

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
УКРАЇНСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ЗАЛІЗНИЧНОГО ТРАНСПОРТУ
ІНСТИТУТ ФІЛОСОФІЇ ім. Г. СКОВОРОДИ НАН УКРАЇНИ
НАЦІОНАЛЬНИЙ ПЕДАГОГІЧНИЙ УНІВЕРСИТЕТ ім. М. ДРАГОМАНОВА
КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ» ім. І. СІКОРСЬКОГО



ЛЮДИНА, СУСПІЛЬСТВО, КОМУНІКАТИВНІ ТЕХНОЛОГІЇ

**МАТЕРІАЛИ XII МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ
«ЛЮДИНА, СУСПІЛЬСТВО, КОМУНІКАТИВНІ ТЕХНОЛОГІЇ»**

м. Харків, 25 жовтня 2024 р.

**Харків
2024**

УДК 316.05

Л 93

Затверджено до друку Вченою радою Українського державного університету залізничного транспорту (протокол № 8 від 25.10.2024 р.)

Головні редактори:

Панченко С. В., доктор технічних наук, професор, академік Транспортної академії України, в. о. ректора Українського державного університету залізничного транспорту

Андрущенко В. П., доктор філософських наук, професор, член-кореспондент НАН України, академік Національної академії педагогічних наук України, заслужений діяч науки і техніки України, ректор Національного педагогічного університету ім. М. Драгоманова

Редакційна колегія:

Абашик В. О., д-р філос. наук, професор

Вельш Вольфганг, габілітований доктор філософії, професор

Каграманян А. О., канд. техн. наук, доцент

Коростельов Є. М., канд. техн. наук, доцент

Лях В. В., д-р філос. наук, професор

Новіков Б. В., д-р філос. наук, професор

Панченко В. В., канд. техн. наук, доцент

Соломніков І. В., канд. екон. наук, доцент

Толстов І. В., канд. філос. наук, доцент

Людина, суспільство, комунікативні технології: матеріали XII Міжнар. наук.- практ. конф. 25 жовтня 2024 р. / відп. за випуск І. В. Толстов. — Харків: УкрДУЗТ, 2024. — 217 с.

УДК 316.05

Список використаних джерел

1. Семанюк В. З. Облікова філософія в системі теоретичного знання. *Науковий вісник Ужгородського університету: серія Економіка*. 2018. Вип. 1 (51). С. 442-448. DOI: [https://doi.org/10.24144/2409-6857.2018.1\(51\).442-448](https://doi.org/10.24144/2409-6857.2018.1(51).442-448).
2. Жук В. М. Інституціональна теорія бухгалтерського обліку: відповідь на виклики сучасності. *Бухгалтерський облік і аудит*. № 8-9. 2015. С. 14-23. URL: <https://magazine.faaf.org.ua/institutsionalna-teoriya-bukhgalterskogo-obliku-vidpovid-na-vikliki-suchasnosti.html>.
3. Моделі мислення і мисленнєві навички [інтерактивний ресурс про критичне мислення] : Uchoose.info. URL: <https://uchoose.uacrisis.org/modeli-myslennya-i-myslennyevi-navychky/>.
4. Кундря-Висоцька О., Вагнер І., Демко І. Іманентна філософія сучасного обліку в контексті поглиблення сутності його предмету. *Financial and Credit Activity Problems of Theory and Practice*. 2022. Вип. 1(42). С. 145-153. DOI: <https://doi.org/10.55643/fcaptp.1.42.2022.3725>.

ЗАЙКІНА Г. М., д-р юрид. наук, доцент,
Український державний університет залізничного транспорту,
м. Харків, Україна

ДЕЯКІ ПИТАННЯ АДМІНІСТРАТИВНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ: ДОСВІД США ТА ЄС

В умовах повномасштабної війни кібербезпека є головним і стратегічним питанням в економічному, політичному, соціальному та воєнному аспектах. Сьогодні гібридні загрози спрямовані на використання вразливості країн і підриєв фундаментальних демократичних цінностей і свобод.

США та ЄС мають чітке розуміння того, що кіберзагрозам необхідно запобігати як «пасивними» методами, такими як підвищення стійкості до різного виду потрясінь і несподіванок, так і більш активними, включаючи жорсткі заходи з підготовки та захисту окремих структур.

Виділення певних заходів у напрямі протидії кіберзагрозам яскраво демонструє сформований пріоритет у ЄС. Вектор розвитку системи кібербезпеки в ЄС досить детально охарактеризовано в підсумкових документах: спільні комюніке Європейського Парламенту і Європейської Ради щодо реалізації заходів з протидії гібридним загрозам у Європейському Союзі (06.04.2016 р. [1]; 19.07.2017 р. [2]; 13 червня 2018 р. [3]); звіт про виконання плану дій 2016 р. з

протидії гібридним загрозам; Спільного повідомлення 2018 р. щодо підвищення стійкості та посилення можливостей для подолання гібридних загроз від 28.05.2019 р. [4]. Загальний аналіз цих документів дає можливість виокремити основні напрями адміністративно-правового та організаційного забезпечення кібербезпеки, зокрема боротьби з гібридними загрозами. Основною метою цих щорічних звітних документів є подання звіту Європейському Співтовариству про прогрес і наступні кроки у впровадженні дій у чотирьох сферах, запропонованих у Спільній діяльності: 1) підвищення обізнаності про ситуацію; 2) стійкість суспільства; 3) зміцнення спроможності запобігати кризам і реагувати на них; 4) координувати відновлення та розширення співпраці з НАТО для забезпечення взаємодоповнюваності в діяльності.

Розгляд останніх законодавчих ініціатив, направлених на посилення кібербезпеки США, дає підстави стверджувати, що головну роль у захисті держави від гібридних загроз відіграє розроблення заходів із підвищення обізнаності щодо кіберзагроз, при цьому з акцентуванням на виявленні суспільної вразливості до них і скоординованих діях для оцінювання цих загроз.

Так, 12.05.2021 р. [5] було підписано виконавчий наказ про зміцнення кібербезпеки США, що посилює наглядовий контроль за законами та нормативними актами в кібербезпековій галузі. Документ закликає федеральні відомства співпрацювати з приватним сектором шляхом застосування технологій та обміну інформацією, що підвищить стійкість до кібератак держави в цілому. Також основним елементом розпорядження є SBOM (Software Bill of Materials) - технічний набір матеріалів, покликаний сприяти аналізу факторів вразливості програмного забезпечення для керування ризиками.

Також розробляють законопроект, відповідно до якого від державних і приватних організацій потребуватимуть оповіщення уряду протягом 24 годин у разі порушення безпеки кіберпростору, що загрожує економічній і національній безпеці США.

Проаналізувавши міжнародний досвід, можна стверджувати, що для забезпечення вищого рівня мережевої та інформаційної безпеки в межах НАТО та ЄС як необхідні заходи визначено три основні напрями: підвищення спроможності системи кібербезпеки на національному рівні; підвищення рівня загальноєвропейського співробітництва; запровадження управління ризиками та зобов'язання повідомляти про кіберінциденти органи публічної влади.

Розвиток ІТ-законодавства в Україні, що регулює всі відносини всередині і навколо сектора кібербезпеки, ще не досягнув високої ефективності його функціонування в такому масштабі, як у розвинених західних країнах, тому удосконалення адміністративно-правового забезпечення цієї царини є пріоритетним напрямом розвитку чинного законодавства. Сучасна система

забезпечення інформаційної безпеки та кібербезпеки в Україні має бути єдиною та ефективною системою, орієнтованою на попередження ймовірних викликів і загроз у кіберпросторі, що має включати стратегічні цілі, пріоритети і державну основу; заходи щодо підготовки, реагування та відновлення після кіберінцидентів, принципи державно-приватного партнерства; більш тісну координацію зусиль між урядом і приватним сектором.

Список використаних джерел

1. Спільне повідомлення Європейському парламенту та Раді про спільну рамкову програму протидії гібридам загрожує відповіддю Європейського Союзу. 2016. URL: <https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=CELEX%3A52016JC0018>.

2. Спільна доповідь Європейському Парламенту та Раді про імплементацію Спільної рамкової програми щодо протидії гібридним загрозам - відповідь Європейського Союзу. 2017. URL: <https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=CELEX%3A52017JC0030>.

3. Спільний звіт для Європейського Парламенту, Європейської Ради та Ради щодо імплементації Спільної рамкової програми щодо протидії гібридним загрозам з липня 2017 року по червень 2018 року. URL: <https://eurlex.europa.eu/legal-content/EN/TXT/?uri=JOIN:2018:014:FIN>.

4. Звіт про спільний робочий документ штабу про реалізацію Спільної рамкової програми 2016 року щодо протидії гібридним загрозам та Спільного повідомлення 2018 року з підвищення стійкості та зміцнення можливостей протидії гібридним загрозам. URL: <https://eeas.europa.eu/>.

5. Указ про покращення кібербезпеки нації. URL: <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/>.

*КАЛИЧЕВА Н. Є., д-р екон. наук, професор,
ТОКМАКОВА І. В., д-р екон. наук, професор,
Український державний університет залізничного транспорту,
м. Харків, Україна*

КОНКУРЕНТНІ РИНКИ ЯК КЛЮЧОВИЙ АСПЕКТ ЕФЕКТИВНОСТІ ЕКОНОМІКИ

Політика конкуренції полягає в застосуванні правил, що забезпечують чесну конкуренцію підприємств і компаній. Це заохочує підприємливість і

Наукове видання

ЛЮДИНА, СУСПІЛЬСТВО,
КОМУНІКАТИВНІ ТЕХНОЛОГІЇ

МАТЕРІАЛИ XII МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ
«ЛЮДИНА, СУСПІЛЬСТВО, КОМУНІКАТИВНІ ТЕХНОЛОГІЇ»

25 жовтня 2024 р.

Відповідальність за редагування та достовірність інформації несуть автори робіт.

Відповідальний за випуск Толстов І. В.

Підписано до друку 25.10.2024 р.
Умовн. друк. арк. 13,5. Тираж . Замовлення № .

Художнє оформлення Л.І. Мачулін

Свідоцтво про держреєстрацію: сер. ХК №125 від 24.11.2004

Видавець та виготовлювач Український державний університет
залізничного транспорту,

61050, Харків-50, майдан Фейсбаха, 7.

Свідоцтво суб'єкта видавничої справи ДК № 6100 від 21.03.2018 р.