НАЦІОНАЛЬНА АКАДЕМІЯ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ

# КОМУНІКАТИВНІ СТРАТЕГІЇ ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА: ЛІНГВІСТИКА, ПРАВО, ПРАВО, ІНФОРМАЦІЙНА БЕЗПЕКА

МАТЕРІАЛИ
XII ВСЕУКРАЇНСЬКОЇ НАУКОВОЇ КОНФЕРЕНЦІЇ
МОЛОДИХ УЧЕНИХ, СТУДЕНТІВ ТА КУРСАНТІВ

(Київ, 9 квітня 2021 року)

**Київ**
**2021**

**НАЦІОНАЛЬНА АКАДЕМІЯ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ**

# КОМУНІКАТИВНІ СТРАТЕГІЇ ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА: ЛІНГВІСТИКА, ПРАВО, ІНФОРМАЦІЙНА БЕЗПЕКА

Матеріали
XII Всеукраїнської наукової конференції
молодих учених, студентів та курсантів
Частина І

(Київ, 9 квітня 2021 року)

Київ
2021

**Матеріали XII Всеукраїнської наукової конференції молодих учених, студентів та курсантів «Комунікативні стратегії інформаційного суспільства: лінгвістика, право, інформаційна безпека».** – Київ : Нац. акад. СБУ, 2021. Ч. І. – 196 с.

До збірника увійшли матеріали XII Всеукраїнської конференції молодих учених, студентів та курсантів «Комунікативні стратегії сучасного інформаційного суспільства: лінгвістика, право, інформаційна безпека», присвяченої актуальним питанням стратегічних комунікацій в умовах ООС; публічної дипломатії та зв'язків з громадськістю; кризових комунікацій, зокрема стратегіям налагодження взаємопорозуміння; технологій інформаційно-психологічного протиборства; взаємодії інститутів сектору безпеки і оборони та суспільства; ґендерного підходу до забезпечення національної безпеки; комунікативних стратегій у правовому вимірі; лінгвістики тексту й теорії комунікації в системі національної безпеки; сучасної лінгвоконцептології та лінгвокультурології; перекладу; методики викладання іноземних мов, тощо.

Запропонований збірник матеріалів буде корисною для здобувачів вищої освіти, аспірантів, наукових співробітників.

Автори несуть повну відповідальність за підбір, точність наведених фактів, цитат, галузевої термінології, власних імен та інших відомостей.

Матеріали конференції публікуються в авторській редакції.

# ЗМІСТ

до протесту і під час масового зібрання неодноразово повторював, що *«кожний **має сам приймати рішення** щодо свого життя. Нам не потрібні політики»* [2]. Дискурс фанатів розширив свої межі і відбулося переплетіння з іншим дискурсом. Представники фанатського угруповання вийшли з гаслами *«Freiheit»* (нім. *свобода*) і схвально відреагували на виступ лідера праворадикальної ініціативи. Це відбувалося в той час, коли комунікації суспільства спрямовані на взаємопідтримку і пропагування розуміння того, що вихід із складної ситуації залежить від свідомості кожного. Такі комунікації в поєднанні з праворадикальними течіями сприяють формуванню негативного образу футбольного фаната в суспільстві і посилюють сприйняття його як каталізатора і учасника масових заворушень.

Отож, дослідження показало, що дискурс фанатського угруповання відреагував на виклики сьогодення, адаптувався до нових комунікативних умов. Семіотика їх комунікації зазнала змін. В умовах пандемії активувалися невербальні й паравербальні засоби. Це відбулося в позитивній площині у вигляді підтримки команд і усвідомлення суспільних проблем та пропозиції щодо їх вирішення. Водночас знайшло вираження і негативне спрямування через масові заворушення.

**ЛІТЕРАТУРА**

1. Антоненко О. Фанат на карантине. Как пандемия меняет футбол и его болельщиков, 2020. Режим доступу: https://www.bbc.com/russian/features-54609485.
2. BZ. Bei Demo gegen Corona-Maßnahmen. Режим доступу: https://www.bz-berlin.de/sport/fussball/weltmeister-thomas-berthold-fordert-neue-partei.
3. Claus R. Die Mobilisierung für den Anmarsch. Режим доступу: https://twitter.com/robertclaus13/status/1333345143135612930.
4. Faszination Fakurve. Режим доступу: https://twitter.com/FasziFankurve/status/1354742954120896517/ photo/1.
5. MUFC Fans' Foodbank. Режим доступу: https://twitter.com/mufcfoodbank.
6. tarasov23. Інстаграм. Режим доступу: https://www.instagram.com/p/B99PW43iF0-/?utm_source=ig_embed.
7. WBC Ультрас Динамо, 29.05.2020. Режим доступу: https://t.me/wbc_kyiv/3078.
8. WBC Ультрас Динамо. Фейсбук. Режим доступу: https://www.facebook.com/wbc.kyiv/posts/2818386268408432.

**Городянська Л. В.,** кандидатка економічних наук, доцентка
Військовий інститут КНУ імені Тараса Шевченка

## ЕКОНОМІЧНА БЕЗПЕКА ПІДПРИЄМСТВА В СУЧАСНИХ УМОВАХ

Світова економічна криза, що спричинена низкою негативних факторів, тривалий геополітичний конфлікт на Сході України та наслідки пандемії призвели до регресу економіки країни та суттєвому зниженню частки висококваліфікованих працівників. Інтеграція України до Європейського освітнього простору, підсилення глобалізаційних процесів на тлі ускладнення соціально-економічних явищ супроводжується витоком молоді та кваліфікованих трудових ресурсів разом із значними втратами населення нашої країни шляхом природного убутку. Усе це призвело до суттєвих негативних

структурних змін в економіці країни, зростання рівня безробіття, зниження інтелектуального потенціалу вітчизняних підприємств та їх економічної безпеки.

Тісні взаємозв'язки й обумовленість світових економічних процесів разом із насиченням усіх видів діяльності та сфер життєдіяльності суспільства електронно-цифровими пристроями й засобами, розвитком і поширенням інформаційних технологій (ІТ) в контексті налагодження електронного комунікаційного обміну між ними вимагають комплексного підходу щодо їхнього вивчення й удосконалення. Це соціальне явище є цифровізацією або цифровими технологіями й ним охоплено усі сфери суспільного життя. Однак застосування усіх цих новітніх інформаційних технологій в економіці є дуже привабливим для кіберзлочинців по всьому світу й вимагають дотримання певних заходів економічної безпеки. Масштаб і темпи цифрових трансформацій, що відбуваються в суспільстві разом із убутком значної частки кваліфікованих працівників, вимагають відновлення інтелектуального потенціалу держави та дотримання вимог кібербезпеки як частини інформаційної безпеки будь-якого суб'єкта підприємництва (підприємства), господарська діяльність якого має бути захищеною від впливу зовнішніх та внутрішніх загроз.

Інформаційною базою для проведення дослідження стали чинні нормативно-правові документи та прогнози, що розкривають перспективні напрями розвитку України [1; 3; 7], дозволяють прогнозувати наслідки пандемії [1; 8] та регламентують особливості функціонування ІТ, які дедалі ширше використовуються як в економіці, так і в сфері безпеки [1, с. 4-7]. Беручи до уваги, що з метою модернізації економіки та «подолання економічної відсталості потрібні інвестиції» [1, с. 23], проаналізуємо основні джерела надходження капітальних інвестицій. Огляд [1, с. 17-25] показав, що основними серед капітальних інвестицій є власні кошти підприємств (65,4 % у 2019 р.), натомість банки майже виключені з інвестиційного процесу, частка кредитних коштів становить лише 10,8 % за підсумками 2019 року (7,8 % – у 2018 р.). Враховуючи, що відновлення економіки та покращення макроекономічної ситуації залежить від фінансової політики держави та від успішного управління підприємствами власними економічними ресурсами, серед яких ключовими є фінансові ресурси, трудові ресурси та техніко-технологічні ресурси, проблема є комплексною. Разом із тим, створення умов для економічного розвитку підприємства в сучасних умовах нерозривно пов'язано з процесами цифровізації економіки та важливістю дотримання вимог економічної безпеки.

**Метою** дослідження є формування пропозицій щодо напрямів економічної безпеки суб'єктів підприємництва в сучасних умовах.

Напрям цифровізації, як підкреслено у Концепції [3], є ключовим напрямом розвитку світової економіки. Разом з тим виникає нагальна потреба у розробці пропозицій щодо подолання негативних наслідків світової економічної кризи, пандемії та інших викликів. У розв'язанні цих завдань важливе значення набуває інтелектуальний потенціал підприємства. Так, аналіз консенсус-прогнозу [8, с. 13-14] щодо напрямів економічної політики держави виявив можливість вибору одного з 15 варіантів підтримки бізнесу під час карантинних заходів або можливість їх комбінування. Серед цих напрямів

важливе місце займають питання збільшення фінансування на перенавчання та систему соціальної підтримки безробітних. Вважаємо доцільним планувати на підприємстві заходи з навчання та перенавчання з метою оволодіння працівниками навичками й уміннями не лише в професійній сфері, а й в сфері цифрових технологій, баз даних, принципів інформаційної безпеки та захисту інформації, можливих способів атак зловмисників, а також методів їх уникнення.

Тісні взаємозв'язки й обумовленість наукових категорій «економічна безпека», «інформаційна безпека», «суб'єкти підприємництва» вимагають комплексного підходу щодо їхнього вивчення та формування пропозицій для керівництва підприємств з метою подолання негативних викликів і загроз фінансово-господарській діяльності підприємства.

Огляд чинної нормативно-правової літератури [4-6] показав, що визначення дефініції «інформаційна безпека» розкривається лише у [5]. Згідно зі ст. 13 Закону України «Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» [5] «інформаційна безпека» тлумачиться як «стан захищеності життєво важливих інтересів людини, суспільства й держави, при якому запобігається нанесення шкоди» через:

- неповноту, невчасність та невірогідність інформації, що використовується;
- негативний інформаційний вплив;
- негативні наслідки застосування інформаційних технологій;
- несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації.

Використання інформаційних технологій, наприклад, таких як технологія великих даних, штучний інтелект, технологія блокчейн, квантові технології, робототехніка, віртуальна реальність тощо, потребують визначення комплексу заходів з метою дотримання вимог економічної безпеки. Забезпечення вимог економічної безпеки на підприємстві потребує визначення функціональних складових, серед яких провідними є:

- фінансова – досягнення найбільш ефективного використання ресурсів;
- політико-правова – дотримання чинного законодавства, всебічне правове забезпечення правової діяльності підприємства;
- інтелектуальна і кадрова – збереження і розвиток інтелектуального потенціалу підприємства, ефективне управління персоналом;
- техніко-технологічна – ступінь відповідності застосованих на підприємстві технологій сучасним світовим аналогам за умови оптимізації витрат ресурсів;
- інформаційна – ефективне інформаційно-аналітичне забезпечення господарської діяльності підприємства;
- екологічна – дотримання чинних екологічних норм;
- силова – забезпечення фізичної безпеки працівників підприємства.

Враховуючи, що рушійною силою покращення макроекономічної ситуації в країні в умовах цифрової економіки є зростання рівня інтелектуального потенціалу та покращення стану техніко-технологічних видів ресурсів (активів), як ключових видів економічних ресурсів, важливим є їх ефективне використання та відтворення. Своєчасне відтворення економічних ресурсів може забезпечити економічний розвиток підприємства та зростання його

конкурентоздатності. Так, техніко-технологічні види ресурсів уособлюють об'єкти необоротних матеріальних та нематеріальних активів підприємства. До технологічних активів, які за суттю є нематеріальними, належать власна технологія у формі патентів, авторських прав і виробничих секретів, а також ноу-хау.

Економічний розвиток підприємств у сучасному інформаційному суспільстві пов'язаний із потребою безпечного зберігання, обробки та передачі значних масивів вхідної й вихідної інформації. Безпека, цілісність та конфіденційність економічної, кадрової (про якісний склад персоналу), планової, прогнозної й вихідної інформації підприємства пов'язані з можливим завданням економічної шкоди власникам і користувачам такої інформації. Загроза є потенційною причиною інциденту, події або дії, які можуть завдати шкоди підприємству та інформації про нього. Якщо неповна, невчасна, невірогідна або упереджена інформація впливає на прийняття рішень, які не відповідають інтересам суб'єкта господарювання, тоді можна стверджувати про загрозу інформаційній безпеці його фінансово-господарської діяльності. Віддалений доступ до мережі підприємства, який зараз набуває все більшого поширення і вважається чи не єдиним способом розв'язання соціальних проблем, має бути максимально захищеним і відповідати нормам інформаційної безпеки.

Інформаційна безпека, як складова економічної безпеки, характеризує стан інформаційного захисту підприємств в умовах, коли існує ймовірність загроз. Це забезпечується дотриманням системи заходів, спрямованих на попередження, виявлення та ліквідацію інформаційних загроз. Під загрозою розуміють подію, яка може викликати порушення цілісності функціонування інформаційної системи, зокрема її спотворення, знищення або несанкціоноване використання бази даних підприємства. Загрози є: ненавмисними (природними, технічними, технологічними, помилковими, у тому числі обумовлені людським фактором); штучними, що містять ознаки можливої (потенційної) кібератаки. Ненавмисні та/або штучні загрози становлять загрозу безпеці систем електронних комунікацій. У такому розумінні кібербезпека розглядається як методи й прийоми, які потрібно використовувати при формуванні програми безпеки, дотримання якої дозволить зберегти конфіденційність інформації, уникнути людських за характером загроз і зберегти ділову репутацію (гудвіл) підприємства.

Володіння цифровими технологіями передбачає дотримання вимог захисту інформації та мінімізації ризиків. Нестача на підприємстві часу, ресурсів або обізнаності працівників можуть призвести до викрадення кіберзлочинцями інформації та грошей підприємства, а також негативно вплинути на загальну репутацію підприємства. Керівництво підприємства повинно мати комплексну програму безпеки та регулярно проводити навчання всіх співробітників, які працюють з даними, щодо принципів інформаційної безпеки та захисту даних, можливих способів кібератак, а також методів їх уникнення. Отже, важливим напрямом забезпечення вимог безпеки є складання на підприємстві комплексної програми безпеки, яка має враховувати інформацію щодо:

- фінансових ресурсів та захисту банківської інформації (номерів банківських рахунків та доступу до них, кредитних карток та ін.);

- кількісного і якісного складу трудових ресурсів та плану навчання працівників вимогам кібербезпеки;
- конфіденційності особистої інформації та захисту персональних даних працівників і власників підприємства;
- ділової репутації (гудвілу) підприємства й збереження у таємниці списків контактів і персональних даних клієнтів та ін.

Незадовільна якість складу трудових ресурсів, зниження мотивації людини до праці пов'язана із збереженням моделі «дешевої робочої сили» та неналежною якістю професійно-технічної та вищої освіти [1, с. 27]. Це спричинило низький рівень конкурентоспроможності та суттєвої професійно-кваліфікаційної невідповідності робочої сили потребам ринку. Враховуючи сучасний стан інформаційного суспільства й цифрової економіки, втрати значної кількості трудових ресурсів, вважаємо, що одним із напрямів розв'язання проблеми підвищення якості трудових ресурсів є планування заходів відновлення інтелектуального потенціалу висококваліфікованих працівників підприємства. Таким вимогам відповідає методологія прогнозного аналізу відтворюваних економічних ресурсів, особливе місце серед цієї сукупності ресурсів займає методика відновлення потенціалу трудових ресурсів [2, с. 155-197].

Що стосується макрорівня, то цифровізація державних послуг передбачає різноманітні онлайнові дії та банківські послуги. На мезорівні, що є проміжною ланкою системи поміж макро- та мікросистемами, відбувається вивчення окремих галузей й підсистем національної економіки (агропромисловий комплекс, військово-промисловий комплекс, торговельно-промисловий комплекс, територіально-економічні комплекси, вільні економічні зони та ін.). Порушення безпеки так званих «критичних» додатків у державному і військовому управлінні, атомній енергетиці, медицині, ракетно-космічній галузі та у фінансовій сфері може призвести до важких наслідків для навколишнього середовища, економіки і безпеки держави, здоров'я і навіть для життя людей.

Отже, у статті визначено й проаналізовано характерні ознаки цифровізації сучасного суспільства. Зазначено, що прогрес у середовищі цифрових технологій вимагає застосування заходів інформаційної безпеки, в першу чергу, в фінансово-господарській діяльності суб'єктів підприємництва.

Уточнено тлумачення дефініцій «інформаційна безпека» та «економічна безпека». Визначено види інформації суб'єктів малого підприємництва, які підлягають захисту, та складові економічної безпеки. Сформовано пропозиції щодо створення комплексної програми безпеки, до складу якої має увійти комплекс заходів, спрямований на захист конфіденційності, доступності, цілісності даних від внутрішніх і зовнішніх, шкідливих та випадкових загроз фінансово-господарській діяльності підприємства.

Перспективою подальших досліджень є інтенсифікація діяльності підприємств у таких напрямах як відновлення потенціалу персоналу та забезпечення вимог кібербезпеки. Загальні зусилля підприємств дозволять зробити внесок у розв'язання проблеми у сфері інформаційної безпеки на мікрорівні та формування безпекового середовища на державному рівні.

**ЛІТЕРАТУРА**
1. Аналітична доповідь до щорічного Послання Президента України до Верховної Ради України «Про внутрішнє та зовнішнє становище України». Режим доступу: https://niss. gov. ua/publikacii/poslannya-prezidenta-ukraini/analitichna-dopovid-do-schorichnogo-poslannya-prezidenta-4.
2. Городянська Л.В. Відтворювані економічні ресурси: теорія та методологія обліку і аналізу: монографія. Київ: КНЕУ, 2013.
3. Концепція розвитку цифрової економіки та суспільства України на 2018-2020 роки. Режим доступу: https://zakon.rada.gov.ua/laws/show/67-2018-p#Text.
4. Про основні засади забезпечення кібербезпеки України: закон України № 2163-VIII від 05.10.2017 р. зі змінами та доповненнями. Режим доступу: https://zakon.rada.gov.ua /laws/show/2163-19#Text.
5. Закон України «Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» № 537-V, від 09.01.2007 р. Режим доступу: https://zakon.rada.gov.ua/ laws/show/537-16#n1.
6. Рекомендації парламентських слухань на тему: «Законодавче забезпечення розвитку інформаційного суспільства в Україні». Режим доступу: https://zakon.rada.gov.ua/ laws/show/1565-VII.
7. Україна 2030 Е – країна з розвинутою цифровою економікою. *Український Інститут майбутнього.* Режим доступу: https://strategy.uifuture.org/kraina-z-rozvinutoyu-cifrovoyu-ekonomikoyu.html.
8. Україна у 2020-2021 роках: наслідки пандемії. Режим доступу: https://www.me.gov. ua/Documents/Detail?lang=uk-UA&id=5d3fea53-45e7-4641-8d48-f0c865a2447&title= VipuskukrainaU2020-2021.

**Гуцуляк Д. М.,** Військовий інститут КНУ імені Тараса Шевченка, м. Київ
**Праута М. В.,** Військовий інститут КНУ імені Тараса Шевченка, м. Київ

## ЗАХОДИ ЩОДО ЗАХИСТУ НАЦІОНАЛЬНОГО ІНФОРМАЦІЙНОГО ПРОСТОРУ ТА НАЦІОНАЛЬНОЇ БЕЗПЕКИ НА ПРИКЛАДІ ПРОТИДІЇ НЕБЕЗПЕЧНИМ ЗАЯВАМ ОКРЕМИХ ПУБЛІЧНИХ ОСІБ

Події, які сталися у ніч на 3 лютого 2021 року, можна назвати визначною для новітньої історії української журналістики – інформаційний медіапростір і соціальні мережі вибухнули реакцією на вилучення з українського ефіру одразу трьох телеканалів: «112 Україна», NewsOne і ZiK. Президент України Указом [1] ввів у дію рішення Ради національної безпеки і оборони України (далі – РНБО) від 2 лютого 2021 року «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)», яким на 5 років запроваджуються санкції, зокрема, щодо юридичних компаній, яким належать телеканали «112 Україна», ZIK та NewsOne.

Майже опівночі телемедійники «112 Україна», NewsOne і ZiK видали спільну заяву [2], в якій висловили переконання у тому, що «діючи за прямою вказівкою Президента, РНБО за надуманим приводом заборонила діяльність телеканалів медіахолдингу «Новини» та підкреслили, що «мають намір боротися за своє право мовити для українців, доносити правду до громадян».

На жаль, реакції на цю заяву телеканалів від пресслужби Офісу Президента і РНБО України довелося чекати до ранку. Таким чином, відсутність чіткої взаємодії між цими владними структурами призвела до збільшення резонансу цієї новини у національному інформаційному просторі.

Наукове видання

# КОМУНІКАТИВНІ СТРАТЕГІЇ ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА: ЛІНГВІСТИКА, ПРАВО, ІНФОРМАЦІЙНА БЕЗПЕКА

**Матеріали**
**XII Всеукраїнської наукової конференції**
**молодих учених, студентів та курсантів**
**Частина І**
**(м. Київ, 9 квітня 2021 року)**

Електронне видання

Друкується в авторській редакції

Технічне редагування, макетування *О. С. Соболєва*

Формат 60х84/16. Ум. друк. арк. 12,32.
Обл.-вид. арк. 15,03. Тираж прим. Зам. №

Видавець і виготовлювач
Національна академія Служби безпеки України,
вул. М. Максимовича, 22, Київ, 03066
факс: (044)257-30-35
E-mail: academy@ssu.gov.ua
Свідоцтво суб'єкта видавничої справи ДК № 6844 від 17.07.2019