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

Циклова комісія економіки, управління та адміністрування

Гутовський Даниїл Васильович
ПІБ здобувача

КУРСОВА РОБОТА

Комплексне забезпечення безпеки діяльності банку
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 _____ Д.В. Гутовський
підпис здобувача ПІБ здобувача

Підсумкова оцінка: **70** (балів)

Члени комісії з захисту:

_____ Н. О. Постольна
(підпис)

_____ О.М. Тимошенко
(підпис)

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

Циклова комісія економіки, управління та адміністрування

Гутовський Даниїл Васильович

ПІБ здобувача

ЗАВДАННЯ НА КУРСОВУ РОБОТУ

Навчальна дисципліна: Фінансово-економічна безпека організації

назва навчальної дисципліни

Тема роботи: Комплексне забезпечення безпеки діяльності банку

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 І розділу	31.03 – 19.04.2025
Написання розрахункової частини (ІІ 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

_____ Наталія ПОСТОЛЬНА
(підпис)

«06» березня 2025 р.

Завдання отримав

Здобувач

_____ Даниїл ГУТОВСЬКИЙ
(підпис) ПІБ здобувача

«06» березня 2025 р.

ЗМІСТ

ВСТУП

У сучасних умовах функціонування фінансової системи України стабільна діяльність банківських установ є ключовим фактором забезпечення економічної безпеки держави. Зростання ризиків, пов’язаних з кіберзлочинністю, шахрайськими операціями, внутрішніми порушеннями, нестабільною політичною ситуацією та військовими загрозами, обумовлює необхідність формування ефективної системи комплексного захисту банківських організацій. Особливої актуальності це питання набуває для системно важливих банків, таких як АТ КБ «ПриватБанк», на які припадає значна частка фінансових операцій в країні.

Актуальність дослідження полягає у потребі постійного вдосконалення системи безпеки банківських установ відповідно до новітніх викликів і умов, що динамічно змінюються. Комплексне забезпечення безпеки діяльності банку передбачає не лише технічні заходи, а й організаційні, кадрові, правові, інформаційні механізми, які повинні функціонувати як єдина цілісна система.

Мета курсової роботи полягає в дослідженні теоретичних основ і практичних підходів до організації системи комплексної безпеки банківської установи, аналізі чинної моделі безпеки в АТ КБ «ПриватБанк» та розробці рекомендацій щодо її вдосконалення.

Завдання дослідження:

- розглянути поняття та структуру економічної безпеки банку;
- класифікувати загрози банківській діяльності;
- проаналізувати систему безпеки в АТ КБ «ПриватБанк»;
- виявити основні ризики та недоліки у сфері безпеки;
- запропонувати напрями підвищення ефективності безпекових заходів.

Об’єктом дослідження є процес забезпечення економічної безпеки банківської установи.

Предметом дослідження виступають методи, механізми та інструменти комплексного забезпечення безпеки банку.

Практичне значення роботи полягає в обґрунтуванні та рекомендаціях, які можуть бути використані банківськими установами для зміцнення власної безпеки, мінімізації ризиків та підвищення довіри клієнтів.

РОЗДІЛ 1. ТЕОРЕТИЧНІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ БАНКІВСЬКОЇ ДІЯЛЬНОСТІ

1.1. Поняття та сутність економічної безпеки банку +Класифікація загроз банківській безпеці

Економічна безпека банку – це стан захищеності банківської установи від внутрішніх і зовнішніх загроз, який забезпечує її стабільне функціонування, фінансову стійкість, конкурентоспроможність та здатність до розвитку в умовах постійних змін ринкового середовища.

Це поняття охоплює низку аспектів:

Фінансова стійкість – здатність банку зберігати платоспроможність, достатність капіталу та прибутковість у складних умовах;

Операційна безпека – захист від порушень у внутрішніх процесах, включно з шахрайством, помилками персоналу чи технічними збоями;

Інформаційна безпека – забезпечення цілісності, доступності та конфіденційності даних;

Юридична безпека – дотримання законодавства, недопущення порушень, що можуть спричинити фінансові чи репутаційні втрати;

Кадрова безпека – зменшення ризику ненадійності, лояльності та професійної некомпетентності персоналу;

Стратегічна безпека – здатність адаптуватися до змін макроекономічного середовища, зокрема політичної, воєнної, регуляторної ситуації.

Основною метою економічної безпеки є гарантування стабільної діяльності банку в умовах ринкових коливань, загроз та викликів. Особливо актуальним це питання є для системно важливих установ, таких як АТ КБ «ПриватБанк», який обслуговує мільйони клієнтів, включаючи значну частину держсектору.

Класифікація загроз банківській безпеці – це систематизація потенційних негативних факторів, які можуть вплинути на стабільність, цілісність,

репутацію та прибутковість банківської установи. Така класифікація дозволяє ефективніше здійснювати заходи з протидії ризикам.

Класифікація загроз банківській безпеці є необхідною умовою ефективного управління ризиками в банківській установі. Вона дозволяє систематизувати різноманітні джерела небезпеки – як зовнішні, так і внутрішні – за характером їх впливу, масштабом наслідків та імовірністю виникнення. Такий підхід забезпечує глибше розуміння потенційних загроз, дозволяє встановити пріоритети в побудові системи захисту та розробити відповідні превентивні й реактивні заходи. Крім того, обґрунтована класифікація є основою для виконання нормативних вимог регуляторів та стандартів інформаційної і фінансової безпеки. У результаті банк отримує можливість не лише ефективно захищатися від ризиків, а й підвищувати довіру клієнтів та інвесторів, зберігаючи свою стабільність та репутацію. А обґрунтування класифікації базується на:

– Системному підході – дозволяє розуміти, звідки можуть виникати загрози, та впроваджувати диференційовані засоби захисту.

– Ефективному управлінні ризиками – кожен тип загрози потребує свого інструменту реагування.

– Фінансовому плануванні – розподіл ресурсів на безпеку залежить від того, які загрози є пріоритетними.

– Правовому регулюванні – дозволяє дотримуватись законів і стандартів безпеки.

– Попередженні системних криз – виявлення слабких місць до того, як вони призведуть до катастрофічних наслідків.

Визначимо основні класифікації загроз банківській безпеці:

1. За джерелом походження:

– Внутрішні загрози. Походять із середини банку (співробітники, внутрішні процеси). До них ми можемо віднести зловживання службовим становищем, несанкціонований доступ до інформації, помилки або халатність персоналу, внутрішнє шахрайство.

– Зовнішні загрози. Походять ззовні установи (клієнти, конкуренти, злочинці). До них відносяться: хакерські атаки, шахрайські дії клієнтів, тиск або втручання з боку держави, кримінальних структур, Політична або економічна нестабільність.

2. За характером впливу:

– Фінансові загрози. Збитки через шахрайство, крадіжки, ризик дефолту контрагентів.

– Інформаційні загрози. Несанкціонований доступ, витік або знищення даних.

– Технічні загрози. Відмова систем, поломка обладнання, кібератаки.

– Правові загрози. Порушення законодавства, судові позови, штрафи.

– Репутаційні загрози. Негативна публічність, зниження довіри клієнтів.

3. За формою прояву:

– Явні/відкриті – легко виявляються (наприклад, фізичне пограбування, кібератака).

– Приховані/латентні – можуть діяти довго та непомітно (внутрішні змови, повільне виведення коштів).

4. За ступенем впливу:

– Критичні – здатні призвести до повної втрати платоспроможності (наприклад, крах IT-інфраструктури або масовий витік коштів).

– Середні – викликають значні, але відновлювані збитки.

– Малі – мають обмежений локальний вплив.

Таким чином, загрози економічній безпеці банку класифікуються за джерелом походження (внутрішні та зовнішні), характером впливу (економічні, політичні, технологічні тощо) та тривалістю дії (разові, тривалі, стратегічні).

Підтримка економічної безпеки вимагає системного підходу, де управління ризиками, відповідність нормативним вимогам, впровадження сучасних технологій і розвиток корпоративної культури – діють комплексно.

1.2. Система управління безпекою банку: структура та функції та принципи її побудови

Сучасний банківський сектор функціонує в умовах динамічного фінансового середовища, стрімкої цифровізації та посилення кіберзагроз. У зв’язку з цим особливої актуальності набуває побудова ефективної системи управління безпекою банку, яка забезпечує захист його активів, інформації, інфраструктури, персоналу та клієнтів. Така система є інтегральною частиною загального управління банківською установою й охоплює комплекс заходів правового, технічного, організаційного та кадрового характеру.

Система управління безпекою банку складається з кількох взаємопов’язаних елементів, кожен із яких виконує специфічні функції. Організаційна складова охоплює роботу спеціалізованих структур, таких як служба безпеки, відділ інформаційних технологій, підрозділи комплаєнс-контролю, внутрішнього аудиту та управління ризиками. Кожен із них відповідає за конкретні напрями забезпечення безпеки: від виявлення шахрайства й аналізу загроз до розробки заходів протидії та контролю їх ефективності.

Інформаційно-технічна складова системи безпеки включає в себе впровадження й обслуговування програмно-апаратних засобів захисту – систем контролю доступу, фаєрволів, антивірусного програмного забезпечення, засобів шифрування інформації, систем резервного копіювання та моніторингу інформаційних ресурсів. Такі заходи дозволяють ефективно реагувати на інциденти інформаційної безпеки, попереджати втрати даних і збої в роботі банківських сервісів.

Правова складова системи базується на дотриманні чинного законодавства України, вимог Національного банку України, а також міжнародних стандартів (зокрема ISO/IEC 27001, Basel III). Вона передбачає наявність внутрішніх нормативно-правових актів, що регламентують порядок реалізації заходів безпеки, відповідальність працівників, правила обробки конфіденційної інформації тощо.

Не менш важливою є кадрова складова, яка передбачає відбір надійного персоналу, його навчання та інструктаж, формування культури безпеки в колективі. Працівники повинні усвідомлювати потенційні загрози, бути обізнаними з політиками захисту та чітко дотримуватись регламентів безпечної поведінки в робочому середовищі.

Функціонально система управління безпекою виконує низку важливих завдань: виявлення та аналіз загроз, оцінка вразливостей, розробка захисних заходів, організація превентивного захисту, оперативне реагування на інциденти, постійний моніторинг і вдосконалення політик безпеки. Усі ці функції реалізуються як в автоматизованому, так і в ручному режимах із залученням відповідних фахівців.

Побудова ефективної системи безпеки банку має ґрунтуватися на низці ключових принципів:

– системність, яка передбачає охоплення всіх аспектів діяльності банку;

– комплексність, тобто поєднання різних засобів і методів захисту;

– безперервність функціонування системи незалежно від зовнішніх обставин;

– гнучкість і здатність до адаптації до нових умов та загроз;

– превентивність, спрямована на попередження ризиків;

– конфіденційність даних клієнтів і внутрішньої інформації;

– відповідальність усіх співробітників за дотримання політик безпеки.

Таким чином, система управління безпекою банку виступає як цілісна інфраструктура, яка забезпечує стабільність, довіру з боку клієнтів та партнерів, відповідність нормативним вимогам і стійкість до зовнішніх та внутрішніх викликів. Її ефективність визначається не лише технічними рішеннями, а й якістю управління, професійністю персоналу та наявністю стратегії розвитку безпекової політики установи.

1.3. Система управління безпекою банку: структура та функції та принципи її побудови

Ефективна система управління безпекою банку є важливою передумовою стабільного функціонування фінансової установи в умовах зростаючих загроз економічного, технічного та інформаційного характеру. Забезпечення банківської безпеки передбачає не лише протидію шахрайству чи технічним збоям, а й створення цілісної інфраструктури захисту, яка охоплює всі сфери банківської діяльності.

Структура системи управління безпекою банку зазвичай має багаторівневий характер і складається з декількох основних компонентів. Перш за все, це організаційна структура, яка включає спеціалізовані підрозділи, відповідальні за безпеку: службу безпеки, відділ інформаційних технологій, підрозділ комплаєнс-контролю, внутрішній аудит та управління ризиками. Вони взаємодіють між собою з метою виявлення загроз, аналізу ризиків, формування політик захисту і контролю за їх дотриманням.

До технічної складової системи безпеки належать засоби захисту інформаційної інфраструктури банку: мережеві екрани, системи виявлення атак, антивірусне програмне забезпечення, шифрування даних, контроль доступу до інформаційних систем і серверів, резервне копіювання та хмарні сервіси. Їхнє функціонування забезпечується фахівцями IT-відділу та спеціалістами з кібербезпеки.

Правова складова управління безпекою включає розробку та впровадження внутрішньобанківських нормативних документів – регламентів, положень, інструкцій, а також дотримання вимог чинного законодавства України, нормативно-правових актів Національного банку України, міжнародних стандартів (зокрема, ISO/IEC 27001, Basel III). Важливим аспектом є юридична відповідальність працівників за порушення політик безпеки.

Кадровий аспект полягає в залученні кваліфікованого персоналу, проведенні регулярних навчань, інструктажів з питань безпеки, формуванні

етичної культури, виявленні та усуненні факторів внутрішніх загроз (наприклад, несанкціонованого доступу чи витоку інформації через недбалість співробітників).

Функціонально система управління безпекою виконує низку завдань, що охоплюють повний цикл забезпечення безпеки:

1. ідентифікацію загроз і вразливостей;
2. оцінку ризиків та наслідків їх реалізації;
3. розробку політик захисту та механізмів реагування;
4. впровадження технічних і організаційних заходів безпеки;
5. постійний моніторинг стану безпеки;
6. розслідування інцидентів та підвищення ефективності реагування;
7. планування безперервності бізнесу в разі надзвичайних ситуацій.

Для ефективної побудови системи безпеки слід дотримуватися низки основоположних принципів:

1. Системність – охоплення усіх аспектів функціонування банку, включно з технічними, юридичними та людськими факторами.

2. Комплексність – взаємодія всіх складових системи в єдиній логічній структурі.

3. Превентивність – акцент на запобіганні загрозам, а не лише на реагуванні після їх реалізації.

4. Гнучкість – адаптація системи до нових ризиків, змін законодавства, розвитку технологій.

5. Безперервність – функціонування системи безпеки у будь-яких обставинах, включно з кризовими ситуаціями.

6. Конфіденційність – збереження комерційної та особистої інформації в режимі обмеженого доступу.

7. Відповідальність – розподіл обов’язків і контроль за виконанням функцій кожного працівника.

Застосування цих принципів забезпечує не лише технічну захищеність банку, а й зміцнює його ділову репутацію, підвищує рівень довіри клієнтів і партнерів та сприяє дотриманню нормативних вимог.

Отже, система управління безпекою банку є невід’ємною частиною загальної стратегії діяльності установи. Її структура, функції та принципи формують основу для стабільного, безпечного та конкурентоспроможного функціонування банківської організації в умовах ринкової економіки та постійних викликів.

РОЗДІЛ 2. АНАЛІЗ СИСТЕМИ БЕЗПЕКИ В АТ КБ «ПРИВАТБАНК»

2.1. Загальна характеристика діяльності банку

Акціонерне товариство комерційний банк «ПриватБанк» є однією з найважливіших фінансово-кредитних установ України, що відіграє провідну роль у забезпеченні банківського обслуговування населення, підприємств і державного сектору. Заснований у 1992 році, банк пройшов тривалий етап розвитку від регіональної фінансової структури до всеукраїнського системно важливого банку з державною формою власності. З 2016 року ПриватБанк повністю належить державі в особі Міністерства фінансів України, що зумовило підвищення суспільної відповідальності банку та посилення вимог до його фінансової стабільності й безпеки.

ПриватБанк має найбільшу в Україні мережу відділень, банкоматів і терміналів самообслуговування, що охоплює всі регіони країни. Завдяки високому рівню діджиталізації банківських процесів, установа стала одним із лідерів за впровадженням інновацій у сфері обслуговування клієнтів. Зокрема, широкого визнання набули такі цифрові сервіси, як мобільний застосунок «Приват24», система електронної ідентифікації BankID, платіжні технології Apple Pay та Google Pay, а також сервіс миттєвих онлайн-кредитів і відкриття рахунків.

Основними напрямами діяльності банку є:

– обслуговування фізичних осіб (депозити, поточні рахунки, карткові продукти, споживче кредитування);

– обслуговування малого, середнього та великого бізнесу (розрахунково-касове обслуговування, кредитування, лізинг, еквайринг, зарплатні проєкти);

– обслуговування державного сектору (виплати соціальних допомог, обслуговування рахунків бюджетних установ тощо);

– інвестиційна діяльність, валютні операції, операції на фондовому ринку.

На кінець останнього звітного періоду ПриватБанк утримує провідні позиції за ключовими фінансовими показниками: обсягами активів, депозитною базою, обсягами кредитного портфеля та кількістю клієнтів. Зокрема, банк обслуговує понад 18 мільйонів фізичних осіб та близько 1 мільйона юридичних осіб. За результатами аудиту, проведеного за міжнародними стандартами, ПриватБанк демонструє позитивну динаміку фінансової звітності, попри складну макроекономічну ситуацію та ризики, пов’язані з воєнним станом.

Окрему увагу в діяльності банку приділено питанням безпеки. У зв’язку з тим, що ПриватБанк є найбільшим роздрібним банком країни та основним провайдером цифрових банківських послуг, питання кібербезпеки, захисту інформації та запобігання шахрайству є ключовими. Банк впроваджує сучасні системи багаторівневої аутентифікації, моніторингу транзакцій, машинного навчання для виявлення аномалій, а також бере участь у державних і міжнародних програмах з обміну інформацією про кіберзагрози.

Таким чином, ПриватБанк є не лише найбільшим банком країни, а й одним із ключових суб’єктів національної фінансової системи, що відіграє значну роль у підтримці економічної стабільності, розвитку цифрової трансформації та впровадженні сучасних стандартів банківської безпеки. Його діяльність становить особливий інтерес для дослідження в контексті організації банківської безпеки, що є актуальною темою даної курсової роботи.

2.2. Аналіз внутрішніх загроз і ризиків

Забезпечення банківської безпеки передбачає врахування широкого спектру загроз, серед яких важливе місце займають внутрішні загрози. На відміну від зовнішніх, внутрішні загрози виникають у межах самої банківської установи та пов’язані з діяльністю її працівників, внутрішніми процесами, помилками управління або зловживаннями службовим становищем. Їх особливість полягає в тому, що вони часто є менш помітними, але водночас можуть спричинити значні матеріальні та репутаційні збитки.

До основних внутрішніх загроз банківській безпеці можна віднести:

1. Шахрайські дії персоналу – несанкціоноване використання ресурсів банку, підробка документів, розголошення конфіденційної інформації, змова з третіми особами.

2. Помилки персоналу внаслідок недостатньої кваліфікації або неуважності – можуть призводити до витоку інформації, помилкових транзакцій, втрати даних.

3. Недостатній контроль за внутрішніми процесами – створює можливості для порушення процедур, що регламентують доступ до інформаційних систем, грошових потоків, клієнтських даних.

4. Низький рівень корпоративної культури та мотивації – сприяє зниженню відповідальності персоналу, байдужості до порушень правил безпеки.

5. Використання слабких паролів, нехтування політиками інформаційної безпеки – збільшує ризик несанкціонованого доступу до критичних систем.

6. Конфлікти інтересів – виникають, коли працівники ставлять власні інтереси вище за інтереси банку або діють в інтересах третіх осіб.

7. Надмірна централізація функцій або непрозора система делегування повноважень – може ускладнити виявлення шахрайських схем.

Аналіз внутрішніх загроз здійснюється шляхом оцінки внутрішніх ризиків, які визначаються як імовірність того, що реалізація певної загрози призведе до небажаних наслідків для банку. Внутрішні ризики класифікують за такими основними ознаками:

1. Операційний ризик – ризик втрат у результаті недоліків або збоїв у внутрішніх процесах, діях персоналу, технічних системах.

2. Кадровий ризик – пов’язаний з неналежним добором, навчанням або поведінкою працівників.

3. Інформаційний ризик – ризик витоку, спотворення або знищення конфіденційної інформації через дії співробітників.

4. Комплаєнс-ризик – ризик порушення внутрішніх політик, інструкцій або зовнішніх регуляторних вимог.

Для ефективного виявлення й оцінки внутрішніх загроз банки використовують методи аудиту, аналітики ризиків, моніторингу поведінкових патернів персоналу, застосування систем управління інцидентами, а також аналізу журналів доступу до інформаційних систем.

У контексті забезпечення банківської безпеки особливої уваги потребує розробка внутрішніх політик контролю за діяльністю персоналу. Це включає:

- впровадження систем обмеження та розподілу доступу до ресурсів;
- регламентацію дій у критичних системах;
- регулярні перевірки внутрішніх процесів;
- обов’язкове навчання працівників з питань безпеки;
- створення умов для анонімного повідомлення про порушення (впровадження системи «whistleblowing»).

Таким чином, внутрішні загрози становлять серйозний виклик для банківської безпеки, оскільки часто є складними для виявлення та контролю. Їх системний аналіз, своєчасна ідентифікація ризиків, розробка механізмів профілактики та реагування є ключовими умовами для запобігання потенційним втратам і підвищення стійкості банку до внутрішніх викликів.

2.3. Дослідження інформаційної, кадрової та фінансової безпеки Оцінка чинної системи безпеки банку

У системі банківської безпеки особливу роль відіграють три ключові складові – інформаційна, кадрова та фінансова безпека, які є взаємопов’язаними та впливають на загальну стійкість банківської установи. Їхнє дослідження дає змогу оцінити реальний стан захищеності банку та визначити вразливі місця в організаційній структурі, управлінні персоналом, фінансових операціях і технологічній інфраструктурі.

Інформаційна безпека є критичним компонентом діяльності сучасного банку, оскільки більшість операцій здійснюється в цифровому форматі. Її мета – забезпечення конфіденційності, цілісності та доступності інформації. Основними загрозами інформаційній безпеці є кібератаки, віруси, фішинг, внутрішнє шахрайство, витоки даних через недотримання політик доступу.

У банку впроваджуються наступні заходи інформаційної безпеки:

- багаторівнева система автентифікації користувачів;
- шифрування передавання та зберігання даних;
- системи виявлення вторгнень (IDS/IPS);
- резервне копіювання та планування відновлення після інцидентів;
- аудит дій користувачів та контроль доступу.

Особливу увагу приділено захисту мобільних сервісів (зокрема, «Приват24») та карткових розрахунків. Для цього банк застосовує системи моніторингу транзакцій у режимі реального часу та технології поведінкової аналітики.

Кадрова безпека охоплює заходи, спрямовані на запобігання загрозам з боку персоналу, які можуть виникати внаслідок навмисних чи випадкових дій співробітників. Вона включає:

- ретельний добір персоналу з перевіркою ділової репутації;
- підписання договорів про нерозголошення конфіденційної інформації (NDA);
- регулярне навчання з питань інформаційної та економічної безпеки;
- внутрішній контроль за дотриманням посадових інструкцій;
- моніторинг потенційних конфліктів інтересів.

Загрозами кадровій безпеці є шахрайство з боку працівників, передача конфіденційної інформації третім особам, халатність, саботаж, підкуп, зловживання службовим становищем. Для зменшення цих ризиків використовуються процедури ротації кадрів, обмеження повноважень та принцип «розділених обов’язків», що мінімізує концентрацію ризику в одних руках.

Фінансова безпека забезпечує стабільність банку як суб’єкта фінансової системи, його здатність своєчасно виконувати зобов’язання перед клієнтами, партнерами та державними органами. Основними загрозами фінансовій безпеці є:

- кредитні ризики (неплатоспроможність позичальників);
- ліквідні ризики (нестача коштів для покриття короткострокових зобов’язань);
- ринкові ризики (коливання валютних курсів, відсоткових ставок);
- шахрайські фінансові операції (відмивання коштів, фальсифікація документів).

З метою контролю банк впроваджує системи оцінки та управління фінансовими ризиками, застосовує stress-testing сценарії, використовує стандарти Базельського комітету, проводить регулярний внутрішній та зовнішній аудит. Також запроваджено механізми KYC (знай свого клієнта) та AML (протидія легалізації доходів, отриманих злочинним шляхом).

Особлива увага приділяється забезпеченню достатнього рівня капіталізації та ліквідності, контролю динаміки активів і зобов’язань, диверсифікації кредитного портфеля та ефективному управлінню грошовими потоками.

Таким чином, інформаційна, кадрова та фінансова безпека формують критичну триєдину основу захищеності банківської установи. Їх належний стан є запорукою надійної роботи банку, захисту інтересів клієнтів, інвесторів і держави. Недооцінка хоча б одного з цих компонентів може призвести до комплексних кризових явищ, тому їх системне вивчення та вдосконалення має стратегічне значення для банківського сектору.

Оцінка чинної системи безпеки банківської установи є ключовим етапом аналізу її здатності протистояти внутрішнім і зовнішнім загрозам. Вона дозволяє виявити слабкі місця, визначити рівень готовності до кризових ситуацій, а також оцінити ефективність заходів, які реалізуються у сфері інформаційної, фізичної, фінансової та кадрової безпеки. Як об'єкт оцінки

розглянемо систему безпеки ПриватБанку як однієї з найбільш цифровізованих та масштабних банківських структур України.

У ПриватБанку функціонує розгалужена система служб безпеки, до складу якої входять:

- департамент безпеки;
- підрозділ інформаційної безпеки;
- служба внутрішнього контролю;
- підрозділи комплаєнс-контролю;
- підрозділи захисту персоналу та фізичної охорони;
- фінансовий моніторинг (AML-команда).

Функції чітко розмежовані між структурними підрозділами, існує вертикаль підзвітності, а також діє система взаємного контролю та координації дій між службами.

Банк активно впроваджує сучасні технології захисту даних, зокрема:

- багатофакторну аутентифікацію клієнтів і співробітників;
- шифрування каналів зв'язку;
- системи моніторингу транзакцій у режимі реального часу;
- поведінкову аналітику для виявлення аномальних дій;
- регулярне оновлення програмного забезпечення та випробування на проникнення.

Оцінка свідчить, що ПриватБанк має високий рівень інформаційної безпеки, адаптований до вимог національних і міжнародних стандартів, зокрема ISO/IEC 27001.

Банк впровадив політику комплексного управління персоналом у контексті безпеки:

- здійснюється перевірка кандидатів під час прийому на роботу;
- проводяться регулярні навчання та тестування з питань безпеки;
- є система внутрішнього аудиту та контролю за порушеннями службових інструкцій;

- діють програми етичного кодексу та інформування про конфлікт інтересів.

Однак у звітах про інциденти відзначено окремі випадки порушень з боку персоналу, що свідчить про потребу в посиленні превентивних заходів і вдосконаленні мотиваційних механізмів доброчесності.

ПриватБанк утримує високий рівень капіталізації та ліквідності. Здійснюється регулярне управління кредитним ризиком, проводиться фінансовий моніторинг згідно з вимогами НБУ та FATF. Діє система виявлення підозрілих операцій, підкріплена алгоритмами машинного навчання.

Також банк впроваджує stress-testing сценарії для оцінки стійкості до криз. Водночас актуальним залишається ризик втрат внаслідок застарілих кредитних портфелів, що потребує додаткових резервів і контролю реструктуризацій.

Банк оснащений системами охоронної сигналізації, відеоспостереження, фізичного контролю доступу до офісів і серверних приміщень. Відділення забезпечено сучасними технічними засобами безпеки. Разом з тим, враховуючи воєнний стан, необхідна постійна адаптація планів безперервної роботи (BCP) та евакуаційних заходів для персоналу та інфраструктури.

Чинна система безпеки ПриватБанку загалом демонструє високий рівень зрілості та ефективності, що відповідає статусу системно важливого банку. Основні переваги включають інтегровану структуру управління безпекою, сучасні технологічні рішення, наявність політик управління ризиками та чіткий регламент дій у кризових ситуаціях.

Водночас визначені потенційні зони вдосконалення:

- підвищення рівня превенції внутрішніх порушень серед персоналу;
- удосконалення підготовки до нестандартних або воєнних загроз;
- подальший розвиток аналітики інцидентів і прогнозування ризиків на основі big data.

Таким чином, ПриватБанк має ефективну, але динамічну систему безпеки, яка вимагає постійного розвитку в умовах змінного середовища та високих загроз кіберпростору.

РОЗДІЛ 3. УДОСКОНАЛЕННЯ КОМПЛЕКСНОЇ СИСТЕМИ БЕЗПЕКИ БАНКУ

3.1. Напрями оптимізації безпекової політики та впровадження сучасних технологій захисту банку

У сучасних умовах нестабільного фінансового середовища, активної цифровізації та зростання кіберзагроз перед банківською системою України, зокрема – перед системно важливими банками як АТ КБ «ПриватБанк», постає завдання удосконалення безпекової політики з урахуванням нових викликів. Ефективна безпекова стратегія повинна поєднувати системну організацію захисту інформаційних, фінансових, кадрових та юридичних компонентів.

Таблиця 3.1. - Оцінка ефективності напрямів безпеки банку

Напрям	Очікуваний ефект (1-5)
Інтеграція безпеки у стратегічне управління	4
Кадрова політика з елементами превентивного контролю	3
Юридичний комплаєнс і регуляторна відповідність	4
Інформаційно-технологічні рішення	5
Технології кібербезпеки	5
Аналітичні технології управління ризиками	4

Впровадження сучасних технологій захисту забезпечення безпеки банку:

1. Інформаційно-технологічні рішення
2. SIEM-системи для моніторингу безпеки в реальному часі;
3. Системи DLP для захисту конфіденційної інформації;
4. Платформи на базі штучного інтелекту для виявлення шахрайських операцій;
5. Мобільна автентифікація з використанням біометрії та криптографії.

Детальне зображення впливу інноваційних технологій на зниження ризиків банку наведено на рис. 3.1.

Очікуваний ефект від впровадження інноваційних технологій припускає підвищення рівня стійкості до зовнішніх атак і внутрішніх інцидентів, зниження фінансових втрат і штрафів через недотримання комплаєнсу,

поліпшення репутаційного рейтингу банку та формування довіри клієнтів до банківських сервісів, оптимізацію витрат на реагування, завдяки запровадженню превентивного контролю.

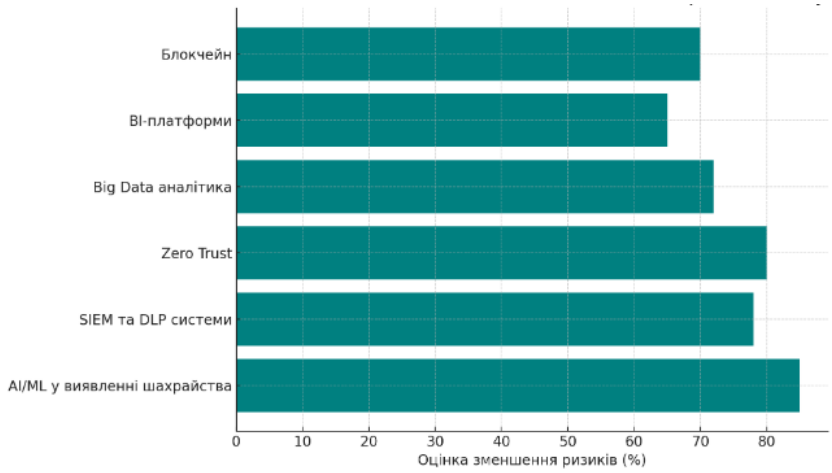

Рисунок 3.1. – Вплив інноваційних технологій на зниження ризиків банку

Графік демонструє, як інноваційні технології (AI/ML, SIEM, Big Data тощо) знижують ризики діяльності банку, досягаючи до 85% ефективності.

Отже, у сучасних умовах динамічного розвитку загроз у фінансовому секторі, оптимізація безпекової політики банку є ключовим чинником забезпечення його стабільного функціонування та конкурентоспроможності. Впровадження новітніх технологій, таких як системи кіберзахисту, аналітичні платформи моніторингу ризиків та автоматизовані системи контролю доступу, довели свою ефективність у зниженні рівня ризиків та втрат.

Оцінка ефективності впроваджених заходів засвідчила, що саме комплексний підхід, який охоплює технологічні, організаційні та кадрові аспекти, дає змогу досягати максимального рівня безпеки. Зокрема, стратегічна інтеграція безпеки у загальну політику банку та формування культури безпеки серед персоналу виступають як основа сталого захисту від загроз.

Таким чином, застосування запропонованих напрямів оптимізації сприяє посиленню економічної безпеки банку, мінімізації потенційних ризиків і підвищенню довіри клієнтів та партнерів.

3.2. Посилення кадрової та інформаційної безпеки, формування культури безпеки в банківському середовищі

У сучасному банківському середовищі, де основним активом виступає інформація, а персонал – ключова ланка у забезпеченні її захисту, питання кадрової та інформаційної безпеки набувають стратегічного значення. Несанкціонований доступ, витоки даних, внутрішнє шахрайство та низька мотивація працівників можуть завдати банку суттєвих репутаційних та фінансових збитків. Тому посилення цих напрямів безпеки є обов’язковим елементом економічної стабільності банківської установи.

Основними ризиками в кадровій сфері є: доступ до конфіденційної інформації некваліфікованих або ненадійних осіб; конфлікт інтересів; незадоволеність умовами праці, що може призводити до порушень.

Для підвищення кадрової безпеки доцільно впровадити такі заходи:

1. Комплексна система перевірки персоналу на етапі прийому (бекграунд-чек, психометричне тестування);

2. регулярні тренінги з етичної поведінки та інформаційної безпеки;

3. система ротації працівників у критичних напрямках діяльності;

4. політика "розмежування повноважень" – мінімізація надмірних доступів;

5. прозора система мотивації та преміювання, що стимулює лояльність і професіоналізм.

Інформаційні активи банку включають дані клієнтів, внутрішні фінансові документи, алгоритми роботи IT-систем. Основними загрозами є зовнішні кібератаки, фішингові атаки, витоки даних через незахищені канали та людський фактор.

Для зміцнення інформаційної безпеки рекомендовано: впровадження сучасних систем захисту – DLP, SIEM, двофакторна автентифікація, шифрування конфіденційної інформації, обмеження доступу до систем за принципом мінімальної необхідності, регулярне оновлення політик безпеки відповідно до змін нормативного поля, інцидент-менеджмент – створення

окремої команди реагування на кіберзагрози та внутрішнє інформування та навчання персоналу щодо загроз кібербезпеці.

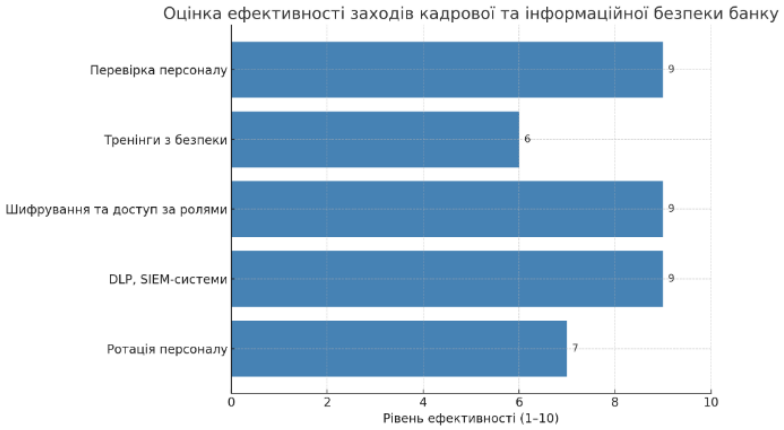

Рисунок 3.2. – Оцінка ефективності заходів кадрової та інформаційної безпеки банку

На основі оцінки ефективності основних заходів з кадрової та інформаційної безпеки банку видно, що найбільш результативними є впровадження DLP та SIEM-систем, а також обмеження доступу до інформації через шифрування та рольове управління. Ці технології дозволяють істотно зменшити ризики витоку конфіденційної інформації, несанкціонованого доступу та внутрішніх загроз.

Поряд із цим, значний ефект демонструє перевірка персоналу на етапі відбору та систематичне оновлення політик безпеки через навчальні програми. Ротація кадрів також допомагає зменшити можливості зловживань, однак її ефективність дещо нижча, оскільки вона не усуває причини ризиків, а лише мінімізує наслідки.

Таблиця 2.5 - Порівняльна ефективність заходів кадрової та інформаційної безпеки

Захід	Сфера застосування	Очікуваний результат	Рівень ефективності
Перевірка персоналу	Кадрова	Зменшення випадків шахрайства	Високий

Захід	Сфера застосування	Очікуваний результат	Рівень ефективності
Тренінги з безпеки	Кадрова/Інформаційна	Підвищення обізнаності, зменшення помилок	Середній
Шифрування та доступ за ролями	Інформаційна	Захист даних від витоку	Високий
DLP, SIEM-системи	Інформаційна	Виявлення та реагування на загрози	Високий
Ротація персоналу	Кадрова	Унеможливлення змови або зловживань	Середній

Посилення кадрової та інформаційної безпеки є взаємопов’язаними елементами загальної системи безпеки банку. Комплексна реалізація організаційних, технічних та освітніх заходів дозволяє не лише знизити рівень ризиків, а й сформувати відповідальне безпечне середовище, що забезпечує довіру клієнтів та партнерів. У поєднанні з іншими напрямами безпеки ці складові створюють основу для стійкого функціонування банківської установи в умовах високої турбулентності зовнішнього середовища.

Загалом, посилення кадрової та інформаційної безпеки вимагає комплексного підходу з використанням сучасних технологій захисту, управлінських рішень та формування корпоративної культури безпеки. Реалізація таких заходів не лише підвищує захищеність банківської установи, а й сприяє зростанню довіри клієнтів та стабільності фінансових операцій.

Формування культури безпеки є критично важливим елементом системи економічної безпеки банківської установи, оскільки саме людський фактор залишається однією з найвразливіших ланок у забезпеченні стійкості до загроз. Культура безпеки – це сукупність цінностей, переконань, норм поведінки й практик, які спрямовані на підвищення рівня відповідального ставлення співробітників до збереження інформації, фінансів, технологій та репутації банку.

До основних елементів культури безпеки відносяться:

Політика безпеки: чітко сформульовані правила, інструкції, кодекси етики, що регламентують поведінку працівників у сфері інформаційної, кадрової, фізичної та фінансової безпеки.

Навчання та підвищення обізнаності: регулярне проведення тренінгів, симуляцій кіберзагроз, семінарів з етики, ознайомлення з новими методами атак.

Приклади з боку керівництва: демонстрація дотримання безпекових норм менеджерами всіх рівнів для формування єдиних стандартів поведінки.

Мотиваційна політика: заохочення за ініціативність у виявленні порушень або ризиків, створення безпечних каналів для повідомлення про загрози (анонімні скарги, лінія довіри).

Інтеграція безпеки в щоденні бізнес-процеси: автоматизація безпечних дій, нагадування у внутрішніх IT-системах, спрощення дотримання правил без втрати продуктивності.

Успішне формування культури безпеки в банківській установі вимагає системної роботи, яка включає навчання, контроль, заохочення та лідерство. Така культура є не лише запобіжним інструментом, а й конкурентною перевагою у сучасному фінансовому середовищі, особливо в умовах високої кіберзагрозливості та динамічних змін у регуляторному полі.

ВИСНОВКИ

У процесі дослідження було розглянуто теоретичні та практичні аспекти організації системи фінансово-економічної безпеки банківської установи, зокрема АТ КБ «ПриватБанк». Встановлено, що в сучасних умовах нестабільного макроекономічного середовища, кіберзагроз, регуляторних змін та військових ризиків питання забезпечення економічної безпеки набуває особливої актуальності.

Комплексне забезпечення безпеки діяльності банку передбачає цілісну, інтегровану систему, що включає кадрову, інформаційну, фінансову, правову, технічну та організаційну складові. Кожен із цих компонентів потребує регулярного моніторингу, аналізу ризиків та впровадження інноваційних рішень, зокрема штучного інтелекту, аналітичних платформ та систем контролю доступу. Значну роль відіграє й формування культури безпеки серед персоналу.

Проаналізовано фінансовий стан і основні операційні напрямки банку, зокрема депозитну, кредитну політику, платіжні інструменти, дистанційний банкінг. Було виявлено, що ПриватБанк демонструє достатній рівень стійкості та адаптації до умов воєнного часу, що підтверджується зростанням кількості користувачів цифрових сервісів і стабільними фінансовими показниками.

Запропоновані у курсовій роботі напрями підвищення ефективності системи безпеки – інтеграція в стратегію, цифровізація, кадрові заходи, правове оновлення, побудова аналітики ризиків – є обґрунтованими та можуть стати основою для вдосконалення внутрішніх політик банку.

Отже, сформована система комплексної фінансово-економічної безпеки забезпечує не лише захист від внутрішніх і зовнішніх загроз, а й слугує основою для довгострокової стійкості, конкурентоспроможності та довіри клієнтів до банківської установи.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Блащук-Дев'яткіна Н.; Бацман І. Фінансова безпека банківської системи України. Галицький економічний вісник https://doi.org/10.33108/galicianvisnyk_tntu Galician economic journal, No 6 (85) 2023. С. 104-112

2. Брусакова О.В. Фінансова безпека банківської системи держави. Актуальні питання забезпечення фінансової безпеки держави в умовах глобалізації. Харків, 2022. С. 115-117

3. Добровольська Н., Ушкаленко І. Моделювання механізму моніторингу фінансової безпеки банківської справи. Формування ринкової економіки в Україні. 2017. Вип. 38. С. 64–70

4. Економічна безпека суб'єктів підприємництва : підручник / З.С. Варналій, Т.Г. Васильців, О.І. Ілляш та ін.; за ред. З.С. Варналія. Чернівці: Технодрук, 2020. С. 120-121

5. Іванова Н.С. Економічна безпека : навч. посібник. Кривий Ріг: ДонНУЕТ, 2020. 139 с.

6. КорченкоА.О., Скачек Л.М, Хорошко В.О. Банківська безпека : Підручник. Київ : ПВП «Задруга», 2014. с.185.

7. Кузенко Т. Б., Сабліна Н. В. Фінансова безпека підприємства : навчальний посібник. Харків : ХНЕУ ім. С. Кузнеця, 2020. 123 с.

8. Лісняк А. Є. Чинники фінансової безпеки банків. Вісник університету банківської справи. 2017. № 3 (30). С. 77–82.

9. Рац. О.М. Шляхи удосконалення організаційного забезпечення управління економічною безпекою банку. Ефективна економіка. 2017. № 5.

10. Реверчук Н. Й., Малик Я. М., Кульчицький І. І., Реверчук С. К. Економічна безпека в Україні: держави, фірми, особи : навчальний посібник. Львів: ЛФМАУП, 2000. 192 с.

11. Як не стати жертвою шахраїв. ПриватБанк. URL: https://privatbank.ua/safeness

12. Ситник Н.С, Васьків І.М. Фінансова безпека банків як один зі складників фінансової безпеки держави. Вчені записки ТНУ імені В. І. Вернадського. Серія: Економіка і управління. 2018. Том 29 (68). № 6, С. 129-132

13. Теслюк С.А., Матвійчук Н.М., Левчук А.О. Фінансова безпека банківських установ в умовах цифровізації. Економіка та суспільство. 2024. Вип.60.