Міністерство освіти і науки України
Національний університет
«Полтавська політехніка імені Юрія Кондратюка»

Тези

77-ї наукової конференції професорів, викладачів, наукових працівників, аспірантів та студентів університету

ТОМ 2

16 травня – 22 травня 2025 р.

Полтава 2025

– втрата довіри з боку контрагентів,
– ризик банкрутства.

Виходячи з даних проблем, можна із впевненістю стверджувати, що грошові кошти – це ключовий фактор, від якого залежить фінансова стабільність та життєдіяльність будь якого суб'єкта господарювання. В авторському баченні, основними шляхами вирішення даних проблем можуть бути: уніфікація законодавчої та нормативної бази, уточнення критеріїв для еквівалентів грошових коштів, адаптація критеріїв класифікації до електронних грошей, врахування валютного фактору, деталізація класифікаційних ознак, гармонізація обліку з міжнародними стандартами та ін. Вирішення цих проблем сприятиме підвищенню якості облікової інформації, покращенню фінансового аналізу та прийняттю більш обґрунтованих управлінських рішень щодо грошових коштів підприємств та держави в цілому.

Література:

1. *Пономарьова Т. В., Стріляна Я. О. Шляхи вдосконалення обліку грошових коштів на торговельному підприємстві. Вісник Харківського національного університету імені В. Н. Каразіна. Бізнес Інформ. Харків, 2023. № 10, с. 270-275.*
2. *Нікуліца Д.Р. Облік грошових коштів: проблеми та шляхи вдосконалення: матеріали міжнародної науково-практичної конференції , м. Київ, 2020.*
3. *Загорулько К.В. Організація обліку грошових коштів. Вісник Університету «Україна». Київ, 2023. № 8.*

УДК 658

А.А. Жукова, студентка групи 301 – ЕО
Науковий керівник – А.В. Дмитренко, д.е.н., доцент
Національний університет
«Полтавська політехніка імені Юрія Кондратюка»

КІБЕРБЕЗПЕКА ЯК КЛЮЧОВИЙ ЕЛЕМЕНТ ЕКОНОМІЧНОЇ БЕЗПЕКИ ДЕРЖАВИ В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

У сучасному світі цифрова трансформація стає невід'ємною частиною розвитку держав, підприємств та суспільства в цілому. Зростання залежності від інформаційних технологій супроводжується новими викликами у сфері безпеки [1]. Кібербезпека, як складова економічної безпеки, відіграє вирішальну роль у забезпеченні стабільності та стійкості

держави. В умовах глобалізації та постійних змін в інформаційних технологіях, захист критичної інфраструктури та інформаційних систем стає пріоритетом для урядів.

Кібератаки мають суттєвий вплив на економіку держави. Згідно з дослідженнями, збитки від кібератак у світі зростають щорічно [5]. Також, дослідження впливу кібератак на економіку показує їхній багатогранний характер. Прямі фінансові втрати включають викрадення коштів, збої в роботі платіжних систем, витрати на відновлення пошкоджених систем та виплати страхових відшкодувань.

Крім того, атаки на фінансові установи можуть викликати дестабілізацію фінансових ринків. Непрямі збитки проявляються у вигляді порушення виробничих процесів, логістичних ланцюгів, втрати ділової репутації, відтоку клієнтів та інвестицій [2]. Наприклад, атака на банківську систему може призвести до масових втрат клієнтів, зниження інвестицій та економічної активності. Споживчий сектор також зазнає збитків, коли компанії втрачають доступ до даних клієнтів і не можуть виконувати свої зобов'язання.

Кібератаки на об'єкти критичної інфраструктури, такі як енергетичні мережі, транспортні системи та фінансові установи, можуть призвести до масштабних економічних криз та загрожувати національній безпеці.

Аналіз сучасних кіберзагроз демонструє зростання їхньої складності та цілеспрямованості [3]. Тому для протидії загрозам у сфері кібербезпеки держава повинна розробляти комплексні стратегії. Основні складові таких стратегій включають:

– розробку та впровадження законодавчих актів, які регулюють діяльність у сфері кібербезпеки. Це також включає захист персональних даних, відповідальність за кібератаки та механізми реагування;

– інвестування в освіту та підготовку спеціалістів з кібербезпеки. Важливо розвивати навички у сфері інформаційних технологій, а також підвищувати обізнаність населення щодо кіберзагроз;

– Встановлення партнерств між урядом і приватними компаніями для обміну інформацією про загрози та кращі практики захисту;

– інвестування в сучасні технології захисту, такі як шифрування, системи виявлення вторгнень та антивірусні програми. Важливо також забезпечити регулярні оновлення програмного забезпечення;

– розробка планів реагування на кібератаки, що включає створення команд швидкого реагування, які можуть оперативно реагувати на загрози та відновлювати роботу систем.

Кібербезпека є невід'ємною складовою економічної безпеки держави в умовах всеосяжної цифрової трансформації. Зростаюча кількість та складність кібератак становлять значну загрозу для економічної стабільності, завдаючи прямих та непрямих фінансових збитків,

порушуючи функціонування критичної інфраструктури та підриваючи довіру до цифрової економіки. Ефективна протидія цим загрозам вимагає комплексного підходу, що включає удосконалення законодавства, підвищення обізнаності, створення національної системи кібербезпеки, впровадження сучасних технологій захисту, активну міжнародну співпрацю та підтримку вітчизняної індустрії кібербезпеки. Інвестиції в кібербезпеку є стратегічно важливим елементом забезпечення економічного процвітання та національної безпеки держави в цифровому майбутньому. Успішна реалізація цих стратегій дозволить не лише знизити ризики, але й підвищити довіру до цифрових технологій, що в свою чергу сприятиме економічному зростанню та стабільності держави. Таким чином, кібербезпека має стати пріоритетом на всіх рівнях управління, адже її успішна реалізація є запорукою економічної безпеки та розвитку держави в умовах швидкозмінного цифрового середовища.

Література:

1. Баранова В. В. Підходи до оцінки економічної безпеки національного господарства. Науковий вісник Ужгородського національного університету. 2018. С. 13-17.

2. Бабенко С. І., Костенко О. М. Кібербезпека: проблеми та рішення. Науковий вісник Хмельницького національного університету. 2020. С. 23-28.

3. Лисяк О. І. Економічна безпека держави в умовах її становлення. Економічний аналіз. 2021. С. 11-13.

4. Акімова Л. М. Механізми державного управління економічною безпекою України: аналіз чинників впливу, систематизованих за окремими сферами її розвитку. Аспекти публічного управління. 2018. С. 34-38.

5. Левченко О. В. Загрози та виклики у сфері кібербезпеки : роль штучного інтелекту. Вісник Національної академії Служби безпеки України. 2022. С. 9-14.

УДК 657

Я.В. Слинько., студентка групи 301-ЕО
Науковий керівник – А.В. Дмитренко, д.е.н., доцент
Національний університет
«Полтавська політехніка імені Юрія Кондратюка»

КОНЦЕПТУАЛЬНІ ЗАСАДИ БЕЗПЕКООРІЄНТОВАНОГО ІНФОРМАЦІЙНОГО СЕРЕДОВИЩА ЯК ФАКТОРА ЕКОНОМІЧНОЇ БЕЗПЕКИ

В умовах інтенсивної цифровізації економіки та зростання кількості кіберзагроз, формування концептуальних засад безпекоорієнтованого інформаційного середовища є надзвичайно важливим для забезпечення економічної безпеки як держави, так і суб'єктів господарювання. Таке