# ДОДАТОК А

Копія публікації

**Харківський національний університет радіоелектроніки**

**Кафедра економічної кібернетики та управління економічною безпекою**

# СУЧАСНІ СТРАТЕГІЇ ЕКОНОМІЧНОГО РОЗВИТКУ: НАУКА, ІННОВАЦІЇ ТА БІЗНЕС-ОСВІТА

**матеріали**
**II Міжнародної науково-практичної конференції**


**2 листопада 2021 року**
**м. Харків**

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ

Кафедра економічної кібернетики та управління економічною безпекою

**СУЧАСНІ СТРАТЕГІЇ ЕКОНОМІЧНОГО РОЗВИТКУ: НАУКА, ІННОВАЦІЇ ТА БІЗНЕС-ОСВІТА**

**матеріали**
**II Міжнародної науково-практичної конференції**

**2 листопада 2021 року**

Харків 2021

**УДК 330.341; 338.24; 005 (06)**

Сучасні стратегії економічного розвитку: наука, інновації та бізнес-освіта. Матеріали II Міжнародної науково-практичної конференції (м. Харків, 2 листопада 2021 р.) / За заг. ред. Т. В. Полозової [та ін.]. Харків. ХНУРЕ. 2021. 189 с.

У збірнику містяться матеріали, що були подані на II Міжнародну науково-практичну конференцію «Сучасні стратегії економічного розвитку: наука, інновації та бізнес-освіта» (м. Харків, 2 листопада 2021 року).

Праці науковців охоплюють такі тематичні напрями досліджень: сучасні економічні теорії та історія економічної думки; світове господарство: нові виклики та інноваційні форми міжнародних економічних відносин; єдиний цифровий ринок Європейського союзу; економіка та управління національним господарством; розвиток сучасного підприємництва в умовах впливу та протидії гібридним загрозам; інформаційні технології в бізнесі: електронна комерція та віртуальна торгівля; економіка природокористування та сучасні проблеми охорони навколишнього середовища; демографія, економіка праці, соціальна економіка і політика; бухгалтерський облік, аналіз і аудит: національні особливості та світові тенденції; сучасні математичні методи, моделі та інформаційні системи в економіці; фінанси, страхування та банківська справа; економіка підприємства та корпоративне управління: безпека бізнесу та модернізація бізнес-процесів; інновації в бізнес-освіті.

Для науковців, викладачів, аспірантів, а також фахівців, що займаються дослідженням питань соціально-економічного розвитку та забезпечення економічної безпеки підприємств, галузей, регіонів та країни.

**УДК 330.341; 338.24; 005 (06)**



**ISBN 978-966-659-334-7**
**DOI: 10.30837/978-966-659-334-7**

**Гришко С.В.**
*к.е.н., доцент кафедри економічної кібернетики*
*та управління економічною безпекою,*
*Харківський національний університет радіоелектроніки*
**Могилат В. А.**
*студент,*
*Харківський національний університет радіоелектроніки*

## ЗОВНІШНІ КОМУНІКАЦІЇ БІЗНЕСУ В БЕЗПЕКОВОМУ ЛАНДШАФТІ

Зовнішня комунікація – це передача інформації між бізнесом та іншою особою (фізичною чи юридичною) у зовнішньому середовищі компанії [1]. Хоча взаємодія із зовнішніми «гравцями» необхідна для забезпечення процесів життєдіяльності бізнесу, такі комунікації також можуть стати потенційним каналом витоку даних. В такому випадку об'єктом вразливості стає канал комунікації, тобто спосіб, яким організація передає / отримує інформацію. Як правило, окремі канали комунікацій підприємства знаходяться в управління різних підрозділів та мають різні безпекові вимоги та складові.

Але сучасний ландшафт загроз швидко змінюється, має комплексний характер та характеризується як невизначеністю, так і зростаючою залежністю від зовнішнього середовища, що створює високу турбулентність для бізнесу [2]. Зовнішні комунікації починають відігравати більш впливову роль у виживанні та розвитку бізнесу. Тому підхід до розгляду окремих каналів зовнішніх комунікацій як єдиного безпекового об'єкту стає популярним. Спираючись на такий підхід, пропонується наступна концептуальна модель безпеки зовнішніх комунікацій бізнесу (рис.1). Така структура організації безпеки зовнішніх комунікацій бізнесу дозволить провадити комплексні заходи, об'єднавши різні операційні домени – інформаційну безпеку, яка зазвичай має ІТ спрямованість, та репутаційну безпеку, якою опікується маркетинговий сектор.




Рисунок 1 – Концептуальна модель безпеки зовнішніх комунікацій бізнесу

*Джерело: розроблено авторами*

### Перелік джерел посилання

1. Організація та управління системою економічної безпеки підприємства: навчально-методичний посібник / З. Б. Живко, О.В. Черевко, Н.В. Зачосова та іню; за ред. З.Б. Живко. Черкаси: видавець Чабаненко Ю.А., 2019. 120 с.

2. Meng W., Gollmann D., Jensen C., Zhou J. (ed.). *Information and Communications Security: 22nd International Conference, ICICS 2020, Copenhagen, Denmark, August 24-26, 2020, Proceedings*. Springer Nature, 2020.

Наукове видання

**СУЧАСНІ СТРАТЕГІЇ ЕКОНОМІЧНОГО РОЗВИТКУ:**
**НАУКА, ІННОВАЦІЇ ТА БІЗНЕС-ОСВІТА**

Матеріали
ІІ Міжнародної науково-практичної конференції

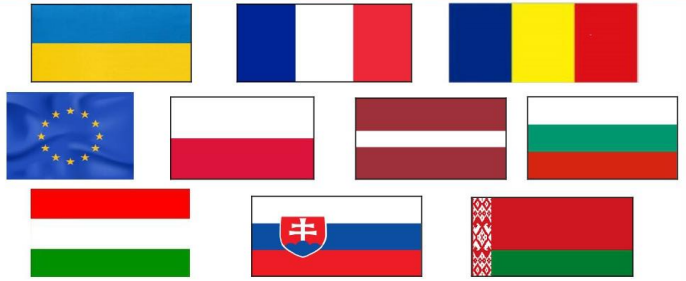
2 листопада 2021 року
м. Харків

**Редактори:**
**Полозова Тетяна Василівна**
**Колупаєва Іріна Володимирівна**
**Мурзабулатова Олена Вячеславівна**

Файл надано:
Харківський національний університет радіоелектроніки,
Кафедра економічної кібернетики та управління економічною безпекою,
61166, Україна, м. Харків, пр. Науки, 14,
тел. (057) 702-14-90,
e-mail: sser.conf@gmail.com

Підп. до друку 20.11.2021. Формат 60x84 1/16.
Спосіб друку – ризографія. Умов. друк. арк. 11,0.
Тираж 50 прим. Ціна договірна.

Віддруковано в типографії ФОП Андреєв К.В.
61166, Харків, вул. Богомольця, 9, кв. 50.
Свідоцтво про державну реєстрацію
№ 24800170000045020 від 30.05.2003 р.
ep.zakaz@gmail.com
тел. 063-993-62-73

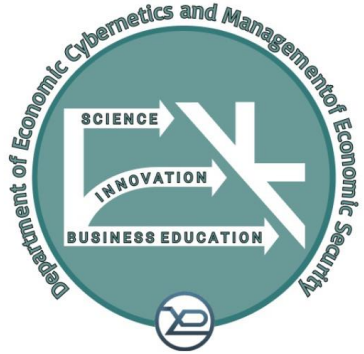


**Kharkiv National University of Radio Electronics**

**Department of Economic Cybernetics and Management of Economic Security**

**MODERN STRATEGIES OF ECONOMIC DEVELOPMENT:**
**SCIENCE, INNOVATION AND BUSINESS EDUCATION**

**Proceedings of the Conference**
**II International Scientific and Practical Conference**




**November 2, 2021**
**Kharkiv, Ukraine**

ДОДАТОК Б

Доповідь на Міжнародній конференції

II Міжнародна науково-практична конференція

«УПРАВЛІННЯ ТА АДМІНІСТРУВАННЯ В УМОВАХ ПРОТИДІЇ ГІБРИДНИМ ЗАГРОЗАМ НАЦІОНАЛЬНІЙ БЕЗПЕЦІ»

7 грудня 2021 року

Подано до друку

# БЕЗПЕКА ЗОВНІШНІХ КОМУНІКАЦІЙ БІЗНЕСУ В УМОВАХ ГІБРИДНИХ ЗАГРОЗ

**Могилат В.А.**
магістрант кафедри економічної кібернетики та управління економічною безпекою Харківського національного університету радіоелектроніки
**Гришко С.В.**
к.е.н., доцент, доцент кафедри економічної кібернетики та управління економічною безпекою Харківського національного університету радіоелектроніки

В епоху гібридних загроз в безпековому середовищі відбуваються глибокі зміни [1], які відбились і на інформаційній сфері. Структура дезінформації стрімко розвивається і стає дедалі ефективнішою. Нове бачення цієї ситуації було запропоноване Європейським центром з протидії гібридним загрозам Hybrid CoE. Воно базується на тому, щоб замість дослідження дезінформації як Дезінформації 2.0 або Дезінформації 3.0, 4.0, аналізувати зміни в дезінформації як "Дезінформацію h.0" (Disinformation h.0) [2].

З точки зору гібридних загроз, "Дезінформація h.0" поєднує між собою ієрархічні та мережеві канали впливу (рис.1), підсилюючи ефект такої взаємодії сінергетичним ефектом.

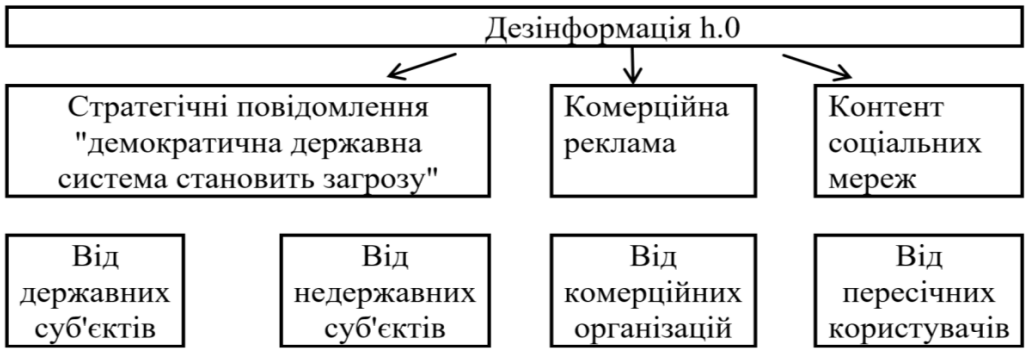



Рисунок 1 – Структура "Дезінформації h.0" (складено за матеріалами [2])

Це означає, що вплив зовнішнього середовища на бізнес-процеси принципово ускладнюється, набуває комплексного характеру, стає більш невизначеним. Крім того, гібридні впливи змінюють роль самого бізнеса в безпековому ландшафті: окремі підприємства та організації тепер можуть відігравати роль як об'єкта гібридного впливу, так і ставати його інструментом, несвідомо віддаючи "гібридному" агресору свої бізнес-ресурси [3].

В такому випадку одним з головних об'єктів вразливості стає канал комунікації, тобто спосіб, яким організація передає / отримує інформацію. Такі канали, забезпечуючи формальні та неформальні зв'язки бізнесу із клієнтами, постачальниками, державними структурами, суспільством тощо, в умовах гібридних впливів починають виконувати роль провідника інтересів гібридних гравців. Комплексний, багатоступінчастий вплив та знаходження поза межами виявлення не дозволяє "виловлювати" сигнали таких загроз та ідентифікувати їх звичайними засобами захисту зовнішніх комунікацій.

Зазвичай підприємство використовує не пов'язані між собою стратегії управління різними видами зовнішніх комунікацій, а використовуваний підхід залежить від обставин, мети та цільового одержувача. Тому, як правило, окремі канали комунікацій підприємства знаходяться в управління різних підрозділів та мають різні безпекові вимоги та складові.

В умовах "Дезінформації h.0" безпека зовнішніх комуникативних каналів бізнесу піддається одночасному впливу різних за своїм характером тенденцій: фрагментація концепції істини (особливо в тому, що стосується соціальних тенденцій та нових інформаційних потоків); комплексні зміни в мас-медіа як галузі; зростання впливу приватних медіа-платформ, які вже на рівних конкурують із традиційними ЗМІ; нові технології, які породжують нові інструменти для втручання та впливу.

Саме тому комплексний підхід до розгляду окремих каналів зовнішніх комунікацій як єдиного безпекового об'єкту стає популярним як в науковому середовищі [4], так і в практичній діяльності окремих компаній [5].

Об'єднання механізмів інформаційної безпеки (домен комп'ютерних наук) та репутаційної безпеки (домен соціальних наук) в єдиний контур управління дозволить координувати та синхронізувати зусилля компанії для забезпечення безпеки завнішніх комунікацій бізнесу в умовах гібридних загроз.

## Список використаних джерел

1. Гришко, С. В., Головянко, М. В., Титаренко, М., Чех, М., Василиця, О., Ланюк, Є., ... & Наумов, І. (2021). Гібридні загрози. Глосарій з гібридних загроз.

2. Hybrid CoE (2020). Trends in the Contemporary Information Environment. *Hybrid Centre of Excellence Trend Report*, 4. Finland: Hybrid CoE, 2020. 28 p.

3. Єфіміна, О., Гришко, С. (2020) Від чого та як захищати бізнес в умовах гібридних загроз. *Управління та адміністрування в умовах протидії гібридним загрозам національній безпеці:* матеріали Всеукраїнської науково-практичної конференції, м.Київ, 7 грудня 2020 р. Київ: ДУІТ, 2020. 130 – 132.

4. Information and Communications Security Policy. Getac Technology Corp. https://en.getacgroup.com/upload/document_report_list_files/14602a7c7e713bca66dcd9502823cc1a.pdf

5. Шульга В. Атаки на репутацію компанії. Сайт компанії Ліга-закон (2020, листопад 13). https://biz.ligazakon.net/aktualno/8192_ataki-na-reputatsyu-kompan-