Інтернету речей. Зокрема: в США прийнята національна стратегія Інтернету речей (2016 р.) та законопроект «Розвиток інновацій и сприяння Інтернету речей» (2017 р.); у Великій Британії діє «Цифрова стратегія Великої Британії 2017»; У Південній Кореї прийнятий генеральний план створення IoT (2014 р.); в Японії - «Стратегії росту Японії – 2016» (Індустрія 4.0, розвиток IoT, великих даних, робототехніки); у Китаї виділено $127,5 млрд. на державну програму з розвитку Інтернет речей до 2020 року та створення 500 розумних міст (2017 р.); в уряді ОАЕ введено посаду міністра з питань штучного інтелекту [3, с. 75].

Однак, враховуючи стрімке зростання пристроїв Інтернету речей у всіх без винятку сферах (розумні будинки, розумні авто, ферми, годинники та інше), та імплементацію електронних складових цих технологій в людський організм (розумні кардіостимулятори, розумні імплантати), виникають нові можливості для вчинення різного роду злочинів, що становлять загрозу не лише інформаційній безпеці, а й зазіхають на здоров'я і життя людини.

Загалом, підключені до мережі речі стають надзвичайно вразливими для вторгнення у порівнянні з традиційними електронно-обчислювальними машинами. На думку більшості науковців, основними проблемами використання Інтернету-речей, яке передбачає накопичення та використання великого обсягу даних про конкретну особу, є забезпечення інформаційної безпеки та захисту персональних даних.

Крім загроз суто технічного характеру, до яких відносять перебої в роботі пристроїв, їх вихід з ладу чи з-під контролю операторів, небезпеку становлять сплановані та скоординовані деструктивні дії певних суб'єктів з метою завдання шкоди інформаційній безпеці особи, суспільства чи держави в цілому.

Як приклад, у вересні 2016 року було здійснено одну з найпотужніших DDoS атак в історії, основу якої склали саме пристрої Інтернету речей. Після цієї атаки, 30 вересня 2016 року, програмний код зловмисного програмного забезпечення «Mirai» (що у перекладі з японської – «майбутнє»), за допомогою якого відбулося зараження пристроїв Інтернету речей, потрапив до мережі Інтернет, де є доступним дотепер. Ця подія слугувала початком

цілої низки DDoS атак на різні інформаційні ресурси з використанням «розумних» пристроїв [4].

Разом з тим, технології Інтернету речей значно посилюють ризики порушення конфіденційності персональних даних внаслідок того, що вони передбачають накопичення, циркулювання і використання великого, територіально і технологічно розподіленого обсягу інформації (даних) про конкретну людину. Це викликає цілком закономірні питання про надійність зберігання таких даних та забезпечення їх захисту від несанкціонованого використання. Можна зазначити, що широке використання технологій Інтернету речей призводить до необхідності вирішення таких основних правових проблем: визначення механізмів реалізації принципу попередньої згоди на використання та «на стирання» персональних даних (ст. 17 Регламенту ЄС 2016/679 від 27.04.16 р.); правовий вплив на регулювання транскордонних потоків персональних даних; використання персональних даних інтелектуальними комплексами, що функціонують без участі суб'єктів (юридичних або фізичних осіб) [5, с. 53].

Загрози у сфері Інтернету речей стали предметом уваги Європейського агентства з мережевої та інформаційної безпеки (ENISA) та Європейської групи кібербезпеки. Так, у доповіді на Європейській нараді з питань кібербезпеки 2016 року було зазначено, що глобальне розповсюдження Інтернету речей буде знижувати рівень безпеки попри застосування належних методів захисту, а також наголошено, що людський фактор завжди негативно позначатиметься на стані вразливості до інформаційних загроз[6].

Інтернет речей є новітнім етапом розвитку світового інформаційного суспільства, до складу якого увійшла і Україна. Проте, на національному законодавчому рівні залишається невирішеним питання правового регулювання використання таких новітніх технологій, а також юридичне закріплення інформаційних відносин, що виникають щодо використання Інтернету речей.

На нашу думку, основними кроками в даному напрямку має бути законодавче визначення відповідної термінології, встановлення юрисдикції учасників, чітко виокремлене коло суб'єктів таких відносин. Надзвичайно важливим аспектом в цьому напрямку повинне стати закріплення в національному законодавстві загальних принципів регулювання інформаційних відносин, що виникають у сфері Інтернету речей, а також відповідальності за їх порушення.

Науковці пропонують закріпити наступні принципи правового регулювання вказаних відносин:

1. Інформованість. Користувачі сервісів Інтернету Речей повинні мати інформацію щодо того, збір яких даних здійснюється тим чи іншим пристроєм, якими способами, в якому обсязі, де і яким чином такі дані зберігаються.

2. Вільна участь в Інтернеті речей. Незважаючи на те що Інтернет речей - об'єктивна тенденція розвитку інформаційного суспільства, громадяни та організації не можуть бути дискриміновані в тому випадку, якщо вони не бажають бути повністю залученими до системи Інтернету речей.

3. Захист персональних даних і приватного життя. Будь-який пристрій може прив'язуватися до інтернет-профілю свого власника; навіть якщо декларується анонімізація даних, за наявними накопиченими відомостями в істотній кількості випадків можливо ідентифікувати суб'єкта. По-друге, виникає необхідність вироблення нових принципів щодо отримання розробником (продавцем) пристроїв (програмного забезпечення) згоди суб'єкта персональних даних на використання (обробку) персональних даних, в тому числі всіма учасниками Інтернету речей.

4. Захист персональних даних на ринку «Big data». Формується ринок Великих даних, які фактично виступають предметом угод. Крім питання про правовий режим інформації як об'єкта правовідносин, необхідно визначити, в якому обсязі в принципі Великі дані можуть бути об'єктом торгівлі [5, с. 54-55].

Проаналізувавши запропоновані принципи правового регулювання, варто погодитись з їх автором та зауважити, що лише за вдалої реалізації вищенаведеного можливо забезпечити необхідний рівень інформаційної безпеки у зв’язку з використанням технологій Інтернету речей.

Список використаних джерел:

1. Грайворонський М. В. Безпека пристроїв інтернету речей. Інтернет речей: проблеми правового регулювання та впровадження: Матеріали науково-практичної конференції. Київ. Політехніка. 2017. С. 29-34. URL: https://bit.ly/2HcMDYY

2. Интернет вещей. Безграничные возможности взаимодействия человека и машины. Медиасектор и индустрия развлечений. URL: https://go.ey.com/2kiQzzQ

3. Баранов О. А. Місія, мета і роль інформаційного права Інформаційне право: сучасні виклики і напрями розвитку: Матеріали першої науково-практичної конференції. Київ. Політехніка. 2018. 196 с.

4. Баранов О. А., Брижко В. М. Захист персональних даних в сфері Інтернет речей. Інформація і право. 2016. № 2(17). С. 85-91.

5. Шахбазян К. С. Інтернет речей: ризики порушень у сфері прав людини. Інтернет речей: проблеми правового регулювання та впровадження:

Матеріали науково-практичної конференції. Київ. Політехніка. 2017. С. 53-62. URL: https://bit.ly/2HcMDYY

6. European Foresight Cyber Security Meeting 2016 //Режим доступу: https://bit.ly/2lV9Esq

----------***----------

Фарадж Д. Ю., студент ФСП КПІ ім. Ігоря Сікорського.
Науковий керівник: ***Фурашев В. М.,*** к.т.н., доцент, с.н.с.

ТОП-9 ЕТИЧНИХ ПИТАНЬ В ШТУЧНОМУ ІНТЕЛЕКТІ

Оптимізація логістики, виявлення шахрайства, створення мистецтва, проведення досліджень, забезпечення перекладів: інтелектуальні системи машин змінюють наше життя на краще. У міру того, як ці системи стають більш дієздатними, наш світ стає більш ефективним і, отже, багатше. Технічні гіганти, такі як Alphabet, Amazon, Facebook, IBM і Microsoft, а також такі люди, як Стівен Хокінг і Ілон Маск, вважають, що зараз саме час поговорити про майже безмежному ландшафті штучного інтелекту. Багато в чому це не менш новий кордон для оцінки етики та ризиків, ніж для нових технологій. Так які питання і розмови турбують експертів ШІ вночі?
Безробіття. Що відбувається після закінчення роботи?

Ієрархія праці в першу чергу пов'язана з автоматизацією. Оскільки ми винайшли способи автоматизації робочих місць, ми могли б створити простір для людей, щоб взяти на себе більш складні ролі, переходячи від фізичної роботи, яка домінувала в доіндустріальному світі, до когнітивної праці, яка характеризує стратегічну і адміністративну роботу в нашому глобалізованому суспільстві. Подивіться на вантажоперевезення: в даний час в ньому працюють мільйони людей тільки в Сполучених Штатах. Що буде з ними, якщо самохідні вантажівки, обіцяні Елоном Маском Тесла, стануть широко доступними в наступному десятилітті? Але з іншого боку, якщо ми розглянемо більш низький ризик нещасних випадків, самохідні вантажівки здаються етичним вибором. Такий же сценарій може статися і з офісними працівниками, а також з більшістю робочої сили в розвинених країнах. Саме тут постає питання про те, як ми збираємося проводити наш час. Більшість людей як і раніше покладаються на те, що продають свій час, щоб мати достатній дохід для підтримки себе і своїх сімей. Ми можемо тільки сподіватися, що ця можливість дозволить людям знайти сенс в позатрудовій діяльності, такої як турбота про свої сім'ї, взаємодія з їхніми

громадами та вивчення нових способів внесення вкладу в людське суспільство. Якщо ми доб'ємося успіху з переходом, то одного разу ми можемо озирнутися назад і подумати, що було варварством, що люди повинні були продати більшу частину свого часу пробудження тільки для того, щоб мати можливість жити.

Нерівність. Як ми розподіляємо багатство, створене машинами?

Світова економічна система заснована на компенсації за внесок в економіку, яку часто оцінюють з використанням погодинної заробітної плати. Більшість компаній як і раніше залежать від погодинної роботи, коли справа доходить до продуктів і послуг. Але, використовуючи штучний інтелект, компанія може різко скоротити використання людських ресурсів, а це означає, що доходи підуть на меншу кількість людей. Ми вже бачимо, що збільшується розрив в багатстві, де засновники стартапів забирають у себе більшу частину економічного надлишку, який вони створюють. Якщо ми дійсно розуміємо суспільство після роботи, то постає питання, як нам структурувати справедливу пост-трудову економіку?

Людяність. Як машини впливають на нашу поведінку ? та взаємодія з ними

Штучно інтелектуальні боти стають все краще і краще в моделюванні людської розмови та відносин. Наприклад у 2015 році, бот на ім'я Євген Goostman вперше пройшов тест Тьюринга. У цьому завданні люди використовували введення тексту для спілкування з невідомою сутністю, а потім здогадувались, спілкувались вони з людиною чи машиною. Даний бот обдурив більше половини людей, які думали, що вони розмовляють з людиною. Це тільки початок епохи, коли ми будемо часто взаємодіяти з машинами, так якби вони були людьми.

Штучна дурість. Як ми можемо захистити себе від помилок ?

Інтелект набувається шляхом навчання, незалежно від того будь то людина або машина. Системи зазвичай мають етап навчання, в якому вони «вчаться» виявляти правильні моделі і діяти відповідно до їх введення. Після того, як система повністю навчена, вона може перейти до тестової фази, де вона вражена великою кількістю прикладів, і ми бачимо, як вона працює. Очевидно, що етап навчання не може охоплювати всі можливі приклади, з якими система може мати справу в реальному світі. Ці системи можуть бути обдурені різними способами. Наприклад, випадкові точкові шаблони можуть привести до того, що машина «побачить» речі, яких там немає. Якщо ми покладаємося на ШІ, щоб привести нас в новий світ праці, безпеки та ефективності, нам потрібно переконатися, що машина працює так, як планувалося, і що люди не можуть здолати її, щоб використовувати її в своїх цілях.

Расистські роботи. Як ми виключаємо зміщення ШІ?

Хоча штучний інтелект здатний на швидкість і здатність обробки, яка далеко за межами людей, йому не завжди можна довіряти, щоб бути справедливим і нейтральним. Google і його материнська компанія Alphabet є одним з лідерів, коли справа доходить до штучного інтелекту, як видно з сервісу Google фото, де AI використовується для ідентифікації людей, об'єктів і сцен. Але завжди щось може піти не так, наприклад, коли камера промахнулася на расову чутливость, або коли програмне забезпечення використовується, щоб передбачити майбутні злочини. Ми не повинні забувати, що системи ШІ створюються людьми, які можуть бути упередженими і суб'єктивними. Знову ж таки, при правильному використанні або використанні тих, хто прагне до соціального прогресу, штучний інтелект може стати каталізатором позитивних змін.

Безпека. Як ми захищаємо ШІ від супротивників?

Чим потужнішою стає технологія, тим більше її можна використовувати, як по мерзенним причинам, так і для користі. Це відноситься не тільки до роботів, вироблених для заміни людських солдатів або автономної зброї, але і до систем ШІ, які можуть завдати шкоди, якщо вони використовуються зловмисно. Оскільки ці бої не вестимуться тільки на полі бою, кібербезпека стане ще більш важливою. Зрештою, ми маємо справу з системою, яка на порядки швидша і більш здібна за нас.

Злі джини. Як ми захищаємо від непередбачених наслідків?

Ми повинні турбуватися не тільки про супротивників. Що, якщо штучний інтелект сам обернеться проти нас? Це не означає, що перетворення «зла» в спосіб людської мощі або те, як лиха ШІ зображені в голлівудських фільмах. Швидше, ми можемо уявити собі просунуту систему AI як «джин в пляшці», який може виконувати бажання, але з жахливими непередбаченими наслідками. У разі машини, навряд чи буде злий умисел у грі, тільки відсутність розуміння повного контексту, в якому було зроблено бажання. Уявіть собі систему ШІ, яку просять викорінити рак в світі. Після багатьох обчислень він випльовує формулу, яка, насправді, призводить до кінця раку - вбиваючи всіх на планеті. Комп'ютер досяг би своєї мети «більше ніякого раку» дуже ефективно, але не так, як люди його задумали.

Особливість. Як ми можемо контролювати складну інтелектуальну систему?

Причина, по якій люди перебувають на вершині харчового ланцюга, не зводиться до гострих зубів або сильних м'язів. Людське домінування майже повністю пов'язано з нашою винахідливістю і інтелектом. Ми можемо отримати найкраще з великих, більш швидких, сильних тварин, тому що ми можемо створювати і використовувати інструменти для їх

управління: як фізичні інструменти, такі як клітини і зброю, так і когнітивні інструменти, такі як навчання і кондиціонування. Це ставить серйозне питання про штучний інтелект: чи буде він, в один прекрасний день, мати такі ж переваги над нами? Ми також не можемо покладатися тільки на «тягне вилку», тому що досить просунута машина може передбачити рух і захистити себе. Це те, що деякі називають «сингулярність»: точка в часі, коли люди перестають бути найрозумнішими істотами на землі.

Робот прав. Як ми визначаємо гуманне поводження з ШІ?

У той час як нейробіологи все ще працюють над розгадкою секретів свідомого досвіду, ми більше розуміємо основні механізми винагороди і відрази. Ми ділимося цими механізмами навіть з простими тваринами. У певному сенсі, ми будуємо схожі механізми винагороди і неприязні в системах штучного інтелекту. Наприклад, підкріплення навчання аналогічно дресируванню собаки: підвищення продуктивності посилено віртуальною нагородою. Зараз ці системи досить поверхневі, але вони стають все більш складними і схожими на життя. Чи можемо ми вважати, що система страждає, коли її функції винагороди дають їй негативний внесок? Більш того, так звані генетичні алгоритми працюють, створюючи безліч екземплярів системи відразу, з яких тільки найуспішніші «виживають» і об'єднуються, щоб сформувати наступне покоління примірників. Це відбувається протягом багатьох поколінь і є способом поліпшення системи. Невдалі екземпляри видаляються. На якому етапі ми можемо розглядати генетичні алгоритми як форму масового вбивства? Як тільки ми розглядаємо машини як об'єкти, які можуть сприймати, відчувати і діяти, це не величезний стрибок, щоб обміркувати їх правовий статус. Чи повинні вони розглядатися як тварини порівнянного інтелекту? Чи будемо ми розглядати страждання які «відчувають» машини? Деякі етичні питання стосуються пом'якшення страждань, деякі-ризику негативних наслідків. Хоча ми розглядаємо ці ризики, ми повинні також мати на увазі, що в цілому цей технічний прогрес означає краще життя для всіх. Штучний інтелект має величезний потенціал, і його відповідальна реалізація залежить від нас.

----------***----------

Князєв С. О., Національна академія СБ України, кандидат юридичних наук, старший науковий співробітник.

ВИТІК ІНФОРМАЦІЇ: СУЧАСНІ СВІТОВІ ТЕНДЕНЦІЇ

Під витоком інформації прийнято розуміти протиправне заволодіння чужою інформацією незалежно від того, яким способом це було здійснено. У випадку витоку інформації з обмеженим доступом, власник або розпорядник цієї інформації ризикує отримати цілий ряд неприємних наслідків починаючи від штрафних санкцій з боку держави, фінансових збитків і до втрати своєї репутації, переходу клієнтів до конкурента, колективних позовів тощо.

Проведення аналітичних досліджень стосовно світових тенденцій можливих каналів витоку інформації з обмеженим доступом здійснюється значною кількістю різних, у тому числі, міжнародних організацій. Як правило, такі дослідження ґрунтуються на зборі, накопиченні та опрацюванні відомостей щодо подібних фактів витоку інформації з обмеженим доступом.

Варто уваги узагальнена інформація, отримана різними аналітичними центрами, щодо співвідношення витоків інформації з обмеженим доступом за різними категоріями у світі: персональні дані – 89,8%; комерційна таємниця, но-хау – 3,5%; державна таємниця – 1,8%; інша, конфіденційна інформація – 4,4% не встановлено – 0,5%.

Досить часто витоки інформації з обмеженим доступом розподіляють за впливом та наміром. Їх реалізація може відбуватись завдяки діям співробітників компанії та має назву інсайдерська атака. У випадку зовнішнього впливу виток може статися від хакерської атаки.

На думку експертів «Ponemon Institute» у шести випадках з десяти для банкрутства компанії достатньо витоку лише п’ятої частини комерційних секретів.

При цьому, це не єдина неприємність, яка може виникнути на шляху тих, у кого стався виток інформації, зокрема можливо: погіршення іміджу компанії, що здатне призвести до зниження кількості нових клієнтів та відтік наявних; втрата технологічних секретів, що тягне за собою послаблення позицій на ринку; судові позови від клієнтів та санкції наглядових органів; звільнення співробітників; необхідність витрат за наслідками перерахованими вище т.п.

У січні 2019 року компанія із дослідження кіберризиків «Hacken» представила інформацію щодо результатів розслідування, відповідно до якого особисті дані понад 202 мільйонів осіб, які шукають роботу у Китаї протягом 3 років знаходились у відкритому доступі. Інформація включала номера телефонів, адреси електронної пошти, водійські права, заробітні очікування, сімейний стан, політичні погляди і, навіть зріст і вагу.

Фактори пов'язані з витоком інформації з обмеженим доступом розмежовуються на умисні і з необережності. Тобто, співробітники певної компанії можуть спеціально викрасти конфіденційну інформацію, та в подальшому передавати її іншим особам. Або це трапляється випадково, з необережності, не урегульованості необхідних режимних заходів тощо.

У грудні 2018 року стало відомо про масштабний виток даних жителів Бразилії. Із-за помилки на веб-сервері Apache у відкритому доступі опинились ідентифікаційні номери платників податків (Cadastro de Pessoas Físicas, CPF) 120 мільйонів осіб або 57% населення Бразилії.

Згідно даних порталу інформаційної безпеки «Content Security» ступінь загрози витоку інформації з обмеженим доступом з організації співвідноситься наступним чином: розголошення – 32%; несанкціонований доступ шляхом підкупу або схилення працівника конкурентами – 24%; відсутність в організації необхідного контролю та жорстких умов забезпечення збереження інформації – 14%; традиційний обмін виробничим досвідом – 12%; безконтрольне використання інформаційних систем – 10%; наявність передумов виникнення серед співробітників конфліктних ситуацій, пов'язаних з відсутністю виробничої дисципліни, психологічною невідповідністю, випадковим підбором кадрів, відсутністю роботи щодо єднання колективу – 8%.

На початку грудня 2017 року аналітики компанії 4iQ виявили у «даркнеті» величезну інтерактивну базу, яка об'єднувала інформацію отриману завдяки 252 витокам. При цьому, база, загальним обсягом 41 Гб. Постійно оновлюється та пропонує бажаючим 1,4 млрд. облікових даних у форматі звичайного тексту. Утворювач цієї бази не відомий, автором вказані тільки електронні гаманці Bitcoin та Dogecoin для внесків. Фахівці 4iQ відмічали появу 385 мільйонів нових пар логін/паролів та 318 мільйонів нових скомпрометованих користувачів.

Медичні заклади все більше потрапляють під інформаційні атаки. Так, у липні 2018 року в Сінгапурі група медичних закладів «Sing Health» стала жертвою цілеспрямованої хакерської атаки. Зловмисникам вдалось викрасти персональні дані 1,5 мільйонів осіб, у тому числі декількох високо посадовців, а також амбулаторні рецепти 160 тисяч чоловік, включаючи

прем’єр-міністра країни та інших членів уряду. Викрадена інформація стосувалась періоду з 1 травня 2015 року по 4 липня 2018 року.

Зростає й доля витоків інформації з обмеженим доступом за «не встановленими каналами». За останні роки на їх долю, в різних країнах, припадає майже 31%.

Наприклад, у жовтні 2017 року, колишнім співробітником, оператором громадського транспорту у Відні (Wienner Linen), були оприлюднені дані 20000 користувачів. При цьому, представники кампанії навіть не змогли визначити, яким чином це могло трапитись, а звільненому співробітнику отримати такий доступ до інформації.

Окремий сегмент витоки пов’язані із використанням USB – носіїв інформації та мобільними пристроями. Поширення такої причини як виток інформації з обмеженим доступом через викрадення персональних комп’ютерів становить все більшу проблему. Це пов’язано із сучасними особливостями використання персональних комп’ютерів, особливо ноутбуків, мобільної техніки співробітниками компаній.

Дуже часто зникає межа яка розділяє особисте життя співробітника з його корпоративною діяльністю що й стає головною причиною можливого витоку інформації з обмеженим доступом.

Американське аналітичне агентство «Insight Express» вважає, що близько 80% всіх корпоративних витоків інформації з обмеженим доступом відбувається завдяки наступним основним причинам:

- спілкування зі знайомими на предмет професійної інформації;
- спільне використання зі знайомими засобів комп’ютерної, мобільної техніки де може знаходитись професійна інформація;
- використання офісної техніки для особистих потреб, включаючи доступ до різних ресурсів мережі Internet;
- винос офісних носіїв інформації за межі організацій тощо.

Є чинники, які не залежать від компаній: катастрофи великого масштабу; стихійні лиха; аварії на технічних станціях, відмова роботи апаратури; погані погодні умови тощо.

Представники аналітичних організацій відмічають, що значна частина витоків інформації відбувається через канали, які можливо контролювати технічними засобами.

За результатами проаналізованих витоків інформації з обмеженим доступом, які були навмисно або не навмисно здійснені співробітниками організацій можливо виділити наступні відомості, що більш за все становлять предмет зацікавленості:

- документи, які характеризують фінансовий стан та плани організації, в тому числі, фінансові звіти, різна бухгалтерська документація, бізнес-плани, договори тощо;
- персональні дані працівників та клієнтів організації;
- технологічні та конструктивні розробки («ноу-хау») організації;
- внутрішні документи, службові записки, записи нарад, презентації «тільки для співробітників» організації тощо;
- технічні відомості, які дозволять здійснювати несанкціонований доступ до мереж організації, відомості стосовно реалізації засобів захисту інформації.

Список використаних джерел:

1. Головні витоки інформації 2018 року. URL : https://www.itweek/security/news-company/detail.php?ID=204871
2. Наймасштабніші витоки інформації 2017-го року // URL : https://www.mogroup.com.ua/?p=944
3. Расценки пользовательских данных на рынке киберпреступников // URL : http://www.tadviser.ru/index.php
4. Объем утечек конфиденциальной информации в мире в 2017 году вырос в 8 раз // URL : news.finance.ua/ru/news/-/412278/obem-utechek-konfidentsialnoj-informatsii-vyros-v-8-raz
5. Месть, шпионаж и невнимательность. Как компании защититься от утечки информации? // URL : kv.by/post/1054212-mest-shpionazh-i-nevnimatelnost-kak-kompanii-zashchititsya-ot-utechki-informacii
6. На сотрудников приходится две трети случав утечки информации в компаниях // URL : ko.com.ua/na_sotrudnikov _prihoditsya_dve_treti_sluchaev_utechki_informacii_v_kompaniyah_126155
7. Госпитали и страховые — основные виновники утечки информации о пациентах // URL : fainaidea.com/interesnoe /neobychnoe / gospitali-i-strahovye-osnovnye-vinovniki-utechki-informatsii-o-patsientah-154519. Html

----------***----------

Когут Н. Д., к. ю. н., старший викладач КПІ ім. Ігоря Сікорського.

ІНФОРМАЦІЙНА БЕЗПЕКА В МЕДИЧНІЙ СФЕРІ УКРАЇНИ

Життя і здоров’я людини є найвищою цінністю як для кожної окремої людини, так і для держави в цілому. Однією з важливих складових забезпечення якісної медицини є правильність поводження з медичною

інформацією. Для цього необхідно врегулювати прядок систематизації і верифікації медичної інформації та встановлення порядку доступу до неї.

В Україні є великі проблеми як в *систематизації законодавства в сфері медицини,* так і в сфері *систематизації інформації про пацієнтів* та доступу до неї. Надмірна нормотворчість на рівні виконавчих органів влади має негативний характер у всіх сферах, а майже єдиним законом в сфері охорони здоров'я в Україні є Основи законодавства України про охорону здоров'я від 19 листопада 1992 року [1] , решта – накази Міністерства охорони здоров'я, тож, давно назріла необхідність в прийнятті Медичного кодексу [2]. Це надасть можливість пацієнтам знати свої права та порядок надання медичної допомоги і медичних послуг, а також забезпечить сталість правового регулювання в цій сфері. Інформація про пацієнтів (медичні картки), зокрема, в електронному вигляді, до якої, за потреби, могли б долучатися різні медичні заклади, а саме ті, в які звернувся або потрапив пацієнт, наразі, законодавством не передбачена та не сформована на практиці. Проте, ця інформація є дуже важливою для швидкого та правильного лікування пацієнтів, особливо у разі екстреної ситуації. На даний час, кожна клініка заводить окрему картотеку щодо своїх пацієнтів та щодо напряму лікування чи діагностики, на якому вона спеціалізується. В той же час, інформація про хронічні захворювання, наявність алергічних реакцій на медичні препарати та інші збудники, перенесені хвороби, генетичні паталогії тощо надає можливість лікарям оперативно прийняти вірне рішення та уникнути ряду помилок, що особливо важливо у разі, якщо пацієнт потрапляє у лікарню в непритомному стані. Така картотека має формуватися на державній електронній платформі і всі медичні заклади, в які звертається пацієнт, мають вносити свою інформацію в неї по уніфікованим правилам, звісно, що доступ до неї має бути обмеженим і надаватися уповноваженим медичним працівникам лише у разі звернення пацієнта у відповідний медичний заклад. Інформація про групу крові та резус-фактор могла вноситися в паспорт за бажанням власника для того, щоб працівники швидкої могли вчасно зробити переливання потрібної крові. Наразі внесення такої інформації не передбачено в нових зразках паспортів.

Вже тривалий час точаться суперечки щодо правил трансплантації органів. В цілому, існують два варіанти надання згоди на трансплантацію органів: «презумпція згоди» та «презумпція незгоди» на трансплантацію органів від особи. *Презумпція згоди,* що підтримувалася останнім часом Міністерством охорони здоров'я України (далі МОЗ України) містить ряд загроз, особливо за нинішнього стану правоохоронної системи в Україні та

низького рівня захисту прав людей. Оскільки, якщо дозволити трансплантацію органів без необхідності отримання згоди пацієнта чи його близьких родичів, то можливе зловживання з боку як медичних працівників, так і інших осіб, що мають доступ до інформації про сумісність пацієнтів, що іноді трапляється навіть у розвинених правових державах. Зокрема, існують неоднозначні підходи щодо часу прийняття рішення про трансплантацію, після клінічної смерті чи після смерті мозку (кома не завжди свідчить про смерть мозку), оскільки таке рішення необхідно приймати в якомога коротші строки після смерті людини чи ще за її життя, оскільки чим швидше відбудеться трансплантація, – тим вища ймовірність приживання органу та збереження його функціонування. Склади злочинів у формі штучного введення в незворотну кому в післяопераційний період за наслідками нескладних операцій з метою трансплантації органів від відносно здорових людей, особливо іноземців та осіб, які не мають близьких родичів, траплялося в багатьох країнах, де існує «презумпція згоди на трансплантацію». В Україні й так низький рівень довіри до медичної галузі, що призводить до низького рівня ранньої діагностики багатьох хвороб, самолікування та відсутності належного оформлення медичних карток.

Для забезпечення довіри до медицини в Україні слід також запровадити ведення відеоспостереження оперативних втручань для того, щоб у разі наявності суперечок щодо медичних помилок чи халатного ставлення була можливість переглянути відео виключно особами, які є медичними та судово-медичними експертами.

Важливим медичним правом особи є право знати, які медичні маніпуляції їй будуть надаватися та можливі побічні ефекти. Наразі, це особливо актуально щодо щеплень, які згідно зі ст. 15 Закону України «Про захист населення від інфекційних хвороб» від 6 квітня 2000 року [3] є обов'язковими для відвідування дитячих закладів всупереч Конституції України [4]. Інформація про *світові дослідження* щодо побічних ефектів вакцин, їх склад та якість, правила зберігання, зареєстровані побічні ефекти та летальні випадки має бути надана кожним батькам для прийняття ними рішення про вакцинацію їхніх дітей. *Небезпечні для життя і здоров'я примусові медичні маніпуляції порушують ряд конституційних прав людини,* а середня шкільна освіта гарантується державою. До того ж, порушується логіка пояснення МОЗ України щодо порушення прав на здоров'я нещепленими дітьми відносно інших, адже та частина діток, які щеплені не можуть заразитися від нещеплених дітей відповідною інфекційною хворобою, з іншого боку зниження імунітету за наслідками щеплення може призвести до підхоплення ними інших інфекційних хвороб, від яких

вакцинація не проводиться. Тож, такі недемократичні підходи до медичної галузі слід переглядати, або відміняти деякі нормативно-правові акти через їх неконституційність.

Отже, слід зазначити, що знання пацієнтів про свої права, можливості, ризики та побічні ефекти є важливими для захисту їх здоров'я. З іншого боку, знання в медичній сфері, особливо прогнози є недосконалими і існують труднощі щодо медичної етики та користі для пацієнта щодо оголошення про наявність смертельної хвороби та прогнозу у вигляді тривалості життя пацієнта. Давно доведено факт дієвості плацебо, тому, на наш погляд, повідомлення про важкі хвороби та про ймовірний прогноз має містити інформацію про відсутність точності медичних прогнозів та про всі зареєстровані випадки позитивного лікування чи мимовільного одужання у подібних випадках. Проте, положення п. 3 ст. 285 Цивільного кодексу України [5] про те, що у разі побоювань щодо погіршення стану здоров'я або процесу лікування медичні працівники можуть приховати інформацію від повнолітньої особи про стан її здоров'я або стан здоров'я її неповнолітньої дитини, на наш погляд, слід прибрати. *Приховування або неповідомлення інформації про стан здоров'я неповнолітньої особи від 14 років та необов'язковість надання батьками (опікунами) дозволу на вчинення медичних маніпуляцій* щодо такої дитини (включно з перериванням вагітності до 12 тижнів, що може потягнути за собою безпліддя), на наш погляд, взагалі є неприпустимим явищем, яке, тим не менше, закріплене в ст. 43 Основ законодавства України про охорону здоров'я.

Крім того, законодавство не регулює можливість вибору методів лікування та діагностичних процедур особами щодо своїх близьких родичів у разі їх перебування в непритомному стані, а отже і не передбачає обов'язковість надання інформації про стан їх здоров'я. З іншого боку, більшість медичних маніпуляцій здійснюється на оплатній основі, що по факту передбачає прийняття фінансової участі близьких родичів у лікуванні. Проте, у разі прийняття змін до законодавства щодо використання органів померлої особи для трансплантації за «презумпцією згоди», право на участь в прийнятті рішень близькими родичами щодо лікування повнолітніх хворих, що перебувають у непритомному стані або стані, що не дає можливості усвідомлювати дійсність, та на здійснення захисту їх прав, поставатиме ще більш гостро. Наразі, близькі родичі мають лише право на дослідження причин смерті свого родича.

Список використаних джерел:

1. Закон України «Основи законодавства України про охорону здоров'я» від 19 листопада 1992 року // Відомості Верховної Ради України. – 1993. – № 4. – Ст. 19.
2. Майданик Р. Законодавство України в сфері охорони здоров'я: система і систематизація // Доктрина медичного права. – Ст. 63-74.
3. Закон України «Про захист населення від інфекційних хвороб» від 6 квітня 2000 року // Відомості Верховної Ради України. – 2000. – № 29. – Ст. 228.
4. Конституція України від 28 червня 1996 року // Відомості Верховної Ради України. – 1996. – № 30. – Ст. 141.
5. Цивільний кодекс України від 16 січня 2003 року // Відомості Верховної Ради України. – 2003. – №№ 40-44. – Ст. 356.

----------***----------

Ткачук Т., д.ю.н., доцент
Навчально-науковий інститут
інформаційної безпеки
Національної академії СБ
України.

СУЧАСНІ ДОМІНАНТИ ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА

Світ вступає в епоху грандіозних соціальних змін, технологічних і культурних перетворень. Потенціал техніки, незмінно нарощуваний, робить вирішальний вплив на всі сфери життя людського суспільства. Зростає продуктивність праці, змінюється в десятки, сотні разів його зміст. Вони змінюють лад культури і впливають на формування всієї цивілізації. Людський інтелект, його міць багаторазово збільшуються завдяки революції інформаційно-комунікаційних технологій. Соціальна структура суспільства опиняється під надмірним впливом технологічних нововведень. Процес технологічної сингулярності пройшов етап свого філософського осмислення до повсякденної реальності: роботи почали витісняти людей із звичних для них професій, більше того, окремі роботи вже отримали громадянство. І що саме головне, у роботів з'явилась здатність до еволюції, що було виключно прерогативою людства. Не дарма на останньому форумі в Давосі генеральний секретар Організації Об'єднаних Націй Антоніу Гутерреш виступив з ініціативою розробити закони ведення активності у кіберпросторі та застосування штучного інтелекту у військових умовах [1].

Суть у тому, що відбуваються трансформації, бо народжується новий цивілізаційний устрій, в якому сфера праці, наука та освіта, державне

управління, культура будуть носити принципово інший характер. Зміни, як відомо, це завжди і можливості, і загрози.

Формування інформаційного суспільства є закономірним етапом еволюції сучасного соціуму, що характеризується, в першу чергу, масштабним впровадженням інформаційних технологій і розвитком глобального інформаційного простору. Процес становлення нового суспільства, обумовлений впровадженням інформаційних технологій, вимагає правильного усвідомлення його інформаційної специфіки і конструктивного розвитку закладеного в ньому потенціалу.

В інформаційному суспільстві основним чинником розвитку є перетворення людиною науково-технічної та іншої інформації у знання. Кодифікація знань і технологічний прогрес визначаються як системо утворюючі чинники соціального прогресу. Формування економіки, культури і психології відбувається в певних умовах, що складаються під впливом техніки і електроніки. IT-сфера в багатьох країнах, в тому числі і в Україні, займає лідируючі позиції по наповненню бюджету держави та у сфері зайнятості населення. Теорія постіндустріального суспільства стала своєрідним підґрунтям формування сучасної концепції інформаційного суспільства.

У цьому процесі також має велике значення вже накопичений позитивний досвід попередніх поколінь, як правило, закріплений в міфах, переказах, моральних нормах і принципах, інакше - культурі соціуму. Так, в сутнісному плані інформаційна безпека - це стан об'єкта (суб'єкта), при якому інформаційне середовище, в якому він функціонує, дозволяє зберігати можливість і здатність реалізовувати свої рішення, відповідно до цілей, спрямованих на прогресивний розвиток. Подібний стан рівноваги всієї системи визначається нами як стійкий [2].

Можна зробити висновок, що безпека визначається, як можливість системи протистояти небезпекам, а так само - здатність переходити в своєму розвитку до більш високого рівня. Процедура захисту безпечного стану необхідна для нормального функціонування і прогресивного розвитку системи. На наш погляд, безпека розглядається в якості однієї з характеристик життєзабезпечення будь-якого об'єкта, а також - у якості іманентної здатності даного об'єкта реагувати на спотворення власних цінностей, цілей, інтересів, інакше - підстав існування даної системи.

Зазначене вище означає, що інформаційна безпека досягається не тільки за рахунок засобів, методів і заходів, спрямованих на захист інформаційного середовища і захист об'єкта (суб'єкта) від деструктивного впливу, але й через розбудову спроможності у об'єкта (суб'єкта) ухилятися

від деструктивного інформаційного впливу. Таким чином, завдання забезпечення інформаційної безпеки полягає в тому, щоб створити оптимальні умови для функціонування інформаційної інфраструктури, головний елемент якої, не комп'ютер, але людина, міг прогресивно розвиватися і діяти, згідно зі своїми цінностями та цілями. Підкреслимо зазначену думку як вузлову в нашому дослідженні.

Отже, невід'ємною характеристикою інформаційного суспільства є наявність людей здатних до критичного мислення, тобто здатності перетворювати інформацію у знання. Дані процеси мають своє філософсько антропологічний та екзистенціальний вимір. Суть якого, гіпотетично, концентрується в ноосфері.

Людина, володіючи здатністю розумно мислити і перетворювати світ навколо себе, створила ноосферу (від *грец. noos – розум і sphere – сфера*). Давньогрецькі філософи Платон і Аристотель вважали, що «нус» – це найбільш важлива частина людської душі: «розум»; «розумна частина душі» [3, с. 11].

У цьому антропогенному середовищі виділилися три основні сфери людської діяльності, що направляють соціальний розвиток: *виробнича, технологічна* та *інформаційна*. На сучасному етапі суспільного розвитку, завдяки своєму визначальному значенню для подальшому глобальному розвитку цивілізації, домінуючою стає інформаційна. Остання й є втіленням ноосфери про яку говорив видатний французький філософ, вчений (палеонтолог, антрополог, археолог) і католицький теолог (член ордена єзуїтів, священик) П'єр Тейяр де Шарден. Авторство даного терміну належить теж французькому мислителю, представнику католицького модернізму, математику Едуару Луі Емманюелю Жюльєн Леруа [4]. Ідеї Леруа розвинув його близький друг П'єр Тейяр де Шарден. У своїй праці «Феномен людини» П'єр Тейяр де Шарден резюмує, що найбільш проникливий дослідник нашої сучасної науки може виявити тут, що все цінне, все активне, все прогресивне, з самого початку містилося в космічному клапті, з якого вийшов наш світ, тепер сконцентровано в «короні» ноосфери [5, с. 295]. Наступним кроком розвитку людства, окрім самоконцентрації ноосфери, є приєднання її до іншого розумового центру, ступінь розвитку якого вже не потребує матеріального носія – вважав П'єр Тейяр де Шарден. Варто зазначити, що основні праці П'єр Тейяр де Шарден написав у 40-их роках минулого століття. З появою Інтернету, розвитком інформаційно-комунікаційних технологій та штучного інтелекту філософські погляди цього видатного вченого, на які Ватикан накладав

заборони і вважав єретичними, сьогодні здаються цілком логічними та обґрунтованими.

За П.Т. де Шарден людство пройшло розвиток від інстинкту до думки. Людство дійсно навчилось мислити за декілька останніх тисячоліть, що виявилось у спадщині творів науки, мистецтва, музики, літератури, архітектури тощо і наблизилось до переходу на новий виток своєї еволюції. Що ж буде після «думки»? Однозначно можна стверджувати, що в основі подальших еволюційних витків людства буде покладено знання, які отримані на основі інформації, тобто її критичного аналізу. Також можна спрогнозувати більш тісне «співробітництво» релігії й науки про що також говорив П.Т. де Шарден: «Релігія і наука – дві нерозривно пов'язані сторони, або фази, одного і того ж повного акту пізнання, який тільки один зміг би охопити минуле й майбутнє еволюції, щоб їх розглянути, виміряти і завершити» [5, с. 245].

Все це може призвести або до розвитку унікальних можливостей «черпати» («підключатися») до універсального глобального банку даних, або до можливостей управління колективним розумом з єдиного центру. Людський розум створив техніку наділену штучним інтелектом – розумні речі, як прийнято їх називати Інтернет речі. Тепер цей породжений людиною інтелект створює для цієї людини блага, більше того він вже думає за неї. Людина створила не мов би ще один мозковий центр для себе. На найбільш примітивному рівні це виглядає так: наш смарт годинник, порахувавши кількість калорій за день, дає команду нашому холодильнику щодо варіантів вечері; чи ранішній будильник дає сигнал кавоварці про те що ми прокинулись і можна заварювати каву. Уявімо що буде у найближчій перспективі через 10-20 років, зважаючи на шалений прогрес за останнє десятиліття.

Список використаних джерел:

1. Укрінформ. URL: https://www.ukrinform.ua/rubric-technology/2626228-gensek-oon-vvazae-so-potribni-zakoni-dla-zastosuvanna-robotiv-u-vijnah.html

2. Ткачук Т. Ю. Забезпечення інформаційної безпеки в умовах євроінтеграції України: правовий вимір: моногр. К.: ВД «АртЕк», 2018.422с.

3. Швецова-Водка Г. Учення про ноосферу як підстава розвитку ноокомунікації // Український журнал з бібліотекознавства та інформаційних наук. № 2. 2018. С. 10-22

4. Le Roy E. Les origines humaines et Г evolution de Г intelligence. Paris, 1928. 376 p.

5. Тейяр де Шарден П. Феномен человека: Сб. очерков и эссе: пер. с фр. / сост. и предисл. В.Ю. Кузнецов. М.: ООО «Издательство АСТ». 2002. 553с.

----------***----------

Дубняк М. В., к. ю. н.,
старший викладач КПІ ім.
Ігоря Сікорського.

ТЕХНОЛОГІЯ DEEPFAKE: ЗАГРОЗА ІНТЕЛЕКТУАЛЬНІЙ ВЛАСНОСТІ ЧИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ?

Використання передових нейромережевих технологій може призводити як до порушення прав інтелектуальної власності так і нести загрози інформаційній безпеці. Метою даної публікації є визначення ризиків, які виникають у зв'язку із використанням нейромережевих технологій під час створення фото та відеоматеріалів з використанням зображень фізичної особи (Deepfake).

У цій публікації під поняттям Deepfake будемо розуміти метод поєднання та накладення існуючих зображень (як правило, людини) з метою синтезу нових реалістичних зображень та відеозаписів.

Процес створення Deepfake можна представити наступним чином.

Як і для інших нейромереж, спочатку створюється датасет — набір об'єктів на яких зображені люди у різних місцях та за різних умов наприклад, різне освітлення, відстань та кут повороту тіла і обличчя до камери тощо. Потім виконується маркування ключових областей (очі, ніс, обличчя, волосся, тіло тощо).

Відмінністю саме Deepfake є те, що у наступних кроках використовується генеративно-змагальна нейромережа (generative adversarial network - далі GAN). Це алгоритм, який застосовує комбінацію роботи двох нейромереж. Перша генерує (створює) образ, друга намагається відокремити справжні образи від згенерованих. Якщо перший алгоритм запропонував неякісну підробку, яку одразу визначив другий алгоритм, перший алгоритм удосконалює свою роботу, і далі пропонує більш реалістичний образ. За результатами такої сумісної змагальної роботи двох нейромереж можна отримати доволі непоганий результат, адже друга нейромережа визначає очевидні фейки, запропоновані першою [1].

Також існує програмне забезпечення, яке здатне імітувати голос людини. Вхідними даними є аудіозапис тривалістю кілька десятків хвилин, з якого нейромережа здатна відтворити інтонацію, мовленнєві обороти,

перетворити голос з жіночого на чоловічий і навпаки тощо. Автори проекту в етичних принципах стверджують, що модуляція голосу направлена на забезпечення права свободи візуальної ідентичності, в тому числі і права на зміну голосу в Інтернеті. Але не виключають, що технологію можуть використати не за призначенням [2].

Необхідно зауважити, що створення відеоматеріалів із зображенням фізичної особи з використанням Deepfake може відбуватись як за згодою (ініціативою) людини з урахуванням її власних дій, так і без її участі чи відома.

У першому випадку мова іде про використання особами програмного забезпечення, яке за допомогою нейромережевих технологій здійснює модифікації вихідного зображення, яке створюється або завантажується самим користувачем.

Наприклад, у 2017 році набуло вірусного поширення програмне забезпечення FaceApp, яке використовує нейромережеві алгоритми для перетворення фотографій або відео в об'єкти образотворчого мистецтва. Ця програма дозволяє виконувати зміну фону або переднього плану, накладання об'єктів один на одного, клонувати / копіювати стиль або ефект з іншого зображення або відео, та навіть робити імітацію стилів різних відомих художників. Програма дозволяє робити фотографії / відео шляхом безпосереднього використання додатка або завантажувати в додаток вже існуючі фотографії / відео [3].

У вересні 2019 року з'явилось програмне забезпечення ZAO, яке дозволяє замінювати обличчя акторів у фрагментах відеофільму на обличчя користувача. Для здійснення цих дій користувач надає право збирати про себе таку інформацію: номер мобільного телефону, фото та відеоматеріали із зображенням користувача, що містяться у його мобільному телефоні, камеру мобільного телефону та інші дані [4]. У бібліотеці містяться короткі фрагменти відомих відеофільмів (наприклад, кінофільм "Титанік" з Леонардо ДіКапріо, або фрагменти серіалу "Гра престолів").

Отже, правилами користування встановлено, що при завантажені вказаного програмного забезпечення користувач погоджується із цими умовами та надає згоду на збір і обробку усіх перелічених даних, необхідних для перетворення зображень, за допомогою нейромережевих технологій.

Чи відповідають такі правила користування програмним забезпеченням умовам охорони інтересів фізичної особи, яка зображена на фотографіях та інших художніх творах? Чи не порушуються майнові і немайнові права акторів з фрагментів кінофільмів, які завантажені у додаток?

Відповідно до ст. 307, 308 ЦК України фізична особа може бути знята на фото-, кіно-, теле- чи відеоплівку лише за її згодою. Фотографія, інші художні твори, на яких зображено фізичну особу, можуть бути публічно показані, відтворені, розповсюджені лише за згодою цієї особи.

Таким чином, користувач шляхом вчинення конклюдентних дій (як під час завантаження програмного забезпечення, так і під час завантаження власних фотографій / відео для обробки) надає свою згоду на використання його зображень і збереження персональних даних на серверах компанії-розробника програмного забезпечення.

Щодо використання нейромережевих технологій, результатом яких є фото та відео із зображенням фізичної особи без її участі та без її відома, прикладом можуть слугувати наступні випадки.

Створений американським режисером Джорданом Пілом за допомогою нейромереж і графічного редактора Adobe After Effects відеоролик, на якому, 44 - й президент США Б.Обама принижує нинішнього Президента США Д. Трампа. Таким чином режисер хотів показати загрози, які несе в собі використання нових технологій: “коли будь-хто може змусити будь-кого сказати що завгодно у будь-який момент часу”[5].

Інший приклад — скандальний стартап DeepNude, який за допомогою нейромереж “роздягає” жінок, зображених на фото[1].

Ризики для системи права інтелектуальної власності

Ризик втрати творчого самовираження

Бачили фразу у кінці титрів “створення цього фільму забезпечило 15000 робочих місць”? А тепер уявіть процес створення кінофільму нейромережею. З розвитком технологій deepfake ні актори, ні звукорежисери, ні оператори ні сценаристи будуть не потрібні, що призведе до втрати таких професій і створення контенту абсолютно новим способом.

Культура цінна своєю багатоманітністю способів її вираження у матеріальних формах. Світ, в якому об’єкти авторського права буде створювати нейромережа на основі аналізу великих даних, приречений на обмеження культурного розвитку людства.

Таким чином, ризикуємо опинитись у замкнутому середовищі синтезованого контенту, без альтернатив до розвитку інших видів творчості, які не виражені в інтернеті або не додані в датасет.

Порушення прав на недоторканість твору

1 Нейромережу DeepNude навчили роздягати жінок на фото. Як це працює URL: https://fakty.com.ua/lifestyle/20190627-nejromerezhu-deepnude-navchyly-rozdyagaty-zhinok-na-foto-yak-tse-pratsyuye/ (дата звернення:6 0.09.2019)

Відповідно до ст. 9 Закону України “Про авторське право і суміжні права” частина твору, яка може використовуватися самостійно, у тому числі й оригінальна назва твору, розглядається як твір і охороняється відповідно до цього Закону.

Отже, використання фрагментів кінофільмів для заміни своїм обличчям справжніх кіноакторів має наслідком порушення прав на недоторканість твору, і одночасно посягає на немайнові права акторів та актрис.

Вказані дії не можуть підпадати під правовий захист пародій, адже пародія — це твір, який є творчою переробкою іншого правомірно оприлюдненого твору або його частини, що за своїм змістом має комічний, сатиричний характер або спрямовується на висміювання певних подій або осіб.

У випадку відеороликів створених за допомогою ZAO, технологія заміни обличчя не має ознак творчого комічного і сатиричного характеру, адже діалог, сюжетна лінія і показ образів залишаються без творчих і переробок, що має наслідком лише спотворення оригінального твору.

Ризики для інформаційної безпеки

Інформаційна безпека — стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації.

Несанкціоноване розповсюдження недостовірної інформації та використання технологій Deepfake для скоєння злочинів, кібератак, провокацій (в тому числі і як елементів гібридної війни).

За даними Wall Street Journal, шахраї за допомогою програм голосової імітації підробили голос директора компанії в видали розпорядження про перерахунок 220 000 євро. Генеральний директор енергетичної компанії з Великобританії думав, що розмовляє по телефону зі своїм керівником, генеральним директором німецької материнської компанії, який попросив відправити кошти угорському постачальнику.

Традиційні інструменти кібербезпеки, розроблені для захисту хакерів від корпоративних мереж, не можуть виявити підроблення голосу [6]. Сервіси із розробки стратегій кіберзахисту виявились неготовими до таких ризиків. Відповідних протоколів із захисту даних чи алгоритму дій працівника по підтвердженню наказу керівника не розроблено. Фактично,

така ситуація призводить до необхідності розробки алгоритмів верифікації з багатоступеневим рівнем перевірки — що, потенційно, перетворить процес управління і ведення бізнесу у тотальну верифікацію.

Нанесення шкоди фізичній особі через негативні наслідки застосування технологій.

Зображення фізичної особи залежно від форми вираженням має подвійний правовий режим — як об'єкт авторського і суміжного права, так і інформаційний об'єкт. При створенні діпфейків з використанням зображення фізичної особи без її відома порушуються такі права: поширення фото та відео із зображенням фізичної особи без її дозволу, право на особисте життя та його таємницю, право на повагу гідності і честі, право на індивідуальність, право на недоторканість репутації, порушення гарантій щодо невтручання в особисте життя.

Висновок: у світі триває обговорення етичних принципів розробки та використання нових технологій, але вже зараз можна побачити, що технології будуть використовувати із порушенням будь-якого етичного і правового регулювання. У цій публікації лише поверхнево описані ризики, які порушують інтереси осіб, і одночасно посягають на права, захист яких передбачений різними інститутами права — як цивільного, інформаційного права та права інтелектуальної власності. Вказане свідчить про складний і комплексний характер цих ризиків і необхідності розробки комплексних правових механізмів для їх мінімізації.

Список використаних джерел:

1. Баловсяк Н. Deep fake: когда нейронные сети становятся искуснее пропагандистов URL: https://www.stopfake.org/ru/deep-fake-kogda-nejronnye-seti-stanovyatsya-iskusnee-propagandistov/ (дата звернення: 10.09.2019)
2. ETHICS URL: https://modulate.ai/ (дата звернення: 10.09.2019)
3. FaceApp: Terms of Use 08.03.2017 URL: https://www.faceapp.com/terms (дата звернення: 10.09.2019)
4. ZAO: Terms of Use 07.09.2019 URL: https://h5.ai-factory.com/zao/static-pages/protocol.html?name=privacy (дата звернення: 10.09.2019)
5. You Won`t Belive What Obama Says in This Video URL: http://youtu.be/cQ54GDm1eL0 (дата звернення: 10.09.2019)
6. Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case URL: https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402 (дата звернення: 10.09.2019)

----------***----------

Ямковий О. В., Качинський А. Б.,
КПІ ім. Ігоря Сікорського.

ПОШУК АНОМАЛІЙ В ПОВЕДІНЦІ КОРИСТУВАННЯ ІНТЕРНЕТ-РЕСУРСАМИ ЗА ДОПОМОГОЮ АЛГОРИТМІВ КЛАСТЕРИЗАЦІЇ МАШИННОГО НАВЧАННЯ

Анотація. В роботі представлені основні механізми машинного навчання, що вирішують задачу кластеризації як засіб для виявлення аномалій в діяльності інтернет-користувачів, а також метрики, що використовуються для оцінки якості роботи кластеризатора.

Вступ. Інформаційні технології сьогодні поширені у всіх сферах людської діяльності, тому інформація представляє велику цінність та є предметом купівлі-продажу. Здебільшого саме через це інформаційні ресурси стають об’єктом атаки з метою їх заволодіння. Це призводить до того, що актуальним стає питання захисту. У зв’язку зі збільшенням обсягів інформації, що розповсюджується в світовій мережі, та розширенням спектра завдань, що вирішуються за допомогою інформаційних систем, виникає проблема, пов’язана зі зростанням числа загроз і підвищенням вразливості інформаційних ресурсів.

В більшості систем безпеки застосовують стандартні механізми захисту: ідентифікацію та аутентифікацію, механізми обмеження доступу до інформації згідно з правами суб’єкта і криптографічні механізми. Такий традиційний підхід має певні недоліки, а саме: незахищеність від власних користувачів – зловмисників, розмитість поділу суб’єктів системи на “своїх” і “чужих” через глобалізацію інформаційних ресурсів, порівняна легкість підбору паролів внаслідок використання їхнього змістового різновиду, зниження продуктивності й ускладнення інформаційних комунікацій внаслідок обмеження доступу до ресурсів організації. Тому виникла потреба в механізмах, які би доповнювали традиційні та давали можливість виявити спроби несанкціонованого доступу й інформували про це відповідальних за безпеку або реагували у відповідь. Важливим фактором є те, щоб такі системи могли протистояти атакам, навіть якщо зловмисник вже був аутентифікований та авторизований і з формального погляду додержання прав доступу мав необхідні повноваження на свої дії. Такі функції і виконують системи виявлення вторгнень IDS (intrusion detection systems). Оскільки передбачити всі сценарії розгортання подій в системі з активним

“чужим” суб’єктом неможливо, потрібно або якомога детальніше описати можливі “зловмисні” сценарії або ж, навпаки, – “нормальні” і прийняти, що всяка активність, на яку не поширюється прийняте розуміння “нормальності”, є небезпечною. Системи IDS поділяються на системи, що реагують на відомі атаки, – системи виявлення зловживань MDS (misuse detection systems) і системи виявлення аномалій ADS (anomaly detection systems), які реєструють відхилення розвитку системи від нормального перебігу.

В даній роботі пропонується розглянути і застосувати деякі методи машинного навчання для вирішення задачі кластеризації, що в свою чергу можуть застосовуватися як механізм виявлення аномалій в поведінці користувачів.

1. Основні алгоритми кластеризації

Кластеризація (або кластерний аналіз) - це задача розбиття множини об'єктів на групи, які називаються кластерами. Усередині кожної групи повинні виявитися «схожі» об'єкти, а об'єкти різних груп повинні бути різними.

Застосування кластерного аналізу в загальному вигляді зводиться до наступних етапів:

- Відбір вибірки об'єктів для кластеризації.
- Визначення змінних, за якими будуть оцінюватися об'єкти у вибірці. При необхідності - нормалізація значень змінних.
- Обчислення значень міри схожості між об'єктами.
- Застосування методу кластерного аналізу для створення груп схожих об'єктів (кластерів).
- Представлення результатів аналізу.

1.1 К-середніх(K-means)

Алгоритм К-середніх, напевно, є найпопулярнішим та найпростішим алгоритмом кластеризації, та має не складне представлення у вигляді псевдокоду:

1. Обирається кількість кластерів K, що на думку експерта здається оптимальним для отриманих даних.
2. Висипати випадковим чином в простір даних k точок (центроїдів).
3. Для кожної точки набору даних порахувати, до якого центроїду вона ближче.
4. Перемістити кожен центр ваги в центр вибірки, яку відносимо до цього центроїду.

5. Повторювати останні два кроки фіксовану кількість разів, або до тих пір поки центроїди не «зійдуться" (зазвичай це означає, що їх зміщення відносно попереднього положення не перевищує якогось заздалегідь заданого невеликого значення).

У випадку звичайної евклідової метрики для точок, що лежать на площині, цей алгоритм дуже просто розписується аналітично.

На відміну від завдання класифікації або регресії, в разі кластеризації складніше вибрати критерій, за допомогою якого було б просто уявити завдання кластеризації, як задачу оптимізації.

У разі К-середніх поширений ось такий критерій - сума квадратів відстаней від точок до центроїдів кластерів, до яких вони належать

$$J(C) = \sum_{k=1}^{K} \sum_{i \in C(k)} \|x(i) - \mu(k)\|^2 \to \min_C \quad ,$$

де С - множина кластерів потужності К μ(k) - центроїд кластера С(k).

Кінцевою метою є отримання ситуації, коли точки розташовуються якомога ближче біля центрів своїх кластерів. Але мінімум такого функціоналу буде досягатися тоді, коли кластерів стільки ж, скільки і точок, тобто кожна точка - це кластер з одного елемента.

Для вирішення цього недоліку вибирають таке число кластерів, починаючи з якого описаний функціонал J(c) падає "вже не так швидко".

$$D(k) = \frac{|J(C(k)) - J(C(k+1))|}{|J(C(k-1)) - J(C(k))|} \to \min_K$$

1.2. Метод поширення близькості (affinity Propagation)

На відміну від алгоритму К-середніх, даний підхід не вимагає заздалегідь визначати число кластерів, на яке ми хочемо розбити дані. Основна ідея алгоритму полягає в тому, що нам хотілося б, щоб наші спостереження кластеризувалися в групи на основі того, наскільки вони схожі один на одного.

Необхідно створити метрику подібності, що визначається наступним чином:

$$s(x(i), x(j)) > s(x(i), x(k)) \,,$$

тобто, якщо спостереження x(i) більш схоже на спостереження x(j), ніж на x(k). Простим прикладом такої схожості буде негативний квадрат відстані:

$$s(x(i), x(j)) = -\|x(i) - x(j)\|^2$$

Наступним кроком є ініціалізація двох матриць, перша описує наскільки добре k-те спостереження підходить для того, щоб бути "прикладом для наслідування" для і-того спостереження щодо всіх інших потенційних "прикладів", а друга буде описувати, наскільки правильним було б для і-того спостереження вибрати k-те як такого "прикладу". Після цього елементи матриць оновлюються за наступними правилами:

$$r(i,k) \leftarrow s(x(i),x(k)) - \max_{k \neq k}\{a(i,k) + s(x(i),x(k)\},$$

$$a(i,k) \leftarrow \min\left(0, r(i,k) + \sum_i \max(0, r(i,k)\right), i \neq k$$

$$a(k,k) \leftarrow \sum_i \max(0, r(i,k)$$

1.3 Спектральна кластеризація (spectral clustering)

Спектральна кластеризація об'єднує кілька описаних вище підходів, щоб отримати максимальну точність від складних різноманіть розмірності, меншої від початкового простору.

Для роботи алгоритму необхідно визначити матрицю схожості спостережень (adjacency matrix):

$$A(i,j) = -\|x(i) - x(j)\|^2$$

Ця матриця описує повний граф з вершинами в спостереженнях і ребрами між кожною парою спостережень з вагою, відповідним ступенем схожості цих вершин. Далі необхідно розділити отриманий граф на дві частини таким чином, щоб отримані точки в двох графах були більш схожі на інші точки всередині отриманої своєї половини графа, ніж на точки в другій половині.

1.4 Агломеративна кластеризація (agglomerative clustering)

Агломеративна кластеризація – найпростіший алгоритм кластеризації без фіксованої кількості кластерів. Алгоритм складається з наступних кроків:

- Кожному спостереженню присвоюється своє значення кластеру;
- Сортуються попарні відстані між центрами кластерів по зростанню;
- Обирається пара найближчих кластерів, відбувається їх об’єднання в один і перераховується центр кластера;
- Попередні дві дії повторюються до тих пір, поки всі дані не об’єднаються в один кластер.

Процес пошуку найближчих кластерів може відбуватися з використанням різних методів об'єднання точок:

Single linkage - мінімум попарних відстаней між точками з двох кластерів

$$d(C(i),C(j)) = \min_{x(i) \in C(i), x(j) \in C(j)} \|x(i) - x(j)\|$$

Complete linkage - максимум попарних відстаней між точками з двох кластерів

$$d(C(i),C(j)) = \max_{x(i) \in C(i), x(j) \in C(j)} \|x(i) - x(j)\|$$

Average linkage - середнє попарних відстаней між точками з двох кластерів

$$d(C(i),C(j)) = \frac{1}{n(i)n(j)} \sum_{x(i) \in C(i)} \sum_{x(j) \in C(j)} \|x(i) - x(j)\|$$

Centroid linkage – відстань між центроїдами двох кластерів

$$d(C(i),C(j)) = \|\mu(i) - \mu(j)\|$$

2. Метрики якості кластеризації

2.1 Adjusted Rand Index (ARI)

Передбачається, що відомі істинні мітки об'єктів. Дана міра не залежить від самих значень міток, а тільки від розбиття вибірки на кластери. Нехай n - число об'єктів у вибірці. Позначимо через a - число пар об'єктів, що мають однакові мітки і знаходяться в одному кластері, через b - число пар об'єктів, що мають різні мітки і знаходяться в різних кластерах. Тоді Rand Index має наступне представлення:

$$RI = \frac{2(a+b)}{n(n-1)}$$

Rand Index (RI) показує схожість двох різних кластеризацій однієї і тієї ж вибірки. Щоб цей індекс давав значення близькі до нуля для випадкових кластеризацій при будь-якому n і числі кластерів, необхідно унормувати його. Так визначається Adjusted Rand Index:

$$ARI = \frac{RI - E[RI]}{\max(RI) - E[RI]}$$

Даний індекс є мірою відстані між різними розбивками вибірки. ARI приймає значення в діапазоні [-1, 1]. Негативні значення відповідають "незалежним" розбиття на кластери, значення, близькі до нуля, - випадковим розбиття, і позитивні значення свідчать про те, що два розбиття схожі (збігаються при ARI = 1).

2.2 Silhouette

Даний коефіцієнт не передбачає знання істинних міток об'єктів, і дозволяє оцінити якість кластеризації, використовуючи тільки нерозмічену вибірку і результат кластеризації. Спочатку силует визначається окремо для кожного об'єкта. Позначимо через a середню відстань від даного об'єкта до об'єктів з того ж кластера, через b середню відстань від даного об'єкта до об'єктів з найближчого кластера (відмінного від того, в якому лежить сам об'єкт). Тоді силуетом даного об'єкта називається величина:

$$s = \frac{b-a}{\max(a,b)}$$

Силуетом вибірки називається середня величина силуету об'єктів даної вибірки. Таким чином, силует показує, наскільки середня відстань до об'єктів свого кластера відрізняється від середньої відстані до об'єктів інших кластерів. Дана величина лежить в діапазоні [-1, 1]. Значення, близькі до -1, відповідають поганим (розрізненим) кластеризаціям, значення, близькі до нуля, кажуть про те, що кластери перетинаються і накладаються один на одного, значення, близькі до 1, відповідають чітко виділеним кластерам. Таким чином, чим більше силует, тим чіткіше виділені кластери.

Висновки. В роботі розглянуто основні алгоритми машинного навчання для вирішення задачі кластеризації, запропоновані алгоритми використовуються як механізм виявлення аномалій в поведінці користування інтернет-ресурсами, представлені метрики оцінки якості роботи кластеризатора для побудови оптимальної моделі з найкращими значеннями параметрів.

Список використаних джерел:

1. Denning D.E. An intrusion-detection model / Denning D.E. // In Proc. IEEE Symposium on Security and Privacy. – 1986. – С. 118-131.
2. Somayaji A. Automated response using system-call delays / Somayaji A. // In Proc. of USENIX Security Symposium 2000. – 2000. – С. 185-197.
3. Forrest S., Hofmeyr S.A., Somayaji A., and Longstaff T.A. A sense of self for Unix processes / Forrest S., Hofmeyr S.A., Somayaji A., and Longstaff T.A // In Proc. of the 1996 IEEE Symposium on Research in Security and Privacy, IEEE Computer Society Press. – 1996. – С. 120-128.
4. Lane T. and Brodley C. E.. Temporal sequence learning Lviv Polytechnic National University Institutional Repository. – http://ena.lp.edu.ua, 104 and data reduction for anomaly detection / Lane T. and Brodley C. E. // ACM Transactions on Information and System Security. – 1999. – 2(3). – С. 295-331.
5. Theus M. and Schonlau M. Intrusion detection based on structural zeroes / Theus M. and Schonlau M. // Statistical Computing and Graphics Newsletter. – 1998. – 9(1). – С. 12-17.
6. Tan K. The application of neural networks to unix computer security / Tan K. // In Proc. of the IEEE International Conference on Neural Networks. – 1995. – С. 476–481.
7. Ryan J., Lin M., and Miikkulainen R. Intrusion detection with neural networks / Ryan J., Lin M., and Miikkulainen R. // Advances in Neural Information Processing Systems. – 2015. – С. 254-272.

----------*----------**

Мнишенко М. О., *4 курс, ФСП*
КПІ ім. Ігоря Сікорського.

«ДЕРЖАВА В СМАРТФОНІ», ЯК ШЛЯХ ДО ЕЛЕКТРОННОГО КОНЦТАБОРУ

В часи швидкого розвитку технологій з’являється все більше пропозицій до того, щоб швидкими темпами перейти до концепції «Держава в смартфоні», яка нам пропонує полегшений, швидкий та навіть прямий доступ до державного управління. В даних тезах Я викладу свою думку стосовно даної тенденції та зазначу що на мою думку є негативного в спробах провадити цифрові технології в усі сфери життя суспільства.

Слід зазначити, що частина функцій цієї концепції вже певний час діє і дійсно частково полегшує здійснення адміністративної діяльності, дозволяє більш швидко подавати документи та отримувати відповіді на звернення тощо. Але далі нам пропонують здійснювати підприємницьку, цивільну, адміністративну діяльність лише таким способом створюючи максимальну залежність від цієї технології. Врешті-решт реформи в цій сфері зводяться до того, щоб особа була прив'язана до свого телефону і не могла без нього здійснити фактично жодних дій. Окрім цього, нам пропонують в майбутньому обирати і керівництво держави через пристрій.

Все що викладено вище має пряме відношення до інформаційної безпеки і саме ця концепція напряму створює ще більшу загрозу ніж існувала до цього часу. Характерно, що з розвитком інформаційних технологій рівень інформаційної небезпеки лише збільшувався. «Держава в смартфоні» прив'язує людину до телефону, картки, коду чи іншого пристрою, який буде необхідний для завершальної стадії проекту в цьому ж аспекті передбачається і надання особою своїх даних, які розповсюджуватимуться на все де існує електронний зв'язок, а це навіть на даний момент фактично усі сфери життя. Я не буду стверджувати щодо очевидних речей про порушення права на конфіденційність та інших так званих прав людини, бо не має сенсу визнавати декларації ООН, які сприяють концепціям, що порушують їх же декларативні акти.

Тут слід говорити про те, що у випадку проникнення до електронної системи, або використання її розпорядниками зі злочинним умислом ми стикаємось із ситуацією, коли фактично всі державні, економічні та соціальні функції будуть паралізовані або направлені в те русло, яке може бути необхідним особі або особам, що здійснюватимуть злочинну діяльність. Доступ та можлива відкритість особистих даних є лише меншою проблемою, що стає більш гострою при впровадженні цієї системи.

Прямий доступ громадян до управління державою є так само завершальною стадією до створення охлократії, що впроваджувалася шляхом демократичних перетворень, в свою чергу підкріплення цієї охлократії електронним контролем ми отримуємо електронне єдиновладдя згори, бо буде відсутня реальна можливість довести втручання в систему або її збій чи використання отриманих даних зі злочинним умислом та хаос знизу, коли переконаний у своїй абсолютній владі народ буде вважати себе господарем ситуації здійснюючи те, що насправді продиктовано «електронним урядом».

Підбиваючи підсумки, і повертаючись до назви даної теми, Я наголошую на тому, що шлях «до смартфону» це шлях до концтабору з

цифровою залежністю населення і неможливістю вийти з-під такої системи законним шляхом, а тому це є пряма інформаційна небезпека для всіх громадян.

----------***----------

Дмитренко М. А., ІСЗРУ,
в. о. проректора з наукової
роботи, доктор політичних
наук, професор, заслужений
діяч науки і техніки України.

ПРОБЛЕМНІ ПИТАННЯ ІНФОРМАЦІЙНОЇ ПОЛІТИКИ УКРАЇНИ ТА ШЛЯХИ ЇХНЬОГО ВИРІШЕННЯ

Аналіз тенденцій у міжнародному інформаційному просторі дає підстави стверджувати, що наша держава стала об’єктом інформаційних атак (інформаційно-психологічних акцій), які є свідченням спроби встановити контроль над усіма сферами існування української держави та суспільства. Це зумовлює необхідність перегляду організаційних засад управління інформаційною політикою держави, переосмислення ролі державних органів в протистоянні зовнішньополітичним впливам, розробки системи нових підходів до організації і проведення спеціальних інформаційних операцій як однієї з форм забезпечення національної безпеки, вдосконалення методів організаційно-управлінської адаптації системи забезпечення національної безпеки до вимог сьогодення. Недооцінка важливості проведення з боку України акцій інформаційного впливу, спрямованих на підтримку її національних інтересів і державної політики за кордоном, як засвідчують останні події, завдає державі величезних економічних, політичних, іміджевих та інших збитків.

Інформаційна, і не лише інформаційна, війна РФ проти України зумовлена її стремлінням будь-якою ціною утримати Україну в зоні своїх стратегічних інтересів, створити таким чином у західному напрямі «пояс безпеки» для Росії. Сам характер та особливості ведення російсько-української війни засвідчує, що її метою є зміна ідентифікацію населення і перетворення східного регіону нашої держави на «сіру зону», яка залишить їй важелі впливу на український уряд через постійну загрозу поширення нестабільності на всю Україну. Це війна не за території, а за світогляд, думки і душі людей. Нажаль цю війну ми доки не виграли. У чому ж причина проблем нашої інформаційної політики.?

По перше, - це нескінченні конфлікти всередині політичної еліти, яка виявляє нездатність усвідомити розкол як внутрішню проблему суспільства й тяжіє до розуміння цих проблем як підступів зловмисників і конкурентів, яких потрібно виявити, а ще краще знешкодити.

Жодні зовнішні інформаційні впливи не могли завдати більшої шкоди для консолідації нації, ніж свої чи заслані політики, які десятиліттями вмонтовували в свідомість українського народу ідеї меншовартості російського або українського етносу. Слід визнати, що до розколу в Україні, який відбувся на ментальному рівні, доклали чимало зусиль українські політики. Принцип управління «розділяй і владарюй» особливо активно почали культивувати політичні сили з 2004 р. в боротьбі за владу, поділяючи Україну на «бандерівський» захід і «бандитський» схід та прищеплюючи українському народові постулати високої культури й інтелігентності одних і варварства інших тощо. Перемога, отримана через розкол нації, – це піррова перемога, тому що сили, які програли на певних виборах, робитимуть усе для свого реваншу, діючи за принципом «що гірше, то ліпше».

Тому маємо констатувати, що для пошуку політичної злагоди в суспільстві влада повинна запропонувати свою програму досягнення консенсусу між традиційними цінностями й реальними суспільними відносинами Ігнорування цього факту призводить до тяжких, непередбачуваних наслідків. Нинішня ситуація в Україні чимось нагадує проблеми становлення США, війну між цивілізованою північчю і рабовласницьким півднем за відстоювання своїх традиційних цінностей, яка закінчилася прийняттям конституції 1787 р. після довгих і складних перемовин.

По-друге, -це корупція. Корупція як внутрішня агресія багато в чому більш небезпечна за зовнішню. Вона не тільки послаблює фронт боротьби на Донбасі, а й сіє зневіру суспільства до влади, в успішності реформ і можливості поліпшення життя. Корупція нині проникла в усі сфери суспільного життя, а чесність, порядність, обов'язковість, професіоналізм уже не сприймаються як моральні орієнтири соціальної поведінки. Це створює загрозу не лише для майбутнього української демократії, а й для існування самої держави. Якщо держава не здатна отримати перемогу на внутрішньому фронті боротьби з корупцією, то не може бути мови про перемогу на інформаційному фронті.

По-третє демагогія, яка перетворилася на основний засіб прикриття неспроможності владних структур. Донині декларування влади щодо проведення певних дій зовсім не означало, що це насправді буде зроблено.

Парадокс полягає в тому, що політична еліта розмовами про євроінтеграцію, шлях до цивілізаційного простору, підвищення соціальних стандартів прикривала небажання що-небудь радикально змінювати: чи це стосується боротьби з корупцією, чи проведення реформ у судовій, правоохоронній, економічній та інших сферах.

По-четверте, критерієм ефективності влади є рівень довіри й підтримки її дій народом або хоч би основною його частиною чи основними соціальними групами. Зрозуміло, що такої довіри до політичних владних структур в Україні досі немає, оскільки влада елементарно не виконує своїх обіцянок. Крім того, політична влада в Україні всіх рівнів недооцінює, а може, й не розуміє необхідності створення оптимально сприятливого суспільного середовища свого функціонування в нинішніх умовах.

По п'яте, довіра до влади починається з рівності всіх перед законом, з правової держави. А особливістю правової держави є повна гарантованість і непорушність свобод громадян, а також принцип взаємної відповідальності громадянина і держави. Як громадяни несуть відповідальність перед державою, так і державна влада повинна нести відповідальність перед громадянами. У цьому напрямі значна роль відводиться ЗМІ. І украй важливо не допускати насильницьких дій з боку влади проти журналістів, точка зору яких не співпадає з провладною з тих або інших питань.

Необхідно розуміти, що нинішні інформаційні війни – це один з основних інструментів досягнення геополітичного домінування. І доки ми не перестанемо сприймати людей – об'єктів інформаційної політики (читачів, глядачів, слухачів) як масу не здатну критично мислити, доти всі наші зусилля, направлені на реалізацію дій влади не матимуть успіху. Наразі маємо багато альтернативних джерел інформації таму у людей є можливість аналізувати й виокремлювати раціональне зерно з явної чи скритої неправди, підтасовки фактів або дезінформації.

Відсутність довіри народу до влади це - одна з ключових проблем української політичної реальності, а якщо бути точніше - взаємного неприйняття між народом і політичними елітами. За недовіри і конфліктів будь-які потенційні реформи і зміни приречені на невдачу. Звичайно, в умовах конкурентної боротьби контроль над політичною інфраструктурою перетворюється на один із основних ресурсів влади, дає підстави для формування суспільної думки, яка завжди спочатку виявляється в певних переконаннях, а вже потім у конкретних діях. Але щоб цей контроль давав необхідну віддачу треба користуватися ним професійно, зокрема, на інституційному рівні.

Нині забезпеченням окремих напрямів інформаційної безпеки опікується низка органів державної влади, зокрема МІП , Національна рада України та Державний комітет з питань телебачення й радіомовлення, Національна комісія державного регулювання у сфері зв'язку та інформатизації, МЗС, МВС , СБУ, МОУ, СЗР тощо. Проблема в тому, що кожен із державних органів, які беруть участь у забезпеченні інформаційної безпеки України відповідає за свій сегмент і жоден, не відповідає за загальний стан протидії інформаційній агресії через відсутність суб'єкта юридичної координації зусиль забезпечення національної безпеки в інформаційній сфері. Кожен виконує свою функцію і не знає, що роблять інші відомства в цій сфері.

Свого часу «Концепція національної безпеки України» передбачала протидію інформаційній експансії іноземних держав[1]. Спеціальні інформаційні операції, які було визначено як одну з форм такої протидії, мали стати одним із ключових напрямів політики національної безпеки. Згодом в опублікований Доктрині інформаційної безпеки України також зазначалося, що «…за умов глобальної інтеграції та жорсткої міжнародної конкуренції головною ареною зіткнень і боротьби різновекторних національних інтересів держав стає інформаційний простір»[2].

У «Стратегії національної безпеки України»., до пріоритетних завдань забезпечення інформаційної безпеки визначено протидію інформаційним операціям проти України, маніпуляціям суспільною свідомістю і поширенню спотвореної інформації[3].

Проте навіть у разі успішної протидії всім інформаційним загрозам нашу державу, якщо вона не знайде можливостей проводити акції інформаційного впливу в таборі супротивника (чого також не передбачено в Стратегії), і надалі сприйматимуть як постійну державу – жертву інформаційних атак. У цьому контексті постає нагальна потреба у створенні й організації єдиної державної системи інформаційного протиборства для розроблення та «ув'язування» міжвідомчих складників (окремих акцій) у єдиному задумі скоординованої інформаційної операції держави.

Саме відсутність дієвої координації, децентралізація управління і відомчість заважають просуванню національних інтересів і державної політики України за кордоном, що призводить до негативних наслідків на інформаційному фронті. Координатором діяльності державних органів у протидії інформаційним впливам стосовно України за кордоном, який би опікувався підготовкою і проведенням акцій спеціального інформаційного впливу, спрямованого на аудиторію конкретних іноземних країн, могла б стати СЗР України, якій Законом України «Про Службу зовнішньої розвідки

України» одним із головних завдань визначено «…здійснення спеціальних заходів впливу, спрямованих на підтримку національних інтересів і державної політики України в економічній, політичній, військово-технічній, екологічній та інформаційній сферах…»[4].

Крім цього, у світовій практиці, на локалізацію зовнішніх загроз орієнтовані переважно саме розвідувальні органи. Наприклад, у системі забезпечення національної безпеки США основну роль відведено РНБ та підпорядкованому їй розвідувальному співтовариству (Intelligence Community), до складу якого входять як окремі міністерства й відомства, так і спеціальні органи відомчого підпорядкування. Поточною діяльністю розвідувального співтовариства, *яке фактично відіграє роль системи забезпечення національної безпеки на тактичному рівні*, керує Директор національної розвідки, який за посадою є радником президента США з питань розвідувальної діяльності та виконує координаційні функції. Координація та централізація розвідувальних і контррозвідувальних органів відбувається в межах розвідувального співтовариства не випадково. Згідно з американською доктриною національної безпеки розвідка й контррозвідка не є окремими ланками спеціальних служб, навпаки – контррозвідка є частиною розвідки.

У наказі президента США № 12333 від 4 грудня 1981 р. визначено, що «Розвідка повинна забезпечувати президента необхідною інформацією, на якій ґрунтується процес прийняття рішень щодо проведення та розвитку зовнішньої, оборонної чи економічної політики й захисту національних інтересів Сполучених Штатів від посягань органів безпеки іноземних держав»[5].

Чому необхідно взяти за основу формування та реалізацію державної політики у сфері інформаційної безпеки саме системи забезпечення національної безпеки США або ЄС ?

По-перше, своєчасне, упереджувальне реагування на сучасні виклики та загрози потребує побудови принципово нової системи забезпечення національної безпеки України, яка забезпечувала б скоординовану, законодавчо регламентовану діяльність її суб'єктів, спрямовану на захист національних цінностей та інтересів, а американська система нині є однією з найефективніших.

По-друге, з огляду на те, що основними цілями «Стратегії національної безпеки України» є забезпечення інтеграції України з Європейським Союзом та формування умов для вступу до НАТО, наша система забезпечення національної безпеки має бути дієво пов’язаною з

системою міжнародної й регіональної безпеки як їхній невід'ємний складник.

По-третє, у зв'язку із зовнішньополітичним інтеграційним вибором України доцільно вже зараз закладати підвалини тих нових відносин, які стануть визначальними, якщо не вирішальними, для майбутнього держави, ураховувати вимоги Європейського Союзу до сектору європейської безпеки і вносити відповідні корективи до наших нормативно-правових актів у безпековій сфері.

Список використаних джерел:

1. Доктрина інформаційної безпеки України. Електронний ресурс. Режим доступу:http://zakon5.rada.gov.ua/laws/show/514/2009
2. Концепція національної безпеки України. Електронний ресурс. Режим доступу:http://old.niss.gov.ua/book/otch/roz23.htm
3. Стратегії національної безпеки України. Електронний ресурс. Режим доступу:http://www.president.gov.ua/documents/2872015-19070
4. Наказ президента США № 12333 від 4 грудня 1981 рЕлектронний ресурс. Режим доступу: http://kodeksy.com.ua/pro_sluzhbu_zovnishnoyi_rozvidki_ukrayini.htm
5. Закону України «Про Службу зовнішньої розвідки України» Електронний ресурс. Режим доступу: http://kodeksy.com.ua/pro_sluzhbu_zovnishnoyi_rozvidki_ukrayini.htm

----------***----------

Бежевець А. М., аспірантка
Національного технічного
університету України
КПІ ім. Ігоря Сікорського.

ПРОБЛЕМИ ПРАВОВОГО РЕГУЛЮВАННЯ ІНФОРМАЦІЙНИХ ВІДНОСИН В ПЕРІОД ЧЕТВЕРТОЇ ПРОМИСЛОВОЇ РЕВОЛЮЦІЇ

Цілеспрямований розвиток інформаційних відносин, зростання обсягу застосування новітніх інформаційних технологій призвів до формування інформаційного суспільства, яке характеризується, перш за все, переорієнтацією економіки з використанням матеріальних ресурсів на ефективне впровадження знання технологій.

Інтернет речей, 3D друк, застосування роботів зі штучним інтелектом в різноманітних процесах людської діяльності та інші яскраві новинки в сфері автоматизації вже стали невід'ємними атрибутами сучасного інформаційного суспільства.

Цифрові дані оточують людину протягом вже тривалого часу, постійно зростаючи в кількості та якості. Величезний масив цифрової інформації являє собою середовище, в якому висвітлюються різні події реального світу, які не знаходять свого відображення в іншому (аніж цифровому) вигляді. Людина здатна на розпізнавання цих подій, однак лише при зручному відображенні і на доступних для сприйняття масштабах інформації. Наприклад, людина здатна ідентифікувати наявність предмета на фотографії, але не впорається, якщо перед нею будуть мільйони фотографій. Для роботи з таким масштабом даних стає доцільним машинними (автоматизованими) методами обробити і структурувати масив цифрової інформації, визначивши та виокремивши необхідну.

Технічний прогрес завжди спрямований та неодмінно призводить до підвищення ефективності у виробничому секторі, нові креативні та інноваційні моделі обслуговування створюють революцію в сфері послуг і виробництва.

Промислове виробництво має бути інтегровано з сучасними інформаційними і комунікаційними технологіями. Технічною основою для цього є інтелектуальні та цифрові мережеві системи. З їх допомогою стає можливим створення «самоорганізованого» виробництва: люди, машини, заводи, логістика та продукти взаємодіють, в тому числі безпосередньо один з одним.

Однією з базових технологій, за допомогою яких стануть можливі такі зміни у виробництві, називають інтернет речей (IoT), який являє собою сукупність технологій, що забезпечують підключення до інтернету будь-яких предметів для їх автономної роботи без участі людини. Різновидом IoT визначають промисловий (індустріальний) інтернет речей (IIoT), що стане основою автоматизації виробництва і побуту в майбутньому, хоча його вплив відчутний вже зараз. Існування інтернету речей є невід'ємним елементом Індустрії 4.0.

Термін «Індустрія 4.0», скорочено - I4.0 або просто I4, отримав свою назву від ініціативи, очолюваної бізнесменами, політиками і вченими, які визначили її як засіб підвищення конкурентоспроможності обробної промисловості Німеччини через посилену інтеграцію «кіберфізичних систем» (CPS) в виробничі процеси. Фахівці запропонували інтегрувати в промислові процеси так звані «кіберфізичні системи» (CPS), або автоматизовані машини і обробні центри, підключені до інтернету. При цьому за мету було визначено створення таки систем, які дозволили б машинам самостійно (автономно) змінювати, при необхідності, виробничі шаблони.

Цифровий (пов'язаний з інтернетом) підхід зачіпає всі етапи життєвого циклу продукту, включаючи дизайн і створення прототипу, наладку і обслуговування виробничої лінії, контроль і оптимізацію виробництва, а також дані, отримані в результаті зворотного зв'язку від клієнтів і споживачів. «Індустрія 4.0» докорінно змінює не тільки процес виробництва, але і сферу послуг, пов'язаних з продукцією, що випускається.

Термін «Індустрія 4.0» був публічно представлений в 2011 році на Ганноверському ярмарку. Сьогодні він використовується для позначення четвертої промислової революції.

Кіберфізичні системи виробництва докорінно змінять традиційну логіку виробництва, оскільки кожен виробничий об'єкт буде сам визначати, яку роботу необхідно виконати на даному етапі. Ця абсолютно нова архітектура промислових систем може бути впроваджена поступово за допомогою цифрової модернізації існуючих виробничих потужностей. І це означає, що дану концепцію можна реалізувати не тільки на абсолютно нових підприємствах, а й поетапно розгортати на існуючих підприємствах в процесі еволюційного розвитку.

Кіберфізичні системи здатні приймати незалежні рішення і виконувати завдання максимально автономно. Тільки у виняткових випадках, наприклад, у разі збоїв або суперечливих цілей, вони передають завдання вищому органу (рівню).

Добре відомими прикладами з галузі робототехніки і штучного інтелекту є так звані «розумні» фабрики, автомобілі без водія, безпілотники доставки. Уже зараз в нашому повсякденному житті роботи можуть бути використані в різних сферах життя суспільства, наприклад, замість солдатів для військової промисловості, в медицині для проведення надскладних і точних операцій, в соціальній сфері роботи можуть подбати про літніх людей тощо.

Модні сьогодні слова «Індустрія 4.0» і «цифровий бізнес» представляють собою початок складного трансформаційного процесу, який глибоко вплине на промисловість і суспільство протягом наступного десятиліття. Це перетворення засноване на зближенні реального (аналогового) світу і віртуального (цифрового) світу за допомогою машинно-машинного (M2M) зв'язку, автономних систем (наприклад, робототехніки) та Інтернету речей (IoT).

Виробництво з підтримкою IoT передбачає збір даних в реальному часі і обмін ними між різними виробничими ресурсами, такими як машини, матеріали і робочі місця.

Зв'язок M2M, IoT і автономних машин та пристроїв в рамках I4.0 відкривають дивовижні можливості для бізнесу. Однак, одночасно, ці досягнення створюють нові правові проблеми, які повинні бути вирішені невідкладно. В першу чергу йдеться про визначення суб'єкта відповідальності за шкоду, яка завдана роботами зі штучним інтелектом, - як договірної, так і позадоговірної (деліктної).

Таким чином, серед основних правових проблем, які постають перед суспільством в рамках індустрії 4.0, підставно виділити питання правового регулювання даних та відповідальності за завдання шкоди роботами зі штучним інтелектом, визначивши їх наступним чином:

1. Процес аналізу даних і перетворення їх в систематизовані дані включає перетворення інформації в знання, наповнені цінністю для бізнесу. Власники цих даних мають на меті забезпечити юридичний захист таких даних (навіть якщо вони не є особистими або персональними даними), і що компанії, які створюють і аналізують такі дані, можуть претендувати на права власності на них. При правильному аналізі та інтерпретації даних власник даних має можливість максимально точно прогнозувати ситуацію на ринку, приймати економічно вигідні управлінські рішення. Наведемо приклади таких даних: велика торговельна мережа аналізує і систематизує інформацію щодо видів та обсягів продажу певної продукції. Дані такого характеру є «паливом», рушійною силою для I4.0.

Однак, зазначені дані (інформація) не є ні матеріальним об'єктом, ні об'єктом захисту відповідно до встановлених норм у сфері захисту права інтелектуальної власності. Тому такі дані на сучасному етапі розвитку законодавчої бази не захищені спеціальним правом власності, і не існує такої речі, як законне «володіння» даними.

2. Збільшення використання виробничих автономних роботів неодмінно принесе правові проблеми, в тому числі і проблеми відповідальності за заподіяння шкоди суспільству або людині. Ця проблема вимагає обов'язкового законодавчого врегулювання. Проте на даному етапі для максимально швидкого заповнення цієї прогалини необхідне втручання науковців та юристів для формування однозначної правової позиції з урахуванням судової практики, що складається у світі.

До цього часу чинне законодавство не передбачає можливості укладення договору автономними пристроями (роботами зі штучним інтелектом), що в свою чергу унеможливлює функціонування автономного виробництва. На правовідносини за участю таких систем можна умовно поширити норми, що регулюють правовідносини, об'єктом яких є джерело підвищеної небезпеки.

Таким чином, Індустрія 4.0, поєднуючи технології вбудованих виробничих систем з інтелектуальними виробничими процесами, впевнено прокладає шлях до нового технологічного століття, яке здатне докорінно змінити бізнес-моделі підприємств та суспільство в цілому. Для цього необхідно формування правової бази, здатної забезпечити функціонування оновлених суспільних відносин.

----------***----------

Каздобіна Ю. К., Українська фундація безпекових студій, Голова, Магістр політології та міжнародних відносин.

ПИТАННЯ ДЕРЖАВНОГО РЕГУЛЮВАННЯ КОНТЕНТУ В ІНТЕРНЕТІ

Сьогодні Україна, як і інші країни стикається з необхідністю врегулювати відносини в інформаційній сфері, де під впливом розвитку цифрових технологій відбулось багато змін. В Україні дуже часто публічні дискусії на цю тему зводяться до питання блокувати чи не блокувати веб сайти, і чи порушує блокування права людини. Проблема ж є набагато ширшою, та в Україні має три таких виміри:

1) Необхідність адаптувати українське законодавства до норм європейського законодавства відповідно до задекларованих намірів євроінтеграції;

2) Необхідність адаптувати законодавчу базу до змін в інформаційній та інших сферах, спричинені розвитком цифрових технологій;

3) Необхідність протидіяти активним заходам РФ, ефективність яких зросла через появу нових механізмів впливу у віртуальному просторі.

На сьогодні, підхід держави до регулювання в інформаційній сфері не співпадає з міжнародним. Доктрина інформаційної безпеки України говорить про необхідність захищати інформаційний суверенітет, визначений як «здатність держави контролювати і **регулювати потоки інформації з-поза меж держави** з метою додержання законів України, прав і свобод громадян, гарантування національної безпеки держави».

Цей підхід контрастує з підходом міжнародних організацій, які керуються Загальною декларацією прав людини. Стаття 19 декларації говорить, що «кожна людина має право на свободу переконань і на вільне їх виявлення; це право включає свободу безперешкодно дотримуватися своїх переконань та свободу шукати, одержувати і поширювати

інформацію та ідеї будь-якими засобами і **незалежно від державних кордонів**.»

Різниця підходів обумовлює шлях, яким рухатися – створювати однакові правила для всіх учасників інформаційного поля, чи намагатися диференціювати між внутрішніми гравцями та різними зовнішніми гравцями за певними ознаками.

Також слід відмітити, що між різними стейкхолдерами[2] в Україні нема спільного розуміння критеріїв та умов, за яких держава може запроваджувати обмеження свободи слова. У той час, як представники силових структур апелюють до того, що свободу висловлення можна обмежувати в інтересах національної безпеки, ГО наполягають, що такі обмеження мають відповідати умовам та критеріям, визначеним міжнародним правом. Технічна спільнота взагалі проти будь-яких обмежень.

Також, слід зазначити, що у світі є невизначеність щодо застосування норм міжнародного права прав людини за нових умов. Зокрема, у доповіді ООН щодо епохи цифрової взаємозалежності йдеться про те, що «*У багатьох випадках далеко не очевидно, як закони та договори про права людини, складені в пре-цифрову еру, повинні застосовуватися в епоху цифрових технологій*». [2, 23] Разом з тим, права людини залишаються базовою цінністю, порушення яких має бути зведено до мінімуму у ситуаціях загрози національній безпеці, і Україні слід це враховувати у процесі нормотворчості.

Особливості інтернет середовища.

Як середовище, де відбувається взаємодія між різними гравцями, інтернет має певні особливості, які обумовлюють складності застосування раніше вироблених механізмів регулювання. До таких належать:

- Обмежена здатність держави безпосередньо регулювати правовідносини в інтернеті, адже держава, як і інші користувачі, має доступ до мережі лише через посередників, таких як інтернет провайдери.
- Інтернет є глобальною мережею, в якій нема формальних кордонів. Це означає, що інформаційні ресурси, що містять заборонений/шкідливий контент, фізично можуть знаходитися поза юрисдикцією держави, але мешканці України матимуть вільний доступ до них.

[2] Зустріч стейкхолдерів відбувалася в рамках проекту “Зелена книга з управління інтернетом та інформаційної політики в Україні як інструмент адвокації в процесі вироблення рішень”, втілюваного спільно Українською фундацією безпекових студій та ГО “Інтерньюз-Україна”. У вересні 2019 року УФБС та “Інтерньюз-Україна” планують опублікувати "Зелену книгу", базовану на результатах обговорень.

- Поза юрисдикцією держави можуть знаходитися і деякі посередники, такі, як соціальні мережі та інші технологічні гіганти. Це означає, що на них не розповсюджується дія українського законодавства, і українська держава не має жодного впливу на те, як вони регулюють контент у себе на платформі. Більше того, таке регулювання є непрозорим, адже воно часто здійснюється за допомогою алгоритмів, які є комерційною таємницею.
- Запровадження механізмів відповідальності є ускладненим через право на анонімність та недоступність даних про користувачів та виробників контенту, яку захисники прав людини розглядають, як позитивну, особливо в державах з репресивними режимами.
- Переважна більшість інтернет-ресурсів не лише надає користувачу доступ до певної інформації, а ще й збирає інформацію про нього. В подальшому ці дані використовуються для спрямованої подачі інформації (або таргетингу) в інтересах комерційних, політичних або інших суб'єктів, які намагаються впливати на вибір користувача.
- Механізми модерації контенту відсутні або недосконалі через неузгодженість критеріїв між різними гравцями, ускладненість їх застосування через різні юрисдикції або її відсутність, великий об'єм інформації, недосконалість механізмів, базованих на штучному інтелекті (нечутливість до контексту, невірна ідентифікація забороненого або дозволеного контенту (false positives, false negatives).
- Наявні механізми швидкого, вірусного та повторюваного розповсюдження інформації та висловлювань, поданих у відповідний момент з відповідним емоційним забарвленням.
- Відсутні механізми видалення контенту, який знайшов широке розповсюдження в мережі, навіть якщо такий контент визнано судом або іншим легітимним органом як такий, що підлягає видаленню.
- Відсутність ефективних механізмів швидкого реагування у разі вірусного розповсюдження контенту, який порушує права та/або може призвести до негативних наслідків у реалі (наприклад, стрімінг насильства).

Визначення загрози.

Непрямий зв'язок між поширенням інформації/висловлювань та наслідком таких дій в реальному світі значно ускладнює визначення загрози та законодавче встановлення обмежень. Нема згоди щодо цього і серед стейкхолдерів в Україні. Норми міжнародного права прав людини в першу чергу захищають індивідуальні права та свободи. Разом з тим, навіть цілком законні висловлювання, які не обмежуються законодавством, можуть стати

загрозою, якщо вони багаторазово повторюються або йдуть з багатьох джерел одночасно. Такий інструмент, як астротурфінг – створення ілюзії широкої підтримки певного явища, серед іншого і у віртуальному просторі – широко використовується пропагандистами з метою впливу на суспільні процеси в інших державах.

Фахівці НІСД визначають гібридну війну та активні заходи РФ як «деструктивний вплив, підпорядкований єдиному політичному стратегічному задуму» [1, 36]. Для досягнення визначеної мети агресор використовує широкий набір засобів, з яким можна ознайомитися у цитованій доповіді. На використанні вразливих місць суспільства для збільшення ефективності такого впливу наголошує дослідниця вмісту електронної пошти Владислава Суркова Аля Шандра [22]. Отже, загроза лежить на перетині вразливостей та зкоординованого впливу на ці вразливості. Наприклад, припинення саме зкоординованої діяльності (а не обмеження певного контенту) лежить в основі реагування на операції впливу, яке у себе на платформі запроваджує Фейсбук.

Взаємозв'язок між діями агресора та умови, за яких загроза в інформаційній сфері може бути реалізована через наявну вразливість, потребує подальшого вивчення.

Відповідальність посередників.

Відповідальність посередників є суперечливим питанням в Україні. Представники технічної спільноти наголошують, що як нейтральні посередники, вони не можуть нести відповідальність за контент, розміщений третіми особами. Представники деяких ГО вважають регулювання через посередників перекладанням відповідальності на них. У світі існує три підходи до такої відповідальності – американський, європейський та російський/китайський. [4] Вони різняться ступенем відповідальності. В Україні необхідне глибше знайомство та широке обговорення цих підходів.

Так само дискусії потребує питання стимулювання посередників до співпраці з державою, адже силові методи в демократичних країнах застосовуються у крайніх випадках.

Питання довіри.

На сьогодні серед технічної спільноти та громадянського суспільства існує глибока недовіра до державних інституцій, а, особливо до правоохоронних органів. Під час дискусій зі стейкхолдерами цю недовіру відмічали, як представники ГО, так і представники держави. Вона дуже часто стає на заваді надання силовим органам повноважень, необхідних для виконання їх обов'язків.

Список використаних джерел:

1. «Активні заходи» СРСР проти США: пролог до гібридної війни: аналіт. доп. / Д.В. Дубов, А.В. Баровська, Т.О. Ісакова, І.О. Коваль, В.П. Горбулін; за заг. ред. Д.В. Дубова. – 2-ге вид. – К. : НІСД, 2017. – 52 с.
2. “The Age of Digital Interdependence” Report of the High-level Panel on Digital Cooperation. URL: https://digitalcooperation.org/wp-content/uploads/2019/06/DigitalCooperation-report-web-FINAL-1.pdf
3. Шандра А, Сілі Б «Surkov Leaks: Внутрішня кухня гібридної війни Росії проти України»/ URL: http://euromaidanpress.com/wpcontent/uploads/2019/08/Surleaks_ukr_book_small_online.pdf
4. MacKinnon, Rebecca, Hickok, Elonnai, Bar, Allon, Lim, Hae-in Fostering freedom online: the role of Internet intermediaries/ URL : https://unesdoc.unesco.org/ark:/48223/pf0000231162

----------***----------

Самчинська О. А., студентка ФСП КПІ ім. Ігоря Сікорського.
Науковий керівник : ***Фурашев В. М.,*** к. т. н, доцент КП ім. Ігоря Сікорського.

ЗАСОБИ МАСОВОЇ ІНФОРМАЦІЇ ЯК АПАРАТ ІНФОРМАЦІНО - ПСИХОЛОГІЧНОГО ВПЛИВУ НА СВІДОМІСТЬ ГРОМАДЯН

Одним із найдавніших просторів поширення інформаційно-психологічного впливу, безперечно є засоби масової інформації. Газети, радіо, телебачення, онлайн видання - це те з чого ми отримуємо найбільшу частину інформацію кожного дня і завдяки чому у нас створюється уявлення про те, що відбувається навколо. Наївно надіятися, що читаючи газети чи дивлячись новини, ми застраховані від брехні та маніпуляцій. Недарма, в наш час засоби масової інформації негласно називають «четвертю гілкою влади», адже їх здатність впливати на свідомість та поведінку громадян просто вражає.

Прийомів та способів впливу на свідомість індивіда та суспільства у даному просторі є безліч, проте, у даній роботі ми розглянемо лише чотири з них, які стали особливо популярними та ефективними.

Напевно, одним із найпопулярніших способів маніпуляції в мас-медіа є так зване «посилання на авторитет». Для цього способу характерні такі словесні конструкції як «вчені довели…» або «на основі досліджень відомі науковці встановили…», особливо полюбляють посилатися на дослідження британських вчених, саме вони, відповідно до інформації, яку нам надають

ЗМІ роблять найбільше відкриттів, «відповідно до слів людини з найближчого оточення Президента, яка побажала залишатися невідомою…», «лікарі рекомендують…», «за прогнозами політологів…» – таких прикладів можна навести дуже багато. Основною особливістю цього способу є те, при таких голосних заявах ніколи не згадуються конкретні прізвища та джерела, однак, у більшості громадян це не викликає сумніву і таких давно відомих кліше достатньо, щоб довіритися такому авторитету. [1]

По-іншому цей спосіб зазвичай використовують у рекламах. Напевно кожен з нас помічав, що продукти харчування, непродовольчі товари, операторів мобільного зв'язку та багато інших товарів та послуг дуже часто рекламують саме відомі особистості, які мають уже встановлений авторитет та прихільність серед населення, та вибір яких є важливим для більшості. Зазвичай, після перегляду таких роликів, в супермаркеті, коли перед нами широкий асортимент продукції, ми все ж таки виберемо йогурт, який так полюбляє відома телеведуча Маша Єфросиніна та каву, яку обирає її колега Олександр Педан. Звичайно не можна стверджувати, що після перегляду реклами усі будуть купляти лише ті продукти, а інші не будуть користуватися попитом, це не так. Однак, факт, що певний відсоток людей все ж це зроблять заперечувати не можна.

Наступним досить популярним засобом є так званий спосіб сендвіча. Метод який полягає в накладанні та правильному структуруванні інформації. При цьому, факти, які висвічуються по суті є правдивими, однак, завдяки правильній послідовності їх подання вони сприймаються саме так, як це потрібно маніпулятору. Є два види цього способу маніпуляції.

Перший – «отруйний сендвіч», його суть полягає в тому, що спочатку як передумова подається якась позитивна подія, а потім негативний виступ та негативне закінчення, або позитивну інформацію поміщають між двома негативними. [1] При такому порядку подачі інформації позитивний факт нівелюється і у глядачі сприймають лише негативну ситуацію. Цей спосіб активно використовується в політиці для того, щоб скласти неправильне або просто негативне враження про якогось політика чи просто громадського діяча. Яскравим прикладом може слугувати порядок подачі новим російським каналом НТВ під час парламентських виборів у 1999 році. Повідомлення Володимира Путіна про те, що він підтримує партію «Єдність» був поданий між двома репортажами про хід подій в Чечні, де в цей час відбувалися військові дії. Така подача інформації в результаті, створила у громадян враження, що для політиків головне - отримати владу, і поки молоді хлопці гинуть на війні, їх хвилює лише перемога на майбутніх виборах. Це

притаманно практично для всіх засобів масової інформації, в тому числі українських.

Протилежним видом цього методу є так званий «солодкий сендвіч», коли негативну інформацію подають перед, або між позитивною. [1] Цей метод дуже часто використовують для того, щоб зменшити негативне сприйняття трагічних подій. Так, у день пожежі в торговому центрі в Кемерево, де заживо згоріло близько 40 дітей, по провідних каналах Росії майже цілий день показували ділові зустрічі Володимира Путіна і лише між цим згадували про страшну пожежу.

Перекликається та доповнює цей спосіб метод відволікання уваги. Сьогодні інформаційний простір просто перенасичений різноманітною інформацію, однак, якщо задуматися та звернути увагу на те, чим нас «годують», то можна дійти до висновку, що більшість інформації, яку ми споживаємо через інтернет та засоби масової інформації не носить в собі змісту як такого.

В сюжеті новин, в друкованих та онлайн виданнях більша частина контенту спрямована на те, щоб відволікти увагу споживача інформації та посприяти, щоб дійсно важлива інформація не дійшла до пересічних громадян, або була подана лише у певному обсязі. Від нас приховують проблеми та відкриття у різних сферах, які є реально важливими для життя та діяльності суспільства і змушують нас вважати, що ми насправді дуже обізнані.

Відволікання уваги від дійсно серйозних питань та проблем та заміна їх на теми, які не мають реального значення – стала негласною політикою діяльності засобів масової інформації як в світі, так і в Україні.

І, можливо, спочатку незрозуміло для чого це все робиться, однак, насправді у цьому є серйозний сенс. Відволікання уваги пригнічує здатність критично мислити. Суспільство, яке постійно зайняте так званим «інформаційним сміттям» не здатне та і не має бажання шукати, перевіряти та аналізувати отриману інформацію. Саме такий соціум є найкращим об’єктом інформаційно-психологічного впливу, який здійснюється задля отримання влади та досягнення інших цілей верхівки нашої держави.

Зовсім протилежним є наступний спосіб – перебільшення, залякування та створення паніки серед населення. Цю маніпуляцію можна виявити відкривши стрічку новин та просто прочитавши заголовки. Більша половина видань, у заголовках статей використовують досить голосні фрази, які не мають свого відображення у самому тексті статті, або відображаються у зовсім іншому сенсі.

Одним із прикладів використання цього прийому на практиці є штучно створена масова паніка у зв'язку з так званим поширенням коров'ячого сказу у Великій Британії. Все почалося з того, що у європейських засобах масової інформації почали одна за одною з'являтися статті про нібито поширення епідемії коров'ячого сказу, який передавався через вживання м'яса цих тварин і є смертельно небезпечним для людини, так як спричиняє руйнування тканини головного мозку. За цей період в Англії від цієї хвороби померло десять людей. Преса «досить серйозно» поставилася до цього питання і не просто публікувала новини про випадки смерті, а й біографії кожного померлого та навіть опис м'ясних страв, які вони вживали. [2]

Така увага до даної події спричинила масову паніку, під тиском якої Євросоюз заборонив Великобританії експортувати м'ясо та зобов'язав знищити всіх корів, яким понад три роки та спалити їх трупи. Ця новина настільки полонила свідомість людей, що почали будуватися спеціальні крематорії для знищення тушок корів, адже, постало питання в короткий термін знищити усіх тварин.

Звичайно, пізніше було встановлено, що це було ніщо більше як так звана сіра пропаганда і насправді ця проблема не була такою глобальною як її подали. Однак, визначити хто саме поширив цю чутку так і не вдалося. Але якби брехня не була вчасно викрита і вимоги Європейського Союзу були реально виконані – це б стало катастрофою англійської економіки і могло мати невідворотні наслідки.

Однією з сучасніших новин, яка сколихнула безпосередньо українців, стало введення воєнного стану в країні. Всі українські ЗМІ тільки про це і говорили, люди з неабиякою тривогою чекали рішення чи буде введено його чи ні. А все тому, що завдяки гучним повідомленням преси, люди сприймали введення воєнного стану як початок справжньої війни. В кожній новині говорилося про обмеження деяких прав і свобод громадян, про введення комендантського часу, обмеження діяльності деяких державних структур. Однак, ніхто не хотів пояснити пересічним громадянам про те, що цей стан запроваджується лише в деяких областях, а не по всій території України, що обмеження прав та свобод громадян та діяльності організацій буде здійснюватися лише в виключних випадках, що ніякого дефіциту продуктів це не спричинить. І як показала практика, що життя та діяльність українців під час воєнного стану жодним чином не постраждала та нічим не відрізнялася від звичайної.

Це лише короткий перелік того, як та за допомогою чого діяльність засобів масової інформації не лише не висвітлює об'єктивний стан подій, що відбуваються навколо нас, а й здійснює негативний інформаційно

психологічний вплив на свідомість окремого індивіда, так і суспільства в цілому.

Список використаних джерел:

1. Макарова В.О. «Культура страху» як етична проблема діяльності засобів масової комунікації. *Електронна бібліотека інституту журналістики.* URL: http://journlib.univ.kiev.ua/index.php?act=article&article=2360

2. Методи маніпулятивного впливу ЗМІ: веб-сайт. URL: balakliya-school2.edu.kh.ua

----------***----------

Давидюк А. В., аспірант
ІПМЕ ім. Г.Є. Пухова НАН України.

ПРОБЛЕМИ ВПРОВАДЖЕННЯ РИЗИКОРІЄНТОВНОГО ПІДХОДУ ДО ЗАБЕЗПЕЧЕННЯ ПРОЦЕСУ ЗАХИСТУ ІНФОРМАЦІЇ

Існуюча парадигма захисту інформації, що полягає у забезпеченні таких властивостей інформації як конфіденційність, цілісність та доступність при своїй реалізації, зокрема при побудові комплексних систем захисту інформації (далі - КСЗІ), відповідно до НД ТЗІ 3.7-003-005 та НД ТЗІ 2.6-001-11 [1], [2] вимагає розробки моделі загроз та моделі порушника. Проте в наш час, коли рівень інформатизації значно виріс, врахування можливих загроз та категорій порушників без імовірності настання несприятливих подій (інцидентів) є недостатнім при формуванні необхідного переліку ефективних засобів захисту, тому доцільним є впровадження та застосування ризикорієнтованого підходу до забезпечення безпеки інформації, який буде враховувати імовірність настання інциденту та величину можливих збитків, що дасть можливість виокремити пріоритетні напрями захисту та відповідно здійснювати ефективний розподіл коштів на забезпечення безпеки інформації.

Кращі міжнародні практики в сфері управління інформаційною безпекою (далі - ІБ) використовуються у нашій державі, зокрема міжнародні стандарти серії ISO 27k та ISO 31K представлені у вигляді ДСТУ ISO/IEC. Водночас відповідно до чинного законодавства державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинні оброблятися в системі із застосуванням КСЗІ з підтвердженою відповідністю [3]. Проте застосування ДСТУ ISO/IEC не є обов’язковим на законодавчому рівні, а носить більше рекомендаційний характер. Тому процес управління ризиками інформаційної безпеки не може

строго бути реалізованим в рамках чинного законодавства України при побудові КСЗІ. З урахуванням рівня зрілості інформаційних процесів, пов'язаних із захистом інформації, доцільним було б на законодавчому рівні внести доповнення щодо альтернативного використання систем управління інформаційною безпекою (далі - СУІБ) відповідно до ISO 27k.

Але тут виникає нова проблема, так як побудова систем управління інформаційною безпекою не є можливою без інвентаризації всіх інформаційних активів та профільної перепідготовки кадрів у сфері ІБ. Також не варто забувати про те що, процес ратифікації та кореляції вимог документів ISO з чинним законодавством є досить трудомістким та часозатратним. Зокрема, при цьому слід першочергово враховувати сучасні кращі світові практики, а вже потім редакції чинного законодавства 90-х та початку 2000-х– років.

Для адекватного визначення імовірності появи інциденту ІБ необхідним є розробка та впровадження системи збору та обробки даних про інциденти у державних та приватних організаціях. Водночас підготовка нових документів у сфері ІБ вимагає додатково створення методологічної бази, що буде спроможною чітко та однозначно описати механізми реалізації вимог чинних нормативно-правових документів.

Список використаних джерел:

1. НД ТЗІ 3.7-003 -2005 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі // ДСТСЗІ СБ України. – 2005. URL : https://tzi.ua/ru/nd_tz_3.7-003_-2005.html.

2. НД ТЗІ 2.6-001-11 Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах // Адміністрація Державної служби спеціального зв'язку та захисту інформації України. – 2011. URL : https://tzi.com.ua/downloads/2.6-001-11.pdf.

3. Закон України Про захист інформації в інформаційно-телекомунікаційних системах. – 2014. URL : https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80.

----------*----------**

Касперський І. П., Національна академія СБ України, доцент спеціальної кафедри, к.ю.н., с.н.с., доцент.

ПРОБЛЕМИ ЗАХИСТУ ПУБЛІЧНОЇ ІНФОРМАЦІЇ ПРО МАЙНОВИЙ СТАН ГРОМАДЯН

Боротьба із корупцією на сьогодні є одним із пріоритетних напрямів розвитку нашої держави, а прозорість у роботі державних органів стала важливою запорукою ефективності цієї боротьби. В частині доступу до публічної інформації Україна досягла суттєвого прогресу: за даними всесвітнього рейтингу відкритості даних The Open Data Barometer наша держава перебуває на 18-му місці, піднявшись з 2013 року на 25 позицій [1].

Проте доступність публічної інформації породжує суттєві ризики для тих осіб, які безпосередньо ініціюють та реалізовують заходи державного примусу. Справа в тому, що відповідно до вимог ст.ст. 3, 45 Закону України «Про запобігання корупції» (далі – Закон) усі судді, поліцейські, посадові та службові особи органів прокуратури, Служби безпеки України, Державного бюро розслідувань, Національного антикорупційного бюро України визнані суб'єктами обов'язкового декларування доходів [2].

Відповідно до ст. 46 Закону у декларації про доходи крім відомостей про майно вказані суб'єкти зобов'язані вказувати зареєстроване місце проживання, а також місце фактичного проживання. При цьому відповідно до ст. 47 Закону подані декларації включаються до Єдиного державного реєстру декларацій осіб, уповноважених на виконання функцій держави або місцевого самоврядування, а Національне агентство із запобігання корупції забезпечує відкритий цілодобовий доступ до цього реєстру [2].

Фактично такий доступ провокує зловмисників на прямі посягання на життя, здоров'я та власність суб'єктів декларування:. Так у жовтні минулого року в Києві було здійснено збройний напад на домоволодіння судді, яка напередодні внесла зміни в декларацію - майже два з половиною мільйона гривень прибутку від продажу нерухомості у центрі столиці. В результаті нападу один із грабіжників загинув, поліцейського було поранено, а потерпілі отримали серйозні тілесні ушкодження внаслідок тортур [3].

Такий стан справ вимагає перегляду вимог законодавства в частині необхідності оприлюднення декларацій про доходи посадових осіб правоохоронних органів та суддів.

Варто зауважити, що обов'язковою умовою визнання правомірності обмеження доступу до інформації є «трискладовий тест», закріплений у ст.5

Закону України «Про доступ до публічної інформації». Відповідно до цього положення інформація вважається обмеженою у доступі правомірно виключно в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя якщо розголошення інформації може завдати істотної шкоди цим інтересам і шкода від оприлюднення такої інформації переважає суспільний інтерес в її отриманні [4].

Вбачається, що інформація про місце проживання та майно суддів і співробітників правоохоронних органів має право на обмеження у доступі, оскільки це дозволить забезпечити неупередженість правосуддя та запобігти злочинам, пов’язаним із можливим прямим тиском на цих осіб, який вчиняється із протиправною метою. Загроза життю та здоров’ю правоохоронців є суттєвим аргументом на користь обмеження доступу до інформації про них, а громадськість отримає значно більше переваг від ефективної роботи судів та правоохоронців, ніж від можливості відстежувати їх статки.

Тому на сьогодні вкрай необхідно створити окремий закритий фонд Єдиного державного реєстру декларацій осіб, уповноважених на виконання функцій держави або місцевого самоврядування, зосередивши у ньому декларації посадових осіб, що безпосередньо причетні до реалізації функцій державного примусу. Доступ до такого фонду, звичайно, необхідно гарантувати усім суб’єктам владних повноважень, які здійснюють боротьбу із корупцією та оцінюють доброчесність посадових осіб, уповноважених на виконання функцій держави або місцевого самоврядування.

Список використаних джерел:

1. The Open Data Barometer URL: https://opendatabarometer.org/?_year=2017&indicator=ODB (Date of access: 18.09.2019)

2. Закон України «Про запобігання корупції» від 14.10.2014 р. // Офіційний вісник України від 07.11.2014. — 2014 р., № 87, стор. 156, стаття 2474, код акта 74501/2014

3. Суддя, на київський дім якої здійснили напад, напередодні задекларувала додаткові 2,5 млн. гривень URL: https://tsn.ua/kyiv/suddya-na-kiyivskiy-dim-yakoyi-zdiysnili-napad-naperedodni-zadeklaruvala-dodatkovi-2-5-mln-griven-1226052.html (Date of access: 18.09.2019)

Закон України «Про доступ до публічної інформації» від 13.01.11р. // Голос України від 09.02.2011 - № 24

----------***----------

Цирфа Г. О., доцент КПІ ім. Ігоря Сікорського, к.і.н., доцент.

РОЗВИТОК РИНКУ КІБЕРСТРАХУВАННЯ: ПИТАННЯ КІБЕРБЕЗПЕКИ

Все частіше компанії у всьому світі страждають від кібератак. Масштаби кіберзагроз постійно зростають. Атакам у кіберпросторі майже щодня піддаються і США. Згадати, хоча б глобальну кібератаку на Microsoft. Причому, природа кібератак удосконалюється. Беручи до уваги величезний збиток, який можуть спричинити подібні напади, країни світу розуміють важливість ефективного захисту своєї країни.

Ризик у використанні цифрових технологій став реальністю і для українських підприємців та, одночасно, - першочерговим завданням для захисту себе від ризиків кібератак. Не дивлячись на окремі законодавчо-нормативні акти, які посилюють заходи із кібербезпеки нашої держави, слід зазначити, що забезпечення кібербезпеки для підприємств через правові механізми в Україні відбувається ще не на досить належному рівні. Тому слід використовувати й інші механізми мінімізації корпоративних ризиків.

Додатковим інструментом часткового відшкодування збитків може бути і вже застосовується – механізм страхування кіберризиків. Захист конфіденційної інформації, комерційної таємниці, персональних даних (як працівників, так і контрагентів) можна здійснити через отримання послуг з кіберстрахування. Поліс страхової компанії, яка надає послуги кіберстрахування може стати ефективним інструментом захисту на випадок атак хакерів, кібервимагання, будь-яких фінансових втрат тощо.

Тему страхування кіберризиків обговорювали у 2012 році на щорічному Всесвітньому економічному форумі в Давосі. Проте, навіть на світовому рівні не можна ще говорити про надзвичайно широке проникнення кіберстрахування у сферу страхових відносин. Більшість країн світу поки що не застосовують механізм страхування кіберризиків. Не розвинутим є цей сегмент ринку страхування і в Європі.

Цікавою у цьому зв’язку є ситуація в Німеччині. Гартмут Май, - член правління одного з провідних фінансових концернів світу - німецької страхової компанії Allianz Global Corporate & Speciality (AGCS), у розмові з "Made for minds" – DW пояснив: «Власне, то була випадковість. Після червневих викривальних заяв програміста Едварда Сноудена щодо електронного стеження американських спецслужб, компанія Allianz Group запропонувала на ринку новий страховий пакет. Ми, звичайно, не могли на

це розраховувати. Проте для нас це була добра нагода. На сьогодні Allianz Group пропонує підприємствам кілька блоків страхових пропозицій, які залежно від необхідності покривають різні ризики [1].

Проте, ідея щодо кіберстрахування не є новою. Вона належить США. На сьогодні 9 із 10 полісів кіберстрахування використовуються американськими компаніями і пояснюється це масовими зламами декілька років тому корпоративних і урядових ресурсів саме у США. Американські страхувальники сплачують за такі кіберстраховки щороку понад мільярд доларів.

Кіберстрахування по суті стосуються складних корпоративних ризиків. Керівники підприємств іноземних країн на сьогодні вже розуміють важливе значення аналізу кіберризиків та останнім часом все більше схиляються щодо актуальності і доцільності страхового захисту від кіберзагроз. Проте, у кожній окремій країні світу, безумовно, що темпи розвитку кіберстрахування зумовлюються притаманним тій чи іншій країні соціально-економічним та технікотехнологічним становищем а також рівнем інформатизації суспільства та показником впровадженням ІТ-технологій.

На Українському страховому ринку ця сфера страхового сектору нещодавно сприймалась як щось екзотичне і лише два роки тому, коли українські компанії підрахували збитки через вірус Petya.A, кіберстрахування почало розвиватись і в нашій країні, хоча і стримано. Однак, слід зазначити, що попит на страхування кіберризиків в Україні більше простежується зі сторони самих страхових компаній замість потенційних жертв хакерських атак. На сьогодні з боку українських компаній немає чіткого усвідомлення необхідності і користі такого сервісу.

Тому вітчизняним страховикам, які предметом страхування визначатимуть кіберзагрози, слід переймати досвід колег зі США та інших розвинених країн де такі послуги надаються. Перспектива солідної частки на ринку страхування з таким продуктом є у тих українських страховиків, які ретельно прописуватимуть у договорах страхування відповідні послуги, зокрема: «відшкодування витрат на розслідування кіберзлочинів», «відновлення робіт ІТ-системи», «забезпечення захисту замовника в суді» тощо. Тобто, продукт повинен бути актуальним і зрозумілим.

За експертними оцінками світовий ринок кіберстрахування буде розвивається швидкими темпами. Обсяг операцій на такому ринку до 2020 р. може становити від 7,5 до 10 млрд дол.. США, а загальна сума збитків від кібератак зросте до 2,1 трлн дол.. [2].

На нашу думку, кіберстрахування в Україні може стати новою стратегією страховиків, які працюють на українському страховому ринку. Особливо це може стосуватись малого і середнього бізнесу, їх безпосередньої підтримки і захисту від кіберзагроз. Договір кіберстрахування максимально повинен покривати збитки компанії – страхувальника, завдані кібератакою. Навіть, якщо хакерська атака призведе до тривалої зупинки товарообігу або знищення бази даних, що наповнювалася роками – страхові компанії повинні покривати такі та інші, передбачені договором страхування, випадки страховими виплатами. Відшкодованими повинні бути і витрати, що були спрямовані компанією-страхувальником на відновлення інформації, комунікації тощо, знову ж таки, передбачені договором страхування при його укладанні сторонами. Поряд із цим, попит на кіберстрахування повинен стимулюватись держрегулюванням у відповідності із змінами у законодавстві у сфері страхування. Розвиток такого сегменту страхування потребує інноваційного підходу з урахуванням досвіду розвинутих країн світу. Вважаємо, що на законодавчому рівні слід визначити сутність кіберстрахування та місце цього виду у добровільній чи обов'язковій формі страхування. На законодавчому рівні також необхідно більш читко встановити механізм обмеженого доступу до баз даних, що містять конфіденційну інформацію клієнтів – страхувальників. На наш погляд, частина перша і друга статті 40 Закону України «Про страхування» щодо таємниці страхування не прописує сам механізм відповідальності зазначених в цих нормах осіб, який би дозволив виключити будь-яку можливість людського фактора щодо розкриття інформації про страхувальників.

Визначаючи шляхи практичного застосування інноваційних підходів до формування і розвитку ринку кіберстрахування, дослідники цього питання, зокрема, В. П. Ільчук, О. М. Парубець, Д. О. Сугоняко головними серед важливих підходів визначають: «удосконалення інституційного механізму управління інноваційною діяльністю страхових компаній, сприяння розвитку взаємодії останніх з Департаментом кіберполіції, Національною комісією, що здійснює державне регулювання у сфері зв'язку та інформатизації, створення інституту страхових омбудсменів, застосування актуарного моделювання на основі використання персоналізованого маркетингу, індивідуального андерайтингу, впровадження на рівні страхових компаній новітніх технологій» [3].

Список використаних джерел:

1. В. П. Братюк. Сутність кібер-злочинів та страховий захист від кібер-ризиків в Україні. URL: https://mail.ukr.net/desktop#readmsg/15690625202680665670/f0

2. «Made for minds» – DW. Рубрика «Економіка» /Страхування від кібер-атак: тепер і на європейському ринку. URL: https://www.dw.com/uk/

3. В. П. Ільчук, О. М. Парубець, Д. О. Сугоняко. Інноваційні підходи до розвитку ринку кіберстрахування в Україні. Електронний журнал «Ефективна економіка». URL: http://www.economy.nayka.com.ua/?op=1&z=6295

----------*----------**

Косогов О. М., кандидат військових наук, с.н.с.

«ОРГАНІЗАЦІЙНА ЗБРОЯ» РОСІЇ ПРОТИ УКРАЇНИ В КОНТЕКСТІ СТРАТЕГІЇ НЕПРЯМИХ ДІЙ

В умовах формування нового світового порядку, коли центр ваги боротьби на міжнародній арені переноситься в інформаційно-комунікаційний простір, від українських державних інститутів потрібне вміння своєчасно виявляти негативні тенденції в розвитку міжнародної й внутрішньої обстановки з метою їхньої ефективної нейтралізації. Відсутність у державній системі відповідних організаційних структур і розроблених концепцій забезпечення національної безпеки, адекватних реаліям геополітичного протиборства, пророкує країну на втрату свого суверенітету і її руйнування як самостійного державного утворення.

Гостре суперництво між провідними суб'єктами міжнародної політики – Росією й країнами Заходу – за сфери економічного й воєнно-політичного впливу на пострадянському просторі прийняло форму інформаційної війни як на внутрішньодержавної, так і на міжнародної аренах з використанням потенціалу непрямих дій, “твердої” і “м'якої” сили. Насамперед , розглядаються ті інструменти й ресурси, які дозволяють Росії дестабілізувати ситуацію в східних областях України.

Інформаційна війна із широкомасштабним використанням маніпуляції й пропаганди проводиться з метою кардинально змінити або повністю придушити конкуруючу картину миру. Україна, що значно програє в інформаційному протиборстві з Російською Федерацією (РФ), реалізує

політичну стратегію, спрямовану на збереження державної цілісності країни, недопущення її подальшої фрагментації.

Термін “стратегія непрямих дій” був уведений відомим англійським військовим теоретиком і військовим істориком Бэзилом Генрі Лиддел Гартом [1, 18]. Так, Лиддел Гарт уважав, що головною метою війни є не повне знищення збройних сил і економічного потенціалу ворожої держави, а примус правлячих кіл ворожої країни (або навіть декількох держав-супротивників) до прийняття таких умов, які б повністю відповідали політичним, економічним, військовим інтересам держави-агресора.

Що стосується історії появи родинної стратегії “м'якої сили” (soft power), то її автором був Джозеф Най, який розширив сферу стратегії непрямих дій за рахунок залучення арсеналу політичних, дипломатичних, економічних, психологічних і інформаційних методів [2, 26]. При цьому до “твердої сили” Дж. Най відносить економічний і військовий примус, а до “м'якої сили”– політичну ідеологію, суспільні цінності, зовнішню політику.

У Росії наукове співтовариство звернуло увагу на стратегії непрямих дій і “м'якої сили” наприкінці 1980-х рр., позначивши їх терміном “організаційна зброя”.

З кінця 90-х років проблема застосування “організаційної зброї” й “організаційних війн” висвітлюється в наукових доповідях, дисертаціях і на спецкурсах Російської академії генерального штабу як реакція на нову воєнно-стратегічну обстановку. Російські фахівці розглядають як мету дезорганізацію ворога, що у свою чергу веде до інформаційної переваги.

Завдання полягає в тім, щоб противник прийняв правильне з поглядукомунікатора рішення, яке потрібно не противникові, а комунікатору. На практиці це здійснюється застосуванням системи організаційних, пропагандистських, психологічних, інформаційних впливів на державу-мішень, що змушують його рухатися в необхідному для протилежної сторони руслі. З їх допомогою можна направити політику супротивника в стратегічний тупик, вимотати економіку, загальмувати діяльність оборонної промисловості, спотворити ріст суспільної самосвідомості та основи національної культури, створити серед частини населення “п’яту колону”.

У результаті скоординованих дій у державі повинна виникнути обстановка внутрішньополітичного, економічного й психологічного хаосу.

Основна умова застосування організаційної зброї – заміна системи перспективних цінностей держави-мішені, або окремого регіону, базовими конструктами ініціатора, у нашому випадку цінностями “слов'янської єдності” і “російського миру”. Зокрема, мова йде про декілька ключових

концептів, на яких ґрунтується нова картина миру для росіян на пострадянському просторі:

- по-перше, це концепція “розділеного народу”;
- по-друге, тема “захисту співгромадян за рубежем”;
- по-третє, тема “російського миру”;
- по-четверте, значення визнання й збереження, прийняття й просування “російської цивілізації”.

Таким чином, зусиллями сусідньої держави створюється сюжетна історія, віртуальний продукт, наратив, спрямований на стимулювання конкретних дій. Г.Почепцов називає такий тип наратива мобілізуючим, здатним об'єднати суспільство для рішучих змін існуючого порядку [3, 121].

Володимир Путін восени 2014 року заявив: “Росія буде втручатися в українські справи на тій підставі, що український народ є частиною “великого російського миру”, українська держава – помилка історії, штучно створене “складносурядне державне утворення”, а оскільки в Україні кровопролиття, громадянська війна, катастрофа, обов'язок Росії цю ситуацію виправити” [4].

На рівні офіційних документів Росія постійно декларує принципи використання "м'якої сили" у зовнішній політиці. У Концепції зовнішньої політики РФ (2013 р.) мова йде про зміцнення потенціалу “м'якої сили” і про позиціювання Росії як глобального політичного лідера [5]. Обґрунтування переважної доцільності інформаційного впливу подано в Стратегії національної безпеки Російської Федерації до 2020 року (2009 р.) [6]. Політичне керівництво Росії усвідомлює, що в умовах глобалізації, цінності й моделі розвитку стали фактором глобальної конкуренції.

Протягом останніх роківактивно приймаються концептуальні документи РФ у сфері інформації й комунікації, які свідчать про вдосконалення ідеології, способів і інструментів інформаційно-пропагандистського впливу РФ. Насамперед , це Доктрина інформаційної безпеки Російської Федерації. Вона визначає пріоритети й практику інформаційного впливу РФ із метою забезпечення національних інтересів у різних сферах міжнародних відносин [7].

Україна неодноразово ставала жертвою геополітичних інформаційних атак РФ, які були спрямовані на різні сфери життєдіяльності держави.

Зокрема, інформаційні атаки були початі напередодні й у ході проведення Євро-2012, спроб України вступити в НАТО в 2008-2009 р., під час газових і торговельних війн з Росією, і особливо в ході революційних подій 2013-2014 р. На думку Володимира Полевого, заступника керівника

Інформаційно-аналітичного центра Ради національної безпеки й оборони України, інформаційні операції в Україні з боку РФ почалися ще з 1991 року[8].

У всіх цих випадках Україна була об'єктом інформаційних операцій, мішенню для атак з боку суміжної держави, що прагнула в такий спосіб реалізувати свої національні інтереси. Застосування "організаційної зброї""непомітно" для традиційних форм експертного спостереження й "незрозуміло" у рамках традиційної логіки контррозвідувальної діяльності. У цьому зв'язку показовим є первинна реакція не тільки політичного й військового керівництва України, але й Держдепартаменту США й ЦРУ на "Російську весну" як "організаційну операцію" по анексії Криму в лютому-березні 2014 р.

Багатоплановий вплив Росії на внутрішні процеси в Україні є очевидним. У таких умовах вплив російського фактора на відносини обох держав визначаються експертами як інструмент політичної й ідеологічної боротьби [9].

Список використаних джерел:

1. Б. Г. Лиддел Гарт, Энциклопедия военного искусства. Стратегия непрямых действий, Москва, Санкт-Петербург: АСТ, Терра Фантастика 2003, с. 656.
2. J. S. Nye, Bound to Lead: he Changing Nature of American Power, NewYork: BasicBooks 1990, 336 p.
3. Г. Почепцов, Відfacebooky і гламурудоWikiLeaks, Київ 2012, с. 333.
4. В. Путин, Мировой порядок: новые правила или игра без правил? Заседание Международного дискуссионного клуба «Валдай», 24 октября 2014 года. URL : http://kremlin.ru/news/46860
5. Концепция внешней политики Российской Федерации. Утверждена Президентом Российской Федерации В. В. Путиным 12 февраля 2013г. URL : http://www.mid.ru/brp_4.nsf/0/6D84DDEDEDBF7DA644257B160051BF7F, 12.10.2014.
6. Стратегия национальной безопасности Российской Федерации до 2020 года. Утверждена Указом Президента Российской Федерации от 12 мая 2009 г., http://www.scrf.gov.ru/documents/ 99.html, 10.10.2014.
7. Доктрина информационной безопасности Российской Федерации. Утверждена Президентом Российской Федерации В. Путиным 9 сентября 2000 г. URL : http://www.rg.ru/oicial/doc/min_and_vedom/mim_bezop/doctr.shtm, 10.10.2014.
8. Украинское общество позволяет внешнюю манипуляцию общественным мнением – эксперт, http://www.unian.net/politics/995422-ukrainskoe-obschestvo-pozvolyaet-vneshnyuyu-manipulyatsiyu-obschestvennyim-mneniem-ekspert.html, 10.10.2014.

9. Міжнародне безпекове середовище: виклики і загрози національній безпеці України, за заг. ред. К. А. Кононенка, НІСД, Київ 2013, 64 с.

----------***----------

Крицун Т. Р., студентка КПІ ім. Ігоря Сікорського.
Науковий керівник: ***Фурашев В. М.,*** к. т. н., с.н.с. доцент КПІ ім. Ігоря Сікорського.

КОНФІДЕНЦІЙНА ІНФОРМАЦІЯ ЯК НОВЕЛА В ІНТЕРНЕТІ

Щодня все більша кількість людей користується Інтернетом задля передачі, отримання та обробки різноманітної інформації. Контроль зі сторони спеціально уповноважених на це органів та регламентації такої діяльності в законі є невід'ємними від цього процесу. Звідси виникає одразу декілька запитання: « А як бути із захистом інформації, яка є особистою «конфіденційною»?», «Чи існує інформація яка є цілковито захищена ?», «Яку інформацію про особу варто віднести до тієї, яка захищається законом ?». На нашу думку є нагальна потреба у відповідях на вище вказані питання та проведенні детальної характеристики, таких понять як «конфіденційність», «конфіденційна інформація» .

Питанням захисту інформації та конфіденційній інформації зокрема, у доктрині права присвячена велика кількість наукових робіт. Серед тих, що привернули нашу увагу, були праці таких вітчизняних та зарубіжних дослідників як: Бачило І.Л., Брижка В.М., Копилова В.А., Кушакової Н.В., Орлова П.І., Росторгуєва С.П., Нашинець-Наумова А. Ю. та інших.

Відповідно до ч. 2 ст. 21 Закону України «Про інформацію», конфіденційна інформація – це інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, визначених законом [1].

Найкраще на наш погляд поняття конфіденційності розкривається в навчальному термінологічному довіднику «Інформаційна безпека», авторами якого є Богуш В.М., Кривуца В.Г. та Кудін А.М. Згідно з ним, конфіденційність [cofidentiality, privacy] (від латинської confidentia − довір'я) − це властивість не підлягати розголосові; довірчість, секретність,

суто приватність. Поряд із цим терміном також розглядаються поняття адміністративної та довірчої конфіденційності. Оскільки нас цікавить саме конфіденційність інформації, то варто також вказати, ті визначення, які надали науковці в межах даного поняття, а саме: 1) «Конфіденційна інформація − це інформація з обмеженим доступом, що містить відомості, які перебувають у володінні, користуванні чи розпорядженні окремих фізичних чи юридичних осіб або держави і порядок доступу до якої встановлюється ними»; 2)«Конфіденційність інформації − це властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем і (або) процесом» [2 с. 304-305].

В Україні відсутній системний підхід до регулювання сфери Інтернету. Головним чином, це проявляється в відсутності єдиного нормативного акту, що стосувався б такої сфери. Натомість є велика кількість законодавчих актів, у яких норми тільки частково вирішують проблеми які існують в даній сфері.

До загальних законів, які містять норми стосовно регулювання Інтернету належать: 1) Закон України «Про доступ до публічної інформації»; 2)Закон України «Про інформацію»; 3)Законі України «Про авторське право і суміжні права»; 4)Закон України «Про боротьбу з тероризмом»(саме цей нормативний акт визначає обмеження щодо поширення інформації, що можуть бути застосованими до Інтернету).

Стосовно відповідальності за злочини в сфері поширення інформації, то фактично, для правоохоронців та суду немає жодної різниці, яким способом поширюються «кримінально карані відомості». Тобто законодавець не розмежовує фізичне поширення інформації(листівки, публічні виступи) від цифрового (дописи в соціальних мережах, в блогах або на інших он-лайн ресурсах). Інтернет у Кримінальному кодексі України, розглядається на одному рівні з іншими способами поширення інформації, хоча на наш погляд це є помилкою.

Спеціальні законодавчі акти у сфері Інтернет – це Закон України «Про телекомунікації», Закон України «Про основні засади забезпечення кібербезпеки України» та Указ Президента України Про рішення Ради національної безпеки і оборони України від 28 квітня 2017 року «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)»[3].

Отже, можемо зробити висновок, що інформація зберігає свою конфіденційність лише, якщо дотримуються встановлені правила ознайомлення з нею, в іншому ж випадку ніхто не може гарантувати цього.

Навіть на державному рівні немає дієвої досконалої системи захисту такої інформації.

Звідси , судження про те, що особиста інформація в мережі Інтернет абсолютно захищена, на сьогодні є нікчемним.

Незважаючи на сучасні проблеми у цій сфері, слід рухатись у напрямку опановування високих технологій, які застосовують найбільш прогресивні держави, для забезпечення конфіденційності, а також розробляти зміни до законодавства і нормативної бази про інформаційну безпеку, з передбаченням в них поняття інформація поширена в мережі Інтернет та технічні засоби регулювання обігу інформації, тощо.

Не можна залишити поза увагою питання кримінальної відповідальності при заподіянні шкоди поширенням різного роду інформації в Інтернеті. Адже саме при застосуванні для поширення інформації комп'ютерних технологій та мережі Інтернет, суб'єкт злочину, прикладаючи менше зусиль, знано збільшує аудиторію на яку поширеться такий негативний вплив. Саме через це, ми пропонуємо зміни до Кримінального кодексу України, а саме у частині 3 статті 109, до переліку обтяжуючих обставин додати також: використання мережі Інтернет, соціальних мереж та інших інформаційних ресурсів пов'язаних із збільшенням аудиторії, яка отримає таку інформацію.

Наведені міркування є спробою привернути увагу до одного із найважливіших аспектів життя людини − інформації (власне про людину, створеної, поширеної або отриманої нею) та захистити її.

Список використаної літератури:

1. Про інформацію: Закон України від 02 жовтня 1992 року // Відомості Верховної Ради України (ВВР). – 1992. – №48. – Ст. 650.

2. Богуш В. М., Кривуца В. Г., Кудін А. М., «Інформаційна безпека: Термінологічний навчальний довідник» За ред. Кривуци В. Г. — Київ. 2004. — 508 с.

3. Як в Україні регулюються Інтернет та цифрові права користувачів? Аналіз законодавства. *Інтернет свобода*: веб-сайт. URL: https://netfreedom.org.ua/jak-v-ukraini-regulujtsia-internet-ta-tsyfrovi-prava-korystuvachiv/ (дата звернення: 18.09.2019).

----------***----------

Петряєв О. С., аспірант
Національного Інституту
Стратегічних Досліджень.

ВТРУЧАННЯ РОСІЙСЬКОЇ ПРАВОСЛАВНОЇ ЦЕРКВИ У РЕЛІГІЙНІ КОНФЛІКТИ В УКРАЇНІ ЯК ВИКЛИК ДУХОВНО-ГУМАНІТАРНІЙ БЕЗПЕЦІ ТА СОЦІАЛЬНІЙ СТАБІЛЬНОСТІ

Релігійні кризи в Україні, зумовлені наступальною позицією Російської Православної Церкви (далі - РПЦ), яка розглядає Україну як свою «канонічну територію», мають давню історію і налічують багато етапів.

Останній наразі етап подібного духовного протистояння розпочався в 2014 році і триває досі.

Конфлікт в православ'ї слід розглядати й оцінювати не тільки в контексті Російсько-Українського гібридного конфлікту, але і як конфлікт усередині Українського православ'я.

Релігійний елемент гібридної війни Росії проти України полягає в спробі Російської Православної Церкви (РПЦ) впливати на релігійну ситуацію в Україні, використовуючи чинник протистояння Української Православної Церкви Московського Патріархату (УПЦ МП) і Української Православної Церкви Київського Патріархату (УПЦ КП), яка після Об’єднавчого Собору у грудні 2018 року і отримання Об’єднаною Церквою у січні 2019 року Томосу від Вселенського Патріархату на чолі з Патріархом Варфоломієм прибрала нову назву – Православної церкви України (ПЦУ).

Слід зауважити, що третім «гравцем» у зазначеному протистоянні є Українська автокефальна православна церква (УАПЦ). Якщо УПЦ КП та УПЦ МП були до 2019 року спадкоємницями офіційно дозволеної в 1943 році й таємно керованої КДБ СРСР Російської Православної Церкви (РПЦ), то УАПЦ — українська православна церковна організація, що виникла під час національно-визвольних змагань українського народу (1917–1921 рр.) й призупинила своє існування в 1930-му році внаслідок терору та репресій більшовицької влади СРСР. Собор УАПЦ, який відбувся у 1921 році наголосив на непідлеглості Церкви керівництву інших церков і визнав примусовий перехід Київської церкви під зверхність Московського патріархату 1686 року аморальним та антиканонічним актом. Сакральною мовою Церкви була визнана українська.

Попри те, що священство УАПЦ протягом 1926–1937 рр. було винищено більшовицькими каральними органами, єпархії УАПЦ продовжували діяти у Канаді та США.

У 1942-1944 рр. УАПЦ пробувала, скориставшись німецькою окупацією, відновити свою діяльність в Україні, за що радянська пропаганда звинувачувала її згодом у колаборанстві.

5-6 червня 1990 року в Києві відбувся Всеукраїнський Православний Собор, який затвердив факт відновлення УАПЦ і обрав Патріархом Київським Мстислава (Скрипника).

На жаль, хоча архієреї усіх трьох православних церков в Україні - УПЦ КП, УПЦ МП та УАПЦ отримали запрошення на Об'єднавчий Собор від Вселенського патріарха Варфоломія, однак участь у Соборі взяли лише 60 архієреїв (серед них – лише два ієрархи від УПЦ МП; 36 – від УАПЦ). У будь-якому разі, у Об'єднавчому Соборі 15 грудня 2018 року взяли участь представники усіх трьох українських православних Церков, що дало підстави Митрополитові Епіфанієві заявити: «Ми змогли об'єднати три гілки українського православ'я в єдину помісну православну церкву. Ми змогли засвідчити, що ми можемо об'єднатися і створити в Україні єдину помісну церкву нашими спільними зусиллями» [3].

У травні 2019 року виник новий, явно інспірований Москвою, «вектор» протистояння: Почесний Патріарх Філарет (у миру - Михайло Антонович Денисенко) із його «відродженою» УПЦ Церквою Київського Патріархату оголосив «війну» ПЦУ на чолі з Митрополитом Епіфанієм (у миру - Сергій Петрович Думéнко), а заодно – Вселенському Патріархату.

Що б зрозуміти й належним чином оцінити ситуацію із православ'ям в Україні, потрібно навести факти і статистику. За даними статистики [1], станом на 2018 рік, в Україні проживало 44 мільйони населення, з яких 67.3% визнавали себе православними християнами, 9.4% є - греко-католиками, 2.2% - протестантами, 0.8% - католиками. Водночас, лише 0.4% були юдеями.

Серед православних християн 28.7% відносили себе до УПЦ-КП (нині – ПЦУ), 12.8% асоціювали себе з УПЦ МП, а 23,4% просто називавали себе «православними віруючими». Ще 0,3% відносили себе до Української Автокефальної Православної Церкви, 0,2% - до Російської Православної Церкви. 11.9% - «не визначився» [1].

Релігійний конфлікт в Україні виник у контексті взаємовідносин між УПЦ-КП і УПЦ-МП відразу ж після фактичного розпаду СРСР, коли Український екзархат РПЦ перетворився у 1990 році на УПЦ МП (наразі офіційна назва за реєстром — Київська митрополія Української православної церкви).

У 1992 році стався розкол всередині цієї структури. Було відновлено автокефалію Української православної церкви Київського патріархату.

Обидві церкви – ПЦУ як спадкоємниця УПЦ КП і УПЦ Московського патріархату, нарівні з Українською греко-католицькою церквою, вважають себе прямими спадкоємницями Київської митрополії X століття.

Київський Патріархат і його духовний очільник Патріарх Філарет від самого початку збройного конфлікту на Донбасі виступали за беззастережне знищення сепаратизму, повністю підтримавши у цьому відношенні політику президента Петра Порошенка й офіційної влади України у цілому. Ту ж саму лінію продовжила ПЦУ під керуванням Митрополита Епіфанія. Саме ця церква постачає кадри військових капеланів для ЗС України та інших бойових підрозділів, задіяних в АТО (нині – ООС).

Водночас, Очільник УПЦ-МП, митрополит Онуфрій виступав проти «братовбивчої війни», за примирення ворогуючих сторін, за що, його звинувачували в пацифізмі, і потуранні інтересам Москви. На цьому тлі не дивно, що деякі парафії УПЦ-МП переходили в підпорядкування Київського Патріархату та ПЦУ. Зафіксовані й силові захоплення храмів парафій УПЦ-МП.

Багатовекторні релігійні конфлікти в Україні є серйозним викликом стабільності суспільних взаємовідносин, хоча й не загрожують країні «релігійними війнами», як це стверджує московська пропаганда.

Радикалізацію настроїв деякої частини українських віруючих керівництво путінської Росії активно підживлює передусім для того, щоб подавати усе, що відбувається, під кутом зору «неконтрольованості» української соціально-гуманітарної ситуації, яка занурюється нібито у стан некерованого хаосу.

Список використаних джерел:

1. UKRAINE 2018 INTERNATIONAL RELIGIOUS FREEDOM REPORT. 2018. URL : https://www.state.gov/wp-content/uploads/2019/05/UKRAINE-2018-INTERNATIONAL-RELIGIOUS-FREEDOM-REPORT.pdf

2. Митрополит Епіфаній прокоментував обрання на пост предстоятеля Української православної церкви // Новое Время/ 15.12.2018. - https://nv.ua/ukr/ukraine/events/mitropolit-jepifanij-prokomentuvav-obrannja-na-post-predstojatelja-ukrajinskoji-pravoslavnoji-tserkvi-2513628.html

3. Тема дня. Филарет пошел против Епифания. Это грозит ПЦУ расколом? Кондратова В. 13.05.2019. URL : https://www.liga.net/politics/articles/tema-dnya-filaret-poshel-protiv-epifaniya-eto-grozit-ptsu-raskolom

----------*----------**

Гожа Б. Б., **с**тудентка КПІ ім. Ігоря Сікорського.
Науковий керівник: ***Цирфа Г.О.***, доцент КПІ ім. Ігоря Сікорського, к.і.н., доцент.

ПРАВОВІ НАСЛІДКИ ПОДАННЯ АБО НЕПОДАННЯ ІНФОРМАЦІЇ ДО ОРГАНІВ АМКУ

Для здійснення своїх повноважень щодо дослідження та розгляду справ про порушення законодавства про захист економічної конкуренції, органи Антимонопольного комітету України (далі-АМКУ), можуть надсилати суб'єктам, які здійснюють господарську діяльність у письмовій формі вимоги про надання інформації. Слід зауважити, що господарюючі суб'єкти зобов'язані надати відповідну інформацію за отриманим запитом.

У статті 7 Закону України «Про Антимонопольний комітет України», зазначається, що АМКУ наділений повноваженнями здійснювати контроль за дотриманням законодавства про захист економічної конкуренції при розгляді заяв і справ про порушення законодавства про захист економічної конкуренції, проведенні перевірки та в інших передбачених законом випадках АМКУ має повноваження вимагати від юридичних осіб, інших суб'єктів господарювання, їх структурних підрозділів, філій, представництв, посадових осіб та працівників, фізичних осіб надати інформацію, втому числі з обмеженим доступом [3].

Отже, АМКУ та його органи наділені правом запитувати й одержувати від господарюючих суб'єктів фактично будь-яку інформацію. Суб'єкти господарювання надають інформацію, оригінали документів або їх копії безкоштовно. Інформація, яка надійшла до органу АМКУ від суб'єкта використовується для здійснення контролю у відповідній сфері та не може передаватися будь яким іншим третім особам.

Українське законодавство пов'язує настання негативних юридичних наслідків у вигляді відповідальності за подання інформації в неповному обсязі, подання недостовірної інформації та неподання інформації у зв'язку з вимогами про надання інформації, які надсилаються органами Комітету для виконанням ними своїх повноважень[4,22].

У разі виникнення ситуації неподання суб'єктом господарювання інформації, подання недостовірної інформації чи надання інформації у неповному обсязі на господарюючого суб'єкта може бути накладено штрафні санкції, які передбачені законодавством про захист економічної

конкуренції. Також, наслідком такого неподання є створення перешкод для нормального здійснення АМКУ своїх повноважень.

Так, відповідно до пунктів 13, 14, 15 ст.50 Закону України «Про захист економічної конкуренції», порушеннями законодавства про економічну конкуренцію є:

- Неподання інформації у строки, встановлені органами АМКУ чи нормативно правовими актами;
- Подання інформації в не повному обсязі у встановлені строки;
- Подання недостовірної інформації [2].

Згідно з ст.52 Закону України «Про захист економічної конкуренції», органи АМКУ можуть накласти за кожне зазначене вище порушення штраф у розмірі до 1% доходу (виручки) суб'єкта господарювання від реалізації продукції(товарів, робіт, послуг) за останній звітний рік, що передував року, в якому накладено штраф[2].

При притягнені до відповідальності суб'єкта, необхідно також враховувати положення статті 61 Конституції України, яка забороняє притягувати двічі до юридичної відповідальності одного виду за одне й те саме правопорушення [1].

Розглядаючи рішення АМКУ № 34-р/тк від 26.12.2018, можемо побачити, що на підставі доказів, зібраних у справі на суб'єкта господарювання ТОВ "Хуавей Україна" було накладено штраф на загальну суму 109 800 грн за вчинення двох порушень законодавства про захист економічної конкуренції, передбачених пунктом 13 статті 50 Закону України "Про захист економічної конкуренції", у вигляді неподання інформації Антимонопольному комітету України на вимоги Голови Антимонопольного комітету України у встановлені ним строки. Відповідно до ч.8.ст.56 Закону України «Про захист економічної конкуренції» суб'єкт зобов'язаний сплатити штраф у двомісячний строк з дня одержання рішення [6,6].

Аналізуючи звіт АМКУ за 2018 рік, можна зробити висновки, що:

206 інформаційних порушень було припинено АМКУ: серед яких 134 за неподання інформації; 52 - подання інформації не в повному обсязі; 20 – подання недостовірної інформації. [5,240].

12% від загальної кількості накладених штрафів, становлять штрафи за інформаційні правопорушення**.** [5,242]**.**

Відповідальність за порушення інформаційного характеру, які передбачені пунктами 13-15 ст.50 Закону про «Про захист економічної конкуренції», а також при визначенні розміру штрафу, який накладається за таке порушення, органи АМКУ мають брати до своєї уваги загальноправові принципи розумності, справедливості та пропорційності створюючи

співрозмірність між характером, підставами вчиненого порушення та мірою відповідальності [4,23].

Також, необхідно звернути увагу, що основною метою передбаченої законодавством відповідальності за інформаційні правопорушення є не накладення та стягнення з суб'єкта штрафу як такі, а спонукання його до надання органам Комітету відомостей, які є необхідних для повного та об'єктивного дослідження справи або для належного здійснення відповідним органом Комітету інших завдань передбачених законодавством. Якщо суб'єкти буду надавати повну, достовірну інформацію на запити органів АМКУ у встановлені строки, то це полегшить та пришвидшить роботу органу. Адже, штраф виступає як певне застереження для інших господарюючих суб'єктів щодо обов'язковості здійснення законних вимог органів Комітету.

Список використаних джерел:

1. Конституція України: Закон від 28.06.1996 № 254к/96-ВР. База даних «Законодавство України»/ ВР України. URL: https://zakon.rada.gov.ua/laws/ show/254к/96-вр#n4371 (дата звернення 13.09.2019)

2. Про захист економічної конкуренції: Закон від 11.01.2011 № 2210-III. База даних «Законодавство України»/ ВР України. URL: https://zakon.rada.gov. ua/laws/show/2210-14/stru#Stru (дата звернення13.09. 2019)

3. Про Антимонопольний комітет України : Закон від 26.11.1993 № 3659-XII. База даних «Законодавство України»/ ВР України. URL: https://zakon.rada.gov.ua/laws/show/3659-12#n68 (дата звернення 13.09.2019)

4. Про запитування інформації органами Антимонопольного комітету України та застосування відповідальності за порушення, пов'язані з запитуванням інформації: Інформаційний лист від 13.06.2019 № 70/01, С. 43

5. Звіт Антимонопольного комітету України від 12.03.2019 № 2–рп, С.340

6. Рішення Антимонопольного комітету України від 26.12.2018 р. Київ № 34-р/тк.С.7

----------***----------

Бондаренко І. І., студент ФСП КПІ ім. Ігоря Сікорського.
Науковий керівник: ***Фурашев В. М.*** к.т.н., доцент, с.н.с.

ПРАВОВІ ПРОБЛЕМИ ВИКЛИКАНІ СТРІМКИМ ПРОГРЕСОМ ТЕХНОЛОГІЙ

Стрімкий розвиток науки, виробництва створює як нові можливості, так і проблемні питання на які немає однозначної відповіді.

Звісно попри все як використання терміну штучний інтелект, людство поки не може похизуватися їм за суттю. Але певні задатки цього вже є.

В ідеалі штучний інтелект, якщо коротко, це комп'ютерна програма наділена функціями прерогатива яким надана традиційно лише людині. А саме творчість, емоції, свідомість в цілому.

Зараз же ми спостерігаємо як «роботи» можуть робити певні функції як людина та навіть краще. Мова йде про фізичні функції. Роботи точніше за людину відрізають деталі на виробництві. Програми виграють людей у грі в шахи. Автопілот «Tesla» рятує водіїв від ДТП завдяки своїй більш швидкій реакції.

Багато людей боїться автоматизації та штучного інтелектом через те що вони втратять роботу. Так само у свій час боялися промислової революції. Але фермери стали робітниками заводів, а водії візків с конями пересіли на автомобілі. Так само і зараз коли кожному необхідно знати англійську мову, так в найближчому часі кожному необхідно буде знати мови програмування.

І тоді вже можна провести паралель. Що так, швидше за все зникнуть робочі місця які є зараз, але замість них з'являться нові.

Щодо робочої сили зрозуміло, але як бути з творчістю. Програмісти прагнуть створити програми які будуть здатні написати пісню чи намалювати картину і такі вже є, які на базі машинного навчання здатні обробити мільйони витворів мистецтва та на їх базі створити свої. Звісно здавалось би на базі чогось, але хіба творчість людини в своїй більшості у нас час надихатися тим що вже є і переосмилює існуючі твори.

Уявімо такі роботи-андроїди у майбутньому, але хто буде відповідати за плагіат твору який створить робот? Автор програми? Але сам автор може не пам'ятати чи не знати як це відбулося адже машинне навчання уявляє собою закладений алгоритм за яким програма сама розвивається наче дитина, але без нагляду батьків. Чи можна притягнути такого робота до відповідальності? Чи буде у цьому сенс? Якщо він наділений свідомістю то

може і буде. Скажімо в’язниця для роботів. Де їх перевиховують. Адже в тому і суть виправний закладів. «Перевиховати людину більше так не робити».

Також вже в наш час є дилеми через ті самі автопілоти «Tesla». Скажімо ситуація: зненацька вибігає дитина на проїзджу частину. І є вибір наїхати на дитину чи виїхати на зустрічну смугу тим самим пожертвувати життям власника. Так наче зрозуміло що життя дитини важливіше і все таке. Але уявіть як ви ідете в тій машині і вона різко виїзджає на зустрічну смугу та врізається в вантажівку. Погодились би на таке? Можливо компанії «Tesla» треба виробляти дві версії автомобіля: «егоїст» та «альтруїст». Або перед покупкою власник має проставити галочки як автомобіль має діяти в певних ситуаціях . Тим самим покладати відповідальність на власника.

Попри всі бюджети цих розробок автопілот все ж таки досі алгоритм, а не самостійний «організм». Ми не достатньо знаємо з біологічної точки зору як влаштовані наші мізки. Наша свідомість. І якби ми точно знали як це працює тоді точно могли би перекласти це на мову цифр.

Список використаних джерел:

1. 21 урок для 21-го століття, Юваль Ной Харари, -2018. -624 с.
2. Чи з'явиться коли-небудь штучний інтелект з свідомістю? https://hi-news.ru/computers/poyavitsya-li-kogda-nibud-iskusstvennyj-intellekt-s-soznaniem.html. URL: https://vc.ru/p/neural -networks.
3. Бум нейромереж: Хто робить нейронні мережі, навіщо вони потрібні і скільки грошей можуть приносити https://www.skoltech. ru/media/bum-nejrosetej -kto-delaet-nejronnye-seti-zachem-oni-nuzhny-i-skolko-deneg-mogut-prinosit. URL: https://vc.ru/p/neural-networks.

----------***----------

Матіяш А. А., Качинський А. Б.,
КПІ ім. Ігоря Сікорського.

ПОРІВНЯННЯ АЛГОРИТМІВ КЛАСИФІКАЦІЇ МАШИННОГО НАВЧАННЯ НА ПРИКЛАДІ МОДЕЛЮВАННЯ КОЛЕКТИВНИХ РІШЕНЬ У ВЕРХОВНІЙ РАДІ УКРАЇНИ VIII СКЛИКАННЯ

Анотація. В роботі здійснено порівняння основних алгоритмів машинного навчання, що вирішують задачу класифікації, на прикладі моделювання результатів голосувань депутатів Верховної Ради України VIII скликання. Описані теоретичні засади побудови моделей класифікаторів та процес формування навчального та контрольного масивів даних. Надані рекомендації до вибору алгоритмів класифікації у сфері прийняття колективних рішень.

Вступ. Моделювання колективного прийняття рішень сьогодні займає важливе місце в інформаційній сфері та сфері кібербезпеки зокрема, адже будь-які важливі рішення не приймаються одноосібно, більшість сучасних держав живуть за настановами демократії, при дотриманні яких, волевиявлення народу здійснюється через представників, що формують різні органи влади, рішення в яких приймаються колективно. В Україні кожну з гілок влади теж представляє відповідний орган: законодавчу – Верховна Рада України, виконавчу – Кабінет Міністрів України, судову – Конституційний Суд України. Розуміння та моделювання процесів ухвалення рішень в подібних установах є важливим пунктом в сфері національної безпеки для будь-якої держави.

Групове прийняття рішень - це ситуація, в якій люди колективно приймають вибір із альтернатив, що стоять перед ними. Потім рішення більше не приписується жодній окремій особі, яка є членом групи, адже всі люди брали участь або мали вплив на прийняття того чи іншого рішення.. Альтернативи, які приймаються групами, часто відрізняються від прийнятих особами. Групова поляризація є одним із чітких прикладів: групи, як правило, приймають рішення, більш екстремальні, ніж рішення окремих її членів, у напрямку індивідуальних схильностей.

Існує багато дискусій щодо того, чи призводить ця різниця до кращих чи гірших рішень.

Відповідно до ідеї синергії, рішення, що приймаються у сукупності, мають тенденцію бути ефективнішими, ніж рішення, прийняті однією особою. Однак є також приклади, коли рішення, прийняті групою, є хибними. Фактори, що впливають на поведінку різних соціальних груп,

також впливають на групові рішення. Наприклад, зазначалося, що соціальні групи з високою згуртованістю у поєднанні з іншими попередніми умовами (наприклад, ідеологічною однорідністю та відстороненістю від суперечливих думок) негативно впливають на прийняття групових рішень, а отже, і на ефективність групи [1]. Більше того, коли люди приймають рішення як частина групи, спостерігається тенденція проявляти упередженість щодо обговорення спільної інформації (тобто загальної інформаційної упередженості) на відміну від неподіленої інформації.

Розглянемо деякі найбільш популярні підходи до здійснення вибору альтернатив у колективі:

Прийняття консенсусних рішень;

Намагається уникати "переможців" та "переможених". Консенсус вимагає, щоб більшість схвалила певний спосіб дій, але меншість погодилася йти разом із ходом дій. Іншими словами, якщо меншина протистоїть ходу дій, консенсус вимагає змінити хід дій для усунення негативних ознак.

- методи, засновані на голосуванні;

Діапазон голосування дозволяє кожному члену вибрати один або декілька доступних варіантів. Вибирається варіант з найвищим середнім показником. Більшість вимагає підтримки понад 50% членів групи.

- метод Делфі;

Цей метод є структурованою технікою комунікації для груп, спочатку розробленої для спільного прогнозування, але також використовується для ухвалення політичних рішень.

- дотмократія;

Метод, який спирається на використання форм, званих "аркуші дотмократії", що дозволяють великим групам спільно здійснювати мозковий штурм і визнавати згоду щодо необмеженої кількості ідей, які вони написали.

Прийняття рішень у групах іноді розглядається окремо як процес та результат. Процес відноситься до групових взаємодій. Деякі відповідні ідеї включають коаліції серед учасників, а також вплив та переконання.

Ухвалення рішень як задача класифікації

Спробуємо застосувати підходи машинного навчання для моделювання прийняття рішень у колективі. У випадку прийняття рішень у Верховній Раді України застосовується метод голосування, народні обранці можуть проголосувати «за», «проти», утриматись або взагалі бути

відсутніми при процесі голосування. Рішення приймається, якщо сформована більшість голосів «за». Для моделювання такого колективного рішення потрібно отримати інформацію про результат голосування кожного з депутатів. Тому вихідними змінними або класами будемо вважати голос, утримання або відсутність депутата під час того чи іншого голосування. Таким чином маємо багатоцільову класифікацію з декількома можливими значеннями цільових змінних.

Наступним кроком буде формування масиву ознак – вхідних змінних, що так чи інакше впливають на рішення депутата в процесі голосування. Ознакою є атрибут або властивість, яку мають усі елементи навчальної вибірки, щодо яких слід робити аналіз чи прогнозування. Ознака - характеристика, яка може допомогти при вирішенні проблеми. Задача формування ознак не може бути розв'язана однозначно «правильно», особливо в сфері прийняття колективних рішень, адже на результат голосування може впливати величезна кількість факторів, виділити та отримати інформацію про які просто неможливо. Ознаки важливі для прогнозних моделей та впливу на результати. Можна сказати, чим кращі ознаки, тим кращий результат. Це не зовсім вірно, оскільки досягнуті результати також залежать від моделі та даних, а не лише від обраних ознак. Однак, вибір правильних ознак все ще дуже важливий. Кращі ознаки можуть створювати більш прості та гнучкі моделі, і вони часто дають кращі результати.

В якості джерела навчальних даних були обрані результати голосувань Верховної Ради, що доступні на офіційному сайті [2]. Результати оформлені у вигляді .rtf файлів, що містять дату, час та результат голосування кожного з депутатів (включно з відмітками про відсутність). За допомогою отриманих файлів був сформований набір значень вихідних змінних, проте потрібно також виділити та сформувати ознаки, що описували б кожне голосування. Загальновідомі характеристики депутатів, як от кількість каденцій або вік мають занадто мало унікальних значень, тому їх використання, а також дати та часу голосування не має сенсу. Натомість можна використати кількість присутніх депутатів з розбиттям по політичних силах для відображення фракційного впливу на формування рішення. При наявності більшості членів своєї фракції інші члени фракції можуть змінити свою модель голосування. Сформовані ознаки фактично несуть схожу інформацію та потребують доповнення. Інших суттєвих ознак які могли б описати наміри депутата, ситуацію в країні, чи сесійній залі виявити не вдалось (деякі ознаки, як от зарплата депутатів або внутрішньо фракційні настрої оцінити

складно, а отримати достовірні дані із відкритих джерел взагалі неможливо). Через недостатню кількість ознак спробуємо застосувати інший підхід – згенерувати ознаки самостійно використовуючи різні метадані, зокрема – опис та тему голосувань.

Кластеризація тем голосувань за допомогою латентного розміщення Діріхле

В сфері обробки природної мови, латентне розміщення Діріхле (LDA) - це генеративна статистична модель, яка дозволяє описувати набори спостережень за допомогою сформованих груп (кластерів), що пояснюють, чому деякі частини даних схожі [3]. Наприклад, якщо спостереження - це слова, зібрані в документи, це свідчить про те, що кожен документ є сумішшю невеликої кількості тем і що присутність кожного слова можна віднести до однієї з тем документа. LDA – це приклад тематичної моделі, що являє собою алгоритм кластеризації, який формує кластери із словами, що найбільш підходящі до тієї чи іншої теми (так зване розміщення тем).

У LDA кожен документ розглядається як суміш різних тем. Це ідентично імовірнісному латентному семантичному аналізу (pLSA), за винятком того, що в LDA передбачається, що теми мають розподіл Діріхле.

За допомогою пластинного позначення, яке часто використовується для представлення ймовірнісних графічних моделей (PGM), залежності між багатьма змінними можна чітко фіксувати. Поле - це «таблички», що представляють репліки, які є повторюваними сутностями. Зовнішня табличка представляє документи, тоді як внутрішня табличка являє собою повторені позиції слів у даному документі, кожна з позицій яких пов'язана з вибором теми та слова. M позначає кількість документів, N кількість слів у документі.

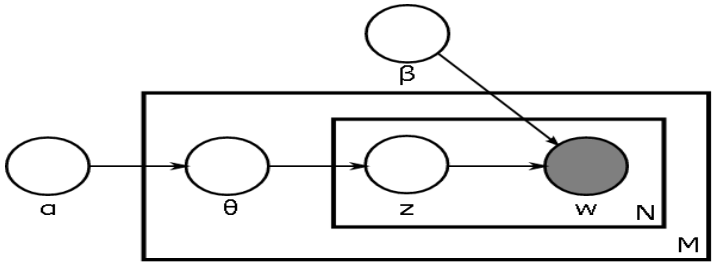

Рис 1. «Пластинне» представлення моделі LDA

- α – параметр розподілу тем по документах;
- β – параметр розподілу слів по темах;
- θ – розподіл тем для певного документа;
- φ – розподіл слів для певної теми;
- z – тема для певного слова в певному документі;
- w – певне слово.

Для моделювання розподілу тематичних слів, використовується припущення, що розподіл ймовірностей зустрічі певних слова в документів перекошений, відповідно лише невеликий набір слів має високу ймовірність бути знайденим у тексті документів. Відповідно до цього припущення використовується розподіл Діріхле. Отримана модель є найбільш широко застосовуваним варіантом LDA на сьогодні.

Виділені теми голосувань були очищені від стоп-слів, слів з найбільшою частотою в корпусі, та слів, що виходять за рамки більшості за індексом TF-IDF. Отриманий набір даних містить 7448 тем голосувань. На основі отриманого набору даних була побудована модель LDA з 30 кластерами (темами).

За допомогою побудованої моделі LDA для кожної з тем голосування була визначена тема (кластер), отримана категоріальна змінна була додана в основний набір даних як ознака «Тема голосування».

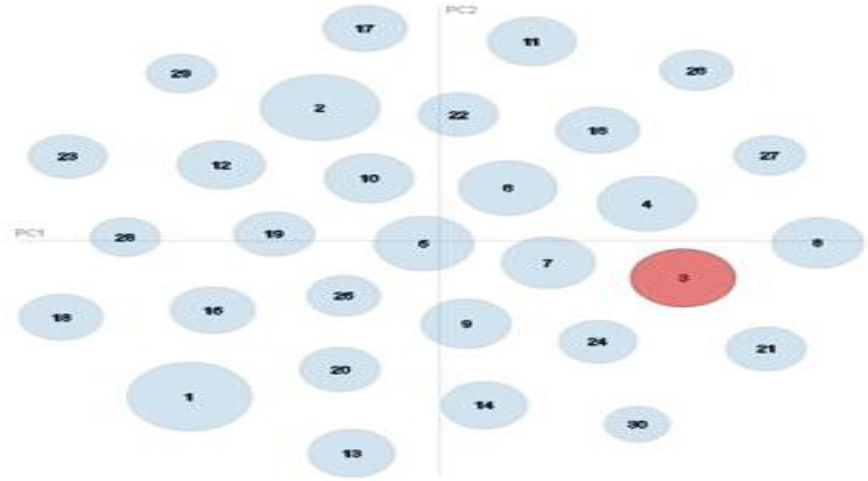

Рис 2. Графічне представлення кластерів моделі

Тематичне моделювання - це класична проблема пошуку інформації. Пов'язані моделі та методи, серед інших, - це латентний семантичний аналіз, незалежний аналіз компонент, ймовірнісний латентно-семантичний аналіз, факторизація позитивної матриці та розподіл Гамма-Пуасона. Модель LDA є високомодульною, тому її можна легко розширити. Основне поле інтересів - моделювання відносин між темами. Воно досягається використанням іншого розподілу замість розподілу Діріхле. Модель корельованої теми дотримується цього підходу [4], індукуючи структуру кореляції між темами, використовуючи логістичний нормальний розподіл замість розподілу Діріхле. Іншим розширенням є ієрархічний LDA (hLDA) [5], де теми об'єднуються в ієрархію за допомогою вкладеного китайського ресторанного процесу, структура якого формується за даними. LDA також

може бути розповсюджений на корпус, в якому документ включає два типи інформації (наприклад, слова та імена), як у подвійній моделі LDA [6].

Огляд основних алгоритмів класифікації

Сформований набір даних готовий до застосування у побудові класифікаторів. Розглянемо обрані алгоритми класифікації.

1.1. KNearestNeighbors (k-найближчих сусідів)

Алгоритм k-найближчих сусідів – метричний метод машинного навчання, що використовується для класифікації та регресії [7]. В обох випадках результат формується з k найближчих навчальних прикладів у просторі сформованого набору даних. k-NN – алгоритм навчання з учителем, де функція лише наближається локально, а всі обчислення відкладаються до класифікації. І для класифікації, і для регресії корисним прийомом може бути присвоєння ваги внескам сусідів, щоб ближчі сусіди робили більший вклад в результат, ніж більш віддалені. Наприклад, загальна схема зважування полягає у наданні кожному сусідові ваги 1 / d, де d - відстань до сусіда. Сусіди взяті з набору значень, для яких відомий клас об’єкта. Це можна вважати навчальним набором для алгоритму, хоча чіткого кроку підготовки не передбачено. Особливістю алгоритму KNN є те, що він чутливий до локальної структури даних. Основними параметрами алгоритму, що використовуються на практиці є кількість сусідів для прийняття рішення, використовувана метрика та степінь p у вибраній метриці. Для побудови моделі KNN використовувалась метрика Мінковського:

$$\rho(x, y) = \left(\sum_{i=1}^{n} |x_i - y_i|^p\right)^{\frac{1}{p}}$$

де x, y – елементи n-мірного простору, степінь p задавався в інтервалі [1; 3].

1.2. DecisionTree (дерево рішень)

Дерево рішень - це інструмент підтримки прийняття рішень, який використовує деревоподібну модель рішень та їх можливі наслідки, включаючи результати випадкових подій, витрати на ресурси та корисність. Дерева рішень зазвичай використовуються в дослідженні операцій, зокрема в аналізі рішень, щоб допомогти визначити стратегію, найбільш ймовірну для досягнення мети, але також є популярним інструментом в машинному навчанні [8].

Дерево рішень - це структура, схожа на блок-схему, в якій кожен внутрішній вузол представляє "тест" на атрибут (наприклад, якою стороною

випаде монета), кожна гілка представляє результат тесту, і кожен вузол являє собою мітку класу (рішення, прийняте після обчислення всіх атрибутів). Шляхи від кореня до листа представляють правила класифікації. Дерева рішень - це клас потужних алгоритмів машинного навчання, що дозволяють досягти високої точності в багатьох завданнях і при цьому бути високо інтерпретованими. Що робить дерева рішень особливими у царині моделей ML, це справді їх чіткість подання інформації. «Знання», засвоєні деревом рішень шляхом навчання, безпосередньо формулюються в ієрархічну структуру. Ця структура утримує і відображає знання таким чином, що їх легко зрозуміти навіть не експертам.

Моделі дерева рішень створюються за допомогою двох етапів: індукція та обрізка. Індукція - це етап, де ми фактично будуємо дерево, тобто встановлюємо всі межі ієрархічного рішення на основі наших даних. Зважаючи на характер дерев, що приймають рішення, вони можуть бути схильні до великих наборів. Обрізка - це процес видалення непотрібної структури з дерева рішень, що ефективно зменшує складність у боротьбі з перенавчанням, що полегшує інтерпретацію.

Серед переваг цього алгоритму можна виділити:

- Легкість в інтерпретації;

На кожному вузлі можна точно бачити, яке рішення приймає наша модель. На практиці можливо повністю зрозуміти, звідки беруться значення та помилок, від того, який тип даних добре спрацює модель і як на вихід впливають значення ознак.

- майже не вимагає підготовки даних.

Багато моделей ML можуть зажадати важкої попередньої обробки даних, такої як нормалізація і можуть вимагати складних схем регуляризації. З іншого боку, дерева рішень досить добре працюють «з коробки» після тюнінгу деяких параметрів.

Недоліки:

- Перенавчання.

Досить часто зустрічається через характер алгоритму дерева рішень. Часто рекомендується виконувати зменшення розмірності, наприклад, за допомогою PCA, щоб зменшити розмір дерева.

1.3. RandomForest (випадковий ліс)

Випадкові ліси або ліси з випадковим рішенням - це ансамблевий метод навчання класифікації, регресії та інших завдань, який функціонує шляхом побудови безлічі дерев рішень під час навчання та отримання класу [9].

RandomForest являє собою ансамблевий алгоритм, що поєднує у собі набір дерев рішень, кожне з яких навчається на окремому піднаборі даних або ознак, результати класифікації або регресії кожного дерева потім агрегуються для отримання остаточного результату алгоритму.

Ключовою є низька кореляція між моделями. Так само, як інвестиції з низьким співвідношенням (наприклад, акції та облігації) збираються, щоб сформувати портфель, більший, ніж сума його частин, некорельовані моделі можуть дати прогнози ансамблю, більш точні, ніж будь-які окремі прогнози. Причина цього чудового ефекту полягає в тому, що дерева захищають одне одного від своїх індивідуальних помилок (до тих пір, поки вони постійно не помиляються в одному напрямку). Хоча деякі дерева можуть помилятися, багато інших дерев виявляться правильними, так що, як група, дерева можуть рухатись у правильному напрямку.

2. Результати порівняння алгоритмів

Розмір сформованого датасету: 15063 x 432. Ознаки: тема голосування (категоріальна), кількість присутніх (по партіях). Цільові змінні: результат голосування кожного депутата. В якості метрики достовірності побудованих моделей використовувалась mean accuracy (середня точність співпадіння змодельованого значення змінної з істинним значенням). Алгоритми порівнювались за стратегією крос-валідації [10], кількість частин: 5. Результати роботи представлені в таблиці 1.

Таблиця 1. Результати порівняння алгоритмів

№	KNN	DecisionTree	RandomForest
1	67.42394609	68.05502566	69.80932472
2	66.02188687	67.80319927	69.82812510
3	68.03960614	68.84818810	70.22286745
4	68.72536486	67.00226689	69.19378346
5	67.36641218	68.56200842	70.87176144

В силу своєї природи KNN та DecisionTree мають схожі результати на різних масивах даних, там, де дані геометрично краще виділяються у класи кращий результат має KNN, в інших місцях – DecisionTree. RandomForest очікувано покращує значення дерева рішень, проте всього на 1-2%. Отримана різниця між оцінками роботи базових та ансамблевих методів свідчить про високу складність зв’язків між сформованими ознаками та вихідними змінними. Отримані результати можуть бути покращені шляхом додання нових, більш інформативних ознак.

Вихідний код програмних сценаріїв доступний в публічному репозиторії [11].

В роботі розглянуто найпопулярніші алгоритми машинного навчання для вирішення задачі класифікації, побудовані моделі мають оптимальні значення параметрів, що були отримані в ході сіткового пошуку значень гіперпараметрів. Отримані значення метрик свідчать про можливість побудови моделей машинного навчання з ціллю моделювання прийняття колективних рішень навіть такими складними структурами як Верховна Рада України.

Отримані моделі можуть бути застосовані в сферах інформаційної та кібербезпеки для прогнозування ухвалення колективних рішень.

Для моделювання процесу ухвалення рішень депутатами Верховної Ради можуть бути застосовані як базові, так і ансамблеві алгоритми машинного навчання, при цьому ансамблеві методи не дали суттєвого приросту значень метрики при встановленому наборі ознак та вихідних змінних.

Список використаних джерел:

1. Moscovici S. The group as a polarizer of attitudes / S. Moscovici, M. Zavalloni. // Journal of Personality and Social Psychology. – 1969. – №12. – С. 125 – 135.
2. Результати голосувань депутатів Верховної Ради України. URL : http://w1.c1.rada.gov.ua/pls/zweb2/webproc2_5_1_J?ses= 10009&num_s=2&num=&date1=&date2=&name_zp=&out_type=&id= - 13.10.2019.
3. Latent Dirichlet Allocation / D.Blei, M. David, A. Ng, R. Jordan. // Journal of Machine Learning Research. – 2003. – №3. – С. 993 – 1022.
4. Girolami M. On an Equivalence between PLSI and LDA / M. Girolami, A. Kaban. – New York: Association for Computing Machinery, 2003.
5. Hierarchical Topic Models and the Nested Chinese Restaurant Process / [D. Blei, M. David, I. Michael та ін.]. // Advances in Neural Information Processing Systems. – 2004. – №16. – С. 24–43.
6. Liangcai S. A Latent Topic Model for Complete Entity Resolution / S. Liangcai, B. Long., 2009.
7. Altman N. An introduction to kernel and nearest-neighbor nonparametric regression / Altman. // The American Statistician. – 1992. – №46. – С. 175 – 185.
8. Quinlan R. Learning efficient classification procedures / Quinlan., 1983. – (Machine Learning: an artificial intelligence approach).
9. Tin K. Random Decision Forests / Kam Tin. – Montreal, 1995. – (Proceedings of the 3rd International Conference on Document Analysis and Recognition).
10. Geisser S. Predictive Inference / Seymour Geisser. – New York: Chapman and Hall, 1993.
11. Diploma computations. URL : https://github.com/AverHLV/diploma-computations - 13.10.2019.

----------*----------**