Отже, Україна витримала іспит впливу пандемії COVID-19. І наразі, ситуація в економіці, переважно, залежить від динаміки та масштабів розповсюдження пандемії, значною мірою зберігає характерні ознаки другої половини минулого року із превалюванням факторів стриманого попиту та високого рівня невизначеності щодо найближчої перспективи.

**Список використаних джерел:**

1. World Health Organization (2021). WHO corona virus COVID19 dashboard. URL: https://covid19.who.int/

2.https://www.unicef.org/ukraine/media/9231/file/UNICEF%20Ukraine%20Concensus%20COVID%20Youth%202020%20ukr.pdf

## ОСОБЛИВОСТІ МОНІТОРИНГУ ОЦІНКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

***Чубаєвський В.І.,*** *канд. політ. наук, доцент,* ***Терешенко Е.Ю.,*** *канд. екон. наук, Київський національний торговельно-економічний університет, м. Київ, Україна*

У сучасному цифровому світі інформаційна безпека країни є ключовою детермінантою її національної безпеки. Питання інформаційної безпеки, а також управління критичною інфраструктурою Інтернету регулярно обговорюються на зустрічах «Великої двадцятки» на майданчику ООН, на зустрічах міністрів телекомунікацій та інформаційних технологій країн [3].

Крім того, слід зазначити, що країни світу активізують свою діяльність в рамках прийнятих вітчизняних стратегій кібербезпеки. Так, у серпні 2021 року Указом Президента України було затверджено рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» [1].

У рамках запропонованої стратегії визначена система пріоритетів, стратегій та механізмів для нарощування потенціалу адаптації уряду і бізнесу до зростаючих кіберризиків у сфері інформаційної безпеки.

За підсумками 2020 року Україна посіла 86 місце у Глобальному індексі кібербезпеки (далі - GCI) [2]. України, на жаль, немає серед країн з низьким рівнем схильності до кіберзагроз.

Україна є найбільш уразливою країною, тобто з дуже низьким рівнем кіберзахищеності, за нею йдуть Білорусь, Вірменія, Киргизстан Боснія та Герцеговина. GCI визначає перспективи формування безпечного інформаційного простору країни та прогалини, які необхідно подолати для зміцнення цифрової екосистеми кожної країни.. GCI містить 82 питання про зобов'язання держав щодо забезпечення інформаційної безпеки за п'ятьма напрямами, а саме: правові; технічні; організаційні заходи; заходи щодо розвитку потенціалу та співробітництва.

В таблиці 1 відповідно до кожного напряму представлені маркери зобов'язань країн щодо забезпечення рівня інформаційної безпеки.

Визначення маркерів зобов'язань країн щодо забезпечення рівня інформаційної безпеки та їх постійний моніторинг дозолить країнам здійснювати перманенту самооцінку рівня інформаційної безпеки та сприяти покращенню координації дій щодо її зміцнення; формувати інформаційний банк даних національних пріоритетів та ресурсів для управління інформаційною безпекою на рівні кожної країни; підвищити обізнаність різних груп стейкхолдерів щодо потреб координації на національному рівні.

З метою досягнення вищезазначених цілей моніторингу оцінки рівня інформаційної безпеки каїн, вважаємо за доцільне визначити наступні принципи його здійснення:

- достовірність передбачає формування та використання банк інформаційних даних та показників, що найбільш повно та обґрунтовано характеризують стан інформаційної безпеки та реалізацію стратегічних національних пріоритетів;

Таблиця 1 – Зобов'язання країн щодо забезпечення рівня інформаційної безпеки

| Напрями забезпечення інформаційної безпеки | Маркери зобов'язань |
|---|---|
| Правові<br>*Вимірювання законів і положення про кіберзлочинність та кібербезпеку* | Країни з певною формою кібербезпеки |
| | Положення про захист даних |
| | Правила критичної інфраструктури |
| Технічні<br>*Вимірювання реалізація технічних можливостей через національні та галузеві агенції* | Активність в Cyber Incident Response Team (далі -CIRT)<br>Участь в регіональному CIRT<br>Механізми звітності щодо захисту дітей в Інтернет |
| Організаційні<br>*Вимірювання національних стратегій та організацій, що впроваджують кібербезпеку* | Національні стратегії кібербезпеки<br>Агенції кібербезпеки<br>Стратегії та ініціативи захисту дітей в Інтернеті |
| Розвиток потенціалу<br>*Вимірювання обізнаності кампанії, навчання, освіта та заохочення для розвитку потенціалу кібербезпеки* | Країни проводять ініціативи щодо кіберобізнаності |
| | Країни з програмами досліджень і розробок у сфері кібербезпеки |
| | Країни, що мають національні галузі кіберзахисту |
| Співпраця<br>*Вимірювання партнерських відносин між агентствами, фірмами, і країнами* | Країни, які займаються кібербезпекою, державно-приватне партнерство |
| | Країни з двосторонніми угодами про кібербезпеку |
| | Країни з багатосторонньоми угодами про кібербезпеку |

Джерело: складено авторами на основі:[2]

- системність дозволяє здійснювати збір, аналітичні дослідження банку інформаційних даних про стан інформаційної безпеки за єдиною методикою,

відповідно до визначеного та затвердженого переліку показників, із встановленою періодичністю на основі даних статистичного спостереження та спеціальних досліджень;

- своєчасність надає можливість негайного реагувати та приймати оперативні управлінських рішення;

- комплексність забезпечує перманенте спостереження тенденцій розвитку показників інформаційної безпеки відповідно до реалізації стратегічних національних пріоритетів, використання існуючих інформаційних баз даних, механізмів моніторингу та інструментів державного та відомчого статистичного спостереження.

Стосовно механізмів моніторингу оцінки стану інформаційної безпеки, слід зазначити, що вони не залежать від суб'єктивних факторів в процедурах обробки та аналізу показників про стан інформаційної безпеки та рівня загроз її забезпечення.

Система моніторингу оцінки рівня інформаційної безпеки реалізується за етапами. Поетапна реалізація системи моніторингу дозволить здійснювати системну, комплексну та об'єктивну оцінку стану інформаційної безпеки та визначати відповідно до кожного етапу заходи щодо її зміцнення.

На першому етапі відображається прогноз потенційних зовнішніх небезпек і загроз інформаційної безпеки.

Змістом другого етапу є визначення методичного інструментарію забезпечення захисту інтересів держави від загроз. Саме на цьому етапі визначаються методи, способи і форми діяльності, спрямовані на нейтралізацію можливих загроз інформаційній безпеці.

В ході третього етапу відбувається розробка заходів, що спрямовані на здійснення протидії загрозам в рамках визначеного на попередньому етапі методичного інструментарію. Результатом цього етапу є формування системи забезпечення інформаційної безпеки, яка відповідає конкретними викликам та загрозам сьогодення.

На четвертому етапі здійснюється опис системи забезпечення інформаційної безпеки відповідно до параметризації її кількісних та якісних складових. Кількісна оцінка інформаційної безпеки дозволяє визначити загрози безпеці, конкретні показники стану безпеки і параметри їх порогових значень.

На завершального етапі здійснюється формування оптимальної набору системи показників та визначається їх індикативні і порогові значення. Саме визначення індикативних та порогових значень поточний стан досліджуваної сфери системи інформаційної безпеки, а в подальшому визначити складові її потенціалу.

Отже, система показників стає основним об'єктом моніторингу оцінки інформаційної безпеки. Моніторинг дозволяє не тільки оцінювати стан відповідної сфери забезпечення інформаційної безпеки, а й визначити найбільш слабкі елементи системи, вибрати оптимальні рішення, виробити практичні рекомендації щодо її зміцнення.

**Список використаних джерел:**

1.Указ Президента України Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України" [Електронний ресурс]. - Режим доступу: https://zakon.rada.gov.ua/laws/show/447/2021#Textpo рішення Ради національн... | від 26.08.2021 № 447/2021 (rada.gov.ua)

2. Global Cybersecurity Index 2020 Measuring commitment to cybersecurity [Електронний ресурс]. – Режим доступу: https://nonews.co/wp-content/uploads/2021/09/GCI2020.pdf

3. Бондаренко В., Литвиненко О. Інформаційна безпека сучасної держави: концептуальні роздуми / В. Бондаренко, О. Литвиненко [Електронний ресурс]. – Режим доступу: http://www.crime-research. iatp. org. ua/ library/strateg. Htm

## ПАНДЕМІЯ COVID-19 ЯК ФАКТОР ЗРОСТАННЯ ТИСКУ ТА ЗАГРОЗ ЕТИЧНОЇ ПОВЕДІНКИ ПРОФЕСІЙНИХ БУХГАЛТЕРІВ

***Чебан Т. М.**, канд. екон. наук, доцент, **Шаля Ю. О.**, студентка, Херсонський національний технічний університет*

Світова спільнота, починаючи з середини грудня 2019 року, потрапила під величезний вплив Всесвітньої епідемії хвороби, яка отримала назву COVID-19. Пандемія вже призвела до численних людських втрат, наклала суттєві обмеження на соціально-культурне життя населення і кардинально змінила тренди глобальної економіки. Внаслідок цього численні суб'єкти господарювання відчувають фінансові, операційні та особисті труднощі, тому шукають нові способи зберегти безперервну діяльність, підтримати операційну стабільність, сприяти стійкості та зростанню у довгостроковій перспективі. За цих умов зростають ризики та створюються можливості для незаконної діяльності та шахрайства, що створює додаткові загрози тиску на професійних бухгалтерів та ускладнює дотримання ними принципів етичної поведінки.

Зважаючи на це Рада з міжнародних стандартів етики для бухгалтерів (РМСЕБ), місія якої полягає у служінні інтересам суспільства шляхом встановлення етичних стандартів, включаючи вимоги до незалежності аудиторів, розробила рекомендації щодо виявлення та запобігання тиску на бухгалтерів в умовах пандемії та шахрайницькою діяльністю. Їх вивчення дозволило констатувати, що умови нестабільності та невизначеності обумовлюють підвищений тиск на професійних бухгалтерів з боку роботодавців, клієнтів і інших зацікавлених осіб (рис. 1).

Згідно Кодексу професійні бухгалтери та аудитори не повинні дозволяти іншим особам чинити на себе тиск, бо це призводить до порушення дотримання фундаментальних принципів етики [1].

Під час пандемії COVID-19 професійний бухгалтер чи аудитор може стикатися з низкою шахрайських дій, зокрема [2]:

- шахрайські заявки на отримання державної допомоги,
- шахрайство з закупівлями та продукцією,
- шахрайство з отриманням вигоди, в тому числі фіктивні позови,
- шахрайство з видаванням себе за іншу особу,