

**Міністерство освіти і науки України**

**Національний університет  
«Полтавська політехніка імені Юрія Кондратюка»**

**Навчально-науковий інститут фінансів, економіки,  
управління та права  
Кафедра фінансів, банківського бізнесу та оподаткування**



# **ЕКОНОМІЧНА БЕЗПЕКА: ДЕРЖАВА, РЕГІОН, ПІДПРИЄМСТВО**

**Матеріали ІХ Міжнародної  
науково-практичної конференції**

**15 травня 2025 р.**

**Полтава  
2025**

## СЕКЦІЯ 2. БЕЗПЕКООРІЄНТОВАНЕ ІНФОРМАЦІЙНЕ СЕРЕДОВИЩЕ В КОНТЕКСТІ ПІДВИЩЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ

---

---

УДК 336.711.025.13(477)

**Філонич Олена Миколаївна,**

*кандидат економічних наук, доцент,  
ректор Національного університету «Полтавська  
політехніка імені Юрія Кондратюка»*

**Черв'як Анна Володимирівна**

*доктор філософії, в.о. ученого секретаря Вченої ради,  
Національний університет «Полтавська політехніка імені  
Юрія Кондратюка»*

### НАГЛЯДОВА ПОЛІТИКА НБУ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ БАНКІВСЬКИХ УСТАНОВ

У сучасних умовах банківський нагляд є фундаментальним інструментом забезпечення стабільності банківського сектору та фінансової безпеки держави. Його основна мета полягає у зниженні системних ризиків, підвищенні прозорості діяльності банківських установ та зміцненні довіри з боку учасників фінансового ринку.

Національний банк України, відповідно до Закону України «Про банки і банківську діяльність» [1], здійснює нагляд і регулювання банків для сприяння безпеці та фінансовій стабільності банківської системи. Банківський нагляд займає одну з ключових позицій у питанні забезпечення довіри до установи з боку клієнтів, вкладників, кредиторів і позичальників надаючи гарантії стабільного функціонування банку та спроможності своєчасно й у повному обсязі виконувати зобов'язання.

Суть інформаційної безпеки банку полягає у захисті інформації від загроз широкого спектру для забезпечення

безперервності роботи установи, мінімізації бізнес ризику, максимізації рентабельності інвестицій і бізнес можливостей. Інформаційна безпека забезпечується шляхом впровадження комплексу заходів, які охоплюють політику, процеси, процедури, організаційні структури і програмні та апаратні функції [2, с. 78].

НБУ здійснює нагляд за інформаційним середовищем банківських установ з метою забезпечення безпеки, фінансової стабільності та стійкості банківської системи до сучасних кіберзагроз. Основні підходи та інструменти нагляду відображені у таблиці 1.

Таблиця 1

Основні підходи нагляду НБУ за інформаційним середовищем банків

Підхід	Суть нагляду
1	2
Впровадження системи контролю за інформаційною безпекою та кіберзахистом	Проведення фахівцями у сфері кіберзахисту та інформаційної безпеки виїзних і безвиїзних перевірок (дистанційний нагляд), що дозволяє оперативно реагувати на ризики та виявляти порушення. Планування виїзних перевірок з питань інформаційної безпеки, кіберзахисту та надання кваліфікованих електронних довірчих послуг здійснюється на підставі ризик-орієнтованого підходу, визначеного Положенням про здійснення контролю за дотриманням банками вимог законодавства з питань інформаційної безпеки, кіберзахисту та електронних довірчих послуг.
Нормативне регулювання	Відповідно до Постанови Правління НБУ №4 від 16 січня 2021 року, банки зобов'язані щорічно проводити самооцінку стану інформаційної безпеки/кіберзахисту та подавати відповідний звіт до НБУ. Це дозволяє регулятору оцінювати ефективність системи управління інформаційною безпекою, повноту виконання банком вимог законодавства та рівень управління ризиками.

## Продовження таблиці 1

1	2
Оцінка ризиків та система раннього реагування	НБУ проводиться аналіз діяльність кожного банку, оцінювання поточних й потенційних ризиків, та впроваджує систему раннього реагування на проблеми, які можуть виникнути у сфері інформаційної безпеки. Ключовий акцент саме банківські установи, які становлять найбільшу небезпеку для стабільності банківської системи.
Комплексний аналіз і аудит	Під час нагляду використовуються як CAMELS-рейтинг (оцінка капіталу, якості активів, менеджменту, прибутковості, ліквідності та чутливості до ринку), так і спеціалізовані аудити інформаційної безпеки. Це дозволяє своєчасно виявляти недоліки та впроваджувати коригувальні заходи.
Застосування заходів впливу	НБУ має право застосовувати заходи впливу до банків, у яких виявлено порушення, відповідно до чинного законодавства для мінімізації потенційних загроз для клієнтів, вкладників і кредиторів.

*Джерело:* складено за даними [1, 3, 5]

Таким чином, нагляд НБУ за інформаційним середовищем банків базується на поєднанні нормативного регулювання, регулярного моніторингу, аудиту, самооцінки банків та оперативного реагування на кіберзагрози, що забезпечує стійкість і довіру до банківської системи України.

Наглядова політика Національного банку України є ключовим інструментом забезпечення стійкості банківської системи, захисту прав і законних інтересів вкладників, кредиторів і контрагентів, а також зниження системних ризиків. Її ефективне функціонування сприяє не лише фінансовій стабільності, а й формуванню довіри до банківських установ з боку суспільства.

## Література

1. Закон України «Про банки і банківську діяльність» № 2121-III від 7 грудня 2000 року.  
URL:<https://zakon.rada.gov.ua/laws/show/2121-14#Text>
2. Напора І. Ю. Інформаційна безпека банківських установ як об'єкт наукових досліджень. Вісник черкаського університету. Серія: Економічні науки. 2014. №39 (332). С. 77-80.
3. Постанова Правління НБУ №4 від 16 січня 2021 року «Про затвердження Положення про здійснення контролю за дотриманням банками вимог законодавства з питань інформаційної безпеки, кіберзахисту та електронних довірчих послуг». URL: <https://zakon.rada.gov.ua/laws/show/v0004500-21#Text>
4. Onyshchenko S., Yanko A., Hlushko A., Sivitska S. Conceptual principles of providing the information security of the national economy of Ukraine in the conditions of digitalization. *International Journal of Management*. 2020. № 11(12). P. 1709-1726. <https://doi.org/10.34218/IJM.11.12.2020.157>
5. Національний банк України. URL: <https://bank.gov.ua/ua/news/all/u-2025-rotsi-u-shistoh-bankah-zaplanovani-perevirki-z-pitan-informatsiynoyi-bezpeki-kiberzahistu-ta-elektronnih-dovirchih-poslug>
6. Onyshchenko S., Yanko A., Hlushko A., Maslii O., Cherviak A. Cybersecurity and improvement of the information security system. *Journal of the Balkan Tribological Association*. 2023. 29(5). pp. 818– 835.
7. Yehorycheva S., Hlushko A., Khudolii Y. Issue of Ukrainian financial sector information security. *Development Management*. 2023. №22(4). P. 45-52.
8. Varnalii Z., Onyshchenko S., Filonych O., Maslii O. (2020) State policy for ensuring budgetary security of Ukraine in terms of financial globalization, *International Journal of Management*, Vol. 11, Issue 12, DOI: <https://doi.org/10.34218/IJM.11.12.2020.215>