

**ВСП «Харківський торговельно-економічний фаховий коледж
Державного торговельно-економічного університету»**

Циклова комісія економіки, управління та адміністрування

Яковлєв Ігор Валерійович

ПБ здобувача

КУРСОВА РОБОТА

Аналіз зовнішніх та внутрішніх загроз підприємства

тема

Навчальна
дисципліна

Фінансово-економічна безпека організації

назва навчальної дисципліни

Ступінь освіти

Фаховий молодший бакалавр

фаховий молодший бакалавр, молодший бакалавр, бакалавр

Галузь знань

07 Управління та адміністрування

шифр і назва галузі знань

Спеціальність

072 Фінанси, банківська справа та страхування

код і найменування спеціальності

Освітньо-професійна
програма

Фінанси і кредит

назва освітньо-професійної програми

Академічна група

Ф-23

назва академічної групи

Харків, 2025 рік

ДОПУЩЕНО ДО ЗАХИСТУ

Керівник:

Постольна Наталія Олександрівна, викладач
циклової комісії економіки, управління та
адміністрування, спеціаліст вищої категорії

Робота містить результати власних досліджень. Використання ідей,
результатів і текстів інших авторів мають посилання на відповідне джерело.


Здобувач


підпис здобувача

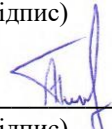
І.В. ЯКОВЛЄВ
ПІБ здобувача

Підсумкова оцінка: **70** (балів)

Члени комісії з захисту:


(підпис)

Н. О. Постольна


(підпис)

О.М. Тимошенко

ВСП «Харківський торговельно-економічний фаховий коледж
Державного торговельно-економічного університету»

Циклова комісія економіки, управління та адміністрування

Яковлєв Ігор Валерійович

ПІБ здобувача

ЗАВДАННЯ НА КУРСОВУ РОБОТУ

Навчальна
дисципліна

Фінансово-економічна безпека організації

назва навчальної дисципліни

Тема роботи

Аналіз зовнішніх та внутрішніх загроз підприємства

тема курсової роботи

Термін подання
завершеної роботи

26.05.2025 р.

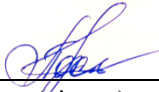
фаховий молодший бакалавр, молодший бакалавр, бакалавр

Графік виконання роботи

Виконання роботи за розділами	Термін виконання
Вибір та затвердження теми	03.03 – 08.03.2025
Добір та аналіз літератури за обраною темою	10.03 – 22.03.2025
Складання плану курсової роботи	24.03 – 29.03.2025
Написання вступу та I розділу	31.03 – 19.04.2025
Написання розрахункової частини (II розділ) курсової роботи	21.04 – 10.05.2025
Написання висновків та пропозицій, оформлення курсової роботи	12.05 – 24.05.2025
Подання курсової роботи керівнику для рецензування (для рекомендації до захисту)	26.05 – 31.05.2025
Захист курсової роботи	02.06 – 07.06.2025

Завдання видав

Науковий керівник,
спеціаліст вищої категорії



(підпис) **Наталія ПОСТОЛЬНА**

«06» березня 2025 р.

Завдання отримав

Здобувач



(підпис) **Ігор ЯКОВЛЄВ**
ПІБ здобувача

«06» березня 2025 р.

ЗМІСТ

ВСТУП.....	5
РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ АНАЛІЗУ ЗАГРОЗ У БАНКІВСЬКІЙ СФЕРІ	
1.1. Поняття загроз у банківській сфері та їх класифікація.....	7
1.2. Методичні підходи до аналізу загроз.....	9
РОЗДІЛ 2. ОРГАНІЗАЦІЙНО-ЕКОНОМІЧНА ХАРАКТЕРИСТИКА АТ «УКРСИББАНК»	
2.1. Загальна характеристика діяльності АТ «УкрСибббанк».....	12
2.2. Заходи мінімізації загроз і підвищення безпеки діяльності банку...	14
ВИСНОВОК.....	17
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	18

ВСТУП

У сучасних умовах нестабільного економічного середовища та зростання глобальних ризиків забезпечення стабільності функціонування банківської системи є одним із головних пріоритетів як державної економічної політики, так і внутрішньої стратегії кожної банківської установи. Особливу увагу в цьому контексті слід приділяти своєчасному виявленню, аналізу та нейтралізації внутрішніх і зовнішніх загроз, що безпосередньо впливають на безпеку банку, його фінансову стійкість та довіру з боку клієнтів і партнерів.

Банки, як ключові учасники фінансового ринку, постійно стикаються з широким спектром загроз, серед яких економічні, технічні, правові, соціальні, інформаційні, організаційні та кадрові. Зовнішні загрози можуть бути пов'язані з макроекономічною ситуацією, змінами у законодавстві, політичною нестабільністю, конкуренцією, кіберзлочинністю тощо. Внутрішні – з неефективною організаційною структурою, недоліками в системі внутрішнього контролю, кадровими проблемами, зловживаннями працівників, порушеннями банківських процедур.

Актуальність дослідження зумовлена необхідністю поглибленого розуміння природи банківських загроз, їх систематизації, а також формування ефективної моделі управління ризиками та загрозами з метою зниження їхнього впливу на діяльність банківської установи. Особливої ваги ці питання набувають в умовах воєнного стану, цифровізації фінансового сектору, трансформації банківських послуг та зростання ролі кібербезпеки.

Метою курсової роботи є дослідження сутності внутрішніх та зовнішніх загроз банківської установи, їх класифікація, аналіз причин виникнення та розробка пропозицій щодо запобігання і мінімізації їх впливу.

Завдання курсової роботи:

- розглянути теоретичні основи поняття банківських загроз;
- класифікувати внутрішні та зовнішні загрози;

- дослідити методологічні підходи до аналізу загроз банківської діяльності;
- надати загальну характеристику АТ «УкрСиббанк»;
- провести аналіз основних внутрішніх і зовнішніх загроз;
- сформулювати рекомендації щодо вдосконалення системи безпеки та управління ризиками.

Об'єктом дослідження є АТ «УкрСиббанк».

Предметом дослідження виступають внутрішні та зовнішні загрози, що впливають на ефективність його функціонування.

РОДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ АНАЛІЗУ ЗАГРОЗ У БАНКІВСЬКІЙ СФЕРІ

1.1. Поняття загроз у банківській сфері та їх класифікація

Загрози безпеці банків за походженням поділяються на внутрішні та зовнішні. Обидві категорії можуть мати економічний, фізичний та інтелектуальний характер впливу на банки.

Економічні загрози включають корупцію, шахрайство, недобросовісну конкуренцію та використання неефективних банківських технологій. Такі загрози завдають збитків банкам або призводять до втрати вигоди. Основні причини їх виникнення: недостатня адаптація банківських систем до змін ринку, загальна неплатоспроможність суб'єктів господарювання, зростання злочинності, споживчий менталітет громадян, низька трудова дисципліна та відповідальність працівників банків, недостатнє правове регулювання та низька кваліфікація працівників і керівництва.

Фізичні загрози проявляються у вигляді крадіжок, пограбувань, поломок та неефективної експлуатації обладнання. В результаті таких дій банкам завдаються прямі збитки, пов'язані з втратою майна та необхідністю додаткових витрат на відновлення. Основними причинами є неефективна кадрова політика, недостатня професійна підготовка фахівців та недоліки в безпеці установ.

Інтелектуальні загрози включають розголошення або неправомірне використання банківської інформації, дискредитацію банку на ринку, а також соціальні конфлікти. Це може призвести до фінансових втрат, погіршення іміджу і соціальної напруженості. Причинами є загострення конкуренції, неефективна кадрова політика, порушення принципу прозорості діяльності та слабкі інформаційні заходи [3].

Зовнішні загрози включають діяльність спецслужб іноземних держав, кримінальних структур, конкурентів, засобів масової інформації, представників

державних установ, приватних детективних фірм, колишніх співробітників банків, консультантів, партнерів, клієнтів та контролюючих органів.

Внутрішні загрози створюються самими працівниками банків, недосконалими технологіями та системами безпеки. Вони часто обумовлюються умовами, що спонукають до негативних або протиправних дій, безконтрольним використанням ресурсів та порушенням стандартів роботи.

У світлі того, що значна частина внутрішніх загроз банків реалізується з участю або за сприяння співробітників, вважати банківський персонал основним джерелом таких загроз є логічним. Виходячи з цього, джерела внутрішніх загроз можуть включати такі аспекти:

- непрофесійні дії співробітників; - недостатній рівень виховної та профілактичної роботи;
- недосконала система оплати праці та мотиваційних механізмів;
- недоліки кадрової політики та її невідповідність умовам банківської діяльності;
- психологічні та комунікаційні особливості персоналу;
- відсутність адекватної нормативної бази, яка б регулювала режим роботи та поведінку співробітників;
- низький рівень трудової та виробничої дисципліни, неефективну вимогливість керівництва.

Внутрішні загрози безпеці банків постійно існують і не залежать від їх ролі, місця або значення на ринку, а також від наявності зовнішніх загроз. Особливості реалізації цих загроз варіюються залежно від об'єктів, на які вони спрямовані. Основними об'єктами загроз для банку виступають персонал, фінансові ресурси, матеріальні активи та інформація.

Загрози для персоналу можуть викликати моральні або фізичні страждання, втрату особистих цінностей або економічну шкоду. Фінансові загрози можуть проявлятися у вигляді крадіжок фінансових ресурсів, шахрайства з грошовими коштами, підробки фінансових документів або банкнот, а також через недосконалі механізми банківських технологій.

Матеріальні активи банку можуть зазнати пошкоджень інфраструктури, виходу з ладу засобів комунікації і систем обслуговування, а також крадіжок обладнання і транспорту. Інформаційні загрози передбачають несанкціонований доступ до даних з обмеженим доступом, модифікацію чи знищення інформації, її неналежне розкриття.

Отже, аналіз загроз безпеці банківської установи свідчить про їхню багатогранність і постійну наявність, незалежно від масштабів діяльності чи ринкової позиції банку. Загрози поділяються на внутрішні та зовнішні й мають різноманітну природу: економічну, фізичну та інтелектуальну. Кожен із цих типів становить потенційну небезпеку для ефективного функціонування банку та збереження його активів, репутації, клієнтської довіри й стабільності.

Особливу увагу слід приділити внутрішнім загрозам, оскільки саме вони часто виникають внаслідок дій або бездіяльності персоналу банку. Недостатній рівень професіоналізму, неефективна кадрова політика, слабка система мотивації та відсутність належного контролю створюють умови для реалізації внутрішніх ризиків. У свою чергу, зовнішні загрози – такі як економічна нестабільність, правове регулювання, кіберзлочинність та конкуренція – також залишаються актуальними, ігнорування яких може призвести до серйозних наслідків [2].

Таким чином, забезпечення комплексної системи безпеки в банках має включати системний підхід до виявлення, оцінки та мінімізації як внутрішніх, так і зовнішніх загроз. Увага до людського фактору, вдосконалення банківських технологій, підвищення рівня професійної етики та організаційної культури, а також розвиток механізмів інформаційної безпеки є ключовими напрямками підвищення економічної безпеки банківської системи в цілому.

1.2. Методичні підходи до аналізу загроз

Аналіз загроз у банківській сфері – це ключовий елемент у системі управління ризиками, що дозволяє своєчасно виявити потенційні небезпеки,

оцінити рівень їх впливу та розробити ефективні стратегії реагування. Методичні підходи до аналізу загроз ґрунтуються на принципах системності, комплексності, динамічності та адаптивності до змін зовнішнього і внутрішнього середовища.

Метою аналізу загроз є виявлення, ідентифікація, оцінка та класифікація загроз, які можуть завдати шкоди банку, його активам, персоналу, репутації, фінансовій стабільності чи інформаційній системі. Аналіз загроз передбачає не лише фіксацію фактів, але й виявлення причинно-наслідкових зв'язків, а також оцінку ймовірності реалізації загроз.

Основними методичними підходами до аналізу загроз є:

1. Системний підхід. Системний підхід розглядає банк як складну динамічну систему, де кожен елемент (структурний підрозділ, технологія, працівник, інформаційна система) взаємодіє з іншими. Аналіз загроз у межах цього підходу охоплює усі підсистеми банку – фінансову, організаційну, інформаційну, технологічну, кадрову, що дозволяє виявити слабкі місця та потенційні вектори атак.

2. Класифікаційний підхід. Цей підхід передбачає класифікацію загроз за різними критеріями:

- За джерелом виникнення: внутрішні та зовнішні.
- За характером впливу: економічні, інформаційні, технологічні, соціальні, політичні, правові.
- За типом наслідків: прямі та непрямі збитки, репутаційні втрати, порушення діяльності.
- За ймовірністю реалізації та критичністю впливу: незначні, середні, критичні загрози.

Це дозволяє ранжувати загрози та визначати пріоритетність заходів реагування.

3. Ризик-орієнтований підхід. Цей підхід полягає у визначенні рівня ризику, який формується як добуток ймовірності реалізації загрози на очікуваний рівень збитків. Він дозволяє оцінити доцільність витрат на

превентивні заходи та сформувати карту ризиків банку. До його основних методів відносяться:

- Кількісна оцінка ризику (метод сценаріїв, статистичний аналіз, побудова моделей).
- Якісна оцінка ризику (експертне оцінювання, SWOT-аналіз, матриці ймовірності та впливу).

4. Інформаційно-аналітичний підхід. Він використовується для збору, обробки та аналізу великого обсягу інформації, що стосується потенційних загроз. Застосовується в комплексі з бізнес-розвідкою, моніторингом ЗМІ, відомостей про клієнтів, партнерів, конкурентів, а також внутрішньою статистикою інцидентів безпеки.

5. Процесно-орієнтований підхід. Аналіз загроз відбувається на рівні бізнес-процесів банку. Кожен процес розглядається як потенційний об'єкт атак або збоїв. Методологія включає:

- побудову процесних карт,
- виявлення критичних точок,
- моделювання впливу збоїв на результати діяльності.

Оскільки банки мають різний масштаб діяльності, організаційну структуру та ІТ-інфраструктуру, методики аналізу загроз повинні адаптуватися індивідуально. У великих банках використовується комплексний підхід, інтегрований у загальну систему корпоративного управління ризиками (ERM), тоді як у малих банках можуть домінувати простіші експертні чи шаблонні методи.

Отже, ефективний аналіз загроз банку базується на поєднанні системного, ризик-орієнтованого, інформаційно-аналітичного та процесного підходів. Лише цілісне та постійно оновлюване бачення потенційних небезпек дозволяє своєчасно запобігати втратам, підвищувати економічну безпеку установи та забезпечувати стабільність банківської системи в цілому.

РОЗДІЛ 2. ОРГАНІЗАЦІЙНО-ЕКОНОМІЧНА ХАРАКТЕРИСТИКА АТ «УКРСИББАНК»

2.1. Загальна характеристика діяльності АТ «УкрСиббанк»

АТ «УкрСиббанк» – один із найбільших та найстабільніших банків в Україні, що надає повний спектр банківських послуг фізичним особам, підприємцям та корпоративним клієнтам. Банк був заснований у 1990 році в місті Харкові, і за понад три десятиліття діяльності пройшов шлях від регіонального банку до одного з ключових гравців фінансового ринку України.

Важливим етапом розвитку банку стало входження до складу міжнародної банківської групи BNP Paribas у 2006 році. Наразі BNP Paribas володіє 60% акцій банку, що забезпечує УкрСиббанку доступ до передових банківських технологій, систем управління ризиками та міжнародного досвіду. Це дозволяє банку впроваджувати європейські стандарти обслуговування та управління.

УкрСиббанк має розгалужену інфраструктуру: центральний офіс розташований у Києві, а банківська мережа охоплює більшість регіонів України. Станом на 2024 рік, банк має понад 250 відділень по країні та обслуговує понад 2 мільйони клієнтів.

Організаційна структура банку включає корпоративний центр, регіональні дирекції, операційні підрозділи, підрозділи ризик-менеджменту, служби безпеки, ІТ-відділ, маркетинг, юридичну службу тощо. Така структура дозволяє ефективно координувати діяльність і швидко реагувати на зміни у зовнішньому середовищі.

АТ «УкрСиббанк» надає комплекс послуг, серед яких:

- Роздрібне банківське обслуговування: відкриття рахунків, депозити, кредити, іпотека, карткові продукти, онлайн-банкінг (My UKRSIB).
- Обслуговування малого та середнього бізнесу: кредитування, факторинг, розрахунково-касове обслуговування, лізинг, валютні операції.

- Корпоративне банківництво: фінансування великих підприємств, супровід зовнішньоекономічної діяльності, фінансовий консалтинг.
- Інвестиційна діяльність: операції з державними цінними паперами, валютні операції, обслуговування випусків корпоративних облігацій.
- Електронні сервіси: мобільний і веб-банкінг, цифрові гаманці, онлайн-оплата послуг.

У 2023 році АТ «УкрСиббанк» продемонстрував стійке фінансове зростання попри економічні виклики. Основні фінансові показники:

- Активи банку – понад 90 млрд грн.
- Кредитний портфель – близько 38 млрд грн.
- Обсяг депозитів – понад 70 млрд грн.
- Чистий прибуток за рік – понад 2 млрд грн.
- Норматив достатності капіталу – більше 20% (при нормативі НБУ – 10%).

Завдяки належному управлінню ризиками, високому рівню капіталізації та міжнародній підтримці, УкрСиббанк успішно витримує макроекономічні виклики та зберігає довіру клієнтів.

УкрСиббанк активно впроваджує стратегію діджиталізації та інновацій, орієнтуючись на покращення клієнтського досвіду, автоматизацію процесів, екологічну відповідальність та розвиток сталого банкінгу. Основними пріоритетними стратегіями банку є:

- Розвиток мобільного банкінгу та дистанційного обслуговування;
- Зміцнення позицій на ринку корпоративного кредитування;
- Інвестування в кібербезпеку та IT-інфраструктуру;
- Підвищення операційної ефективності;
- Підтримка ініціатив ESG (Environmental, Social, Governance).

Проведений аналіз показав, що банк має стійкі фінансово-економічні показники: рівень капіталізації, ліквідності та прибутковості знаходяться на прийнятному рівні, що забезпечує здатність до ефективного функціонування навіть в умовах економічної нестабільності. УкрСиббанк зберігає високі позиції

на ринку банківських послуг, орієнтуючись на розширення роздрібного та корпоративного сегментів, а також розвиток цифрових каналів обслуговування.

Разом із тим, банк функціонує в умовах численних викликів: зростання конкуренції, підвищення вимог з боку регулятора, нестабільна макроекономічна ситуація, а також загрози інформаційній безпеці. Аналіз внутрішніх та зовнішніх загроз показав, що найбільш критичними є ризики кіберзлочинності, нормативно-правові зміни, а також кадрові проблеми, пов'язані з адаптацією до нових технологій.

У відповідь на виклики УкрСиббанк активно розвиває внутрішні системи безпеки, посилює контроль за ризиками, впроваджує сучасні системи управління персоналом і діджитал-інструменти. Значна увага приділяється дотриманню стандартів корпоративного управління, прозорості діяльності та соціальній відповідальності.

Отже, діяльність АТ «УкрСиббанк» є прикладом ефективного функціонування банку в умовах складного середовища. Підвищення стійкості банку до загроз потребує подальшого удосконалення стратегії управління ризиками, розвитку кадрового потенціалу та адаптації до змін у зовнішньому середовищі.

2.2. Заходи мінімізації загроз і підвищення безпеки діяльності банку

У сучасних умовах діяльності банківська система України стикається з численними викликами, як внутрішнього, так і зовнішнього характеру. Відповідно до результатів проведеного аналізу загроз для АТ «УкрСиббанк», особливе значення набуває реалізація системних та превентивних заходів для забезпечення належного рівня економічної, фінансової, інформаційної та кадрової безпеки.

АТ «УкрСиббанк» активно застосовує інструменти внутрішнього контролю, що включають:

- чітке розмежування повноважень структурних підрозділів;
- регулярні перевірки діяльності банку через внутрішній аудит;
- впровадження систем моніторингу ключових показників ризику;
- оновлення регламентів відповідно до змін законодавства та вимог НБУ і міжнародних партнерів (зокрема BNP Paribas).

Ці заходи спрямовані на зменшення ймовірності виникнення загроз та оперативне виявлення порушень у діяльності банку.

У зв'язку зі зростанням кібератак у фінансовому секторі, банк впроваджує сучасні IT-рішення:

- багаторівневу аутентифікацію користувачів;
- системи виявлення загроз (IDS/IPS), шифрування та захист від DDoS-атак;
- резервне копіювання даних у хмарних середовищах;
- навчання співробітників з питань безпечного використання IT-ресурсів.

Ці дії підвищують стійкість банку до зовнішнього втручання та витоків інформації.

Одним з головних напрямків безпеки є управління людськими ресурсами. У цьому контексті УкрСиббанк вживає заходів щодо:

- професійного навчання та підвищення кваліфікації персоналу;
- удосконалення системи мотивації та оплати праці;
- ротації кадрів на ключових позиціях;
- запровадження етичного кодексу та моніторингу корпоративної культури.

Це дозволяє зменшити ризики внутрішнього шахрайства, некомпетентності та зловживань.

Для забезпечення стійкості фінансових потоків банк:

- проводить диверсифікацію кредитного портфеля;
- застосовує системи скорингу та оцінки кредитоспроможності;
- створює резерви на покриття можливих збитків;

– здійснює постійний аналіз ліквідності, валютних ризиків та ринкових впливів.

Ці дії сприяють зниженню фінансової вразливості в умовах нестабільності.

АТ «УкрСиббанк» розробив плани безперервності бізнесу (BCP) на випадок надзвичайних ситуацій:

- формуються кризові команди;
- відпрацьовуються сценарії реагування на кіберзагрози, економічні потрясіння, форс-мажорні події;
- забезпечено взаємодію з НБУ, правоохоронними та наглядовими органами.

Це дозволяє мінімізувати наслідки впливу несприятливих зовнішніх чинників.

Щодо репутаційної безпеки та зовнішніх комунікацій УкрСиббанк приділяє велику увагу своїй репутації та довірі клієнтів:

- запроваджено систему прозорих комунікацій у кризових ситуаціях;
- регулярно публікується звітність, що підтверджується міжнародними аудиторами;
- ведеться активна комунікація в соціальних мережах та ЗМІ.

Це сприяє формуванню позитивного іміджу банку та зниженню впливу репутаційних загроз.

Таким чином, комплексний підхід до управління безпекою дозволяє АТ «УкрСиббанк» не лише ефективно реагувати на загрози, а й створювати фундамент для довготривалої стабільної діяльності в умовах високої конкуренції та зовнішньої нестабільності.

ВИСНОВОК

У ході дослідження стану економічної безпеки банку за рахунок боротьби з внутрішніми та зовнішніми загрозами його діяльності було визначено, що ефективне управління економічною безпекою є ключовим фактором для забезпечення стабільності та довгострокового успіху банківської установи. Внутрішні загрози, такі як шахрайство, корупція та неналежне управління, можуть серйозно підірвати фінансову стабільність банку, тому запобігання та швидке реагування на такі ситуації є необхідними для збереження довіри клієнтів і партнерів. Зовнішні загрози, зокрема економічні кризи, коливання валютних курсів, зміни в законодавстві та регуляторні зміни, вимагають від банку постійного моніторингу макроекономічної ситуації та адаптації до нових умов.

Основними напрямками для зміцнення економічної безпеки банку є: удосконалення системи внутрішнього контролю, посилення заходів щодо запобігання шахрайству, розвиток інноваційних технологій безпеки, а також активне реагування на зміни в зовнішньому середовищі. Окрім того, для забезпечення комплексного підходу до управління безпекою необхідно інтегрувати стратегічне планування, системи моніторингу та управління ризиками, що дозволяють оперативно реагувати на можливі загрози.

Таким чином, ефективна боротьба з внутрішніми та зовнішніми загрозами є основою для підтримання стабільної роботи банку та мінімізації потенційних фінансових втрат, що, в свою чергу, забезпечує його економічну безпеку та конкурентоспроможність на ринку.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Гречка, М. М. Економічна безпека банку: теорія та практика. Київ : Академвидав, 2018. 320 с.
2. Дубовик, О. І. Управління економічною безпекою банку. Харків : ХНЕУ, 2017. 280 с.
3. Усік П.С., Буравченко К.О. Безпека банківських систем : навч. посіб. М-во освіти і науки України, Центральноукр. нац. техн. ун-т. Кропивницький : ЦНТУ, 2022. 194 с
4. Остроменко, В. О. Загрози економічній безпеці банку: внутрішні та зовнішні чинники / В. О. Остроменко // Економіка і фінанси. 2019. № 2. С. 45–58.
5. Державна служба фінансового моніторингу України. Основи управління фінансовими ризиками в банках України. Київ : Держфінмоніторинг, 2020. 192 с.
6. Бернштейн, Л. Внутрішні загрози економічній безпеці банку: діагностика та протидія. Київ : Бізнес-Інформ, 2016. 256 с.
7. Шевчук, Ю. В. Фінансовий моніторинг та безпека банківських установ / Ю. В. Шевчук // Економіка банківської діяльності. 2017. № 3. С. 87–102.
8. Власенко, Т. М. Моделі та методи управління економічною безпекою банку. Київ : Наукова думка, 2015. – 315 с.
9. Костюк, І. А. Проблеми безпеки в умовах глобалізації фінансових ринків / І. А. Костюк // Український економічний журнал. 2018. № 4. С. 33–47.
10. Іванова, І. В. Зовнішні загрози та їх вплив на стабільність банківської системи України / І. В. Іванова // Банківська справа. 2019. № 1. С. 55–67.
11. Михайлова, Н. М. Управління фінансовими ризиками в умовах нестабільної економіки / Н. М. Михайлова // Економіка України. 2018. № 1. С. 14–26.
12. Левченко, С. О. Економічна безпека банку в умовах сучасної економічної ситуації / С. О. Левченко // Бізнес та інновації. 2017. № 6. С. 75–90.

13. Ковальчук, Л. В. Методи захисту банків від внутрішніх загроз: досвід та перспективи / Л. В. Ковальчук // Наукові праці. 2020. № 5. С. 110–123.
14. Соловйова, О. Ю. Фінансові загрози та забезпечення безпеки банку. Київ : Інститут економіки, 2016. 210 с.
15. Таран, С. М. Аналіз впливу зовнішніх загроз на фінансову стабільність банку / С. М. Таран // Фінансові дослідження. 2021. № 7. С. 98–112.
16. Баранов, А. І. Банківська безпека та боротьба з економічними злочинами. Київ : Видавництво "Економіка", 2019. 275 с.
17. Про банк. Офіційний сайт АТ «УкрСиббанк». URL: <https://ukrsibbank.com/about-bank/>