

4. Про затвердження Положення про Міністерство охорони здоров'я України: постанова Кабінету Міністрів України від 25 березня 2015 р. № 267. Верховна Рада України: офіційний веб-сайт. 2022. URL: <https://zakon.rada.gov.ua/laws/show/267-2015-п#Text>

5. Про утворення Національної служби здоров'я України: постанова Кабінету Міністрів України від 27 грудня 2017 р. № 1101. Верховна Рада України: офіційний веб-сайт. 2022. URL: <https://zakon.rada.gov.ua/laws/show/1101-2017-п/ed20240229#Text>

6. Смілій І. А. Форми та методи діяльності Державної міграційної служби України щодо протидії адміністративним правопорушенням іноземців. *Публічне право*. 2013. № 2. С. 355–361.

7. Усачов Є. Адміністративно-правовий статус суб'єктів, що визначають правові засади державної політики у сфері надання медичних послуг в Україні на національному рівні. *Прикарпатський юридичний вісник*. 2018. Том 2. Випуск 1 (22). С. 294–298.

УДК 34

DOI <https://doi.org/10.32844/2618-1258.2024.3.30>

ШАРУК О.Г.

## ОСНОВНІ ЗАГРОЗИ ДЛЯ СТІЙКОСТІ ФУНКЦІОНУВАННЯ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ФІНАНСОВОГО СЕКТОРУ УКРАЇНИ

### MAIN THREATS TO THE SUSTAINABILITY OF FUNCTIONING OF CRITICAL INFRASTRUCTURE FACILITIES OF THE FINANCIAL SECTOR OF UKRAINE

Статтю присвячено розкриттю актуальних загроз для стійкості функціонування об'єктів критичної інфраструктури фінансового сектору України, протистояти яким має національна система захисту критичної інфраструктури. Констатовано, що загрози та ризики можна розглядати з різних боків та з різним інтерпретаційним контекстом. Чинне законодавство у досліджуваній сфері не надає вичерпного визначення означених термінів, чим, власне, зумовлює виникнення актуальних наукових дискусій. З огляду на проаналізовані нормативні положення зроблено висновок, що ризики мають два різновиди: ті, що пов'язані із виникненням загроз (неврахування ризику веде до загрози); ті, що існують паралельно з ймовірністю виникнення загроз (самостійні ризики, що наявними є постійно). Причому другий контекст є значно ширшим. Більшою мірою саме про нього йдеться у нормах чинного законодавства. Натомість загрозою, за таким баченням, є фізичний прояв небезпеки від наявності (виникнення) певного явища. З точки зору наукового суб'єктивізму визначено доцільним твердження, що ризик має бути пов'язаним із загрозою, точніше зумовлювати наявність останніх. У такій інтерпретації актуальними загрозами для стійкості функціонування об'єктів критичної інфраструктури фінансового сектору України наразі є: технічні збої або інші невідворотні обставини, які об'єктивно унеможливають проведення відповідних операцій; вчинення терористичних актів і диверсійних операцій, зокрема і кібератак на фінансову інфраструктуру; світові фінансово-економічні кризи; неефективність регулятивних, контрольних-наглядових та моніторингових заходів; соціально-політична нестабільність; пошкодження чи знищення матеріальних активів суб'єктів фінансового сектору через воєнні дії; втрата міжнародної підтримки; недотримання міжнародних зобов'язань; спад попиту на кредитування; неефективне нормативне регулювання небанківського фінансового ринку; неефективність та недостатня розвиненість інфраструктури ринків капіталу та організованих товарних ринків; неспроможність регулятора ефективно здійснювати свої повноваження.

**Ключові слова:** адміністративно-правовий захист, банківський сектор, заходи охорони та захисту, загрози, критична інфраструктура, національна система захисту критичної інфраструктури, фінансовий сектор, фінансові послуги.

---

© ШАРУК О.Г. – здобувач (Науково-дослідний інститут публічного права)

The article is dedicated to revealing the current threats to the resilience of critical infrastructure objects in Ukraine's financial sector, which the national critical infrastructure protection system must counteract. It is stated that threats and risks can be viewed from various perspectives and interpretative contexts. The current legislation in the studied field does not provide an exhaustive definition of these terms, which, in turn, leads to relevant scientific discussions. Based on the analyzed normative provisions, it is concluded that risks have two types: those associated with the emergence of threats (neglecting the risk leads to a threat); and those that exist parallel to the probability of threats occurring (independent risks that are constantly present). The second context is significantly broader, and it is primarily this context that is referred to in the norms of the current legislation. Conversely, a threat, according to this view, is the physical manifestation of danger from the presence (emergence) of a certain phenomenon. From the perspective of scientific subjectivism, it is deemed appropriate to assert that risk should be associated with a threat, more precisely, it should lead to the presence of the latter. In this interpretation, the current threats to the resilience of critical infrastructure objects in Ukraine's financial sector include: technical failures or other unavoidable circumstances that objectively prevent the execution of relevant operations; acts of terrorism and sabotage operations, including cyberattacks on financial infrastructure; global financial-economic crises; inefficiency of regulatory, supervisory, and monitoring measures; socio-political instability; damage or destruction of material assets of financial sector entities due to military actions; loss of international support; non-compliance with international obligations; a decline in demand for credit; ineffective regulatory framework for the non-banking financial market; inefficiency and insufficient development of capital market infrastructure and organized commodity markets; and the regulator's inability to effectively carry out its powers.

**Key words:** *administrative-legal protection, banking sector, critical infrastructure, financial sector, financial services, national critical infrastructure protection system, security and protection measures, threats.*

**Постановка проблеми.** Стійкість України залежить від спільних зусиль держави, місцевої влади, бізнесу та громадян [1]. Першочерговим в означеному є необхідність усвідомлення важливості координації дій, розподілу обов'язків та здійснення постійного інформаційного обміну між ними. Зокрема Концепцію запровадження національної системи стійкості України, ухваленої рішенням Ради національної безпеки і оборони України 20 серпня 2021 року та введеного в дію Указом Президента України №479 від 27 вересня 2021 року передбачено, що усі суб'єкти забезпечення національної стійкості постійно обмінюються необхідною інформацією, комунікують між собою у різних форматах, спільно виконують визначені завдання у межах своєї відповідальності. Також міститься норма, яка визначає, що безпека та захищеність об'єктів критичної інфраструктури є базовим елементом забезпечення її функціонування. Такий порядок речей є цілком логічним, адже згідно із Концепцією, стійкість визначається як здатність держави та суспільства вчасно виявляти загрози і вразливості, оцінювати ризики для національної безпеки, швидко і ефективно реагувати, повністю відновлюватися після загроз, у тому числі гібридних, надзвичайних ситуацій та криз будь-якого характеру [2].

Національним планом захисту та забезпечення безпеки та стійкості критичної інфраструктури передбачено ряд заходів постійного чи строкового виконання, що мають підтримувати стан захищеності критичної інфраструктури, за якого забезпечуються функціональність, безперервність роботи, відновлюваність, цілісність і стійкість критичної інфраструктури [3].

Тому **метою цієї статті** є розкриття актуальних загроз для стійкості функціонування об'єктів критичної інфраструктури фінансового сектору України, протистояти яким має національна система захисту критичної інфраструктури.

**Аналіз останніх досліджень та публікацій.** Представлена до аналізу проблематика визначається широким змістом, який поглинає загальні та спеціальні її особливості. Зокрема аспект диференціації ризиків та загроз, їхня загальна система, а також універсальні негативні тенденції у сфері захисту критичної інфраструктури можна прослідкувати у працях таких вчених як А. Арістова, Д. Бірюков, С. Кондратов, Г. Мазур, О. Насвіт, Т. Романчик, А. Собакар, М. Сокиран, О. Суходоля. Водночас спеціальні питання захисту критичної інфраструктури фінансового сектору України не мають свого наукового висвітлення, адже є вузькоспеціалізованими, що додатково актуалізує необхідність їхнього вивчення.

**Виклад основного матеріалу.** Перш за все слід вказати, що безпека та стійкість за загальним контекстом перебувають у кореляційному взаємозв'язку. Стійкість є невід'ємною складовою безпеки, що досягається шляхом забезпечення можливості для конкретної системи ефективно реагувати на загрози та ризики.

Загалом терміни «загроза» та «ризик» пов'язані з явищем «небезпеки», тобто за властивість мають настання негативних наслідків у випадку активації механізмів їх реалізації в практичну площину. Причому, на нашу думку: 1) загроза є більш статичним явищем, тоді як ризик характеризується оціночним припущенням про негативний вплив в перспективі; 2) ризик як оціночне явище є комбінацією ймовірностей, тоді як загроза може бути реальною та потенційною; 3) ризик за загальним контекстом має якісні і кількісні показники, а загроза існує незалежно від того, реалізована вона чи ні.

Вчений М. Сокіран узагальнює аналіз визначених ним ідентифікаційних характеристик означених явищ таким чином: категорія «ризик» у контексті забезпечення безпеки та стійкості критичної інформаційної інфраструктури в Україні є формою вияву небезпеки, обумовленою наявністю явищ, чинників, обставини, подій тощо, яка потенційно має завдати наслідків негативного впливу на перебіг суспільних відносин, функціональність об'єктів чи конкретним охоронюваним законом інтересам у цій сфері; під категорією загрози слід розуміти також форму вияву небезпеки, яка обумовлена наявністю явищ, чинників, обставин, подій тощо, однак тільки тої, яка в майбутньому завдасть шкоди безпеці та стійкості критичної інформаційної інфраструктури в Україні (зокрема у разі відсутності дій щодо її нейтралізації вона переросте у ризик) [4, с.100].

Іншої думки вчений Т. Романчик, який при дослідженні небезпеки, загрози та ризику прийшов до висновку, що: «небезпеку можна розглядати як стан, загрозу – як дію, ризик – як імовірність втрати частини ресурсів під негативним впливом випадкових подій, які погано прогноуються» [5].

Аналізуючи положення Закону України «Про критичну інфраструктуру», зокрема пункт 4 частини 2 статті 4, де зазначено, що: «Державна політика у сфері захисту критичної інфраструктури ґрунтується на засадах створення умов та впровадження заходів, спрямованих на ефективне зниження і контроль за ризиками безпеки, на зниження ризику реалізації можливих загроз, ліквідацію та/або мінімізацію наслідків реалізованих загроз, кризових ситуацій та інших їх видів» вбачаємо, що загроза у цьому контексті є основним явищем на мінімізацію наслідків якої спрямовуються дії уповноважених суб'єктів. Водночас ризик визначається як імовірність виникнення цих загроз (зрозуміло, що ризик має свої негативні наслідки, зокрема у цьому контексті у вияві загроз), протидія яким є першим кроком для убезпечення систем від негативного впливу неконтрольованих процесів різного характеру.

З урахуванням нашого бачення розмежування досліджуваних категорій варто зауважити, що загрози для стійкості функціонування об'єктів критичної інфраструктури фінансового сектору України доцільно диференціювати на два різновиди: універсальні, тобто такі, що можуть або спричиняють негативні наслідки для більшості або навіть для усіх об'єктів критичної інфраструктури в Україні та індивідуальні, сутність яких нами зведено до виключно досліджуваної сфери.

Причому загрози критичній інфраструктурі, як правило, розподіляються на три групи, що включають аварії й технічні збої, природні лиха та небезпечні природні явища, зловмисні дії (груп або окремих осіб, таких як терористи, злочинці й диверсанти, промислове шпигунство, а також бойові дії). Особливо небезпечними є комбіновані загрози й загрози, реалізація яких може призвести до катастрофічних і різноманітних каскадних ефектів унаслідок взаємозалежності елементів критичної інфраструктури [6]. Додатково вкажемо, що закордонні вчені, проаналізувавши набір даних у 29 європейських країнах, вказують про те, що на енергетичний сектор припадає 60% усіх каскадів, 28% – на інформаційний сектор (телекомунікацій та Інтернету), 5% – на транспортний сектор, 3% – на водний [7]. Означене свідчить, що енергетичний та інформаційний сектори є найбільш вразливими [8, с. 289], порушення функціональності яких може стати причиною каскадних збоїв в інших сферах, зокрема і у фінансовій.

Зокрема вперше про необхідність захисту критичної інфраструктури фінансового сектору було визначено в «Зеленій книзі з питань захисту критичної інфраструктури в Україні», підготовленій у 2015 році Національним інститутом стратегічних досліджень із залученням українських та зарубіжних експертів і за підтримки Офісу зв'язку НАТО в Україні на основі вивчення досвіду країн-членів ЄС та НАТО з врахуванням безпекової ситуації в Україні та особливостей розбудови елементів сектору безпеки країни. Загалом у ній сформульовані першочергові кроки із побудови

державної системи захисту критичної інфраструктури в Україні [9]. У Додатку А зазначеної книги фінансовий сектор і банки були включені у перелік секторів критичної інфраструктури України.

Власне, її положеннями експерти вперше запропонували наступні категорії загроз, на які має бути налаштований захист критичної інфраструктури, а саме: 1) аварії та технічні збої, зокрема, авіаційні катастрофи, ядерні аварії, пожежі, аварії у системах енергозабезпечення, викиди небезпечних речовин, відмови систем, аварії та надзвичайні події обумовлені недбалістю, організаційними помилками тощо; 2) небезпечні природні явища, зокрема, надзвичайні погодні умови, лісові, степові та торф'яні пожежі, сейсмічні явища, епідемії та пандемії, космічні явища, урагани, торнадо, землетруси, цунамі, повені і т. ін.; 3) зловмисні дії, зокрема, зловмисні дії груп або окремих осіб, таких як терористи, злочинці і диверсанти, а також військові дії в умовах війни [9].

Доречно також навести думку А. Собакаря, який вказує, що залежно від типу інфраструктури, загрози її безпечною та сталому функціонуванню класифікуються на дві групи: фізичні загрози та кібератаки. Зрозуміло, що трубопроводи, підстанції, склади, комунікаційна інфраструктура та промислові заводи в основному піддаються фізичним загрозам. На протидію ним, кіберзагрози піддають небезпеці системи моніторингу та контролю, бази даних, функціональні системи, програмне забезпечення, автоматизовані виробничі засоби тощо [10, с. 266-267].

Враховуючи зазначене та опираючись на власний суб'єктивізм, вбачаємо, що серед основних універсальних загроз, які є актуальними для стійкості функціонування об'єктів критичної інфраструктури фінансового сектору України можна виділити:

1) технічні збої або інші невідворотні обставини, які об'єктивно унеможливають проведення відповідних операцій. Яскравий приклад такого стався першого вересня 2022 року, коли тимчасово перестали працювати термінали, картки та онлайн-банкінг Ощадбанку. Начальник управління банку зі зв'язків із громадськістю та ЗМІ Я. Титова пояснила, що банк проводив планові технічні роботи. За її словами, зазвичай такий процес відбувається непомітно для клієнтів, але цього разу стався технічний збій. При цьому він тривав близько 1,5 години [11]. На основі цього прикладу можемо обґрунтувати, що представники банку не врахували усіх ризиків при проведенні планових технічних робіт, що стало загрозою для безперервності здійснення фінансових операцій з такими наслідками: тимчасове призупинення доступу клієнтів до їхніх рахунків; виникнення паніки серед клієнтів; втрати у вигляді недоотриманих доходів та репутаційні збитки для банку. Цей випадок демонструє, наскільки важливою є підготовка та управління ризиками для підтримки стійкості роботи банківської системи;

2) вчинення терористичних актів і диверсійних операцій. Уточнимо, що загалом напружена воєнно-політична ситуація, в умовах якої наша держава відстоює власну територіальну цілісність і суверенітет, характеризується значним зростанням рівня таких загроз зловмисних дій, як вчинення терористичних актів і диверсійних операцій на території України, спрямованих на об'єкти критичної інфраструктури [9]. Фінансовий сектор не є виключенням, адже майже щоденно стикається з кібератаками ворога. Власне масштабні хакерські атаки на органи влади, Національний банк та банківські застосунки відбувалися і до 24 лютого. Зокрема, віртуальну підготовку до реального нападу на Україну росіяни провели 13-14 січня та 15-16 лютого. Причому, як правило, інтенсивність хакерських атак посилюється, наприклад, під час оголошення українськими волонтерами масштабних зборів. Загалом українська система кіберзахисту виявилася напрочуд стійкою та підготовленою до ударів агресора [12]. Однак тимчасових збоїв у роботі фінансового ринку інколи вдавалось досягти. Як зазначає О. Гороховський (співзасновник проекту Monobank): «За дев'ять місяців вони змогли лише на кілька годин «покласти» сайт, який не впливає на обслуговування клієнтів. Усі атаки були передбачені в архітектурі системи безпеки» [12];

3) світові фінансово-економічні кризи. Причини, через які в економіці виникають кризи, можуть бути різні. Це й невміле фінансово-економічне управління. І перенасичення ринків пропозицією, тобто надмірна конкуренція. І стихійні явища – катаклізми, війни, катастрофи, епідемії [13]. Їхні наслідки значні, адже викликають дестабілізацію всього фінансового сектора або його частини, що проявляється у неспроможності його складовими виконувати свої функції внаслідок критичного погіршення фінансових показників. Вони також можуть супроводжуватися скороченням кількості суб'єктів фінансового ринку і застосуванням державою заходів надзвичайного характеру [14];

4) не ефективність регулятивних, контрольно-наглядових та моніторингових заходів. Наприклад, збільшення випадків шахрайства та відмивання грошей корелює з результативністю означеної діяльності. Заслабкі регулятивні рамки здатні завдати значної шкоди фінансовій системі загалом, а надмірне регулювання може обмежувати гнучкість і інновації в механізмах її розвитку;

5) соціально-політична нестабільність. Будь-які зміни політичного чи соціального характеру здатні завдати шкоди фінансовому сектору як через функціональний вплив (наприклад, масове зняття готівки чи депозитів), так і фізичний вплив (наприклад, порушення роботи банківських установ через акції протесту). Як свого часу зазначив В. Заплатинський, – «сьогодні слід вжити усіх невідкладних заходів, щоб запобігти впливу політичної ситуації на економічну сферу» [15];

6) пошкодження чи знищення матеріальних актів суб'єктів фінансового сектору через воєнні дії. Безпосередніх інфраструктурних втрат зазнали чисельні суб'єкти ринку фінансових послуг. Як приклад, це банк «ПУМБ» у якого під час нічної ракетної атаки РФ на Запоріжжя 18 жовтня 2023 року постраждало відділення за адресою: пр-т Соборний, 149 [16]. Загалом збитки банків від знищення нерухомості сягнули 750 млн грн уже на кінець 2022 року. За очікуваннями Національного банку України, втрати банків унаслідок війни можуть зрости до 20% довоєнного працюючого портфеля. Попри те, що втрати банків зростуть, більшість банків зможе їх поглинути за рахунок прибутку та запасу капіталу [17].

Щодо індивідуальних загроз маємо вказати, що аналізуючи положення оновленої Стратегії розвитку фінансового сектору України [17], загрозами для стійкості функціонування об'єктів критичної інфраструктури фінансового сектору України можуть бути:

1) спад економічної активності – наразі економічна активність почала поступово відновлюватися завдяки усуненню перебоїв у ланцюгах постачання, релокації підприємств, звільненню окупованих територій і поверненню частини переміщених осіб [17];

2) інфляційні процеси – зараз також спостерігається контрольоване середовище інфляційного тиску;

3) втрата міжнародної підтримки – оскільки значна частина дефіциту державного бюджету покривається за рахунок міжнародної допомоги, її втрата чи зменшення обсягів можуть бути катастрофічними для вітчизняної економіки;

4) відсутність стратегічного бачення та плановірності здійснення реформаційних змін – наразі це питання не є критичним в досліджуваній сфері, адже швидка реакція Національного банку України на зміни векторів руху є показником адаптивності та оперативності. Проте все ще не вистачає налагодженого комунікаційного механізму між різними органами влади, що негативно позначається на загальному векторі розвитку держави;

5) недотримання міжнародних зобов'язань – зокрема в аспекті боротьби з корупцією може уповільнити інтеграційні процеси;

6) втрата прибутковості банків – наразі банки мають запас капіталу та ліквідності, є операційно стійкими та ефективними, адже мали плани дій на випадок несприятливих подій [17];

7) спад попиту на кредитування – у кінці 2022 року Національний банк України оприлюднив опитування, яке провели серед банків. У ньому банки проаналізували поведінку своїх клієнтів та надали певні прогнози стосовно своєї діяльності. Виявилось, що: а) у III кварталі зафіксовано незначне відновлення попиту на корпоративні кредити; б) рівень схвалення заявок на корпоративні та роздрібні кредити скорочується від початку повномасштабного вторгнення; в) окремі банки поліпшили оцінки боргового навантаження бізнесу, але погіршили для населення. Загалом банки оцінюють боргове навантаження клієнтів як середнє; г) у наступні 12 місяців очікувалось погіршення якості позик та зростання обсягів фондування [18]. Наприкінці 2023 року банки все ж таки фіксують відновлення попиту на кредити та очікують на подальше зростання корпоративного і роздрібногo портфелів [19];

8) втрата спроможностей системи гарантування вкладів – наразі система гарантування вкладів в змозі демонструвати стійкість та ефективність [17];

9) неефективне нормативне регулювання небанківського фінансового ринку – розвиток небанківського фінансового ринку потребує законодавчих змін у напрямі наближення регуляторного середовища до міжнародних стандартів [17];

10) втрата банками ліквідності – загалом обсяг безготівкових операцій зростає, розширюється перелік фінансових операцій, які здійснюються дистанційно [17];

11) неефективність та недостатня розвиненість інфраструктури ринків капіталу та організованих товарних ринків – сьогодні означене є проблемою, адже питання наявності дієвих механізмів залучення інвестицій (як внутрішніх, так і іноземних) у приватний та державний сектор є ключовою передумовою для швидкого та ефективного повоєнного відновлення України [17];

12) відсутність доступності фінансових послуг – активно впроваджуються інноваційні технології, здатні задовольнити сучасний попит на фінансові послуги.

Окремо зазначимо, що, на нашу думку, система означених загроз має доповнитись ще однією, – неспроможність регулятора ефективно здійснювати свої повноваження. Наприклад, до недавня існувала законодавча проблема щодо виведення з ринку системно важливого банку. Така необхідність виникла на тлі військової агресії з боку РФ, адже власниками фінансових устав України з-поміж інших є представники громадянства цієї країни. У зв'язку з цим було удосконалено чинне законодавство в частині запровадження можливості впливу на банки, які або власники істотної участі у яких є особами, до яких застосовано санкції. Національний банк України отримав ефективний механізм впливу на підсанкційних осіб, що є власниками істотної участі у банку та які, з огляду на застосування до них санкцій, не відповідатимуть вимогам Національного банку України, зокрема щодо ділової репутації. Застосовані санкції ставлять під сумнів платоспроможність підсанкційних осіб і можливість виконання ними грошових зобов'язань, що в подальшому може призвести до невідповідності майнового стану вимогам закону щодо підтримки належного рівня капіталу банку. Тож Національний банк України має можливість відмовляти в допуску підсанкційних осіб до володіння істотною участю в банках України [20]. Означені зміни також дозволяють Національному банку України націоналізувати банки підсанкційних власників. Яскравий приклад тому «Сенс банк» (до 1 грудня 2022 року – «Альфа-Банк») [21].

Наостанок зазначимо і щодо системних ризиків фінансового сектору. Зокрема доцільно вказати, що систему таких визначає та відслідковує їх рівень Рада з фінансової стабільності. Кожне засідання Ради традиційно починається з їхнього огляду. До числа таких у 2023 році віднесено: світова економіка, зовнішня кон'юнктура, економічні умови, державні фінанси, валютний ринок, геополітика [22, с. 5]. Окрім того, Секретаріат Ради відстежує системні ризики, виявлені міжнародними і національними радами та комітетами з фінансової стабільності, а також їхні рекомендації [22, с. 9].

**Висновки.** Маємо констатувати, що загрози та ризики можна розглядати з різних боків та з різним інтерпретаційним контекстом. Чинне законодавство у досліджуваній сфері не надає вичерпного визначення означених термінів, чим, власне, зумовлює виникнення актуальних наукових дискусій.

З огляду на проаналізовані нормативні положення можна зробити висновок, що ризики мають два різновиди: ті, що пов'язані із виникненням загроз (неврахування ризику веде до загрози); ті, що існують паралельно з ймовірністю виникнення загроз (самостійні ризики, що наявними є постійно). Причому другий контекст є значно ширшим. Більшою мірою саме про нього йдеться у нормах чинного законодавства. Натомість загрозою, за таким баченням, є фізичний прояв небезпеки від наявності (виникнення) певного явища.

З точки зору наукового суб'єктивізму нам більше імпонує думка, що ризик має бути пов'язаним із загрозою, точніше зумовлювати наявність останніх. У такій інтерпретації актуальними загрозами для стійкості функціонування об'єктів критичної інфраструктури фінансового сектору України наразі є: технічні збої або інші невідворотні обставини, які об'єктивно унеможливають проведення відповідних операцій; вчинення терористичних актів і диверсійних операцій, зокрема і кібератак на фінансову інфраструктуру; світові фінансово-економічні кризи; неефективність регулятивних, контрольно-наглядових та моніторингових заходів; соціально-політична нестабільність; пошкодження чи знищення матеріальних активів суб'єктів фінансового сектору через воєнні дії; втрата міжнародної підтримки; недотримання міжнародних зобов'язань; спад попиту на кредитування; неефективне нормативне регулювання небанківського фінансового ринку; неефективність та недостатня розвиненість інфраструктури ринків капіталу та організованих товарних ринків; неспроможність регулятора ефективно здійснювати свої повноваження.

### Список використаних джерел

1. Захист критичної інфраструктури від російських атак потребує спільної роботи всіх. *Державна служба спеціального зв'язку та захисту інформації України*, 2023. URL: <https://cip.gov.ua/ua/news/zakhist-kritichnoyi-infrastrukturi-vid-rosiiskikh-atak-potrebuye-spilnoyi-roboti-vsikh>
2. Про рішення Ради національної безпеки і оборони України від 20 серпня 2021 року «Про запровадження національної системи стійкості»: Указ Президента України №479/2021. *Офіційне інтернет-представництво Президента України*. URL: <https://www.president.gov.ua/documents/4792021-40181>
3. Про критичну інфраструктуру: Закон України від 16.11.2021 № 1882-IX. *Верховна Рада України. Законодавство України*. URL: <https://zakon.rada.gov.ua/laws/show/1882-20#Text>

4. Sokiran Maksym. Analysis of Terminology for Identifying the Risks of Ensuring Security and Sustainability of Critical Information Infrastructure in Ukraine. *Visegrad Journal on Human Rights*. № 5, 2023. Pp. 96-104.
5. Романчик Т.В. Небезпека, загроза, ризик: аналіз термінологічного апарату теорії економічної безпеки. *Економічний вісник НТУУ «КПІ»*, 2020. С. 257-267.
6. Загрози критичній інфраструктурі та їх вплив на стан національної безпеки (моніторинг реалізації Стратегії національної безпеки) (аналітична записка). *Національний інститут стратегічних досліджень*. URL: [https://niss.gov.ua/sites/default/files/2017-03/KI\\_Ivanyuta-3a331.pdf](https://niss.gov.ua/sites/default/files/2017-03/KI_Ivanyuta-3a331.pdf)
7. Luijff E, Nieuwenhuijs A, Klaver M, Van Eeten M, Cruz E (2009) Empirical findings on critical infrastructure dependencies in Europe. In: Setola R, Geretshuber S (eds) CRITIS 2008, LNCS 5508, pp. 302–310.
8. Сокіран М. Стан наукової розробленості проблем адміністративно-правового забезпечення безпеки та стійкості критичної інформаційної інфраструктури. *Юридичний науковий електронний журнал*. 2023. №12. С. 287-291.
9. Бірюков Д.С., Кондратов С.І., Насвіт О.І., Суходоля О.М. Зелена книга з питань захисту критичної інфраструктури в Україні. *Національний інститут стратегічних досліджень*, 2015. URL: [https://cdn.regulation.gov.ua/6a/69/2a/fa/regulation.gov.ua\\_File\\_188.pdf](https://cdn.regulation.gov.ua/6a/69/2a/fa/regulation.gov.ua_File_188.pdf)
10. Собакарь А.О. Загрози критичній інфраструктурі та їх вплив на стан національної безпеки України. *Російсько-українська війна: право, безпека, світ*: матеріали VI міжнародної науково-практичної конференції ( 29-30 квітня 2022 року). Тернопіль, 2022. С. 264-267
11. В Ощадбанку стався технічний збій: клієнти скаржаться на роботу сервісів. *Мінфін*, 2022. URL: <https://minfin.com.ua/ua/2022/09/01/91503987/>
12. Вдарити по центру банківських операцій. Чи можуть російські терористи «покласти» банки? *ЕП*, 2022. URL: <https://www.epravda.com.ua/rus/publications/2022/12/15/695046/>
13. Світові фінансово-економічні кризи. *Finance UA*, 2023. URL: <https://finance.ua/ua/goodtoknow/finansovo-ekonomiczni-kryzy>
14. Арістова А., Мазур Г. Інструментарій державного антикризового управління в банківському секторі. *Вісник КНТЕУ*. 2010. № 2. С. 88–102.
15. Соціально-економічні наслідки політичної нестабільності, що виникла після підписання Указу Президента України про дострокове припинення повноважень Верховної Ради було обговорено на розширеному засіданні Комітету з питань економічної політики. *Верховна Рада України. Законодавство України*. URL: <https://www.rada.gov.ua/news/Povidomlennya/10355.html>
16. Прес-центр ПУМБ. *ПУМБ*, 2023. URL: <https://about.pumb.ua/presscenter/news/item/6965-vnasldok-ataki-uf-poshkodzheno-vddlennya-pumb-u-za>
17. Стратегія розвитку фінансового сектору України до 2025 року. *Національний банк України*. URL: [https://bank.gov.ua/admin\\_uploads/article/Strategy\\_finsector\\_NBU.pdf?v=7](https://bank.gov.ua/admin_uploads/article/Strategy_finsector_NBU.pdf?v=7)
18. Чи буде в Україні попит на онлайн кредити в 2023 році? Думки експертів. *ЕП*, 2022. URL: <https://www.epravda.com.ua/press/2022/12/15/694676/>
19. Банки фіксують відновлення попиту на кредити та очікують на подальше зростання корпоративного і роздрібного портфелів – результати Опитування про умови банківського кредитування. *Національний банк України*, 2023. URL: <https://bank.gov.ua/ua/news/all/banki-fiksuyut-vidnovlennya-popitu-na-kreditu-ta-ochikuyut-na-podalshe-zrostannya-korporativnogo-i-rozdribnogo-portfeliv--rezultati-opituvannya-pro-umovi-bankivskogo-kredituvannya>
20. Пояснювальна записка до проекту Закону України про внесення змін до деяких законодавчих актів України щодо удосконалення процедури виведення з ринку банку в умовах воєнного стану. *Верховна Рада України. Законодавство України*. URL: [blob:https://itd.rada.gov.ua/4e286507-1e13-4beb-854b-a5a0e55e7c60](https://itd.rada.gov.ua/4e286507-1e13-4beb-854b-a5a0e55e7c60)
21. НБУ розпочав процес націоналізації Сенс Банку (раніше - Альфа-Банк). *Інтерфакс-Україна*, 2023. URL: <https://interfax.com.ua/news/economic/924069.html>
22. Звіт про діяльність Ради з фінансової стабільності (серпень 2022 – липень 2023). *Національний банк України*. URL: [https://bank.gov.ua/admin\\_uploads/article/FSB\\_Report%202022-2023.pdf?v=7](https://bank.gov.ua/admin_uploads/article/FSB_Report%202022-2023.pdf?v=7)