**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**
**ІНСТИТУТ МОДЕРНІЗАЦІЇ ЗМІСТУ ОСВІТИ**
**АСОЦІАЦІЯ НАВЧАЛЬНИХ ЗАКЛАДІВ УКРАЇНИ ПРИВАТНОЇ ФОРМИ ВЛАСНОСТІ**
**АКАДЕМІЯ WSB У ДОМБРОВІ ГУРНІЧІЙ (ПОЛЬЩА)**
**АСОЦІАЦІЯ СПЕЦІАЛІСТІВ КІБЕРБЕЗПЕКИ**
**ЄВРОПЕЙСЬКИЙ УНІВЕРСИТЕТ**

# ЦИФРОВА ТРАНСФОРМАЦІЯ В ЕКОНОМІЦІ, МЕНЕДЖМЕНТІ І БІЗНЕСІ. ПРОБЛЕМИ НАУКИ, ПРАКТИКИ ТА ОСВІТИ

***Матеріали***
***XXVIII міжнародної науково-практичної конференції***

***24 листопада 2022 р.***

***до 31-річчя Європейського університету***



Київ-2022
Видавництво Європейського університету

**УДК: 004(063)**

**Редакційна колегія: Тимошенко О. І.** - ректор, професор
**Шульга О.А.** – доктор економічних наук, доцент
**Скляренко О. В.** – кандидат фізико-математичних наук, доцент
**Невзоров А.В.** – кандидат технічних наук, доцент

**Відповідальні секретарі:**
к.ф.-м.н., доцент Скляренко О.В., Милашенко В.М.

**Цифрова трансформація в економіці, менеджменті та бізнесі. Проблеми науки, практики і освіти:** Матеріали XXVIII міжнарод. наук.-практ. конф., Київ, 24 листопада 2022 р. / Редкол.: О. І. Тимошенко та ін. – К.: Вид-во Європейського університету, 2022. – 151 с.

Збірник містить матеріали XXVIII Міжнародної науково-практичної конференції

«Цифрова трансформація в економіці, менеджменті і бізнесі. Проблеми науки, практики та освіти».

***Матеріали друкуються за редакцією авторів***

© Європейський університет, 2022

# ЗМІСТ

## СЕКЦІЯ І

## ЦИФРОВА ТРАНСФОРМАЦІЯ В ЕКОНОМІЦІ, МЕНЕДЖМЕНТІ І БІЗНЕСІ: АНТИКРИЗОВІ РІШЕННЯ, МОДЕЛІ КОМПЛЕКСНОГО ВІДНОВЛЕННЯ ПІСЛЯ ВІЙНИ ТА СТРАТЕГІЇ РОЗВИТКУ


**Амбер А.Ю.**
Застосування ГІС-технологій в екологічному менеджменті ..... 8

**Бабій В.М.**
Використання спеціалізованих програм для комунікації всередині команди ..... 9

**Бугайчук М.С.**
Дослідження глобальних інформаційних трендів розвитку приватних медичних лабораторій ..... 11

**Вілянський А.В., Скляренко О. А.**
Цифрова трансформація економіки України: виклики та основні напрямки повоєнної відбудови ..... 12

**Гевці О.І.**
Цифрова трансформація в економіці: глобальний вплив на мікро- та макроекономічні процеси ..... 14

**Геник С.В.**
Порушення прав інтелектуальної власності у мережі Інтернет ..... 20

**Гладуш В.О.**
Цифровізація банківського корпоративного сектору України ..... 22

**Головченко Б.М.**
Управління фінансово-економічними процесами в умовах війни ..... 23

**Гук П.В.**
Моделі відновлення економіки та можливість їх застосування в Україні ..... 25

**Дацьків А.І.**
Цифрові трансформації в українському судочинстві ..... 27

**Дехтяр Б.С.**
Цифрова трансформація судового процесу в умовах воєнного стану ..... 31

**Жила А.В.**
Медіація у бізнесі через призму цифрової трансформації ..... 33

**Здор Д.Л., Ніколаєвський О.Ю.**
Цифрова трансформація бізнесу ..... 35

**Колодінська Я.О., Панченко О.І.**
Розробка цифрового сервісу для створення стартапу ..... 37

**Красьоха В.С, Гаврилюк Д.М.**
Вплив війни на ІТ-ринок України ..... 38

**Курінний С.С.**
Вплив дистанційного режиму роботи на економічну безпеку підприємства ..... 39

**Левцун Я.О.**
Прийоми та методи управління ризиками на підприємстві.....41

**Ліщинський А.М.**
Стратегічний вплив ІТ-галузі на стабілізацію економіки України у воєнний та післявоєнний періоди.....43

**Майстренко Ю. В.**
Дослідження інформаційно-комунікаційних технологій оптимізації бізнес-процесів у сфері готельного бізнесу.....45

**Наложитова К.О.**
Оцінка збитків та інструменти відновлення України в умовах війни.....48

**Несвіт Д.**
Стратегія розвитку організації: теоретичний аспект.....50

**Освійчук Т.П.**
Інститут державної реєстрації спеціального майнового права на об'єкти нерухомого майна.....52

**Панасенко Р.О.**
Проблема ідентифікації осіб електронного правочину при Інтернет-торгівлі.....54

**Покидько Д.Ю., Литвиненко Л.О.**
Створення та розробка ігрових додатків «Економічні онлайн-ігри» на Unity.....56

**Протопопов Д.Я.**
Проблеми регіональної статистики в умовах децентралізації та цифровізації влади...58

**Святобог О.С.**
Стратегії розвитку ринку програмного забезпечення в Україні.....64

**Тарнавський А.С.**
Цифрова трансформація в автомобілебудуванні: основні виклики та перспективи розвитку в Україні.....65

**Троян К.М., Скляренко О.В.**
Практичні кейси та перспективи розвитку технологій штучного інтелекту.....66

**Федько А. В.**
Проблеми та перспективи ведення бухгалтерського обліку за міжнародними стандартами фінансової звітності.....68

**Чабаненко О.С.**
Цифровізація бізнес-процесів підприємства.....71

**Школьнік С.О.**
Соціальні мережі як інструмент просування в професії юриста.....74

## СЕКЦІЯ ІІ

## ТРЕНДИ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ ОСВІТИ В УМОВАХ ВІЙНИ: НОВІ ВИКЛИКИ, ТЕНДЕНЦІЇ У ГАЛУЗІ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

**Артемчук О.Ф.**
Сучасний погляд на формування політичної культури молоді ..... 77

**Голіян Р.Л., Ліщинський А.М.**
Аналіз комп'ютерних технологій перевірки знань ..... 79

**Засадна Х.О., Лозовецький Ю.І.**
Система інформатичної підготовки спеціалістів фінансово-кредитної сфери для нової економіки ..... 80

**Засадна Х.О., Піх О.З., Веретюк К.В.**
Стандарти інтелектуального аналізу даних ..... 83

**Коцун В.І.**
Мобільний додаток для підвищення ефективності навчання ..... 86

**Литвиненко І.В., Опольський М.В.**
Електронна система документообігу в закладах загальної середньої освіти України ..... 87

**Майстренко Г.І.**
Суспільні трансформації: соціальні мережі як засіб комунікації у вищій школі ..... 89

**Маленко І.В.**
Розвиток цифрових платформ навчання ..... 92

**Милашенко В.М., Суслін В.В., Манолі А.І.**
Цифровізація студентоцентрованого навчання в умовах євроінтеграції ..... 94

**Одінцов В.С., Волкова Н.М.**
Вдосконалення цифрового освітнього процесу в умовах війни ..... 95

**Пристайко П.П.**
Методика формування дистанційних курсів з дисциплін кафедри ..... 97

**Сольський В.С.**
Тотальна цифровізація освітнього процесу невідворотна ..... 98

**Троян Д.М.**
Цифрова трансформація освіти в умовах війни: до питання актуальності онлайн-освіти ..... 99

**Хрущ Н.П., Ревула В.В.**
Програмне забезпечення для моделювання нейронних мереж ..... 101

**V. V. Tretynyk**
Machine learning and text mining in realization of clastering of newspaper notes ..... 102

## СЕКЦІЯ ІІІ

## ЗАГРОЗИ ТА БЕЗПЕКА КІБЕРПРОСТОРУ В УМОВАХ ВІЙНИ ТА ГЛОБАЛІЗАЦІЇ. ПЕРСПЕКТИВИ ТА РИЗИКИ КІБЕРБЕЗПЕКИ


**Базилюк К.Ф., Верхоляк П.Г.**
Нові можливості CSS ..... 105

**Базилюк К.Ф., Шлапак А.В., Артим О.Я.**
Сучасні аспекти несанкціонованого стеження за користувачами в інтернеті ..... 107

**Божаткін С.М., Пасюк Б.Б., Довголуцький І.Р.**
Оцінка ризиків інформаційної безпеки підприємства ..... 110

**Васильєв В., Пашорін В.І.**
Технологія Honeypot для захисту комп'ютерної мережі ..... 111

**Ісаєв Я.С., Остапчук І.С.**
Реалії кібербезпеки України в умовах військового стану ..... 113

**Кісельов А.Р., Скляренко П.А.**
Забезпечення інформаційної безпеки бізнес-процесів сучасної компанії ..... 115

**Коваль В.В., Любчак В.О.**
Навчальний центр кафедри кібербезпеки з функціональністю симуляційного кіберполігону ..... 117

**Коміренко Д.В.**
Кібербезпека підприємств критичної інфраструктури міста Дніпро в контексті сучасних викликів ..... 120

**Коцун В.І., Костін М.О., Добиш А.В.**
IP-системи в технологіях безпеки ..... 121

**Мудрик Б.І.**
Особливості забезпечення безпеки кіберпростору України в умовах війни ..... 123

**Онащенко А.О., Левченко С.В.**
Концепція та етапи APT-атак (Advanced Persistent Threat) ..... 125

**Паньова І.**
Етапи впровадження системи управління інформаційною безпекою ..... 128

**Пилипчак Р.В., Горик Д.Ю.**
Апаратні та апаратно-програмні засоби захисту інформації ..... 130

**Савченко Я.О., Чмиренко О.В.**
Розвиток кібербезпеки в умовах сучасної війни ..... 133

**Старчук Є.В.**
Актуальні питання збереження персональної інформації працівників компаній та її розкриття на вимогу контролюючих органів ..... 135

**Фурик Б.Б.**
Кіберпростір в умовах війни та глобалізації ..... 137

## СЕКЦІЯ IV

## ЦИФРОВА ТРАНСФОРМАЦІЯ У СФЕРІ КУЛЬТУРИ ТА СПОРТУ: НОВІ РЕАЛІЇ ТА ВИКЛИКИ

**Анхім Д.**
Креативність як ресурс індивіда, фактор соціально-економічного та соціально-культурного розвитку країни ..... 140

**Букатов Д.В., Романенко О.І.**
Використання штучного інтелекту для генерації цифрового контенту ..... 142

**Дзекунов С.М.**
Цифровізація моніторингу на ринку азартних ігор ..... 143

**Костенко Ю.В.**
Використання цифрових засобів комунікації ..... 145

**Лозинський В.Ю.**
Цифрова трансформація у сфері спорту: нові реалії та виклики ..... 147

**Свириденко А.В., Невзоров А.В.**
Сучасні реалії цифрової трансформації у сфері культури та спорту ..... 149

# СЕКЦІЯ І

# ЦИФРОВА ТРАНСФОРМАЦІЯ В ЕКОНОМІЦІ, МЕНЕДЖМЕНТІ І БІЗНЕСІ: АНТИКРИЗОВІ РІШЕННЯ, МОДЕЛІ КОМПЛЕКСНОГО ВІДНОВЛЕННЯ ПІСЛЯ ВІЙНИ ТА СТРАТЕГІЇ РОЗВИТКУ

## ЗАСТОСУВАННЯ ГІС-ТЕХНОЛОГІЙ В ЕКОЛОГІЧНОМУ МЕНЕДЖМЕНТІ

***А.Ю. Амбер,***
декан факультету економіки та менеджменту,
ПВНЗ «Європейський університет»

02 червня 2022 р. в Стокгольмі (Швеція) коаліція з 1000 зацікавлених сторін із понад 100 країн за підтримки ООН запустила План Дій, щоб спрямувати цифровізацію на прискорення еколого-соціальної складової сталого розвитку, а саме переорієнтувати та визначити пріоритети застосування цифрових технологій для виконання Порядку денного сталого розвитку до 2030 року та вирішення потрійної планетарної кризи: зміни клімату, втрати біорізноманіття та управління відходами.

Саме у документі «Порядок Денний на XXI століття» (Agenda 21), який прийняли на Міжнародній конференції з довкілля та розвитку в Ріо-де-Жанейро (Бразилія) у 1992 році зазначено, що «екологічний менеджмент необхідно віднести до ключової домінанти сталого розвитку та до вищих пріоритетів промислової діяльності підприємств» [4].

З розвитком цифрових технологій, таких як ГІС-системи, за допомогою супутникових даних та застосування математичних методів прогнозування, є можливість зменшити концентрацію забруднюючих речовин у повітрі та ефективно управляти викидами підприємств на національному та глобальному рівнях.

Геоінформаційна система (ГІС) – комп’ютерна програма, що забезпечує збирання, зберігання, перевірку та відображення просторових даних на поверхні Землі, які містять інформацію щодо певного географічного об’єкту у вигляді координат. Дані подаються у вигляді електронних карт з розташуванням об’єктів та пов’язану з ними інформацію у вигляді тексту, чисел та аудіовізуалізації. Все це дозволяє людям аналізувати та розуміти закономірності взаємозв’язку між досліджуваними компонентами [3].

Метою нашого дослідження є встановити зв’язок між наземним та супутниковим моніторингом концентрації забруднюючих речовин в атмосферному повітрі на прикладі м. Києва та розробити модель концентрації забруднюючих речовин, наближених до реально вимірюваних, як цифрового інструменту екологічного менеджменту промислових підприємств.

Для аналізу цифрової складової дослідження використовувалися дані з геопорталу інформаційних послуг, які базуються на космічному спостереженні за навколишнім середовищем та безпекою «Copernicus». Концепція служби «Copernicus» орієнтована на досягнення планетарного, високоякісного та

безперервного спостереження за планетою, а також на забезпечення своєчасною та точною інформацією, яку можна використовувати для оптимізації екологічного менеджменту та забезпечення становлення сталого розвитку регіонів [1,2].

На думку автора, метод регресійного аналізу ідеально підходить для дослідження зв'язку між наземним та супутниковим методами моніторингу концентрації забруднюючих речовин в атмосферному повітрі.

*Список використаних джерел*

1. Забруднення повітря в Україні з космосу / за ред. Ян Лабохи, 2020.
2. Кожушко Л.Ф., Скрипчук П.М. Екологічний менеджмент: підручник. Київ : Академія, 2007. 432 с.
3. Морозов В. В. та ін. Моделювання та прогнозування для проектів геоінформаційних систем. Херсон : ХДУ, 2007. 328 с.
4. AGENDA 21. United Nations Conference on Environment & Development. Rio de Janerio, Brazil, 3 to 14 June 1992.

## ВИКОРИСТАННЯ СПЕЦІАЛІЗОВАНИХ ПРОГРАМ ДЛЯ КОМУНІКАЦІЇ ВСЕРЕДИНІ КОМАНДИ

***В.М. Бабій*,**
аспірант,
ПВНЗ «Європейський університет»

Останнім часом ми інтенсивно переходимо з роботи на місцях на віддалену роботу. До цього призвели спочатку карантинні умови, що з'явились під час пандемії COVID-19, потім – повномасштабна війна. Сьогодні підприємства в Україні часто нехтують комунікацією та підвищенням ефективності своєї діяльності та не застосовують месенджери у корпоративній діяльності. Звичайно, що для вирішення такої проблеми у сфері менеджменту варто розглянути цифрові рішення. Зважаючи на це, для побудови ефективної роботи у команді потрібно використовувати сучасні рішення для обміну інформацією, як месенджери. Зокрема такі, як: Messenger from Meta, Telegram, Skype, Slack та Discord. Вони досить зручні для листування. Їх можливості наведемо у таблиці 1.

*Таблиця 1*

**Порівняння функцій та особливостей месенджерів**

| Месенджер | Групові чати | Основні додаткові переваги | Безпека | Вартість |
|---|---|---|---|---|
| Messenger from Meta | + | комунікації з підписниками сторінки бренду | наскрізне шифрування (end-to-end encryption, E2EE) | Безкоштовний |

| Месенджер | Групові чати | Основні додаткові переваги | Безпека | Вартість |
|---|---|---|---|---|
| Telegram | + | обсяг переданих файлів порівняно великий – до 1.5 ГБ | Шифрування 256 біт за власним протоколом, створення секретних чатів | Безкоштовний. 109,99/місяць |
| Skype | + | є можливість відправки файлів: mp3, зображень, тексту; | Стандартні заходи безпеки | Безкоштовний. Платна версія – $5/місяць |
| Discord | + | організовує всі можливості для комунікації в одному місці | Discord зберігають дані без шифрування, передають інформацію третім особам та спецслужбам | Безкоштовний |
| Slack | + | є можливість запрограмувати ботів, щоб відповідати на типові питання або коментарі співробітників | Робота по HTTPS протоколу, додатково має двохфакторну аутентифікацію | Безкоштовний. Платна версія – $6,67/місяць |

Розглянемо програму Trello. Trello – це така система управління проєктами, що зображується дошками, що містять списки. Списки мають картки, якими подаються задачі. Ці картки перетягуються з одного списку в інший, що може відображати рух якихось функцій або ідеї. Кожна картка може мати різні маркери та списки завдань. Крім того, користувачі дошки можуть об’єднуватись у команди. Також наявні кольорові теги, якими можуть позначатися картки. Кожна картка може мати вкладені файли, коментарі та дату завершення задачі. Сповіщення можуть також у встановлений час приходити на електронну пошту для нагадування про задачу.

Звичайно, важко не згадати програми, які значно спрощують командну роботу та роботу у віддаленому форматі, це – Google Диск, Google Таблиці, Google Документи.

*Список використаних джерел*

1. Trello. URL: https://uk.wikipedia.org/wiki/Trello
2. Telegram. URL: https://uk.wikipedia.org/wiki/Telegram
3. Skype. URL: https://uk.wikipedia.org/wiki/Skype
4. Discord. URL: https://uk.wikipedia.org/wiki/Discord
5. Slack. URL: https://uk.wikipedia.org/wiki/Slack
6. Використання месенджерів як напрям підвищення ефективності управління підприємством. URL: https://www.pdau.edu.ua/sites/default/files/node/4085/ekvay.pdf

# ДОСЛІДЖЕННЯ ГЛОБАЛЬНИХ ІНФОРМАЦІЙНИХ ТРЕНДІВ РОЗВИТКУ ПРИВАТНИХ МЕДИЧНИХ ЛАБОРАТОРІЙ

***М.С. Бугайчук,***
аспірант,
ПВНЗ «Європейський університет»

У сучасних умовах цифрової глобалізації розвиток всіх сфер економіки і суспільного життя знаходиться під активним впливом інформаційно-комунікаційних технологій (ІКТ). Аналіз досвіду використання ІКТ доводить, що помітні трансформаційні технологічні перетворення відбуваються і в медичній сфері також. Це пояснюється, насамперед тим, що медична сфера не мала чітко визначених інформаційно-комунікаційних технологій протягом певного часу, які необхідні сучасному користувачу медичних послуг.

Однією з головних передумов активного впровадження інформаційних технологій у сфері медицини, а саме в медичних лабораторіях – є використання і розвиток Інтернету. У сучасному суспільстві система зв'язку і автоматизації має стійку тенденцію до всебічного розвитку та модернізації, забезпечення новітніми високотехнологічними засобами зв'язку та переходу на сучасні цифрові технології, які передбачають зростання продуктивності праці, а також дозволяють виявляти більше гнучкості на ділових і професійних рівнях.

Глобальний інтернет-трафік у 2023 році згідно з прогнозами авторитетних видань перевищить сумарний інтернет-трафік всіх користувачів до 2016 року. Зважаючи на складну ситуацію у країні, велику кількість людей, які вимушені змінювати своє місце проживання для збереження свого життя та здоров'я, беручи до уваги нещодавній досвід пандемії COVID-19 значна кількість суб'єктів змушена використовувати інформаційні системи та мережу Інтернет для забезпечення стабільної, а головне безпечної роботи.

За оцінками International Telecommunication Union (ITU), на кінець 2019 р. більш, ніж 51 % населення світу, або 4 млрд. людей, використовували Інтернет [2]. При чому за останнє десятиліття вказані показники зросли майже вдвічі (рис. 1).




**Рис. 1 Світові дані про кількість користувачів Інтернету**

**складено за даними* [2]

Дослідження у географічному масштабі свідчать про те, що в Україні у 2019 році доступ до Інтернету мали 77,7% населення, що суттєво перевищує середньосвітовий рівень і трохи нижче від середньоєвропейських показників [3].

Інформаційні технології впливають не лише на діяльність та якість надання інформації у медичних закладах, вони змінюють кінцевого споживача послуг. У зв'язку з цим, не менш важливим інформаційним трендом, як у світовій, так і вітчизняній медичній сфері, є формування цільового сегменту – міленіалів (покоління Y). На сучасному етапі розвитку саме покоління міленіалів активно впливає на розвиток інформаційно-комунікаційних технологій через ряд об'єктивних причин. По-перше, основними споживачами послуг приватних медичних лабораторій є люди середнього віку з доходом середнього рівня і вище, а, по-друге, з розвинутими інформаційно-комунікаційними навичками та активним використанням цифрових технологій.

Отже, в 2015 р. на ринку послуг приватних медичних лабораторій сформувався відносно новий сегмент, що отримав назву «Цифровий споживач» і виділився з покоління Y, для якого є характерною активне залучення до освоєння цифрових технологій. На представників покоління Y вплинув, в першу чергу, розвиток інформаційно-комунікаційних мереж (електронної пошти, месенджерів та соціальних мереж). У зв'язку з цим, приватні медичні лабораторії переважно орієнтуються на залучення саме вказаного сегменту споживачів. Дослідження доводять, що в організаційному плані представники покоління Y цінують швидкість, гнучкість і ефективність обслуговування, отримання інформації здійснюють через Інтернет.

*Список використаних джерел*

1. *Піщуліна О.* Цифрова економіка: тренди, ризики та соціальні детермінанти: доповідь / Центр Разумкова. Київ, 2020. URL: https://razumkov.org.ua/uploads/article/2020_digitalization.pdf (дата звернення 09.11.2022).

2. International Telecommunication Union (ITU): Statistics (2021). URL: https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.

3. Доступ домогосподарств України до Інтернету у 2019 році: статистичний збірник. Київ: Державна служба статистики України, 2020. URL: https://ukrstat.org/uk/druk/publicat/kat_u/2020/zb/07/zb__dd_in19.pdf.

4. *Миронова, Н.* Бумери, міленіали, покоління Z – хто це? Розбираємось у теорії. URL: https://life.pravda.com.ua/society/2020/02/9/239843/.

5. Цифрова грамотність населення України. URL: https://osvita.diia.gov.ua/research.

## ЦИФРОВА ТРАНСФОРМАЦІЯ ЕКОНОМІКИ УКРАЇНИ: ВИКЛИКИ ТА ОСНОВНІ НАПРЯМКИ ПОВОЄННОЇ ВІДБУДОВИ

***А.В. Вілянський,***
***О.А. Скляренко,***
аспіранти,
ПВНЗ «Європейський університет»

Цифрова трансформація є ключовим трендом сьогодення, охоплюючи всі аспекти сучасної соціально-економічної системи. Відповідно до цього цифрова

трансформація впливає на всі групи економічних агентів як в розвинених країнах, так і країнах, що розвиваються. Для України цифрова трансформація набуває особливої актуальності через виклики, спричинені збройною агресією. У контексті даних викликів цифрова трансформація в Україні має діяти за кількома напрямками: антикризове управління, підтримка повноцінного відновлення соціально-економічної системи, стимулювання економічного зростання та всебічного розвитку держави у повоєнний період. Має бути закладено сутнісно новий фундамент для життя громадян на основі принципів доступності, легкості, зручності, інклюзивності, інноваційності. Все це вимагатиме кардинально нових підходів до побудови такої системи, що ґрунтується на цифровій трансформації, а саме: за рахунок залучення відповідних капітальних інвестицій, використання сучасних технологій, розбудови відповідної інфраструктури [1].

Все це потребуватиме комплексної програми заходів в площині цифрової трансформації, що узгоджуватиме державні політики різного напрямку, проєкти бізнесу, ініціативи громадськості та сектору неприбуткових організацій [1; 2]. Такий комплекс дій з цифрової трансформації у рамках повоєнної відбудови України може включати такі рішення:

1. Повноцінна цифровізація державних сервісів.
2. Координація програм модернізації у рамках повоєнної відбудови.
3. Емісія цифрової гривні;
4. Встановлення безпечних цифрових сервісів у розрізі фінансових транзакцій.
5. Розбудова вільного та стабільного доступу до мережі Інтернет.

Зауважимо, що даний комплекс факторів діє як на мікро-, так і макро-рівні – тобто як на рівні окремого бізнесу, так і держави в цілому. Іншою характерною ознакою даного комплексу дій є його мультинаправленість, а саме дія як в площині антикризового управління, так і стимулювання повоєнної відбудови та соціально-економічного розвитку [2; 3].

Повноцінна цифровізація державних сервісів передбачатиме не тільки цифровізацію сервісів з надання довідок, дозволів, ведення архівів, але і зміну парадигми діяльності апарату держави з фокусом на цифрові рішення. Відповідно до цього цифровізація охопить різноманітні сфери роботи держави і не буде сконцентрована виключно на сервісах для населення. Зокрема, цифровізація державних сервісів передбачатиме, наприклад, активне використання аналітики на основі даних супутникового зв’язку, наприклад, у вивченні стану земельних ресурсів, моніторингу та контролі реалізації інфраструктурних проєктів в рамках повоєнної відбудови. Даний комплекс дій також передбачає перехід до застосування цифрових технологій в обробці даних широкого спектру державних реєстрів. Це дозволить, по-перше, суттєво прискорити процес надання сервісу, по-друге, знизить рівень матеріальних і нематеріальних втрат у рамках роботи державних органів.

Цифровізація комплексу дій з координації програм модернізації національної економіки зумовлена потребою в ефективному моніторингу та контролі виділених ресурсів на повоєнну відбудову. Таке рішення сприяє підвищенню ефективності реалізації програм як у короткостроковій, так і в

довгостроковій перспективі (стратегічний аспект розвитку).

Емісія цифрової гривні передбачає використання технології на кшталт блокчейн-технології з метою підтримки унікальності кожної цифрової гривні, що знаходиться в обороті. Відповідно до цього дана технологія буде контрольована регулятором в особі НБУ. Зауважимо, що в світі вже існують приклади успішної реалізації проєкту з емісії цифрової національної валюти в ряді розвинених країн і країн, що розвиваються. Емісія цифрової гривні, зокрема, підвищить ефективність цифрових транзакцій, скоротить витрати фінансової системи. Додатково емісія цифрової гривні уможливить здійснення транзакцій населенням і бізнесом на територіях із зруйнованою банківською інфраструктурою, що особливо актуально в контексті повоєнної відбудови.

Відповідно до цього це зумовить і більшу безпеку фінансових транзакцій для населення та інших економічних агентів. Цифровізація за цим напрямком сприятиме росту транспарентності та посиленню довіри до національної економіки з боку широких кіл як внутрішніх, так і зовнішніх економічних агентів. Це також закладе основу для покращення бізнес-клімату в Україні та вихід українського фінансового ринку та бізнес-практик на провідні позиції поміж країн-лідерів цифрової трансформації, таким чином приваблюючи більше інвестиційного ресурсу та стимулюючи бізнес-активність всередині країни.

На завершення, розбудова вільного та стабільного доступу громадян до мережі Інтернет уможливить ефективну імплементацію всього вище описаного комплексу заходів з цифрової трансформації. Це зумовить пришвидшений потік інформації, фінансових ресурсів, товарів і послуг в національній економіці.

*Список використаних джерел*

1. НІСД. Огляд заходів щодо цифрової трансформації та відновлення економічного розвитку України в умовах війни. URL: https://niss.gov.ua/news/komentari-ekspertiv/ohlyad-.zakhodiv-shchodo-tsyfrovoyi-transformatsiyi-ta-vidnovlennya (дата звернення: 17.11.2022).

2. Ha L.T. Socioeconomic and resource efficiency impacts of digital public services. Environmental Science and Pollution Research. 2022. №29. PP. 83839–83859.

3. Vial G. Understanding digital transformation: A review and a research agenda. The Journal of Strategic Information Systems. 2019. №28(2). PP. 118−144.

## ЦИФРОВА ТРАНСФОРМАЦІЯ В ЕКОНОМІЦІ: ГЛОБАЛЬНИЙ ВПЛИВ НА МІКРО- ТА МАКРОЕКОНОМІЧНІ ПРОЦЕСИ

***О.І. Гевці*,**
аспірант,
ПВНЗ «Європейський університет»

Найважливішим досягненням людства останніх десятиліть є безсумнівно комп'ютеризація та цифровізація всіх ланок суспільного життя. Сьогодні вже важко знайти галузь де б не були присутні цифрові технології, і звичайно економічні процеси були піддані чи не найбільшому впливу цифрових трансформацій. Людство переживає сьогодні перехід від промислової економіки до цифрової економіки – від фізичних продуктів до цифрових товарів і послуг.

На мій погляд, процес цифрової трансформації сучасної економіки

відбувається двома шляхами. По-перше, виникнення абсолютно нових видів продуктів та послуг, які в тому чи іншому сенсі можна назвати цифровими. По-друге, цифрові технології, що докорінно змінили або суттєво вплинули на вже існуючі процеси у виробництві товарів та послуг. Головною метою цифрових трансформацій, на мою думку, є економія часу і ресурсів, в досягненні поставлених задач тих чи інших процесів. Цей процес вже стає нескінченним і зумовлений необхідністю людства отримувати все більше нових продуктів та послуг, які роблять життя зручнішим, якіснішим та безпечним. З вищенаведеного постають питання, який загальний економічний ефект від цифрової трансформації та як впливає цифрова трансформація на мікро- та макроекономічні процеси в сучасній економіці.

Першочергово, варто зупинитись на одному з найважливіших і, на мій погляд, найголовніших секторів економіки, який піддається найбільшому впливу цифрових технологій, це – фінансовий сектор. Різкий ріст цифрових технологій охопив фактично весь сектор фінансових послуг, починаючи від найпростіших буденних процесів (електронних платіжних карток, електронних гаманців, банківських терміналів, банкоматів тощо) до складніших фінансових інструментів, як наприклад, цифрова криптовалюта.

Банки, страхові компанії та інші фінансові установи, впроваджуючи новітні цифрові технології в сфері платіжних послуг, усе більше дозволяють клієнтам керувати своїми фінансами, вільно здійснювати транзакції за мінімальною участю фінансової установи та отримувати доступ до нових продуктів у режимі он-лайн, через додатки які вони можуть обирати на свій розсуд. Різні системи електронних підписів та цифрових ідентифікаторів забезпечують надійний захист користувачів від дій шахраїв та злочинців.

Одним з найбільших секторів фінансового ринку, що пройшов величезну цифрову трансформацію є, – фондовий ринок. Сучасні біржові технології вивели операції з цінними паперами, валютними, іншими продуктами на надзвичайно високий рівень, що вимагає прийняття дуже швидких рішень тому цифрові технології стали надійними інструментами трейдерів. Відомі торгові платформи як наприклад MetaTrade або Libertex Forex, надають користувачам можливість не тільки вести торгівлю в реальному онлайн часі, але і використовувати набір сучасних математичних інструментів для технічного аналізу ринків, його тенденцій, прогнозування росту чи падіння. Наприклад такий важливий інструмент як індекс фондових ринків ( Dow Jones, Nasdaq, S&P500, FTSE то що ) це фактично цифровий математичний інструмент, що використовується інвесторами, фінансистами для того, щоб описати, визначити об’єм і динаміку стану ринку та спрогнозувати рівень дохідності конкретних інвестицій. Окремо хотілось згадати за найновіший з цифрових фінансових інструментів, що з’явився зовсім не давно це, – криптовалюта. Виникнення і запровадження електронної валюти як альтернатива вже існуючим грошовим одиницям вже давно обговорювалась на всіх рівнях фінансового світу. Перш за все її виникнення та подальше впровадження зумовлене швидким розвитком всіх секторів економіки, а стара грошова система паперових і електронних, безготівкових коштів вже не здатна повною мірою задовольнити всі потреби учасників. Це – і доступність, і безпека, і більші можливості контролю над

монетарними процесами з боку емітентів. На жаль сьогодні світ криптовалют існує виключно в паралельному обігу до основних грошових одиниць, фактично це напівлегальний інструмент зосереджений в руках приватних емітентів і котируються вони виключно спекулятивною ситуацією відповідно до ринку на якому розміщені. Найвідоміші крипто валюти такі як (Bitcoin, Ethereum, Dogecoin та інші), набули великої популярності серед учасників фінансових ринків. Віднедавна навіть вже існує окрема крипто біржа на якій учасники вільно торгують всіма наявними крипто-інструментами. Звичайно ж у такого молодого продукту є багато слабких, не досконалих сторін. Наприклад криптовалюту часто використовують для відмивання «брудних грошей» або нелегальних транзакцій великих сум. Оскільки курсове котирування в основному залежить виключно від спекулятивних трендів на ринку, крипто-валюта вважається занадто волатильною і важко передбачуваною. Тільки для прикладу, найпопулярніша криптовалюта Bitcoin за період перших шести місяців 2022 року обвалилась більш ніж у три рази (з 68990 USD до 17630 USD за 1 Btc) [1], так само зростаючи величезними темпами до того. Але попри все, якраз крипто-валюта вважається грошовою одиницею майбутнього. Звичайно ж необхідно щоб контроль за такою грошовою одиницею і право на створення (майнінг) здійснювалися виключно Центральними Банками країн емітентів.

Виробництво товарів та послуг, ще один з секторів який зазнав значних цифрових трансформацій за останні десятиліття. Цифровізація процесів виробництва дало величезний поштовх розвитку високоточних технологій, роботизації складних виробничих процесів, заміни людського ресурсу на лінійних конвеєрних виробництвах. Завдяки величезному попиту на високотехнологічні продукти, країни що ще вчора перебували на нижчих економічних рівнях, стали країнами з високо розвинутою економікою. До прикладу, сьогодні Тайвань являється одноосібним лідером з виробництва напівпровідників, чіпів та мікросхем займаючи 90% ринку. Сьогодні такі країни як, Південна Корея, Сінгапур, Індонезія, Тайвань, Китай, Малайзія завдяки впровадженню високоточних цифрових технологій, домоглися значущого росту в економіці. Основні галузі що найбільше зазнали впливу цифрових технологій – машино- та автомобілебудування, електроніка, медичне обладнання та технології, комунікаційні технології та обладнання та інші. З розвитком Інтернету, надзвичайно змінився і ринок послуг та торгівлі. Розвиток торгово-господарчих процесів на базі Internet-технологій з комерційною формою реалізації (Web-сайтами) сьогодні локалізований на електронних цифрових ринках. Особливостями цифрового ринку є: – ліквідація неінформаційних посередників, прямий контакт клієнта і виробника; можливість формувати в масштабі реального часу будь-які доступні конфігурації виробів за бажанням споживача; умови взаємодії для всіх однакові, зокрема у конкурентній боротьбі; мас-медіа електронного ринку є сприятливим для реклами простором, мережним інтерактивним маркетингом серед аудиторії Internet [2]. Електронна торгівля заснована на структурі традиційної комерції, з використанням електронних мереж додає їй гнучкості. Оперуючи цифровою інформацією в комп'ютерних мережах, електронна торгівля пропонує принципово нові можливості ведення бізнесу, наприклад, полегшує співробітництво ділових груп, поліпшує зв'язки зі

споживачами, знімає обмеження в часі та просторі і т. д. Розвиток Е-торгівлі призводить до значних змін в економіці, що зумовлено використанням нових методів торговельної діяльності. Порівняння електронної торгівлі з традиційною подано в таблиці 1.

*Таблиця 1*

**Інструменти традиційної та електронної торгівлі**

| Інструменти і методи традиційної торгівлі | Інструменти електронної торгівлі |
|---|---|
| Паперовий документообіг | Електронний документообіг |
| Телефонний зв'язок | Зв'язок з використанням комп'ютерних мереж |
| Традиційна пошта | Електронна пошта |
| Традиційна реклама і ЗМІ | Internet-реклама (банерна реклама, пошукова реклама, програми вірусного маркетингу) |
| Використання локальних комп'ютерів тільки у сфері обліку і документообігу | Вся комп'ютерна техніка, що використовується у господарській діяльності, підключена до глобальної мережі через власні веб- і СУБД-сервери. Це усуває вплив географічного фактора на отримання інформації та управлінні фінансовими, матеріальними і інформаційними потоками |
| Мокра печатка і підпис | Електронний цифровий підпис, який не вимагає фізичної наявності учасників в одному місці при укладанні контракту |
| Використання готівки і традиційних безготівкових банківських переказів | Використання систем Клієнт-Банк, Інтернет Банк, електронних грошей, електронних чеків і пластикових карт |
| Сегментація споживачів, орієнтація на масового клієнта | Орієнтація на індивідуальні потреби кожного конкретного споживача |
| Об'єднання співробітників у рамках локальних офісів | Використання механізмів телероботи, мобільної торгівлі і створення віртуальних підприємств |
| Професійні знання і досвід | Безперервний процес навчання протягом життя |
| Опора на безпеку і стабільність | Мобільність, готовність до ризику, схильність до постійного удосконалення |
| Орієнтація на збереження старих робочих місць | Орієнтація на створення нових робочих місць |
| Реалізація всіх бізнес-процесів у межах підприємства | Аутсорсинг - передача компанією частини її завдань або процесів стороннім виконавцям на умовах субпідряду. |

Джерело [3]

Отже, ми бачимо, що основні переваги використання електронної торгівлі в порівнянні з традиційною це – глобальна присутність, підвищення конкурентоспроможності, повна поінформованість про потреби споживачів, скорочення шляху товару до споживача, зниження витрат, нові бізнес-моделі.

Стрімко зростає і вітчизняний ринок електронної комерції. Україна має найбільшу кількість користувачів Internet в Європі, але продажі через Internet не займають лідерських позицій в загальному обсягу. Такі платформи як, Rozetka, Lamoda, Makeup, NEXT UA – найбільші роздрібні торговці електронною комерцією в Україні [4]. За даними The Statistical Portal, вже в 2019 р. обсяг продажу у роздрібній електронній торгівлі становив 3535 млрд. дол. США, що у 2,6 разів більше порівняно з 2014 р. Приріст обсягів роздрібної електронної торгівлі щороку становить в середньому 23-25%, у той час як приріст обсягів

роздрібної торгівлі в цілому щороку становить в середньому 6%. Також зростає частка роздрібної електронної торгівлі у сукупних обсягах продажу в роздрібній торгівлі. До 2023 р. у світі прогнозується зростання обсягів роздрібної електронної торгівлі до 4562 млрд. дол. США, що майже вдвічі більше від показника 2019 р. [5].

Наразі у світі можна виокремити 10 найбільших країн та ринків електронної торгівлі: Китай, США, Великобританія, Японія, Німеччина, Франція, Південна Корея, Канада, та Бразилія. Сьогодні Китай є найбільшим у світі ринком електронної торгівлі на чолі з дочірніми компаніями Alibaba, а саме Taobao, Alibaba.com, Tmall та іншими. Тим часом Сполучені Штати є другою за величиною країною електронної торгівлі в світі, на чолі з гігантами електронної комерції Amazon і eBay. Amazon – один з найдорожчих Internet-майданчиків роздрібної торгівлі, через який здійснюється продаж продукції безпосередньо клієнтові. Amazon посідає перше місце у світі на ринку електронної комерції. Власний капітал компанії складає 43 млрд доларів [6]. Японія також є провідним гравцем e-commerce у світі. Наприклад Rakuten є провідною платформою електронної торгівлі Японії, яка за багато років поглинула вагому кількість веб-сайтів електронної комерції по всьому світу.

Безперечно, цифровізація надає багато переваг, мова йде про численні мультиплікаційні ефекти, коли в єдиний інформаційний простір включаються усі виробничі ланцюжки. Потенційні позитивні ефекти цифрової економіки (цифрові дивіденди) нараховуються, аналізуються потужними аналітичними кампаніями [7] та світовими форумами і за їх даними, розмір цифрової економіки наразі оцінюють від 4,5 до 15,5% світового ВВП[6], і у неї є величезний потенціал для подальшого розширення.

Наразі при всіх величезних перевагах, як, наприклад, і при появі будь-якого нового комплексного технологічного прориву, вплив цифровізації на суспільство та економіку є неоднозначним: з одного боку, спостерігається розвиток економіки на новому рівні взаємодії всіх її елементів, з іншого – руйнується стара система виробництва і розподілу благ. В цьому сенсі не випадково цифрові технології характеризуються як «підривний механізм». Також слід пам'ятати, що коли мова йде про впровадження нових технологій, то їх оцінкам часто притаманний надлишковий оптимізм. Статистика показує, що за останні двадцять років спостерігається стійка тенденція скорочення середніх по світовій економіці темпів зростання продуктивності праці, сукупний ефект від використання цифрових дивідендів виявився слабшим за очікуваний. На практиці тільки 15% проектів з цифровізації підприємств виявилися успішними[8]. Хоча загрози різкого зростання безробіття внаслідок цифрової революції сильно перебільшені і вони легко можуть бути нейтралізовані продуманою державною економічної політикою, проте до цього часу саме вона, була головною причиною ліквідації мільйонів робочих місць і деградації людського капіталу.

До того ж, позитивний ефект від запровадження цифрової економіки розподіляється нерівномірно. Дослідження Світового Банку, показують, що не всі отримують з поширення інтернету рівні вигоди. Так, спостерігається зростання нерівності як між країнами, так і серед груп населення всередині

країни. В залежності від правильного вибору механізмів впровадження цифрової трансформації, для одних це прогрес, для інших – небезпечні тенденції. Наприклад, існує розрив навіть між розвиненими європейськими країнами. Так, користувачів мережі Інтернету в Норвегії 98,4%, тоді як в Сан-Маріно – всього 60,2% [9]. Відмінності між розвиненими країнами і країнами, що розвиваються є ще більш суттєвими. Хоча, найбільш швидкими темпами наразі зростання користувачів інтернету спостерігається у країнах Азії та Африки. Серйозну стурбованість викликає і можливості встановлення загального контролю над громадянами за допомогою цифрових технологій, коли з'являється можливість відстежувати кожен крок, кожне слово людини, а в подальшому — і його думки. Кілька років тому інформаційний простір підірвала новина: — «Китай запроваджує цифрову диктатуру». З такими заголовками можна було побачити статті, що присвячені революційним ініціативам китайського керівництва, коли було прийнято жорстке рішення боротьби з корупцією в масштабах всього суспільства а також відновлення довіри у суспільстві. Це здійснюватиметься за допомогою цифрових технологій, великих масивів даних (Big Data), що дозволяє отримати інтегрований показник по кожному окремому громадянину.

Отже, на сьогодні, можемо з впевненістю зазначити, що в більшій мірі цифрова трансформація основних галузей економіки принесла суспільству більше благ і користі, але існує ще багато проблем з повномірною її інтеграцією в життя людства.

*Список використаних джерел*

1. Top 3 Price Prediction: Bitcoin, Ethereum, Ripple: Who will catch the falling knife? CRYPTOS | 6/20/2022. FX STREET JOURNAL.

2. Коренюк П.І., Попова О.М., Коренюк З.П. Особливості маркетингової діяльності в сучасних умовах пандемії. Український журнал прикладної економіки. 2020. Том 5. № 4. С. 43-50.

3. Кондрус Л.Л., Дзивицька О.А. Проблеми розвитку електронної комерції в Україні. Сімнадцяті економіко-правові дискусії. 2017. URL: ttp://www.spilnota.net.ua/ua/article/id-1885

4. Світовий E-commerce і M-commerce – статистика і факти електронної комерції. URL:2020//marketer.ua/ua/e-commerce-worldwide-statistics-facts

5. Retail e-commerce sale worldwide from 2014 to 2023 (in billion US dollars). The Statistical Portal. URL: https://www.statista.com/statistics/379046/worldwide-retail-e-commerce-sales

6. Global E-Commerce Marketplaces Report. Business Wire. 2018.URL: https://www.businesswire.com/news/home/20180321006098/en/Global-ECommerceMarketplaces-Report-2018-global-online

7. World development report 2016. Digital dividends. — International Bank for Reconstruction and Development. The World Bank. https://openknowledge.worldbank.org/

8. Digitalization is the revolution happening today. The Games for Business learning platform.https://digital-ansformation.gamesforbusiness.com

9. Internet World stats https://www.internetworldstats.com/stats4.htm

# ПОРУШЕННЯ ПРАВ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ У МЕРЕЖІ ІНТЕРНЕТ

***С.В. Геник,***
аспірант,
ПВНЗ «Європейський університет»

Багато компаній регулярно стикаються з порушеннями їхніх прав інтелектуальної власності в мережі Інтернет. Кількість таких порушень та винахідливість порушників зростають по мірі активізації процесу цифрової трансформації.

Зокрема, недобросовісні конкуренти доволі часто незаконно використовують торговельні марки, комерційні назви та захищені авторським правом об'єкти без згоди їх власників. При цьому, чужу інтелектуальну власність використовують для рекламних цілей, несанкціонованого перепродажу продукції компаній-власників і навіть для продажу підробленої продукції.

Для таких цілей, конкуренти створюють профілі в соціальних мережах і реєструють доменні імена, ідентичні або схожі на ті, які належать безпосереднім власникам об'єктів права інтелектуальної власності. Такі дії найчастіше є незаконними та можуть спричинити фінансові та репутаційні збитки компаніям, права яких порушуються. У зв'язку із цим логічно виникає необхідність припинення таких порушень прав інтелектуальної власності.

В Україні доволі часто трапляються ситуації, коли недобросовісні компанії або приватні особи створюють профілі у популярних соціальних мережах для продажу певних товарів. Такі облікові записи часто незаконно використовують об'єкти інтелектуальної власності відомих компаній у рекламних цілях. Найчастіше такі профілі створюються в мережі Instagram.

Найцікавішими з правової точки зору є випадки, коли такі облікові записи продають оригінальну продукцію (яку часто купують безпосередньо в компанії, яка її виробляє та/або офіційно продає) і використовують при цьому назву компанії чи її логотип для просування такого облікового запису. Така діяльність часто вводить споживачів в оману. Споживачі можуть вважати, що купують товари, наприклад, в офіційного дистриб'ютора компанії-виробника. Таким чином, у разі негативного досвіду співпраці з таким недобросовісним продавцем може постраждати репутація безпосередньо компанії-виробника, як такої, яка, на думку споживача, не забезпечила належний рівень сервісу свого дистриб'ютора.

У таких випадках найчастіше можна стверджувати про наявність порушення прав компанії-виробника товару на торговельну марку [1] та (інколи) авторських прав [2] компанії (для прикладу при використанні фотографій продукції із офіційного сайту компанії). З метою захисту порушених прав у таких ситуаціях можна звертатися як до суду із позовом, так і до Антимонопольного комітету України із заявою про недобросовісну конкуренцію [3].

Звернення до суду вимагає більшого рівня попередньої підготовки. До прикладу, у разі виявлення факту використання назви чи логотипу компанії, успішним звернення до суду може бути за умови, що такі об'єкти було попередньо зареєстровано як торговельну марку із поширенням на відповідні

класи товарів. Звернення до Антимонопольного комітету України часто може бути недостатньо ефективним засобом захисту порушених прав.

Ще однією проблемою, з якою регулярно можна зіткнутися є незаконне використання торговельних марок чи комерційних найменувань у доменних іменах. Такий вид порушення прав інтелектуальної власності називається кіберсквотингом [4]. Кіберсквотинг виникає, коли недобросовісний конкурент реєструє доменне ім'я, яке є ідентичним або схожим на зареєстровану торговельну марку чи комерційне найменування, щоб отримати певні переваги в конкурентній боротьбі. Кіберсквотинг, зазвичай, буде вважатися порушенням, якщо доменне ім'я схоже на зареєстровану торговельну марку чи комерційну назву та використовується для просування та реклами подібних товарів чи послуг, які пропонує власник торговельної марки.

Найефективнішими шляхами протидії таким ситуаціям можуть, знову ж таки, бути звернення до суду, подання заяви до Антимонопольного комітету України, а також використання адміністративної процедури згідно з Єдиною політикою вирішення доменних спорів UDRP (тимчасово не діє [5] у зв'язку із воєнним станом [6]). Останній передбачає вирішення спору одним із акредитованих центрів вирішення доменних спорів. Звернення ж до суду та Антимонопольного комітету України у цьому випадку мають недоліки, які є аналогічні наведеним вище.

Таким чином, варто наголосити на важливості проведення компаніями реєстраційної роботи у розрізі прав інтелектуальної власності та підкреслити наявність проблематики, пов'язаної із відсутністю достатньо чіткого регулювання процесу розгляду скарг Антимонопольним комітетом України, що потребує відповідного законодавчого врегулювання. Також важливим кроком назустріч більш ефективному захисту порушених прав інтелектуальної власності у мережі Інтернет було б якнайшвидше відновлення використання адміністративної процедури згідно з Єдиною політикою вирішення доменних спорів UDRP.

*Список використаних джерел*

1. Про охорону прав на знаки для товарів і послуг : закон України від 15.12.1993 No 3689-XII. URL: https://zakon.rada.gov.ua/laws/show/3689-12#Text (дата звернення: 10.11.2022).

2. Про авторське право і суміжні права : закон України від 23.12.1993 No 3792-XII. URL: https://zakon.rada.gov.ua/laws/show/3792-12#Text (дата звернення: 10.11.2022).

3. Про захист від недобросовісної конкуренції : закон України від 07.06.1996 No 236/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/236/96-вр#Text (дата звернення: 10.11.2022).

4. UDRP спір та UDRP правила. Допоможе юрист? URL: https://legalitgroup.com/domenni-batli-worldwide/.

5. WIPO Domain Name Dispute Resolution Service for .UA. URL: https://www.wipo.int/amc/en/domains/cctld/ua/index.html.

6. UDRP suspended in Ukraine. URL: https://domainincite.com/27825-udrp-suspended-in-ukraine.

# ЦИФРОВІЗАЦІЯ БАНКІВСЬКОГО КОРПОРАТИВНОГО СЕКТОРУ УКРАЇНИ

***В. О. Гладуш,***
аспірант,
ПВНЗ «Європейський університет»,
персональний фінансовий консультант
клієнтів середнього бізнесу, АТ КБ «ПриватБанк»

Уряди розвинених країн реалізують спеціальні програми цифрової трансформації (Digital transformation) економіки й бізнесу. В основі останньої лежать кілька ключових технологій: штучний інтелект, роботизація виробництва і бізнес-процесів, багатоканальний збір та аналіз великих даних, застосування на їх основі інструментів поведінкової економіки як для передбачення і задоволення попиту і бажань споживачів, так і активного їх формування. Водночас цифрова трансформація бізнесу – це перегляд корпоративних, ділових, функціональних стратегій та моделей розвитку бізнес-організацій.

Україна є однією з найрозвинутіших країн світу у сфері цифровізації життя і має всі шанси бути лідером у гонці цифрової трансформації. Самий яскравий приклад, коли в делегації України в Сполучених Штатах Америки такий гігант світового ринку, як Apple Inc. дізнавався за державний застосунок «Дія». Так само, цифрова трансформація не обійшла і сектор банківських послуг. Українські банки, а зараз можна казати нео-банки, або прямі банки (це банки без філіальної мережі, яка пропонують свої послуги віддалено через інтернет-банкінг та телефонний банкінг), є найкращими у світі за рівнем якості та швидкості послуг для фізичних осіб і корпоративних клієнтів.

Українці дуже полюбляють застосовувати новітні технології особливо в банківському обслуговуванні. Яскравим прикладом в банківській сфері є коли роздрібний та корпоративний бізнес дуже пов’язані. Це стимулює український бізнес переходити на встановлення платіжного еквайрингу, або його аналогів як NFS мітки чи оплати за допомогою платіжного QR code та значно збільшувати обсяги саме безготівкових розрахунків, що робить бізнес на 100% прозорим та відкритим.

Після додавання можливості зареєструвати підприємців і юридичних осіб через додаток «Дія», більшість банків зробили можливим відкриття рахунку так само онлайн, а не через відділення, що багатьма банками розцінювалося як достатньо ризикова операція.

Більшість банків України вже мають високо розвинені сервіси для клієнтів, але в плані інноваційності продуктів для сегменту середнього і малого бізнесу та великого корпоративного бізнесу, першість тримає найбільший банк України АТ КБ «ПриватБанк». Його найбільший конкурент у плані інноваційності є monobank, але він відносно недавно тільки розпочав працювати з бізнес-клієнтами та відкривати їм рахунки, а про такі послуги, що притаманні більшості великому корпоративному бізнесу, як інкасація торгових точок, підтримка великої розгалуженої еквайрингової мережі, супровід зовнішньоекономічної діяльності, обслуговування великої кількості, особливо бюджетних, організацій,

та навіть військових частин як бізнес-клієнтів за зарплатними проєктами, саме з початку повномасштабних бойових дій, працівники ПриватБанку завдяки технологіям банку могли у будь-якій точці видавати військовим зарплатні картки за 10 хвилин і в той самий день, і, найголовніше, для нашого бізнесу це надання кредитування на поповнення обігових коштів, особливо за президентською програмою 5-7-9.

Є можливість кредитуватися без відвідання відділення банку, для цього є всі сервіси та можливості, фінансову звітність можна до банку подати онлайн, документи для кредитування по заставі, наприклад, так само додаються онлайн, фото бізнесу або застави робляться через спеціальний банківський додаток «Приват Камера», підписати кредитні договори та навіть будь-які документи можна подати через застосунок «Paperless», за допомогою електронно цифрового підпису або нової розробки Smart ID. Саме цей сервіс потім хотіли додати до державної програми «Держава в смартфоні», щоб зробити всі бюрократичні процедури paperless, тобто онлайн і без паперів. Зауважимо, що постійно оновлюються і додаються, як старі, так і нові банківські продукти. Інші банки постійно також додають нові продукти і оновлюють їхній онлайн банкінг для корпоративних клієнтів. У найближчому майбутньому України впевнено з'явиться ще багато банків, які будуть надавати діджиталізовані сервіси для їхніх корпоративних клієнтів.

Таким чином, за допомогою банків країна може зробити обіг готівкових коштів відкритим.

*Список використаних джерел*

1. Цифрова трансформація економіки : мікро- та макроаспекти : колективна монографія / за заг. ред. Н.А. Мазур. Чернівці : Чернівец. нац. ун-т ім. Ю. Федьковича, 2022. 440 с.

2. Купревич Т.С. Цифрові платформи в світовій економіці: сучасні тенденції і напрямки розвитку. Економічний вісник університету. 2018. Вип. 37/1 С. 313.

## УПРАВЛІННЯ ФІНАНСОВО-ЕКОНОМІЧНИМИ ПРОЦЕСАМИ В УМОВАХ ВІЙНИ

***Б.М. Головченко,***
аспірант,
ПВНЗ «Європейський університет»

В ці часи Україна переживає один за найскладніших етапів своєї історії. Військові дії, розпочаті Росією на всій території України, зруйнували всі традиційні підходи до управління фінансово-економічними процесами. Логістика, виробництво та фінансова інфраструктура зазнали значних трансформацій. Товарні потоки реалізуються виключно через західний кордон країни.

Так, у перші місяці російсько-української війни населення на територіях, що перебували під частковою окупацією, мало можливість оплачувати товари та послуги в електронному вигляді, знімати готівку в банкоматах, отримувати державну допомогу у разі втрати роботи тощо. Крім того, існуючі платіжні

системи банків дозволили підприємствам здійснювати банківські платежі навіть у тих регіонах, де фізично закриті відділення. Усе це стало можливим завдяки наявності в Україні розвиненої та розгалуженої мережі банкоматів, терміналів самообслуговування та електронного банкінгу.

У нинішніх умовах виникає необхідність перегляду підходів до оцінки безпеки підприємств з урахуванням впливу фінансової цифровізації, а також відведення їй пріоритетного місця в системі економічної безпеки. Актуальною є не лише розробка підходу до комплексної оцінки економічної безпеки з урахуванням рівня цифровізації, а й визначення рівня впливу кожної складової для прийняття найбільш ефективних управлінських рішень в умовах катастрофічно обмежених фінансових ресурсів.

Ознайомившись із наявними напрацюваннями науковців та аналітиків із забезпечення та оцінки економічної безпеки, а також впливу цифровізації на всі процеси розвитку, можна стверджувати, що не існує усталеного підходу до визначення економічної безпеки та її складових. В кожній країні прийнято дотримуватись власних методів оцінки економічної безпеки, які базуються на безпосередньому розумінні конкретної категорії, а також історичних, фінансових, політичних та інших національних особливостей.

Виходячи з сучасного економічного стану України в умовах воєнного стану, цифровізацію слід враховувати безпосередньо при формуванні економічної безпеки. При цьому основними складовими мають бути безпека фінансового сектору, безпека фондового ринку, а також боргова та бюджетна безпека. Цифровізація впливає на економічну безпеку через банківську інфраструктуру, оскільки цифрові інновації у банківській сфері дозволяють населенню та підприємствам користуватися банківськими послугами та продуктами 24/7 у будь-якій точці України.

Науково-теоретичний підхід до оцінки управління з урахуванням рівня цифровізації є перспективним напрямком досліджень на даний момент, оскільки дані, здебільшого, ґрунтуються на прогнозах, експертних оцінках та не можуть в достатній мірі достовірно враховувати розвиток подій, характер яких часто буває хаотичним.

*Список використаних джерел*

1. Державне фінансове регулювання економічних перетворень: монографія / І.Я. Чугунов, А.В. Павелко, Т.В. Канєва та ін. ; за заг. ред. А.А. Мазаракі. Київ: Київ. нац. торг.-екон. ун-т, 2015.

2. Бюджетно-податкова політика в умовах інституційних перетворень / І.Я. Чугунов, В.Д. Макогон. Вісник КНТЕУ. 2014.

3. Russia’s invasion of Ukraine: Assessment of the humanitarian, economic, and financial impact in the short and medium term / Astrov, V., Ghodsi, M., Grieveson, R., Holzner, M., Kochnev, A., Landesmann, M., Pindyuk, O., Stehrer, R., Tverdostup, M., & Bykova, A. International Economics and Economic Policy, 19(2), 2022.

4. World economic outlook for 2022 and 2023 / Nam, C. W. / CESifo Forum, 23(3), 2022.

5. Russia’s war in Ukraine: Consequences for European countries’ businesses and economies / Prohorovs, A. Journal of Risk and Financial Management, 2022.

# МОДЕЛІ ВІДНОВЛЕННЯ ЕКОНОМІКИ ТА МОЖЛИВІСТЬ ЇХ ЗАСТОСУВАННЯ В УКРАЇНІ

***П.В. Гук,***
аспірант,
ПВНЗ «Європейський університет»

На сьогоднішній день питання повоєнного відновлення України є дуже актуальним. Під час воєнних дій було знищено або пошкоджено велику кількість підприємств, що відповідно призвело до зникнення значної кількості робочих місць та зменшення надходжень в бюджет держави. Для відновлення економіки необхідно мати робочий план відновлення та залучення інвестицій.

Відновлення держави після військових дій не є чимось новим, нажаль, існує безліч прикладів, які вже застосовувались та показали свою ефективність в тій чи іншій країні. Однак, потрібно зважати на те, що такі приклади є дуже прив'язаними до ступеня пошкоджень інфраструктури, наявних ресурсів та сфер виробництв, на яких країна спеціалізується. Через це не існує можливості використати готовий план, який показав свою ефективність десь в іншій країні, адже при різних початкових умовах результат може бути далеким від очікуваного. Саме тому важливо сформувати план відновлення, який буде враховувати особливості економіки України.

Наразі в історії мали місце наступні плани відновлення:

- План Джорджа Маршалла (European Recovery Program, ERP)

План Маршалла почав свою реалізацію в квітні 1948 року та включав план інвестицій в країни Європи на чотири роки. Вже до грудня 1951 року було зроблено інвестицій на загальну суму 13,3-15 млрд. дол. Основний фокус був на відновленні промисловості та обсягів торгівлі.

- Японське відновлення

Після того як близько 70% промисловості не функціонувало в 1939 році, задля відновлення було задіяно наступні інструменти: демонополізація економіки, податкова реформа, земельна реформа, модернізація виробництва та контроль експорту й імпорту.

- Ізраїльське відновлення

Оскільки Ізраїль не мав багатих природних ресурсів та мав нестабільну зовнішньополітичну ситуацію, було вирішено зробити акцент у відновленні на забезпечення безпеки та розвитку. Для підприємців було створено гарні умови, що сприяло збільшенню кількості підприємств і залучення ними іноземних інвестицій, що, в свою чергу, покращило економічну ситуацію в країні.

- План відновлення Боснії і Герцеговини

У випадку з Боснією і Герцеговиною основні зусилля були спрямовані на відновлення цивільної інфраструктури, що мало б сприяти поверненню біженців та тимчасово переміщених осіб. Однак, зовсім мало уваги було приділено промисловості, що вилилось у формування залежної від зовнішньої політики економіки.

Як видно з наведеного вище, існуючі плани відновлення дуже відрізняються один від одного і не завжди були ефективними та оптимальними.

Для України перспективним може бути відновлення експорту електроенергії через велику кількість АЕС, експорт сільськогосподарської продукції через багаті природні ресурси, авіапромисловості і подальший розвиток ІТ-сфери через велику кількість спеціалістів та значні інвестиції. Також важливо під час відновлення, там де можливо, провести цифровізацію, що дасть змогу десь відмовитись від зберігання даних на папері і, як результат, можливість децентралізувати зберігання даних і пришвидшити доступ до них. Цифровізація управління дозволить пришвидшити прийняття рішень та спростить документообіг, що, в свою чергу, відкриє можливість до швидкого реагування на будь-які зміни в майбутньому. Подібні впровадження пришвидшать процес відновлення економіки та закладуть можливість для подальшого покращення.

На міжнародній конференції в Швейцарії уже було представлено план відновлення України. Згідно з ним, для відновлення України необхідно 750 млрд. доларів інвестицій. Загалом, у запропонованому плані йдеться про 15 національних програм. Основні акценти були зроблені на енергетиці, логістиці, військово-промисловому комплексі, агропромисловому комплексі, дерево та металообробці. План відновлення передбачає інвестиції до 2032 року. При цьому на 2022 рік планується наступний розподіл інвестицій:

- 30-35 млрд. дол. – це фінансування дефіциту бюджету;
- 5-10 млрд. дол. – інвестиції в енергетичний сектор;
- 3-10 млрд. дол. – підтримка бізнесу, що постраждав від війни;
- 2-3 млрд. дол. – на відновлення та покращення логістики;
- 2-3 млрд. дол. – на покращення житлового фонду;
- 2 млрд. дол. – на кампанію з повернення біженців;
- 1-2 млрд. дол. – на розмінування територій;
- 1 млрд. дол. – для відновлення соціальної інфраструктури.

Однак, даний план є лише опорним та потребує подальшого вдосконалення. Він вже отримав певну кількість сумнівів та критики у зв’язку зі значними витратами, які дублюють державне фінансування.

Отже, план відновлення України має передбачати відновлення інфраструктури, що дасть можливість повернутися великій кількості біженців, і, в свою чергу, дасть поштовх ринку праці. Важливу роль відіграють подальший розвиток ІТ-сфери, інновацій та цифрова трансформація в усіх сферах людської діяльності. Якщо план відновлення враховуватиме всі особливості української економіки, це дасть змогу не лише відновити ВВП до довоєнного рівня, а й закласти сталий фундамент для подальшого розвитку.

*Список використаних джерел*

1. Іванов С. В. Економічне відновлення і розвиток країн після збройних конфліктів та воєн: невтрачені можливості для України, 2018. С. 75-89.

2. Яка модель повоєнного відновлення спрацює в Україні? URL: https://lb.ua/blog/olena_moshenets/533342_yaka_model_povoiennogo_vidnovlennya.html.

3. Проект плану відновлення України потребує $750 млрд інвестицій. URL: https://espreso.tv/predstavleniy-u-lugano-proekt-planu-vidnovlennya-ukraini-pislya-viyni-potrebue-750-mlrd-investitsiy.

# ЦИФРОВІ ТРАНСФОРМАЦІЇ В УКРАЇНСЬКОМУ СУДОЧИНСТВІ

***А.І. Дацьків,***
партнер,
адвокат ЮК "Алєксєєв, Боярчуков та партнери"

Цифрові трансформації в українському судочинстві тривають уже давно. Цей процес в порівнянні із міжнародним досвідом відбувається доволі консервативно, обережно та поволі. Перші зародки «автоматизованих процесів» виникли після проведення судової реформи Законом України «Про судоустрій і статус суддів» 7 липня 2010 року № 2453-VI. Як наслідок, Рішенням Ради суддів України від 26 листопада 2010 року № 30 було затверджено Положення про автоматизовану систему документообігу суду. Не вдаючись в деталі цих правових актів, слід зауважити, що вперше в процесуальному законодавстві виникло таке поняття, як «електронна пошта» учасника судового процесу. Революційним було також визначення порядку функціонування автоматизованої системи документообігу в судах загальної юрисдикції, яка забезпечувала, серед іншого, об'єктивний та неупереджений розподіл справ між суддями з дотриманням принципів черговості, рівної кількості справ для кожного судді, вірогідності, з урахуванням завантаженості кожного судді, спеціалізації, а також вимог процесуального закону.

Для розуміння, раніше усі справи призначались головою суду, що, не складно здогадатись, створювало корупційну складову та необ'єктивність призначення окремих категорій справ. Що стосується адреси електронною пошти, реформа закінчилась на цьому етапі виключно на згадці про неї у позовній заяві, оскільки кореспонденція здійснювалась як і раніше через «зрозумілі» всім засоби поштового зв'язку.

Наступний відчутний для учасників судового процесу етап діджиталізації українського судочинства запровадився Законом України «Про внесення змін до деяких законодавчих актів України щодо участі у судовому засіданні в режимі відеоконференції» від 4 липня 2012 року № 5041-VI, що надало можливість уже в 2013 році проводити судові засідання в режимі відеоконференції. За задумом законодавця, учасник провадження, який не мав можливість з'явитись в залу судового засідання, повинен був подати відповідне клопотання та зазначити через який конкретно суд він хоче реалізувати своє право на відеоконференцію. Таким чином, суд, який розглядав справу, повинен був синхронізувати дії з іншим судом, який, в свою чергу, забезпечував технічну можливість підключення учасника справи, а також забезпечити можливість чути та бачити хід судового засідання, ставити запитання і отримувати відповіді, реалізовувати інші процесуальні права та виконувати процесуальні обов'язки. У той же час, питання подання документів учасником, їх доступність іншим учасникам провадження та суду, який розглядав справу, для ознайомлення, в первісній моделі «дистанційного» суду було реалізовано, відверто кажучи, в «ручному режимі», та в цілому призводило до автоматичного відкладення розгляду справи.

Тривалий час після таких принципових зрушень в українському судочинстві не відбувалось нічого нового, аж допоки Законом України від 3

жовтня 2017 року № 2147-VIII не було передбачено функціонування Єдиної судової інформаційно-телекомунікаційної системи (надалі – ЄСІТС), яка, в свою чергу, мала забезпечувати:

- принципово новий порядок (алгоритм) призначення та заміни складу суду під конкретну справу;
- реєстрацію в системі усіх процесуальних документів, які релевантні до справи;
- забезпечення обміну документами (надсилання та отримання документів) в електронній формі між судами, між судом та учасниками судового процесу, між учасниками судового процесу;
- реєстрацію електронних адрес адвокатів, нотаріусів, приватних виконавців, арбітражних керуючих та інших учасників справ;
- подання процесуальних документів учасниками з використанням власного електронного цифрового підпису;
- формування матеріалів судових справ та їх розгляд в електронній формі.

Окрім цього, було належним чином закріплено поняття «електронного доказу», як інформації в електронній (цифровій) формі, яка містить дані про обставини, що мають значення для справи, зокрема, електронні документи (в тому числі текстові документи, графічні зображення, плани, фотографії, відео- та звукозаписи тощо), веб-сайти (сторінки), текстові, мультимедійні та голосові повідомлення, метадані, бази даних й інші дані в електронній формі. Зауважено також, що такі дані можуть зберігатися, зокрема на портативних пристроях (картах пам’яті, мобільних телефонах тощо), серверах, системах резервного копіювання, інших місцях збереження даних в електронній формі (в тому числі в мережі Інтернет). З самого початку передбачено було, що ЄСІТС починає функціонувати через 90 днів з дня опублікування відповідного оголошення Державною судовою адміністрацією України у газеті "Голос України" та на веб-порталі судової влади. Згодом, Законом України від 27 квітня 2021 року № 1416-IX врегульовано, що окремі підсистеми (модулі) ЄСІТС запускаються поетапно, але вже за повідомленням Вищої радою правосуддя на тих же ресурсах.

Незважаючи на закріплення на рівні закону окремих революційних технологічних зрушень в українському судочинстві, їх впровадження та використання учасниками судових справ здійснювалось з особливою обережністю та навіть інколи і недовірою.

На перший погляд, і це масово підтримується на рівні стейкхолдерів українського судочинства та парламентаріїв, проблема полягає у відсутності необхідного обладнання, програмного забезпечення тощо. З іншої сторони, слід звернути увагу, що сфера судочинства є дуже консервативною. Для середньостатистичного учасника судової справи перетворення звичного письмового діловодства в електронну форму, а розгляду справ – у дистанційний режим, тобто, без особистої участі, печаток, підписів, інших звичних атрибутів, – чисто психологічно є доволі складно. Пояснити це можна, зокрема, і тим, що будь-яка дія та підготовлений документ – це персональна відповідальність учасника процесу. Тому «контроль процесу» превалює над спокусою використання ноу-хау у часи діджиталізації. Звичайна форма подання документів через канцелярію суду та отримання «заспокійливої» відмітки про

його прийняття наразі забезпечує впевненість клієнтів та їх представників у дотриманні процесуальних вимог. З іншого боку, відправлення документів електронною поштою без доказів підтвердження отримання таких документів адресатом, які можна візуально оцінити, створює безліч конспіративних версій в уяві заявника. Крім цього, необхідно враховувати, що коли мова йде про мільярдні позови, подання принципових для справи документів (апеляційних чи касаційних скарг), та ще й обов'язку в такому випадку дотримуватись процесуальних строків, після спливу яких учасник втрачає право на захист в суді, «збій в системі» може коштувати чийогось бізнесу чи людської долі. Ці, на перший погляд, банальні речі є щоденним головним болем для будь-якого учасника справи, не кажучи вже про відповідальність перед клієнтом, державними інституціями та дисциплінарну відповідальність.

Консервативність, неузгодженість наукового прогресу із законодавчим регулюванням, можливо, також і відсутність належного фінансування програмного та іншого апаратного забезпечення, має наслідком того, що диджитал-революція в судочинстві тривалий час залишалась на рівні ідей та закону.

Поштовхом для зрушень, на наш погляд, було запровадження карантинних обмежень, пов'язаних із Covid-19 пандемією, коли продовження функціонування системи речей у попередній формі стало практично неможливим. Так, Законом України від 30 березня 2020 року № 540-IX передбачено було можливість під час дії карантину учасникам справи взяти участь у судовому засіданні в режимі відеоконференції «поза межами приміщення суду» з використанням «власних технічних засобів». Підтвердження особи учасника справи здійснювалось із застосуванням електронного цифрового підпису. Технічна можливість таких дій була врегульована Порядком, затвердженим Наказом Державної судової адміністрації України від 08 квітня 2020 року № 169. Зокрема, було передбачено систему відеоконференцзв’язку, як комплексу технічних засобів та програмного забезпечення «EasyCon». Для системи українського судочинства таке ноу-хау стало чимось на кшталт теорії всесвітнього вибуху. Уявити ситуацію, за якою учасник судової справи з кухні власної квартири може взяти участь в судовому засіданні ще буквально на початку березня 2020 року сприймалось, як щось фантастичне.

Далі справа, як прослідковується із офіційних повідомлень Вищої Ради Правосуддя, вже розвивалась значно швидшим темпом. Рішенням Вищої Ради правосуддя від 17.08.2021 № 1845/0/15-21 затверджено Положення про порядок функціонування окремих підсистем Єдиної судової інформаційно-телекомунікаційної системи. Уже 05 жовтня 2021 року Вищою радою правосуддя опубліковано оголошення про початок функціонування трьох підсистем (модулів) ЄСІТС – «Електронний кабінет», «Електронний суд», підсистеми відеоконференцзв’язку, що відкрило доступ до більшості із задекларованих раніше опцій ЄСІТС.

Таким чином, довгоочікуваний прогрес такий зрушився з місця, а цифрові технології, як бачимо, не оминули й українське правосуддя. Вказані зміни є як ніколи актуальними в період активних воєнних дій, та забезпечують можливість захисту прав та свобод людей, не створюючи при цьому додаткову загрозу

останнім. Поряд з цим, окремі модулі чи їх реалізація в ЄСІТС потребують доопрацювання та узгодження із нормативним врегулюванням. Наприклад, досі не врегульовано питання допиту свідків через підсистему відеоконференцзв'язку та порядок виклику, ідентифікації таких осіб, адже їх реєстрація в Електронному кабінеті ЄСІТС не є обов'язковою. Також, незважаючи на цифрову ідентифікацію учасників провадження, вони періодично зіштовхуються із ситуацією, коли суд просить на камеру пред'явити посвідчення та інші документи для підтвердження особи чи її повноважень. Дивна, на перший погляд, вимога має насправді абсолютно логічні передумови, адже учасник процесу авторизується в системі через електронний цифровий підпис, який, в свою чергу, зберігається на портативному носії. Не важко здогадатись, що такий носій легко «кочує» чи може «кочувати» з рук в руки, створюючи, таким чином, перешкоди в ідентифікації конкретної особи. Також актуальною проблемою, особливо під час воєнного стану, є періодичні збої в електропостачанні, що автоматично призводить до зриву судових розглядів, оскільки з надто фанатичною довірою до цифрових технологій та їх стабільності віднісся законодавець, тому, на нашу думку, в майбутньому потрібно дотримуватись розумного балансу між використанням інформаційних технологій та звичних, іноді навіть застарілих, проте витриманих часом і надійних інструментів.

Підсумовуючи, слід зазначити, що динаміка цифрових трансформацій в українському судочинстві, дійсно, вражає, а проблеми, на які ми звертаємо увагу, можуть та повинні бути вирішені найближчим часом.

*Список використаних джерел*

1. Про судоустрій і статус суддів: Закон України від 7 липня 2010 року № 2453-VI. URL: https://zakon.rada.gov.ua/laws/show/2453-17#Text .

2. Про затвердження Положення про автоматизовану систему документообігу суду: Рішення Ради суддів України від 26 листопада 2010 року № 30. URL: https://court.gov.ua/sudova-vlada/969076/polozhenniapasds/.

3. Про внесення змін до деяких законодавчих актів України щодо участі у судовому засіданні в режимі відеоконференції: Закон України від 4 липня 2012 року № 5041-VI. URL: https://zakon.rada.gov.ua/laws/show/5041-17#Text .

4. Про внесення змін до Господарського процесуального кодексу України, Цивільного процесуального кодексу України, Кодексу адміністративного судочинства України та інших законодавчих актів: Закон України від 3 жовтня 2017 року № 2147-VIII. URL: https://zakon.rada.gov.ua/laws/show/2147-19 .

5. Про внесення змін до деяких законодавчих актів України щодо забезпечення поетапного впровадження Єдиної судової інформаційно-телекомунікаційної системи: Закон України від 27 квітня 2021 року № 1416-IX URL: https://zakon.rada.gov.ua/laws/show/1416-20#Text .

6. Про внесення змін до деяких законодавчих актів України, спрямованих на забезпечення додаткових соціальних та економічних гарантій у зв’язку з поширенням коронавірусної хвороби (COVID-19): Закон України від 30 березня 2020 року № 540-IX. URL: https://zakon.rada.gov.ua/laws/show/540-20#Text

7. Про затвердження Порядку роботи з технічними засобами відеоконференцзв'язку під час судового засідання в адміністративному, цивільному та господарському процесах за участі сторін поза межами приміщення суду: Наказ Державної судової адміністрації від 8 квітня .2020 року № 169 (втратив чинність) URL: https://zakon.rada.gov.ua/rada/show/v0169750-20#Text .

8. Про затвердження Положення про порядок функціонування окремих підсистем Єдиної судової інформаційно-телекомунікаційної системи: Рішення Вищої ради правосуддя

від 17 серпня 2021 року № 1845/0/15-21. URL: https://zakon.rada.gov.ua/rada/show/v1845910-21#Text.

9. Про затвердження Інструкції щодо роботи з технічними засобами фіксування судового засідання: наказ Державної судової адміністрації України від 06 червня 2022 року № 156. URL: https://zakon.rada.gov.ua/rada/show/v0156750-22#Text .

10. Господарський процесуальний кодекс України (чинна редакція). URL: https://zakon.rada.gov.ua/laws/show/1798-12#Text

## ЦИФРОВА ТРАНСФОРМАЦІЯ СУДОВОГО ПРОЦЕСУ В УМОВАХ ВОЄННОГО СТАНУ

***Б.С. Дехтяр,***
аспірант кафедри права,
ПВНЗ «Європейський університет»

Цифрова трансформація сьогодні активно проводиться не тільки в економіці, менеджменті та бізнесі, а також стрімко розвивається в судовій системі України. Особливе значення, згадані процеси набувають в екстремальних умовах таких, як пандемія або воєнний стан. На сьогодні найбільш затребуваною цифровою системою в українському судочинстві є підсистема «Електронний суд».

Електронний суд – підсистема Єдиної судової інформаційно-телекомунікаційної системи (далі ЄСІТС), що забезпечує можливість користувачам у передбачених законодавством випадках відповідно до наявних технічних можливостей підсистеми ЄСІТС реалізованого функціоналу створювати та надсилати в електронному вигляді процесуальні чи інші документи до суду, інших органів та установ у системі правосуддя, а також отримувати інформацію про стан і результати розгляду таких документів чи інші документи [1].

24.02.2022 Указом Президента України № 64/2022 «Про введення воєнного стану в Україні» в Україні введено воєнний стан, який досі триває [2].

Так, запроваджений 24 лютого 2022 року воєнний стан кардинально змінив повсякденне життя українців. Він вплинув на всі сфери життя та інституції в країні.

У період воєнного стану, відповідно до статті 12-2 Закону України «Про правовий режим воєнного стану» повноваження судів, органів та установ системи правосуддя, передбачені Конституцією України, в умовах правового режиму воєнного стану не можуть бути обмежені. Конституційне право кожного на судовий захист є непорушним, навіть в умовах війни [3].

Проте воєнний стан також вплинув і на судову гілку влади, в результаті чого набуло особливої актуальності застосування підсистеми «Електронний суд».

Так велика кількість громадян, які були вимушені покинути власні домівки та переїхати у більш

безпечні регіони країни, або за кордон зіткнулися з неможливістю фізичного доступу до конкретного суду на території тих населених пунктів де вони проживали. Саме в таких ситуаціях прийшла на допомогу учасникам

судового процесу запроваджена підсистема «Електронний суд».

Ця підсистема включає в себе цілий ряд незамінних функцій, які доречно продемонструвати у вигляді таблиці 1.

| № | Вид переваги | Опис функцій |
|---|---|---|
| 1 | Швидкість обміну електронними документами між судом та учасниками судового процесу | Можливість надсилання документів до суду та інших учасників процесу, які безпосередньо зареєстровані в «Електронному суді» онлайн, у будь який час.<br>Не потрібно йти до суду чи пошти для відправки документів по справі. |
| 2 | Можливість обмінюватися із судом документами онлайн | сплачувати судовий збір<br>отримувати повідомлення про справи в яких особа є учасником процесу<br>відстежувати процесуальні дії свого представника в суді<br>мониторити перебіг справи<br>знайомитися із матеріалами справи<br>отримувати рішення, повістки й інші документи. |
| 3 | Знижена ставка судового збору | відповідно до ч. 3 ст. 4 ЗУ «Про судовий збір» передбачено, при поданні до суду процесуальних документів, передбачених частиною другою цієї статті, в електронній формі - застосовується коефіцієнт 0,8 для пониження відповідного розміру ставки судового збору [4].<br>Якщо учасник судового процесу, подасть процесуальні документи в електронній формі, то в цьому випадку сплата судового збору буде знижена. |
| 4 | Можливість брати участь у розгляді справи дистанційно шляхом проведення відеоконференції із застосування ресурсів "Електронного суду" | після авторизації в підсистемі відеоконференцзв’язку, учасник справи може взяти участь у судовому засіданні онлайн, навіть перебуваючи за кордоном наприклад за допомогою власного смартфону. |

**Таблиця. 1 Переваги застосування Електронного суду**

Джерело: складено автором за [1,4].

Отже, як вбачається з вищевикладеного, застосування підсистеми «Електронний суд» у деяких випадках є єдиним можливим способом повноцінно взаємодіяти з відповідним судом та безпосередньо брати участь у судових засіданнях онлайн.

Однак, функції підсистеми «Електронний суд» і надалі можливо вдосконалювати, в тому числі покращити взаємодію з іншими державними

установами та відповідними реєстрами, для зменшення використання паперового документообігу та переведення його у цифровий формат. Що надасть неоцінену зручність та швидкість для громадян в отриманні необхідних процесуальних документів, довідок та іншої необхідної інформації. З боку держави це матиме позитивний ефект у суттєвому знижені видатків державного бюджету, зменшення впливу бюрократичних механізмів та в цілому підвищить авторитет державних органів серед населення.

*Список використаних джерел*

1. Положення про порядок функціонування окремих підсистем (модулів) Єдиної судової інформаційно-телекомунікаційної системи, затверджене рішенням Вищої ради правосуддя 17 серпня 2021 року №1845/0/15-21//Режим доступу:https://zakon.rada.gov.ua/rada

2. Закон України «Про судовий збір» //Режим доступу: https://zakon.rada.gov.ua/laws/show/3674-17#Text

3. Закон України «Про правовий режим воєнного стану»//Режим доступу: https://zakon.rada.gov.ua/laws/show/389-19#Text

4. Указ Президента України № 64/2022 «Про введення воєнного стану в Україні»//Режим доступу: https://www.president.gov.ua/documents/642022-41397

## МЕДІАЦІЯ У БІЗНЕСІ ЧЕРЕЗ ПРИЗМУ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

***А.В. Жила,***
аспірант,
ПВНЗ «Європейський університет»

У цілому двадцять перше століття можна охарактеризувати як час розквіту Інтернету та засобів дистанційної комунікації. Завдяки цьому людство отримало змогу краще обмінюватися інформацією, швидший доступ до знань та можливість більше спілкуватися. Інтернет та мобільний зв'язок охопили всі сфери людського життя. Час, який проводить в середньому людина в Інтернеті дуже варіюється залежно від країни та рівня доступу до нього, проте це завжди декілька годин. Тому не дивно, що поступово бізнес та економіка взяли собі на озброєння можливості сучасних комунікацій при веденні ділової кореспонденції, зустрічей з клієнтами чи керівниками, командної взаємодії всередині компанії тощо. І, безумовно, ця форма взаємодії вже довела свою практичну цінність. Але, чи є вона корисною та такою, яку можна застосовувати при проведенні медіації між контрагентами, де має місце спір та невдоволення сторонами один одним, коли емоційний фактор виступає одним з наріжних, який, як здається на перший погляд, важко передати у режимі онлайн? [1].

Впродовж багатьох десятиліть, починаючи від зародків медіації, особа, яка керувала цим процесом, завжди мала прямий емоційний контакт зі сторонами конфлікту як під час приватних бесід, так і під час спільного обговорення проблеми. Це давало змогу досвідченому медіатору дізнатися більше про емоційний стан людини, поставити їй правильні запитання, щоб виявити повною мірою суть невдоволення однієї та іншої сторони, та разом знайти шлях їх усунення. Такий спосіб ведення медіації на сьогодні є більш розповсюдженим,

адже містить низку переваг, пов’язаних передусім з особистим контактом між медіатором і сторонами [2].

Але, початок пандемії COVID-19 вплинув на розвиток медіації дуже сильно, а саме повністю перевівши її у цифровий формат. Деякий час, коли авіа- та залізничне сполучення між містами та країнами було скасоване, бізнес переживав не найкращий період. Порушення логістичних ланцюгів, невиконання договорів поставок, банкрутство компаній і таке інше. Усе це у період з 2020 по 2021 рік викликало велику кількість претензій, які господарські товариства мали один до одного, а неможливість особистих зустрічей та пошуку шляхів вирішення лише посилювали це невдоволення. Проте, так само швидко як клієнтоорієнтований бізнес знаходить рішення, так само швидко і медіатори знайшли спосіб пристосуватися до нових реалії ведення перемовин та вирішення спорів контрагентів перебуваючи за тисячі кілометрів від них. Ці методи застосовувались вже тоді, коли пік пандемії вщух та сполучення між регіонами та країнами відновилось. Тому можна стверджувати, що з’явився новий підвид медіації так звана – «цифрова медіація».

Наразі, хоч ми і маємо вже іншу безпекову ситуацію з пандемією, залишається інша загроза, а саме вторгнення російської федерації в Україну, що також часто унеможливлює особисті зустрічі власників бізнесу та медіатора задля вирішення спору в силу різних причин. Звісно, всі ми знаємо, що скоро агресора буде подолано та ми повернемося до звичного способу ведення бізнесу та життя, проте способи, які були напрацьовані у ці періоди будуть актуальними, адже вони дозволяють домовлятися швидко та ефективно знаходячись у будь-якій точці світу. Це все разом з самим процесом медіації (власне для чого вона і була створена) економить купу часу та ресурсів власникам бізнесу, дозволяючи їх приділяти на розвиток своїх компаній та економік країн в цілому.

Розглянемо інструменти та методи спілкування при вирішенні спорів, які набули поширення останнім часом під час вирішення спірних ситуацій:

1) Інтернет листування зі сторонами. Для цього використовуються будь-які зручні сервіси електронної пошти, починаючи від Gmail до Mailbox.org. та безлічі інших. Оскільки мова йде про роботу з документами, які, як правило, не є публічними та становлять комерційну таємницю, то важливо мати захищений акаунт, щоб запобігти його злому зловмисниками. Такий тип листування дуже ефективний, адже дозволяє пересилати листи, документи дуже швидко по всьому світу.

2) Онлайн-зустрічі через платформи Zoom, Google-Meet, Microsoft teams та інші. Куди ж без особистих зустрічей, навіть якщо вони через Інтернет. Зустріч варто проводити як з кожною стороною конфлікту окремо, так і безпосередньо з усіма разом. Як довела практика проведення таких зустрічей, вони є досить продуктивними та корисними, якщо дотримуватися таких вимог: чіткий таймінг, попередня ознайомленість з питаннями розгляду кожної зі сторін, наявність конкретних пропозицій кожної зі сторін (часто варто проговорити з кожною окремо), націленість на результат та позитивний настрій.

3) Месенджери. В залежності від країни контрагентів чи одного з контрагента і обирається месенджер для спілкування. Якщо це представники країн Південно-Східної Азії, то часто це WeChat, якщо країн Європи чи США, то

WhatsApp, а якщо України чи інших країн Східної Європи та Середньої Азії, то, як правило, це Telegram. Основна роль месенджерів – це швидка комунікація медіатора зі сторонами, пересилання коротких повідомлень, нагадувань про підписання тих чи інших документів, виконання дій, надсилання відео та фото файлів. Проте, тут також варто слідувати за питаннями безпеки від зломів особистих даних.

4) Телефонні дзвінки. Якщо питання, яке медіатор чи сторона хоче обговорити досить вузьке та не потребує довгого діалогу, то можна його обговорити телефоном. Це зручно, швидко та економить час сторін. Також це підвищує довіру сторін одна до одної, адже чути голос іншої людини.

5) Методичність. Коли медіатор починає вести справу і він розуміє, що вона, скоріше за все, пройде онлайн, він має скласти план робити – визначити дати зустрічей, листування та дзвінків. Звичайно, вони можуть варіюватися та доповнюватися особистими зустрічами і спілкуванням у месенджері тощо. Але певне уявлення про хід переговорів у гарного медіатора має бути. І коли проєкт повністю диджиталізований, то ця актуальність висока як ніколи.

З власного досвіду можемо сказати, що медіація досить вдало пройшла цифрову трансформацію не тільки не втративши своєї ефективності, а навпаки – отримавши нові інструменти ефективного вирішення спорів. Наразі, значна кількість спорів вирішується через цифрові засоби, навіть якщо контрагенти знаходяться фактично в одному місті. Тому у цифровій медіації є майбутнє через її практичність, економність та високу ефективність. У зв'язку з цим у майбутньому гарний медіатор буде повинен мати не лише базові навички такі, як відповідна освіта та практичний досвід, але й ґрунтовні знання Інтернету та девайсів, їхніх переваг тощо.

*Список використаних джерел*

1. Шпилик С. В. Інтернет як ефективний маркетинговий інструмент сучасного підприємства. Галицький економічний вісник. 2015. Том 49. № 2. С. 212-223.

2. Кохан Г. Чи потрібна медіація Україні? Юридичний радник. 2014. № 2(74).

3. Єрьоменко Г. Перспективи розвитку медіації в Україні. URL: http://ukrmediation.com.ua/files/content/Perspectyvy.pdf.

## ЦИФРОВА ТРАНСФОРМАЦІЯ БІЗНЕСУ

***Д.Л. Здор,***
магістрант факультету інформаційних систем та технологій,
***О.Ю. Ніколаєвський***,
к.т.н., доцент кафедри інформаційних систем,
програмування та кібербезпеки,
ПВНЗ "Європейський університет"

Експерти прогнозують, що протягом наступних п'яти років обов'язковими атрибутами успішних підприємств стануть проєктно-орієнтовані бізнес-підходи та рішення, використання машинного навчання та штучного інтелекту, а також сучасні методи комунікації та постійне відстеження ефективності роботи

працівників. Здатність швидко змінюватися в умовах постійної цифровізації є ключовою конкурентною перевагою, яку слід враховувати.

Універсального способу цифровізації не існує. Кожна компанія накопичує дані по-різному, використовує різні технології в роботі та робить ставку на певні навички своїх співробітників. Але є й загальні рекомендації, які стосуються будь-якої трансформації бізнесу.

Потрібно створити команду трансформації в яку, як правило, обов'язково входять керівник компанії, директор з персоналу і керівник IT-департаменту або технічний директор, а також інші представники топ-менеджменту. Вони повинні працювати разом над серйозною підготовкою, інакше будь-яка ініціатива по змінам буде марною.

Основна мета будь-якої трансформації – підвищити ефективність роботи компанії. Але кожен визначає її по-різному, тому команді з топ-менеджменту потрібно дійти єдиної думки щодо подальшого розвитку бізнесу. Інколи доводиться формулювати з нуля або коригувати місію, візію, стратегію і цінності компанії, а також вибудовувати нову культуру взаємодії працівників один з одним і з клієнтами з урахуванням як ринкового, так і внутрішнього контексту.

Багато компаній, зазвичай, починають з автоматизації, тому що це закладає фундамент для подальшої еволюції. Це автоматизація продажів, виробництва, фінансових процесів, документообігу та інше. Для цього доступні різні рішення – від хмарних технологій до спеціального програмного забезпечення, призначеного для управління діяльністю підприємства (ERP).

Проте навіть найкраща модель цифрової трансформації не дасть результатів, якщо всі етапи та зв’язки не синхронізовані. Тобто плани є, зміни відбуваються, але керівництво компанії та власники не розуміють, як це все має взаємодіяти. Тому важливо постійно тестувати та оптимізувати IT-архітектуру та бізнес-процеси, щоб виявляти проблемні місця та вчасно їх усувати. Адже якщо відділ продажів не «стикується» зі складом, будуть явні проблеми з відправленнями. Або якщо виробнича частина буде жити своїм життям, рано чи пізно з’являться претензії до якості продукту.

Цифрова трансформація – це нескінченні зміни. Автоматизувати той чи інший процес, і забути про нього стане неможливо. По суті, компанія змінює бізнес-модель, корпоративну культуру і переходить на новий рівень. Але при цьому вона постійно вдосконалюється і розвивається. Крім того, в ідеалі має бути створений окремий підрозділ для моніторингу та контролю всіх процесів, пов’язаних із трансформацією та життєдіяльністю «цифрових» організмів, аналізу результатів та постійного розвитку технічних компонентів. Тільки так цифровізація та все, що з нею пов’язано, стане корпоративною культурою, щоб компанії могли легко та швидко реагувати на виклики ринку та повністю відповідати вимогам клієнтів.

*Список використаних джерел*

1. Цифрова трансформація: чому вона необхідна кожній компанії. URL: https://mind.ua/publications/20229223-cifrova-transformaciya-chomu-vona-neobhidna-kozhnij-kompaniyi#three

2. Як цифрова трансформація змінює бізнес. URL: https://devisu.ua/uk/stattia/yak-cifrova-transformaciya-zminyu-biznes

# РОЗРОБКА ЦИФРОВОГО СЕРВІСУ ДЛЯ СТВОРЕННЯ СТАРТАПУ

***Я.О. Колодінська,***
***О. І. Панченко,***
магістранти факультету інформаційних систем та технологій,
ПВНЗ «Європейський університет»

Через сучасні виклики, пов'язані спочатку з пандемію Covid-19, а потім – з повномасштабним вторгненням російської федерації в Україну у лютому 2022 року економіка нашої країни зазнала величезних збитків та втрат. Однак, незважаючи на військову агресію росії, український бізнес рішуче продовжує працювати, передбачати та використовувати альтернативні можливості, щоденно демонструючи свою спроможність трансформуватися та адаптуватися до нової реальності та викликів. На сьогоднішній день країна розпочинає свій шлях до територіальної реконструкції. Водночас, українські технологічні компанії, стартапи та інновації відіграють важливу роль у посиленні опору і відновленні повоєнної економіки.

Попри надскладний період українські стартапи продовжують розвиватись. З лютого 2022 року в Україні було зареєстровано більше 51 000 нових компаній [1]. Більшість українських стартапів планують розширити свою діяльність у найближчі терміни [2]. Розвиток підприємництва, насамперед, інноваційного – це спосіб для українців знайти рішення нагальних проблем та допомогти країні у відновленні. Таким чином, можна з упевненістю сказати, що на сьогодні стартап-рух залишається актуальним та продовжує активно розвиватись.

Кожен стартап-проєкт неминуче проходить такі основні етапи розвитку, як: формування команди, визначення місії, візії та цінностей, пошук проблеми, генерація ідей, валідація цільової аудиторії, проєктування Minimum Viable Product (MVP) – мінімально життєздатного продукту, тестування гіпотез задля виявлення слабких та сильних сторін та подальшого становлення бізнес-компанії. Більшість зазначених стадій формування стартапу потребують заповнення різних template'ів (шаблонів) для візуалізації результатів та опанування нових інтерфейсів, що значно ускладнює процес розробки стартапу та демотивує команду. Тому для стартапів на ранніх стадіях авторами запропоновано ідею створення єдиного універсального мобільного застосунку – Startup Service. Задум авторів полягає у поєднанні усіх необхідних розробникам стартапів інструментів, шаблонів (таких, як Empathy map, Business model canvas, Value proposition canvas, User Persona, Landing page constructor та інших) в одному програмному продукті, що значно полегшить створення і розвиток ідеї, її тестування та представлення потенційним інвесторам. Також сервіс передбачає наявність засобів комунікації і менеджменту задач, необхідних для командної роботи.

Авторами було створено мінімально життєздатний продукт (MVP) цифрового сервісу для перевірки гіпотез на потенційних споживачах. Логіка проєктування софту наступна. Функціонал продукту реалізовано на CMS WordPress, щоб поєднати важливі частини, а саме: чат для взаємодії між

учасниками команди стартапу та можливість заповнювати і передавати вбудовані шаблони бізнес-ідей. В проєкті використовувались такі технології, як HTML та JavaScript для створення візуальної складової та PHP для реалізації внутрішніх компонентів. Також була створена база даних для зберігання файлів шаблонів. JavaScript було використано для написання функцій роботи з інтерфейсом і зв'язку з серверною частиною, а PHP – для обробки отриманих даних і взаємодії з базою даних.

Отже, запропонований авторами цифровий сервіс має на меті значно спростити молодому бізнесу і стартапам процеси створення, проєктування, тестування і запуску інноваційних ідей та проєктів. Розроблений авторами застосунок надає можливості працювати стартаперам спільно командою в одному уніфікованому застосунку, в якому акумульовано всі необхідні форми і шаблони для формування і старту бізнесу, його валідації, монетизації та зібрано інструменти для візуалізації, обговорення, тощо, що надає сучасні цифрові можливості додаткового розвитку і реалізації бізнес-проєктів.

*Список використаних джерел*

1. Стан українських стартапів під час війни: поради, гранти, тенденції. URL: https://hub.kyivstar.ua/news/stan-ukrayinskyh-startapiv-pid-chas-vijny-porady-granty-tendencziyi/

2. *Прес-офіс Міністерства та Комітету цифрової трансформації* Дослідили, як повномасштабна війна вплинула на українські стартапи. URL: https://thedigital.gov.ua/news/doslidili-yak-povnomasshtabna-viyna-vplinula-na-ukrainski-startapi

## ВПЛИВ ВІЙНИ НА ІТ-РИНОК УКРАЇНИ

***В.С. Красьоха,***
***Д.М. Гаврилюк,***
магістранти факультету
інформаційних систем і технологій,
ПВНЗ «Європейський університет»

Повномасштабне російське вторгнення в Україну 2022 року стало великим випробуванням для вітчизняного ІТ-ринку. У сучасному світі жодна країна не стикалася з такими перешкодами, котрі змогли подолати українські ІТ-компанії: мобілізація працівників, вимушений переїзд підприємств, складна економічна ситуація, можливий блекаут. Та навіть у такі складні часи ІТ-компанії продовжують функціонувати, сплачувати зарплатні робітникам та податки, тим самим, підтримуючи державу, її економіку та Збройні сили України.

Починаючи з 24 лютого 2022 року ІТ-компанії роблять все можливе, щоб гарантувати безпеку для працівників, налагодити робочий процес та довести, що ІТ-ринок України здатний функціонувати на всі 100% навіть під час війни. Багато компаній завчасно перед війною завдяки розвідці та інформації про можливий наступ рекомендували та навіть організовували переїзди для робітників у більш безпечні області країни та навіть за кордон. Команди готувались до війни, хоч і не хотіли в це вірити: продумували подальші дії, організовували можливі перевезення та евакуацію. Це дало змогу швидко організувати переїзд робітників

та офісного обладнання в безпечні місця в перші дні війни. Також компанії допомагали шукати місця проживання чи винаймали готелі, апартаменти для своїх працівників та їхніх родин, компенсували витрати на вимушену релокацію. Уже з перших тижнів війни ІТ продовжило працювати в довоєнному ритмі.

Попри війну ІТ-компанії зберегли 85% замовників та продовжували нарощувати експорт. Так, протягом першого кварталу цього року, ІТ-індустрія України встигла стати одним з найбільших експортерів ІТ-послуг в Європі [1].

За підсумками десяти місяців 2022 року ІТ-галузь принесла в економіку України 6 млрд дол. США експортного виторгу та зросла на 10% порівняно з попереднім роком. За прогнозами дослідників, до кінця року індустрія згенерує 7,1 млрд до США та 2,2% зростання обсягу експорту відносно 2021 р. [2]

Таким чином, ми бачимо, що українська ІТ-індустрія продовжує не тільки функціонувати, а й розвивається та знаходить нові шляхи виходу на європейський ринок. На сьогоднішній день Україна входить до лідерів ринку аутсорсингу у світі.

Отже, незважаючи на виклики, ІТ-індустрія продемонструвала феноменальну стійкість та гнучкість, навіть, у воєнний час. На думку авторів, найближчим часом інвестиції в українські стартапи, компанії та співпраця з українськими розробниками будуть типовими явищами, адже увесь світ бачить незламність українців та українського бізнесу.

*Список використаних джерел*

Українські айтівці: війна внесла певні корективи у роботу галузі: https://broadcast.net.ua/ru/tech-articles/6531-ukrainski-aitivtsi-viina-vnesla-pevni-korektyvy-u-robotu-haluzi

Як ІТ-індустрія розвиває інші галузі економіки у 2022 році: https://finance.ua/ua/goodtoknow/jak-it-industrija-rozvyvae-inshi-galuzi-ekonomiky

## ВПЛИВ ДИСТАНЦІЙНОГО РЕЖИМУ РОБОТИ НА ЕКОНОМІЧНУ БЕЗПЕКУ ПІДПРИЄМСТВА

***С.С. Курінний,***
аспірант,
ПВНЗ “Європейський університет”

Події останніх років суттєво змінили підхід до організації робочого процесу. Через COVID-19, а також повномасштабну війну на території України, багато національних та міжнародних компаній були змушені перейти від стандартного до віддаленого режиму роботи. Ще на етапі впровадження нововведень виникало безліч дискусій між скептиками та прихильниками таких змін, оскільки ефективність дистанційної зайнятості було важко спрогнозувати.

Перш за все, керівників бізнес-структур хвилював менталітет українців, відсутність навичок самоорганізації, потреба у освоєнні певних програм, а також соціальна напруженість. Все це могло перешкодити досягненню бажаних результатів. Проте вселяв оптимізм та надію високий рівень відповідальності українців, освіченості та здатності до адаптації.

Мета роботи: оцінити ефективність дистанційної форми організації праці, виявити сильні та слабкі сторони, а також потенційні можливості та загрози; довести або спростувати вплив форми трудової діяльності на фінансові показники підприємства; визначити доцільність збереження дистанційної роботи по завершенню бойових дій на території України та подоланню COVID-19.

Методи збору первинної інформації: опитування, аналіз статистичних показників, спостереження, експеримент. Дослідження проводилося на базі підрозділу українського підприємства, основним напрямком якого є рекламна діяльність (штат – копірайтери та дизайнери – представники творчих спеціальностей).

За результатами дослідження, об'єктом якого є ефективність впровадження дистанційного режиму роботи, встановлено, що за 12 місяців онлайн-зайнятості обсяг виконаної роботи співробітниками підрозділу збільшився на 130 %, показник якості реалізованих проєктів зріс на 125 %. Прибутковість підрозділу також показала позитивну динаміку та на кінець року склала 142 %. При цьому, за результатами опитування, покращилося і відношення співробітників до компанії.

До переваг віддаленого режиму роботи доцільно віднести економію часу, сил та матеріальних ресурсів на щоденні поїздки до офісу та додому, можливість абстрагуватися від сторонніх подразників (розмови колег, гучна музика), вдосконалити навички планування та знизити рівень стресу. Окрім того, таке нововведення дозволяє зменшити витрати на утримання кабінетів та оплату праці обслуговуючого персоналу.

Як свідчать результати опитування, завдяки впровадженню дистанційного режиму роботи створено більш комфортні умови для праці, за рахунок чого плинність кадрів наблизилася до нульової позначки, що позитивно позначилося на кадровій та економічній безпеці підприємства, а також дозволило мінімізувати бюджет на пошук та адаптацію нових співробітників. Мобільність та свобода, які відчули представники підрозділу, стали передумовою для розвитку креативного мислення та розкриття творчого потенціалу.

Однак досягнення більш високих результатів відбувалося також і за рахунок збільшення тривалості робочого дня – переробітку за власною ініціативою співробітників, а також прагнення покращити індивідуальні показники, нехтуючи загальними принципами командної співпраці.

Наразі дистанційний режим роботи відкриває безліч можливостей як для найманого співробітника, так і для власника бізнесу. Наприклад, дозволяє розширити штат та сферу діяльності підприємства за рахунок залучення компетентних кадрів зі всього світу, надає можливість професійної самореалізації попри будь-які життєві обставини, допомагає створити більш безпечні умови праці під час дії воєнного стану.

Попри всі описані переваги дистанційна робота містить і безліч загроз, до яких можна віднести втрату «командного духу», простої через вихід з ладу техніки, відключення електроенергії чи відсутність доступу до Інтернет. Також приводом для хвилювання може бути збільшення ризику витоку конфіденційної інформації, необхідність додаткового контролю найманих співробітників.

Таким чином, запровадження дистанційного режиму роботи позначається

позитивно на діяльності підприємства за умови, що всі бізнес-процеси професійно налаштовані, програмне забезпечення використовується ефективно, впроваджено дієвий механізм організації, мотивації та контролю співробітників. Маючи більше простору та свободи для творчості представники креативних професій (копірайтери, дизайнери) показують кращі результати роботи як у кількісному, так і у якісному вираженні, збільшуючи прибутковість бізнесу.

Проте, наразі дистанційна робота створює певні загрози для підприємства, які спровоковані збільшенням ризику розповсюдження конфіденційної інформації та аварійним відключенням електроенергії. Тому потрібно більше уваги приділяти плануванню, захисту даних та забезпеченню ключових співробітників елементами безперебійного живлення. Окрім того, для підтримки командного духу доцільно проводити корпоративні заходи, направленні на згуртування колективу.

## ПРИЙОМИ ТА МЕТОДИ УПРАВЛІННЯ РИЗИКАМИ НА ПІДПРИЄМСТВІ

***Я. Ю. Левцун,***
магістрант факультету економіки та менеджменту,
ПВНЗ «Європейський університет»

Антикризове управління у значній частині вирішуваних проблем є ризиковим. У кризових ситуаціях виникає безліч ризиків різноманітних за змістом, джерелом прояву, величиною ймовірності та розміром можливих втрат та негативних наслідків для бізнесу. Усе це зумовлює потребу створення системи управління ризиком. Вплив фактора ризику не можна уникнути повністю, але треба постійно прагнути знижувати його рівень до мінімального значення.

Таким чином, управління ризиками повинне мати своєю базою антикризове управління, націлене на зміцнення становища підприємства на ринку, забезпечення його стабільності та сприятливоїперспективи. Після ідентифікації та оцінки ризиків підприємницького проєкту керівник, що приймає рішення, має визначитися з приводу відхилення бізнес-проєкту або його подальшої розробки.

Завдання зниження ризику бізнес-проєкту ставиться як завдання визначення необхідних коригувань в організації проєкту, що не стосуються можливості загальної мети проєкту, але підвищують його стійкість до впливу різних кризових ситуацій. При вирішенні цього завдання виходять з таких основних передумов: певний рівень ризику існує в кожній з сфер діяльності, пов'язаної з управлінням проєктом; зниження (зменшення) ризику в цих областях, пов'язані з певними витратами. Підприємство має визначитись з політикою, орієнтованою на зниження ризику, виходячи з адекватності співвідношення граничних витрат на її реалізацію та корисності застосовуваних заходів.

В залежності від видів ризиків можуть бути застосовані різні заходи. Такі, наприклад, як заходи превенції, посилення контролю, диверсифікації ланцюгів постачання та логістики, портфелю клієнтів, тощо.

Працівник (структурний підрозділ) підприємства, відповідальний за напрямок управління ризиками, має проаналізувати можливі варіанти та сформувати ті, які є найбільш прийнятними для підприємства з урахуванням всіх аспектів наявної ситуації. Завершальним етапом в аналізі засобів зниження ризику є формулювання загального плану управління ризиком бізнес-проєкту. Цей план має включати: результати ідентифікації всіх областей ризику проєкту, перелік основних ідентифікаторів ризику кожної області; результати рейтингової оцінки індикаторів ризику, що відображають їхню значущість для досягнення цілей проєкту; результати статистичного аналізу ризику, аналізу чутливості та глобального аналізу ризику прийняття проєкту; рекомендовані стратегії зниження ризику у кожній сфері діяльності, пов'язаної з реалізацією проєкту; перелік процедур, які забезпечують моніторинг ризиків підприємницького проєкту.

Виникнення ризик-менеджменту як нової філософії стратегічного управління підприємницькими ризиками було викликано дією цілого ряду факторів та тенденцій, які радикально змінили підходи до управління ризиками. До них, зокрема, належать: глобалізація світової економіки; зростання ролі та значення фінансових ринків; вимоги регулюючих органів; інформаційно-технологічний розвиток тощо [2].

Ступінь ризику не завжди необхідно знижувати. Іноді ризик потрібно оптимізувати чи навіть прийняти. Перед прийняттям рішення необхідно провести аналіз усіх можливостей та загроз зовнішнього середовища, сильних та слабких сторін самого підприємства, оскільки при здійсненні ризик-менеджменту будь-яке рішення має бути обґрунтованим.

Організація процесу ризик-менеджменту включає такі кроки:

1. Визначення мети ризику та мети ризикових вкладень капіталу.
2. Отримання інформації про навколишню обстановку, яка необхідна для ухвалення рішення.
3. На основі наявної інформації про навколишнє середовище, ймовірність, ступінь та величину ризику розробляються різні варіанти ризикованого вкладення капіталу [2].
4. Вибір стратегії та прийомів управління ризиком, а також способи зниження рівня ризику.
5. Розробка програми зниження ризику.
6. Організація заходів щодо виконання наміченої програми дії.
7. Контроль за виконанням наміченої програми, аналіз та оцінка результатів обраного варіанта ризикованого рішення. Для результативного виконання вищевказаних кроків на господарському суб’єкті створюються органи управління ризиком.

Слід звернути увагу, що орган управління ризиками повинен бути дієвим, і не лише займатись теоретичними розробками час від часу. В складних кризових умовах та нестабільній ситуації підприємство потребує винятково ефективного планування, організації та контролю, що можливо зробити за допомогою створення чіткої ієрархічної структури управління ризиками, яка повинна функціонувати на системній основі.

Переваги ризик-менеджменту полягають у тому, що він:

- є основою для підвищення ефективності стратегічного планування;
- дозволяє уникати вартісних несподіванок;
- покращує ефективність діяльності підприємства;
- дозволяє оптимально використовувати ресурси;
- сприяє більшій відкритості діяльності керівництва та покращує комунікації;
- забезпечує вище керівництво коротким оглядом головних ризиків, а також відомостями про ресурси, виділені для впливу на високі ризики;
- дає менеджерам ефективну та послідовну методологію вивчення ризиків;
- орієнтує топ-менеджмент на використання факторів ризик-можливостей для підвищення вартості підприємства [3].

Недоліки у сфері ризик-менеджменту:

- часто ключові рішення приймаються однією людиною, що суттєво підвищує ймовірність виникнення суб'єктивних помилок та генерації екстремальних неконтрольованих ризиків;
- часто спеціалізований підрозділ ризик-менеджменту не створюється, це означає, що рівень ризику відстежується лише час від часу [1].

Виходячи з усього вищевикладеного, можна зробити висновок про те, що механізм управління ризиками підприємства в сучасних умовах господарювання повинен мати чітку ієрархічну структуру з необхідністю її коригування за підсумками реалізації програм заходів щодо зниження ризиків та з урахуванням факторів впливу, що змінюються. При цьому така структура повинна в своїй діяльності застосовувати існуючі підходи та методи ризик-менеджменту в науковому спектрі та практичній площині.

*Список використаних джерел*

1. Кузьмін А.Є. Управління ризиками в інноваційній діяльності: [навчально – метод. посібник]. Львів: Вид-во Нац. ун-ту "Львівська політехніка", 2019. 176 с.
2. Лук'янова В.В. Економічний ризик: навч. посіб. Київ: Академвідіван, 2019. 462 с.
3. Прохорова В.В. Управління економічною безпекою підприємств: монографія /за ред. В.В. Прохорова, Ю.В. Прохорова, О.О. Кучеренко. Харків: УКР ДАЗТ, 2010. 282 с.

## СТРАТЕГІЧНИЙ ВПЛИВ ІТ-ГАЛУЗІ НА СТАБІЛІЗАЦІЮ ЕКОНОМІКИ УКРАЇНИ У ВОЄННИЙ ТА ПІСЛЯВОЄННИЙ ПЕРІОДИ

***А.М. Ліщинський,***
аспірант,
ПВНЗ “Європейський університет”

Повномасштабна війна на території України завдала значних та непоправних втрат в усіх галузях економіки країни. Експортні галузі змушені функціонувати в несприятливих умовах, проте саме ІТ-галузь стабільно здійснює свою діяльність, значно підтримує економіку держави та володіє потенціалом щодо швидкого відновлення свого росту у післявоєнний період. ІТ-сфера є менш залежною від географічних та ресурсних умов з акцентом на

людський потенціал, що має можливість здійснювати свою діяльність у дистанційному форматі. Саме тому під час воєнного стану в Україні, мобілізаційних процесів, вимушеній релокації бізнесів та команд, ІТ-галузь є більш гнучкою та пристосованою до нових реалій.

Упродовж десятиліття, ІТ-галузь в Україні стрімко розвивалась, незважаючи на дестабілізуючі впливи на економіку країни (рис.1).

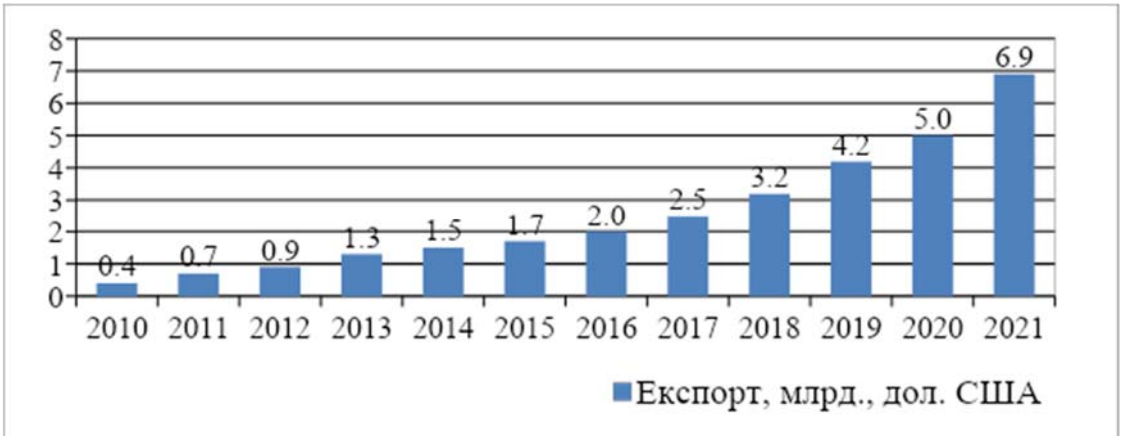



**Рис. 1. Аналіз обсягу українського експорту ІТ-послуг за період 2010-2021 рр. [2].**

Обсяг експорту комп'ютерних послуг за перше півріччя 2022 року становив 3,74 млрд. доларів США, що на 23% більше, ніж за перше півріччя 2021 року, а вітчизняні технологічні компанії та бізнеси-початківці залучили за аналогічний період близько 350 млн. доларів США для розвитку ІТ-сектору України [1].

Дестабілізуючими чинниками, які впливають на діяльність та розвиток ІТ-галузі та відповідно економіки країни під час воєнного стану є:

1. Зменшення притоку інвестицій зі сторони іноземних партнерів.
2. Скорочення кількості робочих місць у зв'язку із зменшенням фінансування компаній з однієї сторони, та мобілізаційними процесами у країні – з іншої.
3. Зменшення податкових надходження до бюджету ІТ-спеціалістами.
4. Криза у локальних ІТ-компаніях, пов'язана із зниженням попиту, розірваними зв'язками у логістичній системі, перебоями у енергетичній системі та інші проблеми на внутрішньому ринку.
5. Значні руйнування у телекомунікаційному та цифровому секторі.

Війна в країні та активні бойові дії здійснюють масштабний вплив на ІТ-галузь, як одну з основних ланок економіки України. Саме тому необхідна першочергова підтримка зі сторони іноземних партнерів та самої держави. Зокрема, зростає необхідність у запровадженні та поглибленні нових цифрових реформ в Україні, побудови тісних інтеграційних зв'язків ІТ-ринку України та Європейського Союзу, залучення стартапів та великих ІТ-компаній до розробки інноваційних планів і рішень стосовно бачення відбудови держави у післявоєнний період, підтримка та фінансування іноземними інвесторами ринку ІТ-послуг України, створення іноземних платформ, конференцій, самітів, де

українські ІТ-спеціалісти матимуть можливість представити власні розробки та ідеї, надання українським вченим та підприємствам доступ до національних та європейських цифрових інфраструктур та ін. Налагодження ефективної співпраці на державному та міжнародному рівнях із засновниками стартапів, розробниками, інвесторами, експертами ІТ-галузі та економіки, дозволить зміцнити соціально-економічний потенціал країни в цілому.

*Список використаних джерел*

1. Мінфін: Обсяг експорту комп'ютерних послуг. URL: https://minfin.com.ua/ua/2022/08/09/90224092/ (дата звернення 08.11.2022.).
2. Опендатабот: Аналітика. URL: https://opendatabot.ua/analytic/ (дата звернення 07.11.2022.).

## ДОСЛІДЖЕННЯ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ ОПТИМІЗАЦІЇ БІЗНЕС-ПРОЦЕСІВ У СФЕРІ ГОТЕЛЬНОГО БІЗНЕСУ

***Ю. В. Майстренко,***
к.е.н., доцент,
доцент кафедри менеджменту та інноваційного провайдингу,
ПВНЗ «Європейський університет»

В умовах глобального розвитку інформаційних технологій і цифровізації економіки відбувається трансформаційне перетворення інтересів і мотивів поведінки економічних суб'єктів у напрямку їх узгодженої взаємодії. Результатом використання інформаційно-комунікаційних технологій є збільшення продуктивності праці за рахунок інформаційної підтримки системи прийняття рішень, що забезпечує економічним суб'єктам додаткові конкурентні переваги. На початку XX століття активне застосування інформаційно-комунікаційних технологій було притаманно лише окремим інноваційним видам діяльності. В свою чергу, епоха цифрової економіки сформувала так звану нову парадигму розвитку, яка охопила всі, без винятку, види економічної діяльності. Найбільш відчутного впливу від розвитку глобального інформатизованого бізнесу зазнала індустрія гостинності, внаслідок чого відбулися змістовні зміни бізнес-процесів. У зв'язку з цим інформаційні тренди стали визначальними факторами розвитку підприємств індустрії гостинності [1].

Виокремлення певних видових груп ІКТ створює підґрунтя для більш поглибленого їх дослідження, зокрема, представляється доцільним визначити, які саме ІКТ використовуються для вдосконалення окремих бізнес-процесів підприємств індустрії гостинності.

З цією метою необхідно провести моніторинг основних бізнес-процесів надання послуг гостинності (рис. 1).

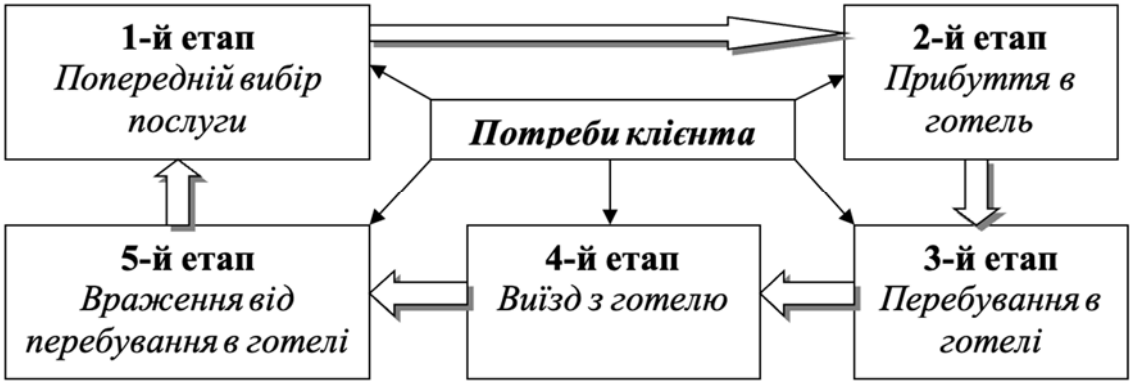



**Рис. 1. Узагальнена схема бізнес-процесів в індустрії гостинності**

**складено за даними* [2]

Процедура надання послуг гостинності складається з п'яти бізнес-процесів та носить циклічний характер. При чому формування кожного бізнес-процесу відбувається на основі урахування потреб клієнта. Якщо клієнти задоволені, то послуга гостинності містить всі етапи, а також носитиме повторювальний характер, в іншому випадку – цикл надання послуг гостинності може бути перервано на будь-якому етапі і готелі втрачають клієнтів. З метою уникнення зазначених негативних наслідків та з урахуванням цифрових трендів розвитку в сфері гостинності активно впроваджують ІКТ на кожному етапі надання послуги. Таким чином, у табл. 1 представляється доцільним розширити схему бізнес-процесів в індустрії гостинності із зазначенням ІКТ, що їх оптимізують.

**Таблиця 1.**
**ІКТ, що оптимізують бізнес-процеси і функції в сфері гостинності**

| Бізнес-процеси | Функції бізнес-процесу | ІКТ оптимізації бізнес-процесу |
|---|---|---|
| 1. Попередній вибір послуги | – Маркетинг і продажі<br>– Бронювання<br>– Клієнтська лояльність | Штучний інтелект, системи бронювання, глобальні системи розподілу, веб-сайти готелів і мобільні додатки, он-лайн туристичні агенції, агрегатори, Google, голосовий пошук і бронювання, готельні системи, інвентар приміщення, прогнозування бронювання, управління доходами і витратами, встановлення тарифів на номери, попередній сервіс, управління відносинами. |
| 2. Прибуття в готель | – Перевірка<br>– Доставка багажу | Системи управління майном, мобільні програми, кіоски самообслуговування, ключі і системи відмикання дверей, роботизовані багажні візки. |
| 3. Перебування в готелі | – Обслуговування гостей<br>– Гостьова кімната<br>– Зручності готелю<br>– Прибирання та | Чат-боти та програми, роботизована доставка, консьєрж, розумні пристрої та Інтернет речей, Системи управління майном, Wi-Fi, розваги в номері, розумні |

| Бізнес-процеси | Функції бізнес-процесу | ІКТ оптимізації бізнес-процесу |
|---|---|---|
| | обслуговування | дзеркала, мобільні програми, системи точок продажу і роботизована доставка, роботи з УФ-обладнанням, технічне обслуговування та інженерія, енергетичний менеджмент, датчики обслуговування, профілактичні датчики. |
| 4. Виїзд з готелю | – Виїзд гостей | Системи управління майном, мобільні програми, самообслуговування, роботизований збір багажу. |
| 5. Враження від перебування в готелі | – Огляд після перебування<br>– Повторний гість | Задоволення гостей, управління іміджем, клієнтська лояльність. |
| Потреби клієнта | х | Системи скрінінгу, навчальні програми та онлайн-ресурси, штатний розклад, біометричний годинник, засоби особистої безпеки, датчики продуктивності. |

**складено за даними* [2, 3]

В якості прикладу представляється доцільним розглянути розвиток конкретного підприємства індустрії гостинності в умовах ефективного використання ІКТ, зокрема KViHotel (Будапешт). KViHotel є повністю комп'ютеризованим і позиціонується як перший «розумний готель» в світі. Реєстрація відбувається через спеціальний додаток, в якому гості самостійно обирають собі номери. При цьому смартфон виконує функції електронного ключа, електронного консьєржа та єдиного пульту управління. В коридорах готелю практично немає персоналу, також відсутня технічна кімната. Під час перебування в готелі спілкування с адміністративним та обслуговуючим персоналом відбувається через будь-який зручний месенджер. Проте, окремі відгуки постояльців KViHotel свідчать про необхідність розвитку «розумних засобів розміщення», що призначені оптимізувати внутрішні бізнес-процеси та підвищити якість послуг. Відсутність досвіду користування зазначеними ІКТ потребує моментальної підтримки, «живого» контакту. Таким чином, для підвищення ефективності в даному готелі важливо зосередитися на персоніфікації користувальницького досвіду, оптимізації бізнес-процесів та створенні зручностей для гостей. Як наслідок, буде створюватися додаткова цінність для клієнтської аудиторії.

В готелі Hilton в Макліні, штат Вірджинія, з'явився новий роботизований консьєрж Connie, який може розповісти гостям про місцеві туристичні визначні пам'ятки, рекомендації ресторанів, можливості готелю та зручності, а також покращити свої рекомендації, оскільки взаємодіє з більшою кількістю гостей.

Застосування ІКТ на всіх етапах надання послуги гостинності створює реальні передумови для підвищення рівня ефективності і обслуговування шляхом прискорення обміну інформацією між людьми і підсистемами управління. Досвід крупних готельних мереж (Hilton, Hyatt, Sheraton, Holiday Inn,

Courtyard, Hampton Inn, Mercure, Ramada, SHANGRI-LA ASIA тощо) свідчить про активне впровадження інформаційно-комунікаційних інструментів майже у всі бізнес-процеси. Проте, поряд з позитивними сторонами є негативні, пов'язані з високими витратами, що не є посильними для невеликих компаній гостинності та засобів розміщення.

*Список використаних джерел*

1. Morozov, M. A., Morozova, N. S. (2016). Attractive Tourist Destinations as a Factor of its Development. *Journal of Environmental Management and Tourism*, VII, 1 (13), 105–112.

2. Stringam, B. B., Gerdes, J. H. (2021). Hotel and guest room technology. In C. Cobanoglu, S. Dogan, K. Berezina, G. Collins (Eds.), Hospitality&Tourism Information Technology, University of South Florida M3 Center Publishing, 1–60. https://www.doi.org/10.5038/9781732127593. (дата звернення : 09.11.2022).

3. Bacik, R., Kmeco, L., Richard, F., Olearova, M., Rigelsky, M. (2019). Marketing Instrument of Improving Hotel Management Service: Evidence of Visegrad Group Countries. *Marketing and Management of Innovations*, 1, 208–220. http://doi.org/10.21272/mmi.2019.1-17. (дата звернення : 08.11.2022).

## ОЦІНКА ЗБИТКІВ ТА ІНСТРУМЕНТИ ВІДНОВЛЕННЯ УКРАЇНИ В УМОВАХ ВІЙНИ

***К.О. Наложитова,***
магістрантка факультету інформаційних систем та технологій,
ПВНЗ «Європейський університет»

Війна в Україні триває 9 місяців. За цей час було пошкоджено та знищено значну кількість об'єктів. Так, за останніми даними офіційного звіту «Швидка оцінка завданої шкоди та потреб на відновлення – серпень 2022» спільно підготовлений Світовим банком, Урядом України та Європейською Комісією загалом пошкоджено об'єктів на суму 97 млрд дол.

Швидка оцінка збитків і потреб (RDNA) представляє першу комплексну оцінку наслідків війни в двадцяти різних секторах після російського вторгнення та визначає потреби у фінансуванні для стійкого, інклюзивного та сталого відновлення та реконструкції та надає дорожню карту для планування.

Загалом обсяг потреб на відновлення та відбудову на 1 червня складав ~ 349 млрд дол. З кожним днем війни ці цифри лише збільшуються.

Уряд України вже почав відновлювати об'єкти критичної інфраструктури та житлового фонду за кошти Державного бюджету України. Так, з резервного фонду було виділено 1,45 млрд грн (39,7 млн дол) для відновлення об'єктів на деокупованих територіях. Це складає лише 5% потреби. На жаль, більше зараз Україна не може знайти коштів, адже війна продовжується.

Мінрегіоном була розроблена програма для відновлення об'єктів критичної інфраструктури та житлового фонду «Rapid recovery for survival», яка передбачає залучення донорських коштів. Це програма, яка направлена на відновлення об'єктів, що потребують переважно поточного або капітального ремонту та можуть бути реалізовані в найближчі місяці.

Категорії об'єктів, які були обрані – об'єкти ЖКГ; заклади освіти; заклади охорони здоров'я; житлові об'єкти; мости та дороги.

Критерії відбору проєктів:

- соціально значущі об’єкти (відновлення допоможе запобігти гуманітарну кризу та масову евакуацію)
- безпечні об’єкти (деокуповані території, розміновані території, 40 км мінімум від лінії фронту)
- об’єкти потребують лише поточного або капітального ремонту
- максимальний термін виконання робіт до 01.04.2023 року

Загальна кількість відібраних об’єктів – 40 560, з них:

- ЖКГ – 1287
- Заклади медицини – 260
- Заклади освіти – 635 (школи – 378; садочки – 257)
- Мости та дороги – 42
- Житло – 38336 ( приватні – 33104; багатоквартирні – 5232)

Для механізму реалізації даної програми були обрані найсучасніші та давно відомі світові практики. Так, буде створено steering committee, куди будуть входити представники донорів та уряду України. Саме цей комітет буде затверджувати проєкти та погоджувати їх фінансування.

Алгоритм дії: Громади/Ода будуть подавати проєкти до PMU (Група управління проєктами), який готує всі пакети документів та подає на затвердження до комітету.

До основних функцій комітету належить – затвердження критеріїв відбору проєктів; затвердження самих проєктів; оцінка впровадження проєктів; моніторинг проєктів.

У той час як звіт містить базові дані щодо галузевої та міжгалузевої інформації щодо потреб у відновленні та реконструкції, пов’язаних зі збитками та втратами, необхідно було терміново розробити стандартизовані методи та IT-рішення для оцінки цих збитків.

Так, на завершальній стадії розробки одне з пропонованих цифрових рішень – «ГІС регіонального відновлення та розвитку». Це геоінформаційна система Мінрегіону, яка стане зручним цифровим інструментом, що дозволить збирати агреговані дані по зруйнованим та пошкодженим об’єктам, створювати прогнозовані моделі та моніторити відбудову таких об’єктів, проводити комплексне та свідоме відновлення всієї території України на основі data-driven підходу.

*Список використаних джерел:*

1. Звіт по оцінці збитків від Світового банку: https://documents.worldbank.org/en/publication/documents-reports/documentdetail/099445109072232395/p1788430c59f110920ae4d04bd31d82c530

2. Звіт RDNA Мінрегіон: https://www.minregion.gov.ua/wp-content/uploads/2022/09/zvit-shvydka-oczinka-zavdanoyi-shkody-ta-potreb-na-vidnovlennya_-ukr-1.pdf

3. Програма для відновлення об’єктів критичної інфраструктури та житлового фонду «Rapid recovery for survival»: https://www.minregion.gov.ua/press/news/oleksij-chernyshov-obgovoryv-z-amerykanskymy-partneramy-podalshu-vidbudovu-ukrayiny/

4. Геоінформаційна система регіонального відновлення та розвитку: https://www.undp.org/uk/ukraine/press-releases/nova-heoinformatsiyna-systema-zadlya-pokrashchennya-informuvannya-ta-vidbudovy-ukrayiny

# СТРАТЕГІЯ РОЗВИТКУ ОРГАНІЗАЦІЇ: ТЕОРЕТИЧНИЙ АСПЕКТ

***Д. Несвіт,***
*студент,*
*ПВНЗ «Європейський університет»*

Характеристикою сучасних організацій є низький рівень конкурентних переваг та короткий період життєвого циклу, причиною яких є, з одного боку, нестабільність економічної ситуації в країні, з іншого – низький рівень ефективності стратегічного управління. Як відомо з теорії менеджменту, управління будь-якою компанією чи організацією необхідно розглядати в двох площинах: оперативній та стратегічній [5]. Мета оперативного управління – прийняття управлінських рішень, які впливають на поточну прибутковість компанії засобами коротко- та середньострокового планування. Стратегічне управління пов'язане з формуванням стратегії підприємства. Потреба застосування поряд із тактичним та операційним управлінням ідеології стратегічного управління полягає в тому, що необхідно в сучасних умовах переносити увагу вищого керівництва компанії із внутрішніх проблем, з якими може впоратися середня ланка управління, на проблеми зовнішнього середовища, іншими словами – концентруватися необхідно на тих проблемах, які в майбутньому можуть нести в собі або додаткові можливості, або додаткові загрози [3].

У ході дослідження наукової літератури встановлено, що стратегії розвитку організацій можна згрупувати у дві групи: активні стратегії та пасивні стратегії. Активні стратегії передбачають:

– швидкі дії на зміну ситуації на ринку, намагання випередити конкурентів;

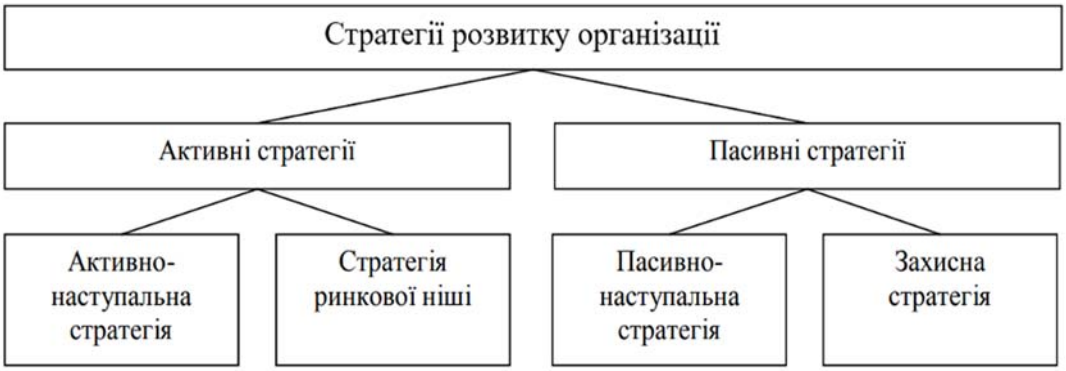
– гнучкість усіх процесів, які відбуваються в організації;

– можливість інтенсивного використання всіх видів ресурсів праці, енергії, сировини і матеріалів, обладнання;

– постійний пошук і запровадження інновацій у всіх сферах діяльності. Пасивні стратегії розвитку передбачають наслідування конкурентів, перегляд діяльності в разі виникнення такої потреби і, таким чином, є менш ризиковими і навіть можуть бути менш витратними [1].

Серед активних і пасивних стратегій розвитку можна виділити декілька видів, а саме: активно-наступальна, ринкової ніші, пасивно-наступальна, захисна (рис. 1).

**Рис.1. Класифікація стратегій розвитку організації**




Основними принципами розроблення активних і пасивних стратегій розвитку організації мають бути: спрямування на довгострокові цілі підприємства; багатоваріантність потенційних напрямків розвитку, яка зумовлена динамікою зовнішнього і внутрішнього середовища організації; безперервність розроблення стратегії; комплексність формування стратегії, узгодженість відповідних стратегічних рішень за окремими напрямами діяльності компанії, видами ресурсів, функціями тощо [2]. Активно-наступальна стратегія розвитку передбачає максимальну реалізацію стратегічних змін у розвитку організації. Її суть полягає у тому, щоб компанія була першою у розробках і впровадженні нових видів продукції та нових технологічних процесів. Така стратегія передбачає використання різноманітних заходів для підтримки позитивних зростаючих позицій. Активно-наступальна стратегія спрямовується на активізацію інтенсивності використання всіх видів ресурсів, праці, фінансів. Для цієї стратегії характерні високий рівень ризику та значна потреба в інвестиціях.

Стратегія ринкової ніші належить до активних стратегій, метою якої є забезпечення високої рентабельності продукції, підвищення якості продукції та її конкурентоспроможності, вдосконалення форм обслуговування продукції. Стратегія ринкової ніші властива для етапу зрілості життєвого циклу організації. Активні стратегії розвитку характеризуються збільшенням обсягів реалізації продукції, зниженням витрат виробництва, збільшенням прибутків, високим рівнем фінансової стійкості, зростанням оборотності оборотних активів, розширенням збутової мережі тощо [6].

Пасивно-наступальна стратегія передбачає виведення на ринок нової (або поліпшеної) продукції після апробації її у компаній лідерів. Стратегія потребує суттєвих витрат на оновлення продукції та характеризується середнім рівнем ризику. Така стратегія може використовуватися на всіх етапах життєвого циклу компанії. Пасивно-наступальна стратегія спрямована на використання відповідних заходів, які забезпечать підтримку і рівномірне зростання результатів діяльності підприємства. Ця стратегія створює всі передумови для забезпечення фінансової стійкості організації.

Отже, стратегічне управління має ряд переваг. Насамперед, це мінімізація негативних наслідків змін та факторів «невизначеності майбутнього». Також стратегічне управління надає можливість враховувати фактори зовнішнього та внутрішнього середовища, які формують зміни; зробити організацію більш

керованою, оскільки за наявності системи стратегічних планів є змога порівнювати досягнуті результати з поставленими цілями, конкретизованими у вигляді планових завдань.

*Список використаних джерел*

1. Артеменко Л.П., Гук О.В., Жигалкевич Ж.М. Реалізація стратегії розвитку підприємства: синергічний підхід. Інвестиції: практика і досвід. 2009. № 19. С. 12-14.
2. Власенко В.А. Розробка та реалізація стратегії розвитку підприємства в умовах трансформації ринкових відносин: принципові підходи та інструменти. Економіка. Менеджмент. Підприємництво. 2014. № 26(1). С. 32-41.
3. Гончаров Ю.В., Лапчик Ю.Ю. Удосконалення стратегії розвитку підприємства. Вісник Київського національного університету технологій та дизайну. 2014. № 1. С. 193-199.
4. Золотаревський А.В. Створення стратегії економічного розвитку підприємства. Формування ринкових відносин в Україні. 2014. № 11(162). С. 107-113.
5. Кузьмак О.І. Інноваційна стратегія як засіб стабілізації розвитку промислового підприємства. Інноваційна економіка. 2016. № 1-2. С. 114-118.
6. Македон В.В. Розробка стратегії розвитку промислового підприємства. Теоретичні і практичні аспекти економіки та інтелектуальної власності. 2013. Вип. 1(1). С. 369-373.

## ІНСТИТУТ ДЕРЖАВНОЇ РЕЄСТРАЦІЇ СПЕЦІАЛЬНОГО МАЙНОВОГО ПРАВА НА ОБ'ЄКТИ НЕРУХОМОГО МАЙНА

***Т.П. Овсійчук,***
аспірант,
ПВНЗ «Європейський університет»

В незалежній Україні історично склалося, що інвестування в будівництво (особливо житлове) є одним із найбільш поширених видів здійснення інвестицій серед фізичних осіб. Зумовлено це, насамперед, відносною простотою такої інвестиції: квартиру чи нежитлове приміщення можна «потримати в руках», їхня вартість частіше зростає, ніж падає тощо. В будь-якому разі, нерухомість можна здавати в оренду, подарувати дітям, заповісти або проживати у ній самому. Проте, значний попит на певний товар завжди породжує бажання «нажитися» у недобросовісних продавців.

Про це свідчить офіційна статистика. Так, за даними Київської міської державної адміністрації, у місті Києві вважаються проблемними 41 об'єкт житлового будівництва, серед яких більшість це – багатосекційні житлові комплекси. Зумовлена така негативна статистика багатьма факторами, в тому числі відсутністю ефективного нормативно-правового регулювання зазначеної сфери діяльності. З одного боку, це сприяло старту нових девелоперських проєктів, адже забудовник міг використовувати багато інструментів під час залучення коштів: попередні договори, договори купівлі-продажу майнових прав, форвардні контракти, створення кооперативів тощо. Однак простота, низька вартість документального оформлення та відсутність державного контролю часто призводила до:

- подвійних продажів одного й того ж об'єкту нерухомого майна;
- відсутності відчуженого об'єкта нерухомого майна в проєктній документації та, як наслідок, неможливості його отримання у власність або

реєстрації права власності;

- зміни технічних характеристик об’єкта нерухомого майна без згоди інвестора;

- інших наслідків, що суттєво впливали на право інвестора володіти, користуватися або розпоряджатися нерухомим майном.

Обравши курс цифрової трансформації, українська держава поставила перед собою багато складних завдань, левову частку серед яких проходить однією з перших. 15 серпня 2022 року в умовах воєнного стану Верховна Рада України прийняла Закон України «Про гарантування речових прав на об'єкти нерухомого майна, які будуть споруджені в майбутньому», відповідно до умов якого спеціальні речові права на майбутні об’єкти нерухомого майна підлягають державній реєстрації. Закон набув чинності 10 жовтня 2022 року. Законом запроваджується:

- виключний перелік способів залучення коштів від фізичних чи юридичних осіб під час будівництва об’єктів нерухомого майна;

- створення гарантійної частки (певної кількості квартир або нежитлових приміщень, яка не може бути відчужена забудовником до прийняття об’єкта в експлуатацію);

- державна реєстрація спеціальних речових прав на об’єкти нерухомого майна, які будуть споруджені у майбутньому;

- обов’язкова нотаріальна форма правочинів щодо відчуження об’єктів нерухомого майна, які будуть споруджені в майбутньому, істотні умови таких правочинів;

- автоматична реєстрація права власності на об’єкт нерухомого майна після прийняття його в експлуатацію.

Необхідно відзначити, що у Законі значна кількість процесів або їх етапів підлягає автоматизації. Наприклад, дотримання вимог закону щодо розміру гарантійної частки у зв’язку з коригуванням проєктної документації на будівництво перевіряється автоматично програмними засобами електронної системи. Відсутність у Державному реєстрі речових прав на нерухоме майно відомостей про речові права на майбутні об’єкти нерухомості, включені до гарантійної частки, та обтяження речових прав перевіряються автоматично шляхом взаємодії програмних засобів електронної системи та Державного реєстру речових прав на нерухоме майно. У разі невідповідності цим вимогам програмні засоби електронної системи не дозволяють подання повідомлення про коригування проєктної документації на будівництво.

Таким чином, реалізація Закону можлива виключно за умови взаємодії між Єдиною державною електронною системою у сфері будівництва, Державним реєстром речових прав на нерухоме майно, Державним земельним кадастром та багатьма іншими базами даних. Інструменти, які запроваджуються Законом з метою захисту прав інвесторів у об’єкти будівництва, можна вважати якісним результатом ефективної співпраці між юридичною та ІТ-спільнотами. Автоматизація процесів державної реєстрації мінімізує ризик людської помилки, а також можливості неправомірного втручання в роботу систем. Це, в свою чергу, призводить до більшої ефективності захисту прав інвесторів.

*Список використаних джерел*

1. Комісія з вирішення проблемних питань по об'єктах незавершеного будівництва. Перелік проблемних об'єктів житлового будівництва (об'єктів самочинного будівництва та довгобудів), які потребують прийняття спеціального Закону України. Офіційний портал Києва. URL: https://kyivcity.gov.ua/mistobuduvannia_ta_zemelni_dilianky/komisiya_z_virishennya_probelmnikh_pitan_po_obyektakh_nezavershenogo_budivnitstva/perelik_problemnikh_obyektiv_zhitlovogo_budivnitstva_obyektiv_samochinnogo_budivnitstva_ta_dovgobudiv_yaki_potrebuyut_priynyattya_spetsialgo_zakonu_ukrani/ (дата звернення: 10.11.2022).

2. Про гарантування речових прав на об'єкти нерухомого майна, які будуть споруджені в майбутньому : Закон України від 15.08.2022 р. № 2518-IX. URL: https://zakon.rada.gov.ua/laws/show/2518-20#Text (дата звернення: 10.11.2022).

3. *Шуляк О., Фріс І., Клочко А.* Пояснювальна записка до проекту Закону України «Про гарантування речових прав на об’єкти нерухомого майна, які будуть споруджені в майбутньому». Електронний кабінет громадянина. URL: https://itd.rada.gov.ua/billInfo/Bills/pubFile/542579 (дата звернення: 10.11.2022).

## ПРОБЛЕМА ІДЕНТИФІКАЦІЇ ОСІБ ЕЛЕКТРОННОГО ПРАВОЧИНУ ПРИ ІНТЕРНЕТ ТОРГІВЛІ

***Р.О. Панасенко,***
аспірант,
ПВНЗ «Європейський університет»,
фізична-особа підприємець, адвокат

Протягом кількох останніх років частка Інтернет торгівлі на загальному ринку демонструє тенденцію до систематичного збільшення. Особливий вплив на зростання попиту на купівлю товарів (робіт, послуг) через мережу Інтернет мав період карантину в зв’язку з пандемією коронавірусу та обмежень на роботу офлайн-продавців які діяли в цей період. Після початку війни онлайн-торгівля, як і решта ринків, була майже паралізована, проте на даний момент відбувається стрімке відновлення онлайн-продажів.

Основним та, по суті, єдиним нормативним документом, що безпосередньо регулює правовідносини продавців та покупців при купівлі-продажу товарів (робіт, послуг) через мережу Інтернет є Закон України «Про електронну комерцію» від 3 вересня 2015 року № 675-VIII (зі змінами та доповненнями). [1]

Стаття 3 зазначеного Закону визначає, що електронний договір – домовленість двох або більше сторін, спрямована на встановлення, зміну або припинення цивільних прав і обов’язків та оформлена в електронній формі, а електронний правочин – це дія особи, спрямована на набуття, зміну або припинення цивільних прав та обов’язків, здійснена з використанням інформаційно-комунікаційних систем.

Стаття 207 Цивільного кодексу України від 16 січня 2003 року № 435-IV [3] (зі змінами та доповненнями) визначає електронний договір як різновид письмової форми договору а також встановлює, що правочин вважається таким, що вчинений у письмовій формі, якщо воля сторін виражена за допомогою телетайпного, електронного або іншого технічного засобу зв'язку.

Виходячи з положень зазначених нормативних актів існують сторони

(суб'єкти, особи), які здійснюють правовідносини в електронній формі спрямовані на встановлення, зміну або припинення цивільних прав і обов'язків. Слід зазначити, що сторони в будь яких правовідносинах мають бути чітко ідентифіковані, зокрема з метою перевірки їх право та дієздатності, оскільки вартість товарів придбаних через Інтернет в деяких випадках вимірюються десятками тисяч гривень. Основними сторонами правовідносин при здійсненні Інтернет торгівлі є продавець (інтернет-магазин) та покупець (здебільшого фізична особа).

Стаття 7 Закону України «Про електронну комерцію» передбачає обов'язок інтернет-магазинів забезпечити прямий, простий, стабільний доступ інших учасників відносин (в першу чергу покупців) у сфері електронної комерції до такої інформації: повне найменування юридичної особи або прізвище, ім'я, по батькові фізичної особи – підприємця; місцезнаходження юридичної особи або місце реєстрації та місце фактичного проживання фізичної особи – підприємця; адреса електронної пошти та/або адреса інтернет-магазину; ідентифікаційний код для юридичної особи або реєстраційний номер облікової картки платника податків для фізичної особи – підприємця, або серія та номер паспорта для фізичної особи – підприємця, яка через свої релігійні переконання відмовилася від прийняття реєстраційного номера облікової картки платника податків та офіційно повідомила про це відповідний податковий орган і має відмітку в паспорті; відомості про ліцензію (серія, номер, строк дії та дата видачі), якщо господарська діяльність підлягає ліцензуванню; щодо включення податків у розрахунок вартості товару, роботи, послуги та, у разі доставки товару, – інформація про вартість доставки; інші відомості, що відповідно до законодавства підлягають оприлюдненню.

Сумлінні інтернет-магазини дану норму виконують і надають зазначену інформацію, проте існують непоодинокі випадки коли покупець не знає у кого він купує товар (роботу, послугу) до моменту отримання розрахункових документів (які також надаються не завжди, або в неналежному вигляді). Крім того адекватної відповідальності за ненадання зазначеної інформації не передбачено, чим активно користуються непорядні продавці.

В крайньому випадку для ідентифікації продавця-власника інтернет-магазину (який за своєю суттю є веб-сайтом) можна скористатися положеннями Закону України «Про авторське право та суміжні права» від 23 грудня 1993 року № 3792-XII [2] (зі змінами та доповненнями) стаття 1 якого передбачає, що власник веб-сайту – особа, яка є володільцем облікового запису та встановлює порядок і умови використання веб-сайту. За відсутності доказів іншим власником веб-сайту вважається реєстрант відповідного доменного імені, за яким здійснюється доступ до веб-сайту, і (або) отримувач послуг хостингу. І за недоліки роботу інтернет-магазину буде відповідати саме реєстрант відповідного доменного імені, якщо не доведе, що передав це доменне ім'я в користування іншим особам та/або не зможе надати дані таких осіб.

З покупцями ситуація складніше. При укладанні правочину в інтернет-магазині покупець зазначає лише свій номер телефон та/або адресу електронної пошти, в деяких випадках вимагається заповнити певну форму з прізвищем та ім'ям (яка знову ж таки відсилає до номеру телефону та/або адреси електронної

пошти покупця) чи надати підтвердження коду, який надсилає інтернет-магазин своєму потенційному покупцю (електронний підпис одноразовим ідентифікатором ). При цьому ні інтернет-магазин, ні, по суті, будь-хто інший не може ні перевірити надану покупцем інформацію, ні однозначно ідентифікувати особу покупця, ні правомірність використання особою номеру телефону та/або адреси електронної пошти. [4]

Механізму ідентифікації та перевірки покупців інтернет-магазинів на даний момент просто не існує, незважаючи на наявність умов для його існування. Зокрема, застосунок ДІЯ однозначно пов'язує ідентифікаційні (паспортні) дані людини з номером телефону, аналогічна інформація може бути запитана у особи при реєстрації електронної пошти та в подальшому бути використаної при ідентифікації особи, яка використовує номер телефону та/або адресу електронної пошти.

При належному нормативному врегулюванні даних питань учасники правовідносин, контролюючі чи правоохоронні органи матимуть змогу однозначно ідентифікувати осіб, які є сторонами в електронному правочині, що є особливо актуальним на даний час, коли, користуючись «анонімністю» онлайн торгівлі, відбуваються махінації як з коштами зібраними волонтерами на придбання товарів необхідних для армії, так і придбання товарів з метою їх подальшої передачі агресору.

*Список використаних джерел*

1. Закон України «Про електронну комерцію» від 3 вересня 2015 року № 675-VIII (зі змінами та доповненнями).

2. Закону України «Про авторське право та суміжні права» від 23 грудня 1993 року № 3792-XII (зі змінами та доповненнями).

3. Цивільний кодекс України від 16 січня 2003 року № 435-IV (зі змінами та доповненнями).

4. Матеріали веб-сайту. URL: https://rau.ua/novyni/ukrainskij-ritejl-u-2021-deloitte/

## СТВОРЕННЯ ТА РОЗРОБКА ІГРОВИХ ДОДАТКІВ «ЕКОНОМІЧНІ ОНЛАЙН-ІГРИ» НА UNITY

***Д.Ю. Покидько,***
магістрант факультету інформаційних систем та технологій,
***Л.О. Литвиненко,***
к.т.н., доцент кафедри інформаційних систем,
програмування та кібербезпеки,
ПВНЗ «Європейський університет»

З розвитком ринку GameDev більшої набирають популярності економічні онлайн-ігри, тобто ігри, які являють собою якийсь світ зі своїми правилами і законами, в якому гравцеві надається можливість займатися активною комерційною діяльністю: будувати торгові та виробничі підприємства та споруди, займатися розробкою природних ресурсів, вести активну фінансову та банківську діяльність у рамках ігрового простору. Unity - найпопулярніший ігровий движок на даний момент. Більше 40% ігор на всіх пристроях створено на Unity.

Існує безліч ігор економічного жанру, але більшість з них не мають суттєвого економічного показника (тобто ґрунтуються тільки на військовому чи іншому показнику), серед них так само існує безліч ігор, що вимагають вкладення коштів у гру "Донат", у зв'язку з цим обрана тема не втратила своєї актуальності нині. Економічні ігри залишаються відкритою своєрідною нішею у сфері ігор.

Основна мета даного дослідження – розгляд економічних чинників, які впливають на створення комп'ютерних ігор, дослідження стану створення програмного забезпечення. Предмет дослідження – економічні онлайн-ігри.

Основний сенс економічних ігор полягає в управлінні деяким ресурсом, який необхідно перетворити на перевагу над супротивником за допомогою оперативного плану, що розробляється з урахуванням мінливої обстановки. Звичайними ресурсами у військових стратегіях є війська (окремі персонажі, підрозділи чи армії) та позиція, які слід розвивати та використовувати для досягнення переваги та перемоги. В економічних стратегіях акцент ставиться на розвиток економічної інфраструктури, підконтрольної певній стороні.

Сучасні стратегічні ігри, зазвичай, поєднують у собі як військові, і економічні ознаки. У більшості стратегій існують економічна (збір ресурсів, підготовка військ) та військові складники.

В роботі було проаналізовано засоби розробки програми. Для створення програми використовуватиметься ігровий рушій Unity 3D. Однією з основних переваг Unity є: скриптування різними мовами, кросплатформність, Asset Store. Також однією з основних переваг є Multiplatform Solutions Framework (MSF).[1] Але варто розуміти, що ігровий рушій не визначає успіху чи невдачі гри, він, швидше, впливає на процес виробництва — і в першу чергу швидкість. Щодо успіху, тут набагато більше значення мають досвід команди, маркетинг, та й, як не дивно, якість самої гри. Зрештою, визнаний усіма шедевр To the Moon канадська студія Freebird Games взагалі зробила на RPG Maker – рушію, на якому (через простоту його освоєння) робиться велика кількість виробів низької якості.

Для онлайн-ігор у жанрі економічні стратегії характерні певні риси: розвиток виробництва, бізнесу та торговельних відносин, будівництво фабрик та заводів, укладання угод. Гравці можуть побудувати величезну імперію або у поєднанні з військовою справою зібрати непереможну армію, що має сучасні технології. Гроші та ресурси – найважливіший елемент будь-якої економічної онлайн-стратегії, необхідний для розвитку економіки та зростання виробництв. Яскравий приклад – гра Uptasia, де гравець має розпочати з пекарні, відкрити квітковий магазин, кафе, побудувати заводи і перетворити село на величезний мегаполіс.

Створення економічної гри ділиться на два етапи: опрацювання логіки та чисельні розрахунки. Без продуманої логіки братися до розрахунків безглуздо.

Математика – важлива частина кожної гри. Вона створює азарт і загальну динаміку ігрової сесії. Але для гарантування безпечного ігрового процесу мають виконуватися чинні норми.

Останнім часом індустрія гемблінгу під пильною увагою: всі процеси мають бути абсолютно прозорими і зрозумілими для кінцевого користувача, без будь-яких прихованих платежів. Створення економічних ігор є не тільки

розвитком розважального контенту, а і хорошим симулятором бізнес-процесів, управлінських процесів, що можна використовувати для навчання. Такі ігри дозволяють початківцям і досвідченим підприємцям побудувати віртуальний прототип свого реального підприємства, допомагають протестувати різні стратегії розвитку, покращити знання і навички в управлінні реальними компаніями і стартапами. Для фанатів ігор економічні стратегії є можливість побудувати корпорацію в реалістичному конкурентному середовищі симуляції.

*Список використаних джерел*

1. Сословский В. Онлайн бізнес-симуляції: класифікація, типологія, вибір, досвід використання. URL: https://dist.karazin.ua/articles/show/onlajn-biznessimulyacii-klassifikaciya-tipologiya-vybor-opyt-ispolzovaniya (дата звернення: 03.11.2022).

## ПРОБЛЕМИ РЕГІОНАЛЬНОЇ СТАТИСТИКИ В УМОВАХ ДЕЦЕНТРАЛІЗАЦІЇ ТА ЦИФРОВІЗАЦІЇ ВЛАДИ

***Д. Я. Протопопов,***
*аспірант,*
*ПВНЗ «Європейський університет»*

В рамках подальшої децентралізації влади в України Верховною Радою України була затвердження Постанова № 3650 «Про утворення та ліквідацію районів» від 17 липня 2020 року, згідно якої було зменшено кількість районів з 490 до 136, що надалі продовжило децентралізацію влади. Почався етап місцевих виборів з подальшою ліквідацією районних адміністрацій та районних рад і формуванням нових органів виконавчої влади згідно з новим адміністративним устроєм. Серед ключових завдань децентралізації влади є завдання з формування ефективного місцевого самоврядування та територіальної організації влади для надання якісних та доступних публічних послуг, задоволення інтересів громадян в усіх сферах життєдіяльності на відповідній території.

На розширеній урядовій нараді з питань децентралізації та регіонального розвитку Віце-прем'єр-міністр – Міністр регіонального розвитку, будівництва та ЖКГ України заявив, що децентралізація – найуспішніша з усіх впроваджуваних реформ в Україні. Він наголосив, що вона має найбільшу довіру й підтримку з боку суспільства, громадян, а також міжнародної спільноти. «Реформа децентралізації і державна політика, яку ми впроваджуємо в її рамках, має одну мету – розвиток людського потенціалу. Тому я хочу сконцентрувати увагу лідерів обласних рад, голів ОДА, міських голів і ОТГ на двох важливих показниках, за якими буде оцінюватись кожен регіон. Перший – індекс регіонального людського розвитку (далі – ІРЛР), який для нас є важливим і базується на основних складових, як здоров'я та довголіття, доступність освіти, гідний рівень життя. Це саме той індекс, який допоможе втримати людей і залучити додатковий ресурс. І другий – індекс конкурентоспроможності регіонів (далі – ІКР), який визначає здатність регіону створювати привабливе середовище для розвитку бізнесу та інвестицій» [1].

Започаткована реформа децентралізації вимагає зміни мислення та

підходів до формування стратегій регіонального розвитку. Прем'єр-міністр зауважив, що рух реформи має бути в одному напрямку – напрямку побудови сильних громад [2].

Існуюча система інформаційно-статистичного забезпечення не повною мірою відображає потреби органів управління регіонального рівня та рівня територіальних громад у процесі стратегічного планування при розробці комплексних програм соціально-економічного розвитку країни та територіальних утворень з урахуванням визначених перспективних напрямків розвитку регіонів. В умовах, коли багато функцій управління передаються з центру на місця, органи влади і органи місцевого самоврядування потребують більш різноманітної і детальної економіко-статистичної інформації в різнорівневому територіальному аспекті, тому дослідження у цьому напрямку є актуальними та своєчасними.

Регіональна економіка – це область наукових знань, яка вивчає розвиток і розміщення продуктивних сил, соціально-економічні процеси на території країни та її регіонів у тісному зв'язку із природно-екологічними умовами. Вона охоплює статистичні дослідження в областях, районах, містах, а також територіальних громадах. Система регіональної інформації базується на сукупності показників державних статистичних спостережень, проведених на державному, відомчому та регіональному рівнях.

Відстеження реалізації стратегічних цілей розвитку територіальних громад передбачає роботи, що проводяться Мінрегіоном спільно із Держстатом і іншими міністерствами та відомствами. Інтеграція інформаційно-статистичних даних у масштабах регіону для інформаційно-статистичного забезпечення органів державної влади проводиться шляхом об'єднання даних офіційної статистики, що формують статистичну інформацію в рамках плану державних статистичних спостережень, з даними інших органів державної влади.

Так, у постанові Кабінету Міністрів України від 20 грудня 2017 р. №1029 «Деякі питання удосконалення системи моніторингу та оцінки результативності реалізації державної регіональної політики» ІКР та ІРЛР розраховуються щороку Мінрегіоном на підставі наявних даних офіційної статистики та інформації, поданої міністерствами, іншими центральними органами виконавчої влади, Національним банком (за згодою), Радою міністрів Автономної Республіки Крим, обласними, Київською та Севастопольською міськими держадміністраціями [3]. Тобто визначено вісім міністерств та відомств, відповідальних за подання даних, які застосовуються для розрахунку індексів результативності реалізації державної регіональної політики (таблиця 1).

Як видно з таблиці, найбільша частка показників (55,7%) забезпечується на підставі наявних даних офіційної статистики. Дані офіційної статистики за переліком показників, подаються Держстатом відповідно до затвердженої в установленому порядку статистичної методології та звітно-статистичної документації статистичних спостережень. Але, поряд із офіційними даними Держстату, використовуються показники Мінрегіону (18,0%), отримані за результатами проведення інтерактивного та/або анкетного опитувань та інших відповідальних за напрямами досліджень.

*Таблиця 1*

**Зведені дані щодо відповідальних за подання даних для розрахунку індексів результативності реалізації державної регіональної політики**

| | Група показників | Кількість відповідальних за подання даних, всього | з них | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | Держстат | Мінфін | Укравтодор Рада міністрів АР Крим, обласні та Севастопольська МДА | Мінрегіон | МОН | Мінекономрозвитку | Національний банк (за згодою) | Мінсоцполітика |
| **Індекс конкурентоспроможності регіонів (ІКР)** | | | | | | | | | | |
| **1.** | **Базові вимоги** | 23 | 11 | 2 | 1 | 3 | 6 | 0 | 0 | 0 |
| **2.** | **Підсилювачі ефективності** | 15 | 10 | 0 | 0 | 3 | 1 | 1 | 0 | 0 |
| **3.** | **Інноваційний потенціал** | 15 | 8 | 0 | 0 | 5 | 0 | 1 | 1 | 0 |
| | **Всього ІКР** | 53 | 29 | 2 | 1 | 11 | 7 | 2 | 1 | 0 |
| **Індекс регіонального людського розвитку (ІРЛР)** | | | | | | | | | | |
| **1.** | **Довге та здорове життя** | 3 | 3 | | | | | | | |
| **2.** | **Добробут та гідні умови праці** | 3 | | 1 | | | | | | 2 |
| **3.** | **Освіта** | 2 | 2 | | | | | | | |
| | **Всього ІРЛР** | 8 | 5 | 1 | 0 | 0 | 0 | 0 | 0 | 2 |
| **Всього ІКР та ІРЛР** | | 61 | 34 | 3 | 1 | 11 | 7 | 2 | 1 | 2 |
| **Відсоток участі відповідальних** | | | **55,7** | **4,9** | **1,6** | **18,0** | **11,5** | **3,3** | **1,6** | **3,3** |

В результаті аналізу динаміки показників визначаються їх зміна (покращення, погіршення) у звітному році порівняно з попереднім роком, зокрема виявлення закономірностей і окремих тенденцій зміни проаналізованих показників у відповідних сферах.

Але при здійсненні порівняння із показниками, які досліджувалися у попередньому періоді, виникає проблема. Якщо дані офіційної статистики є доступними на сайті Держстату, то дані інтерактивного та/або анкетного опитувань за напрямами досліджень Мінрегіону відсутні. Перелік показників, які застосовуються для оцінки результативності реалізації державної регіональної політики зазнали кардинальних змін. Незмінними залишилися лише вісім показників, тобто 4,9% від їх загальної кількості (61 показник). Саме тому

з’являється проблема проведення аналізу динаміки цих показників.

На основі даних регіональної статистики здійснюється оцінка господарської діяльності в регіонах, ринкової економічної кон’юнктури, визначається конкурентоспроможність та інвестиційна привабливість регіонів, що дозволяє встановлювати цілі і завдання управління, розробляти програми і прогнози соціально-економічного розвитку регіонів. Чим точніше і достовірніше дані регіональної статистики, тим більш дієві будуть управлінські рішення і ефективніше контроль над їх виконанням.

При цьому слід зауважити, що при побудові прогнозних моделей, зростає попит на статистику, представлену в тривалій динаміці. В офіційних даних, розміщених на офіційному Інтернет-сайті Держстату, найважливіші статистичні показники країни (Комплексна статистика) в даний час представлені в динаміці починаючи з 2001 року, а найважливіші статистичні показники регіону (Регіональна статистика) за менш короткий період, зокрема показник валового регіонального продукту – з 2004 року [4]. Але, для визначення тенденцій щодо регіонального розвитку потрібні тривалі динамічні ряди по всіх показниках, які враховані у розрахунку інтегрального ІКР та ІРЛР.

Розглядаючи розрахунок показників на базі Луганського регіону, можливо стверджувати, що цей процес є особливо складним. Тому що по регіону взагалі відсутні дані періодів до 2014 року. І це передбачає проведення додаткового комплексу робіт з відновлення тривалих динамічних рядів по найважливіших статистичних показниках і уточнення методології їх розрахунку, що забезпечить порівнянність показників у тривалій динаміці.

Поряд із показниками оцінки результативності реалізації державної регіональної політики на рівні обласного регіону, сучасність вимагає також моніторингу та оцінки ефективності реалізації державної регіональної політики на рівні територіальних громад. Тобто виникає необхідність формування статистики територіальних громад.

Аналізуючи розвиток формування статистики територіальних громад з 2019 року по теперішній час приходимо до висновку щодо її втрати. Так, вперше віддалення статистики від територіальних громад відбулося відповідно до постанови Кабінету Міністрів України №1072 «Про внесення змін та визнання такими, що втратили чинність, деяких актів Кабінету Міністрів України» від 04 грудня 2019 року, згідно з якою органами Держстату було скорочено 985 працівників третього рівня та повністю ліквідовано району ланку відділів/управлінь статистики [5]. Це на фоні завдання зменшення звітного навантаження на респондентів та подальшого переходу на вибіркові методи статистичних спостережень згідно з програмою розвитку державної статистики до 2023 року, яка була затверджена постановою Кабінету Міністрів України №222 «Про затвердження Програми розвитку державної статистики до 2023 року», призвело до більш глибокого переходу на вибірковий метод обстеження в усіх державних статистичних спостереженнях (крім спостережень у сфері статистики фінансів) [6]. Підсумком таких перетворень виявилось зниження репрезентативності статистичних показників на рівні територіальних громад та районних адміністрацій, а в деяких випадках, їх повне закриття на виконання статті 21 Закону України №2614-XII «Про державну статистику» від 19 вересня

1992 року [7]. Так, в умовах децентралізації влади, територіальні громади та районні адміністрації вперше зіткнулися з браком статистичних показників та неможливістю налагодження системи моніторингу та оцінки результативності реалізації державної регіональної політики.

Постійний голод у статистичних показниках на рівні територіальних громад та районних адміністрацій на протязі 2020 року призвів до неможливості моніторингу та оцінки результативності реалізації державної регіональної політики. Це, в свою чергу, призвело до того, що при прийнятті «Національної економічної стратегії на період до 2030 року», затвердженої постановою Кабінету Міністрів України №179 від 3 березня 2021 року на це було звернуто увагу.

Так, згідно напрямку 16 «Регіональний розвиток» за стратегічною ціллю 2 «Підвищення інституційної спроможності місцевих органів виконавчої влади, органів місцевого самоврядування та агенцій регіонального розвитку для ефективного забезпечення розвитку регіонів і територіальних громад» пункту 4 «Налаштування ефективного забезпечення даними» шляху досягнення стратегічної цілі було вказано на необхідність створення управлінь з муніципальної статистики при міських (районних у містах), районних, сільських, селищних радах [8]. Стратегія повною мірою задекларувала необхідність повернення інституцій органів Державної статистики на рівень міських, районних, сільських та селищних рад.

Протягом 2021-2022 рр. територіальні громади, райони адміністрації та області адміністрації з великими надіями очікували від Держстату, Міністерства економіки та Міністерства цифрової трансформації (як куратора органів державної статистики) проєктів з реалізації регіональної статистики, а замість цього отримали тільки подальший процес віддалення органів державної статистики від регіонів і переорієнтування їх на державний рівень. Про це свідчить прийнятий Верховною Радою Закон України №2524-IX «Про офіційну статистику» від 16 серпня 2022 року. якій вступить в дію з 01 січня 2023 року [9].

Основні показники, які необхідні органам місцевого самоврядування для моніторингу та оцінки результативності реалізації державної регіональної політики у зв’язку в вибірковим методом обстеження проводяться тільки по великим та середнім підприємствам, які в 80 відсотках закриваються, як конфіденційні, органами державної статистики та не дозволяють проводити аналіз. Найважливіші для органів місцевого самоврядування показники для розрахунків економічних показників на рівні територіальної громади можуть бути отримані тільки на основі суцільного статистичного обстеження підприємств, що знаходяться в його межах.

Проблеми регіональної статистики, які виникли в умовах децентралізації та цифровізації влади:

– віддалення органів державної статистики від територіальних громад, районних адміністрацій;

– втрата репрезентативності статистичних показників та закриття їх за конфіденційністю, які визначаються вибірковим обстеженням;

– відсутність законодавчої бази щодо регіональної/муніципальної статистики;

– відсутність статистичної термінології стосовно територіальних громад в умовах децентралізації влади;

– відсутність автоматизовано-цифрових систем при проведенні обстеження суцільним методом та обробки отриманих результатів.

Можливі шляхи подальшого розвитку регіональної статистики в умовах децентралізації та цифровізації влади на територіальному рівні:

1) розроблення законодавчої та нормативної бази щодо функціонування регіональної/муніципальної статистики;

2) відкриття муніципальних відділів/управлінь та налагодження їх співпраці з органами державної статистики на рівні обласних управлінь;

3) розробка статистичної методології щодо проведення суцільних методів обстеження на рівні територіальних громад;

4) розробка автоматизовано-цифрових систем для проведення обстеження;

5) створення інформаційно-аналітичної системи моніторингу показників результативності реалізації державної регіональної політики на рівні територіальних громад, районних адміністрацій.

Підсумовуючи вищесказане, можна стверджувати, що децентралізація та цифровізація влади підняла великий пласт проблем на регіональному рівні як в місцевих органах влади, так і в органах центральної виконавчої влади. Саме тому вирішення інституціональних проблем регіональної статистики та її цифрової автоматизації потребує подальшого дослідження.

*Список використаних джерел*

1.Регіони будуть оцінюватися по двом ключовим показникам. URL: http://decentralization.gov.ua/news/8631..

2.Децентралізація вимагає зміни мислення і підходів до формування регіональних стратегій розвитку. URL: http://decentralization.gov.ua/news/8634.

3.Постанова Кабінету Міністрів України «Деякі питання удосконалення системи моніторингу та оцінки результативності реалізації державної регіональної політики» від 20 грудня 2017 р. № 1029. Урядовий кур'єр від 11.11.2015 . №210.

4.Сайт Держстату. URL: http://www.ukrstat.gov.ua.

5.Постанова Кабінету Міністрів України « Про внесення змін та визнання такими, що втратили чинність, деяких актів Кабінету Міністрів України» від 04 грудня 2019 р. №1072. Урядовий кур'єр від 24.12.2019. №247.

6.Постанова Кабінету Міністрів України «Про затвердження Програми розвитку державної статистики до 2023 року» від 27 лютого 2019 р. №222. Урядовий кур'єр від 27.03.2019. №59.

7.Закон України «Про державну статистику» від 17 вересня 1992 р. №2614-XII // Відомості Верховної Ради України від 27.10.1992. 1992р. №43, стаття 608.

8.Постанова Кабінету Міністрів України «Про затвердження Національної економічної стратегії на період до 2030 року» від 03 березня 2021 р. №179. Урядовий кур'єр від 06.03.2021. №45.

9.Закон України «Про офіційну статистику» від 16 серпня 2022 р. №2524-IX. Урядовий кур'єр від 10.09.2022. №196.

# СТРАТЕГІЇ РОЗВИТКУ РИНКУ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ В УКРАЇНІ

***О.С. Святобог,***
аспірант,
ПВНЗ «Європейський університет»

В умовах війни з рф важливим є розірвання будь-яких стосунків з агресором та позбавлення його можливості отримувати дохід. Не менш важливим є побороти монополію російського ПЗ, яке заполонило наш ринок. Бітрікс24, FREDO, 1С/BAS, які прикриваються українськими та європейськими офісами є фактично загрозою для безпеки нашого бізнесу. Неодноразові хакерські атаки на підприємства України з боку рф доводять нам – ворогу довіряти не можна і використовувати його ПЗ в жодному разі не можна. Але ці програми досі використовують як приватні, так і державні компанії та установи.

Чому при одночасному старті програмних продуктів Парус та 1С остання захопила панівне становище? Різна політика компаній та маркетинговий підхід. 1С зробила в середині 90-х років версію 1С, яку продавали в коробці, з ліцензійним ключем і платила високий відсоток своїм дистриб'юторам на теренах колишнього радянського союзу. Згодом до продажу додалась необхідність здійснювати підтримку на місцях і це збільшило дохід 1С, поглибило їх експансію. При цьому Парус вибрала напрямок роботи з великими підприємствами, без великої кількості представників і дистриб'юторів свого часу і, таким чином, віддала першість.

На сьогоднішній день ситуація змінилася ось ще з якої причини – у світі шалено зростає кількість користувачів смартфонів, дані зберігаються у хмарах, бізнес потребує отримувати дані на ходу і зручно. І це є шансом для нового повороту розвитку ПЗ яким буде користуватися український бізнес. Уже зараз активно розвиваються бухгалтерські програми, програми для роботи бізнесу, програмні РРО, які можуть працювати безпосередньо у телефоні. Уже зараз можна отримати відтермінування на оплату товару, не йдучи у банк, а безпосередньо у додатку в телефоні, підписавши угоду у декілька кліків. Шанси на успіх досить значні, особливо, коли за справу беруться монстри фінтеху, які уже дали Україні цікаві та передові продукти.

*Список використаних джерел*

1. Касовий апарат не потрібен. URL: https://tech.liga.net/technology/novosti/kassovyy-apparat-ne-nujen-dubilet-zapustil-servis-programmnyh-kass-video

2. Сайт компанії Парус. URL: http://www.parus.ua/

3. Аналоги 1С та BAS в Україні.URL: https://tqm.com.ua/ua/likbez/ua-articles/bezkoshtovni-analohy-1s

4. Сайт компанії Хмарна система jSolutions. URL: https://jsolutions.ua/ua

5. Інтерв'ю з CEO Bookkeeper SaaS. URL: https://youtu.be/OD15bwi-Sdg

6. Презентація роботи в програмі Navkolo Bookkeeper. URL: https://navkolo.bookkeeper.kiev.ua/home

7. Презентація роботи в програмі DN Trade. URL: https://testname.dntrade.com.ua/site/index

# ЦИФРОВА ТРАНСФОРМАЦІЯ В АВТОМОБІЛЕБУДУВАННІ: ОСНОВНІ ВИКЛИКИ ТА ПЕРСПЕКТИВИ РОЗВИТКУ В УКРАЇНІ

***А.С. Тарнавський,***
аспірант,
ПВНЗ «Європейський університет»

З настанням ери інформаційних технологій, основне призначення автомобіля як виробу не змінилося, однак докорінно змінилася якість виконання цього призначення. Нині автомобіль – це не просто транспортний засіб, а інтелектуальна мехатронна система, що забезпечує високий рівень комфорту, безпеки та розваги для водія та пасажирів [1].

Світовий ринок автомобільної електроніки покриває практично кожен вузол транспортного засобу. Загальний обсяг ринку електронних компонентів та програмного забезпечення для них оцінюється в межах $215-235 млрд. До 2028 року цей показник має збільшитися до $300-350 млрд. [2].

Жоден електронний виріб не несе користі, якщо його не оснащено мікроконтролером, який керує роботою конкретного вузла. Глобальний ринок мікроконтролерів має обсяг $16 млрд, але у найближчі 5 років прогнозується його потрійне збільшення до $48 млрд. Це свідчить про те, що автомобільна галузь готується до технологічного стрибка, ймовірно, запровадження доступної, масової системи повністю автономного керування (автопілот).

В Україні офіційно зареєстровано близько 5000 IT-компаній, серед яких майже 1500 стартапів. Кількість проєктів, що обслуговують винятково автомобільну галузь - 23 [3].

Розглянемо присутність українського IT серед деяких виробників світового масштабу.

| | |
|---|---|
| BMW AG | - програми для кліматичних систем;<br>- алгоритми для систем курсової стабілізації;<br>- алгоритми моделювання поведінки автомобіля в реальному часі, інтегровані з активними системами безпеки |
| STELLANTIS | - програми для систем діагностики;<br>- алгоритми для систем курсової стабілізації;<br>- контролери тиску в шинах, датчики опадів та освітлення |
| Volkswagen Group | - програмування сенсорної системи адаптивного дальнього світла IQ Light;<br>- адаптація інтерфейсу Skoda Connect |
| Hyundai Motor | - паливні мапи для ЕБК, що працюють з бензиновими та гібридними силовими установками |

Відтак, українські IT-фахівці є затребуваними у світовій автомобільній галузі та розв’язують важливі високоспеціалізовані задачі [4]. А оскільки обсяги програмних продуктів для транспортних засобів лише зростатимуть, Україна мусить подбати як про сприяння розвитку цього сектору в цілому (податкова

політика, інфраструктурні рішення, тощо), так і про підготовку спеціалістів для цієї галузі.

Основною проблемою в секторі є дефіцит кадрів і підготовка спеціалістів у закладах освіти. Наявність у молодого спеціаліста диплома – для IT-компаній не є аргументом на користь того, щоб узяти спеціаліста на роботу. Більшість таких бізнесів вибудували власні освітні та кваліфікаційні програми, завдяки яким вони відсіюють і залучають нові кадри. Відтак, долучитися до професії за наявності бажання може будь-яка людина, незалежно від її основної освіти. Відповідно до цього, молоді спеціалісти з IT-дипломом державного зразка мають стільки ж шансів отримати роботу, ніж люди без такого диплому.

Тож саме сприяння держави розвитку української IT-освіти може стати основою для подальшого зростання цього сектору і збільшення надходжень від нього до державного бюджету. Відтак, і у гравців ринку з'явиться чимало ресурсів для розширення сфер своєї діяльності та збільшення загальної частки українського IT у світовій промисловості.

*Список використаних джерел*

1. Automotive Electronics. URL: https://www.sciencedirect.com/topics/engineering/automotive-electronics

2.Automotive Electronics Market Size, Share & Trends Analysis Report By Component (Electronic Control Unit, Sensors, Current Carrying Devices), By Application, By Sales Channel, By Region, And Segment Forecasts, 2021 - 2028. URL: https://www.grandviewresearch.com/industry-analysis/automotive-electronics-industry

3.Microcontroller Market Size, Share | Industry Trends & Analysis by 2027. URL: https://www.alliedmarketresearch.com/microcontrollers-market

4. Automotive software development companies in Ukraine. URL: https://extract.co/automotive-companies/ukraine

## ПРАКТИЧНІ КЕЙСИ ТА ПЕРСПЕКТИВИ РОЗВИТКУ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ

***К.М. Троян***,
аспірант,
***О.В. Скляренко,***
к.ф.-м.н., доцент,
завідувач кафедри математичних дисциплін
та інноваційного проектування,
ПВНЗ «Європейський університет»

Технології штучного інтелекту й машинного навчання вже стали важливою частиною сучасної економічної діяльності. Саме алгоритми машинного навчання допомагають приймати оперативні рішення щодо видачі банком кредиту, релевантності реклами, надання інформації користувачам про діяльність компанії або існування та переваги певного продукту чи послуги. Алгоритми, що лежать в основі цих прикладів, стали стандартом IT галузі впродовж останнього десятиріччя, хоча були винайдені ще в минулому сторіччі.

Дослідження в галузі штучного інтелекту продовжуються й показують

перспективні результати. У 2017 році групою дослідників була опублікована стаття *Attention is All you Need*, в якій було презентовано нову архітектуру нейронних мереж під назвою трансформер (англ. *Transformer*) [1]. Ця стаття є визначною, так як спричинила своєрідну революцію в галузі обробки природних мов. На основі архітектури трансформера вже створено безліч комерційних і некомерційних продуктів, які різняться від аналізу тексту до аналізу фінансових даних, голосових асистентів й пошукових систем.

У 2021 році компанія DeepMind презентувала програму AlphaFold на основі архітектури трансформеру, яка створена для пошуку нових форм згортання білків [2]. Раніше проблема згортання білків вирішувалась методом перебору за допомогою суперкомп'ютерів або на основі розподілених систем, таких як проект Folding@Home. За допомогою штучного інтелекту AlphaFold було знайдено 200 мільйонів білкових структур, які вже використовуються для створення нових фармацевтичних препаратів [3]. А у жовтні 2022 року була презентована програма AlphaTensor, задача якої зводиться до пошуку оптимальних алгоритмів для перемноження матриць за допомогою штучного інтелекту. AlphaTensor також побудований на основі архітектури трансформера, що забезпечує пам'ять для програми, так як традиційні бази даних не підходять для вирішення цієї задачі [4]. Як результат, вперше за 50 років були відкриті нові швидкі способи перемноження матриць. Такий результат був досягнутий завдяки розкладанню задачі у вигляді гри, так як алгоритм штучного інтелекту розроблявся на комп'ютерних іграх. Ці кейси цікаві не лише тим, що показують як технології штучного інтелекту можуть рухати науку, але й тим, що на швидких тензорних операціях зараз базується вся галузь штучного інтелекту й комп'ютерної графіки, тобто, технології штучного інтелекту направлені на вирішення складних значних проблем науки, що мають вплив на всю галузь.

Подібні відкриття призводять до появи нових напрямів. Наприклад, CRM системи зі штучним інтелектом (англ. *AI enabled CRM systems*) [5], які дозволяють автоматично заносити дані клієнтів в систему й видавати менеджеру з продажів підказки в режимі реального часу під час розмови з клієнтом, що дозволяє оптимізувати й автоматизувати роботу менеджерів.

У квітні 2022 року була презентована програма Dall-E 2, яка побудована на основі алгоритму дифузійних нейронних мереж (англ. *Diffusion Neural Network*). Вона є прикладом моделі штучного інтелекту, що перекладає текстові дані в зображення (англ. *Text-to-Image Model*). Як результат, програма спроможна створювати реалістичні зображення на основі текстових запитів, домальовувати або перемальовувати окремі частини зображення [6]. Логічно припустити, що в найближчому майбутньому професія й інструментарій графічного дизайнера зазнає змін, відповідно, ефективність роботи дизайнера підвищиться. Крім цього, на основі дифузійних нейромереж вже створюються проєкти з відкритим вихідним кодом, які перетворюють текст в звук, що дозволяє створювати музику на основі текстових запитів, в той же час, такий алгоритм може бути використаний для вирішення інших проблем [7].

Наведені кейси показують основні тенденції в розвитку технологій штучного інтелекту, а саме, як з ускладненням проблем ускладнюються і підходи до їх вирішення, хоча універсальність алгоритмів машинного навчання

залишається. Наразі існує певна кількість задач, які все ще можуть бути вирішені вже існуючими технологіями, оскільки подальше вивчення та удосконалення методів та технологій вимагає технічної експертизи й чималих ресурсів для дослідження і створення нових комерційних та некомерційних продуктів. Також варто очікувати появу нових архітектур в середньостроковій перспективі.

*Список використаних джерел*

1. Vaswani, A., Shazeer, N., Parmar, N., Uszkoreit, J., Jones, L., Gomez, A. N., Kaiser, L., & Polosukhin, I. (2017, December 6). Attention is all you need. arXiv.org. Retrieved November 7, 2022, from https://doi.org/10.48550/arXiv.1706.03762

2. Jumper, J., Evans, R., Pritzel, A., Green, T., Figurnov, M., Ronneberger, O., Tunyasuvunakool, K., Bates, R., Žídek, A., Potapenko, A., Bridgland, A., Meyer, C., Kohl, S. A. A., Ballard, A. J., Cowie, A., Romera-Paredes, B., Nikolov, S., Jain, R., Adler, J., … Hassabis, D. (2021, July 15). Highly accurate protein structure prediction with alphafold. Nature News. Retrieved November 7, 2022, from https://www.nature.com/articles/s41586-021-03819-2

3. Callaway, E. (2022, July 28). 'the entire protein universe': AI predicts shape of nearly every known protein. Nature News. Retrieved November 7, 2022, from https://www.nature.com/articles/d41586-022-02083-2

4. Fawzi, A., Balog, M., Huang, A., Hubert, T., Romera-Paredes, B., Barekatain, M., Novikov, A., R. Ruiz, F. J., Schrittwieser, J., Swirszcz, G., Silver, D., Hassabis, D., & Kohli, P. (2022, October 5). Discovering faster matrix multiplication algorithms with reinforcement learning. Nature News. Retrieved November 7, 2022, from https://www.nature.com/articles/s41586-022-05172-4

5. Chatterjee, S., Mikalef, P., Khorana, S., & Kizgin, H. (2022, April 22). Assessing the implementation of AI integrated CRM system for B2C relationship management: Integrating contingency theory and dynamic capability view theory - information systems frontiers. SpringerLink. Retrieved November 7, 2022, from https://link.springer.com/article/10.1007/s10796-022-10261-w

6. Marcus, G., Davis, E., & Aaronson, S. (2022, May 2). A very preliminary analysis of dall-E 2. arXiv.org. Retrieved November 7, 2022, from https://arxiv.org/abs/2204.13807

7. Mittal, G., Engel, J., Hawthorne, C. G.-M., & Simon, I. (1970, January 1). Symbolic music generation with diffusion models. Google Research. Retrieved November 7, 2022, from https://research.google/pubs/pub50552/

## ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ ВЕДЕННЯ БУХГАЛТЕРСЬКОГО ОБЛІКУ ЗА МІЖНАРОДНИМИ СТАНДАРТАМИ ФІНАНСОВОЇ ЗВІТНОСТІ

***А.В. Федько,***
аспірант кафедри економіки, фінансів та обліку,
ПВНЗ «Європейський університет»

Відповідно до чинного законодавства частина підприємств, наприклад, публічні акціонерні товариства, зобов'язані подавати фінансову звітність відповідно до Міжнародних стандартів фінансової звітності (МСФЗ) [4].

Фінансова звітність за МСФЗ на міжнародному рівні складається та розкривається для учасників фінансового ринку – інвесторів та кредиторів, які можуть оцінити фінансові показники для прийняття економічних рішень. Тому міжнародні стандарти та звітність потрібні тим компаніям, які працюють на міжнародному ринку і хочуть залучити на своє підприємство іноземний капітал

[1]. Таким чином, виникли проблеми трансформації фінансової (бухгалтерської) звітності, складеної за національними положеннями (стандартами) бухгалтерського обліку (НП(С)БО), у звітність, що відповідає МСФЗ.

На практиці, як правило, застосовується принцип «Співвідношення між вигодами і витратами», тобто, витрати на отримання фінансової інформації не повинні перевищувати вигоди від її використання. Таким чином, формування фінансової звітності неможливе без використання програмних продуктів [5]. Автоматизація процесу звітності дозволяє досягти таких результатів:

- зменшити непродуктивну працю працівників бухгалтерії;
- мінімізувати кількість помилок через людський фактор;
- підвищити ефективність, надійність і узгодженість даних;
- використовувати цілісну систему звітності для управління підприємством.

Залежно від мети, яку переслідує підприємство щодо складання фінансової звітності за МСФЗ (юридична необхідність або вихід і ведення бізнесу на міжнародному рівні), звітність за міжнародними стандартами може бути отримана трьома способами:

- метод паралельного обліку;
- спосіб перекладу проводок;
- метод трансформації звітності.

Ці три методи відрізняються як складністю реалізації, так і якістю вихідних звітів. Найскладнішим в плані реалізації є перший спосіб – метод паралельного обліку, але тільки він здатний забезпечити найвищий рівень відповідності звітності. Метод трансформації менш трудомісткий, але похибка в оцінці фінансової звітності може бути дуже високою. Спосіб перекладу є проміжним за шкалою складність – якість.

Перший спосіб вибирають великі компанії, які прагнуть міцно утриматися на світовому ринку і мати можливість швидко отримувати і надавати абсолютно достовірні звіти за будь-який період часу відразу в двох стандартах.

Другим методом зазвичай користуються невеликі компанії, які виходять на світовий ринок, але вони не мають такої кількості облікових операцій, як великі компанії, і не вистачає фінансових ресурсів для повноцінного впровадження паралельного обліку.

Третій спосіб обирають компанії, які не зацікавлені у зовнішньому ринку, але мають періодично надавати звіт за МСФЗ відповідно до законодавства [3].

Вимога вести паралельний облік або трансформувати звітність випливає з відмінностей між НП(С)БО та МСФЗ.

Відповідно до МСФЗ, у Міжнародних стандартах бухгалтерського обліку (МСБО) немає плану рахунків, є лише назва статей, на відміну від звичайного затвердженого плану рахунків НП(С)БО. Тому підприємство само має розробити власний план рахунків для ведення бухгалтерського обліку за МСФЗ/МСБО, який би дозволяв відбирати інформацію з плану рахунків бухгалтерського обліку НП(С)БО та відносити її до рахунків бухгалтерського обліку за МСФЗ/МСБО.

План рахунків, складений за МСФЗ для кожного окремого підприємства, буде відрізнятися від інших. Структура плану рахунків залежить від багатьох факторів – від виду діяльності підприємства, від вимог до звітності, від ступеня

деталізації інформації для потреб МСФЗ.

Але при складанні плану рахунків за МСФЗ необхідно дотримуватися певних правил. Наприклад, відповідно до МСФЗ не існує такого поняття, як активно-пасивний рахунок. Кожен рахунок має дебетове або кредитове сальдо на кінець періоду. На відміну від рахунків у НП (С) БО, де сальдо деяких рахунків може потрапляти в актив чи пасив балансу залежно від того, є воно кредитовим чи дебетовим на момент складання балансу.

Відмінність МСФЗ від НП(С)БО також полягає у відображенні деяких операцій, принципі формування та групування даних. Відповідно до МСФЗ нематеріальні активи (необоротні матеріальні активи) у звітності рекомендовано відображати у групах Гудвіл, Патенти, Ліцензії, Торгові марки. У НП(С)БО Торгова ліцензія відображається як Витрати майбутніх періодів.

Якщо виходити з бухгалтерських проводок, то важливим стає період віднесення витрат/витрат на момент їх виникнення. Потрібні додаткові коригувальні записи за МСФЗ. Амортизація основних засобів за МСФЗ нараховується з моменту готовності об’єкта, а за НП(С)БО з місяця, наступного за введенням в експлуатацію [2].

Для повноти обліку може знадобитися введення додаткових операцій. Наприклад, про переоцінку основних засобів за ринковою вартістю відповідно до вимог МСФЗ.

Загалом для ведення бухгалтерського обліку та звітності в підсистемі МСФЗ повинні бути передбачені такі можливості:

- автоматичне формування проводок за МСФЗ на основі бухгалтерських проводок за НП(С)БО та формування звітів про результати конвертації;
- формування проводок за МСФЗ в ручному режимі;
- облік основних засобів та нематеріальних активів за МСФЗ (включаючи об’єкти лізингу та інвестиційну нерухомість);
- облік операцій за договорами підряду згідно з МСФЗ;
- розрахунок і визнання оцінених резервів і нарахованих зобов'язань відповідно до МСФЗ;
- облік фінансових інструментів за МСФЗ;
- облік операцій з пов'язаними особами згідно з МСФЗ;
- розрахунок відстрочених податків згідно з МСФЗ;
- розрахунок собівартості за МСФЗ;
- формування стандартної звітності за МСФЗ.

При цьому, як правило, немає необхідності розробляти підсистему МСФЗ з нуля, оскільки на ринку є програмні продукти, які надають певні можливості ведення обліку за МСФЗ, які необхідно буде адаптувати/доопрацювати враховувати специфіку та потреби конкретного підприємства. Наприклад, Система програм BAS.

МСФЗ є міжнародною мовою фінансового спілкування. Українську звітність неможливо швидко представити іноземному користувачеві. Тому одним із ключових рішень при переході на МСФЗ є питання механізму підготовки міжнародної звітності, адаптації програма безпеки системи ведення облік поява Міжнародних стандартів бухгалтерського обліку зовнішній вигляд і міжнародні фінансові стандарти звітності.

*Список використаних джерел*

1. Міжнародні стандарти фінансової звітності (International Financial Reporting Standards) Електронний ресурс]. – Режим доступу: https://mof.gov.ua/uk/mizhnarodni-standarti-finansovoi-zvitnosti https://mof.gov.ua/uk/307-international_financial_reporting_standards_archive

2. Положення (стандарт) бухгалтерського обліку 7 «Основні засоби», затверджене наказом Міністерства Фінансів України від 27.04.2000 р. N 92 (зі змінами та доповненнями) / [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/z0288-00

3. Порядок подання фінансової звітності затверджене постановою Кабінету Міністрів України від 28 лютого 2000 р. № 419 (зі змінами та доповненнями) / [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/419-2000-%D0%BF#Text

4. Про бухгалтерський облік та фінансову звітність : Закон України : від 16.07.1999 р. № 996-XIV [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/996-14

5. Про затвердження Порядку та методології проведення оцінки інвестиційного проекту із значними інвестиціями: Постанова Кабінету Міністрів України: від 08.07.2021 р. № 819 [Електронний ресурс]. – Режим доступу : https://zakon.rada.gov.ua/laws/show/819-2021-%D0%BF

## ЦИФРОВІЗАЦІЯ БІЗНЕС-ПРОЦЕСІВ ПІДПРИЄМСТВА

***О.С. Чабаненко,***
аспірант,
ПВНЗ «Європейський університет»

Сучасні підприємства знаходяться в конкурентному ринковому середовищі, яке вимагає від керівництва постійно шукати інструменти спрямовані на підвищення ключових показників ефективності підприємства. Для того, щоб бути конкурентоспроможним підприємством необхідно стежити за сучасними тенденціями і вчасно впроваджувати новації в свою діяльність. Наразі важко уявити успішне підприємство, яке не прагне цифровізувати свої бізнес-процеси для збільшення швидкості та підвищенні їх надійності.

Головна мета цифрової трансформації підприємства полягає в забезпечені простішого та ефективнішого управління бізнес-процесами за рахунок автоматизації більшості рутинних завдань. Це дозволяє працівникам підприємства фокусувати свою увагу на виконанні більш важливих і нагальних завданнях [3]. Цифрова трансформація призводить до зростання організації, збільшення доходів та підвищення іміджу підприємства, однак попри такі вагомі переваги є й певні недоліки, які описані в табл. 1.

*Таблиця 1*

**Переваги та недоліки цифрової трансформації бізнес-процесів підприємства**

| Переваги | Недоліки/складнощі |
|---|---|
| **Автоматизація.** Головним завданням автоматизації бізнес-процесів є скорочення обсягу роботи, яка виконується вручну в повторюваних процесах, щоб зробити її менш схильною до людських помилок. | **- Безпека.** Цифрова трансформація бізнес-процесів вимагає звернути особливу увагу на безпеку. Особиста інформація та фінанси підприємства постійно перебувають під загрозою кібератак. |

| Переваги | Недоліки/складнощі |
|---|---|
| **- Оптимізація.** Після проведення цифрової трансформації бізнес-процесів підприємство здатне швидше реагувати на зовнішні чинники та вчасно ухвалювати оптимальні рішення.<br>**- Нові можливості.** Хмарні технології та готові рішення значно полегшують ведення господарської діяльності підприємства.<br>**- Спрощення роботи з інформацією.** Цифровізація спрощує процес збору та обробки інформації, а також дає можливість аналізувати та зберігати величезні обсяги інформації. | **- Культурні зміни.** Зміна ролі співробітників в компанії внаслідок проведення цифрової трансформації може потребувати часу для їх адаптації.<br>**- Великий ризик.** Підприємство проводить радикальну перебудову бізнес-процесів, що несе за собою великі ризики виникнення непередбачуваних подій. |

Джерело: складено автором на основі [2].

Підприємства створюють як власні цифрові продукти для управління бізнес-процесами, так і користуються вже існуючими. На ринку цифрових продуктів представлено величезну кількість програмного забезпечення для управління бізнес-процесами, які використовують компанії по всьому світу.

Програмне забезпечення для керування бізнес-процесами – це цифровий інструмент, який дає можливість організаціям цифровізувати, стандартизувати та автоматизувати складні бізнес-процеси, зменшувати операційні витрати та забезпечувати конкурентні переваги [5].

Вибір програмного забезпечення спрямованого на цифрову трансформацію підприємства насамперед залежить від мети підприємства. Однак, при виборі програмного забезпечення також варто звернути увагу на те, яке рішення пропонується – хмарне чи коробкове, комплексна чи вибіркова система автоматизації, особливості функціоналу, наявність можливості моделювання процесів, наявність аналітики, особливості встановлення, тарифи та відгуки користувачів.

Розглянемо які рішення по цифровізації бізнес-процесів пропонуються на ринку програмного забезпечення (табл. 2).

*Таблиця 2*

**Порівняння програмного забезпечення (ПЗ) для керування бізнес-процесами**

| Назва ПЗ | Тип бізнесу | Тип розгортання | Функціонал |
|---|---|---|---|
| Monday | Малий Середній Великий | Хмарний, відкритий API | Створення власних інформаційних панелей та миттєвого відстеження прогресу, часових рамок та бюджетів, програмне забезпечення Kanban для будь-якого робочого процесу, керування файлами в одному просторі для спільної роботи в команді |
| | | | Creatio надає повний набір інструментів для ефективного управління бізнес-процесами, |

| Назва ПЗ | Тип бізнесу | Тип розгортання | Функціонал |
|---|---|---|---|
| Creatio | Середній Великий | Хмарний, локальне розміщення | включаючи моделювання, виконання, моніторинг і аналіз процесів. Дозволяє планувати роботу, завдання та зустрічі за допомогою календаря Creatio та спілкуватися безпосередньо з командою та клієнтами |
| Kissflow | Малий Середній Великий | Хмарний, відкритий API | Допомагає бізнес-користувачам автоматизувати потоки процесів, застосовувати бізнес-правила та вносити спеціальні зміни в процеси без будь-якого кодування. Легко інтегрується з іншими програмними рішеннями та стандартними програмами продуктивності |
| ProcessMaker | Малий Середній Великий | Хмарний, локальне розміщення | ProcessMaker дозволяє проєктувати, автоматизувати, розгортати бізнес-процеси та робочі процеси. Потужні рішення на базі штучного інтелекту для автоматизованої обробки документів |
| Wrike | Малий Середній Великий | Хмарний, відкритий API | Відстеження показників продуктивності співробітників, контроль циклів узгодження матеріалів, автоматизація та оптимізація з урахуванням специфіки роботи команди |

Джерело: складено автором на основі [4].

Програмне забезпечення Monday пропонує спеціальні інструменти, які надають індивідуальні рішення для широкого кола галузей. Інструменти спеціально розроблені для управління проєктами, управління маркетинговими ресурсами, CRM і продажів, віддаленої роботи, розробки програмного забезпечення, творчих завдань, будівництва, IT і HR. Платформа Creatio допомагає стимулювати зміни та прискорювати процеси в будь-якій організації, незалежно від її розміру та бізнес-моделі. Kissflow складається з низки окремих інструментів, які можуть допомогти різним відділам і організаціям, таким як відділ кадрів, закупівель і навіть навчальним закладам, оцифрувати всі їхні процеси. Унікальність програмного забезпечення ProcessMaker полягає в тому, що він пропонує рішення з відкритим кодом, локальне та хмарне розміщення. На ринку програмного забезпечення існує не так багато продуктів, які можуть запропонувати споживачам одразу всі три функції. Якщо потрібне універсальне програмне забезпечення, то одним з найкращих рішень буде використовувати Wrike, який відповідає потребам більшості організацій і відомий своїм широкими можливостями налаштування. Wrike також пропонує чудові інструменти для спільної роботи над документами, які можуть принести підприємству значну користь. Багато з цих інструментів вже інтегрували відомі корпорації і за відносно невеликі кошти суттєво підвищили ефективність діяльності підприємств [1].

Отже, цифрова трансформація бізнес-процесів може принести суттєву користь підприємству без потреби вкладання величезних інвестицій, так як на ринку програмного забезпечення представлений величезний спектр готових продуктів, які пропонують різноманітні рішення по автоматизації та оптимізації бізнес-процесів.

*Список використаних джерел*

1. *Tekic, Z., & Koroteev, D.* (2019). From disruptively digital to proudly analog: A holistic
2. *He, F., & Liu, H. X.* (2019). The performance improvement effect of digital transformation enter prises from the digital economy perspective. Reform, 4, 137-148.
3. *Martinez, F.* (2019). Process excellence the key for digitalisation. Business Process Management Journal, 25 (7), 1716-1733.
4. *Saarikko, T., Westergren, W. H., & Blomquist, T.* (2020). Digital transformation: Five recommendations for the digitally conscious firm. Business Horizons, 63 (6), 825–839.
5. *Reinartz, W., Wiegand, N., & Imschloss, M.* (2019). The impact of digital transformation on the retailing value chain. International Journal of Research in Marketing, 36 (3), 350-366.

## СОЦІАЛЬНІ МЕРЕЖІ ЯК ІНСТРУМЕНТ ПРОСУВАННЯ В ПРОФЕСІЇ ЮРИСТА

***С.О. Школьнік***
аспірант,
ПВНЗ "Європейський університет",
волонтер Житомирського місцевого центру БВПД

Коронавірус змінив спосіб життя людства, фактично трансформуючи людей в електронне суспільство. Люди стали менше спілкуватися «в живу» і більше взаємодіяти в соціальних мережах. Одним з головних чинників впливу на зміну способу життя українців, починаючи з 2020 року, виявився фактор поширення пандемії COVID-19. Велике значення для поширення інформації в сучасному світі отримали соціальні мережі. Відбувся перехід людства в електронне суспільство і Інтернет став базовим правом і потребою людини.

В період з 2010 до 2020 року поступово зникають класичні джерела інформації та відбувається їх заміна новими джерелами. Так, шпальти газет замінили пости в соціальних мережах, а перегляд телебачення змінився переглядом відео-контенту на сервісах YouTube, TikTok та інших онлайн-кінотеатрах. Також радіо почало мовлення в мережі Інтернет в онлайн форматі. Сучасна людина більше не витрачає час на прослуховування радіоприймача, перегляд телевізора чи читання газет. Фактично зазначені носії інформації припинили своє існування в останнє десятиліття. Навіть мистецтво мігрувало в мережу Інтернет. З'явились онлайн-музеї, галереї та виставки. Автори створюють та продають цифрові зображення – токени тощо.

Не може стояти осторонь і професія юриста. Юридична сфера тривалий час уникала широкого використання ІТ-технологій, хоча в інших сферах вони активно застосовуються. Поштовхом для змін стала поява пандемії COVID-19. Багато юристів та юридичних фірм тривалий час притримувались класичної

моделі поширення інформації про свою діяльність. Раніше для суспільства основним джерелом інформації про юриста або юридичну фірму було так зване «сарафанне радіо». Клієнти усно обмінювалися інформацією про отримані юридичні послуги та результати розгляду справ, чи вирішення їхніх питань. Громадяни дізнавались про юриста з вдало розміщеного оголошення поряд з його офісом та в місцевій газеті. Проте, з плином часу, ці механізми втратили ефективність. З'явились нові засоби поширення інформації та комунікацій в суспільстві – соціальні мережі.

Потенційний споживач юридичних послуг може отримати корисну для нього інформацію або поспілкуватись з фахівцем в соціальній мережі. Застосування соціальних мереж та засобів комунікацій знімає кордони щодо надання таких послуг в певному місті. Сучасний юрист може надавати консультації, готувати документи, приймати участь в засіданнях в суді, отримувати гонорар в режимі онлайн.

Для ефективного просування своїх послуг в юридичній сфері важливим є використання соціальних мереж. Найбільшого поширення в світі та Україні набули мережі Facebook, Telegram, Instagram, YouTube і TikTok. Значна кількість юридичних фірм та окремих фахівців активно застосовують ці мережі для просування свого бренду і комунікації з клієнтами. Вміння вибудувати особистий бренд або бренд юридичної фірми в соціальній мережі є не менш важливим, ніж вміння вдало виграти справу в суді.

Фахівець або фірма, які не вміють побудувати стратегію просування в соціальних мережах, приречені на кризу в своїй сфері діяльності. Те, що застосування соціальних мереж важливіше, ніж будь-коли, зрозуміли митці, навчальні платформи, заклади культури, публічні особи та політики. Для того, хто вірно перебудує життя в нових умовах, відкриваються нові безмежні можливості.

Аналізуючи можливості соціальних мереж стає зрозумілим, що сучасна аудиторія найбільш сприймає аудіовізуальний контент. Тому важливим є створення та просування в мережах YouTube та TikTok. Знову стає актуальним вміння бути красномовним та доносити думки до глядачів, вміння зацікавити аудиторію і підтримувати інтерес. Юрист повинен вести живе спілкування зі своїм майбутнім клієнтом, використовуючи онлайн-стріми як інструмент, створювати контент, який буде цікавий і доступний для широких мас. Варто уникати складності та сухості в подачі матеріалу, не боятись слідувати за світовими трендами, ініціювати глядачів залишати коментарі, брати участь в опитуваннях, вести дискусію.

Не менш важливим є і текстова інформація. Мережі Facebook та Telegram надають можливість швидко розміщувати текстові новини супроводжуючи їх фото або відео. Аудиторія може відслідковувати корисну їй інформацію і реагувати в коментарях.

Платформи Zoom або Google meet дозволяють проводити круглі столи, тренінги, семінари, конференції, що дає можливість обмінюватись досвідом у професійній сфері та поширювати інформацію серед широкого кола учасників.

Також важливим є застосування електронного інструментарію для підготовки та участі в судових засіданнях. Серед яких: сервіс електронного суду

https://id.court.gov.ua, сервіс захищеного відеоконференцзв'язку з судом https://vkz.court.gov.ua, сервіс Єдиного державного реєстру судових рішень https://reyestr.court.gov.ua, сервіс підписання документів «Центральний засвідчувальний орган» від Міністерства цифрової трансформації України https://czo.gov.ua та багато інших електронних сервісів, які необхідні для роботи юриста в сучасних умовах.

Можна очікувати, що наступним кроком буде відкриття та постійне представництво юридичних компаній в мета-світі «Horizon Worlds» від компанії Meta або подібних мета-світах. Також набудуть поширення тематики, пов'язані з розв'язанням спорів між учасниками мета-світу, захисту прав інтелектуальної власності на твори створені з застосуванням електронних технологій, в тому числі твори створені штучним інтелектом, регулювання обігу електронних грошей та криптовалют.

Отже, можна зробити наступні висновки:

1. Досягти успіху та стати «лідером думок» може кожен, хто має телефон, як інструмент для створення контенту і вміє вдало застосовувати соціальні мережі для PR та комунікації.

2. Просування особистого бренду або бренду юридичної фірми в сучасних умовах неможливе без залучення соціальних мереж.

3. Важливим є створення зворотного зв'язку з аудиторією, оцінка потреб та запитів.

4. Вміння використовувати електронний інструментарій для взаємодії з правосуддям та клієнтами дозволить скоротити витрати часу і ресурсів на участь в судових засіданнях.

5. Застосування всіх факторів наведених вище дозволить юристу не тільки «вижити» в сучасних умовах, а також бути ефективним і розвиватись.

6. Хто швидко опанує сфери електронного суспільства, той прокладе собі шлях в майбутнє в юридичній професії.

# СЕКЦІЯ ІІ

# ТРЕНДИ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ ОСВІТИ В УМОВАХ ВІЙНИ: НОВІ ВИКЛИКИ, ТЕНДЕНЦІЇ У ГАЛУЗІ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

## СУЧАСНИЙ ПОГЛЯД НА ФОРМУВАННЯ ПОЛІТИЧНОЇ КУЛЬТУРИ МОЛОДІ

***О.Ф. Артемчук,***
аспірант спеціальності "Політологія"
ПВНЗ "Європейський університет"

Сталий розвиток держави пов'язаний з формуванням політичної культури молоді. Рівень політичної культури молоді пов'язується із функціонуванням громадянського суспільства.

Особливості формування різних аспектів культури молоді розкрито у наукових працях учених О. Балакірєвої, В. Бебика, І. Галактіонової, М. Головатого, Є. Головахи, В. Дунця, О. Зеленої, О. Каретної, Н. Краснянської, Н. Колесніченко, С. Лисової, І. Мартинюка, В. Ребкало, С. Рябова та ін.

Молодь є важливою складовою сучасного українського суспільства, носієм інтелектуального потенціалу, визначальним фактором соціально-економічного прогресу. Від спрямованості молоді на те, щоб бути активною творчою силою значною мірою залежить процес державотворення. Нажаль, за останні роки в результаті непродуманої молодіжної політики держави відбулося відторгнення молодого покоління від тих культурно-історичних цінностей, якими жили і завдяки яким живе старше покоління.

Політична культура – це частина загальної культури, що включає історичний досвід, пам'ять про соціальні і політичні події, політичні цінності, орієнтації і навички, що безпосередньо впливають на політичну поведінку. У 1956 році американський політолог Х. Файнер ввів поняття «політична культура» у науковий обіг.

Політична культура – це соціальне явище, яке характеризує спосіб діяльності людей у сфері соціально-політичних відносин, це досягнутий рівень політичної зрілості й активності громадян. Її специфіка полягає в тому, що вона зумовлена конкретною історичною системою матеріальних та ідеологічних відносин і виступає як сукупність ідей, думок та потреб, якими живуть партії, нації та соціальні групи. Поняття «політична культура» може застосовуватися при визначенні соціального рівня розвитку як суспільства загалом, так і окремої людини, у цьому разі студентської молоді. С. Лисова визначає поняття «політична культура» як частину загальнолюдської культури, що визначає своє ставлення до політики, до участі в політичному житті, вона нерозривно пов'язана з політичною владою і є засобом її досягнення [5].

О. Зелена розглядає поняття «політична культура» як ставлення молодих українців до політики чи політичного процесу загалом, а також до самих себе й своєї ролі у цьому процесі [2, с. 44].

Політична культура молоді, як підкреслює В. Дунець, є відображенням всього змінного, динамічного, нестабільного, перш за все становить частину політичної культури суспільства, а вже потім ототожнюється із специфікою цієї соціальної групи [1, с. 16]. Так само і визначення «політичної культури молоді» включає в себе загальні положення «політичної культури», враховуючи при цьому вікові, психологічні та фізіологічні особливості молоді.

Соціально-економічне й духовне відродження України, як вказує Н. Колесніченко, неможливе без концентрації уваги та зусиль на вирішенні проблем молоді як майбутнього країни, гаранта суспільно-економічного прогресу, адже непорушною істиною є те, що подальший розвиток суспільства чи не найбільшою мірою залежить від забезпечення гідних стартових умов для життєдіяльності молодих поколінь [4, с. 43]. Нам імпонує думка вченої про те, що деякою мірою апатія молоді зумовлена, перш за все, тим, що реформи, які проводяться в Україні, найболючіше вдарили саме по ній, і тим, що в країні відсутня будь-яка осмислена політика щодо молоді як самостійної соціально-демографічної групи, з тим, що вона, з одного боку, не бачить необхідності будь-що кардинально змінювати в оточуючому середовищі, а з іншого – не розглядає політичну діяльність як значущу для себе, знаходячи більш перспективні способи і форми самореалізації [4, с. 43].

Молоде покоління ставиться до політики і влади як до таких, що не викликають ні захоплення, ні особливо різких негативних емоцій. Це, перш за все, виявляється у відстороненості досить значної частини молоді від політичного життя. О. Каретна акцентує увагу на тому, що здійснення реформ найболючіше вдарили саме по молоді і в країні протягом останніх років була відсутня будь-яка осмислена політика стосовно молоді як самостійної соціально-демографічної групи [3]. У довоєнний час молодь, з одного боку, не бачила необхідності що-небудь кардинально змінювати в сформованому укладі життя, а з іншого, не розглядала політичну діяльність як значиму для себе, знаходячи більш перспективні способи і форми самоствердження і особистої самореалізації.

Таким чином, продовження трансформаційних процесів у сфері суспільних цінностей та ідеалів, яке характерно для сучасного етапу розвитку українського суспільства, викликає модифікації глибинних взаємовідносин людини з державою, владою, політикою і призводить до значних змін у перебігу та формах становлення політичної культури молоді. У військовий час формується активістський тип політичної культури через інтерпретацію ставлення молоді до політики і переосмислення своєї ролі у захисті української держави.

*Список використаних джерел*

1. Дунець В. Б. Політична культура молоді в польській науковій думці: теоретико-понятійний аналіз. Вісник НТУУ «КПІ». Політологія. Соціологія. Право. Вип. 4 (20) 2013. С.14–18.

2. Зелена О. Я. Молоде покоління в координатах політичної культури України. Науковий журнал «Політикус». 2019. №6. С. 42–48.

3. Каретна О. О. Особливості молодіжної політичної культури. URL: http://app.nuoua.od.ua/archive/39_2010/75.pdf

4. Колесніченко Н. М. Політична культура молоді україни та її розвиток в умовах реформ. Наукові праці. Політологія. 2014. Т. 236. №224. С. 42–45.

5. Лісова С. проблема формування політичної культури студентської молоді на сучасному державному етапі. Актуальні проблеми навчання і виховання людей з особливими потребами: Збірник наукових праць. 2007. №2 (4). URL : http://ap.uu.edu.ua/article/547

## АНАЛІЗ КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ ПЕРЕВІРКИ ЗНАНЬ

***Р.Л. Голіян,***
***А.М. Ліщинський,***
магістранти,
Львівська філія ПВНЗ «Європейський університет»

Традиційний тест являє собою стандартизований метод діагностики рівня та структури підготовленості. У такому тесті всі співробітники відповідають на однакові завдання, протягом однакового часу, в однакових умовах і з однаковими правилами оцінювання відповідей.

Підготовку та проведення тестового контролю знань можливо розбити на наступні етапи:

I) розробка тестових запитань та відповідей на них (тестових завдань);
II) генерація достатньої кількості варіантів тестів;
III) проведення тестування;
IV) аналіз результатів тестування.

Перший етап є творчим завданням, автоматизація якого можлива лише після розробки експертної системи з дисципліни, для перевірки якої слід розробити тестові запитання. В даній роботі ці питання не розглядаються.

Другий етап можливо повністю автоматизувати як при комп'ютерному, так і при "класичному" (заповнення паперових бланків) варіантах тестування.

Для розробки варіантів тестових завдань існують спеціалізовані підсистеми у більшості сучасних програмних продуктах як для реалізації комплексного дистанційного навчання, так і в спеціалізованих тестових системах.

У більшості таких систем введення переліку тестових завдань здійснюється або безпосередньо засобами самої системи, або експортується з звичайних текстових файлів. Такий підхід утруднює включення в набір тестових завдань графічної інформації, таблиць і т. ін. Тому для автоматизації цього етапу в даній роботі при розробці Windows-застосування для генерування наборів тестових завдань застосовано COM-технологію. Оскільки текстовий редактор WORD є зовнішнім COM-сервером, то розроблене програмне забезпечення безпосередньо аналізує перелік тестових питань у Word-документі, який оформлений згідно таких правил.

1) Текст з переліком запитань має бути підготовлений у форматі Word-документу або у RTF-форматі.

2) Кожне запитання та кожен з варіантів відповідей (надалі – блок) складається з одного або декількох абзаців, і не містить порожніх абзаців. В тексті переліку запитань послідовно розташовують:

– блок з запитанням, блоки з відповідями на це запитання,

– блок з наступним запитанням

– і т.д.

Блоки між собою розділяються порожніми абзацами.

3) Малюнки, формули та таблиці довільно розташовують у блоках.

4) Запитання повинно бути виділеним жирним шрифтом (достатнім є виділення першого символу запитання).

5) Правильна відповідь повинна бути виділена червоним кольором шрифту (достатнім є виділення першого символу відповіді).

Варіанти наборів тестових запитань генеруються з одного або декількох файлів, що містять оформлені вказаним чином тестові запитання. Це дозволяє отримувати варіанти з рівномірним розподілом запитання по темам або складності, що відповідає вимогам формування педагогічних тестів.

Для збереження блоків запитань та блоків відповідей на ці запитання використовується SQL сервер MySQL 5.0.

Етапи III та IV можливо автоматизувати лише для комп'ютерного тестування. Для автоматизації етапу IV на основі CGI технології з використанням JavaScript-сценаріїв розроблене відповідне Web-застосування, що встановлюється на комп'ютер, який є Web-сервером (програмне забезпечення перевірене в середовищі Web-сервера Apach). На користувацьких комп'ютерах для проведення тестування достатньо наявності одного з Web-браузерів.

Під час тестування здійснюється контроль як за часом відповіді на одне запитання, так і за час виконання тесту в цілому. Якщо співробітник не встигне відповісти на запитання за встановлений час — він отримає за нього 0 балів. Питання, на які у співробітника не вистачило часу з загального часу, відведеного на тест – також зараховуються з нульовим балом.

Етап V також здійснюється з використанням Web-технологій. Викладач може переглянути хід тестування кожного випробуваного. Можливо переглянути: питання, відповіді, відповідь, яку обрав випробуваний та вірну відповідь.

Такий підхід до реалізації всіх етапів реалізації тестового контролю знань дозволить залучити широке коло співробітників навчальних установ як до підготовки текстових завдань, так і до проведення тестування.

## СИСТЕМА ІНФОРМАТИЧНОЇ ПІДГОТОВКИ СПЕЦІАЛІСТІВ ФІНАНСОВО-КРЕДИТНОЇ СФЕРИ ДЛЯ НОВОЇ ЕКОНОМІКИ

***Х.О. Засадна,***
к. ф.-м. н., доцент кафедри математики
та комп'ютерних дисциплін,
***Ю.І. Лозовецький,***
магістрант,
Львівська філія ПВНЗ «Європейський університет»

Розвиток «нової економіки» є важливою умовою забезпечення економічного зростання, яке відбувається головним чином не за рахунок

збільшення традиційних факторів виробництва (сировинних ресурсів, чисельності зайнятих і обсягу основного капіталу), а на основі, з одного боку, зростання кількості винаходів і їх активного впровадження в економіку через венчурний бізнес, а з іншого боку, через широке використання нових інформаційних і комунікаційних технологій. «Нова економіка» добре розвинена в США, оскільки саме в цій країні зосереджені найбільші світові корпорації інформаційних технологій – виробники напівпровідників, програмного забезпечення, комп'ютерів і мережевого устаткування. Фінансування перспективних проектів у США зіграло ключову роль у стрімкому розвитку в цій країні електронної комерції, дистанційних банківських послуг, хмарних та інших сучасних технологій [1].

Сьогодні ринкова економіка є відкритою, оскільки це є інформаційна економіка. Сучасні технології змінили уявлення про робоче місце фахівця: його офіс може знаходитися у власному домі, салоні авто, у вагоні поїзда, в кафе – поза основним робочим місцем. Адже завдяки інтернету і множинності шляхів доступу до нього будь-яка інформаційна система може бути доступна цілодобово з використанням як персонального комп'ютера, так і мобільних пристроїв.

Використання інтегрованих інформаційних технологій в економіці висуває вимоги щодо зростання професійної компетентності її учасників, зокрема працівників фінансово-кредитної сфери. Сьогодні практично триває її трансформація, пов'язана з активним впровадженням в економіку та повсякденне життя інформаційно-комунікаційних та соціально-комунікаційних технологій. На поточному етапі функціонування фінансово-кредитні установи потребують кваліфікованих працівників, які володіють сучасними інформаційними технологіями, аналізують їх використання та здатні впроваджувати нові технології.

В Україні фахівців для фінансово-кредитної сфери готує значна кількість ВНЗ, однак комплексної системи підготовки кадрів для цієї сфери в частині вивчення сучасних інформаційних технологій сьогодні не існує. Інформатична компетентність майбутнього фахівця у ВНЗ реалізується через дисципліни інформаційного циклу. На жаль, кількість таких дисциплін для студентів економічних спеціальностей щороку лише скорочується. Сучасна молодь активно використовує наявні засоби інформаційних та комп'ютерних технологій, але в умовах перебування в інформаційному суспільстві і його швидкого розвитку цього недостатньо – потрібні базові знання функціонування названих технологій, розуміння особливостей та ризиків їх використання, можливостей інтеграції.

Побудова освітніх програм бакалаврів та магістрів фінансово-кредитної сфери повинна передбачати вивчення і дослідження сучасних Інтернет-технологій. Адже фінансово-кредитні установи завжди були центрами практичних компетентностей у їх використанні. Кожен ВНЗ на свій розсуд формує навчальні плани, в яких дисципліни циклу інформатичної практичної підготовки, якими є інформаційні системи і технології, переважно належать до групи «варіативна частина». І лише «Інформатика», яка читається на першому курсі, належить до циклу «нормативні дисципліни». Безумовно, вона є базовою компонентою сучасної освіти і повноцінним загальнонауковим навчальним

предметом [2].

Сьогодні у фінансово-кредитній, обліковій та інших сферах використовуються такі види традиційних і нових інформаційних технологій: опрацювання електронних даних, автоматизоване керування, підтримка прийняття рішень, експертні системи, електронний офіс. Всі названі технології є інтегрованими, тобто мають засоби інформаційної взаємодії. Окремі технології реалізуються одним додатком, наприклад за допомогою електронного офісу. Що стосується нових інформаційних технологій, то вони використовують персональні комп'ютери і телекомунікаційні засоби та забезпечують інтерактивний режим роботи з персональним комп'ютером і мобільними пристроями, а також інтегрування більшості використовуваних програмних продуктів [3].

Щодня із засобів масової інформації отримуємо дані про зловживання у фінансово-кредитній сфері, які пов'язані з низькою грамотністю населення в частині використання інформаційних технологій. Зменшити їх кількість дозволить інформатична компетентність та інформаційна культура сьогоднішніх студентів. Чималою проблемою є також неперервність комп'ютерної підготовки протягом усього періоду навчання у ВНЗ. Вона забезпечується наявністю в навчальних планах щорічних дисциплін, пов'язаних із сучасними комп'ютерними технологіями. Адже ці дисципліни мають дуже тісні міжпредметні зв'язки і відіграють важливу роль у практичній підготовці майбутніх спеціалістів фінансово-кредитної сфери.

Отже, пропонуємо у навчальних планах ВНЗ економічного профілю перемістити дисципліни «Інформаційні системи» та «Інформаційні технології» з варіативної частини у нормативну в групу «дисципліни професійної підготовки». Далі слід доповнити навчальні програми переліком комп'ютерно-орієнтованих технологій, вивчення яких у ВНЗ зумовлене потребами фінансово-кредитної та облікової сфер: інформаційна безпека у фінансово-кредитних установах; інформаційні технологій впливу та безпечна поведінка; платіжні системи, Інтернет-комерція, IT-аутсорсинг, цифрові технології в економіці (в т.ч. електронний документообіг, Інтернет речей, хмарні технології, технології аналізу big data, бот-технології, дистанційне банківське обслуговування, ID-технології, електронний уряд, цифрові криптовалюти та ін.). Для цього слід суттєво збільшити кількість годин на вивчення дисципліни «Інформаційні технології», а ще краще – організувати вивчення окремих дисциплін на третьому і четвертому курсах ВНЗ.

Висновки. Тенденції розвитку простору інформаційної взаємодії сучасних технологій формують попит на спеціалістів у фінансово-кредитній сфері нової економіки. Пріоритетним для ВНЗ економічного профілю сьогодні є практична підготовка студента до використання сучасних інформаційних технологій. Систему інформатичної підготовки спеціалістів фінансово-кредитної сфери для нової економіки у ВНЗ слід переглянути і вдосконалити. Засоби сучасних інформаційних технологій повинні бути інструментом навчальної діяльності сучасного внз, бо вони активно впроваджуються у повсякденне життя і згодом будуть використовуватися у професійній діяльності.

*Список використаних джерел*

1. [Електронний ресурс]. – Режим доступу: http://www.industrialnet.com.ua/nova-ekonom-ka/.

2. Кухарська Н.П. Особливості навчальної дисципліни «Інформатика» / Н. П. Кухарська // Вісн. нац. ун-ту «Львівська політехніка». - Львів, 2014. - № 803: Інформатизація вищого навчального закладу. - С. 70-74. [Електронний ресурс]. – Режим доступу: http://vlp.com.ua/node/13427.

3. https://uk.wikipedia.org/wiki/Інформаційні_технології.

## СТАНДАРТИ ІНТЕЛЕКТУАЛЬНОГО АНАЛІЗУ ДАНИХ

***Х.О. Засадна,***
к.ф.-м.н., доцент кафедри математики
та комп'ютерних дисциплін,
***О.З. Піх,***
***К.В. Веретюк,***
магістранти,
Львівська філія ПВНЗ «Європейський університет»

Інтелектуальний аналіз даних (Data Mining) – це виявлення прихованих закономірностей або взаємозв'язків між змінними у великих масивах необроблених даних. Він передбачає завдання моделювання, класифікації, прогнозування та інші.

Data Mining – це також процес підтримки ухвалення рішень, заснований на пошуку в даних прихованих закономірностей (шаблонів інформації).

Технологію Data Mining достатньо точно визначив Григорій Піатецкий-Шапіро – один із засновників цього напряму: "Data Mining – це процес виявлення в сирих даних раніше невідомих, нетривіальних, практично корисних і доступних інтерпретації знань, необхідних для ухвалення рішень в різних сферах людської діяльності" [1].

Суть і мету технології Data Mining можна визначити так: це технологія, яка призначена для пошуку у великих об'ємах даних неочевидних, об'єктивних і корисних на практиці закономірностей. Неочевидних – це значить, що знайдені закономірності не виявляються стандартними методами обробки інформації або експертним шляхом. Об'єктивних – це значить, що знайдені закономірності повністю відповідатимуть дійсності, на відміну від експертної думки, яка завжди є суб'єктивною. Практично корисних – це значить, що висновки матимуть конкретне значення, якому можна знайти практичне застосування.

Наведемо ще кілька визначень терміну Data Mining:

Data Mining – це процес виділення з даних неявної і неструктурованої інформації і представлення її у вигляді, придатному для використовування.

Data Mining – це процес виділення, дослідження і моделювання великих об'ємів даних для виявлення невідомих до цього шаблонів з метою досягнення переваг в бізнесі (визначення SAS Institute).

Data Mining – це процес, метою якого є пошук нових значущих кореляцій, зразків і тенденцій в результаті просіювання великого об'єму збережених даних

з використанням методик розпізнавання зразків, плюс застосування статистичних і математичних методів (визначення Gartner Group).

Перш ніж використовувати технологію Data Mining, необхідно проаналізувати її проблеми [2]. Data Mining не може замінити аналітика, не може складати розробки і експлуатації додатку Data Mining, вимагає підвищеної кваліфікація користувача; видобування корисних відомостей неможливе без доброго розуміння суті даних. Окрім того, Data Mining характеризується складністю підготовки даних, високою вартістю, вимагає наявності достатньої кількості репрезентативних даних.

Стандарти, що мають пряме або опосередковане відношення до Data Mining, можна об'єднати в групи:

- стандарти, що базуються на послугах Data Mining (послуги створення моделі управління, скорингові послуги, послуги аналізу даних, послуги дослідження даних, статистичні послуги моделювання);
- стандарти web-служб (SOAP / XML, WSRF, і т.д), Grid-Послуги (OGSA, OGSA / DAI, і т.д.),
- семантичні стандарти Web (RDF, OWL, і т.д.).

*Стандарт CWM* включає опис базових елементів об'єктної моделі, реляційних відносин, мови XML, структури семантики предметної області, архітектури OLAP, видобування даних, технології перевантаження даних і деяких розширень. JDM – це перша спроба створити стандартний Java API (програмний інтерфейс програми) для отримання доступу до інструментів Data Mining з Java-додатків. Друга група стандартів спрямована на розробку надбудови над мовою SQL, яка дозволяла б звертатися до інструментарію Data Mining, вбудованому безпосередньо в реляційну базу даних. До цієї групи можна віднести такі стандарти: SQL / MM, OLE DB for Data Mining. Стандарт SQL/MM є набором певних процедур користувача SQL для можливостей обчислень і використання моделей Data Mining. The OLE DB for Data Mining standard of Microsoft дозволяє, застосовувати методи Data Mining в структурі реляційних баз даних. Цей стандарт є розширенням OLE DB.

*Стандарт CRISP*. CRISP-DM – стандартний процес міжгалузевої Data Mining, що є найбільш популярною і поширеною методологією. Згідно зі стандартом CRISP, Data Mining є безперервним процесом з багатьма циклами і зворотнім зв'язком. Data Mining за стандартом CRISP-DM включає такі фази: осмислення бізнесу (Business understanding); осмислення даних (Data understanding); підготовка даних (Data preparation); моделювання (Modeling); оцінка результатів (Evaluation); впровадження (Deployment). До цього набору фаз іноді додаються сьомий крок – контроль, який закмикає коло. За допомогою методології CRISP-DM Data Mining перетворюється у бізнес-процес, в ході якого технологія Data Mining фокусується на вирішенні конкретних проблем бізнесу. Методологія CRISP-DM описується в термінах ієрархічного моделювання процесу, який складається з набору завдань, описаних чотирма рівнями узагальнення (від загальних до специфічних): фази, спільні завдання, спеціалізовані завдання і запити.

*SEMMA* методологія реалізована в середовищі SAS Data Mining Solution

(SAS). Її абревіатура утворена від слів «Відбір даних» (створення вибірки), «Дослідження відносин в даних», «Модифікація даних», «Моделювання взаємозалежностей», «Оцінка отриманих моделей і результатів». Підхід SEMMA передбачає, що всі процеси виконуються в межах гнучкої оболонки, яка підтримує виконання всіх необхідних робіт з обробки та аналізу даних. Він поєднує структурованість процесу і логічну організацію інструментальних засобів, що підтримують виконання кожного з кроків. Завдяки діаграмам процесів обробки даних, підхід SEMMA спрощує застосування методів статистичного дослідження і візуалізації, дозволяє вибирати і перетворювати найбільш значущі змінні, створювати моделі з цими змінними з метою прогнозування та передбачення результатів, підтвердити адекватність моделі і підготувати модель до розгортання. Ця методологія не нав'язує жодних жорстких правил. Розробник може мати у своєму розпорядженні наукові методи побудови концепції проекту, його реалізації, а також оцінки результатів проектування.

Описані вище стандарти є методологіями Data Mining, тобто розглядають організацію процесу і розробку систем Data Mining. Крім цієї групи, існує ряд стандартів, мета яких – узгодити досягнення в Data Mining, спростити управління моделюванням процесів і подальше використання створених моделей. Ці стандарти умовно можна поділити на дві категорії: стандарти, які стосуються вироблення єдиної угоди зі зберігання і передачі моделей Data Mining і стандарти, які стосуються уніфікації інтерфейсів.

Стандарт PMML дозволяє здійснювати обмін моделями, створеними в додатках різних постачальників програмного забезпечення Data Mining. Основа цього стандарту – мова XML. Прикладом іншого стандарту, також заснованого на мові XML, є стандарт обміну статистичними даними та метаданими (PMML). Стандарт PMML використовується для опису моделей Data Mining і статистичних моделей. Основна мета стандарту PMML – забезпечення можливості обміну моделями даних між програмним забезпе

ченням різних розробників. За допомогою стандарту PMML сумісні додатки можуть легко обмінюватися моделями даних з іншими PMML-інструментами. Таким чином, модель, створена в одному програмному продукті, може використовуватися для прогнозного моделювання в іншому. Стандарт PMML включає: опис аналізованих даних (структура і типи даних); опис схеми аналізу (використовувані поля даних); опис трансформацій даних (наприклад, перетворення типів даних); опис статистик, прогнозованих полів і самих прогнозних моделей. Стандарт PMML забезпечує підтримку найбільш поширених прогнозних моделей, створених за допомогою алгоритмів і методів аналізу даних, зокрема – нейронних мереж, дерев рішень, алгоритмів асоціативних правил, кластерного аналізу, логічних правил та інших інструментів Data Mining – критерії порівняння, класифікація.

*Список використаних джерел*

1. https://ru.wikipedia.org/wiki/Data_mining
2. https://studfiles.net/preview/2045693/page:13/

# МОБІЛЬНИЙ ДОДАТОК ДЛЯ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ НАВЧАННЯ

***В.І. Коцун,***
к.т.н., доцент, завідувач кафедри математики
та комп'ютерних дисциплін,
Львівська філія ПВНЗ «Європейський університет»

Зацікавленість до інтеграції мобільних додатків в освітній процес зростає. Сьогодні потрібні такі методи навчання, які полегшували б і прискорювали передачу знань студентам, активізували процес засвоєння ними знань, навчали їх прийомам самостійної роботи з матеріалом, підвищували продуктивність навчальної праці і праці педагога. Такі методи навчання можна реалізувати на основі використання інформаційних технологій в освіті.

Мобільні технології можуть зробити процес навчання цікавішим, що відповідає вимогам сьогоднішнього дня, надаючи потрібну інформацію в потрібний час. Реалізується діяльнісний підхід, пізнавальна діяльність дитини організовується в тій формі, при якій вона самостійно відкриває для себе знання. Використання мобільних пристроїв на заняттях дозволяє розвивати вміння студентів орієнтуватися в інформаційних потоках навколишнього світу, опановувати практичні способи роботи з інформацією, розвивати вміння, що допомагають обмінюватися інформацією з допомогою сучасних технічних засобів. Основною проблемою є потреба в розробці методів і ресурсів для підтримки і навчання студентів використанню мобільних технологій.

В сучасній літературі пропонуються таке визначення мобільного навчання:

Мобільне навчання – це діяльність, здійснювана регулярно за допомогою компактних, портативних мобільних пристроїв і технологій та дозволяє слухачам курсу стати більш продуктивними, спілкуючись, отримуючи або створюючи інформацію. Аналіз літературних джерел показує, що мобільне навчання є, з одного боку, різновидом дистанційного навчання, а з іншого – електронного навчання. Але у порівнянні з цими видами навчання, мобільне навчання надає студенту вищу інтерактивність, більшу свободу руху, більшу кількість технічних засобів [1].

Багато вчених і педагогів впевнені, що майбутнє навчання з підтримкою ІКТ пов'язано і залежить саме від розповсюдження мобільних засобів зв'язку, популярності смартфонів і планшетів, появи великої кількості навчальних програм, а також нових технологій типу жестикуляційного інтерфейсу, які розширюють можливості і якість освіти, та інтеграцію мобільного навчання в систему освіти [2].

Правильно розроблені мобільні додатки допомагають підтримувати навчання в зоні найближчого розвитку за рахунок варіативності змісту навчальних завдань, способів і засобів їх вирішення та можливості оцінювання в реальному часі. В цьому і полягає актуальність роботи.

Проаналізувавши сучасний стан питання було виявлено, що використання мобільного навчання є невід'ємною частиною сучасного освітнього процесу. Дослідження джерел дозволило зробити висновок, що мобільний додаток є

оптимальним способом для підвищення ефективності процесу навчання та якості знань. З'ясовано особливості розробки мобільних додатків, які будуть використовуватися в навчальних цілях.

Встановлено проблематику процесу розроблення мобільного додатку, та запропоновано модель життєвого циклу, яка допоможе у подальшій розробці проекту. Виявлено особливості розробки додатків для операційної системи Android та здійснено вибір інструментальних засобів розробки мобільного Android-додатку.

Для розробки було обрано середовище Unity, яке орієнтоване на розробку додатків для Android, має простий і зрозумілий інтерфейс та інструментальні засоби для упаковки і маркування коду, багато помічників та шаблонів для загальних елементів програмування. У якості мови програмування було обрано C#.

*Список використаних джерел*

1. Blended learning – очно-заочное обучение для "продвинутых" [Електронний ресурс] – Режим доступу : http://www.dw.de/dw/article/ 0,,4310546,00.html.

2. Collis B. Flexible learning in a digital world: experiences and expectations / Betty Collis, Jef Moonen. – London : Kogan Page Limited, 2017. – 231 p.

## ЕЛЕКТРОННА СИСТЕМА ДОКУМЕНТООБІГУ В ЗАКЛАДАХ ЗАГАЛЬНОЇ СЕРЕДНЬОЇ ОСВІТИ УКРАЇНИ

***І.В. Литвиненко,***
магістрант факультету інформаційних систем і технологій,
***М.В. Опольський,***
ст.викладач кафедри математичних дисциплін
та інноваційного проектування,
ПВНЗ "Європейський університет"

Світ цифрових технологій, в який наразі входить Україна — це не лише новий логічний етап розвитку технологічної сфери людства, а й усієї існуючої правової та соціально-політичної реальності. Цифровізація відіграє роль найважливішого фактора економічного зростання економіки країни і загалом є сучасним трендом розвитку.

В Україні сміливо можна говорити про цифровізацію освіти, спираючись на показники цифрового портрету учня, які демонструють, що 99% мають смартфон та доступ до інтернету, 37% мають планшет, 84-94% мають комп'ютер (показник залежить від класу). Це актуальні показники на квітень 2022 року за дослідженнями Інституту цифровізації освіти НАПН України. Однак є 15% учнів, які потребують допомоги Міністерства освіти та науки щодо забезпечення гаджетами.

Цифровий портрет вчителя у сфері використання цифрових майданчиків задля підтримки зв'язку з учнями виглядає наступним чином: 42% освітян надають перевагу використанню сервісам Google class, Zoom та Viber, ще 40 відсотків використовують сервіси Office 365. Загалом вчителями було зазначено 33 сервіси, які можна використати під час дистанційного навчання, що свідчить

про високий рівень цифрової компетенції вчителів.

Спочатку пандемія коронавірусу, а згодом і війна вплинули на систему української освіти та вимагали негайного прийняття рішень щодо цифровізації всіх навчальних процесів.

Найбільш актуальним та своєчасним став електронний документообіг, а саме: ведення електронних журналів та електронних щоденників. Це значно спрощує комунікацію між адміністрацією та вчителями, між вчителями, учнями і батьками. Також дає можливість оперативно згенерувати певні документи, які необхідні учням (довідка про успішність, табель, звіт досягнень тощо). Цифровізація реалізується за допомогою використання будь-яких технічних засобів: телефони, планшети, ноутбуки, комп'ютери. Батьки легко можуть моніторити успішність своєї дитини в онлайн режимі, вчителі мають можливість спілкуватися з учнями та батьками. Корисним є формат індивідуальних батьківських зборів, що є більш продуктивним, ніж усталений формат.

Варто визначити етапи щодо впровадження електронного документообігу в школі. Для прикладу візьмемо досвід Тернопільської загальноосвітньої школи №28, де використовуються електронний журнал та щоденники.

Для початку необхідно провести опитування всіх учасників освітнього процесу, щоб дізнатися, чи вони готові до впровадження цифрових технологій в освітній процес. Надалі потрібно опрацювати отримані дані, провести бесіди освітнього спрямування з незгодними. Найважчим етапом є дотримання нормативно-правової бази, оскільки є багато законодавчих актів, що регулюють документообіг в освіті, однак ніде не зазначається можливість електронної версії. Тому закладам освіти потрібно розробляти власну правову базу, наприклад, «Інструкцію щодо ведення електронного журналу», різні положення. Далі слідує етап навчання педагогів основам роботи з електронними документами. І кінцевий етап – ознайомлення учнів та батьків із запровадженою системою.

Саме цей аспект цифровізації вимагає створення нової нормативної бази на загальнодержавному рівні.

Далі розглянемо практику, яка вже реалізується в Україні, однак ще потребує доопрацювання, значного вкладу та деталізованої розробки, – це одночасна наявність очного та дистанційного навчання. Початковою умовою є проведення опитування батьків, далі формування класів, проведення добору вчителів, розробка інтегрованого розкладу (або окремого для очного та дистанційного навчання). Також необхідно продумати використання техніки, інтернету, приміщень для онлайн зв'язку, дібрати цифровий контент, сформувати банк контактів. Важливою трудомісткою та часозатратною особливістю цифровізації освіти є створення хмарно орієнтованого середовища школи (система завдань, дистанційне завдання, оцінювання).

Ще одним викликом є необхідність оновлення вимог до друкованих підручників, а саме: включення в друковану продукцію сучасних маркерів та QR-кодів для відтворення цифрового контенту: відео, аудіо, доповненої реальності, тестів, зображень, анімації, зокрема для предметів природничого циклу. Оскільки такий контент допомагає посилити ефективність цього навчання, що є надзвичайно актуальним в умовах війни.

Також варто посилювати інтеграцію цифрового контенту у середовище

освітян, формувати у вчителів компетентності з аналізу сервісів і ресурсів саме, як педагогічного, а не технологічного інструментарію. Тобто вчителі повинні знати і розуміти, коли варто застосувати той чи інший сервіс, ресурс, функцію чи інструмент.

Під час воєнних дій найактуальнішим залишається адаптивне навчання, що включає індивідуальний підхід до кожної дитини, яка постраждала внаслідок воєнних дій, розробку індивідуальних навчальних програм та забезпечення індивідуальних темпів навчання.

Варто розпочинати роботу з системами штучного інтелекту задля удосконалення змісту освіти на засадах реалізації тематичних освітніх проєктів, що включають: робототехніку, дрони-дослідники, AR&VR, інтернет речей та інформаційну безпеку.

Наразі система освіти має першочергові завдання щодо загальнодержавного запровадження електронних журналів та щоденників, розроблених за хмароорієнтованими технологіями з можливостями функцій друку. Актуальним є також підвищення рівня цифрової компетентності вчителів, яке може бути у формі курсів підвищення кваліфікації та поглиблення зв'язку з вчителями інформатики. Одночасно цифровізація у комплексі з цифровою компетентністю вчителів дає останнім можливість використання цифрових ресурсів Електронної бібліотеки НАПН України для удосконалення науково-методичної роботи закладів освіти.

Впровадження в життя будь-яких нових технологій, зокрема цифрових є, безумовно, тривалий процес, що несе в собі масу невідомих донедавна викликів та небезпек. Однак вже чітко виділяються пріоритетні напрямки розвитку: дистанційне управління закладом освіти, забезпечення всіх учасників процесу ресурсами та інструкціями щодо користування, посилення науково-методичної роботи освітян за допомогою цифровізації. Саме за цими напрямками потрібно першочергово здійснювати цифрову трансформацію освіти в умовах війни.

*Список використаних джерел*

1. Глобальні тренди, які формуватимуть освітні тенденції у 2022 році. Дослідження ОЕСР. URL: https://nus.org.ua/articles/globalni-trendy-yaki-formuvatymut-osvitni-tendentsiyi-u-2022-r-doslidzhennya-oesr/

2. Цифрова трансформація освіти в умовах війни: антикризові рішення, можливості, плани. Міністерство освіти і науки України. URL: https://mon.gov.ua/ua/news/cifrova-transformaciya-osviti-v-umovah-vijni-antikrizovi-rishennya-mozhlivosti-plani

## СУСПІЛЬНІ ТРАНСФОРМАЦІЇ: СОЦІАЛЬНІ МЕРЕЖІ ЯК ЗАСІБ КОМУНІКАЦІЇ У ВИЩІЙ ШКОЛІ

***Г.І. Майстренко,***
аспірант кафедри менеджменту та інноваційного провайдингу,
ПВНЗ "Європейський університет"

Глобальна мережа Інтернет відкриває безмежні можливості у віртуальному просторі. Швидкість, зручність та простота, – ось ті базові принципи, яким слідує стратегія всесвітньої павутини. Збільшення ролі мережі інтернет в житті

сучасного суспільства вплинуло, в тому числі, і на систему освіти у всьому світі, змінивши, таким чином, освітню парадигму. На сьогоднішній день найбільш прогресивним інтернет інструментом в освітньому процесі є соціальні мережі, які вже зайняли власну нішу в поколінні “зумерів”. У Всесвітній доповіді ЮНЕСКО визнало це покоління як «глобальне інформаційне суспільство» [1, с. 29]. Тому в освітні стандарти всіх рівнів освіти впроваджуються інформаційно-комунікаційні технології як обов’язкова складова реформування вітчизняної освіти.

Таким чином, метою даного дослідження є аналіз особливостей соціальних мереж у формуванні комунікаційного зв’язку у вищій школі.

У стратегії розвитку вищої освіти в Україні на 2021–2031 роки вказано, що необхідно більш ефективно впроваджувати сучасні інформаційно-комунікаційні технології, що забезпечать удосконалення навчально-виховного процесу, доступність та ефективність освіти, підготовку молодого покоління до життєдіяльності в інформаційному середовищі [2].

Стратегія розвитку системи вищої освіти повинна формуватися адекватно сучасним інтеграційним і глобалізаційним процесам, тому актуальним питанням в розвитку освіти є активне включення в освітній процес сучасних комунікаційних каналів, а саме соціальних мереж, призначених для встановлення зв’язків, взаємин між людьми, розширення їх кола спілкування. Соціальні мережі – найважливіша тенденція сучасності, яка пронизує всі сфери життя мільйонів користувачів і стає їх невід’ємною частиною. Сам термін «соціальна мережа» запропонував відомий соціолог Манчестерської школи Джеймс Барнс в 1954 році ще задовго до появи Інтернету у своїй праці "Людські відносини", де також було подано кілька соціограм – візуальних діаграм, в яких кожна особа виглядала як крапка, а лінії поміж ними вказували на їх зв'язок [3].

За минулий рік кількість користувачів соціальних медіа зросла на 227 млн і станом на початок липня 2022 року досягла 4,7 млрд. За останні 12 місяців глобальна база користувачів соціальних мереж зросла більш ніж на 5% і становить 59% від загального населення планети [4]. Вибір соціальної мережі є важливим завданням при реалізації комунікаційної політики в навчальному процесі у вищій школі. Лідируючою платформою за кількістю скачуваньвідвідувать та завантажень стала TikTok, стрімко набравши 12 млн українських користувачів, переважно серед молоді. Якщо говорити про загальну статистику, то рейтинг виглядає так:

1. YouTube – 23 млн
2. Facebook – 15,6 млн
3. Instagram – 13,2 млн
4. TikTok – 12 млн

Порівняння відеохостингу YouTube та платформи коротких відеороликів TikTok зображено на рис. 1. З нього видно, що перевагу TikTok надає молода аудиторія, в той час як YouTube більше цікавить старше покоління.

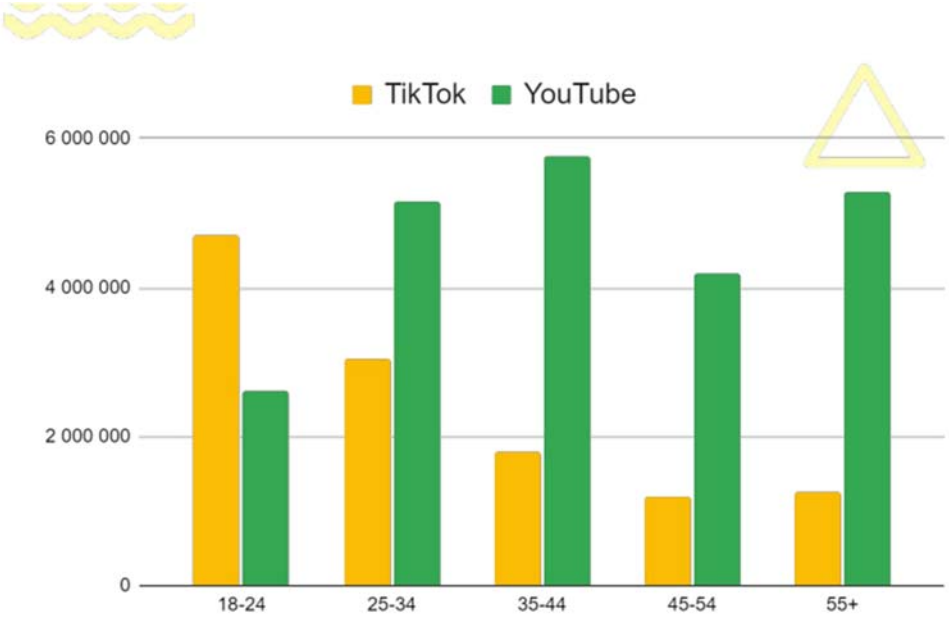



**Рис. 1 Порівняння активності YouTube та TikTok**

Така сама тенденція спостерігається у протистоянні Facebook та Instagram. Покоління до 29 років обирають Instagram, від 30+ користуються Facebook (рис. 2).

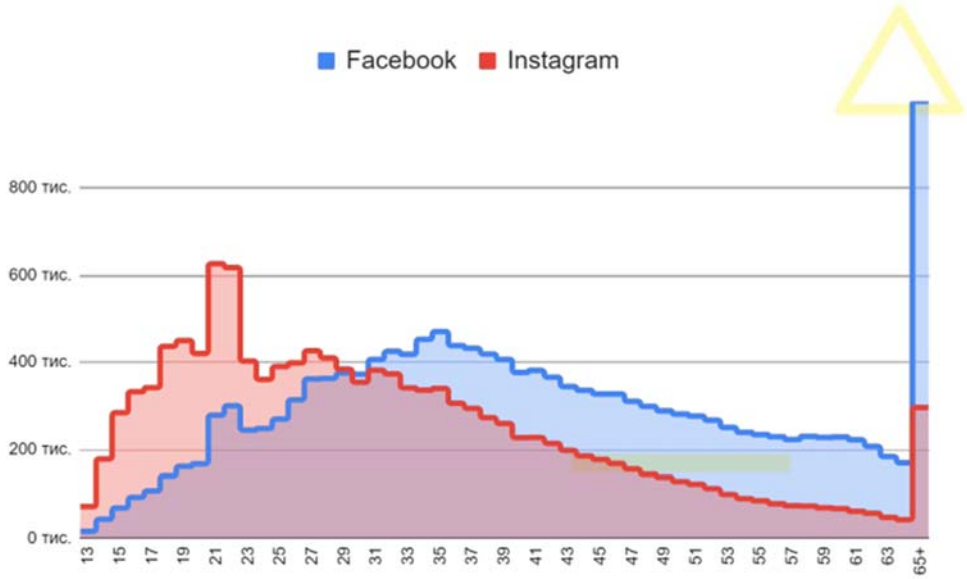



**Рис. 2 Порівняння активності Facebook та Instagram**

На даний момент Instagram та TikTok – це ті соціальні мережі, які найшвидше розвиваються у світі та цікавлять студентську аудиторію, адже їх основний контент – це зображення та відео. Як і в інших соціальних мережах тут існує можливість коментування, лайків, додавання в друзі, репостів.

Отже, для сучасного навчального процесу, відкривається широкий діапазон можливостей і форм взаємодії, різноманітні форми комунікації: прямі ефіри, форуми, опитування, голосування, коментарі та обмін цікавими й корисними посиланнями на інші ресурси. Крім того, в нинішніх умовах, комунікація в соціальних мережах дозволяє студентам в сучасному форматі бути

в курсі всіх змін, що відбуваються в процесі навчальної діяльності, відслідковувати освітню активність одногрупників і викладачів, що надзвичайно важливо при дистанційній формі навчання.

В останні роки в світовому педагогічному співтоваристві обговорюються питання розширення застосування соціальних мереж в освітньому процесі. Безумовно, соціальні мережі не можуть бути єдиним засобом мережевої комунікації, але, тим не менше, їх освітні можливості, особливо в період дистанційного навчання у вищій школі, недооцінені. Таким чином, можна зробити висновок, що соціальні мережі грають велику роль в освітньому процесі, формулюють нові структури взаємовідносин. Соціальні мережі, насамперед, відкривають широкі можливості в суспільному навчальному процесі: допомагають встановити контакт, налагодити спілкування, допомогти в самореалізації, розширити обмін інформацією в зручний для всіх час.

*Список використаних джерел*

1. United Nations Educational Scientific and Cultural Organization : Towards Knowledge Socienties. Paris : UNESCO Publishing. 2005. 226 p.

2. Про Національну стратегію розвитку вищої освіти в Україні на 2021-2031 роки : Міністерство освіти і науки України. Київ. 2020 рік. URL : https://mon.gov.ua/storage/app/media/rizne/2020/09/25/rozvitku-vishchoi-osviti-v-ukraini-02-10-2020.pdf (дата звернення : 10.11.2022).

3. Granovetter M. The Strength of Weak Ties // American Journal of Sociology. Vol. 78. № 6. 1973.

4. Укрінформ. 2022. URL : https://www.ukrinform.ua/rubric-technology/2870117-do-seredini-roku-bils-ak-polovina-naselenna-svitu-bude-koristuvacami-socmerez.html (дата звернення : 09.11.2022).

## ТРЕНДИ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ ОСВІТИ В УМОВАХ ВІЙНИ: НОВІ ВИКЛИКИ, ТЕНДЕНЦІЇ У ГАЛУЗІ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

***І.В. Маленко,***
магістрант,
ПВНЗ «Європейський університет»

Актуальність теми даної роботи зумовлена швидкими змінами парадигми сьогодення. З початком нового тисячоліття розвиток інформаційних технологій, доступний інтернет та персональні комп’ютери дали можливість отримувати інформацію та навчатись в будь-якому місці.

Епідемія COVID-19 та повномасштабне вторгнення рф 2022 року продемонстрували, наскільки важливою та актуальною є можливість продовження навчання, незважаючи на всі виклики. І тому постає питання існування відповідних цифрових платформ, які дають можливість якісно взаємодіяти студентам та викладачам.

Таку важливу тему я хотів би розглянути на прикладі системи LMS школи програмування GoIt. LMS (learning management system. Це є система організації навчання, в якій зберігаються всі учбові матеріали, студенти виконують домашні

завдання та мають можливість стежити за прогресом свого навчання. Платформа LMS персоналізована та налаштована саме під IT-навчання.

Домашня сторінка платформи зустрічає нас трьома важливими віджетами це:

1. Відвідування – показує скільки днів поспіль студент навчається. Ведеться рахунок днів при щоденному навчанні на платформі більше 15 хвилин. Це мотивує не пропускати навчання і користуватися платформою кожного дня.

2. Години навчання поточного тижня – показує кількість проведеного часу на платформі.

3. Виконані та невиконані домашні роботи.

Далі ми можемо перейти до сторінки трекінгу навчального часу. Тут ведеться статистика кількості витрачених годин студентом при роботі з системою. Також важливою та зручною функцією є відслідковування навчання за основними чотирма напрямками : робота з конспектом, завдання з автоперевіркою, час практичного кодингу та додаткові матеріали. Завдяки цьому є можливість статистично відслідковувати затрачений час та коригувати його при потребі.

Модель навчання школи це – «70/20/10»: 70% - практика, 20% - зворотній зв’язок з менторами та 10% - теорія. І тому далі переходимо до головної сторінки навчальної платформи – розділу навчання. Тут в зручному форматі зберігається:

- лаконічний конспект, який увібрав у себе основну потрібну інформацію. Також присутні теорія, практичні приклади і пошук по конспекту для зручності.
- вкладка з додатковими матеріалами від викладачів та студентів, де можна знайти велику кількість суміжної інформації.
- автоперевірка – це автоматичні міні завдання (написання коду), що перевіряються програмно.
- вкладка домашнього завдання – в ній зберігається завдання до кожної теми, перевіряються менторами та повертаються на доопрацювання, якщо є помилки.

Як бонус варто згадати про такі розділи в LMS як Турнір та Дуелі. В них студенти мають можливість в ігровій формі та формі суперництва демонструвати та тренувати свої навички і вміння, що приносить більше інтерактивності та зацікавленості в процес отримання знань.

Весь процес навчання в школі організований в онлайн форматі за допомогою відеоконференцій та корпоративного месенджера Slack, що дає змогу навчатися всім, завжди і скрізь.

Як ми бачимо на прикладі тільки цієї однієї платформи, сучасний розвиток сфери освіти дає можливість отримувати висококваліфіковані та затребувані знання усім, і потрібно лише одне – це бажання навчатися та розвивати власний професіоналізм у своїй сфері.

# ЦИФРОВІЗАЦІЯ СТУДЕНТОЦЕНТРОВАНОГО НАВЧАННЯ В УМОВАХ ЄВРОІНТЕГРАЦІЇ

***В.М. Милашенко,***
декан факультету інформаційних систем та технологій,
***В.В. Суслін,***
магістрант факультету інформаційних систем та технологій,
***А.І. Манолі,***
студентка факультету інформаційних систем та технологій,
ПВНЗ "Європейський університет"

Захищаючись від агресії та терору рф, українське суспільство разом із світовою спільнотою проявляє стійкість і бажання до системної інтеграції на основі загальнолюдських цінностей. Вища освіта відіграє важливу роль у підтримці соціального згуртування та економічного розвитку. Зростання вимог до навичок та компетентностей вимагає від вищої освіти реагувати по-новому.

Розширення доступу до вищої освіти надає можливість використовувати все більш різнорідний індивідуальний досвід. Відповідь на різноманітність і зростаючі очікування вимагає фундаментальних змін у її наданні. Це потребує більш студентоцентрованого підходу до навчання і викладання, включаючи гнучкі освітні траєкторії та визнання компетентностей, набутих поза формальними освітніми програмами.

Вища освіта спрямована на досягнення багатьох цілей, включаючи підготовку студентів до активного громадянства, до їх майбутньої кар'єри (наприклад, сприяючи розвитку їх здатності до працевлаштування), підтримку їх особистого розвитку.

Студентоцентроване навчання і викладання відіграють важливу роль у стимулюванні мотивації студентів, їх самоаналізі та залученні до освітнього процесу.

Ключові підходи до студентоцентрованого навчання і викладання:

• повага і врахування різноманітність студентів та їх потреби, уможливлюючи гнучкі навчальні траєкторії;

• врахування та використання різні способи надання освітніх послуг, якщо це доцільно;

• гнучке використання різноманітних педагогічних методів;

• регулярне оцінювання та коригування способів надання освітніх послуг і педагогічних методів;

• підтримання відчуття автономності у того, хто навчається, водночас забезпечення йому відповідний супровід і підтримку з боку викладача;

• сприяння взаємній повазі у стосунках «студент-викладач»;

• наявність належних процедур для розгляду скарг студентів.

Велику роль для прогресу студентів має також стимулююче оцінювання.

Бажано послідовно застосовувати визначені наперед та опубліковані інформаційні блоки та інструкції, що охоплюють усі стадії «життєвого циклу» студента, наприклад, зарахування, досягнення, визнання та атестацію .

Забезпечення умов і підтримки, необхідних для досягнення студентами

прогресу у своїй академічній кар'єрі, відповідає інтересам кожного студента та університету.

Необхідно постійно впроваджувати процеси та інструменти для збору і моніторингу інформації щодо прогресу студентів і вжити відповідних дій на основі цієї інформації.

Визнання кваліфікацій, неформального та інформального навчання, є важливими складовими забезпечення прогресу студентів у навчанні.

Університет прагне забезпечити загальну підтримки студентів і, зокрема, персональну підтримку у формі наставників, радників та консультантів. Роль послуг підтримки має особливе значення у сприянні мобільності студентів. Потреби різноманітного студентського контингенту, а також перехід до студентоцентрованого навчання і гнучких методів навчання і викладання, враховуються при наданні навчальних ресурсів і підтримки студентам.

Підтримка студентів і ресурсне забезпечення можуть бути організовані у різний спосіб залежно від умов в університеті. Поряд із цим, внутрішнє забезпечення якості гарантує, що всі ресурси відповідають цілям, є загальнодоступними, а студенти поінформовані про наявність відповідних послуг.

Інформаційний менеджмент для належної підтримки студентів потребує постійного вдосконалення. Пропонується створення спільної інформаційної служби факультету та університету, яка може включати представників адміністрації та студради. Можна виділити два основні напрями: по перше, загальна інформаційна підтримка (спільні інформаційні блоки, довідники та інструкції), по-друге, персональна інформаційна підтримка (структурована персональна веб-папка із правильним регулюванням доступу). Цей підхід може поступово систематизуватися і вдосконалюватися шляхом використання сучасних цифрових інструментів та технологій.

*Список використаних джерел*

1. Стандарти і рекомендації щодо забезпечення якості в європейському просторі вищої освіти (ESG). URL: https://www.britishcouncil.org.ua/sites/default/files/standards-and-guidelines_for_qa_in_the_ehea_2015.pdf (дата звернення: 1.11.2022).

2. INTERNATIONAL TRENDS AND INNOVATION IN CAREER. European Training Foundation, 2020 GUIDANCE https://www.etf.europa.eu/sites/default/files/2020-11/innovation_in_career_guidance_vol._1.pdf (дата звернення: 1.11.2022)

## ВДОСКОНАЛЕННЯ ЦИФРОВОГО ОСВІТНЬОГО ПРОЦЕСУ В УМОВАХ ВІЙНИ

***В.С. Одінцов,***
студент факультету інформаційних систем та технологій,
***Н.М. Волкова,***
викладач кафедри математичних дисциплін
та інноваційного проектування,
ПВНЗ «Європейський університет»

Розвиток освітньої галузі в Україні шляхом використання цифрових технологій є ключовим засобом забезпечення широких можливостей вільного

розвитку особистості, про що йдеться в Законі України «Про освіту», Концепції реалізації державної політики у сфері реформування загальної середньої освіти «Нова українська школа» на період до 2029 року тощо [3].

Однак, напад Росії на Україну, що супроводжується варварськими бомбардуваннями міст, які є науково-освітніми центрами, спричинив розвиток кризових процесів в системі освіти. Це проявляється в тому, що традиційні методи ведення освітнього процесу неможливо застосувати, оскільки фактично знищена матеріальна база, а викладачі і студенти внаслідок вимушеної евакуації знаходяться у різних регіонах країни чи навіть за кордоном [2].

В цих умовах, одним з дієвих способів швидкого відновлення навчального процесу в освітніх закладах є цифрова трансформація усіх аспектів освітньої діяльності. В цьому напрямку накопичено певний позитивний досвід, оскільки в умовах пандемії COVID-19 значна їх частина впровадила в освітній процес сучасні інформаційні комп'ютерні технології [1].

Наявна практика свідчить, що цифровізація дозволяє вести освітній процес в умовах значних пошкоджень матеріальної бази та неможливості забезпечити фізичну присутність викладачів і студентів на заняттях. Необхідною умовою застосування сучасних цифрових комп'ютерних технологій є наявність у студентів і викладачів гаджетів (смартфонів, ноутбуків тощо) з доступом до мережі Інтернет, у т.ч. мобільного інтернету [2].

Проте в умовах сучасних реалій більша частина території України зіткнулась з новою проблемою – систематичною відсутністю електроенергії та навіть аварійним відключенням на невизначений термін, що унеможливлює мати повноцінний безперебійний доступ до мережі Інтернет та бути присутніми при освітньому процесі онлайн. Виконання домашніх завдань та опрацювання пройденого матеріалу також стає важко доступними.

Саме тому з'явилась необхідність трансформації освітнього процесу та пошуків нових шляхів вирішення цих проблем. Наразі до віддаленого доступу до розкладу занять, віддаленого доступу до бібліотечних ресурсів та можливості дистанційного проведення занять має додатись обов'язковий відеозапис не тільки лекційної частини навчання, а й практичних занять. Саме цей тип занять потребує максимального вдосконалення, адже є найбільш дієвим способом засвоєння матеріалу та має найвищу продуктивність.

В умовах відсутності електроенергії найбільш дієвим способом навчання є мобільний телефон, який може працювати довгий період часу та має доступ до мобільного інтернету. Наразі повна адаптація до всіх вищезазначених методів освітнього процесу відсутня, а, отже, подальші дослідження мають бути спрямовані на створення мобільних додатків для виконання практичних робіт широкого спектру.

*Список використаних джерел*

1. Ілляшенко С.М., Шипуліна Ю.С. Застосування гаджетів на практичних заняттях з маркетингу // Вища освіта за новими стандартами: виклики у контексті діджиталізації та інтеграції в міжнародний освітній простір: матеріали наук.-метод. Інтернет-конф., м. Харків, 25 бер. 2021 р. / ХНАДУ. Харків, 2021. С. 33-34. URL: https://dl.khadi.kharkov.ua/course/view.php?id=2342

2. Ілляшенко С.М., Шипуліна Ю.С., Ілляшенко Н.С. Цифрова трансформація освітньої

діяльності закладів вищої освіти України в умовах війни: матеріали Міжнар. наук.-метод. конф., 10 травня 2022 р. / Харків. нац. автомобільно-дорожній ун-т. Електрон. текст. дані. Харків, 2022. С. 7-10. URL: https://drive.google.com/file/d/1rkQRD3BxwdE8pu0DJ33Brw2cU_xCzpJF/view, вільний (дата звернення 20.05.2022 р.).

3. Концепція «Нова українська школа». URL: https://mon.gov.ua/storage/app/media/zagalna%20serednya/nova-ukrainska- shkolacompressed.pdf (дата звернення: 31.04.2020).

# МЕТОДИКА ФОРМУВАННЯ ДИСТАНЦІЙНИХ КУРСІВ З ДИСЦИПЛІН КАФЕДРИ

***П.П. Пристайко,***
магістрант,
Львівська філія ПВНЗ «Європейський університет»

Описано запропонований автором підхід до формування дистанційних курсів кафедр, який дозволяє мінімізувати дисковий простір та забезпечує полегшення модифікації дистанційних курсів кафедри.

В роботі розглянуті результати удосконалення дистанційних курсів кафедри комп'ютерних наук, що здійснені в результаті проведення сумісних досліджень викладачами кафедри. Такі удосконалення можуть бути корисними і при формуванні дистанційних курсів іншими ВНЗ.

Перше удосконалення дозволяє формувати курси кафедри з використанням загальнокафедральних ресурсів.

Наявність таких ресурсів вимагає створення загальнокафедральної бази ресурсів. Для формування бази ресурсів утворено користувача kn, що є менеджером всіх курсів кафедри КН. База даних ресурсів кафедри зберігається в особистих файлах даного користувача. При потребі звернення до загальнокафедральних ресурсів в одному з курсів кафедри, користувач kn надає цьому курсу право використовувати посилання на потрібний ресурс.

Така ієрархічна організація дистанційних курсів кафедри КН дозволяє:

1. Заощаджувати дисковий простір серверу дистанційного навчання.
2. При модернізації ресурсів змінювати їх в єдиному місці — особистих файлах користувача kn. Ця зміна автоматично оновить цей ресурс в усіх курсах кафедри.

Друге вдосконалення пов'язане з оформленням навчальних матеріалів дистанційних курсів.

Оформлення цих матеріалів визначається темою Moodle [1,2], що обрана для сайту дистанційного навчання. Оформлення деяких елементів конкретного курсу (наприклад, таблиць) за цією темою може виявитись не оптимальним. В такому випадку адміністратор сайту надає автору курсу права на його оформлення іншою темою. Це дозволяє оформити елементи курсу у форматі, який найбільше відповідає вимогам до оптимального засвоєння навчальних матеріалів.

*Список використаних джерел*

1. http://rumoodler.com/course/view.php?id=13.
2. https://moodle.org/mod/data/view.php?id=8172.

# ТОТАЛЬНА ЦИФРОВІЗАЦІЯ ОСВІТНЬОГО ПРОЦЕСУ НЕВІДВОРОТНА

***В.С. Сольський,***
адвокат, арбітражний керуючий,
аспірант ПВНЗ «Європейський університет»

Цифровізація і цифрова трансформація в сучасній освіті вже не тренд, а об'єктивна вимога сьогодення.

Технологічна та цифрова модернізація інфраструктури усіх закладів освіти, від початкової школи, до закладів післядипломної освіти, повинна бути одним із першочергових пріоритетів.

Якісний прорив у цифровій трансформації освіти неможливий без розвитку цифрової компетентності педагогічних, науково-педагогічних та адміністративних кадрів всієї системи освітнього процесу.

Зусилля наукового середовища мають бути спрямовані на створення якісного освітнього контенту у нових формах.

Цифрове освітнє середовище повинно бути максимально безпечним для його учасників.

Цифровізація освітнього процесу зробить його дешевшим і доступнішим для мешканців віддалених та важкодоступних регіонів (за умови належного рівня інтернетизації).

Описані вимоги викликають необхідність законодавчих змін для якісної та ефективної цифрової трансформації.

Нові для України форми дистанційної освіти повинні отримати продовження застосування і розвиток не лише в умовах воєнного стану і ковідних обмежень, але й після завершення війни та пандемії.

*Список використаних джерел*

1. *Арешонков В. Ю.* Цифровізація вищої освіти: виклики та відповіді. Вісник НАПН України. 2020. № 2 (2). С. 1-6.

2. *Духаніна Н. М., Лесик Г. В.* Цифровізація освітнього процесу: проблеми та перспективи. The 12th International scientific and practical conference "Modern directions of scientific research development" (May 18-20, 2022), Chicago, USA. - Chicago : BoScience Publisher, 2022. - P. 406-409.

3. *Колеснікова І. В.* Цифровізація освітнього процесу в закладі післядипломної педагогічної освіти. Науковий часопис Нац. пед. ун-т імені М.П. Драгоманова. Серія 5. Педагогічні науки: реалії та перспективи, 2020. Випуск 78. С.117-120.

4. *Кучерак І. В.* Цифровізація та її вплив на освітній простір у контексті формування ключових компетентностей. Інноваційна педагогіка. Випуск 22. Т. 2. 2020. С. 91-94.

# ЦИФРОВА ТРАНСФОРМАЦІЯ ОСВІТИ В УМОВАХ ВІЙНИ: ДО ПИТАННЯ АКТУАЛЬНОСТІ ОНЛАЙН-ОСВІТИ

***Д.М. Троян,***
магістрант факультету
інформаційних систем та технологій,
ПВНЗ «Європейський університет»

Найбільш значимими викликами останніх років для абсолютної більшості сфер людської діяльності, зокрема, і в сфері вищої освіти, стали глобальна пандемія коронавірусу та повномасштабна війна РФ проти України. Відповіддю на ці виклики є адаптація освітнього процесу до екстремальних умов роботи. Поставимо собі за мету не дати об'єктивну оцінку процесу цифрової трансформації освіти в умовах війни (це неможливо зробити, оскільки процес цифрової трансформації наразі не є завершеним), проте розглянути деякі тенденції в цифровій трансформації освіти та можливі перспективи їх розвитку. Цифрова трансформація у сфері освіти і науки – це комплексна робота над побудовою екосистеми цифрових рішень у сфері освіти та науки, включно зі створенням безпечного електронного освітнього середовища, забезпеченням необхідної цифрової інфраструктури закладів та установ освіти і науки, підвищення рівня цифрової компетентності, цифровою трансформацією процесів та послуг, а також автоматизацією збору і аналізу даних [1]. В Україні цей процес триває вже тривалий час. Так, зокрема, рішенням Кабінету Міністрів України №67-р від 17 січня 2018 року було затверджено «Концепцію розвитку цифрової економіки та суспільства України на 2018–2020 роки» та затверджено план заходів щодо її реалізації. Ця концепція передбачає здійснення заходів щодо впровадження відповідних стимулів для цифровізації економіки, суспільної та соціальної сфер, усвідомлення наявних викликів та інструментів розвитку цифрових інфраструктур, набуття громадянами цифрових компетенцій, а також визначає критичні сфери та проекти цифровізації, стимулювання внутрішнього ринку виробництва, використання та споживання цифрових технологій [2].

Найбільш характерною тенденцією в адаптації навчальних закладів до нових реалій є масове переведення освітнього процесу в онлайн - рішення, яке могло бути прийняте ще задовго до початку пандемії (передумови, необхідні для онлайн-навчання, а саме – всі необхідні технічні засоби, такі як Zoom, Microsoft Teams Google і Meet Google Class існували і використовувались задовго до першого зафіксованого випадку COVID-19 в грудні 2019 року), але здавалося неактуальним в інших, менш екстремальних умовах. Нові реалії виступили каталізатором змін в освітньому процесі, передумови яких були закладені ще задовго до вищезазначених подій. Так, зокрема, Стенфордський університет відкрив доступ до власних онлайн-курсів ще в 2011 році [3]. Подібні курси у відкритому доступі мають Єльський [4] і Гарвардський [5] університети. На платформі Coursera [6] з 2012 року розміщуються тисячі курсів з різних напрямків знань від провідних університетів світу. В таких умовах формальній освіті стає все складніше конкурувати з неформальною.

Розглянемо практичні наслідки від переведення навчального процесу в онлайн. Ця тенденція, що протягом останнього часу набула масового характеру в Україні, хоч і спричинена дією на навчальний процес несприятливих обставин непереборної сили, проте, ймовірно, є незворотньою. Зокрема, перехід на онлайн-навчання має суттєві економічні наслідки для закладів освіти: більше немає необхідності в утриманні та обслуговуванні навчальних корпусів з аудиторіями, їх опалюванні в зимовий період тощо. Таким чином, з переходом освітнього процесу в онлайн вивільняються значні грошові та людські ресурси, внаслідок чого вартість навчання може стати більш доступною. Також зникає необхідність в щоденних переміщеннях студентів і педагогів до місця навчання чи роботи, а отже – більш вільний графік, більше можливостей поєднувати роботу і навчання, відтак – підвищується доступність освіти. Крім того, онлайн-навчання вирішує проблему гуртожитків і необхідності для студентів з інших міст переїжджати на період навчання до місць розташування навчальних закладів. Всі вище перелічені чинники призведуть до більшої доступності освіти. Університет без навчальних корпусів може стати реальністю вже найближчим часом. Перехід на навчання виключно в онлайн-режимі, ймовірно, стане серйозним викликом для університетів, оскільки значно посилить конкуренцію між університетами – за відсутності територіальних та фінансових чинників найістотнішою конкурентною перевагою стане якість освіти. В той же час якісна освіта стане більш конкурентною і, водночас, доступнішою: при переході на модель онлайн навчання, наприклад, студентам з інших країн вже немає необхідності переїжджати до країни розташування університету, чим знімаються численні економічні, мовні та культурні бар'єри, подолання яких було необхідною умовою в процесі отримання освіти за кордоном. Відповідно, кількість університетів вже в найближчому майбутньому може значно скоротитись внаслідок необхідності пристосування до роботи в нових умовах і зростаючої конкуренції.

Таким чином, можна зробити висновок, що цифрова трансформація в освіті носить незворотній характер, і, вже найближчим часом, можуть з'явитися університети без аудиторій, або, навіть, повністю віртуальні університети, подібно до того, як кількома роками раніше з'явилися, наприклад, банки без відділень, сама ідея яких не могла бути реалізована поза цифровою трансформацією. Потрібен певний час, аби подолати скепсис, що існує в суспільстві з приводу якості онлайн-освіти. Цей скепсис буде подолано лише коли сьогоднішні студенти, які вже навчаються виключно в онлайн-режимі, зарекомендують себе як фахівці своєї справи.

*Список використаних джерел*

1. https://mon.gov.ua/ua/tag/cifrova-transformaciya-osviti-ta-nauki
2. Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки та затвердження плану заходів щодо її реалізації [Електронний ресурс] – Режим доступу: http://zakon0.rada.gov.ua/laws/show/67-2018-%D1%80
3. https://online.stanford.edu/free-courses
4. https://oyc.yale.edu
5. https://www.harvardonline.harvard.edu
6. https://www.coursera.org

# ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ДЛЯ МОДЕЛЮВАННЯ НЕЙРОННИХ МЕРЕЖ

***Н.П. Хрущ,***
***В.В. Ревула,***
магістранти,
Львівська філія ПВНЗ «Європейський університет»

Програмою моделювання нейронної мережі (НМ) зазвичай називають програму-імітатор або нейропакет, маючи на увазі програмну оболонку, яка емулює для користувача середовище нейрокомп'ютера на звичайному комп'ютері.

До основних парадигм нейронних мереж відносять наступні: Adaptive Neuro-Fuzzy Inference System (ANFIS) – нечітка нейронна мережа; ART-1, ART-1 Network – штучний резонанс 1,2; BAM Network – двонаправлена асоціативна пам'ять; Boltzmann Machine – Больцманівське навчання; Back Propagation – обернене поширення; Cognitron – когнітрон; Counter Propagation – мережа зустрічного поширення; Delta-Bar-Delta (DBD) Network – мережа Delta-Bar-Delta; Elman and Jordan Network – частково-рекурентні мережі Елмана і Жордана; Extended BDB Network – розширена BDB мережа; Feed-Forward MAXNET – мережа пошуку максимуму з прямими зв'язками; Gaussian Classifier – Гаусів класифікатор; Genetic Algorithm – генетичний алгоритм; Hamming Network – мережа Хеммінга; Hopfield Network – мережа Хопфілда; Instar Network – вхідна зірка; Kohonen Network – мережа Кохонена; MAXNET – мережа пошуку максимуму; Neocognitron – неокогнітрон; Outstar Network – вихідна зірка; Radial Basis Function Network – мережа радіальної основи; Simulated Annealing – модельований відпал; Single Layer Perceptron – одношаровий персептрон.

У даний час на ринку програмного забезпечення присутні дуже різноманітні програми для моделювання нейронних мереж в різних операційних середовищах. За даними журналу «Нейрокомп'ютер» (Росія) до найбільш потужних зарубіжних нейропакетів належать: NeuroSolutions Neuro фірми Dimension Inc., NeuralWorks Professional II/ Plus з модулем UDND фірми NeuralWare Inc., Process Advisor фірми AlWare Inc., NeuroShell 2 фірми Ward Systems Group, BrainMaker Pro фірми California Scientific Software. Оцінювання проводилось за показниками нейропакетів, пов'язаними з можливостями використання різних нейронних структур, критеріїв оптимізації і алгоритмів навчання мереж, а також за простотою використання нейропакетів і наочністю представлення інформації. До показників, які відображають можливості нейропакетів, були віднесені наступні:

1) простота створення і навчання нейронної мережі, інтуїтивно зрозумілий інтерфейс;
2) простота підготовки навчальної вибірки;
3) наглядність і повнота представлення інформації в процесі створення і навчання нейронної мережі;
4) кількість реалізованих стандартних нейропарадигм, критеріїв і алгоритмів навчання нейронної мережі;

5) можливість створення власних нейронних структур;
6) можливість використання власних критеріїв оптимізації;
7) можливість створення власних алгоритмів навчання нейронної мережі;
8) простота обміну інформацією між нейропакетом та іншими додатками операційної системи;
9) відкритість архітектури, тобто можливість розширення нейропакета за рахунок власних програмних модулів;
10) можливість генерації вихідного коду;
11) наявність макромови для прискорення роботи з нейропакетом.

Перші три показники є важливими для початківців при користуванні нейропакетами, наступні п'ять  для досвідчених користувачів, які розв'язують конкретні прикладні задачі, а останні п'ять показників є визначальними при створенні інтегрованих нейронних інструментальних систем на базі нейропакетів і є вагомими для професійних розробників і програмістів.

Результати оцінювання нейропакетів за вказаними показниками у десятибальній шкалі наведені у наступній таблиці.

| Пакети | Показники | | | | | | | | | | | Сумарна оцінка |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | |
| NeuroSolutions Neuro | 9 | 9 | 10 | 8 | 10 | 8 | 10 | 10 | 10 | 10 | 10 | 104 |
| NeuralWorks Professional II/ Plus з модулем UDND | 9 | 9 | 9 | 10 | 8 | 7 | 7 | 8 | 10 | 10 | 0 | 87 |
| Process Advisor | 8 | 7 | 7 | 5 | 5 | 0 | 3 | 5 | 3 | 0 | 0 | 43 |
| NeuroShell | 10 | 8 | 6 | 8 | 5 | 0 | 0 | 8 | 2 | 10 | 0 | 57 |
| BrainMaker | 6 | 7 | 4 | 6 | 5 | 0 | 4 | 5 | 0 | 0 | 0 | 37 |

## MACHINE LEARNING AND TEXT MINING IN REALIZATION OF CLASTERING OF NEWSPAPER NOTES

***V.V. Tretynyk,***
assoc. prof., PhD
National Technical University of
Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"

Text clustering is an effective approach to collect and organize text documents into meaningful groups for mining valuable information on the Internet. The data we receive from the Internet is usually raw, unstructured. Therefore, there is an urgent task of creating intelligent systems that allow extracting knowledge from unstructured information, to somehow consolidate the flow of data using methods of classification and clustering of the initial text, thereby facilitating the interpretation of this text. Text

mining, which is part of a more general concept of intelligent data analysis or Data mining, deals with the automated search for extracting useful information from text documents. Webpages, microblogs, and social networks provide much useful information for us, and text clustering is an important text mining method to collect valuable information on the Internet. Text clustering helps us to group an enormous amount of text documents into small meaningful clusters, which have been used in many research fields such as sentiment analysis, text classification, text summarization.

Before analyzing text data, it is necessary to carry out preprocessing. It includes the following stages: tokenization, stemming or lemmatization, removal of stop words, frequency analysis of word forms based on vector model technologies.

One of the common forms of intelligent data analysis is the categorization of texts, that is, the assignment of a text to one or another class or category. Here, clustering methods can be used when there is no a priori information about the classes of documents under consideration. As a rule, in the process of clustering, a vector of topics is compared to each document, which determines the weighting measure of correspondence to each cluster.

Clustering methods [1] are divided into hierarchical and non-hierarchical. In the hierarchical method [4], sequential detailing of texts by context is implemented. In non-hierarchical methods, the set of all texts is divided into a given number of non-intersecting clusters. The formal formulation of the clustering problem is as follows: we have a sample $S^l = \{s_1, \dots, s_l\}$ and a distance function between objects $\rho(s, s)$. It is necessary to divide the sample into subsets that will not overlap and that each cluster consists of objects that are close in terms of metrics $\rho$, while objects of different clusters are significantly different. Therefore, each object $s_i \in S^l$ is assigned a cluster number $t_i$. Thus, the clustering algorithm is a function $f: S \to T$ that matches each object with a cluster label $t \in T$.

Ensemble clustering is another clustering algorithm. Ensemble clustering combines the multiple results of different clustering algorithms to obtain final results. Multiview clustering is an extension of ensemble clustering and combines different data that have different properties and views. Matrix factorization-based clustering is an important clustering approach [7] that can be successfully used for text clastering.

Machine learning models that use text clustering need to translate text into a vector representation. The simplest representation is a Bag-of-words [3]. This representation is simple to implement, but has disadvantages: it does not take into account either the syntax or the context of the word. This model only calculates the frequency characteristics of the word in the document. More progressive is the Tf-idf ( term frequency-inverted document frequency) method [3], which normalizes the frequency of the word in this document taking into account the frequency of its appearance in other documents. But the best vector implementation of words is realized by Word2Vec [6] and GloVe models in which the word is a vector in space in such a way that the vectors of similar words are next to each other. The cosine measure can be chosen as a measure of the distance between vectors.

In this paper we carry out the clastering of text that has written in Arabic. We have analyzed 31000 papers from Arabic newspapers (Saudi Newspapers Corpus). The papers divided by clasters according to the topic. The system of intelligent analysis of these papers is represented on Fig.1.

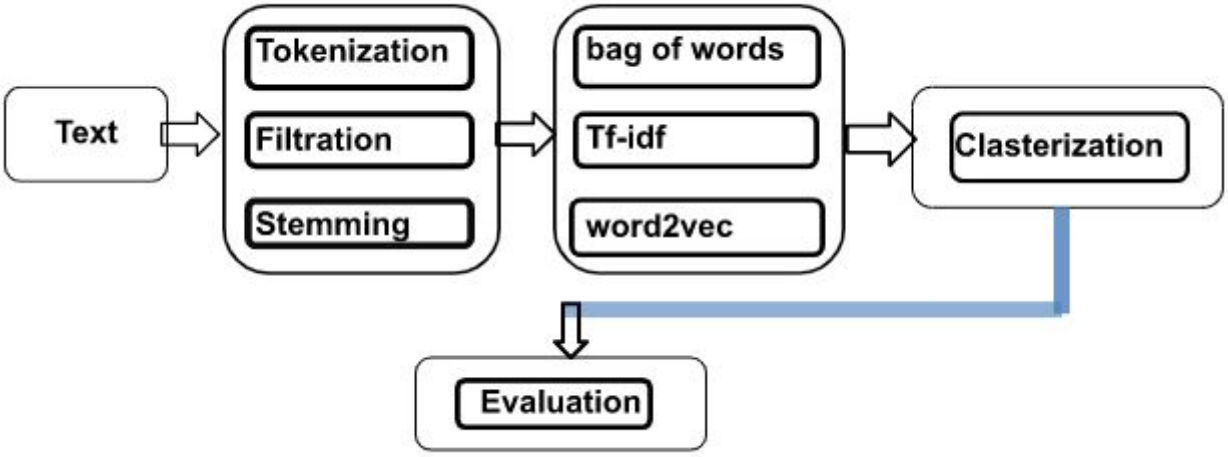



**Figure 1. System of clasterization**

The program WEKA (Waikato Environment for Knowledge Analysis) was used for realization of the problem. It has graphical interface for model projection. There are components for preprocessing, clasterization, deep learning, and visualization. This tool is suitable for quickly model prototyping and then it is possible to integrate these models in Java, R, Python.

Thus we have classified a number of Arabic newspapers, classifying their information to make it easier for users to obtain the information they want, which has worked on getting the most results in the shortest time that are close to the input we have given.

*References*

1. *Agrawal, R., Gehrke, J., Gunopulos, D., & Raghavan, P.* (1998). Automatic subspace clustering of high dimensional data for data mining applications, Vol. 27, No. 2, pp. 94-105.

2. *P. Achimugu, A. Selamat, R. Ibrahim,* A clustering based technique for large scale prioritization during requirements elicitation, in Recent Advances on Soft Computing and Data Mining, vol. 287, ed. by T. Herawan, R. Ghazali, M. Deris (Springer, Cham, Switzerland, 2014), p. 3039.

3. *C.D.Manning, P. Raghavan, H. Schutze,* Introduction to Information Retrieval, Cambridge University Press. 2008.

4. *David Eppstein,* Fast Hierarchical Clustering via Dynamic Closest Pairs, Dept. Information and Computer Science, Univ. of California, Irvine, http://www.ics.uci.edu/~eppstein/

5. *Dempster, A.P.; Laird, N.M.; Rubin, D.B. (1977*). "Maximum Likelihood from Incomplete Data via the EM Algorithm". Journal of the Royal Statistical Society. Series B (Methodological).

6. *T Mikolov, K Chen, G Corrado, J Dean,* Efficient estimation of word representations in vector space, (2013), arXiv preprint arXiv:1301.3781

7. *X. Pei, T. Wu, and C. Chen,* "Automated graph regularized projective nonnegative matrix factorization for document clustering," IEEE Transactions on Cybernetics, vol. 44, no. 10, pp. 1821–1831, 2014.

# СЕКЦІЯ ІІІ

# ЗАГРОЗИ ТА БЕЗПЕКА КІБЕРПРОСТОРУ В УМОВАХ ВІЙНИ ТА ГЛОБАЛІЗАЦІЇ. ПЕРСПЕКТИВИ ТА РИЗИКИ КІБЕРБЕЗПЕКИ

## НОВІ МОЖЛИВОСТІ CSS

***К.Ф. Базилюк,***
к. т. н., доцент кафедри математики та комп'ютерних дисциплін,
***П.Г. Верхоляк,***
магістрант,
Львівська філія ПВНЗ «Європейський університет»

Сучасна еволюція багатьох галузей характерна не поступовими покращеннями, а кардинальними перетвореннями, що докорінно змінюють загальноприйняті підходи і методології. У повній мірі це стосується і методології розробки веб-сторінок.

У 2006 році був вперше впроваджений модуль Flexible Box Layout, що забезпечував можливість роботи з флексбоксами. Тоді цей модуль був застосований в Mozilla для побудови інтерфейсів Firefox. У 2009 році Mozilla запропонувала додати цю систему в CSS. Друга версія модуля з'явилася в IE 10 у 2012 році. Флексбокси в сучасному вигляді, з переносами flex-wrap, стали широко підтримуватися в 2014 році з виходом Firefox 28. Зараз майже 98% браузерів світу підтримують флексбокси у тій чи іншій версії.

Флексбокси - це перша система розкладки в CSS, орієнтована на роботу з блоками, яка не є хаком. Раніше CSS дозволяв імітувати роботу з блоками за допомогою використання різних можливостей таблиць, флоатів, інлайн-блоків, хоч насправді вони були придумані зовсім для іншого.

Наступний крок, що докорінно змінить спосіб верстки веб-сторінок, це поява CSS-ґрідів. З березня 2017-го року їх підтримують усі основні браузери: Chrome, Firefox, Opera і Safari.

Ґрід – це інструмент для розкладки, що застосовується для контейнера і може керувати розміщенням і вирівнюванням дочірніх елементів. CSS-ґрід не замінить флексбокси і навпаки. Оскільки флексбокс працює тільки в одному вимірі, то флекс-елементи можна розміщувати тільки уздовж головної осі або вздовж поперечної осі. Неможливо розмістити флекс-елементи відразу на декількох осях. CSS-ґрід дозволяє працювати з розміткою в двомірному просторі і вирівнювати вміст контейнерів в обох вимірах. Однак, ґрід-контейнер (яким стає елемент з display: grid) сприймає як ґрід-елементи тільки своїх безпосередніх нащадків. Це означає, що однією сіткою для складнішого макета не обійтися. Замість цього необхідно створювати ґріди на рівні компонентів, фактично кілька різних ґрідів з однаковими властивостями. До речі, у специфікації ґрідів була пропозиція ввести підсітки, що дозволило б дочірнім елементам успадковувати батьківський ґрід і застосовувати його до власних нащадків. Функцію підсіток перенесли на другий рівень специфікації, а це означає, що в найближчому майбутньому в браузерах її не буде. Рейчел Ендрю, яка є, мабуть, головним

експертом з ґрідів у світі, пильно стежить за розробкою підсіток і публікує детальну інформацію: в якому стані підсітки зараз і чого чекати в майбутньому. А до тих пір практичнішим буде обходити це, вкладаючи ґріди в ґріди, щоб нащадки ґріда самі фактично ставали ґрідом.

Безліч макетів, від яких раніше відмовлялися, тому що їх не можна було реалізувати на CSS, можуть виявитися можливими завдяки CSS-ґрідам.

За даними сайту Can I Use, побудованого та підтримуваного Алексісом Деверіа, що містить сучасні таблиці з даними підтримки інтерфейсних веб-технологій на настільних і мобільних веб-переглядачах, наданих спільнотою веб-розробників, глобальна підтримка CSS Grid Layout на даний час становить 69.57%, або 75.34%, якщо враховувати версію з префіксом IE10-11 і Edge. До цього часу не було новинок, які б впроваджувались настільки швидко.

Стосовно підтримки модуля CSS Grid Layout в різних браузерах, то в специфікаціях ґрідів і флексбоксів точно визначено, як ці специфікації перевизначають старі методи розкладки, тобто, при верстці допускається використання таких елементів як флоати, інлайн-блоки, багатоколонкова розкладка в якості фолбека при розкладці на ґрідах. Усі браузери зрозуміють стилі для фолбека. Ті, що не підтримують ґріди, на цьому і зупиняться. А ті, що підтримують, будуть використовувати стилі для ґрідів завдяки правилам, які описані в специфікації. Крім того, CSS володіє також можливістю перевірки підтримки браузером ґрідів у вигляді директиви supports.

CSS-ґріди – абсолютно нова технологія, і, хоча сучасні браузери їх підтримують, зворотна сумісність у них відсутня. Для когось це автоматично означає «використовувати не можна», але напевно це – хороша можливість переглянути підхід до забезпечення сумісності.

CSS-ґріди – це розкладочний модуль: він дозволяє змінювати розкладку документа, не втручаючись у порядок у вихідному коді. Іншими словами, CSS-ґріди – це чисто візуальний інструмент, який при правильному застосуванні не повинен впливати на передачу змісту документа.

На думку Рейчел Ендрю, замість домагатися однакового виду розкладки у всіх браузерах, краще дати мобільну вертикальну в один стовпчик розкладку, а потім додавати поверх просунуту функціональність для тих браузерів і розмірів, для яких вона може бути корисною. Це дає доступну, кросбраузерну, зворотно сумісну основу, на якій можна надбудовувати просунуті розкладки і функціональність за допомогою сучасних веб-технологій на зразок CSS-ґрідів і JavaScript.

Останні 15 років вигляд вебу диктувався технічними обмеженнями CSS. Нові розкладочні методи  ґріди, флексбокси і засоби на зразок веб-фігур  суттєво змінять його вигляд і функціональність.

*Список використаних джерел*

1. *Рейчел Эндрю. Is it really safe to start using CSS Grid Layout?*– 06.07.2017. – URL: https://rachelandrew.co.uk/archives/2017/07/04/is-it-really-safe-to-start-using-css-grid-layout/

# СУЧАСНІ АСПЕКТИ НЕСАНКЦІОНОВАНОГО СТЕЖЕННЯ ЗА КОРИСТУВАЧАМИ В ІНТЕРНЕТІ

***К.Ф. Базилюк[1]***
***А.В. Шлапак[2]***
***О.Я. Артим[2]***
к. т. н., доцент кафедри математики та комп'ютерних дисциплін
Львівської філії Європейського університету
[2]магістр, Львівська філія ПВНЗ «Європейський університет»

Критика сучасного стану капіталізму сконцентрована не лише на нерівномірному розподілі доходів та можливостей. Інша її грань – звинувачення технокомпаній в тому, що вони будують свої бізнес-моделі на експлуатації персональних даних часто без згоди їх власників. Ця модель отримання нібито безкоштовних послуг за незриме жертвування приватністю набула значного поширення і отримала назву "капіталізму спостереження". Якщо ця модель набуде значного поширення, що відбувається нині, то суспільство ділитиметься на людей двох типів – "спостерігачів і тих, за ким спостерігають" [1]. Ця асиметрія інформації призводить до асиметрії влади, що може негативно відбитися на демократії.

Капіталізм спостереження ґрунтується на тому, що певна кількість компаній із діджитал-сектору стежить за поведінковими даними користувачів (лайки, кліки, репости) й на їхній основі робить портрет користувача, формує й передбачає його подальшу поведінку [2]. Це позитивно впливає на продажі тих чи інших компаній, але негативно — на офлайнове життя користувача. Однією з головних проблем тут є те, що часто користувачі самі ж добровільно надають на це дозвіл, оскільки безкоштовні у фінансовому плані сервіси зовсім не безкоштовні відносно персональних даних. По суті, персональні дані — це плата за користування інтернетом. Але найстрашніше те, що майже половина користувачів не знає, що їхні дані відстежуються і зберігаються.

Через активність на сервісі людина залишає дані про свою поведінку, які потім збираються та вивчаються компаніями. У результаті компанії можуть передбачати та, що найгірше, формувати подальші дії користувача, тобто впливати на вас не лише як на споживача, але й втручатися в інші сфери вашого життя і впливати на ваш вибір не тільки під час покупок.

В останні роки все частіше в ЗМІ з'являються повідомлення про порушення у сфері конфіденційності з боку відомих діджитал-компаній.

Так, за даними досліджень [3] 2017 року більше 70 відсотків додатків для смартфонів повідомляють про особисті дані стороннім компаніям, таким як Google Analytics, API API Graph або Crashlytics. Дослідники виявили 598 інтернет-сайтів, які, ймовірно, відстежують користувачів з рекламною метою, включаючи послуги соціальних медіа, таких як Facebook, великі інтернет-компанії, такі як Google та Yahoo, та компанії, що займаються інтернет-маркетингом, під егідою таких інтернет-провайдерів, як Verizon Wireless. Наприклад, Alphabet, головна компанія Google, володіє декількома доменами стеження, включаючи Google Analytics, DoubleClick або AdMob, і через них

збирає дані з більш, ніж 48 відсотків програм. Крім того, дані проходять через національні кордони і часто потрапляють до країн із "недружніми" законами про конфіденційність, таких як США, Великобританія, Франція, Сінгапур, Китай та Південна Корея – шість країн, де впроваджені технології масового спостереження [4].

За даними Financial Times [5] 12 травня 2019 року експерти з безпеки WhatsApp виявили нову хакерську атаку на месенджер WhatsApp, яким користуються півтора мільярда осіб у всьому світі. Шпигунська програма Pegasus поширюється ізраїльською фірмою NSO Group, яку в минулому називали "дилером кіберзброї". Програма може непомітно для жертви атаки читати SMS і електронну пошту, включати мікрофон і камеру телефону, дізнаватися про розташування користувача і копіювати персональні дані.

У кінці лютого 2019 року Федеральна торгова комісія США оштрафувала розробників сервісу обміну короткими відео TikTok майже на $6 млн. Як виявилось, особиста інформація неповнолітніх користувачів була використана у відкритому доступі.

13 липня 2019 року хакери розкрили таємні проекти ФСБ для стеження в інтернеті. BBC не виключає [6], що йдеться про найбільший в історії витік даних про роботу російських спецслужб в інтернеті. Хакери зламали сервер московської компанії "Сайтек", яка є великим підрядником російських спецслужб і відомств, і передали журналістам опис її проектів у сфері інтернету. "Сайтек" виконувала роботи для щонайменше 20 непублічних IT-проектів, замовлених російськими спецслужбами й відомствами. Більшість проектів виконувались на замовлення військової частини №71330, яка входить до складу 16-го управління ФСБ Росії, що веде радіоелектронну розвідку.

У кінці серпня 2019 року дослідники із команди Project Zero («білі» хакери, які працюють на Google і шукають уразливості в популярних технологіях незалежно від виробника) виявили, що зловмисники протягом як мінімум двох років мали можливість зламувати чужі iPhone через вразливості операційної системи iOS. Згідно зі звітом експертів, недоліки дозволяли хакерам зламувати смартфони і отримувати повідомлення, геолокацію і файли користувачів, якщо ті заходили на шкідливі сайти. За даними дослідників Google, у системі було 14 вразливостей, які діяли протягом двох років, а шкідливі сайти відвідували «тисячі користувачів у тиждень». Деякі видання назвали атаку «найбільшою в історії iOS».

Цікавий спосіб збору даних користувачів був винайдений одним з технічних університетів Німеччини. Брауншвейгский університет зробив доповідь на IEEE European Symposium on Security and Privacy у 2017 році, згідно з якою, в останні роки все більше набирає обертів технологія збору даних за допомогою ультразвуку, яка називається uXDT (ultrasound cross-device tracking). Технологія uXDT уже зараз викликає побоювання в експертів. За словами науковців, сьогодні не існує стандартів захисту від ультразвукових передатчиків та сигналів.

Водночас великі IT-корпорації офіційно демонструють політику запобігання неправомірному використанню засобів стеження. Цього року Microsoft відхилила урядові запити на доступ до програмного забезпечення для

розпізнавання облич. Компанія закликає до більш суворого регулювання технології розпізнавання осіб, яка використовується в Китаї для відстеження етнічних меншин. Microsoft підтримує жорсткість норм поширення цього ПЗ, але виступає проти повної заборони цієї технології.

У травні 2019 року Google повідомила, що впроваджує нову функцію для облікових записів, яка дозволить автоматично видаляти дані про історію місцезнаходження, дані про веб-сайти та дані про використання додатків після певного періоду часу.

13 жовтня цього року Instagram вимкнула функцію, що дозволяла стежити за користувачами, відслідковуючи дії акаунтів, на які користувач був підписаний.

Сьогоднішній світ живе в еру інформаційних технологій, коли можливості мережі є не лише приємним джерелом можливостей, знань та спілкування, але й джерелом підвищеної небезпеки бути «відкритою книгою» та жертвою зловживань і маніпуляцій.

*Список використаних джерел*

1. 'The goal is to automate us': welcome to the age of surveillance capitalism [Електронний ресурс] – Режим доступу до ресурсу: https://www.theguardian.com/technology/2019/jan/20/shoshana-zuboff-age-of-surveillance-capitalism-google-facebook?utm_source=pocket&utm_medium=email&utm_campaign=pockethits

2. «Наші дані — це плата за користування інтернетом». Павло Бондаренко про капіталізм спостереження [Електронний ресурс] – Режим доступу до ресурсу: https://ms.detector.media/mediaprosvita/master_clas/nashi_dani_tse_plata_za_koristuvannya_internetom_pavlo_bondarenko_pro_kapitalizm_sposterezhennya/

3. 7 in 10 smartphone apps share your data with third-party services [Електронний ресурс] – Режим доступу до ресурсу: https://theconversation.com/7-in-10-smartphone-apps-share-your-data-with-third-party-services-72404

4. List of government mass surveillance projects [Електронний ресурс] – Режим доступу до ресурсу: https://en.wikipedia.org/wiki/List_of_government_mass_surveillance_projects

5. Хакерська атака на WhatsApp: У чому суть проблеми та як захистити свій телефон від встановлення шпигунських програм [Електронний ресурс] – Режим доступу до ресурсу: https://ua.112.ua/golovni-novyni/khakerska-ataka-na-whatsapp-u-chomu-sut-problemy-ta-iak-zakhystyty-svii-telefon-vid-vstanovlennia-shpyhunskykh-prohram-491676.html

6. Москит, Надежда, Наутилус: хакеры раскрыли суть проектов тайного подрядчика ФСБ [Електронний ресурс] – Режим доступу до ресурсу: https://www.bbc.com/russian/features-49050982

7. Google says hackers have put ‘monitoring implants’ in iPhones for years [Електронний ресурс] – Режим доступу до ресурсу: https://www.theguardian.com/technology/2019/aug/30/hackers-monitoring-implants-iphones-google-says

8. https://techcrunch.com/2019/10/07/instagram-is-killing-its-creepy-stalking-feature-the-following-tab/

# ОЦІНКА РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

***С.М. Божаткін,***
***Б.Б. Пасюк,***
магістранти,
***І.Р. Довголуцький,***
ст. викладач
ПВНЗ «Європейський університет»

Оцінка ризиків інформаційної безпеки – це незалежний аудит поточного стану інформаційної системи підприємства, який встановлює рівень її відповідності певним критеріям безпеки. Станом на сьогодні, за умов воєнних дій, спостерігається тенденція зростання кіберзагроз інформаційних ресурсів підприємств, тому їх захист є однією з найважливіших проблем що потребують вирішення. Розв'язання такої проблеми вимагає підготовки відповідних спеціалістів, а також прийняття організаційних і технічних заходів щодо забезпечення кібербезпеки інформаційних ресурсів (активів) підприємств. В сучасних умовах актуальна задача організації системи захисту інформації підприємства, що дозволила б гарантувати безпеку функціонування телекомунікаційного обладнання і обороту інформації в мережевій системі.

Звісно, ефективність захисту критично приватної інформації підприємства залежить від підходу до її організації та правильного вибору методів розрахунку ризиків інформаційної безпеки. Аналіз ризиків інформаційної безпеки передбачає процедуру виявлення певних чинників ризиків, оцінку їх значимості і методи зниження ризиків або зменшення пов'язаних із цим несприятливих наслідків. Актуальні задачі аналізу і оцінки ризиків інформаційної безпеки дозволяють визначити необхідний рівень захисту інформації, а також розробити рекомендації щодо удосконалення системи захисту і мінімізації ризиків[1].

Одним із найважливіших видів діяльності із забезпечення інформаційної безпеки підприємства є виявлення, оцінка та обробка ризиків інформаційної безпеки [2]. За основу та «best practices», прийнятих на міжнародному рівні, необхідно звертатись до міжнародного стандарту ISO/IEC 27001, який дає можливість отримувати цілісну картину ситуації відносно оцінки та удосконалення методик для мінімізації ризиків інформаційної безпеки підприємства [3]. Організації, які відповідають вимогам стандарту після проходження відповідного аудиту ISO 27001 – отримують статус «ISO 27001 compliant» та досить високо цінуються на міжнародному рівні. Сучасний підхід при виборі оцінки ризиків інформаційної безпеки зводиться до максимально можливого використання статистичних або нестатистичних методів які вимагають людських, матеріальних та часових ресурсів [4].

Проведений аналіз ISO/IEC 27001 стандарту та існуючих методик оцінювання ризиків інформаційної безпеки підприємств будь якого напряму , дає можливість стверджувати, що механізм ефективного управління ризиками має забезпечити прийняття та реалізацію ефективних управлінських рішень на підприємстві. Система управління ризиками, має забезпечувати надійний захист через такі безперервні процеси як:

• моніторинг критичних точок мережевої інфраструктури;

• контроль процесів та доступів користувачів в інформаційній системі у вигляді Access Matrix (матриці доступів);

• прогнозування захищеності (не рідше одного разу на півроку, згідно з поточним станом захищеності від нових експлоїтів та можливих векторів атак 0-го дня (zero-day));

• імплементація нових політик захисту інформації.

Запропоновані методи вдосконалюють існуючі методи і заходи щодо уникнення ризиків інформаційної безпеки і пропонуються для впровадження безперервного циклу захисту інформації, як основа при розбудові політики інформаційної безпеки підприємства.

*Список використаних джерел*

1. Карпович І.М., Гладка О.М., Наконечна Ю.А. Наконечна Ю.А., «Аналіз ризиків безпеки інформаційної системи іт-підприємства», Вчені записки ТНУ імені В.І. Вернадського. Серія: технічні науки. Том 31 (70) № 5 2020, с. 69-74 DOI: https://doi.org/10.32838/2663-5941/2020.5/12 (дата звернення 01.11.2022).

2. Гаркуша В.О., «Методичний підхід до оцінки ризиків інформаційної безпеки підприємства», Приазовський економічний вісник. Випуск 2(19) 2020, с. 85-90 DOI: https://doi.org/10.32840/2522-4263/2020-2-15 (дата звернення 01.11.2022).

3. ISO/IEC 27000:2009. Information technology – Security techniques – Information security management systems – Overview and vocabulary (Інформаційні технології. Методи безпеки. Системи управління інформаційною безпекою. Огляд і словник). URL:https://www.iso.org/standard/41933.html (дата звернення 01.11.2022).

4. Л. В. Загоруйко, Т. А. Мартьянова, і Скирда Т., «Моделі аналізу ризику безпеки інформаційних технологій», Опт-ел. інф-енерг. техн., вип. 40, вип. 2, с. 16–20, Вер 2021. DOI: https://doi.org/10.31649/1681-7893-2020-40-2-16-20 (дата звернення 02.11.2022).

## ТЕХНОЛОГІЯ HONEYPOT ДЛЯ ЗАХИСТУ КОМП'ЮТЕРНОЇ МЕРЕЖІ

***В. Васильєв,***
магістрант факультету інформаційних систем та технологій,
***В.І. Пашорін,***
к.т.н., професор,
завідувач кафедри інформаційних систем,
програмування та кібербезпеки,
ПВНЗ «Європейський університет»

Honeypot – це комп'ютерна система, яка створена для того, щоб заманити кіберзлочинців, а також виявляти, відхиляти або вивчати спроби отримати несанкціонований доступ до інформаційних систем. Як правило, вона складається з комп'ютера, програм та даних, які імітують поведінку реальної системи, яка, як видається, є частиною мережі, але насправді є ізольованою і ретельно контролюється. Всі зв'язки з honeypot вважаються ворожими, оскільки немає підстав для законних користувачів доступу до honeypot. Перегляд та реєстрації даної діяльності дає змогу зрозуміти рівень та типи загрози мережевої інфраструктури, відволікаючи злочинців від активів реальної вартості [1].

Об’єктом технології *Honeypot* є будь-яка компанія, яка має перед собою мету виявити зловмисника, або визначити якими засобами він буде впливати на систему інформаційної діяльності.

На відміну від таких механізмів, як міжмережеві екрани і системи виявлення вторгнень, технологія *Honeypot* не вирішує певні завдання з нейтралізації загроз і вразливостей. *Honeypot* – це інструмент, який вносить свій внесок в повну архітектуру безпеки. Значення засобів *Honeypot* і проблеми, які вони допомагають вирішувати, залежить від того, як ці засоби побудовано, розгорнуті і використовуються.

Технологія *Honeypot* – ресурс безпеки, призначення якого полягає в тому, щоб стати дослідженим або бути атакованим [2]. Це означає, що незалежно від того, яку структуру має засіб *Honeypot*, мета полягає в тому, щоб даний ресурс був досліджений, атакований і використаний зловмисником. Не має значення, чим є ресурс: імітованим сервісом або повноцінною операційною системою. Головне, що сенс функціонування ресурсу полягає в нападі на нього.

*Honeypot* може бути підключений (в залежності від задач, що він має вирішувати) до різних точок ІТС. Узагальнена схема системи із підключенням *Honeypot* перед файєрволом і після роутера наведена на рис.1.

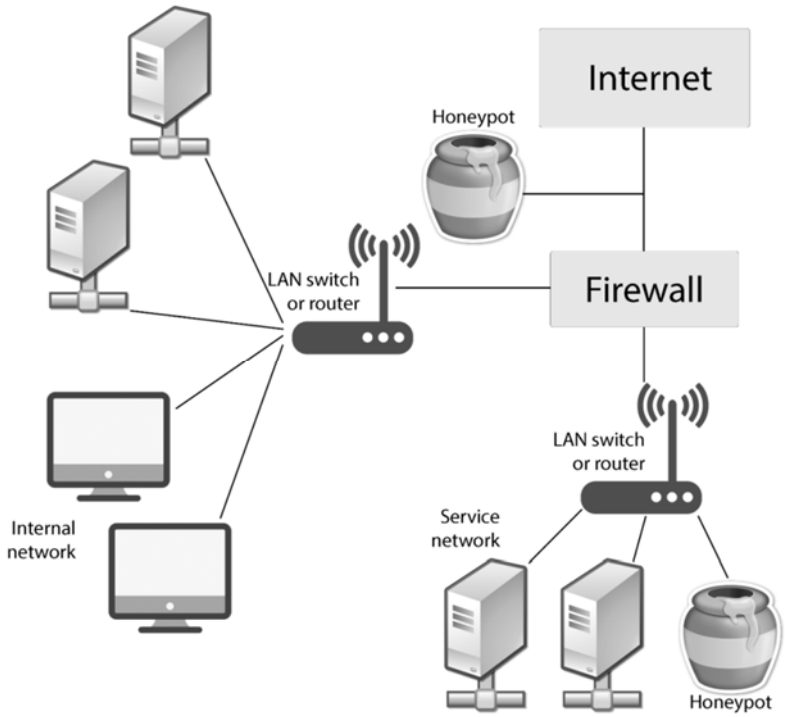



**Рисунок 1 – Схема системи *Honeypot***

У загальному випадку, дослідні *Honeypot* не зменшують ризик для організації, але отримана інформація може бути застосована на реальних системах, наприклад, для поліпшення попередження, виявлення, можливостей протоколювання і необхідної реакції, а виробничі *Honeypot* вирішують задачі прикладного рівня. Задачі, вирішувані *Honeypot* можна розглядати на різних рівнях реалізації політики безпеки.

Honeypots допомагають усвідомлювати загрози мережевим системам, але виробничі honeypots не повинні розглядатися як заміна стандартного IDS. Якщо

вони не належним чином налаштовані, вони можуть бути використані для доступу до реальної виробничої системи або використовуватись як стартовий майданчик для атак проти інших систем [3].

*Список використаних джерел*

1. Гіпервізор, віртуалізація і хмара: Про Гіпервізор, віртуалізації систем і про те, як це працює в хмарному середовищі [Електронний ресурс]. Режим доступу: http://www.ibm.com/developerworks/ru/library/clhypervisorcompare/ 4.The Honeynet

2. Dynamic Honeypots [Електронний ресурс]. Режим доступу: http://www.symantec.com/connect/articles/dynamic-honeypots

3. Intrusion Detection FAQ: What is a Honeypot? [Електронний ресурс]. Режим доступу: https://www.sans.org/security-resources/idfaq/honeypot3.php

## РЕАЛІЇ КІБЕРБЕЗПЕКИ УКРАЇНИ В УМОВАХ ВІЙСЬКОВОГО СТАНУ

***Я.С. Ісаєв,***
аспірант,
***І.С. Остапчук,***
магістрант факультету інформаційних систем та технологій,
ПВНЗ «Європейський університет»

Зростання інформаційної обізнаності громадян, попит на інформаційні технології, пристрої, ресурси призводить до зростання кількості і якості кіберзагроз які спрямовані для отримання вигоди шахраями. Спільноти від малих до великих, від бізнесу до країн створюють організовані центри протидії кіберзагрозам, і Україна не є винятком. В Україні прийнято закон "Про основні засади забезпечення кібербезпеки України", який визначає основи забезпечення захисту національних інтересів України в кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, а також повноваження державних органів у цій сфері, основні принципи координації їх діяльності щодо забезпечення кібербезпеки. Суб'єктами національної безпеки країни є Служба безпеки України, Міністерство оборони України, Національна поліція України та інші суб'єкти описані в законі. Кібербезпека - це актуальна складова нашої країни, як в мирний час, так і зараз, під час війни вона набуває ще більшої актуальності. Україна посідає 24 місце за рейтингом Національного індексу кібербезпеки (National Cyber Security Index), випереджаючи такі країни, як Канада, Ізраїль, Японія станом на 2022 рік. За цим самим рейтингом Україна піднялася на 5 позицій з 2019 року, тоді ми займали 29 місце. Отже, план відновлення України має передбачати відновлення інфраструктури, що дасть можливість повернутися великій кількості біженців, що, в свою чергу, дасть поштовх ринку праці. Якщо план відновлення враховуватиме всі особливості української економіки, це дасть змогу не лише відновити ВВП до довоєнного рівня, а й закласти сталий фундамент для подальшого розвитку.

З початку повномасштабної війни 24 лютого 2022 року кількість кібератак на Україну збільшилось на 50%, значна кількість атак націлена на державний, фінансовий та медіа сектори. Кількість кібератак росії на державно-військовий сектор України зросли на 196% порівняно з довоєнним періодом. При цьому

Україна теж розгорнула активні дії. За чотири місяці війни наша ІТ-армія атакувала понад 4 200 російських онлайн-ресурсів. Кількість фішингових листів зросла в сім разів. Третина шкідливих листів була надіслана російським одержувачам з українських адрес електронної пошти. Один із провідних центрів реакції на кіберзагрози є CERT-UA (Computer Emergency Response Team of Ukraine / Команда реагування на комп'ютерні надзвичайні події України). Це державна структура, яка належить до Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації України й забезпечення захисту державних інформаційних ресурсів та інформаційних і телекомунікаційних систем від несанкціонованого доступу, неправомірного використання, а також порушень їх конфіденційності, цілісності та доступності. Ця установа щоденно фіксує кібератаки, які здійснюються на території України, визначає, які методи використовуються для атаки та дає інструкції з протидії, інформація вільно розповсюджується на офіційному державному порталі.

Згідно зібраній статистиці "Платформа прав людини", яка будується на даних державної служби спеціального зв'язку та захисту інформації України, станом на вересень 2022 року було виявлено 25 165 386 кібератак, які були здійснені на державний сектор та ще 1 060 940 фішингових атак. Більш як 25 мільйонів атак за 7 місяців війни, якщо інтенсивність атак залишилася такою ж, то станом на листопад кількість атак має сягати 32 мільйонів. Найбільша частина атак (24 мільйони) – це сканування, далі 640 тисяч спроб експлуатації вразливостей, 151 тисяча шкідливих підключень та 63 тисячі спроб авторизації або входу у систему без дозволу. Це 240 спроб на добу доступу до систем. Аби зменшити ризики стати жертвою кіберзлочинців необхідно дотримуватися перш за все авторизації. Ці цифри дають зрозуміти, що кожен громадянин має можливість зменшити загрози атак, якщо він буде дотримуватися норм інтернет "гігієни" так само, як він це робить щоденно у побуті, тим самим ми можемо допомогти зменшити навантаження на наших кіберзахисників. Наведемо кілька простих, але дієвих порад з кібергігієни, а саме:

- встановлювати надійні паролі та не розголошувати їх;
- використовувати різні паролі для різних облікових записів;
- паролі від особистих та державних сервісів мають бути різними;
- посилювати захист 2-факторною автентифікацією;
- завантажувати програмне забезпечення з надійних джерел;
- не відкривати вкладені файли чи переходити за посиланням при отриманні підозрілого листа чи повідомлення від невідомого відправника.

*Список використаних джерел*

1. Закон про кібербезпеку України https://zakon.rada.gov.ua/laws/main/2163-19#Text

2. Національний індекс кібербезпеки (National Cyber Security Index) https://ncsi.ega.ee/ncsi-index/?order=-ncsi&type=c

3. Кібераналіз компанії Check Point за 2022 рік. https://pages.checkpoint.com/cyber-attack-2022-trends.html

4. Як росія та Україна воюють на кіберфронті https://www.epravda.com.ua/columns/2022/09/28/691925/

# ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ БІЗНЕС-ПРОЦЕСІВ СУЧАСНОЇ КОМПАНІЇ

***А.Р. Кісельов,***
магістрант,
***П.А. Скляренко,***
аспірант,
ПВНЗ «Європейський університет»

Нинішнє складне, динамічне та агресивне зовнішнє середовище вимагає від сучасних компаній підтримки своєї інформаційної інфраструктури, вдосконалення корпоративних схем та бізнес-процесів з точки зору їх безпеки та контролю [4].

Під бізнес-процесом ми розуміємо певний набір різних видів діяльності підприємства, що у сукупності створюють результат (продукт, послугу, зокрема інформаційну), має цінність кінцевого споживача (клієнта чи замовника) [3]. Як замовник може також виступати бізнес-процес вищого порядку. З іншого боку [4], бізнес-процес – це ланцюжок операцій (робіт), результатом якого є продукт чи послуга. У ланцюжок можуть входити операції, які виконуються структурними елементами, розташованими різних рівнях організаційної структури підприємства.

Конструювання бізнес-системи неможливе без такого її компонента, як інформаційна інфраструктура, важливою складовою якого є оцінка та захист інформаційних активів у складі активів корпорації. Підтримка та захист системи управління корпорацією передбачає підтримку та захист самих бізнес-процесів. Розвиток інформаційної інфраструктури бізнес-системи ґрунтується на подоланні інфраструктурної та інформаційної роз'єднаності підрозділів корпорацій. Інвестиції в управління бізнес-процесами можуть приносити певні доходи за рахунок підвищення ефективності роботи та прискорення бізнес-процесів, а також за рахунок підвищення ринкової вартості компанії в частині нематеріальних активів та, насамперед, інформаційних [2].

Одним із основних завдань корпоративної інформаційної системи (КІС) як і будь-якої іншої технічної системи є сервісний супровід бізнес-процесів. Будь-яка технічна система, яка використовується в бізнесі, будучи важливим елементом інфраструктури, повинна надавати бізнесу певний тип сервісу. КІС надає бізнесу інформаційний сервіс, але й сама потребує підтримки та захисту [18–21]. Сервіс полягає у наданні бізнесу необхідної інформації потрібної якості, у потрібний час та у потрібному місці, тобто. зрештою інформації, достатньої управління самим бізнесом. Інформація в такому розумінні стає одним із ключових елементів інформаційної інфраструктури [3].

Ще одним бізнес-завданням корпоративної системи інформаційної безпеки підприємства є забезпечення гарантій достовірності інформації або гарантій довірливості інформаційного сервісу КІС. Забезпечення інформаційної безпеки має комплексний характер і передбачає необхідність поєднання законодавчих, організаційних та програмно-технічних заходів.

Під інформаційною безпекою підприємства слід розуміти захищеність

його інформаційних активів (як частини інфраструктури бізнес-процесів) від випадкових чи навмисних впливів власного чи штучного характеру, що можуть спричинити шкоду власникам або користувачам інформаційних активів у бізнес-системі. Захист інформаційних активів підприємства полягає у підтримці цілісності, доступності та, якщо потрібно, конфіденційності інформаційних активів у бізнес-системах. Принцип забезпечення інформаційної безпеки підприємства ілюструє рис. 1.




**Рисунок 1 – Принципи забезпечення інформаційної безпеки підприємства**

Цілісність інформаційних даних означає здатність інформації зберігати початковий вигляд та структуру як у процесі зберігання, так і після неодноразової передачі [3]. Вносити зміни, видаляти чи доповнювати інформацію вправі лише власник чи користувач із легальним доступом до даних.

Конфіденційність – характеристика, що вказує на необхідність обмежити доступ до інформаційних ресурсів для певного кола осіб. У процесі дій та операцій інформація стає доступною лише користувачам, які включені до інформаційних систем та успішно пройшли ідентифікацію.

Доступність інформаційних ресурсів означає, що інформація, яка знаходиться у вільному доступі, має надаватися повноправним користувачам ресурсів своєчасно та безперешкодно.

Інформаційна інфраструктура сучасної компанії повинна мати властивість захищеності інформації, що використовується в її бізнес-процесах. Ця властивість характеризує здатність системи забезпечувати захист комерційної, службової, технологічної та іншої інформації на підприємстві від її несанкціонованого (навмисного чи випадкового) отримання, зміни, знищення чи використання.

*Список використаних джерел*

1. J. Meza, S. Campbell, D. Bailey, “Mathematical and statistical opportunities in cybersecurity,” Paper LBNL-1667E, Lawrence Berkeley National Laboratory, Berkeley, CA, pp. 1–11, 2009.

2. L. Lin, R. Zuo, S. Yang, Z. Zhang, “SVM ensemble for anomaly detection based on rotation forest,” Proc. Of the third international conference on intelligent control and information processing (ICICIP), pp. 150-153, 2012.

3. P.A.R. Kumar, S. Selvakumar, “Distributed denial of service attack detection using an

ensemble of neural classifier," Computer Communications, Vol. 34, pp. 1328–1341, 2011.
4. M.-L. Zhang, Z.-H. Zhou, "A k-nearest neighbor based algorithm for multi-label classification," Proc. of the International Conference on Granular Computing, pp. 718–721, 2005.

# НАВЧАЛЬНИЙ ЦЕНТР КАФЕДРИ КІБЕРБЕЗПЕКИ З ФУНКЦІОНАЛЬНІСТЮ СИМУЛЯЦІЙНОГО КІБЕРПОЛІГОНУ

***В.В. Коваль,***
к.ф.-м.н., ст.викладач,
***В.О. Любчак,***
к.ф.-м.н., доцент,
Сумський державний університет

Щоб захистити інформаційний простір України від кіберзагроз сучасності надзвичайно важливо навчати та тренувати фахівців, здатних до кіберзахисту. Підготовкою фахівців у цьому напрямку, а особливо за спеціальністю Кібербезпека, займаються заклади вищої освіти. Згідно до Стандарту вищої освіти України [1] потрібно готувати спеціалістів, здатних: «..розв'язувати складні спеціалізовані задачі та практичні проблеми з забезпечення кібернетичної безпеки інформаційно-комунікаційних систем».

Під час підготовки спеціалістів з кібербезпеки вимагається баланс між теорією та практикою. Студенти повинні розуміти теорію, логіку основних концепцій кібербезпеки, але також повинні вміти практично впроваджувати інструментарій та протоколи, які застосовують ці концепції. Потрібно дати студентам реальний досвід кібербезпеки з практичною складовою та надати навички, щоб вони могли стати успішними професіоналами.

Для вирішення цих актуальних завдань на кафедрі кібербезпеки Сумського державного університету (СумДУ) спроектовано та відбувається розбудова навчально-тренувального центру кібезбезпеки (Центр). Однією з ключових особливостей Центру є тренувальна складова кіберполігону для моделювання кіберінцендентів.

Основною концепцією розгортання кіберполігону є практичне відпрацювання студентами, дослідниками та спеціалістами тактик відбиття кібератак, а також симуляція кібератак з одночасним напрацюванням методик кібернападів.

Крім того, для інтеграції та ефективного застосування потужної системи електронного навчання СумДУ та реалії сучасності (наприклад, онлайн навчання) під час проектування концепції Центру закладалась невід'ємна складова: підтримання онлайн-навчання з кібербезпеки, можливість віртуалізації класів, особливо під час військового стану та застосування інструментарію для доступу студентів до ресурсів Центру, незалежно від того, навчаються вони в оффлайні чи дистанційно.

Під час створення Центру був вивчений досвід навчальних центрів університетів України. Центри, лабораторії та навчальні аудиторії з галузі кібербезпеки створені і функціонують у багатьох ЗВО України. Ось деякі з них:

1. Київський національний економічний університет імені Вадима

Гетьмана: Навчально-наукова лабораторія «Полігон кібербезпеки» [2].

2. Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського» [3].

3. Харківський національний економічний університет імені Семена Кузнеця: «Кіберполігон» [4].

4. Хмельницький національний університет: віртуальна лабораторія «Кіберполігон» [5].

5. Військовий інститут телекомунікацій та інформатизації імені Героїв Крут: Навчально-тренувальний комплекс кібербезпеки [6].

6. Харківський національний університет радіоелектроніки.

7. Державний університет телекомунікацій.

8. Національний авіаційний університет.

Центр, що розбудовується в СумДУ, на даний час складається з двох основних зон, які направлені на:

- програмні методи та засоби захисту інформації;
- технічні методи та засоби захисту інформації.

Зона «програмних засобів захисту інформації» направлена на вивчення та розробку системних та прикладних програм, які призначені для захисту інформації, що передається по телекомунікаційним каналам, зберігається в базах даних на інформаційних носіях, тощо. В межах зони створена автономна локальна мережа, що дозволяє її використання як захищеного майданчика для навчання, дослідження та протидії загрозам.

Зона «технічних засобів захисту інформації» направлена на вивчення та дослідження інженерно-технічних заходів та технічних засобів унеможливлення витоку, знищення та блокування інформації, порушення цілісності та режиму доступу до інформації.

Для симуляцій кібератак та активної протидії використовується різноманітне спеціалізоване програмне забезпечення.

Також у даний час вивчаються та інтегруються у роботу Центру ресурси таких потужних платформ для навчальних тренувань та симуляцій:

- Платформа «Practice Labs» [7]. Має кілька десятків онлайн практичних лабораторій: Practice Labs Vulnerability Sandbox, Red&Blue Team Fundamentals та інші.
- Платформа «CYBER RANGES» [8]. Платформа Міжнародного союзу електрозв’язку (ITU) для проведення національних, регіональних і глобальних кібернавчань. Має повноцінний симулятор роботи Blue Tteam з можливістю вибору сценарія атаки, тренування в ігровій формі з хакінгу, надання практичних навичок з тестування на проникнення, інструмент для симуляції злому та атак із відкритим вихідним кодом тощо.

Створення фізичного та віртуального простору, дозволить фахівцям проводити реальні симуляції кібератак та відпрацьовувати захист від них.

Кіберполігон дозволить створити симуляцію комп’ютерної мережі в безпечному закритому середовищі, щоб атаки можна було досліджувати та тестувати без ризику впливу на реальну зовнішню інфраструктуру Це буде технічне навчання, яке буде імітувати реальні кібератаки.

Ключовою особливістю Центру є те, що відпрацювання кіберподій

здійснюється в замкненому віртуально-реальному середовищі, яке, при необхідності, не має виходу до мережі Інтернет.

Локалізація програмного забезпечення та систем віртуалізації, за допомогою яких відбувається моделювання кібератак на комп'ютерні мережі, дозволяє зменшити (або зовсім виключити) витрати на придбання ресурсів хмарних обчислень та зайвого залучення пропускної здатності загальних комунікаційних каналів, щодо виконання завдань роботи кіберполігону.

Платформа, яка розбудовується, буде застосовуватись також для дослідження проблематик кібербезпеки та корисна для підвищення кваліфікації фахівців з кіберзахисту.

Планується, що Центр будуть використовувати не тільки для навчання студентів, а також компанії, державні служби безпеки і команди підтримки безпеки критичних інфраструктур.

Також планується виконання наступних напрямків діяльності:

- Симуляція кібератак і ефективного захисту:
  - моделювання мережевих атак на інфраструктуру;
  - аналіз нових стратегій наступу та ефективного захисту;
  - симуляція нових видів атак.
- Методика ефективної освіти з кібербезпеки:
  - розробка концепції активного навчання в кібербезпеці.
- Класифікація та аналіз даних і кіберзагроз:
  - дослідження аналітичних методів обробки даних;
  - методи візуалізації та взаємодії в кібербезпеці;
  - правові аспекти використання інструментів кіберзахисту.

*Список використаних джерел*

1. Стандарт вищої освіти за спеціальністю 125 «Кібербезпека» галузі знань 12 «Інформаційні технології» для першого (бакалаврського) рівня - URL:https://mon.gov.ua/storage/app/uploads/public/5bb/626/1a8/5bb6261a8477616640916 4.pdf (дата звернення: 04.11.2022).

2. Навчально-наукова лабораторія "Полігон Кібербезпеки". URL: https://kneu.edu.ua/ua/depts9/k_komp_matematyky_ta_informacijnoi_bezpeku/ SELabs_of_KMIB/sel_CSP/ (дата звернення: 04.11.2022).

3. Структурні підрозділи ФТІ - Фізико-Технічний Інститут. URL: http://ipt.kpi.ua/pidrozdili-ta-kafedri (дата звернення: 04.11.2022).

4. Кіберполігон –Кафедра кібербезпеки та інформаційних технологій, ХНЕУ ім. С. Кузнеця. URL: http://www.kafcbit.hneu.edu.ua/кіберполігон/ (дата звернення: 04.11.2022).

5. Кіберполігон - Кафедра кібербезпеки, Хмельницький національний університет. URL: https://kb.khmnu.edu.ua/kiberpoligon/ (дата звернення: 04.11.2022).

6. У ВІТІ розгорнуто кіберполігон– Інформаційне агентство АрміяInform. URL: https://armyinform.com.ua/2021/12/29/viti-otrymav-kiberpoligon/ (дата звернення: 04.11.2022).

7. Practice Labs Platform | Virtual IT labs | Practice Labs | Hands-on Learning for Digital & IT Skills. URL: https://skills.practice-labs.com/platform (дата звернення: 04.11.2022).

8. CYBER RANGES For Academia and Training Providers. URL: https://www.cyberranges.com/academia-and-training-providers/ (дата звернення: 04.11.2022).

# КІБЕРБЕЗПЕКА ПІДПРИЄМСТВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ МІСТА ДНІПРО В КОНТЕКСТІ СУЧАСНИХ ВИКЛИКІВ

***Д.В. Коміренко***,
аспірант,
ПВНЗ "Європейський університет"

Кіберпростір у великій мірі нагадує собою "поле бою". Напади на об'єкти, які забезпечують життєдіяльність окремих підприємств, населених пунктів або держав, ставлять загрози для здоров'я і життя людей. Виходячи з цього, безпека кіберпростору є актуальною.

Наші дослідження присвячені аналізу критичної інфраструктури економіки на прикладі підприємств критичної інфраструктури міста Дніпра. 23.07.2022 р. уряд затвердив «Порядок проведення моніторингу рівня безпеки об'єктів критичної інфраструктури», який, на нашу думку, є недостатньо акцентованим на сучасні наукові досягнення і можливості. Тому метою досліджень, що проводяться у даній роботі, є аналіз, систематизація та пропозиції щодо розробки дієвих механізмів моніторингу підприємств критичної інфраструктури для їх належного функціонування та інформаційного захисту. Розроблений Міністерством економіки вищезгаданий документ передбачає моніторинг рівня безпеки критичних об'єктів раз на три роки, – і це в період ведення інтенсивних бойових дій та ударів по цих та суміжних об'єктах. За результатом моніторингу має складатися акт, де вказують одну з оцінок: «забезпечує», «обмежено забезпечує» та «не забезпечує». Проте такий підхід до оцінки реального стану кіберзахисту є застарілим та втратив свою актуальність.

Оператор критичної інфраструктури отримує акт і зобов'язаний вжити відповідних заходів.

На законодавчому та адміністративному рівнях не прописано не лише кримінальної, а навіть адміністративної чи фінансової відповідальності . І все це на фоні відключень, аварій та блекаутів.

Заслуговує на увагу проект Агентства США з міжнародного розвитку USAID «Кібербезпека критично важливої інфраструктури України». Цей напрямок є одним із пріоритетних у наших дослідженнях. Цей проект передбачає адаптацію правових та інституційних баз до міжнародних стандартів кібербезпеки, розбудову стійкої індустрії кібербезпеки та розвиток національного кадрового потенціалу в галузі кібербезпеки.

Гіпотезою наших досліджень є твердження про те, що система заходів із забезпечення необхідного рівня кібербезпеки надасть можливість стабілізувати роботу установ та підприємств критичної інфраструктури.

# IP-СИСТЕМИ В ТЕХНОЛОГІЯХ БЕЗПЕКИ

***В.І. Коцун*[1]**
***М.О. Костін*[2]**
***А.В. Добиш*[2]**
[1]к. т. н., завідувач кафедри математики та комп'ютерних дисциплін
Львівська філія ПВНЗ «Європейський університет»
[2]магістр, Львівська філія ПВНЗ «Європейський університет»

Системи відеоспостереження (англ. Closed-circuit television, CCTV) – це програмно-апаратний комплекс (відеокамери, об'єктиви, монітори, реєстратори та ін. обладнання), призначений для організації відеоконтролю як на локальних, так і на територіально-розподілених об'єктах.

Відеоспостереження сьогодні є невід'ємним елементом будь-якої сучасної системи безпеки.

На поточний момент серед систем відеоспостереження особливо важливе місце займають системи IP-спостереження. Це зумовлено тим, що такі системи дозволяють встановлювати відеоконтроль за об'єктами будь-якої складності, а робота оперативного персоналу з їх експлуатації не вимагає високої кваліфікації. Такі системи не потребують прокладання додаткових ліній зв'язку, передача даних відбувається за мережевої інфраструктури, побудованої на протоколі IP. Контроль і адміністрування системи здійснюється з будь-якого комп'ютера, що має доступ до мережі і спеціальне програмне забезпечення.

Відеоспостереження на базі IP-технологій здійснюється на базі стандартної мережної архітектури – локальної мережі Ethernet. Фактично користувач отримує розподілену цифрову систему охоронного відеоспостереження, яка дозволяє застосовувати для аналізу і обробки даних сучасні інформаційні технології. Ключовим елементом мережі IP-відеоспостереження є мережева (IP) відеокамера, яка має об'єктив, оптичний фільтр, ПЗЗ-матрицю, вбудований мікропроцесор для оцифровування/стиснення відеозображення в різних форматах (найчастіше в H.264, MPEG-4 або M-JPEG), мережевий контролер для підключення в мережу Ethernet і інші елементи. Потужність процесора визначає продуктивність і швидкість передачі відеопотоку по мережі. По ряду характеристик, таких як тип матриці, чутливість, настройки зображення (баланс білого, АРУ, гамма-корекція і ін.), IP-камери можна порівняти з аналоговими, однак наявність мережевого інтерфейсу і додаткових процесорів дозволяє їм виконувати відеоаналіз, масштабування зображення, накладення на нього титрів і передачу цифрового відео на великі відстані та ін. Найголовніше, що кожна мережева відеокамера має свою власну IP-адресу, обчислювальні функції і вбудоване ПЗ, що дозволяє їй функціонувати як повноцінний мережевий пристрій. На відміну від аналогової відеокамери, IP-камера не потребує прямого підключення до комп'ютера або до будь-якого іншого апаратного або програмного засобу. Її підключення може здійснюватися як за допомогою дротового з'єднання (по мідним проводам або оптичному волокну) так і бездротового (Wi-Fi, GPRS/EDGE, 3G, супутниковий зв'язок тощо). Таким чином, досягається повна або часткова мобільність

користувача, який здатний стежити за віддаленими об'єктами практично з будь-якої точки земної кулі.

Основні переваги відеоспостереження на основі IP-камер:

• Оператор системи може здійснювати візуальний контроль як локально, так і віддалено (з комп'ютера, мобільного телефону тощо), та здійснювати функції адміністрування системи відеоспостереження використовуючи переваги веб-технологій.

• Спрощена установка при малих витратах на монтаж - мережеві відеосистеми IP не вимагають прокладки додаткового коаксіального кабелю, як в аналогових системах, а підключаються до існуючої системи охорони об'єкта або за допомогою бездротових технологій.

• Якість відеозображення – в сучасних IP-системах застосовується формат MPEG-4, який дозволяє більш ефективно використовувати ресурси мережі в порівнянні з форматом M-JPEG. Оцифровування зображення відбувається у самій камері, що надає можливість розвантажити центральне обладнання системи та зайняти його вирішенням інших насущних задач.

• Можливість передавати по одному кабелю не тільки відео, але і звук, а також управляти і керувати IP-камерою.

• Застосування цифрових камер дозволяє відмовитись від використання черезстрокової розгортки і, як наслідок її – деінтерлейсінгу.

• Мережеві камери можуть приймати та опрацьовувати сигнали тривоги, що надходять з датчиків, і управляти зовнішніми виконавчими пристроями через цифрові порти вводу-виводу.

• Гнучкість і масштабованість систем IP відеоспостереження полягає в можливості будівництва фізично розподілених мереж відеомоніторингу, контролю та дистанційного керування без прив'язки до відстані.

• Інтеграція з багатьма існуючими на даний момент системами відеоспостереження.

• Використання хмарного спостереження.

Водночас масове застосування IP-систем стримує декілька причин.

1. Якість зображення. Якщо не використовується стиснення, то можна отримати вражаючі цифри. Так якщо у пристрою є буфер на один кадр, то при стандартному розмірі кадру 768x576x2, отримуєм розмір кадра рівний 885 Кбайт! В секунду знімається 25 кадрів (живе відео), тобто 2 Мбайт/с або 177 Мбод! В даний час тільки гігабітний Ethernet або мережі на основі оптоволоконних з'єднань здатні забезпечувати обмін на таких швидкостях.

Обмеження пропускної здатності каналів зв'язку призводять до застосуванню алгоритмів стискання зображення з невідновною втратою якості або зниження швидкості відео потоку (до 1-3 кадрів/с) при збереженні якості. При цьому зображення губить придатність для систем розпізнавання облич або автомобільних номерів.

2. Якість матриці і оптики в самих IP-відеокамерах. Виробники, намагаючись зробити IP-камери дешевшими і універсальними, встановлюють середні по всім параметрам матриці, які призводять до «сліпоти» камери вночі і її перевантаження при денному світлі.

3. Складності з інтеграцією камер різних виробників в систему з

програмним забезпеченням третіх виробників. Вся множина аналогових камер має, як мінімум, один інтерфейс — композитний відеосигнал, який підтримується будь-яким обладнанням. В цифровому світі все більш складно. Багато виробників підтримують всі протоколи передачі даних, але ретельно приховують алгоритм кодування зображення, змушуючи клієнтів користуватися тільки їх утилітами перегляду або архівування зображення.

Як зазначалось вище, при організації передачі відеоінформації через Internet, основною проблемою являється вибір пропускної здатності каналу зв'язку і вибір якості зображення. Для фахового вирішення цих проблем доцільно застосовувати спеціалізоване програмне забезпечення. Серед програм щодо розрахунків подібних параметрів виділяється хорошою ефективністю програма Axis Design Tools — зручний і багатофункціональний калькулятор, що застосовується для розрахунків при побудові системи відеоспостереження з камерами і відеосерверами Axis.

Підсумовуючи, можемо зробити наступні висновки:

1. Системи IP-відеоспостереження дозволяють використовувати більш рентабельні рішення, такі як стандартні сервери для запису і збереження відеоданих.

2. При використанні системи IP-відеоспостереження є можливість вибору програмного забезпечення, створеного для управління відео і забезпечення необхідної аналітичної підтримки.

3. Системи IP-відеоспостереження дозволяють організовувати децентралізовану обробку і збереження інформації.

4. Системи IP-відеоспостереження легко реконфігуруються і переносяться, що заважає потенційним зловмисникам легко віднаходити слабкі місця в системі.

5. В цілому, мережеві системи відеоспостереження находять все ширше застосування для віддаленого контролю стану об'єктів, що не вимагають запам'ятовування і аналізу дрібних деталей зображення.

## ОСОБЛИВОСТІ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ КІБЕРПРОСТОРУ УКРАЇНИ В УМОВАХ ВІЙНИ

***Б.І. Мудрик,***
аспірант спеціальності «Право»,
ПВНЗ "Європейський університет"

З моменту появи Інтернету, як всесвітньої мережі, суспільство усвідомило безмежні перспективи розвитку цієї технології та почало невпинно зосереджувати свою увагу на її подальшій розробці та вдосконаленні. Наслідком таких досліджень стала глобалізація та цифровізація усіх сфер та напрямків суспільного життя. Згідно з даними Міжнародного телекомунікаційного союзу, станом на 2022 рік, доступ до мережі Інтернет мають близько 5,3 мільярдів людей[1]. При цьому, відповідно до відкритої інформації, у 2021 році загалом було зламано понад 22 мільярди особистих записів у 2021 році[2].

Особливої ж актуальності питання належного рівня кібербезпеки набирає в умовах війни, адже заволодіння доступом до секретної інформації, в тому числі

захищеної державною таємницею, може здійснювати значний негативний вплив на перебіг бойових дій в тому числі.

Саме тому метою цього дослідження є з'ясувати порядок нормативно-правового регулювання кібернетичної безпеки України, встановити особливості та способи забезпечення кібербезпеки та проаналізувати зміни, які були реалізовані за період дії воєнного стану з метою захисту інтересів держави.

Відповідно до Закону України №2163 від 17.08.2022 «Про основні засади забезпечення кібербезпеки України», поняття «кібербезпека» визначається як захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі[3].

Баранов О.А., провівши аналіз існуючих у різних державах підходів до визначення поняття кібербезпеки, робить висновок, що базовою метою забезпечення кібербезпеки – це забезпечення стану захищеності життєво важливих інтересів людини, суспільства і держави[4]. Тому, враховуючи ступінь аналізу, можна стверджувати, що закріплене у законодавстві України поняття відповідає загальнопоширеній світовій практиці у сфері кібернетичної безпеки.

Згідно із статтею 5 згаданого вище Закону №2163, координація діяльності у сфері кібербезпеки здійснюється Президентом України через Раду національної безпеки і оборони України, при якій створено Національний координаційний центр кібербезпеки. Саме цьому центру делеговано повноваження контролю за сектором безпеки і оборони у галузі кібербезпеки, в тому числі щодо формування Стратегії кібербезпеки України, що була затверджена Указом Президента України від 26.08.2021 р. №447/2021.

Серед загроз кібербезпеці, передбачених вищезазначеною Стратегією, вказано також гібридна агресія Російської Федерації проти України у кіберпросторі[5]. 24 лютого 2022 Російська Федерація розпочала військову агресію проти України, у зв'язку з чим було ухвалено Указ Президента України №64/2022 «Про введення воєнного стану в Україні», що спричинило необхідність внесення змін до нормативно-правового регулювання усіх сфер суспільного життя, в тому числі і сфери кібербезпеки, наслідком чого стало прийняття Закону України №2149-IX «Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану».

Даний нормативно-правовий акт створив передумови для приведення галузі кібернетичної безпеки до реалій сьогодення та заклав фундамент для побудови більш досконалої і ефективної системи боротьби з кіберзлочинністю. Зміни стосувались двох ключових аспектів: розширення меж діяльності правоохоронних органів при розслідуванні такого роду злочинів та посилення відповідальності за їх вчинення, особливо в умовах воєнного стану. Крім того, цим законом також було закріплено намір розробити окремий порядок, за умов дотримання якого вчинення дій у сфері комунікацій не вважатиметься несанкціонованим, тобто, фактично, передбачається легалізація так званого «білого» хакінгу[6].

Таким чином, можемо зробити висновок, що кібербезпека в сучасному суспільстві відіграє достатню значну роль не лише в житті громадян, але й в обороноздатності держави в цілому. Саме тому і відслідковується позитивна тенденція до подальшого розвитку і врегулювання сфери забезпечення кібербезпеки країни, з врахуванням реалії та потреб воєнного стану, що закладає міцне підґрунтя належного рівня захищеності життєвого важливих інтересів суспільства під час використання кіберпростору.

*Список використаних джерел*

1. ITU estimates that approximately 5.3 billion people – or 66 per cent of the world's population – are using the Internet in 2022. URL: https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

2. Over 22 billion records exposed in 2021. URL: https://www.securitymagazine.com/articles/97046-over-22-billion-records-exposed-in-2021#:~:text=There%20were%204%2C145%20publicly%20disclosed,5%25%20fewer%20than%20in%202020.

3. Баранов О. А. Про тлумачення та визначення поняття "кібербезпека" / О. А. Баранов. // Правова інформатика. – 2014. – №2. – С. 60

4. Єрема М. Боротьба з кіберзлочинністю в умовах дії воєнного стану: Закон 2149-IX [Електронний ресурс] / Микола Єрема. – 2022. – Режим доступу до ресурсу: https://jurliga.ligazakon.net/analitycs/210562_borotba-z-kberzlochinnstyu-v-umovakh-d-vonnogo-stanu-zakon-2149-ix.

5. Закон України "Про основні засади забезпечення кібербезпеки України" [Електронний ресурс] // Відомості Верховної Ради України. – 2017. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2163-19#top.

6. Указ Президента України №447/2021 "Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України" [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/447/2021#n7.

## КОНЦЕПЦІЯ ТА ЕТАПИ APT-АТАК (ADVANCED PERSISTENT THREAT)

***А.О. Онащенко,***
магістрант,
***С.В. Левченко,***
ст.викладач кафедри інформаційних систем,
програмування та кібербезпеки,
ПВНЗ «Європейський університет»

У будь-якій справі є професіонали та любителі. У світі інформаційної безпеки також існують хакери, для яких зламування цифрових ресурсів – це професія та основне, досить грошове джерело доходу. Багато хто з них має вузьку спеціалізацію або переваги за цілями, інструментами злому. «Вищий ешелон» такого виду діяльності – це професійні угруповання хакерів, з високим рівнем організації, технічного оснащення і навичок. Вони не бояться важких завдань і беруться за найзахищеніші цілі. Їхні атаки прийнято називати APT-атаками.

APT-атака є різновидом цільової (цілеспрямованої, таргетованої) атаки. Цільові атаки відрізняються від масових атак тим, що спрямовані на конкретну

компанію або цілу галузь. APT-атака добре спланована, сильно розподілена в часі (від кількох днів до кількох років) і включає кілька етапів, поєднуючи комбінацію методів: соціальної інженерії, експлуатації вразливостей, застосування ВПО і т.д. Як правило, проводиться вона злочинними групами – так званими APT-угрупованнями, які мають гроші, технології та знання. Мотивами APT-угруповань можуть бути [2]:

Пряма фінансова вигода (крадіжка коштів компанії, особливо актуальна для банківської галузі). Отримання цінних даних – конфіденційних відомостей або компрометуючих повідомлень (наприклад, для подальшого перепродажу чи шантажу). Саботаж (зупинення діяльності компанії) та ін.

Після атак зловмисники часто-густо залишають «бекдори» для повторного злому. Експерти FireEye опублікували звіт, що підтверджує, що більше половини компаній (64%) зазнають повторної атаки протягом 19 місяців після першої.

Як визначити, що компанія зазнала APT-атаки? Як правило, великі компанії стають об'єктами для APT-атак частіше, ніж невеликі організації.

Деякі ознаки, що вказують на APT-атаку [3].

1. Ненормальні з’єднання. Постійний аудит журналів мережі допоможе виявити аномалії у з'єднаннях. Тільки завдяки усвідомленню нормальної мережі можна виявити можливі аномалії. Наприклад, мережна активність, виявлена в неробочий годинник, може бути ознакою атаки.

2. Ненормальні протоколи. Необхідно перевіряти протоколи, які використовуються у з'єднаннях, особливо якщо це з'єднання з внутрішньої мережі. Наприклад, зловмисники можуть використовувати протокол HTTPS для підключення до зовнішньої сторони, але під час перевірки вмісту там виявляться лише дані HTTP. Часто атакуючі можуть обирати протокол виходячи зі списку дозволених у компанії, тому важливо вивчати з'єднання, навіть якщо вони виглядають нормальними.

3. Збільшена активність електронної пошти. Можна перевіряти поштові журнали, щоб побачити, чи є дивні сплески активності для окремих користувачів. Аномальна активність має бути досліджена, оскільки може бути ознакою атаки фішингу.

4. Невдалі та нерегулярні входи (логіни) [1]. Під час просування через мережу зловмисники можуть знайти Active Directory, поштовий або файловий сервер і отримати доступ до них через експлойт. Або якщо цей спосіб не застосовується – спробувати зламати облікові записи адміністраторів. Перевірка невдалих та успішних спроб входу може виявити спроби зловмисників переміщатися через мережу.

5. Попередження від систем безпеки. Зловмисники можуть використовувати для вирішення своїх завдань не тільки спеціально розроблений інструментарій хакерів, але і легітимні інструменти (наприклад, засоби віддаленого доступу). Деякі рішення безпеки позначають ці, начебто, не шкідливі інструменти як підозрілі. Якщо немає вагомих причин для використання такого інструменту, це може бути ознакою горизонтального пересування зловмисника.

6. Дивні файли. Необхідно перевіряти невідомі великі файли, знайдені в мережі, оскільки вони можуть містити цінні дані, які підготовлені атакуючими

до відправки за межі периметра. Зловмисники зберігають ці файли в системах своєї мети до етапу ексфільтрації, часто приховуючи їх «звичайними» іменами і типами файлів. IT-адміністратори можуть перевірити це за допомогою програмного забезпечення для керування файлами.

Етапи цільової атаки APT [4]:

APT-атаки складаються з кількох етапів – від розвідки до остаточної ексфільтрації даних та наступних атак.

Розвідка. Зловмисники розпочинають свою кампанію з розвідки. Відбувається збір інформації (пошук у відкритих джерелах, соціальна інженерія для отримання додаткових даних, моніторинг даних про нові вразливості тощо). Ведеться підготовка до злому, підбір чи навіть розробка відповідних інструментів.

Проникнення до інфраструктури. Використовуючи знання та інструменти, зібрані на першому етапі, зловмисник проникає в мережу компанії через експлуатацію вразливостей, соціальну інженерію, за допомогою різних технік обходу захисту. Далі він може використати внутрішню розвідку, щоб дізнатися, де саме опинився, інвентаризувати мережу та продумати шляхи закріплення в інфраструктурі.

Закріплення та поширення в інфраструктурі. На цьому етапі зловмисник забезпечує собі зв'язок із командним центром, переміщається по мережі в пошуках доступів до цільових систем або машин, а також підвищує свої привілеї у мережі.

Досягнення мети та ексфільтрація. Зловмисник вирішує своє головне завдання – отримує конкретні дані, порушує бізнес-процеси тощо. Нарешті, зловмисник переказує дані (або кошти) за межі компанії.

Наступні атаки. Якщо зловмисник залишив бекдор, то зможе повернутися до компанії та атакувати її ще раз у будь-який час.

Наведемо кілька прикладів атак APT. Атаки Deep Panda – угруповання, ймовірно, з Китаю провело атаку на Відділ з управління персоналом при уряді США, скомпрометувавши понад 4 мільйони записів, які могли містити подробиці про співробітників спецслужб.

Атаки GhostNet – угруповання з Китаю (згідно з дослідженнями Information Warfare Monitor) провело атаку за допомогою фішингових листів, зосередившись на отриманні доступу до мереж урядових міністерств та посольств. Були скомпрометовані комп'ютери у більш ніж 100 країнах, перетворивши їх камери та мікрофони на пристрої спостереження.

Атаки Stuxnet – імовірно, хробак, розроблений Ізраїлем та США, для атаки на ядерну програму Ірану. Це ВПО могло порушувати роботу машин в іранській ядерній програмі без відома операторів.

*Список використаних джерел*

1. J. Meza, S. Campbell, D. Bailey, “Mathematical and statistical opportunities in cybersecurity,” Paper LBNL-1667E, Lawrence Berkeley National Laboratory, Berkeley, CA, pp. 1–11, 2009.

2. L. Lin, R. Zuo, S. Yang, Z. Zhang, “SVM ensemble for anomaly detection based on rotation forest,” Proc. Of the third international conference on intelligent control and information processing (ICICIP), pp. 150-153, 2012.

3. P.A.R. Kumar, S. Selvakumar, “Distributed denial of service attack detection using an ensemble of neural classifier,” Computer Communications, Vol. 34, pp. 1328–1341, 2011.
4. M.-L. Zhang, Z.-H. Zhou, “A k-nearest neighbor based algorithm for multi-label classification,” Proc. of the International Conference on Granular Computing, pp. 718–721, 2005.

## ЕТАПИ ВПРОВАДЖЕННЯ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

***І. Паньова,***
студентка,
ПВНЗ «Європейський університет»

Забезпечення інформаційної безпеки має бути спрямоване насамперед на запобігання ризикам, а не на ліквідацію їх наслідків. Саме вжиття запобіжних заходів щодо забезпечення конфіденційності, цілісності, а також доступності інформації є найбільш правильним підходом у створенні системи інформаційної безпеки.

Управління інформаційною безпекою - це циклічний процес, що включає усвідомлення ступеня необхідності захисту інформації та постановку завдань; збір та аналіз даних про стан інформаційної безпеки в організації; оцінку інформаційних ризиків; планування заходів щодо обробки ризиків; реалізацію та впровадження відповідних механізмів контролю, розподіл ролей та відповідальності, навчання та мотивацію персоналу, оперативну роботу щодо здійснення захисних заходів; моніторинг функціонування механізмів контролю, оцінку їх ефективності та відповідні коригувальні дії [29]. Управління інформаційною безпекою полягає у плануванні, розгортанні та підтримці комплексу регламентів та процедур, спрямованих на мінімізацію ризиків порушення інформаційної безпеки. Тобто, за своєю суттю, управління інформаційною безпекою є управлінням інформаційними ризиками, націленим на досягнення прийнятного рівня цих ризиків.

Впровадження системи управління інформаційною безпекою (СУІБ) – процес досить тривалий та трудомісткий. У загальному випадку, він включає ряд послідовних етапів, які виконуються організацією, як правило, за допомогою зовнішніх консультантів.

На першому етапі проводиться попередній аудит СУІБ, в ході якого оцінюється поточний стан, здійснюється інвентаризація і документування всіх основних складових СУІБ, визначаються та межі сертифікації та виконується ще ціла низка необхідних підготовчих дій. За результатами аудиту розробляється детальний план заходів щодо підготовки до сертифікації.

На другому етапі виконується оцінка інформаційних ризиків, основною метою якої є визначення застосовності описаних у стандарті механізмів контролю в даній конкретній організації, підготовка декларації щодо застосовності та плану обробки ризиків. На третьому етапі виконується аналіз розбіжностей з вимогами стандарту, в результаті якого оцінюється поточний стан механізмів контролю в організації та ідентифікуються розбіжності із декларацією про застосування. На наступних етапах здійснюється планування та

використання відсутніх механізмів контролю, по кожному з яких розробляється стратегія та план впровадження. Роботи з впровадження механізмів контролю включають три основні складові: підготовка співробітників організації: навчання, тренінги, підвищення обізнаності; підготовка документації СУІБ: політики, стандарти, процедури, регламенти, інструкції, плани; підготовка свідоцтв функціонування СУІБ: звіти, протоколи, накази, записи, журнали подій тощо.

Ефективне інформаційне забезпечення з адекватним захистом інформації є важливим для організації з низки причин. По-перше, ефективне функціонування організації можливе лише за наявності доступу до достовірної та повної інформації. Рівень ІБ має відповідати цьому принципу [2]. По-друге, в результаті діяльності організації створюються продукти та послуги, які доступні ринку або суспільству та потрібні для виконання певних соціально-практичних завдань. Неадекватне інформаційне забезпечення тягне за собою виробництво неякісних продуктів і надання неякісних послуг, які не можуть використовуватися споживачами і ставлять під загрозу існування організації або безпеку процесів, що залежать від неї [3].

Говорячи про систему управління інформаційною безпекою, важливо також виділити методи захисту інформації. Хоча кількість загроз постійно зростає, з'являються нові і нові віруси, збільшується інтенсивність і частота DDoS-атак, розробники засобів захисту інформації теж не стоять на місці. На кожну загрозу розробляється нове захисне програмне забезпечення або вдосконалюється вже наявне. Серед засобів інформаційного захисту можна виділити такі.

Фізичні засоби захисту. До них відносяться обмеження або повна заборона доступу сторонніх осіб на територію, пропускні пункти, оснащені спеціальними системами. Велике поширення набули HID-картки для контролю доступу. Наприклад, при впровадженні цієї системи пройти в серверну або інше важливе підрозділ компанії можуть лише ті, кому такий доступ надано за протоколом.

Основні засоби захисту електронної інформації. Це незамінний компонент забезпечення інформаційної безпеки компанії. До них відносяться численні антивірусні програми, а також системи фільтрації електронної пошти, які захищають користувача від небажаної чи підозрілої кореспонденції. Корпоративні поштові скриньки обов'язково мають бути обладнані такими системами. Крім того, необхідна організація диференційованого доступу до інформації та систематична зміна паролів.

Анти-DDoS. Грамотний захист від DDoS-атак власними силами неможливий. Багато розробників програмного забезпечення пропонують послугу анти-DDoS, яка здатна захистити від таких нападів. Як тільки в системі виявляється трафік незвичайного типу або якості, активується система захисту, яка виявляє та блокує шкідливий трафік. При цьому бізнес-трафік надходить безперешкодно. Система здатна спрацьовувати необмежену кількість разів, допоки загроза не буде повністю усунена.

Резервне копіювання даних. Це рішення, яке передбачає збереження важливої інформації не тільки на конкретному комп'ютері, але й на інших пристроях: зовнішньому носії чи сервері. Останнім часом особливо актуальною

стала послуга віддаленого зберігання різної інформації в хмарі дата-центрів. Саме таке копіювання здатне захистити компанію у разі надзвичайної ситуації, наприклад, у разі вилучення сервера органами влади. Створити резервну копію та відновити дані можна у будь-який зручний для користувача час, у будь-якій географічній точці.

План аварійного відновлення. Крайній захід захисту інформації після втрати даних. Такий план необхідний кожній компанії для того, щоб у максимально стислий термін усунути ризик простою та забезпечити безперервність бізнес-процесів. Якщо компанія з якихось причин не може отримати доступу до своїх інформаційних ресурсів, наявність такого плану допоможе скоротити час на відновлення інформаційної системи та підготовки її до роботи. У ньому обов'язково має бути передбачена можливість запровадження аварійного режиму роботи на період збою, а також усі дії, які мають бути вжиті після відновлення даних. Сам процес відновлення слід максимально відпрацювати з урахуванням усіх змін системи.

Шифрування даних під час передачі інформації в електронному форматі (end-to-end protection). Для забезпечення конфіденційності інформації при її передачі в електронному форматі застосовуються різні види шифрування. Шифрування дає можливість підтвердити справжність інформації, що передається, захистити її при зберіганні на відкритих носіях, захистити ПЗ та інші інформаційні ресурси компанії від несанкціонованого копіювання та використання.

*Список використаних джерел*

1. J. Meza, S. Campbell, D. Bailey, “Mathematical and statistical opportunities in cybersecurity,” Paper LBNL-1667E, Lawrence Berkeley National Laboratory, Berkeley, CA, pp. 1–11, 2009.

2. L. Lin, R. Zuo, S. Yang, Z. Zhang, “SVM ensemble for anomaly detection based on rotation forest,” Proc. Of the third international conference on intelligent control and information processing (ICICIP), pp. 150-153, 2012.

3. P.A.R. Kumar, S. Selvakumar, “Distributed denial of service attack detection using an ensemble of neural classifier,” Computer Communications, Vol. 34, pp. 1328–1341, 2011.

4. M.-L. Zhang, Z.-H. Zhou, “A k-nearest neighbor based algorithm for multi-label classification,” Proc. of the International Conference on Granular Computing, pp. 718–721, 2005.

## АПАРАТНІ ТА АПАРАТНО-ПРОГРАМНІ ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ

***Р.В. Пилипчак[1]***
***Д.Ю. Горик[1]***
[1]магістр, Львівська філія ПВНЗ «Європейський університет»

Метою даної публікації є дослідження можливостей апаратних засобів захисту інформації для їх використання в комп’ютерних та інформаційних системах підприємств.

Апаратні засоби захисту – це електронні, електронно-механічні та інші пристрої, які вмонтовуються або вставляються в блоки електронних систем

опрацювання і передавання даних для внутрішнього захисту засобів обчислювальної техніки - пристроїв введення-виведення даних, процесорів, терміналів, ліній зв'язку.

Основні функції апаратних засобів захисту:

- заборона несанкціонованого (неавторизованого) внутрішнього доступу до баз даних в результаті випадкових чи умисних дій персоналу;
- заборона несанкціонованого (неавторизованого) зовнішнього доступу віддаленого користувача до ресурсів локальної мережі;
- захист цілісності програмного забезпечення.

До апаратних засобів захисту даних *від їх пошкодження* належать:

1) джерела безперебійного живлення апаратури;
2) пристрої стабілізації напруги;
3) пристрої екранування апаратури, ліній зв'язку та приміщень.

До апаратних засобів захисту *від несанкціонованого доступу* належать:

1) пристрої захисту портів комп'ютерної техніки;
2) засоби блокування пристроїв та інтерфейсів введення/виведення;
3) апаратні ключі (призначені для захисту програмного забезпечення і даних від копіювання, нелегального використання і несанкціонованого розповсюдження);
4) електронні замки (виконують контроль завантаження комп'ютера і перевіряють цілісність операційної системи).

До програмно-апаратних пристроїв захисту належать:

1) засоби резервування та архівування даних, що дозволяють повернути стан системи на момент її резервування;
2) пристрої ідентифікації та фіксації терміналів і користувачів при спробах несанкціонованого доступу до комп'ютерної мережі;
3) Е-токени (OTP-токени, смарт-карти, смарт-карти з генератором одноразових паролів, ActiveCard, USB-ключі, USB-ключі з генераторами одноразових паролів). Е-токени найбільш поширені в автоматизованих банківських системах.
4) апаратні шифратори (плати розширення, що вставляються в роз'єми системної плати ПК або виготовляються у вигляді USB-ключа з криптографічними функціями);
5) криптографічні плати, за допомогою яких можна зашифрувати дані та накласти електронний цифровий підпис (ЕЦП) на електронний документ.

OTP-токени використовуються для генерації шестизначних одноразових паролів. Пароль змінюється кожні 60 секунд і призначений для аутентифікації власника з метою його доступу до віддалених інформаційних ресурсів. Цей прилад не є сховищем ключів, він автономний (не прив'язаний до комп'ютера власника). Кожен OTP-токен має унікальний серійний номер.

Смарт-карти – це магнітні карти для зберігання таємних ключів, накладання ЕЦП та шифрування паролів доступу. Для смарт-карти потрібен спеціальний зчитувач карток, який повинен завжди бути з користувачем. У смарт-картах з генератором одноразових паролів останній формується на чіпі

смарт-карти. E-Token з функціями смарт-карти має недолік: PIN-код вводиться не з власної клавіатури пристрою, а з клавіатури терміналу, до якого пристрій підключений.

Одноразовий пароль (OTP) дійсний тільки для одного сеансу аутентифікації, його дія також може бути обмежена певним проміжком часу. Перевага такого паролю порівняно зі статичним полягає в тому, що його не можна використовувати повторно (зловмисник, що перехопиши дані з успішної сесії автентифікації, не може використовувати скопійований пароль для отримання доступу до захищеної інформаційної системи). Алгоритми створення OTP зазвичай використовують випадкові числа, щоб не можна було передбачити подальші паролі на основі знання попередніх. Одноразові паролі можуть генеруватися банком – в цьому випадку користувач має можливість отримувати їх різними способами: в банкоматі, як SMS-повідомлення (в Україні найпоширеніший нині спосіб), як список (TAN-коди) тощо. Одноразові паролі також можуть генеруватися і на боці клієнта з використанням автономних генераторів одноразових паролів (токенів) або рішень, інтегрованих у смарт-карти останнього покоління.

ActiveCard – це пристрій для введення паролю доступу (динамічного коду), який розраховується. Всередині ActiveCard вмонтований мікропроцесор, у пам’яті якого зберігається секретний код. Чотиризначний пароль, що вводиться користувачем, перераховується, тобто створюється спеціальний код. Для зчитування паролю потрібен SmartReader.

USB-ключі (апаратні токени) призначені для захищеного зберігання і використання ключів ЕЦП: формування і перевірки ЕЦП, шифрування, автентифікації, зберігання ключової інформації. Для апаратного токена потрібен USB-порт.

USB-ключі з генераторами одноразових паролів можна використовувати і без USB-порта, тобто в поєднанні з такими пристроями, як смартфони або планшети.

За допомогою USB-ключа можна захистити обліковий запис на комп’ютері, використовуючи складний пароль, який не треба запам’ятовувати. Для цього потрібне програмне забезпечення і USB-ключ, який для нього підходить. За допомогою програми USB отримає ключ для входження в систему. При повторному завантаженні слід вставити апаратний ключ (наприклад, в USB-порт) і ввести PIN-код.

Використовувати цілу плату тільки для функцій шифрування недоцільно з точки зору економічних показників, тому виробники апаратних шифраторів зазвичай намагаються дооснастити їх різними додатковими можливостями, серед яких є такі:

1) *Контроль завантаження комп’ютера*. При його включенні пристрій вимагає від користувача ввести персональну інформацію (наприклад, вставити дискету з ключами). Робота буде дозволена тільки після того, як пристрій розпізнає пред’явлені ключі і вважатиме їх «своїми». В іншому випадку доведеться вилучати шифратор, щоб завантажити комп’ютер. Проте, інформація на ПК теж має підлягати шифруванню.

2) *Контроль цілісності файлів операційної системи.* Використання цього

підходу не дозволить зловмиснику змінити які-небудь дані. Шифратор зберігає в собі список всіх важливих файлів із заздалегідь розрахованими для кожного з них контрольними сумами (або хеш-значеннями). І якщо при наступному завантаженні не співпаде еталонна сума хоча б з одним з них, комп'ютер буде блокований.

3) *Генерація випадкових чисел* для отримання криптографічних ключів та ЕЦП. При кожному обчисленні підпису використовується нове випадкове число.

Плата з усіма перерахованими можливостями називається пристроєм криптографічного захисту даних.

Токени можуть підключатися до персонального комп'ютера і з використанням безпровідникових технологій (RFID, Bluetooth). Тапкі токени передають ключову послідовність локальному клієнту або до найближчої точки доступу без фізичного підключення. Bluetooth-токени можуть працювати в поєднанні з мобільними пристроями. Bluetooh-токенам потрібний власний елемент живлення, тому в них вмонтовується акумулятор, який періодично потрібно заряджати (час безперебійної роботи близько 40 годин). Bluetooth-аутентифікація працює на відстані до 10 метрів. Безпровідникові токени мають відносно невеликий термін придатності – 3-5 років. У їх якості можуть використовуватись також мобільні пристрої – смартфони та планшети. Вони також можуть забезпечувати аутентифікацію, в тому числі з використанням криптографічних ключів.

Висновки. Апаратно-програмні засоби захисту використовуються для аутентифікації користувачів в корпоративних локальних мережах, автоматизованих банківських системах, апаратурі шифрування в системі електронних платежів НБУ, апаратурі накладання ЕЦП відповідальних осіб на електронні документи та його перевірці.

*Список використаних джерел*

1. [Електронний ресурс]. – Режим доступу: http://uk.wikipedia.org/.
2. [Електронний ресурс]. – Режим доступу: http://ua.prostobank.ua/.

## РОЗВИТОК КІБЕРБЕЗПЕКИ В УМОВАХ СУЧАСНОЇ ВІЙНИ

***Я.О. Савченко,***
***О.В. Чмиренко,***
магістранти,
ПВНЗ "Європейський університет"

Сучасна війна — це не ведення активних бойових дій, а також і кібератаки. За даними розвідки, росія розгорнула від 8 до 9 різних вірусів для атаки на обчислювальні системи України. Ця гібридна війна змусила країни та їхні збройні сили створити ефективну систему кібербезпеки, щоб запобігти наслідкам негативних атак у кіберпросторі.

Вторгнення росії в Україну є головною кіберподією, загалом, цього року та найближчого майбутнього. Це має вплив на всі кіберподії, які можуть відбутись найближчими роками. Російський уряд зробив максимально можливе, щоб завдати шкоди критичній та іншим інфраструктурам України. Ще за

декілька тижнів до вторгнення росія почала також завдавати шкоди енергетичним компаніям у Європі. Вона здійснювала це через кіберзлочинні організації. Ці злочинні угруповання атакували також і нафтогазові компанії.

Важливою датою стало 24 лютого – початок вторгнення росії в Україну. Того ж дня російський уряд зламав супутники Viasat, щоб зашкодити українському командуванню під час вторгнення. Збитки поширилися й за межі України, наприклад, було пошкоджено і відключено силові турбіни у Німеччині.

Компанії технологічного та кіберзахисту брали значну участь у припиненні атак разом із спецслужбами та військовими і цим не дозволили росії досягти успіхів у кіберпросторі. Це сталося також завдяки поєднанню систем оборони та розвідки.

Багато російських кібератак були зірвані завдяки активній та швидкій діяльності західних компаній кіберзахисту, обміну розвідданими та зміцненню співпраці з гігантами високих технологій, насамперед Google, Microsoft та ESET. Оборонні компанії стали ключовими цілями у міждержавному конфлікті, що також матиме вплив у майбутньому. Дослідники безпеки Microsoft зафіксували 247 спроб кібератак на Україну, і світ повинен навчитися на цьому прикладі, як продовжувати працювати в умовах постійних атак.

Кіберпростір включає незліченну кількість комп'ютерів по всьому світу, отже жодна держава чи організація не може в односторонньому порядку підтримувати ефективну кібербезпеку. Тісна співпраця та своєчасний обмін кіберподіями та інформацією про нові загрози допоможе покращити колективну кібербезпеку.

Війна в Україні також породила безпрецедентне явище онлайн-війни. Великі групи учасників, які не належать до жодної країни, можуть діяти одночасно, без єдиного центрального органу для координації їхніх зусиль. Ідея мобілізації «глобальної кібер армії» народилася з початком війни ще наприкінці лютого, коли по містах України влучили перші ракети.

Військові всього світу, зокрема України, повинні продовжувати досліджувати можливі способи захисту своїх мереж від зловмисних загроз, а також інвестувати в людей і технології та розробки для створення та підтримки кіберпростору, які є надзвичайно важливими для національної кібербезпеки, оскільки кіберпростір стає загальновизнаною військовою сферою конфлікту, і також потребує необхідного розподілу ресурсів нарівні з придбання військової зброї. В Україні кроки в напрямку покращення кібербезпеки почались ще до початку повномасштабного вторгнення. Президент України Володимир Зеленський в серпні 2021 року підписав указ про створення кібервійськ, мета яких - реагувати на загрози у кіберпросторі, відповідати за інформаційну безпеку та захищати критичну інфраструктуру. А з початком війни влада дозволила незалежним ІТ-фахівцям тестувати вразливості інформаційних систем, що також допомогло покращити кібербезпеку держави. ІТ-спільнота України отримала змогу легально тестувати державні інформаційні системи на наявність вразливостей.

*Список використаних джерел*

1. Захист інформаційного та кіберпростору. Служба безпеки України. URL: https://ssu.gov.ua/zabezpechennia-informatsiinoi-bezpeky

2. УкрІнформ. URL: https://www.ukrinform.ua/rubric-economy/3450550-pisla-vtorgnenna-rf-intensivnist-kiberatak-na-ukrenergo-zrosla-utrici.html
3. План реалізації Стратегії кібербезпеки України від 03.02.2022. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/n0087525-21#n3
4. GlobalSign Blog. URL: https://www.globalsign.com/en/blog/cybersecurity-challenges-companies-must-tackle-now
5. Forbes. URL: https://forbes.ua/news/v-ukraini-stvoryat-kiberviyska-uzhe-pochali-priymati-zayavki-dlya-chogo-tse-17022022-3738

# АКТУАЛЬНІ ПИТАННЯ ЗБЕРЕЖЕННЯ ПЕРСОНАЛЬНОЇ ІНФОРМАЦІЇ ПРАЦІВНИКІВ КОМПАНІЙ ТА ЇЇ РОЗКРИТТЯ НА ВИМОГУ КОНТРОЛЮЮЧИХ ОРГАНІВ

***Є.В. Старчук,***
аспірант,
ПВНЗ "Європейський університет"

Питання захисту персональних даних фізичних осіб в епоху бурхливого розвитку інформаційного суспільства набуває все більшого значення.

Важливим аспектом в цьому напрямку є захист персональних даних працівників компаній, як пов'язаних із виробничими процесами, так і не пов'язаних, оскільки сьогодні значна кількість персоналу працює за віддаленою формою роботи, часто з власних помешкань, з використанням особистих телефонів та комп'ютерів.

Роботодавці завжди прагнуть ефективно контролювати використання робочого часу працівника, тому деякі з них встановлюють спеціальні програми для відстеження та запису дій своїх працівників, в тому числі тих, що працюють віддалено.

Однак, навіть ті працівники, які знаходяться на робочому місці в офісі, також можуть використовувати свої приватні мобільні телефони та електронну пошту для реалізації робочих завдань.

У зв'язку з викладеним, важливим є питання розмежування та ефективного розподілу приватних та робочих процесів, щоб дотримуватися загальновизнаних прав на свободу та недоторканість особистого життя кожної людини.

Щодо національного законодавства, яке на сьогодні регулює вказане питання, можна зазначити наступне. Так, ст. 16 Закону України «Про захист персональних даних» передбачає лише загальний порядок отримання доступу до таких даних за відповідним запитом до носія персональних даних. Ст. 14 цього Закону зазначено, що поширення персональних даних без згоди суб'єкта персональних даних або уповноваженої ним особи дозволяється у випадках, визначених законом, і лише (якщо це необхідно) в інтересах національної безпеки, економічного добробуту, дотримання прав людини та для проведення Всеукраїнського перепису населення. Тобто регулювання доступу до персональних даних закон передає до сфери регулювання діяльності відповідного органу запитувача. Так, наприклад слідчий буде керуватися нормами Кримінально-процесуального кодексу України, який очевидно не містить тих гарантій та інструментів захисту, що має профільний закон. Так, в

параграфі 4 глави 4 КПК України взагалі немає поняття «інформація». Кодекс оперує лише поняттями «документи».

Водночас, інші органи, які не мають конкретних процесуальних законів з питань доступу до персональних даних, взагалі не підпадають під жодні регламентовані процедури щодо обробки цих даних.

Так, виконання вимог Антимонопольного комітету України про надання інформації є обов'язковим згідно ст. 221 Закону України «Про Антимонопольний комітет України». Однак жодного спеціального порядку обробки саме персональних даних закон не містить. Більш того, закон ще й дозволяє поширення таких даних після проведення «консультацій» з суб'єктом персональних даних, не роз'яснюючи що саме за консультації та який їхній формат.

На думку автора, це є прогалиною чинного законодавства, яка підлягає подальшому врегулюванню.

Враховуючи на те, що Україна наразі знаходиться на шляху до Європейського Союзу, було б доцільно проаналізувати безпосередньо підхід країн ЄС до питань захисту персональних даних особи, а саме практику Суду ЄС.

Так, Суд ЄС у своєму рішенні в об'єднаних справах C-339/20 «VD» та C-397/20 «SR» (20.09.2020) постановив, що загальне та невибіркове збереження даних про трафік операторами, які надають послуги електронного зв'язку протягом року від дати, коли вони були записані, не дозволяється як запобіжний захід з метою боротьби із зловживаннями на ринку, включаючи інсайдерські операції.

Такий підхід забезпечує загальні гарантії захисту персональних даних працівників, оскільки дозволяє застосовувати збереження таких даних лише стосовно конкретної особи. При цьому, ми вважаємо, що така конкретна особа повинна бути належним чином ідентифікована за допомогою національних процедур, наприклад адміністративного чи кримінального провадження. І лише з моменту такої її ідентифікації можливо забезпечувати доступ до її даних.

По-друге, Суд ЄС у своєму рішенні в об'єднаних справах C-793/19 «SpaceNet» і C-794/19 «Telekom Deutschland» (20.09.2022) підтверджує, що законодавство ЄС забороняє загальне та невибіркове збереження трафіку та даних про місцезнаходження, крім випадків серйозної загрози національній безпеці. Проте, з метою боротьби з серйозними злочинами, держави-члени можуть, суворо дотримуючись принципу пропорційності, передбачити, серед іншого, цільове або прискорене збереження таких даних і загальне та невибіркове збереження IP-адрес.

Так, Суд у своїх висновках конкретизує що саме і коли може бути розкрито:

– провайдерам можуть бути надані інструкції щодо збереження трафіку та геолокації;

– можуть бути збережені IP адреси;

– може бути дозволена конкретна ідентифікація осіб, які користуються електронними системами.

Враховуючи те, що Україна сьогодні знаходиться у воєнному стані, вказані рішення Суду ЄС можуть бути враховані для розуміння можливостей держави отримувати повний доступ до всієї персональної інформації як працівників

компаній, так і взагалі будь-яких приватних осіб. Звичайно, на сьогодні, рішення суду ЄС не входять до системи джерел права України. Однак, абсолютно логічним є орієнтування на правозастосовну практику сьогодення, щоб ми не мати проблем в майбутньому.

Водночас, після відновлення мирного життя, вважаємо, що надання доступу до персональних даних повиннне відбуватися виключно в індивідуальному порядку та за наявності підстав, встановлених законодавством.

*Список використаних джерел*

1. Кримінально-процесуальний кодекс України, від 13.04.2012 № 4651-VI (Відомості Верховної Ради України (ВВР), 2013, № 9-10, № 11-12, № 13, ст.88)

2. Закон України «Про захист персональних даних», від 01.06.2010 № 2297-VI (Відомості Верховної Ради України (ВВР), 2010, № 34, ст. 481)

3. Закон України «Про Антимонопольний комітет України», 26.11.1993 № 3659-XII (Відомості Верховної Ради України (ВВР), 1993, № 50, ст.472)

4. Рішення суду ЕС в об'єднаних справах C-339/20 «VD» та C-397/20 «SR» (20.09.2020). Режим доступу: https://curia.europa.eu/juris/document/document.jsf?text=&docid=265882&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=2195884 (дата звернення 07.11.2022).

5. Рішення суду ЕС в об'єднаних справах C-793/19 «SpaceNet» і C-794/19 «Telekom Deutschland» (20.09.2022) https://curia.europa.eu/juris/document/document.jsf?text=&docid=265881&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=2021240 (дата звернення 07.11.2022).

## КІБЕРПРОСТІР В УМОВАХ ВІЙНИ ТА ГЛОБАЛІЗАЦІЇ

***Б.Б. Фурик,***
аспірант,
ПВНЗ «Європейський університет»

Прискорення технологічного прогресу в XIX – XX ст. безумовно призвело до розвитку інформаційно сфери, а саме комп'ютерних технологій, в тому числі появи Інтернету. За звітом інтернет-видання *DataReportal* «Digital 2022 Global Statshot» у 2022 році кількість користувачів Інтернету досягла 5 мільярдів людей [1]. Сьогодні майже не існують галузі діяльності (державні, суспільні, промислові, наукові і т.п.), котрі б не використовували інтернет мережі та різноманітне програмне забезпечення. Разом з цим, стрімко зросла зацікавленість до цієї сфери з боку різноманітних розвідувальних та оборонних організацій і, як наслідок, виникли нові поняття «кіберпростір», «хакер», «кібератака» та «кібервійна». Це, в свою чергу, розпалює гонку озброєнь у війнах інформаційних технологій, що призводить до зростання нестабільності та зменшення безпеки для всіх суб'єктів. На сьогодні існує багато визначень поняття «кіберпростір», основними з яких є такі:

- У рекомендації «Про розвиток та використання багатомовності та загальному доступі до кіберпростору», прийнятій на 32-й сесії Генеральної конференції ЮНЕСКО у 2003 р., кіберпростір визначається як віртуальний світ цифрової та електронної комунікації, пов'язаної з глобальною інформаційною інфраструктурою.[2]
- На думку Д.В. Дубова , кіберпростір - середовище, створене

організованою сукупністю інформаційних процесів на підставі об’єднаних загальними принципами та правилами інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем незалежно від форми власності.[3]

- В. М. Фарушев вважає, що кіберпростір – це форма співіснування сукупності матеріальних та нематеріальних об’єктів і процесів, спрямованих на породження, сприйняття, запам’ятовування, переробку та обмін інформацією.[4]
- За визначенням Вікіпедії, хакером особа, що намагається отримати несанкціонований доступ до комп'ютерних систем, як правило з метою отримання конфіденційної інформації. Основною метою кібератак, як правило скоординованих і реалізованих хакерами, є порушення роботи інфраструктури, урядових та військових організацій, а також підрив довіри громадськості до державних інституцій. Кібервійною зазвичай вважають серію кібератак, спрямованих на конкретну країну з метою завдавання збитків, як матеріальних, так і людських.[5]

Розглянемо декілька яскравих випадків:

- У 2018 році команда комп'ютерного реагування на надзвичайні ситуації США випустила попередження про те, що російський уряд проводить «багатоступеневу кампанію вторгнення російських урядових кіберспеціалістів, які націлилися на мережі невеликих комерційних компаній, де вони встановлювали шкідливе програмне забезпечення, проводили фішинг і отримували віддалений доступ до мереж енергетичного сектору». Він також зазначив, що «після того як вони отримали доступ, російські урядові кіберспеціалісти проводили розвідку мережі, пересувались з боку в бік та збирали інформацію, що стосується промислових систем управління». Крім того, хакери були націлені щонайменше на десяток американських електростанцій, водоочисних, авіаційних та державних установ.[6]
- У 2021 році деякі країни-члени ЄС спостерігали зловмисну кібер-діяльність, яку спільно називають Ghostwriter, і пов’язували її з російською державою. Ці атаки були спрямовані на багатьох членів парламентів, урядовців, політиків, представників преси та громадянського суспільства в ЄС шляхом доступу до комп’ютерних систем і особистих облікових записів і крадіжки даних.[7]
- Лише цього 2022 року, за заявою начальника Департаменту кібербезпеки СБУ І. Вітюка, Україна зазнала 3500 кібератак проти українських підприємств, державних установ та військових об’єктів [8].

Якщо в класичному розумінні при веденні активної війни по зброї можна визначити державну належність нападника, то у кіберпросторі це зробити складніше. Коли відбувається атака у кіберпросторі, часто не відома особа та мета атакуючого. Можливості інформаційних технологій стрімко розвиваються, і всі використовують однакову зброю: хакери, злочинці, національні шпигуни, військові, терористи тощо. На сьогодні не існує жодних географічних або адміністративних (в межах кордонів держав) обмежень для здійснення кібератак. І ця зброя практично не має ніяких маркувань, по яким можна було б прив’язати напад до тієї або іншої держави/організації/групи. Це надзвичайно ускладнює оборону та кіберзахист на державному рівні. В умовах війни надзвичайно гострим стає питання забезпечення безпеки кіберпростору держави.

На сьогодні можна виділити по типам поставлених задач у воєнний час такі

методи ведення кібервійни:

- Шпигунство – викрадення секретної інформації на військових об’єктах.
- Саботаж – виведення з ладу логістичних шляхів постачання зброї, інфраструктури та підприємств оборонного значення.
- Пропаганда – контроль як суспільної так і власної думки людей, які живуть у цільовій країні або воюють за неї. Пропаганда може бути використана для викриття ганебної правди, поширення дезінформації, щоб змусити людей втратити довіру до своєї країни або стати на бік ворогів.
- Підрив економіки – атака комп’ютерних мереж економічних установ/підприємств, з метою викрадення або блокування доступу до необхідних ресурсів.

З огляду на вищевикладене можна стверджувати, що в умовах глобалізації та надзвичайно стрімкого розвитку інформаційних технологій робота над кібербезпекою ніколи не припиниться. Уряди мають об’єднатися, щоб спільно визначити, що потрібно зробити, щоб підвищити якість і стандарти для всіх технологій з точки зору кібербезпеки.

Для уряду України на шляху розвитку кібербезпеки країни високопріорітетними повинні бути такі напрямки :

- підвищення цифрової грамотності громадян;
- підтримка освітніх програм у галузі кіберзахисту;
- створення грантів на залучення спеціалістів для забезпечення кібербезпеки держави;
- подальший розвиток вітчизняної нормативно-правової бази у сфері захисту інформації;
- розвиток технологій кіберзахисту засобів рухомого зв'язку, забезпечення апаратної, контентної безпеки, безпеки додатків та сервісів зв'язку;
- підведення кіберпростору України до стандартів ЄС та НАТО, розвиток міжнародного співробітництва, підтримку міжнародних ініціатив у сфері кібербезпеки.

*Список використаних джерел*

1. Звіт «Digital 2022 Global Statshot» / DataReport/2022.
2. Рекомендації «Про розвиток та використання багатомовності та загальному доступі до кіберпростору»/ЮНЕСКО/2003.
3. Кіберпростір як новий вимір геополітичного суперництва : монографія / Д.В. Дубов/НІСД/2014.
4. «Кіберпростір та інформаційний простір, кібербезпека таінформаційна безпека: сутність, визначення, відмінності»/ “Інформація і право”, No 2(5)/2012
5. «Хакер»/Дописувачі вікіпедії/Українська Вікіпедія/
https://uk.wikipedia.org/wiki/Хакер
6. «Russian Hackers Attacking U.S. Power Grid and Aviation»/ Інформаційна агенція Bloomberg/- 2018.
7. Заява високого представника ЄС/Ж.Боррель/сайт Європейської ради/24.09.2021.
8. Інтерв’ю/ начальник Департаменту кібербезпеки СБУ І.Вітюк/телеканал «Ми-Україна»/16.10.2022.

# СЕКЦІЯ IV

# ЦИФРОВА ТРАНСФОРМАЦІЯ У СФЕРІ КУЛЬТУРИ ТА СПОРТУ: НОВІ РЕАЛІЇ ТА ВИКЛИКИ

## КРЕАТИВНІСТЬ ЯК РЕСУРС ІНДИВІДА, ФАКТОР СОЦІАЛЬНО-ЕКОНОМІЧНОГО ТА СОЦІАЛЬНО-КУЛЬТУРНОГО РОЗВИТКУ КРАЇНИ

***Д. Анхім,***
студент,
ПВНЗ «Європейський університет»

Стан сучасного світу характеризується глобалізацією всіх соціально-економічних і суспільно-політичних процесів, трансформацією цінних систем і поглядів, перенасиченістю інформаційного простору і комунікаційних систем. Розглядаючи соціально-економічну ситуацію, необхідно відзначити, що невизначеність ринку, динаміка соціокультурних утворень, підвищені вимоги споживачів і співробітників, гіперконкурентність, призводять до настання кризових явищ і різних міжнаціональних конфліктів. В даний час відбувається зміна епохи світового соціокультурного розвитку на нову епоху креативності [2]. Даний висновок було представлено дослідниками провідного японського аналітичного центру-Інституту Номура (Nomura Research Institute – NRI).

Ядром і змістовим центром нової креативної економіки є творчість та креативна ідея, яку створює людина. Саме творчий потенціал людського ресурсу представлений породжуючим центром існуючої формації. Креативний потенціал індивіда генерує нові відкриття та ідеї, дає можливість продуктивно вирішувати складні проблеми, і, що дуже важливо, одразу впроваджувати їх у практику [1]. У такому підході вже не інформація відіграє ключову роль, а творчі та креативні люди, які генерують нові ідеї та втілюють їх у життя. При цьому саме креативність є оціночним ресурсом індивіда, і рухомим фактором соціально-економічного та соціально-культурного розвитку країни. Разом з тим, важливо підкреслити, що в сучасній економіці креативність розглядається не тільки як ключовий фактор економічної стабільності країни, але і як місія розвитку суспільства, регіону, особистості і т.д. У свою чергу, якщо ключовим фактором економічних знань є освіта та інтелектуальний продукт, інноваційна економіка зосереджує увагу на шляхах використання цих знань, то завдання креативної економіки є забезпеченням умов для генерації ідей, на засобах трансформації запропонованих ідей у якісно новий продукт.

Осмисленням нової креативної епохи стали займатися у другій половині 20 століття такі вчені, як Т.Манро, С.Аріеті, Р.Флоріда та ін. [3]. На думку Т.Монро, основними характеристиками креативної епохи є наявність геніальних людей, держава може надати робочі місця, і у зв'язку з цим є люди, які здатні оцінити і визнати їх творіння [2]. Дослідженням нової креативної економіки продовжив займатися С.Аріети. На думку вченого С. Аріети [4], деякі культури здатні бути

креативними більше, ніж інші, і він назвав ці культури «креативогенними» (creativogenic). Він вважав, що люди стають креативними завдяки впливу трьох факторів (стимулюючої культури, генів і відповідної взаємодії). При цьому автор визначив дев'ять соціально-культурних факторів креативогенного суспільства, серед яких можна виділити:

- наявність культурних засобів і ресурсів, відкритість до різних культурних стимулів, збільшення членами суспільства прагнення до високих досягнень;
- вільний доступ до засобів культури, свободи думок і дій;
- чутливість до різних і навіть контрастних рухів культурним стимулам;
- терпимість до різних думок;
- взаємодія значущих особистостей, стимулювання за допомогою нагороди і поощрения.

Сьогодні можна говорити про становлення та утвердження нової «креатологічної формації», особливого культурно-творчого простору, яке містить у собі такі відносно самостійні сфери й автономні заходи, як креатогенне суспільство, креативна економіка, тотальне мистецтво та універсальна творча особистість.

Термін «креативність» виникло від латинського слова «creato», яке в перекладі означає «творення» або «створення». У вузькому сенсі поняття «креатив» – це процесний фактор творчої діяльності індивіда, в результаті якого з'являється інноваційний продукт праці, що раніше був відсутній на ринку товарів та послуг. При цьому під інноваційним продуктом праці ми розуміємо не лише товар або послугу, але і нові методи дослідження, концепції, алгоритм прийняття рішення тощо.

У свою чергу головною метою управління креативним розвитком організації є залучення, концентрація, стимулювання та розвиток талантів, створення стимулюючої культурно-творчої середовища, організація інноваційної діяльності, а його новими моделями – такі якісно нові форми управління, як креативний менеджмент і менеджмент креативності.

*Список використаних джерел*

1. Божидарнік Т. Формування й розвиток креативного менеджменту на підприємстві / Т. Божидарнік, Н. Василик // Економіст. – 2015. – № 3. – С. 37–39.

2. Arieti S. Creativity: The Magic Synthesis/ S. Arieti - New York: Basic Books, 1976. – P. 429. 2. Day G. A Brief History of How Culture and Commerce were really. Made for each other, Critical Quarterly 2002. – V. 44. – №3 – P. 37–44.

3. Савицька Н.В. Сутність креативного потенціалу підприємства / Н.В. Савицька // Науковий вісник НЛТУ України. – 2011. – Вип.21.6. – С. 301–307.

4. Портер М. Конкурентна перевага. Як досягати стабільно високих результатів / пер. з англ.: Ірина Ємельянова, Ірина Гнатковська. Київ. Наш формат. 2019. 622 с

# ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ГЕНЕРАЦІЇ ЦИФРОВОГО КОНТЕНТУ

***Д.В. Букатов,***
викладач кафедри математичних дисциплін
та інноваційного проектування,
***О.І. Романенко,***
магістрант факультету інформаційних систем та технологій,
ПВНЗ "Європейський університет"

У наш час штучний інтелект постійно впливає на бізнес-процеси, автоматизуючи повторювані та повсякденні завдання навіть для таких складних галузей, як медицина.

Штучний інтелект (ШІ) або, як його ще називають, "допоміжний інструмент генерації контенту" останнім часом наробив доволі багато шуму у сфері створення цифрового контенту. Оскільки компанії намагаються не відставати від зростаючого попиту на оригінальний контент, все частіше в процесах створення цифрового продукту починають використовувати програмне забезпечення або онлайн сервіси, які допомагають згенерувати новий контент за значно менший відрізок часу, ніж це було раніше, зокрема, у сфері розваг. З цієї причини ШІ продовжує знаходити свій шлях до багатьох сучасних творчих бізнес-процесів, приходячи на заміну більшості робітників, які займаються створенням творчого контенту, особливо, це стосується професій, пов'язаних зі створенням творів, музики та візуального контенту.

Розглянемо, яким же чином штучний інтелект вплинув та впливає на даний момент на більшість професій пов'язаних з творчістю. Почнемо з того, яким чином штучний інтелект генерує "оригінальний" контент. Штучний інтелект для генерації ідеї на початку потребує певної початкової інформації, наприклад, текстового опису, частини зображення або, можливо, якогось відрізку звукового запису. В залежності від поданих даних, штучний інтелект аналізує матеріали та створює контент, який, за своєю суттю, є комбінацією даних, що знаходяться у інформаційних базах, доступних цьому штучному інтелекту. Таким чином, мінімізуючи потребу втручання людини, під час створення контенту навіть звичайні люди, які не мають потрібних навичок для виконання роботи творчої направленості, можуть використовувати генератори контенту для автоматизації або "програмування" процесів створення нового контенту. [1]

Головна проблема використання штучного інтелекту для професійних сфер, пов'язаних зі створенням ідейного контенту полягає у тому що його ніхто не обмежує використанням тільки баз даних, якими володіють розробники конкретного ШІ, а якщо бути точнішим - розробники самі надають йому доступ до інтернет-ресурсів для зменшення часу навчання штучного інтелекту [2]. Тобто штучний інтелект у більшості випадків просто витягує і використовує дуже багато інформації з усіх типів баз даних (платних та безплатних) розміщених в інтернеті.

З таким підходом до використання штучного інтелекту без розвинутої світової системи авторського права (прав інтелектуальної власності), існування

дуже багатьох творчих професій може припинитись.

Матеріалу для навчання ШІ в інтернеті на даний момент так багато, що, майже, в кожному жанрі ілюстративної, писемної та музичної сфери генератори контенту можуть створити велику конкуренцію на проектування схожого по стилістиці контенту.

Єдиними реалістичними варіантами вирішення цієї проблеми вважаються варіант адаптації виконавців творчих задач під нові реалії взаємодії людини і штучного інтелекту при створенні нового контенту або розвиток єдиної світової системи контролю та захисту авторського права, який буде обмежувати або враховувати можливе використання ШІ під час розробки комерційного контенту.

*Список використаних джерел*

1.“Deep Dive: How AI content generators work” by Victor Dey
2.“Why You Should (and Shouldn’t) Use AI Content Generation” by Holly Stanley

## ЦИФРОВІЗАЦІЯ МОНІТОРИНГУ НА РИНКУ АЗАРТНИХ ІГОР

***С.М. Дзекунов,***
аспірант,
ПВНЗ «Європейський університет»

Ринок азартних ігор має велику світову історію. Проте ця історія досить суперечлива: відсутність регулювання, легалізація, заборона (тіньовий сектор), повторна легалізація без кінцевого формування ринку. Пропускаючи історичний розвиток, зміну вимог, систем оподаткування та підходів до регулювання галузі акцентуємо увагу на поточних проблемах, шляхах подолання та перспективах розвитку, а саме на цифровізації результатів діяльності гемблінгових компаній з точки зору оподаткування та боротьби з тіньовим сектором.

Згідно Закону України “Про державне регулювання діяльності щодо організації та проведення азартних ігор” [1] в Україні має бути впроваджена система онлайн моніторингу. Відповідно до статті 1 Закону: «Державна система онлайн-моніторингу – спеціалізований програмно-апаратний комплекс, призначений для забезпечення здійснення моніторингу господарської діяльності організаторів азартних ігор, забезпечення відповідності ліцензійним умовам та технічним стандартам; отримання або передачі інформації в режимі реального часу від (до) відповідного грального обладнання через мережу Інтернет або інші канали зв’язку, збору, обробки, накопичення та реєстрації інформації про прийняті ставки, виплачені виграші (призи), здійснені виплати та інші операції, пов’язані з організацією та проведенням азартних ігор, забезпечення захисту інформації від втрати, розкрадання, спотворення, підробки, несанкціонованих дій щодо її знищення, модифікації, копіювання тощо, від несанкціонованого доступу через мережу Інтернет, а також для забезпечення принципу відповідальної гри».

Основна сутність системи полягає в тому, що компанії, які отримали ліцензії будуть фіксувати всі свої трансакції, які призводять до фінансових змін (прийняття і виплата платежів від клієнтів, зроблені ставки та їх результати,

баланси клієнтів, нараховані та відіграні бонуси) у режимі реального часу. Це, в свою чергу, дасть змогу зафіксувати реальну базу для оподаткування виграшів фізичних осіб (18% податок на доходи фізичних осіб та 1,5% військовий збір) та розмір податку на доходи компанії (5-30% в залежності від виду діяльності). [2] До впровадження Системи компанії сплачують потрійний розмір вартості ліцензії.

Слід зазначити, що поточна вартість ліцензії є найбільшою у Європі, тому впровадження Системи дасть змогу знизити її вартість, зробити ринок більш прозорим та привабливим для іноземних інвесторів, особливо, в частині онлайн оперування. Саме цифровізація моніторингу зробить галузь відкритою, прозорою та однією з передових в Євросоюзі та унеможливить корупційні дії Регулятора та силових структур.

**ВАРТІСТЬ ЛІЦЕНЗІЙ РІЗНИХ ВИДІВ АЗАРТНИХ ІГОР**
**на період 2021 року**

| Вид ліцензії | Кількість мін-х заробітних плат | Вартість за 1 рік |
|---|---|---|
| Казино в м. Київ | 60 000 | 72 000 000 |
| Казино в інших містах | 30 000 | 36 000 000 |
| Казино в мережі Інтернет | 6 500 | 23 400 000 |
| Букмекерська діяльність в мережі Інтернет | 30 000 | 108 000 000 |
| Зал ігрових автоматів | 7 500 | 9 000 000 |
| Покер в мережі Інтернет | 5 000 | 6 000 000 |

*Одна мінімальна заробітна плата станом на 2021 рік складає 6 000 грн

*Щорічна плата за ліцензію до впровадження Державної системи онлайн-моніторингу

КОМІСІЯ З РЕГУЛЮВАННЯ АЗАРТНИХ ІГОР ТА ЛОТЕРЕЙ

На сьогоднішний день держави-члени Євросоюзу мають національні системи онлайн-моніторингу, але вони не повноцінні та недосконалі. Для прикладу, в Румунії компанія щодня направляє відомості за попередній день, на Кіпрі та Мальті такі системи взагалі відсутні, Естонія – має майже еталонну систему, в Польщі – щомісячні звіти, в Іспанії – частково реалізовано онлайн систему.

Попередня оцінка вартості підтримки Системи мала скласти близько 2 млн. грн. на рік. [3] Вартість розробки, наразі, не оцінена. Варто зазначити, що альтернативним методом цифровізації моніторингу є впровадження оподаткування кожної платіжної транзакції, яку проводить банк або фінансова установа від імені клієнта на рахунок оператора азартних ігор. За такою схемою працює досить велика кількість країн. Зазвичай, з кожного депозиту утримується 1-2% і з кожної виплати, в залежності від розміру 1-23% (прогресивна шкала з порогами). За такої схеми постає існує потреба ліцензування уповноважених фінансових агентів на проведення фінансових трансакцій в сфері бетінгу і їх затвердження, як податкових агентів. [4]

У будь-якому випадку, обидві схеми передбачають боротьбу з міскодінгом та доступністю нелегальних сайтів. Окрім цього, важливим є верифікація клієнтів та інтеграція різноманітних реєстрів, зокрема – Реєстр лудоманів.

*Список використаних джерел*

1. Закон України “Про державне регулювання діяльності щодо організації та проведення азартних ігор”. URL: https://zakon.rada.gov.ua/laws/show/768-20#Text
2. Манзюк В.В., Заборовський В.В. Динаміка становлення грального бізнесу в Україні. URL: https://doi.org/10.32782/2524-0390/2020.1.57
3. Комісія з регулювання ринку азартних ігор та лотерей. URL: https://www.gc.gov.ua/
4. Воронцова Ю. В. Кримінально-правові заборони щодо проведення та організації азартних ігор і лотерей на тлі змін регулятивного законодавства України. Вісник ЛДУВС ім. Е. О. Дідоренка. 2022. Вип. 1 (97).

## ВИКОРИСТАННЯ ЦИФРОВИХ ЗАСОБІВ КОМУНІКАЦІЇ

***Ю.В. Костенко,***
аспірант,
ПВНЗ «Європейський університет»

Останні роки економічні процеси швидко переходять в онлайн. Цього року в Україні з'явився ще один дуже сумний чинник, який прискорює цей процес. Цим чинником стала, на жаль, війна. В цих умовах набуває широкого вжитку використання цифрових засобів комунікації. Майже всі розуміють, скільки часу і грошей можна заощадити, проводячи зустрічі онлайн замість оренди приміщень. Також на сьогоднішній день відбувається зменшення концентрації людей в одному й тому самому місці, що являється додатковим чинником безпеки.

Існує значна кількість таких засобів, які прийнято називати месенджерами. Але передача повідомлень - це не єдина, хоча і основна їх функціональна задача та можливість. Окрім неї також доступні такі функції, як передача аудіо- та відеофайлів в різних режимах, відеоконференції, спільна робота з файлами, планування задач, зберігання файлів.

Можна виділити два великих продукти, які зараз широко використовуються у багатьох сферах бізнесу. Один з них це – Zoom, розроблений компанією Zoom Video Communications [1]. Інший продукт – це Microsoft Teams від корпорації Microsoft [2]. Ці продукти призначаються для ведення онлайн конференцій, але кожен з них має свою специфіку, завдяки якій визначається сфера їх використання.

Microsoft Teams позиціонується, як корпоративний інструмент для проведення відеоконференцій серед співробітників організації. Zoom же, навпаки, є інструментом для проведення відкритих конференцій, хоча виробник цього сервісу також позиціонує його, як рішення для освіти, фінансів, органів влади та закладів охорони здоров'я. У свою чергу, Microsoft Teams також пропонує платформу Microsoft Teams for education. На сайті компанії Microsoft вона описана таким чином: “Цифровий центр, який об’єднує зустрічі, вміст і програми в одному місці. Педагоги можуть створювати спільні класи, об’єднуватися в професійні навчальні спільноти та спілкуватися з персоналом школи” [3].

Якщо порівнювати основну функціональність цих програм, то можна побачити, що вони мають багато спільного (табл. 1).

*Таблиця 1*

**Порівняльна характеристика функціональності програм**

| Функція | Microsoft Teams | Zoom |
|---|---|---|
| Відео, аудіодзвінки | Так | Так |
| Чат | Так | Так |
| Запис | Так | Так |
| Обмін файлами | Так | Так |
| Сумісна робота над файлами | Так | Ні |
| Підтримка ботів | Так | Ні |
| Планування зустрічей з поштовими клієнтами | Так в MS Outlook | Ні |

Але між цими платформами також є і відмінності. Microsoft Teams - це платформа для сумісної роботи. Вона надає повну інтеграцію з офісним пакетом Microsoft 365, що може бути значною перевагою для багатьох компаній, які використовують цей офісний пакет [4]. Також значною відмінністю цих двох систем є життєвий цикл чату конференції. В Microsoft Teams чат конференції може існувати ще до початку трансляції та залишається доступним для обміну повідомленнями після її закінчення. В Zoom можна зберегти чат локально і передивлятися його при перегляді запису конференції, але не мати можливості додавати та отримувати нові повідомлення. Корисно також розглянути тарифні плани обох програмних продуктів.

Microsoft Teams в безкоштовному варіанті надає можливість проводити групові конференції тривалістю до 60 хвилин, а приватні дзвінки взагалі мають обмеження 30 годин по тривалості [5]. В Zoom з безкоштовним тарифним планом тривалість конференції обмежена до 40 хвилин і є можливість використовувати автоматичні субтитри, хоча лише англійською мовою [6]. Також в Microsoft Teams кожен користувач має 5 ГБ хмарного сховища, в той час, як в Zoom хмарне сховище користувачам безкоштовної версії не надається. Якщо порівняти максимальні тарифні плани, то ми побачимо, що вартість даного тарифу Zoom становить 199,90 доларів США за кожного користувача на один рік, і це за умови придбання від 10 ліцензій одразу. При цьому користувачі отримують 5 ГБ хмарного сховища. В той час, як при використанні максимального тарифного плану для Microsoft Teams доведеться сплатити 150 доларів на рік за користувача. І при цьому користувач фактично отримує не лише Microsoft Teams, а весь офісний пакет Microsoft 365 Бізнес Стандарт. Субтитри при цьому доступні більш ніж 30 мовами, в тому числі й українською.

Дивлячись на зазначені особливості, можна зробити висновок про те, що Microsoft Teams навіть у безкоштовному варіанті пропонує дещо більші

можливості, а максимальний тариф взагалі надає можливість користуватись одним з найвідоміших інтегрованих офісних пакетів, а не лтше засобом комунікації. Завдяки більш тісній інтеграції з офісними пакетами, Microsoft Teams є більш прийнятним варіантом для використання у бізнесі.

На жаль, сьогодні треба відмітити ще один момент. Жоден з засобів цифрової комунікації не може працювати стабільно в умовах пошкодженої інфраструктури. Але кожен з цих програмних пакетів намагається бути максимально стійким до коливань якості Інтернет-з'єднання.

*Список використаних джерел*

1. Відеоконференцзв'язок, хмарна телефонія, вебінари, чат, віртуальні заходи Zoom. (2022, Nov. 5) Zoom US. URL: https://zoom.us

2. Довідка Microsoft Teams (2022, Nov. 5)Microsoft. URL: https://support.microsoft.com/uk-UA/teams

3. Teams for education on Microsoft Learn. (2022, Nov. 5) Microsoft Learn. URL: https://learn.microsoft.com/en-us/training/educator-center/product-guides/teams

4. Вхід і початок роботи в Teams. (2022, Nov. 5) Підтримка Office. URL: https://support.microsoft.com/uk-ua/office/вхід-і-початок-роботи-в-teams-6723dc43-dbc0-46e6-af49-8a2d1c5cb937

5. Порівняння планів Microsoft Teams і цін на них. (2022, Nov. 5) Microsoft Teams. URL: https://www.microsoft.com/uk-ua/microsoft-teams/compare-microsoft-teams-options?activetab=pivot:primaryr1

6. Тарифні плани та вартість Zoom Video Communications. (2022, Nov. 5) Zoom. URL: https://zoom.us/pricing

## ЦИФРОВА ТРАНСФОРМАЦІЯ У СФЕРІ СПОРТУ: НОВІ РЕАЛІЇ ТА ВИКЛИКИ

***В.Ю. Лозинський,***
аспірант спеціальності “Право”,
ПВНЗ “Європейський університет”

Актуальність теми обумовлена тим, що невід'ємною частиною розвитку сучасного суспільства є впровадження цифрових технологій у всі сфери життя. Серед них спорт не є виключенням. Фізична культура і спорт відіграють одну з найважливіших ролей у житті людини та суспільства. Зараз сучасна спортивна галузь України переживає суттєві потрясіння.

З початком пандемії COVID-19 сфера спорту в Україні отримала великий для себе виклик. А з початком війни 24 лютого 2022 року ці виклики лише зросли та стали найтяжчими і найоб’ємнішими за всю історію нашої незалежності. Для спортсменів настав час, який унеможливлює нормально тренуватися та приймати участь у змаганнях. Вболівальникам також стала недоступною функція відвідування спортивних заходів і слідкування за спортивними подіями та своїми кумирами. Для звичайних громадян тема спорту відійшла ледь не на останній план. У підсумку всі негативні події прямо пропорційно впливають на результати у спорті вищих досягнень, адже є певна вертикаль: любитель, аматор, професіонал. Чим більше людей цікавляться спортом, тим більша конкуренція, тим вагоміші результати, тим краще для держави, тим більше впізнаваність

країни.

Цифрова трансформація у сфері спорту ледь не остання надія на збереження цього важливого для суспільства напрямку. Першим тригером для розвитку цифрової трансформації у спорті стала пандемія COVID-19, а війна з російською федерацією повинна суттєво прискорити цей процес. Нові реалії потребують негайних дій для втілення цифровізації у спорт в цілому.

Щоб вирішити цю проблему, по перше, треба використовувати цифрові технології у тренуванні спортсменів і у підсумку зробити їх більш безпечними і менш ризикованими в реаліях війни та після її закінчення. По друге, завдяки цифровим технологіям треба залучати вболівальників до перегляду спортивних подій (а можливо і перегляду тренування спортсменів) в режимі он-лайн. По третє, потрібен механізм для залучення більшої кількості людей до занять спортом. Для потенційних та діючих спортсменів і вболівальників потрібно забезпечити безпечність, доступність та зручність, і тут не обійтися без цифрової трансформації.

В підсумку запропоновано створення єдиної всеукраїнської спортивної платформи та додатку, які можуть об'єднати всі види професійного та аматорського спорту, де кожна людина може у будь-який час подивитися ту чи іншу подію, або банально дізнатися результат протистояння, чи просто знайти місце, де їй можна безпечно займатися спортом, будь то індивідуальний чи командний вид. Також потрібно заохоти і підвищити загальну мотивацію людей до занять спортом завдяки цифровізації.

Таким чином, розвиток спорту в теперішні часи просто не можливий без цифрової трансформації, якій треба приділяти особливу увагу в нинішніх реаліях. І саме цифрова трансформація в сфері спорту дасть новий поштовх у розвиток цього напрямку. Саме тому державі так важливо приділяти необхідну увагу зміцненню та розвитку спортивної сфери, а цифрова трансформація нині є найперспективнішим та дієвим механізмом її модифікації, вдосконалення та розвитку. Отже, цифрова трансформація у спорті є актуальним вектором розвитку та формуванням здорового суспільства.

*Список використаних джерел*

1.Digital Transformation of Sports Entities by 2025. How will it look like? GSIC (Based on GSIC Members Survey) 48c.

2.Pandemic speeds up digital transformation in sports By Eric Avidon. Published: 01 Oct 2020 techtarget.com

3.Сучасні проблеми фізичного виховання у спорті. Вісник ЛНУ імені Тараса Шевченка № 3 (351), 2022

# СУЧАСНІ РЕАЛІЇ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ У СФЕРІ КУЛЬТУРИ ТА СПОРТУ

***А.В. Свириденко***,
аспірант,
***А.В. Невзоров***,
к.т.н., доцент,
доцент кафедри математичних дисциплін
та інноваційного проектування,
ПВНЗ «Європейський університет»

На сьогоднішній день можна чітко сказати, що саме цифрова трансформація виділяє Україну у світі. Гарним прикладом є онлайн-сервіс «Дія» - Держава у смартфоні, ініційований Міністерством цифрової трансформації України. Саме за допомогою цифрових технологій ми будуємо цифрову державу, яка стає сервісом, без черг та корупції. Тому розвиватися та діджиталізуватись мають усі галузі, а особливо, ті, що сприяють духовному та фізичному розвитку людини і загалом всього суспільства.

Розглянемо, які цифрові трансформації впроваджують у сфері культури. Зі слів заступника Міністра культури та інформаційної політики з питань цифрового розвитку, цифрових трансформацій та цифровізації Артема Льозіна, вже на стадії реалізації знаходяться декілька масштабних цифрових проєктів, які за словами заступника Міністра, дозволять створити умови для осучаснення та прозорості ведення процесів у сферах охорони культурної спадщини, мистецтва, туризму та курортів, бібліотек та видавничої справи. Серед них такі проєкти, як цифрова трансформація охорони культурної спадщини (е-Спадщина), цифрова трансформація мистецтва (е-Мистецтво), цифрова трансформація бібліотек та книговидавничої справи (е-Книга).

Якщо розібрати детально ці проєкти, можна сказати, що кожен з них не тільки допомагатиме розвивати культуру, а й сформує чіткий механізм роботи. Наприклад, проєкт е-Спадщина забезпечить цифровізацію інфраструктури музеїв, що стане основою для осучаснення та прозорості ведення процесів, впровадить онлайн-реєстр, що містить інформацію про об’єкти культурної спадщини. Така інформація є необхідною для коректного планування видатків, відновлення об’єктів у первинному вигляді та надання дозволів. А онлайн-сервіс, що містить у собі всі елементи національного переліку нематеріальної культурної спадщини у вигляді списку та облікових карток, посилання на інші сайти, що зберігають культурну спадщину, допоможе зареєструвати нематеріальну спадщину. Щодо проєкту е-Мистецтво – це онлайн-платформа для викладачів та здобувачів освіти з відкритим доступом до інноваційних методичних напрацювань. Матеріали, розміщені в репозитарії, дозволять вчасно модернізовувати змістовну компоненту мистецької освіти та справедливо оцінювати інноваційність та ефективність розроблених і оприлюднених методик. Це система для прозорого та анонімного оцінювання заявок експертами та членами комітетів з присудження премій, стипендій та грантів діячам культури і мистецтв. Платформа е-Мистецтво дозволить заощадити час, пришвидшити

процес підготовки документів, спростити участь в комітетах експертів з регіонів України та контроль за дотриманням законодавства в сфері фінансової підтримки діячів культури і мистецтв. Чудове рішення старих проблем по-сучасному.

Також не слід забувати і про розвиток фізичної культури і спорту. Міністр цифрової трансформації України Михайло Федоров повідомив, що сучасний розвиток спорту у всьому світі неможливий без використання інформаційних технологій. Для цього у Стратегії розвитку фізичної культури та спорту передбачена діджиталізація цієї сфери. Мета проєкту: створення електронних реєстрів, з якими стане можливий підрахунок статистики та аналіз поточного стану галузі з точними показниками, що дуже важливо для прийняття зважених управлінських рішень та відстеження ефекту від впроваджених реформ; налаштування бізнес-процесів у Мінмолодьспорті та підпорядкованих йому закладах, установах та підприємствах; розроблення механізму відстеження фізичної активності людей різних груп населення зі шкільних років, завдяки цьому можна оцінити спортивний потенціал кожної людини, та розробка і впровадження технічного механізму для впровадження та адміністрування пілотного проєкту «Гроші ходять за послугою», який допоможе населенню отримувати доступні та якісні фізкультурно-оздоровчі послуги. Тут же додали дуже зручну функцію, яка позбавить користувачів бюрократичних наслідків. Йдеться про отримання звань майстра спорту, майстра спорту міжнародного класу, заслуженого майстра спорту, заслуженого тренера України. Отже, буде створено можливість подавати документи в електронному вигляді. Той, хто подав необхідні документи, бачитиме всі деталі їх розгляду. Окрім цього, завершується розробка публічного реєстру, де кожен бажаючий матиме змогу дізнатися, коли, кому і за які досягнення були присвоєні ті чи інші звання. У подальшому із запуском наступних електронних ресурсів дані будуть синхронізуватися і відпаде навіть потреба сканувати частину документів.

Це лише незначні кроки до кардинальних змін, але те, що процес запустився – додає впевненості, що майбутні цифрові трансформації набуватимуть ще більших об’ємів та дозволять покращити всі сфери життя кожної людини.

Таким чином, цифрова трансформація у сфері культури та спорту дійсно набуває нових масштабів. На даний момент в Україні діджиталізація проходить на належному рівні, навіть у порівнянні з іншими, більш економічно розвиненими країнами. Тому, незважаючи на нові реалії та виклики, можна стверджувати, що в Україні спорт та культура розвиваються за сучасними вимогами та технологіями.

*Список використаних джерел*

1. Проєкти цифрової трансформації. Інтернет-ресурс. URL: https://plan2.diia.gov.ua/projects

2. Департамент освіти і науки Рівненської обласної державної адміністрації. URL: https://www.rvosvita.org.ua/

3. Інтернет - ресурс федерації боксу України. URL: https://www.fbu.org.ua/

# ЦИФРОВА ТРАНСФОРМАЦІЯ В ЕКОНОМІЦІ, МЕНЕДЖМЕНТІ І БІЗНЕСІ. ПРОБЛЕМИ НАУКИ, ПРАКТИКИ ТА ОСВІТИ

***Матеріали***
***XXVIII міжнародної науково-практичної конференції***

***24 листопада 2022 р.***

***до 31-річчя Європейського університету***

Підписано до друку 20.12.2022. Формат 60x84 1/16.
Папір офсетний. Гарнітура Times New Roman.
Ум. друк. арк. 8,83. Зам. № 40.

Друк: поліграфкомбінат Європейського університету.
03115, Україна, Київ-115, вул. Депутатська, 15/17.
Тел.: (+38044) 503-33-96

Реєстраційне свідоцтво ДК №3833 від 14.07.2010 р.