МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ
МІЖРЕГІОНАЛЬНА АКАДЕМІЯ УПРАВЛІННЯ ПЕРСОНАЛОМ

МАУП

Матеріали
Міжнародної науково-практичної
конференції

“ІННОВАЦІЙНІ МЕТОДИ УПРАВЛІННЯ ЕКОНОМІКОЮ В УМОВАХ ЦИФРОВІЗАЦІЇ БІЗНЕСУ”

10 жовтня 2023 р.

Київ
2023

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ КОНФЕРЕНЦІЇ:

Голова оргкомітету:
Гончаренко Михайло Федорович – ректор Міжрегіональної Академії управління персоналом, д-р екон. наук, проф.

Заступники голови:
Семенець-Орлова Інна Андріївна — директор Навчально-наукового ін-ту управління, економіки та бізнесу, д-р наук з держ. упр., проф.;
Каліна Ірина Іванівна — заступник директора Навчально-наукового ін-ту управління, економіки та бізнесу, д-р екон. наук, проф.

Члени оргкомітету:
Дацій Олександр Іванович — завідувач кафедри маркетингу ННІУЕБ, д-р екон. наук, проф.;
Братусь Анна Анатоліївна — завідувач кафедри економіки та управління бізнесом ННІУЕБ, д-р екон. наук, доц.;
Дмитренко Геннадій Анатолійович — завідувач кафедри управління персоналом та економіки праці ННІУЕБ, д-р екон. наук, проф.;
Коваль Микола Іванович — завідувач кафедри обліку і оподаткування ННІУЕБ, канд. екон. наук, доц.;
Кришталь Галина Олександрівна — завідувач кафедри фінансів, банківської та страхової справи ННІУЕБ, д-р екон. наук, проф.;
Кривоберець Марина Миколаївна — завідувач кафедри організації туристичної діяльності ННІУЕБ, канд. екон. наук, доц.;
Мазур Юлія Володимирівна — декан ННІУЕБ, канд. екон. наук, доц.

Схвалено Вченою радою Міжрегіональної Академії управління персоналом (протокол № 10 від 29.11.23)

Міжнародна науково-практична конференція "Інноваційні методи управління економікою в умовах цифровізації бізнесу": зб. матеріалів конференції (м. Київ, 10 жовтня 2023 р.) / ред. кол.: І. А.Семенець-Орлова (гол. ред.), І. І.Каліна (заст. гол. ред.), Ю. В. Мазур (упоряд. і відп. ред.) та ін. Київ: Міжрегіональна Академія управління персоналом, 2023. 274 с.

ISBN 978-617-02-0389-2 (електронне видання)

Опубліковано наукові статті, в яких висвітлено теоретико-методологічні засади та практичний досвід роботи в таких галузях, як: економіка, маркетинг, менеджмент, публічне управління, туризм в умовах цифровізації бізнесу.

Для науковців, викладачів, наукових співробітників, промисловців, підприємців, аспірантів і студентів.

Тексти тез надано в авторській редакції. Автори несуть повну відповідальність за зміст публікацій, а також добір, точність наведених фактів, цитат, власних імен та інших відомостей.

ISBN 978-617-02-0389-2

© Міжрегіональна Академія управління персоналом, 2023

ЗМІСТ

Азоян Артем Акопович, Гнесь Софія Вадимівна
Використання гендерних стереотипів в рекламі 9

Андрікевич Вікторія Олександрівна, Теплюк Марія Анатоліївна
Мотивація персоналу та її вплив на ефективність підприємства 12

Баля Іван Олександрович
Аналіз змін у структурі запитів, пов'язаних з торгівлею меблями,
у пошуковій системі Google 15

Барандич Богдан Олександрович, Головач Наталія Василівна
Автоматизація управлінських процесів:
впровадження цифрових інструментів управління
та адміністративних завдань 19

Барановська Віра Миколаївна
Цифрові злочини: правовий аспект 21

Барингольц Сергій Михайлович
Сили конкуренції на ринку системної інтеграції в галузі
інформаційних технологій України 26

Бережинський Денис Володимирович
Маркетингова інвестиційна економічна привабливість України
та шляхи залучення іноземних інвесторів 32

Бігдаш Володимир Дмитрович
Тенденції розвитку в Україні цифровізації страхової діяльності 34

Білобовський Святослав Володимирович
Еволюція звітування в контексті викликів сталого розвитку 37

Братусь Ганна Анатоліївна, Ганганов Кирило Євгенійович
Сучасні маркетингові стратегії в умовах цифрової економіки 41

Братусь Ганна Анатоліївна, Домрачов Андрій Павлович
Вплив цифровізації бізнес-процесів підприємств
на розвиток економіки України 44

Братусь Ганна Анатоліївна, Козлова Алла Іванівна
Управління розвитком українських стартапів під час війни 47

Брюховецька Ірина Олександрівна
Вплив інноваційних бізнес-моделей
на конкурентоспроможність підприємств 50

Література

1. Автоматизовані системи управління персоналом. 2022. URL: Автоматизовані системи управління персоналом — Вікіпедія (wikipedia.org).
2. *Баєва О. В., Новальська Н. І., Згалат-Лозинська Л. О.* Менеджмент і адміністрування: навч. посіб. Ч. ІІ. Менеджмент. К.: ДП "Вид. дім "Персонал", 2017. 326 с.
3. *Кріско Ю.* Що таке автоматизація бізнес процесів: визначення, приклади та сервіси. *Snowio*. 2022. URL: https://snov.io/glossary/ua/business-process-automation-ua/

БАРАНОВСЬКА Віра Миколаївна
кандидат юридичних наук, доцент,
професор кафедри цивільно-правових дисциплін та міжнародного права
Навчально-наукового інституту права ім. Володимира Великого,
Міжрегіональна Академія управління персоналом

ЦИФРОВІ ЗЛОЧИНИ: ПРАВОВИЙ АСПЕКТ

Виникнення і розповсюдження такого явища, як кіберзлочинність набуло статусу транснаціональної загрози.

Стрімкий розвиток інформаційних технологій поступово трансформує світ. Відкритий та вільний кіберпростір розширює свободу і можливості людей, збагачує суспільство, створює новий глобальний інтерактивний ринок ідей, досліджень та інновацій, стимулює відповідальну та ефективну роботу влади і активне залучення громадян до управління державою та вирішення питань місцевого значення, забезпечує публічність та прозорість влади, сприяє запобіганню корупції. Саме ці слова є першими, які визначені в "Загальних положеннях" Стратегії кібербезпеки України [1].

Загалом термін інформаційне суспільство виник набагато раніше ніж інформаційні злочини пов'язані з ним.

Перші дослідження цього поняття зустрічаються в працях американських вчених таких як Фріц Махлуп та Деніел Белл. Отже, ще в 30-х роках минулого століття вже розуміли важливість інформаційних технологій. Але ще тоді не розуміли, що з подальшим розвитком і поглибленням інформаційного прогресу людству доведеться боротися з інформаційною злочинністю. Стрімкий розвиток високих технологій (high technology), в тому числі інформаційних технологій (information technology — IT) значно підвищує та полегшує якість життя сучасного суспільства, проте має і низку негативних факторів таких, як сприяння інформаційним злочинам. З 1991 року за класифікатором Інтерполу 1991 до інформаційних злочинів належать[1]:

- QA — Несанкціонований доступ та перехоплення.
- QD — Зміна комп'ютерних даних.

- QF — Комп'ютерне шахрайство.
- QR — Незаконне копіювання.
- QS — Комп'ютерний саботаж.
- QZ — Інші комп'ютерні злочини [4].

Усе це можна назвати одним словом кіберзлочинність. Кіберзлочинність (cybercrime) — це злочинні дії, які відбуваються в віртуальному інтернет-просторі за допомогою інформаційних технологій. На жаль єдиного офіційного визначення цього поняття не має ні в Україні, ні за кордоном. На сайті Інтерполу навіть зазначено той факт, що незважаючи на відсутність єдиного універсального визначення кіберзлочинності, правоохоронці загалом виріз-няють між двома основними видами злочинів, пов'язаних із Інтернетом: це розширений комп'ютерний злочин (або високотехнологічна злочинність) — вишукані напади на комп'ютерне обладнання і програмне забезпечення та злочинність, пов'язана з кіберзахопленням. Багато "традиційних" злочинів активізувалися з появою Інтернету, — злочини проти дітей, фінансові злочини та навіть тероризм [5].

Європейське співтовариство також не залишило поза увагою дану проблему і також визначає, що кіберзлочинність — це є інформаційна злочинність, яку можна класифікувати як злочини, специфічні для Інтернету, — такі як напад на інформаційні системи або фішинг (наприклад, фальшиві веб-сайти банку, щоб вимагати паролі, які дозволяють отримувати доступ до банківських рахунків жертв), інтернет-шахрайство (масштабне шахрайство), яке може здійснюватися такими способами, як крадіжка особистих даних, фішинг, спам, шкідливий код та незаконний контент в Інтернеті, включаючи матеріали про сексуальне насильство дитинства, підбурювання до расової ненависті, підбурювання до терористичних актів та прославляння насильства, тероризм, расизм та ксенофобія [2].

Нині кіберзлочинність становить надзвичайну небезпеку як для всього світу. Існує низка факторів, які сприяють розвитку кіберзлочинності, зокрема, низький соціально-економічний рівень певної держави, недосконаліть законодавчої бази, корумпованість суб'єктів владних повноважень, військові конфлікти, відсутність міжнародних партнерських домовленостей у співпраці щодо подолання кіберзлочинності тощо.

Зауважимо також, що зростання кіберзлочинності є наслідком не лише вищезазначених факторів, а й результатом попиту на протиправні дії, які приносять злочинцям надприбуток. Це — обіг наркотичних засобів та психотропних речовин і їх прекурсорів; розповсюдження дитячої порнографії та снафф-відео; різна закрита (заборонена) інформація; наукові розробки; послуги в легалізації фінансового шахрайства; продаж і лізинг обладнання для підробки грошей та документів; продаж зброї, вибухових речовин та вибухових пристроїв; послуги кілерів, хакерів, кур'єрів; чорний ринок трансплантатів органів, а також інших анатомічних матеріалів людини; обіг контрафактної фармацевтичної продукції і багато іншого.

Серед кіберзлочинців надзвичайно популярним є DeepWeb — це частина Інтернету, яка не індексується переважною більшістю браузерів, тому

користувачі не ідентифікуються в системах, що забезпечує достатньо високий рівень анонімності. В DeepWeb можна потрапити за допомогою програм:“TOR”, “AdvOR”, “SoftEther VPN Client”, “JonDonym” та інших. Також розробляються нові програми-аналоги програми “TOR”, наприклад: “Vuvuzela”, “Alpenhorn”, “Aqua”, “Herd”, “Dissent”, “Riffle”. За непідтвердженими даними, існують і більш таємні рівні Інтернету, ніж DeepWeb. Але навіть потрапивши до “глибинного Інтернету” певного рівня, користувачу залишається недоступною переважна більшість інформації. Для входу на певні сайти потрібні спеціальні посилання. Оплата послуг відбувається за допомогою крипто-валюти на спеціальних електронних платіжних платформах. Тобто, враховуючи вищезазначене, стає цілком зрозумілим, що Інтернет не лише дає змогу злочинцям швидко знаходити “покупців” у всьому світі (що надає таким злочинам статус транснаціонального характеру), але й створює можливість отримати високий рівень анонімності (конфіденційності). Масштаби кіберзлочинності вражають [3].

Якщо підсумувати, то виходить, що такі держави як Україна є надзвичайно комфортним майданчиком для кіберзлочинців, оскільки мають дуже низький рівень захищеності і характеризуються відсутністю правового поля для вирішення цих проблем. Низький рівень відповідальності та незначне фінансування на кіберзахист, військові дії на Сході України, роблять уразливими навіть стратегічно важливі об’єкти держави.

Нині розвинені країни витрачають щороку мільярди доларів на інформаційну безпеку (для посилення кіберзахисту) і щорічно ця сума збільшується. Ту ж тенденцію можна спостерігати в приватному бізнесі.

Сильними країнами в сфері інформаційно-комунікаційних технологій прийнято вважати: США, Німеччину, Велику Британію, Китай, Францію, Ізраїль, Японію. Всі зазначені країни мають потужні економічні потенціали.

Першою країною, яка розпочала боротьбу з протиправними діями у сфері інформаційно-комунікаційних технологій, були США, ухваливши Закон “Про комп’ютерне шахрайство та зловживання” (англ. *Computer Fraud and Abuse Act, CFAA*), який в подальшому оновлювався (18 U.S.C. §1029–1030, §1361) [5], а також посилював покарання. Це — цілком зрозуміло, враховуючи те, що в США значна частка грошей перебуває в безготівковому форматі.

Якщо звернутися до європейського досвіду, то з метою боротьби з кіберзлочинністю, ЄС запровадив законодавство та підтримав оперативну співпрацю, як частину Стратегії кібербезпеки ЄС. Документ “Еластичність, стримування та захист: створення сильної кібербезпеки для ЄС” спирається на подальшу розробку Стратегії кібербезпеки ЄС. Європейська комісія продовжує працювати над ефективним кібернетичним стримуванням в Європі, серед іншого, шляхом сприяння транскордонному доступу до електронних доказів для кримінальних розслідувань [5].

Зважаючи на такий вже наявний досвід розвинутих країн, законодавцям в нашій державі варто задуматися на побудовою ефективного і дієвого правового поля для вирішення ряду проблем, які ми маємо:

Необхідно, зокрема, законодавчо закріпити дефініції (визначення) таких ключових термінів, як: "Цифровий доказ" (англ. *Digital evidence*), "Електронний доказ" (англ. *Electronic evidence*), "Кіберсквоттинг" (англ. *Cybersquatting*), "Кіберсквотер" (англ. *Cybersquat*), "Домейнінг" (англ. *Domaining*), "Хайджекінг" (англ. *Hijacking*), "Манімейкінг" (англ. *Money-making*), "Тайпосквотінг" (англ. *Typosquatting*), "Інтелектуальний кіберсквотінг" (англ. *Intellectual cybersquatting*), "Фішинг" (англ. *Phishing*), "Кіберпростір" (англ. *Cyberspace*), "Віртуальний простір" (англ. *Virtual space*), "Кіберінфраструктура" (англ. *Cyberinfrastructure*), "Кібербезпека" (англ. *Cybersecurity*), "Кіберзахист" (англ. *Cyber-defence*), "Кіберзлочинність" (англ. *Cybercrime*), "Комп'ютерна злочинність" (англ. *Computer-related crime*), "Кіберзалякування" (англ. *Cyberbullying*), Кіберпереслідування (англ. *Cyberstalking*), "Кіберпроступок" (англ. *Cyber-offense*), "Кібердиверсія" (англ. *Cybe-diversion*), "Кібератака" (англ. *Cyberattack*), "Кіберзброя" (англ. *Cyber-weapons*), "Кібертероризм" (англ. *Cyberterrorism*), "Комп'ютерний тероризм" (англ. *Cyber-terrorism*), "Кіберкорупція" (англ. *Cyber-corruption*), "Кібершпигунство" (англ. *Cyber-espionage*), "Кібервійна" (англ. *Cyberwarfare*), "Хакер" (англ. *Hacker*)/"Кіберзлочинець" (англ. *Cybercriminal/Black hat*), "Кібер-угрупування"(англ. *Cyber-grouping*)/"Хакерське угрупування" (англ. *Hacker grouping*), "Комп'ютерний саботаж" (англ. *Computer sabotage*), "Кардінг"(англ. *Carding*), "Вішинг" (англ. *Vishing*), "Скімінг" (англ. *Skimming*)/"Шимінг" (англ. *Shimming*), "Піратство" (англ. *Piracy*), "Онлайн-шахрайство" (англ. *Online-fraud*), "Соціальна-інженерія" (англ. *Social engineering*), "Кардшарінг" (англ. *Card-sharing*), "Мальваре" (англ. *Malware*), "Рефайлінг", "Протиправний контент" (англ. *Illegal content*), "Криптовалюта" (англ. *Cryptocurrency*), "Блокчейн" (англ. *Blockchain*).

І це далеко не повний перелік. Як бачимо, зазначена термінологія має неукраїнськомовне походження.

Позитивний крок вбачаємо в тому, що ця проблема обговорюється в Україні державними установами.

Проте, на нашу думку, з метою досягнення дієвих результатів, потрібна плідна співпраця з іншими країнами. Це, зокрема, включає:

- законодавче закріплення згаданих дефініцій на міжнародному рівні (в міжнародному нормативно-правових договорах з подальшою ратифікацією) для однозначності тлумачення цих термінів в країнах-партнерах;
- посилення відповідальності правопорушників та досягнення узгодження з міжнародними партнерами щодо покарань за протиправні дії в кіберпросторі;
- створення єдиного міжнародного органу з питань кібербезпеки;
- узгодження методики оцінки завданих збитків через протиправні дії у кіберпросторі (така методика має постійно удосконалюватися залежно від технологічного прогресу).

Держави (країни) повинні досягти домовленості з питань щодо законодавства, адже кіберпростір не має кордонів і кіберзлочинність є загальносвітовою проблемою сучасності.

Вважаємо, що з боку державних і політичних діячів України було б доцільно порушити дані питання перед міжнародною спільнотою. Звісно важливим кроком для України стала ратифікація Верховною Радою України (07.09.2005 р.) Європейської конвенції про кіберзлочинність, що була підписана в Будапешті у рамках Ради Європи 23.11.2001 р. 21.07.2006 р. Україна ратифікувала протокол № 1 до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи. Ухвалення доповнення до Конвенції є реакцією світової спільноти на появу комп'ютерного тероризму, який покликаний завдати шкоду комп'ютерам та/або комп'ютерним мережам керуючись релігійними, політичними, ідеологічними, расовими цілями та мотивами.

Система захисту і покарання в українському законодавстві за злочини, вчинені з використанням інформаційно-телекомунікаційних технологій є надзвичайно м'якою, особливо якщо порівнювати з законодавством США. Кримінальним кодексом України [1] максимальне покарання передбачає, згідно зі ст. 301 "Ввезення, виготовлення, збут і розповсюдження порнографічних предметів", позбавлення волі на строк до 20 років. Покарання за іншими статями Кримінального кодексу України щодо злочинів, пов'язаних з інформаційно-комунікаційними технологіями, зафіксовано у [2]: (ст. 176 "Порушення авторського права і суміжних прав"; ст. 190 "Шахрайство"; ст. 200 "Незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима, обладнанням для їх виготовлення"; ст. 231 "Незаконне збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю"; розділ XVI "Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку" та деяких інших актах. Як правило, у справах щодо злочинів, вчинених із застосуванням інформаційно-комунікаційних технологій, правопорушнику в Україні загрожує незначний грошовий штраф або умовне тюремне ув'язнення (обмеження волі), що дає змогу винній особі продовжувати злочинну діяльність. Не надто втішна ситуація спостерігається і в напрямі комп'ютерно-технічної експертизи — через низький рівень фінансування в Україні бракує фахівців в державних експертних установах.

В Україні витрати на кіберзахист є незначними. Цьому значно сприяють військові дії на Сході країни. Проте не можна стверджувати, що для посилення інформаційної безпеки не робляться кроки з боку держави.

Аналізуючи вищезазначену інформацію, маємо констатувати, що досвід країн-учасниць НАТО поступово запроваджується в Україні, проте цих дій недостатньо без комплексного підходу до питання кібербезпеки, належного фінансування та впровадження нових підходів та методів до захисту кіберпростору.

Література

1. Указ Президента України № 96/2016 Про рішення Ради національної безпеки і оборони України від 27 січня 2016 р. "Про стратегію кібербезпеки Украї-

ни" [Електронний ресурс]. Режим доступу: http://www.president.gov.ua/documents/962016-19836
2. Police Organization [Електронний ресурс]. Режим доступу: https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime
3. European Commission: Migration and Home Affairs [Електронний ресурс]. Режим доступу: https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/cybercrime_en
4. 18 U.S.C. [Електронний ресурс]. Режим доступу: https://www.justice.gov/usam/criminal-resource-manual-1001-119 https://www.law.cornell.edu/uscode/text/18/part-I/chapter-47
5. The 2011 U.S. Department of Defense Strategy for Operating in Cyberspace [Електронний ресурс]. Режим доступу: http://csrc.nist.gov/groups/SMA/ispab/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf
6. The 2011 U.S. Department of Defense Strategy for Operating in Cyberspace [Електронний ресурс]. Режим доступу: http://csrc.nist.gov/groups/SMA/ispab/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf

БАРИНГОЛЬЦ Сергій Михайлович
аспірант
ПрАТ "ВНЗ "Міжрегіональна Академія управління персоналом (МАУП)"
e-mail: sergbarin@ukr.net
ORCID: https://orcid.org/0000-0002-1579-6334

СИЛИ КОНКУРЕНЦІЇ НА РИНКУ СИСТЕМНОЇ ІНТЕГРАЦІЇ В ГАЛУЗІ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ УКРАЇНИ

Ринок системної інтеграції та конкурентне середовище галузі

Ринок системної інтеграції є одним з важливих секторів галузі інформаційних технологій (ІТ галузі) України. Компанії системні інтегратори забезпечують впровадження сучасних ІТ рішень для забезпечення ефективної роботи підприємств та задоволення потреб громадян України.

Одним з визначальних параметрів стану галузі, а також важливим чинником визначення стратегії роботи компаній на ринку є стан конкурентного середовища.

Рівень конкуренції в галузі має прямий зв'язок з нормою прибутку та інвестиційним потенціалом галузі. Таким чином, інтенсивність впливу конкурентних сил у галузі визначає інтенсивність припливу капіталу і змушує прибуток знижуватися до рівня вільного ринку, стимулюючи цим здатність підприємств утримувати норму прибутку вище середнього рівня [2]. Відповідно, аналіз конкурентного середовища галузі відіграє провідну роль при формуванні стратегії роботи компаній на ринку.