ЦЕНТРАЛЬНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
ЕКОНОМІЧНИЙ ФАКУЛЬТЕТ

Кафедра фінансів, банківської справи та страхування

«Допущено до захисту»
Завідувач кафедри фінансів,
банківської справи та страхування
д.е.н., професор
_____ Володимир СИБІРЦЕВ
«____» _____ 20 __ р.

КВАЛІФІКАЦІЙНА РОБОТА

за другим (магістерським) рівнем вищої освіти

на тему:

«Удосконалення системи управління кадровою безпекою банківської установи»

Виконав: здобувач вищої освіти 2 курсу, групи ФС-22м ОПП «Фінанси, банківська справа та страхування» спеціальності 072 «Фінанси, банківська справа та страхування»

_____ ***Євгеній ТКАЧЕНКО***

Керівник: доктор економічних наук, професор, завідувач кафедри фінансів, банківської справи та страхування

_____ ***Володимир СИБІРЦЕВ***

Рецензент: посада

Підпис ***ПІБ рецензента***

Рецензент: науковий ступінь, посада, вчене звання

Підпис ***ПІБ рецензента***

м. Кропивницький

Завідувачу кафедри фінансів, банківської справи та страхування
Володимиру СИБІРЦЕВУ
здобувача вищої освіти економічного факультету групи ФС-22М
(ОПП «Фінанси, банківська справа та страхування спеціальності 072 «Фінанси, банківська справа та страхування»)
Ткаченка Євгенія Костянтиновича

ЗАЯВА

Прошу дозволити мені виконати кваліфікаційну роботу за другим (магістерським) рівнем вищої освіти на тему: «Удосконалення системи управління кадровою безпекою банківської установи».

«_30__» _червня_ 2023 р. _____

(підпис)

Погоджено:

Керівник кваліфікаційної роботи:
_____ доктор економічних наук, професор, завідувач кафедри фінансів,
(підпис) банківської справи страхування **Володимир СИБІРЦЕВ**

«_30__» _червня_ 2023 р.

Завідувач кафедри фінансів, банківської справи та страхування:
_____ доктор економічних наук, професор **Володимир СИБІРЦЕВ**
(підпис)

«_30__» _червня_ 2023 р.

Центральноукраїнський національний технічний університет

Факультет економічний _____

Кафедра фінансів, банківської справи та страхування

Ступінь вищої освіти магістр

Галузь знань 07 «Управління та адміністрування»

Спеціальність 072 «Фінанси, банківська справа та страхування»

Освітньо-професійна (освітньо-наукова) програма «Фінанси, банківська справа та страхування»

ЗАТВЕРДЖУЮ
завідувач кафедри
Володимир СИБІРЦЕВ
_____
«_04_» _вересня_ *2023* року

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ
ЗА ДРУГИМ (МАГІСТЕРСЬКИМ) РІВНЕМ ВИЩОЇ ОСВІТИ
ЗДОБУВАЧА ВИЩОЇ ОСВІТИ
Ткаченка Євгенія Костянтиновича

1. Тема роботи: **«Удосконалення системи управління кадровою безпекою банківської установи».**
2. Керівник роботи: **Сибірцев Володимир Васильович, д-р екон. наук, професор**
3. Строк подання роботи до захисту _____
4. Мета та завдання кваліфікаційної роботи:

Метою кваліфікаційної роботи є визначення чинників впливу на рівень кадрової безпеки банку та розробка пропозицій щодо вдосконалення системи управління кадровою безпекою банківської установи в умовах сучасного фінансового середовища, з урахуванням викликів технологічних та форс-мажорних обставин.

Завдання кваліфікаційної роботи: вивчення теоретичних основ кадрової безпеки в банківській сфері; характеристика складових елементів системи управління кадровою безпекою банківської установи; дослідження стратегії розвитку та системи управління кадровою безпекою АТ «А-Банк»; оцінка чинників впливу на кадрову безпеку АТ «А-Банк»; розробка напрямів удосконалення діючої системи управління кадровою безпекою АТ «А-Банк»; визначення перспективи удосконалення системи управління кадровою безпекою банку в контексті технологічних інновацій.

Консультанти по роботі, із зазначенням розділів роботи:

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1			
2			
3			

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів виконання кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Складання плану дослідження	*жовтень 2023 р*	
2.	Підбір та вивчення літературних джерел за темою кваліфікаційної роботи	*жовтень 2023 р*	
3.	Підготовка та подання керівнику: - першого розділу - другого розділу - третього розділу - вступу та висновків	 *листопад 2023 р* *листопад 2023 р* *листопад 2023 р* *грудень 2023 р.*	
4.	Подання робочого варіанту роботи керівнику	*грудень 2023 р.*	
5.	Доопрацювання роботи з урахуванням зауважень керівника	*грудень 2023 р.*	
6.	Нормо-контроль секретаря ЕК, перевірка н академічну доброчесність	*грудень 2023 р. – січень 2024 р.*	
7.	Відгук керівника	*грудень 2023 р. – січень 2024 р.*	
8.	Рецензування роботи. Підготовка документів, що подаються до ЕК (листи, довідки, інформаційний листок, висновок-виписка, опубліковані статті).	*грудень 2023 р. – січень 2024 р.*	
9.	Подання роботи завідувачу кафедри на допуск до захисту	*січень 2024 р.*	
10.	Доопрацювання роботи з урахуванням зауважень завідувача кафедри.	*січень 2024 р.*	
11.	Подання роботи та супровідних документі до ЕК	*січень 2024 р.*	
12.	Захист роботи	*січень 2024 р.*	

Дата видачі завдання:

«_*04*_»_*вересня*_ *2023* року _____ ___Сибірцев В.В.____

(підпис керівника) (прізвище та ініціали)

Завдання прийнято до виконання:

«_*04*_»_*вересня*_ *2023* року _____ ____Ткаченко Є.К.___

(підпис здобувача) (прізвище та ініціали)

АНОТАЦІЯ

Ткаченко Є. К. Удосконалення системи управління кадровою безпекою банківської установи. Рукопис.

Кваліфікаційна робота за ступенем вищої освіти «Магістр» за ОПП «Фінанси, банківська справа та страхування», спеціальністю 072 «Фінанси, банківська справа та страхування». Центральноукраїнський національний технічний університет, Кропивницький, 2023.

У кваліфікаційній роботі вивчено теоретичні основи кадрової безпеки в банківській сфері; дано характеристику складових елементів системи управління кадровою безпекою банківської установи; досліджено стратегію розвитку та систему управління кадровою безпекою АТ «А-Банк»; дано оцінку чинників впливу на кадрову безпеку АТ «А-Банк»; розроблено напрями удосконалення діючої системи управління кадровою безпекою АТ «А-Банк»; визначено перспективи удосконалення системи управління кадровою безпекою банку в контексті технологічних інновацій.

Наукова цінність одержаних результатів дослідження кваліфікаційної роботи полягає у проведені оцінки діючої системи управління кадровою безпекою АТ «А-Банк» та розробці напрямів удосконалення діючої системи управління кадровою безпекою у контексті технологічних інновацій.

Ключові слова: кадрова безпека, кадрова політика, кібербезпека, електронна автентифікація, діагностика рівня кадрової небезпеки, ризик-менеджмент, блокчейн, лояльність персоналу.

ABSTRACTS

Tkachenko E. K. Improving the system of personnel security management of a banking organization. Manuscript.

Qualification thesis for the degree of higher education "Master" in the OPP "Finance, Banking and Insurance", specialty 072 "Finance, Banking and Insurance". Central Ukrainian National Technical University, Kropyvnytskyi, 2023.

The qualification thesis examines the theoretical foundations of personnel security in the banking sector; characterizes the components of the personnel security management system of a banking institution; studies the development strategy and personnel security management system of JSC «A-Bank»; assesses the factors influencing the personnel security of JSC «A-Bank»; develops directions for improving the current personnel security management system of JSC «A-Bank»; determines the prospects for improving the bank's personnel security management system in the context of technological innovations.

The scientific value of the obtained results of the qualification thesis is to assess the current system of personnel security management of JSC «A-Bank» and to develop directions for improving this system in the context of technological innovations.

Keywords: personnel security, personnel policy, cybersecurity, electronic authentication, diagnostics of the level of personnel danger, risk management, blockchain, staff loyalty.

ЗМІСТ

ВСТУП

У сучасних умовах форс-мажорних обставин та невизначеності, швидких технологічних змін та постійної динаміки фінансового ринку, банківські установи стикаються з великими викликами у забезпеченні ефективного управління кадровою безпекою. Зростання обсягів фінансових операцій, зміни в регуляторному середовищі та зростання кількості кіберзагроз створюють необхідність удосконалення систем управління кадровою безпекою для забезпечення стійкості, надійності та конфіденційності банківської діяльності. Враховуючи такі передумови, дослідження способів оптимізації та вдосконалення системи управління кадровою безпекою стає актуальним завданням, спрямованим на забезпечення високого рівня захисту, надійності та конфіденційності банківської діяльності в умовах непередбачуваних ситуацій та форс-мажорних подій.

Метою кваліфікаційної роботи є визначення чинників впливу на рівень кадрової безпеки банку та розробка пропозицій щодо вдосконалення системи управління кадровою безпекою банківської установи в умовах сучасного фінансового середовища, з урахуванням викликів технологічних та форс-мажорних обставин.

Для досягнення поставленої мети кваліфікаційної роботи передбачено вирішення наступних завдань:

– вивчення теоретичних основ кадрової безпеки в банківській сфері;

– характеристика складових елементів системи управління кадровою безпекою банківської установи;

– дослідження стратегії розвитку та системи управління кадровою безпекою АТ «А-Банк»;

– оцінка чинників впливу на кадрову безпеку АТ «А-Банк»;

– розробка напрямів удосконалення діючої системи управління кадровою безпекою АТ «А-Банк»;

– визначення перспективи удосконалення системи управління кадровою безпекою банку в контексті технологічних інновацій.

Об’єктом дослідження виступає є система управління кадровою безпекою банківської установи АТ «А-Банк».

Предметом дослідження є процеси та стратегії управління персоналом, спрямовані на забезпечення стійкості, надійності та конфіденційності діяльності банківської установи в контексті кадрової безпеки, з урахуванням технологічних змін та форс-мажорних обставин.

Для вирішення завдань кваліфікаційної роботи і досягнення її мети автором використано загальнонаукові і спеціальні методи, а саме: теоретичного узагальнення – для визначення сутності категорії «кадрова безпека»; логіко-структурного аналізу – для проведення оцінки діючої системи управління кадровою безпекою АТ «А-Банк»; кореляційного аналізу – для обґрунтування складу показників, що впливають на кадрову безпеку; метод порівняння – для оцінки динаміки фінансових показників діяльності АТ «А-Банк»; метод абсолютних та відносних величин – для кількісної та якісної характеристики трудових ресурсів банку; по-факторний аналіз – для впливу чинників на рівень кадрової безпеки; SWOT-аналіз – з метою визначення сильних та слабких сторін функціонування АТ «А-Банк» в умовах війни, а також виявлення можливостей та загроз кадровій безпеці; графічний і табличний – для візуалізації результатів дослідження.

Інформаційну базу кваліфікаційної роботи становлять законодавчі акти, нормативно-правові документи, інструктивні матеріали, наукові джерела за темою дослідження, дані фінансової звітності та річна інформація емітента за 2018-2022 роки, установчі документи та інформаційно-аналітичні ресурси офіційних сторінок АТ «А-Банк» в соціальних мережах.

Наукове та практичне значення результатів дослідження кваліфікаційної роботи полягає у проведені оцінки діючої системи управління кадровою безпекою АТ «А-Банк» та розробці напрямів удосконалення діючої системи управління кадровою безпекою у контексті технологічних інновацій. Обґрунтовані рекомендації впровадження сучасних методів діагностики кадрової небезпеки в систему банківського менеджменту забезпечать

збільшення швидкості реакції на загрози та виклики, високий рівень кібербезпеки та захисту персональних даних, автоматизацію процесів та зменшення ризику людського фактору, конкурентоспроможність АТ «А-Банк» та досягнення стратегічних цілей в умовах сучасного бізнес-середовища та воєнного стану.

Апробація результатів дослідження за темою кваліфікаційної роботи здійснена шляхом публікації основних положень та наукових результатів кваліфікаційної роботи, які обговорювалися і отримали позитивні відгуки на VI Міжнародній науково-практичній конференції «Конкурентоспроможна модель інноваційного розвитку економіки України» (7-8 грудня 2023 р., м. Кропивницький).

Кваліфікаційна робота складається із вступу, трьох розділів, висновків, списку використаних джерел із 46 найменування, 11 рисунків, 6 таблиць, 9 додатків. Загальний обсяг кваліфікаційної роботи – 80 сторінок.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ОСНОВИ ФОРМУВАННЯ СИСТЕМИ УПРАВЛІННЯ КАДРОВОЮ БЕЗПЕКОЮ БАНКІВСЬКОЇ УСТАНОВИ

1.1. Теоретичні підходи до визначення поняття кадрової безпеки банківської установи

Визначити сутність поняття кадрова безпека та підкреслити її ролі в системі управління персоналом банківської установи допоможе розгляд теоретичних підходів до питання формування системи управління кадровою безпекою.

Кадрова безпека визначається як важлива складова економічної безпеки поряд із фінансовою, інформаційною, технологічною, правовою та екологічною. Домінуюча роль кадрової безпеки у системі банківського менеджменту пояснюється пріоритетністю саме людських ресурсів, оскільки персонал в будь-якій організації є первинним.

У цьому контексті кадрова безпека містить наступні складові:

1. Ефективний відбір та розміщення персоналу: з метою забезпечення відповідності кожного працівника вимогам конкретної посади у контексті не лише професійних компетентностей, але й відсутності загроз для безпеки банку.

2. Організація професійного навчання та тренінгів: надання персоналу необхідних знань та навичок для роботи в умовах динамічних змін банківського середовища.

3. Внутрішні контрольні процедури: розробка та впровадження механізмів контролю за діяльністю персоналу для попередження можливих внутрішніх шахрайств та зловживань.

4. Захист конфіденційної інформації: забезпечення конфіденційності та захисту банківської інформації від несанкціонованого доступу персоналу.

Практика банківського менеджменту доводить, що кадрова безпека виконує ключову роль у фінансових установах. Вона сприяє: стабільності та

надійності фінансової установи шляхом захисту від потенційних загроз, які можуть виникнути внаслідок дій або необачних рішень персоналу; дотриманню нормативів та стандартів шляхом забезпечення відповідності фінансової установи законодавчим та регуляторним вимогам у сфері персоналу; захисту від внутрішніх та зовнішніх загроз за рахунок мінімізації ризиків, пов'язаних з діяльністю персоналу.

Науковці та менеджери-практики виокремлюють різні підходи до визначення категорії «кадрова безпека». Сучасні вітчизняні та зарубіжні дослідники поєднують кадрову складову з інтелектуальною, мета якої трактується як збереження та розвиток інтелектуального капіталу компанії в межах ефективної системи управління персоналом [15; 40; 46]. Такий підхід пояснюється тим, що безпека організації залежить не тільки від кількісних характеристик персоналу, але, в першу чергу, від якісних параметрів: рівня освіти, професіоналізму, компетентності, досвіду тощо.

Характеристика підходів до визначення поняття «кадрова безпека» представлена в табл. 1.1.

Таблиця 1.1

Теоретичні підходи до трактування поняття «кадрова безпека»

№	Визначення	Автори
1.	Під кадровою безпекою бізнесу пропонується розуміти стан захищеності господарського суб'єкта від кадрових небезпек і загроз, механізмом забезпечення цього стану є ефективне управління персоналом	Андрєєва Т. Є., Бутенко О. П., Гненна Є. В. [1]
2.	Кадрова безпека – сукупність заходів, спрямованих на запобігання протиправним діям або сприяння їм із боку персоналу підприємства	Балабанова Л. В., Сардак О. В. [2]
3.	Кадрова безпека – це такий стан індивідуумів, колективу підприємства, його людського потенціалу та системи управління персоналом, при якому забезпечується ефективне використання економічного потенціалу та розвиток підприємства	Дороніна О.А. [10]
4.	Кадрова безпека – це генеральний напрямок кадрової роботи, сукупність принципів, методів, форм організаційного механізму з опрацюванням цілей, завдань, спрямованих на збереження, зміцнення й розвиток кадрового потенціалу, на створення відповідального і високопродуктивного згуртованого колективу, здатного вчасно реагувати на постійно мінливі вимоги ринку з урахуванням стратегії розвитку організації	Дребот Н. П. [11]

Продовження табл. 1.1

5.	Кадрова безпека – правове та інформаційне забезпечення процесу управління персоналом: вирішення правових питань трудових відносин, підготовка нормативних документів, що їх регулюють, забезпечення необхідною інформацією всіх підрозділів управління персоналом	Єкімова О. О. [16]
7.	Кадрова безпека – це процес запобігання негативним діям на безпеку підприємства за рахунок усунення ризиків та загроз, пов'язаних з інтелектуальним потенціалом та трудовими відносинами в цілому	Гаврилко П, Кужелєв М. Брітченко І. [19]
8.	Кадрова безпека – це характеристика стану економічної системи, при якому відбувається ефективне функціонування всіх її функціональних складових, забезпечення захищеності та здатності протистоянь внутрішнім і зовнішнім впливам і загрозам пов'язаних з персоналом, змістовний та структурний аналіз, діагностика та прогнозування впливу діяльності персоналу на внутрішні та зовнішні показники вказаної економічної системи	Крушельницька О., Мельничук Д. [20]
9.	Кадрова безпека – це таке становище організації як соціальної спільності й індивіда в ній, за якого вплив на них із боку природного, економічного й соціального середовищ, а також внутрішнього середовища самої людини не здатні заподіяти шкоди	Лепейко Т.І. [21]
10.	Кадрова безпека – це діяльність щодо створення умов для стабільного функціонування й розвитку компанії, за яких забезпечують гарантовану законодавством захищеність інтересів компанії та власників від ризиків і загроз, пов'язаних із персоналом	Мехеда Н. Г., Маренич А. І. [22]
11.	Кадрова безпека – це таке становище організації як соціальної спільноти й індивіда в ній, за якого вплив на них із боку природного, економічного й соціального середовищ, а також внутрішнього середовища самої людини не здатні заподіяти шкоди	Назарова Г.О. [23]
12.	Кадрова безпека – це процес запобігання негативних впливів на економічну безпеку підприємства за рахунок ризиків і загроз, пов'язаних з персоналом, його інтелектуальним потенціалом і трудовими відносинами	Пластун О.І. [29]
13.	Кадрова безпека – стан захищеності суспільно-прогресивних інтересів організації з розвитку й удосконалення її людського капіталу, підтримки ефективної системи управління людськими ресурсами й мінімізації ризиків компанії, пов'язаних із її складовою	Сибірцев В. Сочинська-Сибірцева І. [32]
14.	Кадрова безпека є беззбитковістю трудових відносин підприємства	Шубалий О. М., [36]
15.	Кадрова безпека – найважливіший фактор безпеки усіх сфер діяльності підприємства, нехтування яким здатне не лише нанести серйозну шкоду підприємству, але й зруйнувати його	Щокін Г. В. [39]
16.	Кадрова безпека – це забезпеченість підприємства кадровими ресурсами, формування ефективної системи управління персоналом і комунікативної політики	Улріх Девід [40]

Джерело: складено автором з використанням джерел [1; 2; 10; 11; 16; 19; 20; 21; 23; 29; 32; 40]

Науковці сходяться на думці, що кадрову безпеку у банківській сфері доцільно визначати як комплекс технологій та інструментів, що спрямовуються на забезпечення надійності банківської установи за допомогою ефективного менеджменту персоналу. Систему управління кадрової безпекою слід спрямовувати на захист банку як від зовнішніх, так і внутрішніх загроз, а також на синхронізацію персоналу із нормативами і стандартами, що регулюють фінансовий сектор.

Існують підходи до визначення кадрової складової економічної безпеки, в межах яких персонал розглядається виключно як загроза. Треба мати на увазі, що загрози можуть йти як з боку персоналу, так і на адресу персоналу, тому метою системи управління кадровою безпекою має бути не тільки запобігання та попередження негативних впливів від персоналу, але й всебічний захист персоналу шляхом створення сприятливих умов роботи.

В результаті розгляду теоретичних підходів до визначення кадрової безпеки можемо сформулювати власне визначення категорії «кадрова безпека». У межах нашого дослідження кадрова безпека визначається як система моніторингу та синхронізації трудових відносин у колективі, яка сприяє встановленню довірчих взаємин серед працівників, а у випадку потенційної загрози чітко і швидко усуває негативні прояви без шкоди для інших.

Отже, кадрова безпека є складовою економічної безпеки, яку доцільно досліджувати як сукупність певних умов, які дозволяють попереджати потенційно небезпечні дії чи обставини; а також зводити їх до такого рівня, за якого вони не спроможні заподіяти шкоди встановленому порядку функціонування організації. Ефективність системи управління кадровою безпекою проявляється у вигляді збереження й відтворення майна організації, її інфраструктури та досягнення стратегічних цілей.

В сучасних умовах форс-мажору і непередбачуваності актуалізується необхідність здійснення заходів, спрямованих на вдосконалення теоретико-методичного забезпечення моніторингу персоналу та впливу зовнішніх факторів з метою ранньої діагностики ознак потенційної загрози; оцінки її масштабів;

дослідження головних чинників; реалізація кадрових програм щодо попередження і запобігання негативного впливу; зворотний зв’язок щодо виконання заходів управління кадровою безпекою; а також оцінка отриманих результатів за допомогою використання новітніх технологій менеджменту.

Система управління кадровою безпекою буде ефективною лише за умов побудови на основі теоретико-методичних напрацювань сучасної економічної науки і постійного удосконалення. Отже, система управління кадровою безпекою покликана заздалегідь попереджати про виникнення кризових явищ та вчасно усувати потенційні загрози, які можуть призвести до негативних наслідків.

Менеджери успішних банків сьогодні озброєні сучасним арсеналом показників і HR метрик, які дозволяють банку отримати об’єктивні дані та відслідковувати ефективність стратегій з управління кадровою безпекою. Це допомагає визначати слабкі місця, вдосконалювати процеси та забезпечувати високий рівень безпеки в організації.

Серед показників та HR метрик, які найбільш розповсюджені в практиці банківського менеджменту для вимірювання рівня кадрової безпеки особливу увагу привертають:

1. Число інцидентів безпеки - кількість випадків несанкціонованого доступу: вимірює частоту випадків, коли сталася спроба несанкціонованого доступу до конфіденційної інформації чи систем.

2. Рівень успішності тренінгів та тестувань - відсоток успішно пройдених курсів з безпеки: показник ефективності навчань та підвищення кваліфікації персоналу в галузі кадрової безпеки.

3. Час виявлення та реакції на інцидент - середня тривалість виявлення інциденту: час, який потрібен для виявлення потенційної загрози чи порушення безпеки; а також середній час реакції на інцидент: час, який потрібен для прийняття та виконання заходів з реагування на інцидент.

4. Рівень усвідомленості персоналу - відсоток персоналу, що пройшов тренінг з безпеки: метрика, що відображає ступінь усвідомленості персоналу

щодо загроз та правил безпеки.

5. Аналіз доступів та привілеїв - відсоток персоналу із застосованими принципами найменших привілеїв: показник, який визначає, наскільки ефективно керуються рівнями доступу та привілеїв.

6. Відсоток вирішених конфліктів із залученням HR-менеджерів - відсоток конфліктів, що призвели до позитивного врегулювання за участі департаменту з управління персоналом: вимірює ефективність HR-стратегій у вирішенні конфліктів та підтримці кадрової безпеки.

7. Показники кібербезпеки - кількість виявлених та зупинених кібератак: показник моніторингу кількості виявлених та успішно зупинених кібератак на інформаційні системи банку.

8. Аудит та корпоративний комплаєнс - кількість проведених внутрішніх та зовнішніх аудитів з безпеки: вказує на рівень відповідності банку стандартам та політикам з безпеки; а також на ефективність заходів, запропонованих аудиторами, та швидкість їх впровадження.

9. Індекс задоволення персоналу та лояльності - опитування персоналу щодо безпеки та задоволеності роботою: визначає рівень задоволеності та відчуття безпеки серед персоналу.

10. Витрати на безпеку та реакцію на інциденти – затрати на кадрову безпеку: сума коштів, витрачених на заходи з підтримки та покращення кадрової безпеки; а також вартість реагування на інциденти: сума коштів, витрачених на виправлення наслідків інцидентів та відновлення нормального режиму роботи.

Ці показники і метрики надають банку засоби для оцінки ефективності стратегій кадрової безпеки, виявлення слабких місць та впровадження необхідних заходів для підвищення рівня безпеки організації.

Розрахунок HR метрик в системі управління банківською установою являється ключовим інструментом для вимірювання рівня кадрової безпеки, задоволення працівників та впливу стратегій управління персоналом на превентивну кадрову політику.

Розрахунок основних HR метрик в системі банківського менеджменту

міститься в табл. 1.2.

Таблиця 1.2

Основні HR метрики системи банківського менеджменту персоналу

Метрики	Розрахункові формули	Умовні позначення
Коефіцієнт плинності кадрів	$Кпл = \frac{Чзв}{Чсс}$	Чзв – кількість звільнених з усіх причин працівників; Чсс – середньоспискова чисельність працівників, осіб.
Коефіцієнт плинності нових кадрів	$Кпл.н = \frac{Чзв.н}{Чсс}$	Чзв.н – кількість працівників, які звільнилися за власним бажанням в перший рік роботи; Чсс – середньоспискова чисельність працівників, осіб.
Коефіцієнт укомплектованості кадрами	$Кук = \frac{Чф}{Чшт}$	Чф – фактична чисельність працівників; Чшт – чисельність працівників згідно зі штатним розписом, осіб.
Коефіцієнт постійності кадрів	$Кпост. = \frac{Чп}{Чсс}$	Чп – чисельність постійних працівників із стажем роботи більше 2-х років; Чсс – середньоспискова чисельність працівників, осіб.
Рівень утримання персоналу	$Кутр = \frac{Ч_{\geq 1р}}{Чсс}$	$Ч_{\geq 1р}$ – кількість працівників, які залишилися в організації протягом року; Чсс – середньоспискова чисельність працівників, осіб.
Час, витрачений на пошук	$Чпош = Днп - Двв$	Днп – дата наймання працівника; Двв – дата відкриття вакансії.
Вартість найму	$Вн = \frac{\sum В}{Чпр}$	∑В – сума загальних внутрішніх та зовнішніх витрат на пошук за визначений час, тис. грн; Чпр – чисельність прийнятих працівників за той же час, осіб.
Індекс згоди	$Ізг = \frac{Кзап}{Кзг}$	Кзап – кількість запрошень; Кзг – кількість отриманих згод, одиниць.
Коефіцієнт відбору персоналу	$Квп = \frac{В}{Канд}$	В – кількість осіб відібраних із числа бажаючих працювати; Канд – кількість кандидатів на посаду, осіб.
Втрачені вигоди	$ВтрВиг = \frac{\overline{П}}{Чпош}$	П – середній прибуток фірми від працівника на посаді за зміну, тис. грн; Чпош – час, витрачений на пошук працівника, днів.
Коефіцієнт мотивації зарплати	$Кмзп = \frac{ЗПф}{ЗПрин}$	ЗПф – фактична середня зарплата в організації, тис. грн; ЗПрин – середньоринкова зарплата, тис. грн
Коефіцієнт трудової дисципліни	$Ктд = \frac{Тф - Тн}{Тф}$	Тн – неявки на роботу без поважних причин, людино-днів; Тф – фактично відпрацьований фонд робочого часу, людино-днів.

Продовження табл. 1.2

Коефіцієнт професійного рівня працівників	$Кпр = \frac{Чвкп}{Чсс}$	Чвкп – чисельність висококваліфікованих працівників, осіб; Чсс – середньоспискова чисельність працівників, осіб.
Витрати на освіту працівника	$Восв = \frac{Внавч}{Чсс}$	Внавч – вартість навчання, тис. грн; Чсс – середньоспискова чисельність працівників, осіб.
Відсоток робітників, що завершили навчання	$Інавч = \frac{Чнавч}{Чсс}$	Чнавч – кількість співробітників, що закінчили навчання; Чсс – середньоспискова чисельність працівників, осіб.
Продуктивність праці	$Пп = \frac{О}{Чсс}$	О – обсяг продукції, наданих послуг, тис. грн; Чсс – середньоспискова чисельність працівників, осіб.
Залученість співробітників	$Члоял$	Члоял – чисельність працівників, які згодні рекомендувати компанію своїм знайомим, осіб.

Джерело: складено автором з використанням джерел [13-15; 46]

Отже, кожна банківська установа має можливість вибирати ті метрики, які найбільше відповідають її етапу розвитку та стратегічним цілям. Моніторинг, визначення вищеназваних ключових показників, а також відповідна синхронізація системи банківського менеджменту та системи управління кадровою безпекою є необхідною умовою успішного функціонування банківської установи.

1.2. Характеристика складових елементів системи управління кадровою безпекою банківської установи

Реалії сьогодення такі, що сучасні банківські установи вимушені діяти в непередбачуваному і нестабільному середовищі, яке розбалансовується численними геополітичними, економічними та соціальними коливаннями. Така ситуація диктує необхідність швидкої адаптації до технологічних та інформаційних викликів за рахунок активного впровадження ефективних систем управління кадровою безпекою фінансових установ.

Умови воєнного стану посилюють виклики перед українськими банками, що потребує від менеджменту інтеграції сучасних технологій управління

кадровою безпекою в систему банківського менеджменту. З цих міркувань, впровадження новітніх методів та інструментів в систему управління кадровою безпекою стає актуальною вимогою для гарантії стійкості та захисту у форс-мажорних обставинах.

Ефективна система управління кадровою безпекою банківської установи передбачає взаємодію певних складових елементів, що покликані забезпечити дієвий контроль, захист персональної інформації та низки важливих активів. Головні складові елементи системи управління кадровою безпекою банківської установи представлені на рис. 1.1.

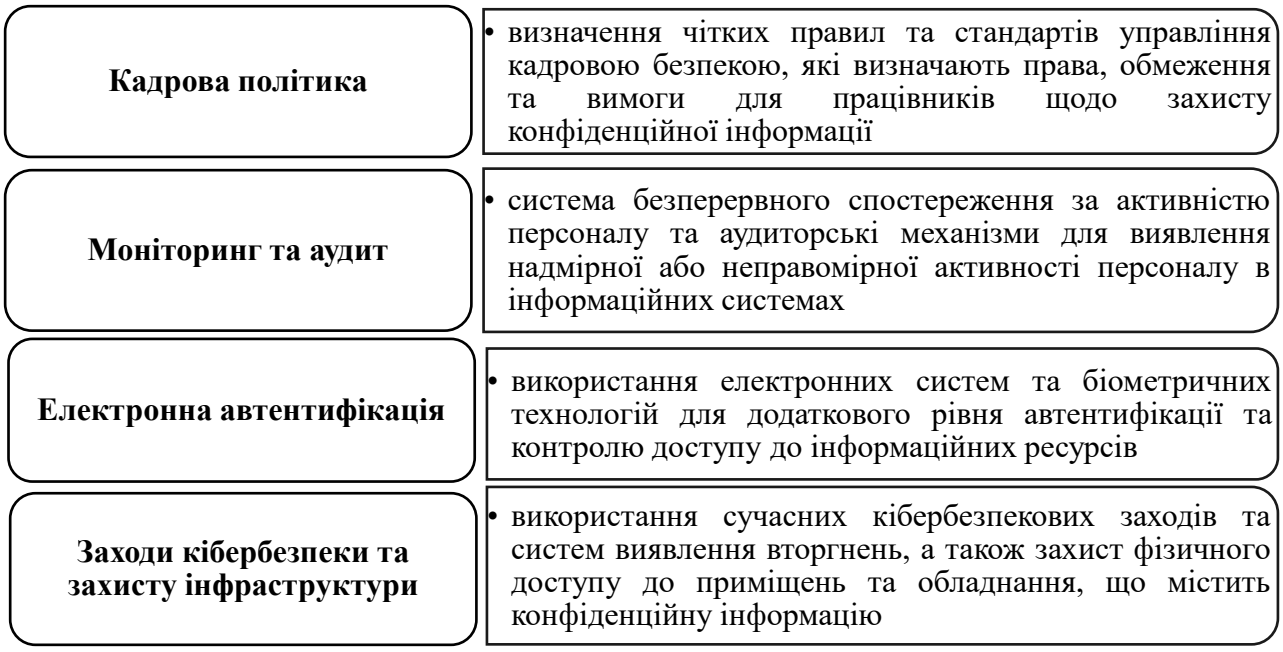

Рис. 1.1. Основні елементи системи управління кадровою безпекою у банківській установі

Джерело: складено автором з використанням джерел [10; 16; 22; 25; 32; 46]

Досконаліть системи забезпечується шляхом впровадження в практику діяльності банківських установ сучасних технологічних інструментів управління кадровою безпекою. В межах нашого дослідження особливу увагу привертають технології, які характеризуються швидкою окупністю та достатньою ефективністю.

1. Адаптація, професійний розвиток та залученість персоналу.

Систематичне проведення тренінгів та освітніх вебінарів для персоналу з питань правил обробки та збереження конфіденційної інформації. Залученість персоналу в процес впровадження культури безпеки на кожному робочому місці, відчуття відповідальності за збереження інформації.

2. Впровадження системи електронного контролю. Застосування електронних карток та мобільних додатків з метою контролю доступу до офісних приміщень, а також обмеження доступу до конфіденційної інформації. Оперативне виявлення порушень та швидке реагування на потенційні загрози за допомогою використання систем інцидент-виявлення.

3. Співпраця з технологічними компаніями. Партнерство з постачальниками новітніх технологій з метою інтеграції передових систем управління кадровою безпекою. Використання біометричних даних, а саме відбитків пальців, розпізнавання обличчя для ідентифікації працівників.

4. Партнерство із зовнішніми експертами. Співпраця з експертами з безпеки з метою оцінки, аудиту та покращення системи управління кадровою безпекою.

Розглянуті технологічні підходи дають можливість банкам будувати комплексні та дієві системи управління кадровою безпекою, забезпечуючи захист від загроз внутрішнього та зовнішнього впливу.

Важливо враховувати той факт, що ефективність системи управління кадровою безпекою банківської установи на пряму залежить від якості виконання функцій HR-менеджменту. Охарактеризуємо пріоритетні функції у цьому напрямку.

Адекватний відбір та розміщення персоналу:

- рекрутинг та якісний відбір шляхом розробки ефективних процедур рекрутингу, включаючи високий стандарт відбору та асесмент-центри для оцінки компетентностей кандидатів;

- корпоративна культура та цінності з акцентом на забезпечення відповідності цінностей та етичних стандартів банку при відборі та адаптації нового персоналу.

Організація навчань та тренінгів:

- професійний розвиток шляхом реалізації програм навчання та тренінгів для підтримки професійного росту та адаптації до новітніх технологій і методів;
- впровадження системи оцінювання, що визначає ефективність навчання та професійного розвитку.

Процедури внутрішнього контролю:

- моніторинг діяльності персоналу через систему постійного моніторингу та оцінки роботи персоналу з метою виявлення аномалій та недоліків;
- регулярні аудити системи управління кадровою безпекою для виявлення та усунення можливих слабких місць.

Захист конфіденційної інформації:

- кіберзахист та безпека інформації за рахунок застосування технологічних заходів для захисту конфіденційної інформації, включаючи шифрування даних та мережеві заходи безпеки;
- розробка та впровадження строгих політик доступу до конфіденційної інформації, включаючи рівні доступу для різних категорій персоналу.

Етичне та соціальне управління персоналом:

- визначення та поширення кодексу етики, який визначає основні принципи поведінки та стандарти взаємодії персоналу;
- соціальна відповідальність шляхом реалізації програм та ініціатив, спрямованих на покращення відносин із спільнотою та соціальну відповідальність банку.

Цифрова безпека та кіберзахист:

- ідентифікація та аутентифікація за рахунок використання біометричних технологій для підвищення рівня ідентифікації та аутентифікації персоналу;
- навчання з кібербезпеки шляхом організації регулярних тренінгів з кібербезпеки для персоналу для попередження фішинг-атак та інших загроз.

Описані функції управління наповнюють складові елементи та утворюють інтегровану систему управління кадровою безпекою банківської установи, спрямовану на ефективний контроль і захист від внутрішніх та зовнішніх загроз.

Важливу роль в процесі побудови та удосконалення системи управління кадровою безпекою відіграють обрані стратегії та методи управління. Серед сучасного арсеналу стратегій, підходів і методів особливу увагу привертають:

1. Стратегія інтегрованого управління ризиками.

Запровадження комплексної системи управління ризиками, орієнтованої на виявлення та управління ризиками, пов'язаними з персоналом.

Використання аналітики та даних для ідентифікації потенційних загроз та розробки стратегій мінімізації ризиків.

2. Гнучка система управління персоналом.

Впровадження гнучких методів управління персоналом, які дозволяють швидко адаптуватися до змін внутрішнього та зовнішнього середовища.

Розвиток системи навчань та розвитку для забезпечення високого рівня компетентності персоналу.

3. Технологічні інновації в управлінні кадровою безпекою.

Використання штучного інтелекту та машинного навчання для виявлення аномалій та попередження можливих внутрішніх загроз.

Застосування біометричних технологій для підвищення рівня аутентифікації та контролю доступу.

4. Етичне та соціальне управління персоналом:

Розвиток етичних стандартів та внесення їх у корпоративну культуру для підвищення довіри та відповідальності персоналу.

Реалізація соціально-відповідальних практик, спрямованих на покращення якості робочого середовища та підтримку спільноти.

5. Цифрова безпека та кіберзахист.

Вдосконалення заходів з кіберзахисту для запобігання атакам та витокам конфіденційної інформації.

Розробка та впровадження стратегій посилення цифрової безпеки персоналу шляхом навчань та обізнаності.

Сучасні стратегії та методи є ключовими компонентами ефективної системи управління кадровою безпекою, які враховують сучасні тенденції та

виклики фінансового сектору.

Отже, сучасні банківські установи мають інвестувати ресурси в регулярні навчальні програми, з метою підвищення рівень свідомості працівників з питань кібербезпеки, соціального інжинірингу та правил користування і збереження конфіденційної інформації.

У підсумку слід підкреслити, що ключові елементи системи кадрової безпеки банківських установ ще раз підкреслюють важливість і специфічність людського фактору, який сприймається як пріоритетніший серед усіх видів економічних ресурсів організації. Менеджери банків прагнуть залучати персонал, готовий та спроможний належним чином здійснювати свої професійні обов'язки, а також активно розглядають і впроваджують технології збереження, задоволення, професійного і соціального розвитку персоналу з метою підвищення його надійності.

1.3. Чинники впливу на рівень кадрової безпеки банку в умовах цифровізації

В умовах цифровізації загострюються виклики та загрози для кадрової безпеки в банківському секторі. Особливий вплив в умовах сьогодення мають наступні:

А. Кібербезпека та кіберзагрози.

Соціальна інженерія: зростання соціально-інженерних атак, спрямованих на маніпулювання персоналу та отримання конфіденційної інформації.

Масштабні кібератаки: загроза масштабних кібератак на банківські установи та можливий витік конфіденційної інформації.

Б. Внутрішні загрози та зловживання.

Інсайдерські загрози: зростання ризику внутрішніх загроз внаслідок зловживання довірою працівників.

Крадіжка конфіденційної інформації: потенційна загроза викрадення конфіденційної інформації для особистої вигоди або продажу на чорному ринку.

В. Технологічні та організаційні зміни.

Неадаптованість персоналу: виклик, пов’язаний з впровадженням нових технологій та процесів, які можуть вимагати додаткового навчання та адаптації.

Перехід до роботизації: загроза автоматизації рутинних завдань та можливого зменшення ролі людей в певних сферах банківської діяльності.

Г. Лояльність та задоволеність персоналу.

Відтік кваліфікованих кадрів: ризик втрати висококваліфікованих працівників через недостатню лояльність або конкуренцію на ринку праці.

Низький рівень задоволеності: можливість виникнення проблем з організаційною культурою та низьким рівнем задоволеності персоналу.

Д. Регуляторні вимоги та внутрішні стандарти.

Збільшення обов’язкових вимог: зростання регуляторних обов’язків у сфері управління кадровою безпекою, що може вимагати додаткових ресурсів та зусиль.

Відповідність стандартам безпеки: зобов’язання банків відповідати стандартам безпеки та підтримувати відповідність корпоративного комплаєнсу в умовах постійних змін.

Зазначені виклики та загрози підкреслюють необхідність постійного вдосконалення систем управління кадровою безпекою в банківському секторі, а також акцентують увагу на важливості гнучкості та готовності до адаптації до нових реалій фінансового ринку.

В системі сучасного менеджменту досліджується ціла низка теоретичних підходів до визначення чинників впливу на кадрову безпеку в банківських установах. Характеристика основних підходів має наступний вигляд (рис. 1.2).

Системний підхід розглядає кадрову безпеку як складову загальної системи управління банком. Аналізує взаємозв’язки та взаємодії між різними елементами, включаючи організаційну культуру, технічні системи та персонал.

Підхід управління ризиками базується на ідентифікації та оцінці ризиків для кадрової безпеки. Фактори визначаються через аналіз потенційних загроз та вразливостей, а також визначення ймовірності та впливу подій.

Рис. 1.2. Підходи до визначення чинників впливу на кадрову безпеку

Джерело: складено автором з використанням джерел [13-15; 26; 33]

Психологічний підхід розглядає вплив психологічних аспектів на кадрову безпеку, таких як мотивація працівників, рівень стресу та вплив організаційної культури на психічний стан персоналу.

Підхід кібербезпеки акцентує увагу на заходах з технічного захисту від кіберзагроз та визначенні факторів, що впливають на ефективність кібербезпеки персоналу та інформаційних ресурсів.

Соціальний підхід зосереджується на соціальних взаємодіях та впливі організаційного середовища на кадрову безпеку. Аналізується роль комунікації, лідерства та соціального клімату.

Юридичний підхід визначає фактори, що випливають із законодавства та регулювань щодо безпеки працівників та конфіденційності інформації.

Організаційний підхід розглядає структуру та системи управління організацією як ключові фактори, що впливають на кадрову безпеку.

Економічний підхід аналізує фактори впливу економічного середовища на рівень інвестицій у кадрову безпеку та ефективність витрат.

Розглянуті підходи можуть використовуватися разом для комплексного визначення та аналізу факторів, які впливають на кадрову безпеку в банківських установах. Комбінація різних підходів дозволяє здійснити глибокий аналіз та врахувати різноманітні аспекти цього питання.

Головними чинниками впливу на рівень кадрової безпеки банку вважаються такі блоки рушійних сил (рис. 1.3):

Блок 1. Культура організації та лідерство. Головний акцент робимо на лідерстві, що активно відстоює принципи та визначає важливість кадрової безпеки для всієї організації. Особливу роль у цьому блоці відіграє розвиток етичної культури, яка формує основні цінності та стандарти поведінки персоналу.

Блок 2. Технічні та кіберзагрози. Головний акцент робимо на захисті інформації шляхом використання технологій для ефективного захисту конфіденційної інформації від кіберзагроз та несанкціонованого доступу. Важливе значення мають регулярні оновлення програм та застосунків для усунення вразливостей та підвищення стійкості до кібератак.

Блок 3. Системи управління персоналом. Увага фокусується на відборі та наймі персоналу шляхом створення ефективної системи пошуку та залучення персоналу, включаючи перевірку даних та дотримання стандартів безпеки. Банківський менеджмент акцентує увагу на впровадженні системи оцінки та моніторингу роботи персоналу, виявлення аномалій та ризиків.

Блок 4. Посадові обов’язки та розподіл доступів. Даний блок передбачає впровадження принципу найменших привілеїв і розподіл доступів на основі такого принципу для мінімізації ризиків внутрішніх загроз. Ключовою вимогою є налагодження системи керування доступом, яка гарантує, що кожен працівник має доступ лише до необхідних ресурсів.

Блок 5. Комплексність та сучасні технології. Передбачається застосування інтегрованих систем для ефективного управління різними аспектами кадрової безпеки, а також використання сучасних технологій з метою моніторингу подій в режимі реального часу та оперативного реагування на загрози.

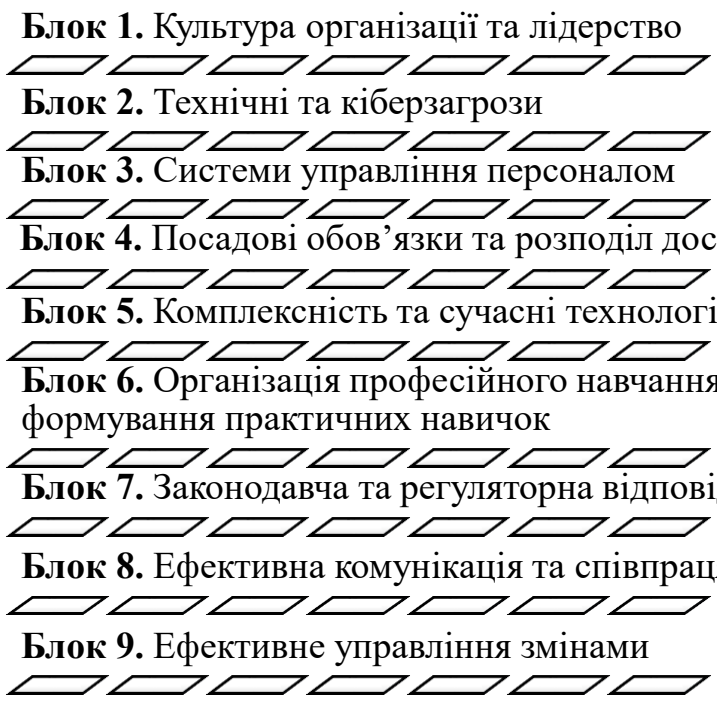

Рис. 1.3. Класифікація чинників впливу на рівень кадрової безпеки банківської установи

Джерело: складено автором з використанням джерел [1; 25; 27; 32; 41; 44]

Блок 6. Організація професійного навчання та формування практичних навичок. Проведення регулярних тренінгів та навчань з кадрової безпеки для всього персоналу, а також формування раціональної свідомості працівників щодо ризиків та ефективних заходів безпеки.

Блок 7. Законодавча та регуляторна відповідність. Важливими аспектами в межах даного блоку є розробка та впровадження внутрішніх стандартів та політик, що відповідають законодавчим вимогам. Головним інструментом при цьому є проведення регулярних аудитів для перевірки відповідності встановленим стандартам та політикам безпеки.

Блок 8. Ефективна комунікація та співпраця. Розвиток ефективних систем звітності та комунікації для оперативного обміну інформацією щодо загроз та подій. Особлива увага фокусується на захисті від внутрішніх конфліктів шляхом створення умов для відкритої комунікації, що сприяє виявленню та вирішенню внутрішніх конфліктів.

Блок 9. Ефективне управління змінами. Управління змінами в системі

банківського менеджменту доцільно спрямовувати на гнучкість та адаптабельність до нових викликів та технологічних тенденцій. Позитивний результат дає періодична оцінка впливу нових технологій та організаційних змін на рівень кадрової безпеки.

Описані чинники взаємодіють та визначають загальний рівень кадрової безпеки банку, формуючи важливу складову його стійкості та надійності в умовах сучасного фінансового середовища.

Сучасний менеджмент банківської установи особливо уважно має прораховувати вплив цифрових технологій на управління кадровою безпекою в банківському секторі. Детально охарактеризуємо актуальні тенденції.

1. Автоматизація процесів безпеки:

- електронна система контролю доступу: застосування біометричних технологій, таких як відбитки пальців або розпізнавання обличчя, для підвищення рівня безпеки в контролі доступу до об’єктів та інформації;

- системи відеоспостереження: використання високоякісних систем відеоспостереження для виявлення та моніторингу можливих загроз в реальному часі.

2. Штучний інтелект та аналітика даних:

- прогнозування ризиків: використання алгоритмів машинного навчання для аналізу великих обсягів даних та прогнозування можливих ризиків в сфері кадрової безпеки;

- виявлення аномалій: застосування аналітики даних для виявлення аномальних патернів у поведінці персоналу, що може свідчити про можливі внутрішні загрози.

3. Електронні системи навчань та тренінгів:

- E-learning (електронне навчання) та онлайн-тренінги: впровадження електронних систем для проведення тренінгів з кадрової безпеки, що дозволяє персоналу отримувати актуальні знання в будь-який час та в будь-якому місці;

- симуляції та віртуальні тренажери: використання технологій віртуальної реальності для проведення симуляцій ситуацій з порушеннями кадрової безпеки.

4. Інтеграція аналітики в реальному часі:

- системи моніторингу: розробка систем, які надають можливість відслідковувати дії персоналу в режимі реального часу та швидко реагувати на будь-які потенційні загрози;

- системи автоматичного сповіщення: використання технологій для автоматичного генерування та розсилання сповіщень у випадку виявлення незвичайної або підозрілої активності.

5. Електронна звітність та обмін інформацією:

- системи електронної звітності: використання електронних платформ для звітності та обміну інформацією між різними підрозділами та рівнями управління;

- електронні системи обліку робочого часу: застосування систем, що автоматизують облік робочого часу, для забезпечення точності та конфіденційності даних.

6. Розвиток та впровадження новітніх технологій:

- роботизація рутинних завдань: використання роботів та інших автоматизованих засобів для виконання рутинних завдань, зменшення ризику людських помилок;

- інноваційні методи аутентифікації: впровадження біометричних технологій та інших інноваційних методів аутентифікації для підвищення безпеки доступу.

У підсумку слід зазначити, що вплив технологій на управління кадровою безпекою включає в себе автоматизацію процесів, покращення аналітики та забезпечення ефективної інтеграції інновацій для підвищення рівня захисту банківської установи та її персоналу. Загальною метою формування системи управління кадровою безпекою є створення комплексного підходу, який об’єднує технічні, соціальні, організаційні та економічні аспекти з метою забезпечення стійкої та ефективної безпеки в банківській установі.

РОЗДІЛ 2
ДОСЛІДЖЕННЯ СТРАТЕГІЇ РОЗВИТКУ ТА СИСТЕМИ УПРАВЛІННЯ КАДРОВОЮ БЕЗПЕКОЮ АТ «А-БАНК»

2.1. Характеристика організаційної структури управління та результатів діяльності АТ «А-Банк»

Акціонерне товариство «АКЦЕНТ-БАНК» (далі АТ «А-Банк») є правонаступником всіх прав та зобов'язань закритого акціонерного товариства «АКЦЕНТ-БАНК». Закрите акціонерне товариство «акцент-банк» є правонаступником Закритого акціонерного товариства «Український кредитний банк», який є правонаступником прав та обов'язків «Київського приватного банку «Київприватбанк», створеного в Україні у 1992 році. У 2018 році у зв'язку зі змінами в законодавстві, назва Банку була змінена на акціонерне товариство «АКЦЕНТ-БАНК», також змінено тип акціонерного товариства з публічного на приватне. Організаційно-правова форма банку - акціонерне товариство. Тип акціонерного товариства – приватне [28; 34].

Основними видами діяльності банку є залучення депозитів, відкриття та ведення рахунків клієнтів, надання кредитів і гарантій, здійснення розрахунково-касового обслуговування, проведення операцій з цінними паперами та іноземною валютою.

Діяльність банку регулюється Національним банком України (НБУ). Банк має банківську ліцензію №16 від 26.10.2011р. на здійснення банківських операцій, входить до державної системи гарантування вкладів в Україні та має статус спеціалізованого банку.

З моменту свого заснування АТ «А-Банк» поступово і ефективно розвивається, пропонуючи своїм клієнтам максимальний вибір банківських продуктів і послуг. Бізнес банку базується на зміцненні і розвитку взаємовигідної співпраці з підприємствами виробничого сектора економіки України. Одним з пріоритетних напрямків своєї діяльності керівництво АТ «А-Банк» визначає:

постійну роботу над підвищенням своєї надійності і стійкості, впровадження сучасних банківських технологій, поліпшення якості і розширення спектру послуг. Пріоритетними напрямками стратегічного розвитку Банку є: орієнтація на клієнта, розвиток регіональної мережі, висока технологічність банківських операцій.

5 березня 2020 року Банк набув статус системно важливого банку. Для системно важливих банків діють підвищені вимоги щодо певних нормативів та додаткового до нормативного значення достатності основного капіталу буферу системної важливості, що покликані забезпечити додатковий запас їх стійкості.

У 2020 році Банк отримав статус члена міжнародних платіжних систем Mastercard та Visa та міжнародної системи термінових грошових переказів Western Union, підключився до BankID НБУ, впровадив процедуру віддаленої ідентифікації та верифікації банківських клієнтів з цифровим паспортом у мобільному застосунку "Дія". За підсумками 2020 року Банк був нагороджений дипломами: VISA - за "Видатне зростання карткового портфеля VISA за підсумками 2020р." та MasterCard - "Великий крок вперед" [28].

За даними Центру соціально-економічних досліджень CASE Україна, Банк увійшов у топ-5 найефективніших банків України у березні-травні 2022 року, зайнявши четверте місце серед банків з найкращим результатом за показником Cost-to-lncome ratio - відношення операційних витрат до операційних доходів.

26 серпня 2022 року відбулася церемонія - нагородження щорічної премії, яка визначає кращих професіоналів фінансового сектору України і фінансові продукти - FinAwards2022. За результатами титул найкращого банку в Україні за дистанційним обслуговуванням отримав А-Банк. Також Банк отримав срібло у номінації «Лідер народного рейтингу» та бронзу у номінації «Найкраща платіжна картка». У грудні 2022 року Банк отримав винагороду Resilience Award 2022 від Mastercard, яка символізує стійкість Банку на фінансовому ринку та перше місце у народному рейтингу банків за версією сайту «Мінфін» [28].

22 листопада 2022 року незалежне рейтингове агентство «Кредит-Рейтинг» підтвердило довгостроковий кредитний рейтинг АТ «А-Банк» на рівні иаАА-

(висока кредитоспроможність) Рейтинг знаходиться у Контрольному списку. Прогноз рейтингу - негативний. 27 грудня 2022 року агентство підтвердило рейтинг надійності вкладів (депозитів) Банку на рівні «4» (висока надійність).

Станом на 31 грудня 2022 року у Державному реєстрі банків зареєстровано 200 відокремлених підрозділів Банку (31 грудня 2021 р. - 237 відділень).

Банк має намір активно і послідовно використовувати накопичений досвід і знання українського бізнесу і розширювати свою діяльність на ринку України.

Статутом банку визначено, що АТ «А-Банк» створений для надання повного спектру внутрішніх та міжнародних банківських, фінансових та інших послуг, включаючи всю без обмеження діяльність, яка пов'язана із здійсненням комерційної, інвестиційної, депозитарної та будь-якої іншої діяльності, яка може бути дозволеною банкам чинним законодавством України, з метою одержання прибутку, максимізації добробуту акціонерів у вигляді зростання ринкової вартості акцій банку, а також отримання акціонерами дивідендів (додаток А).

Органами управління АТ «А-Банк» відповідно до Закону України «Про банки і банківську діяльність» є Наглядова рада та Правління [34].

Наглядова рада є вищим органом управління Банку, що здійснює контроль за діяльністю правління банку з метою збереження залучених у вклади грошових коштів, забезпечення їх повернення вкладникам і захисту інтересів держави як акціонера державного банку, а також здійснює інші функції.

Правління Банку є виконавчим органом банку, здійснює управління поточною діяльністю банку, формування фондів, необхідних для статутної діяльності банку. Голова правління банку керує роботою виконавчого органу та має право представляти банк без доручення.

Організаційна структура управління АТ «А-Банк» включає всі необхідні форми контролю для побудови ефективного і злагодженого механізму: з боку акціонерів, Наглядової ради, Правління, Служби внутрішнього аудиту над різними напрямками діяльності банку. Розподіл повноважень, компетенцій та підпорядкованості органів управління, а також принципи їх взаємодії, закріплені в Статуті банку та положеннях про органи управління. Якісне функціонування

банку забезпечує гнучка та ефективна організаційна структура управління (ОСУ), що обумовлює раціональний розподіл функціональних обов'язків усередині банків. По суті вона є комбінованою, тому що містить ознаки широко розповсюджених у світовій практиці видів організаційної структури управління:

1 - горизонтальна (площинна), оскільки в ній виділено лише 2 рівні управління: «1-й рівень» - Головний офіс (ГО); «2-й рівень» - Відділення.

2 - дивізіональна клієнто- і функціонально-орієнтована, тому що відділення підтримують бізнесові напрямки, які зорієнтовані на комплексне обслуговування певних груп клієнтів або виконання комплексу однорідних функцій (додаток Б).

Узагальнена модель організаційної структури управління АТ «А-Банк» представлена на рис. 2.1.

Рис. 2.1 Узагальнена модель ОСУ АТ «А-Банк»

Джерело: проілюстровано автором з використанням додатку Б

Наглядова рада АТ «А-Банк» підпорядковується загальним зборам і керує роботою Правління та трьох колегіальних органів (комітетів): комітет з питань аудиту, комітет з питань винагород та призначень, комітет з управління ризиками. Також Наглядова рада банку координує роботу напрямку «Внутрішній аудит», департаменту Compliance, напрямків ризик-менеджменту та стягнення проблемних заборгованостей.

Для підготовки, обговорення та прийняття стратегічних і важливих тактичних рішень безпосередньо під керівництвом Голови Правління в Правлінні банку функціонують такі колегіальні органи, як: Комітет по управлінню інформаційною безпекою, Кредитний комітет, Комітет з управління активами та пасивами, Комітет з управління непрацюючими активами, Малий кредитний комітет, Малий комітет з управління непрацюючими активами.

Як видно з рис. 2.1 організаційна структура управління АТ «А-Банк» характеризується горизонтальним та вертикальним поділом праці та лінійні зв’язки.

В структурі Банку виділяються: «бізнесові напрямки», які отримують дохід у результаті прямого контакту із клієнтами та «підтримуючі напрямки», що забезпечують необхідні умови, для функціонування інших напрямків діяльності підрозділів Банку, при цьому не вступаючи в прямий контакт із клієнтами.

Організаційна структура управління АТ «А-Банк» доцільна для даної банківської установи. Перевагою цієї структури є можливість швидко приймати рішення, реагувати на зміни у зовнішньому оточенні і забезпечувати неформальний підхід до мотивації і контролю діяльності співробітників.

Очолює банк Голова правління, який виконує функції керівника, приймаючи важливі рішення, що пов`язані з діяльністю Банку. Голова правління має Першого заступника, який виконує ті ж обов`язки у випадку його відсутності чи зайнятості у сферах корпоративного та індивідуального бізнесів, а також двох заступників – керівників департаментів, які слідкують за роботою підрозділів; проводять найбільш складні і відповідальні операції.

Департамент Compliance - здійснює функції комплаєнс шляхом здійснення

своєчасного виявлення, вимірювання, моніторингу, контролю, пом'якшення та звітування щодо комплаєнс-ризику.

Напрямок «Ризик-менеджмент» здійснює управління кредитним ризиком, процентним ризиком банківської книги, ризиком ліквідності, ринковими ризиками (з урахуванням ризику концентрації), операційним ризиком та іншими ризиками; управління непрацюючими активами; здійснює оцінку кредитоспроможності клієнтів, достатності фінансового стану та прозорості структури власності позичальника відповідно до процедур банку, а також попередження виникнення кредитного ризику на етапі погодження кредитних рішень, оцінка заставного майна; управління процесом ухвалення рішень щодо надання кредитів на базі скорингових моделей.

До напрямку «Бізнес» входять напрямки:

1. «Роздрібні продажі» - здійснює грошові перекази, приймає платежі населення (комунальні, бюджетні, комерційні, перекази P2P та інші).
2. «Заощадження» - здійснює залучення депозитів фізичних осіб.
3. Бізнес А-Кредит - залучення та кредитування фізичних осіб у торгівельних точках, відділеннях банку, мережі Інтернет.
4. Напрямок Internet banking - організовує роботу інтернет-банкінгу.
5. Напрямок «Кредитні картки» - здійснює залучення клієнтів та просування карткових продуктів Банку.
6. Напрямок Корпоративного бізнесу - здійснює залучення та кредитування юридичних осіб.
7. Напрямок споживчого кредитування - здійснює нецільове споживче кредитування фізичних осіб (крім кредитування у формі кредитної лінії).
8. Напрямок «Операційний центр» - здійснює обслуговування в режимі Call-center, здійснює продаж продуктів Банку.
9. Напрямок «Казначейство» - забезпечує ліквідність Банку у всіх валютах при оптимізації витрат.
10. Регіональні директори А-Банк - здійснює планування, організацію розвиток регіональних відділень.

11. Напрямок «Касове обслуговування» - здійснює організацію роботи касового обслуговування.

12. Департамент ломбардного кредитування - здійснює кредитування під заставу золота, ювелірних виробів.

Напрямок «Підтримка» включає:

1. Напрямок «Розвиток УП» - здійснює розвиток та поліпшення умов праці, приміщень Банку.

2. Відділ «Охорона праці» - здійснює охорону праці.

3. Напрямок «Трудових ресурсів» - здійснює прийом, звільнення співробітників, облік. Відділ управління персоналом – це структурний підрозділ загальної системи управління, на який покладаються обов'язки реалізації кадрової політики підприємства. Спеціалісти цього відділу проводять аналітичну й оперативну роботи, здійснюють виконавчі, розпорядчі, контролюючі та координаційні функції в сфері управління персоналом.

4. Юридичний департамент - здійснює юридичній супровід. Розробляє нормативні документи і контролює правильність укладання банківських угод, складає договори, різного роду акти та інші ділові папери, позовні заяви, протести і т. п., веде справи банку в судових та адміністративних установах. Юридичний відділ у своїй діяльності керується Конституцією та законами України, постановами Верховної Ради України, актами Президента України, Кабінету Міністрів України, іншими нормативно-правовими актами, міжнародними договорами України, Загальним положенням про юридичну службу міністерства та іншими нормативно-правовими документами.

5. Напрямок корпоративного навчання - здійснює навчання співробітників.

6. Напрямок «Управлінські технології» - забезпечує менеджмент та комунікацію у банку (по горизонталі та вертикалі).

7. Напрямок «Служба безпеки» - здійснює організацію безпеки. Забезпечує функції охорони та нагляду за діяльністю банку. Впроваджує заходи щодо збереження банківської та комерційної таємниці.

8. Напрямок бюджетування - здійснює підготовку бюджетів.

9. Напрямок «Бухгалтерія» - здійснює бухгалтерський облік.

Напрямок «Back-office» - здійснює операційно-облікову роботу та контроль за операціями. До його складу входять:

1. Департамент з обліку внутрішньобанківських операцій - здійснює облік внутрішньобанківських операцій.

2. Департамент з організації роботи архівів - здійснює організацію роботи архівів.

3. Департамент «Вхідна кореспонденція» - здійснює обробку вхідної кореспонденції.

4. Департамент «Процесінг» - здійснює роботу з Міжнародними платіжними системами та обслуговування карткових транзакцій.

Департамент Фінансового моніторингу - здійснює фінансовий моніторинг.

Напрямок «Інформаційні технології» включає:

1. Департамент експлуатації програмних комплексів - здійснює підтримку програмного забезпечення.

2. Департамент інфраструктури IT - здійснює забезпечення технічними засобами та їх налаштування.

3. Департамент моніторингу та телекомунікацій - здійснює моніторинг телекомунікацій.

4. Департамент «Центр обробки даних» - здійснює та контролює обробку даних.

5. Департамент з тестування програмного забезпечення - здійснює тестування програмного забезпечення, яке використовується або вводиться в експлуатацію.

Ефективність і дієвість організаційно-управлінської структури АТ «А-Банк» підтверджує аналіз фінансових показників діяльності за підсумками 2018-2022 років, який дає можливість стверджувати, що банк послідовно дотримується визначеного керівництвом вектору розвитку.

Активи АТ «А-Банк» за досліджуваний період 2018-2022 років представлені у таблиці 2.1.

Таблиця 2.1

Динаміка показників активів АТ «А-Банк»

№ п/п	Показники, тис. грн	Роки					Динаміка				
		2018	2019	2020	2021	2022	2019 2018	2020/ 2019	2021/ 2020	2022/ 2021	2022/ 2018
1	Грошові кошти та їх еквіваленти	561 682	858 215	1 337 270	3 979 698	10 387 765	у 1,53 рази	у 1,56 рази	у 2,98 рази	у 2,61 рази	у 18,49 рази
2	Кредити та аванси клієнтам	3 473 991	4 868 112	6 931 104	8 983 168	5 516 412	у 1,4 рази	у 1,42 рази	у 1,3 рази	61,4%	у 1,59 рази
3	Інвестиції в цінні папери	28 638	38 881	55 433	54 014	175 703	у 1,36 рази	у 1,43 рази	97,4%	у 3,25 рази	у 6,14 рази
4	Інвестиційна нерухомість	-	-	9 765	10 540	11 946	-	-	у 1,08 рази	у 1,13 рази	-
5	Нематеріальні активи	51 399	54 301	92 367	67 319	74 154	у 1,06 рази	у 1,7 рази	72,9%	у 1,1 рази	у 1,44 рази
6	Основні засоби	102 721	119 575	225 993	254 068	260 894	у 1,16 рази	у 1,89 рази	у 1,12 рази	у 1,03 рази	у 2,54 рази
7	Активи у формі права користування (оренда)	-	62 838	95 371	110 424	78 208	-	у 1,52 рази	у 1,16 рази	70,8%	-
8	Інші фінансові та не фінансові активи	207 211	312 886	477 859	915 347	1 278 269	у 1,51 рази	у 1,53 рази	у 1,92 рази	у 1,4 рази	у 6,17 рази
9	Необоротні активи, утримувані для продажу	2 129	577	727	3 334	3 327	27,1%	у 1,26 рази	у 4,59 рази	99,8%	у 1,56 рази
	Усього активів	**4 849 255**	**6 432 935**	**9 225 889**	**14 377 912**	**17 786 728**	у 1,33 рази	у 1,43 рази	у 1,56 рази	у 1,24 рази	у 3,67 рази

Джерело: [додатки В, Г, Д, Е, Ж]

Як бачимо з наведеної інформації (табл. 2.1), загальна сума активів АТ «А-Банк» у 2019 році порівняно з попереднім 2018 роком збільшилась на 1 583 680 тис. грн (у 1,33 рази). У 2020 році сума активів зросла ще на 2 792 954 тис. грн (у 1,43 рази). У 2021 році відбулось найбільше щорічне збільшення суми активів АТ «А-Банк» на 5 152 023 тис. грн. (у 1,56 рази), і у 2022 році знову відбулось збільшення суми активів на 3 408 816 тис. грн за рахунок значного збільшення кількості грошових коштів та інвестицій у цінні папери. Загальна ж сума активів АТ «А-Банк» за досліджуваний період (2018-2022) збільшилась у 3,67 рази (станом на 01.01.2023 року склала 17 786 728 тис. грн), що свідчить про виважене ставлення банківської установи до якості своїх активів. Такий підхід дозволяє АТ «А-Банк» здійснювати ефективне управління власними активами та досягати позитивного результату за кожною активною операцією. Ефективне управління активами дозволяє вирішувати проблему прибутковості, дотримання нормативів ліквідності та контролю притаманних даній установі ризиків. Розкриття інформації за видами активів у фінансовій звітності АТ «А-Банк» відповідає вимогам Національного банку України та національних положень (стандартів) бухгалтерського обліку.

Щоб більш детально проаналізувати дохідність активів, розрахуємо коефіцієнт дохідності АТ «А-Банк» ($К_{дох}$) за запропонованою формулою:

$$К_{дох} = Да / Ва; \quad (2.1)$$

де *Да* – дохідні активи, тис. грн;

Ва – активи всього, тис. грн.

Тепер підставимо значення із табл. 2.1 у формулу (2.1) і отримаємо значення коефіцієнту дохідності за відповідні роки:

$$К_{дох2018} = 561\ 682 + 3\ 473\ 991 + 28\ 638 / 4\ 849\ 255 = 0{,}84;$$

$$К_{дох2019} = 858\ 215 + 4\ 868\ 112 + 38\ 881 / 6\ 432\ 935 = 0{,}9;$$

$$К_{дох2020} = 1\ 337\ 270 + 6\ 934\ 622 + 55\ 433 + 9\ 765 / 9\ 225\ 889 = 0{,}9;$$

$$К_{дох2021} = 3\ 979\ 698 + 8\ 983\ 168 + 54\ 014 + 10\ 540 / 14\ 377\ 912 = 0{,}91.$$

$$К_{дох2022} = 10\ 387\ 765 + 5\ 516\ 412 + 175\ 703 + 11\ 946 / 17\ 786\ 728 = 0{,}9.$$

Коефіцієнт дохідності у 2018 році становив 0,84, а у 2019 році зріс до 0,9, так як значно збільшилася сума всіх показників дохідних активів банку. Упродовж наступних досліджуваних років коефіцієнт дохідності не опускався нижче встановленого у 2019 році рівня (0,9), що свідчить про високу дохідність активів банку у 2020-2022 роках.

Пасивами банку називають джерела формування фінансових ресурсів. За своїм походженням пасиви не однорідні, і складаються з капіталу та зобов'язань банку перед вкладниками та кредиторами. Капітал являє собою власні кошти банку, що належать засновникам або акціонерам, а зобов'язання – це чужі гроші, тимчасово надані власникам у розпорядження банку.

Специфічна особливість ресурсної бази банківської установи полягає в тому, що її основною частиною є залучені кошти. Вони складають переважну частку в загальній сумі банківських ресурсів комерційного банку. При цьому дуже важливо, щоб їх збільшення підтримувалося підвищенням рівня власних коштів, в протилежному випадку банк може втратити платоспроможність та стати банкрутом.

Залучені кошти поділяються на депозити та інші. Під депозитом розуміють зобов'язання банку по тимчасово залученим коштам фізичних та юридичних осіб за відповідну плату. До інших відносять кошти, які залучаються на міжбанківському ринку чи отримані за рахунок продажу на грошовому ринку довгострокових зобов'язань.

Динаміка показників пасиву АТ «А-Банк» наведена у табл. 2.2.

Дані табл. 2.2 засвідчують, що АТ «А-Банк» у період 2018-2022 років результативно виконував стратегічні завдання подальшого розвитку.

З наведених у табл. 2.2 даних можна побачити, що статутний капітал АТ «А-Банк» постійно поповнюється коштами. Розмір статутного капіталу у 2018 році складав 323 191 тис. грн, у 2019 році – 502 240 тис. грн, у 2020 році – 778 472 тис. грн, у 2021 році статутний капітал збільшився до 1 054 704 тис. грн, і залишився незмінним у 2022 році.

Динаміку нарощення статутного капіталу зображено на рис. 2.2.

Таблиця 2.2

Динаміка показників пасиву АТ «А-Банк»

№ п/п	Показники, тис. грн	Роки					Динаміка				
		2018	**2019**	**2020**	**2021**	**2022**	**2019/ 2018**	**2020/ 2019**	**2021/ 2020**	**2022/ 2021**	**2022/ 2018**
1	Статутний капітал	323 191	502 240	778 472	1 054 704	1 054 704	у 1,55 рази	у 1,55 рази	у 1,35 рази	1	у 3,26 рази
2	Нерозподілений прибуток	494 459	292 162	303 370	804 162	503 281	59,1%	у 1,04 рази	у 2,65 рази	62,6%	у 1,02 рази
3	Емісійний дохід	41	41	41	41	41	1	1	1	1	1
4	Резервні та інші фонди банку	64 140	91 522	104 328	127 834	172 106	у 1,43 рази	у 1,14 рази	у 1,23 рази	у 1,35 рази	у 2,68 рази
5	Інші резерви	25 513	35 056	48 384	46 828	63 526	у 1,37 рази	у 1,38 рази	96,8%	у 1,36 рази	у 2,49 рази
	Усього власного капіталу	**907 344**	**921 021**	**1 234 595**	**2 198 569**	**2 418 459**	у 1,02 рази	у 1,34 рази	у 1,78 рази	у 1,1 рази	у 2,67 рази
6	Кошти банків	-	11 143	47 666	90 812	179 040	-	у 4,28 рази	у 1,91 рази	у 1,97 рази	-
7	Кошти клієнтів	3 672 974	5 167 804	7 584 923	11 524 100	14 572 422	у 1,41 рази	у 1,47 рази	у 1,52 рази	у 1,26 рази	у 3,97 рази
8	Забезпечення винагород працівникам та інше	55 336	37 963	51 024	52 192	49 340	68,6%	у 1,34 рази	у 1,02 рази	94,5%	89,2%
9	Податкові зобов'язання (поточні та відстрочені)	5 211	6 781	44 356	94 030	33 938	у 1,3 рази	у 6,54 рази	у 2,12 рази	36,1%	у 6,51 рази
10	Інші фінансові та нефінансові зобов'язання	149 949	288 223	263 325	418 209	533 529	у 1,92 рази	91,4%	у 1,59 рази	у 1,28 рази	у 3,56 рази
	Усього зобов’язань	**3 941 911**	**5 511 914**	**7 991 294**	**12 179 343**	**15 368 269**	у 1,4 рази	у 1,45 рази	у 1,52 рази	у 1,26 рази	у 3,9 рази
	Усього пасивів	**4 849 255**	**6 432 935**	**9 225 889**	**14 377 912**	**17 786 728**	у 1,33 рази	у 1,43 рази	у 1,56 рази	у 1,24 рази	у 3,67 рази

Джерело: [додатки В, Г, Д, Е, Ж]

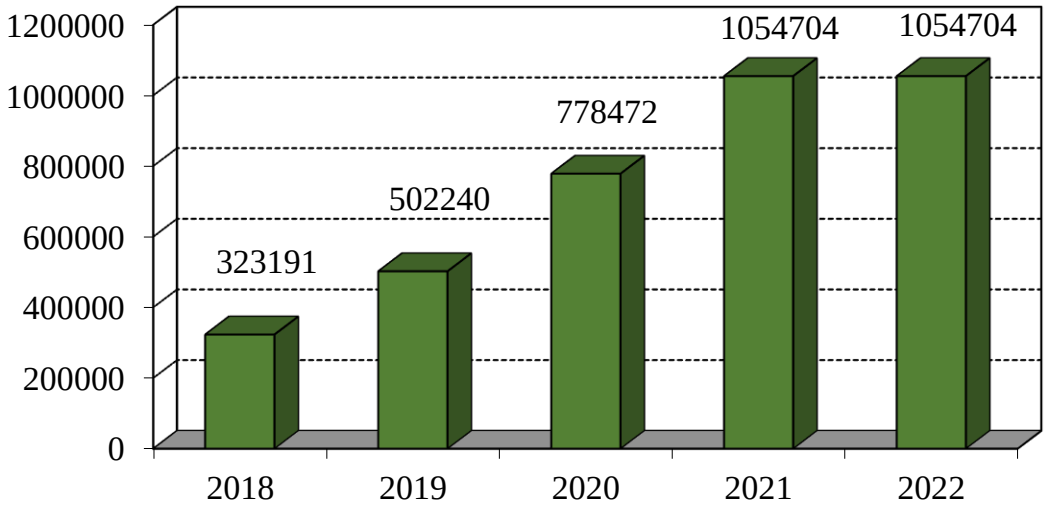

Рис. 2.2. Динаміка розміру статутного капіталу АТ «А-Банк» за 2018-2022 роки

Джерело: [додатки В, Г, Д, Е, Ж]

Статутний капітал займає 43,6% у структурі власного капіталу АТ «А-Банк», які за досліджуваний період 2018-2022 років сумарно збільшився у 2,67 рази тобто на 1 511 115 тис. грн. Отже, прибутковість діяльності банківської установи має позитивну динаміку.

У складі власного капіталу за досліджуваний період окрім статутного капіталу постійно зростають резервні та інші фонди банку. За період 2018-2022 років вони зросли у 2,68 рази, або на 107 966 тис. грн.

Загальне збільшення суми зобов'язань АТ «А-Банк» упродовж досліджуваного періоду склало 11 426 358 тис. грн (майже у 4 рази) з 3 941 911 тис. грн у 2018 році до 15 368 269 тис. грн у 2022 році.

Для наочності структури пасиву АТ «А-Банк» за 2022 рік за даними таблиці 2.2 побудуємо діаграму (рис. 2.3), з якої видно, що найбільшу частку пасиву банку займають кошти клієнтів (84,91%). Це говорить про високу довіру до банку і тенденції постійного збільшення банком свого клієнтського портфелю.

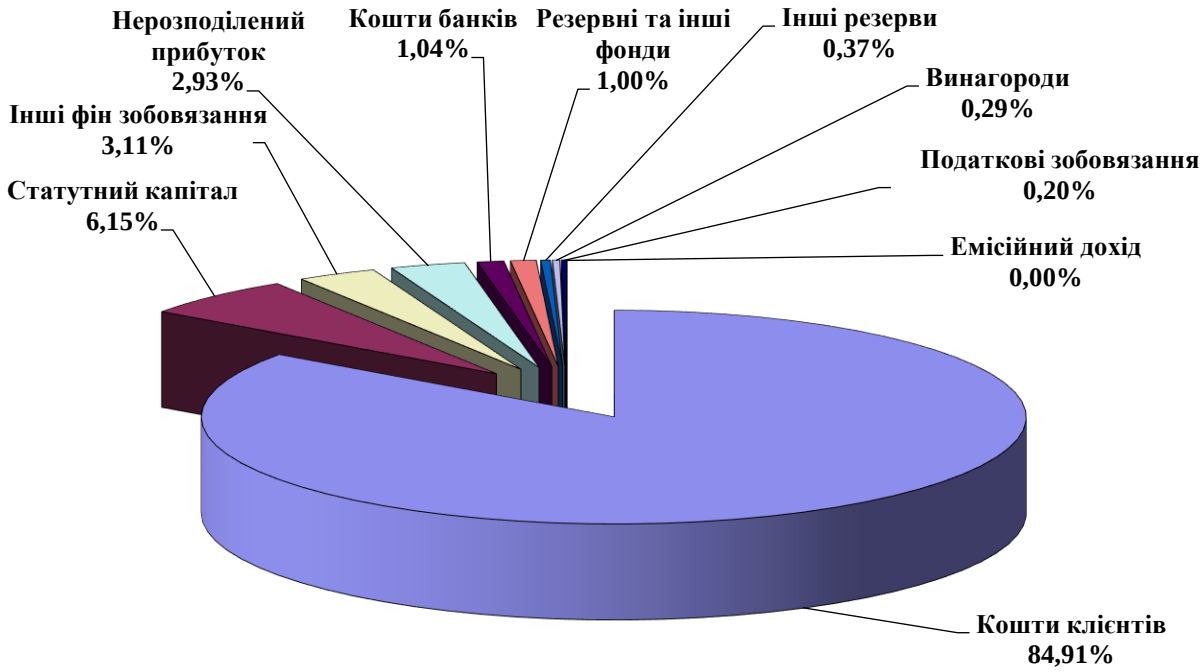

Рис. 2.3. Структура пасиву АТ «А-Банк» за 2022 рік

Джерело: проілюстровано автором за даними табл. 2.2.

Аналіз залишків готівкових коштів, коштів на кореспондентських рахунках, інвестицій в облігації внутрішньої державної позики та депозитних сертифікатах НБУ свідчить про достатній запас ліквідності АТ «А-Банк». Залишки на кореспондентських рахунках та у депозитних сертифікатах Національного банку на 01.01.2023 складають 6 541 597 тис. грн, що забезпечує безперебійні потреби у ліквідності Банку.

Станом на 01.01.2023 по коштах клієнтів спостерігалося значне збільшення (26% в цілому по портфелю: 16% по корпоративним клієнтам, 29% по фізичним особам) у порівнянні з довоєнним рівнем на 01.01.2022. Також спостерігається тенденція зміни у структурі коштів клієнтів, а саме зниження частки строкових на користь поточних та карткових рахунків клієнтів. Обсяг депозитів фізичних осіб з 01.01.2022 по 31.12.2022 збільшився на 560 413 тис. грн, а залишки на поточних рахунках збільшились за даний період на 2 117 701 тис. грн. Відтоку коштів клієнтів юридичних осіб станом на 31.12.2022 року порівняно з залишками на 31.12.2021 року також не відбулося ні за строковими (+42%), ні за поточними рахунками (+6%).

Ліквідність банку на 01.01.2023 є достатньою, Банк дотримується всіх встановлених нормативних вимог регулятора. Станом на 01.01.2023 р. значення коефіцієнта покриття ліквідності (LCR) за всіма валютами становить - 1 207%, на іноземними валютами - 457%, значення коефіцієнта чистого стабільного фінансування (NSFR) - 179%.

Аналіз нормативів ліквідності банку за період 2018-2022 років показав, що АТ «А-Банк» у зазначений період здатний забезпечити своєчасне виконання своїх грошових зобов'язань, що визначається збалансованістю між строками і сумами погашення розміщених активів та строками і сумами виконання зобов'язань банку, а також строками і сумами інших джерел та напрямків використання коштів.

Аналіз невідповідностей за строками до погашення активів та пасивів свідчить, що рівень ліквідності не перевищував рекомендовані НБУ межі (не більше – 10% загальних активів). Зазначена від'ємна невідповідність між активами та пасивами не несе значного навантаження на стан ліквідності Банку.

Отже, з вище приведеного аналізу діяльності АТ «А-Банк», можна зробити наступні висновки:

– принципи формування резервів та регулятивний капітал банку відповідають нормативним вимогам Національного банку України;

– відзначається достатність резервів капіталу банківської установи АТ «А-Банк»;

– якість управління активами і пасивами АТ «А-Банк» є задовільною;

– керівництво банківської установи АТ «А-Банк» на належному рівні забезпечує управління активами і пасивами з орієнтацією на прибутковість операцій та підтримування ліквідності балансу;

– наведені дані свідчать про помірну збалансованість за строками погашення та розміщення активів та зобов'язань АТ «А-Банк»;

– рівень ліквідності та платоспроможності банківської установи АТ «А-Банк» є достатнім;

– наявність негативної невідповідності між активами і пасивами не несе

значного навантаження на стан ліквідності банківської установи;

– банківській установі АТ «А-Банк» необхідно здійснювати постійний контроль за забезпеченням певної частки ліквідних активів у загальній структурі балансу.

АТ «А-Банк» не дивлячись на форс-мажорні обставини, викликані воєнним активно розвиває та впроваджує нові послуги та банківські продукти для фізичних і юридичних осіб, маючи на меті розширення переліку послуг, що надаються клієнтам банку, якомога повне задоволення їх потреб та сподівань, а також охоплення тих сегментів ринку банківських послуг, в яких він досі не був представлений.

Аналіз організаційної структури управління «А-Банку» та оцінка розподілу відповідальності у сфері кадрової безпеки дозволяє зробити висновок, що характерною рисою ОСУ є чітка та зрозуміла ієрархічна структура, яка підтримує ефективність управління кадровою безпекою.

Важливим завданням оцінки діючої системи управління кадровою безпекою є аналіз внутрішніх процесів, спрямованих на управління кадровою безпекою, включаючи планування, виконання та контроль. З цією метою проведемо оцінку ефективності та оптимізації процесів для забезпечення високої якості управління кадровою безпекою; аналіз використання технологій та інформаційних систем в процесі управління кадровою безпекою; оцінку рівня комунікації та співпраці між відділами, які мають відношення до кадрової безпеки; аналіз систем звітності та моніторингу, які використовуються для оцінки результатів та ефективності управління кадровою безпекою; а також визначимо рівень інтеграції кадрової безпеки в загальні стратегії розвитку «А-Банку».

Такий всебічний аналіз дозволить визначити сильні та слабкі сторони системи управління кадровою безпекою в АТ «А-Банк», оцінити фактори та невикористанні резерви впливу та розробити і запропонувати програму заходів у напрямку вдосконалення діючої системи управління кадровою безпекою.

2.2. Оцінка системи управління кадровою безпекою АТ «А-Банк»

Для здійснення комплексної оцінки ефективності системи управління кадровою безпекою в АТ «А-Банк» використаємо теоретичні підходи та метрики, які були детально розглянуті у розділі 1 кваліфікаційної роботи. Аналіз інформації, розрахунок показників та порівняння їх зі стандартами і кращими практиками допоможе визначити сильні та слабкі сторони, а також розробити пропозиції щодо удосконалення системи управління кадровою безпекою для АТ «А-Банк».

З урахуванням особливостей діяльності банку та впливу зовнішніх факторів на кадрову безпеку в умовах воєнного стану, головну увагу сфокусуємо на таких характеристиках:

1. Відповідність законодавству та стандартам: перевірка, наскільки організація відповідає вимогам та стандартам з кадрової безпеки.
2. Технічні заходи кібербезпеки: ефективність заходів, спрямованих на захист інформаційних ресурсів від кіберзагроз.
3. Рівень свідомості та підготовленості персоналу: участь працівників у тренінгах з кадрової безпеки; рівень обізнаності персоналу щодо потенційних загроз та процедур безпеки.
4. Рівень звітності та аналізу інцидентів: якість системи звітності про інциденти та їхній подальший аналіз для уникнення повторення подій.
5. Ефективність систем внутрішнього контролю та аудиту: результати аудитів та внутрішнього контролю щодо кадрової безпеки.
6. Інтеграція кадрової безпеки в загальні стратегії банку: вплив кадрової безпеки на стратегічні цілі та розвиток банку.
7. Застосування інновацій та новітніх технологій: використання сучасних технологій для покращення системи управління кадровою безпекою.

Стратегія розвитку АТ «А-Банк» на 2023-2025 роки спрямована на здійснення головної місії, яка полягає у забезпеченні клієнтів безперервним обслуговуванням у період турбулентності зі збереженням прибуткової

діяльності банку [35]. Генеральна мета сформульована як досягнення 1 млн. активних задоволених клієнтів (Додаток И).

Вся діяльність банку сконцентрована на головних аспектах кібербезпеки і забезпечені стабільної роботи банку за рахунок удосконалення системи протидії кібератакам, а саме:

- відсутність прямих збитків від кібератак;
- моніторинг критичної інфраструктури 24/7 з дотриманням KPI;
- взаємодія з регуляторними органами з метою обміну інформацією щодо актуальних загроз та спільної їх нейтралізації [35].

В межах ризик-культури, яка сформована та ефективно діє в контексті кадрової політики банку, ризик трактується як потенційна можливість виникнення збитків або недоотримання доходів або зменшення ринкової вартості капіталу «А-Банку» внаслідок несприятливого впливу зовнішніх або внутрішніх факторів. У банку впроваджений принцип своєчасного виявлення, пом'якшення та уникнення ризиків у банківських процесах та процедурах.

Стандартом корпоративної ризик-культури є участь всіх працівників банку в межах компетенції у виявленні ризиків, які можуть завдати потенційну шкоду процесам, клієнтам, іміджу банку, здійсненні їх оцінки, доведенні інформації про виявлені ризики до уповноважених підрозділів для вжиття управлінських заходів з метою мінімізації можливих негативних наслідків.

Працівник Банку у межах корпоративної ризик-культури зобов'язаний:

– забезпечити дотримання принципу законності під час виконання трудових обов'язків та спілкування з іншими особами;

– виявляти ризики в межах своєї компетенції;

– повідомляти банк про виявлені ризики, інциденти, порушення положень «Кодексу корпоративної етики та поведінки» з боку працівників банку та інших осіб шляхом направлення повідомлення до Департаменту управління операційним ризиком через канал «Гаряча лінія: Шахрайство», або на електронну пошту керівника Департаменту управління операційним ризиком, або до підрозділу комплаєнсу, а також надавати цим підрозділам всю необхідну

інформацію для попередження порушень, мінімізації або попередження збитків чи недоотримання доходів;

– ініціювати отримання рекомендацій уповноважених підрозділів Банку (підрозділ управління ризиками та підрозділ комплаєнсу) з питань запобігання виникненню ризиків;

– вносити пропозиції щодо уникнення виявлених ним ризиків;

– ініціювати управлінські заходи з метою мінімізації можливих негативних наслідків за підконтрольними йому процесами, або доводити інформацію до власника процесу затвердженими каналами комунікації [18].

Кодексом корпоративної етики та поведінки АТ «А-Банк» передбачений механізм захисту інформації (Додаток К). Будь-яка інформація, у тому числі інформація про працівників Банку, внутрішню структуру, фінансові потоки, плани діяльності, зміну тарифів, керівництва, вчинення угод, здійснення операцій тощо, за винятком загальнодоступної інформації, є інформацією з обмеженим доступом.

Обсяг інформації, що надається клієнтам, діловим партнерам, державним органам та порядок її надання визначається законодавством України, договором чи внутрішніми документами банку.

Клієнти Банку та ділові партнери повинні бути впевнені, що інформація про них та їхню діяльність вважається інформацію з обмеженим доступом та не підлягає розголошенню, за винятком випадків, передбачених законодавством України, або умовами договорів [18].

Менеджмент банку відповідально ставиться до захисту інформації, здійснюючи наступні заходи:

а) дотримується правил конфіденційності щодо інформації, отриманої від клієнтів та інших осіб (ділові партнери, підрядники та інші);

б) не допускає розповсюдження неправдивої інформації, викривлення фактів, що може завдати шкоди банку, його клієнтам, діловим партнерам та іншим особам;

в) захищає власну інформацію: інформація використовується

співробітниками банку виключно для виконання трудових обов’язків і може бути розкрита або передана іншим особам тільки в обсязі та в порядку, що передбачені чинним законодавством України та внутрішніми документами банку;

г) зберігає персональні дані співробітників у режимі конфіденційності; збирання та оброблення персональних даних здійснюється з дотриманням вимог законодавства.

В свою чергу співробітники «А-Банку» в межах принципів Кодексу корпоративної етики та поведінки:

а) забезпечують у встановленому законодавством України порядку зберігання, захист, використання та розкриття банківської таємниці, а також у встановленому банком порядку зберігання, захист, використання та розкриття комерційної таємниці, інсайдерської або іншої конфіденційної інформації та відомостей, які стали відомими у зв’язку із виконанням трудових обов’язків;

б) не діляться інформацією про діяльність Банку, яка не була у встановленому законодавством порядку розкрита або оприлюднена, з будь-ким, включаючи родичів та друзів, крім випадків, коли це становить частину трудових обов’язків;

в) отримують, передають, зберігають, знищують інформацію відповідно до законодавства та внутрішніх документів банку;

г) використовують комп’ютерні системи та обладнання банку з дотриманням встановлених банком заходів безпеки та внутрішнього контролю;

д) не передають своє ім’я користувача або паролі до програмних комплексів банку іншим особам і не дозволяють їм користуватися своїми робочими комп’ютерами;

е) у випадку спроби з боку інших осіб чи інших працівників банку одержати відомості, що відносяться до банківської та комерційної таємниці чи конфіденційної інформації, повинні негайно сповістити про це свого безпосереднього лінійного керівника;

ж) зобов’язуються не використовувати знання банківської та комерційної таємниці, інсайдерської або іншої конфіденційної інформації банку, його

клієнтів, ділових партнерів, інших осіб для занять будь-якою діяльністю, що в якості конкурентної дії може завдати їм шкоди, з метою отримання переваг чи надання таких переваг іншим особам, в особистих цілях чи на користь інших осіб та в інших цілях, не пов'язаних із виконання трудових обов'язків [18].

У випадку припинення трудового договору усі носії з інформацією, що є банківською або комерційною таємницею (рукописи, чернетки, диски, дискети, роздруківки на принтерах тощо), що перебували у користуванні працівника у зв'язку з виконанням ним трудових обов'язків, працівник зобов'язується передати безпосередньому лінійному керівнику не пізніше, ніж за добу до останнього робочого дня.

У випадку втрати або пошкодження носіїв з інформацією, перепусток, ключів від приміщень банку, або про факти, що можуть призвести до розголошення банківської, комерційної таємниці чи конфіденційної інформації, а також про причини й умови можливого витоку відомостей, співробітник негайно повідомляє безпосередньому керівнику.

У період дії трудового договору та після його припинення безстроково, тобто без обмеження строку зберігання таємниці, працівники зобов'язані дотримуватися режиму банківської таємниці або конфіденційності інформації щодо інформації банку, її клієнтів, контрагентів ділових партнерів та інших осіб, яка стала їм відомою під час виконання трудових обов'язків, і вживати заходів для запобігання її несанкціонованому розкриттю [18].

Важливою складовою системи управління кадровою безпекою банку є розроблена процедура повідомлення про порушення. Відповідно до встановленої процедури співробітник банку зобов'язаний невідкладно, але не пізніше одного робочого дня, з дня, коли працівнику стало про це відомо, повідомляти підрозділ комплаєнсу банку про можливі, заплановані, поточні або здійснені дії з боку інших працівників Банку, клієнтів, ділових партнерів, посадових осіб державних органів та інших осіб, що порушують законодавство, положення Кодексу корпоративного управління або інших внутрішніх нормативних документів банку.

Клієнти, ділові партнери, посадові особи та інші особи, які не є працівниками банку, можуть направляти повідомлення про заплановані, поточні або здійснені порушення законодавства, Кодексу корпоративного управління або інших внутрішніх нормативних документів банку з боку працівників банку, інших клієнтів, ділових партнерів та інших осіб. Повідомлення про порушення законодавства, Кодексу та внутрішніх документів банку можна направляти під власним ім'ям або на умовах анонімності [30].

«А-Банк» заохочує практику оперативного та конфіденційного інформування про випадки порушення законодавства, Кодексу та будь-яких інших випадків неетичної поведінки чи інших дій з боку працівників Банку, які можуть зашкодити інтересам банку, створюють загрозу виникнення іміджевих ризиків або спричинення йому збитків.

Менеджмент банку забезпечує нерозголошення інформації про осіб, які повідомляють про порушення, а також недопущення переслідування, утиску або застосування до цих осіб інших негативних наслідків, якщо такі особи особисто не вчиняли правопорушень, за які законом передбачена кримінальна відповідальність та в інших, передбачених законом випадках, якщо розкриття такої інформації є обов'язковим для запобігання порушенню чи відновлення прав і інтересів банку, його клієнтів, інших осіб чи держави. Банк забезпечує перевірку усіх повідомлень про порушення законодавства чи Кодексу корпоративного управління, в тому числі здійснених на умовах анонімності. Разом з тим, банк вважає неприпустимим та таким, що порушує принципи корпоративної етики, повідомлення свідомо неправдивої інформації про порушення з боку працівників [18].

В межах системи управління кадровою безпекою «А-Банк» створив основні канали направлення персоналізованих повідомлень про порушення, а саме:

- система внутрішнього електронного документообігу Банку;
- банківська електронна скринька лінійного керівника;
- банківська електронна скринька підрозділу комплаенс - compliance@a-

bank.com.ua;

- банківські електронні скриньки керівників підрозділу комплаєнсу, підрозділу управління операційним ризиком або підрозділу «Служба безпеки» банку;

- гаряча лінія «Шахрайство» - для направлення конфіденційного повідомлення про порушення.

Для клієнтів банку та ділових партнерів передбачені окремі канали направлення повідомлень про порушення: телефон служби підтримки 7776 (цілодобово, безкоштовно з мобільних в межах України); телефон +380567220555 (для дзвінків з-за кордону); електронна поштова скринька help@a-bank. com.ua; електронна скринька підрозділу комплаєнс (compliance@a-bank.com.ua) [18].

Основою побудови системи управління кадровою безпекою «А-Банку» стали корпоративні цінності. Вони характеризують принципи ведення бізнесу, забезпечують реалізацію стратегії розвитку банку, створення та збереження його ділової репутації. Корпоративними цінностями «А-Банку» є:

1. Клієнти.

Цінність клієнтів підтверджується наданням допомоги у контексті знаходження правильних фінансових рішень, пропозиції послуг та продуктів, що відповідають потребам клієнтів, а також наданням зручного обслуговування і корисних сервісів.

2. Працівники.

Менеджмент банку дбає про своїх співробітників, створюючи умови для повної реалізації їхнього потенціалу, можливостей кар'єрного зростання і професійного розвитку. Система HR-менеджменту побудована на принципах чесності, відкритості, ввічливості і позитиву у спілкуванні, творчості, ініціативності, креативності та лідерства.

3. Технологічність.

АТ «А-Банк» постійно розвивається, створює інноваційне середовище в умовах діджиталізації, впроваджує новітні технології і пропонує ефективні

технологічні рішення.

4. Якість.

Місією банку є забезпечення високої якості здійснення банківських операцій, створюючи високі стандарти якості продуктів та обслуговування клієнтів.

5. Ощадливість.

Така цінність досягається за рахунок відповідального і дбайливого ставлення до власного робочого часу, робочого часу співробітників, партнерів і клієнтів.

6. Відкритість до діалогу.

Персонал банку цінує відкритий і чесний обмін інформацією, завжди демонструє готовність спільно знаходити оптимальні рішення.

Дотримання названих цінностей і підтримка принципів корпоративної культури гарантує досягнення найкращих результатів діяльності банку.

Умови воєнного стану значно вплинули на стратегію розвитку українських банків, АТ «А-Банк» не став виключенням. Важливим досягненням менеджменту банку стала доступність і безперервна робота відділень. Станом на 01.01.2023р. банківська мережа становила 200 відділень (16 відділень знаходяться на окупованих територіях та в зоні бойових дій). Характерною рисою воєнного періоду стала оптимізація 20% відділень діючої мережі, скорочення неефективних відділень у зв'язку зі зменшенням клієнтопотоку та переходом в on-line. Автономність функціонування досягається за рахунок формування мережі ефективних відділень з альтернативними джерелами енергії та резервними каналами зв'язку. 83 відділення «А-Банку» входять до державної об'єднаної мережі «Power banking» та забезпечені 100% альтернативним електроживленням, а також 57% із них вже підключено до альтернативних каналів зв'язку [28; 35].

Головні вектори стратегічних змін в умовах непередбачуваності мають наступний вигляд.

1. Подолання ризиків та збереження стабільності.

Воєнний стан супроводжується великими ризиками, такими як економічна нестабільність, падіння довіри до банківської системи, коливання попиту та трансформації регуляторного середовища. За таких умов «А-Банк» враховує ці ризики в процесі вибору стратегії розвитку та вживає заходи для забезпечення стабільності та мінімізації ризиків.

2. Механізм кредитування та управління ризиковими активами.

Умови воєнного стану супроводжуються змінами ринкової ситуації, попиту та платоспроможності клієнтів. Банк посилив вимоги при наданні кредитів та управлінні ризиками, оцінює потенційні ризики, які зв’язані з падінням платоспроможності вкладників та вживає відповідні заходи для їх мінімізації.

3. Трансформація поведінки клієнтів та попиту на банківські продукти.

Під час воєнного стану «А-Банк» відчув негативний вплив на попит та поведінку клієнтів. Менеджмент банку адаптувався до зміни потреб та очікувань клієнтів, а саме розширив асортимент послуг, розробив додаткові фінансові послуги для підтримки бізнесу та вкладників.

4. Місце у процесі фінансування вітчизняної економіки.

В умовах воєнного стану «А-Банку» відводиться важливу місце у процесі фінансування вітчизняної економіки. Менеджмент банку активізував співпрацю з урядом і регуляторними органами з метою утримання стабільності фінансової системи та підтримки розвитку ключових галузей.

5. Кризове управління та ризик-менеджмент.

З початку воєнного стану «А-Банк» розробив ефективні кризові управлінські стратегії. Банк готовий до швидкого реагування на виклики кризової ситуації, забезпечення стабільності функціонування на захисті інтересів клієнтів.

«А-Банк» розробив свою унікальну стратегію розвитку в умовах воєнного стану з врахуванням наявних ресурсів, етапу розвитку, викликів і загроз.

АТ «А-Банк» в умовах невизначеності продемонстрував свою гнучкість у керуванні залученням вкладів (конкурси, акції, мотивація персоналу),

адаптивність та уміння швидко реагувати на виклики та загрози, стабільність та успішний розвиток банку (сервіси для зручності та довіри клієнтів: замовлення валюти в «А-Банк 24», скасування пролонгації на будь-якому терміні вкладу, спрощення продуктового ряду).

Актуальні стратегічні вектори, цілі та показники розвитку АТ «А-Банк» до 2025 року візуалізовані на рисунку 2.4.

Рис. 2.4. Стратегічні вектори, цілі та показники діяльності АТ «А-Банк»

Джерело: проілюстровано автором з використанням джерел [28; 35]

Пріоритетними стратегічними векторами залишаються посилення системи управління ризиками, зростання обсягів кредитування за рахунок виваженої кредитної політики, а також розширення бізнесу з клієнтами за рахунок

отримання місця в ТОП-5 по впізнаваності бренду «А-Банк».

Ключові стратегічні орієнтири характеризуються через систему показників: зниження вартості ризику (COR - Cost of Risk) до 9,2% (з 23,85% у 2023 році т.т. на 14,65 пунктів); підвищення дохідності власного капіталу (ROE - Return on Equity) до 14,18%; підвищення рентабельності активів (ROA - Return on Assets) до 1,79%; зниження співвідношення витрат до доходів (CIR - Cost/Income Ratio) до 58%; скорочення частки непрацюючих кредитів (NPL - Non-performing loan) на 13,6% у порівнянні з 2023 роком; збільшення чистого процентного доходу (NII - Net Interest Income) до 2 550 млн. грн; утримання рівня індексу підтримки вкладників (NPS - Net Promoter Score) на позначці 88%.

АТ «А-Банк» визнав відчутні кредитні втрати з початку повномасштабної війни. Оцінка потенційних втрат кредитного портфеля через форс-мажорні обставини становить 35%. Банк прогнозує забезпечити стійкість за рахунок своєчасної оцінки кредитного ризику, а також здійснення раціональної реструктуризації. Актуальне завдання, яке сьогодні поставлено перед менеджментом «А-Банку» полягає в розробці стратегії скорочення частки непрацюючих кредитів (NPL–Non-performing loan) з урахуванням положень, прийнятих Радою з фінансової стабільності.

Головною цінністю банку є людський капітал і фокус на співробітниках став пріоритетним напрямком за останні два роки. Команда «А-Банку» швидко адаптувалася до страшних викликів, які супроводжувалися карантином у 2021 році та форс-мажорними обставинами, які спричинила війна. Першочерговим завданням менеджменту банку з лютого 2022 року стала розробка та здійснення програми релокації та збереження персоналу.

Протягом 2018-2022 років чисельність персоналу скоротилась з 2396 до 1912 осіб (484 особи або на 20%). Причинами такої плинності стали фактори зовнішнього впливу. Отже в теперішніх умовах банк взяв курс на розвиток персоналу шляхом складання індивідуальних планів розвитку співробітників, виявлення потенціалу і формування кадрового резерву (особлива увага до позицій системних аналітиків). Важливою складовою менеджменту персоналу є

система професійного розвитку персоналу. «А-Банк» систематично забезпечує своїх співробітників необхідним рівнем професійних знань, навичок та компетентностей. У системі HR-менеджменту здійснюються програми з підготовки кадрового резерву з метою оперативного закриття вакантних посад.

Основні методи професійного розвитку персоналу «А-Банку» описані на рисунку 2.5.

Рис. 2.5. Методи професійного розвитку персоналу АТ «А-Банк»

Джерело: проілюстровано автором з використанням джерел [28; 30; 34; 35]

Персонал «А-Банку» – це кваліфіковані професіонали, які налаштовані професійно розвиватись, вдосконалювати свої компетентності, готові до інновацій та організаційних змін. В сьогоднішніх умовах команда працює над здійсненням стратегії інноваційного розвитку та забезпечення кадрової безпеки.

Протягом 2021-2022 рр. відбулося відчутне омолодження персоналу банку:

43% штату персоналу – це молоді люди віком від 30 до 40 років, 20% з них посідають позиції керівників структурних підрозділів різного рівня.

Статево-віковий та освітній профіль персоналу «А-Банку» проілюстрований на рисунку 2.6.

Рис. 2.6. Статево-віковий та освітній профіль персоналу АТ «А-Банк»

Джерело: проілюстровано автором з використанням джерел [28; 35]

Результати оцінки системи управління кадровою безпекою АТ «А-Банк» доводять, що в сучасну кадрову стратегію банку закладається новітня філософія стосунків із співробітниками, в якій акцентується увага на збереженні персоналу; гарантіях безпеки та підтримці персоналу; високих професійних досягненнях; підвищені рівня лояльності та залученості персоналу, організації ефективного

зворотного зв’язку; визначення та задоволення потреб кожного співробітника.

В результаті дослідження стратегії розвитку АТ «А-Банк» можна зробити висновки щодо трансформації напрямку стратегічного розвитку і типу кадрової політики банку. Зміни відбулися у посилені превентивності кадрової політики. Це означає, що менеджмент банку активно використовує інструменти діагностики кадрової ситуації та своєчасного впливу на негативні прояви. Служба управління персоналом банку здійснює моніторинг якісних і кількісних показників кадрової безпеки, аналізує причини погіршення кадрової ситуації, і впроваджує програми заходів щодо локалізації негативних ситуацій в системі управління персоналом.

У підсумку зазначимо, що діюча система управління кадровою безпекою банку, з одного боку характеризується позитивними аспектами, а саме високою лояльністю та підготовленістю персоналу, які варто зберегти та підтримувати. З іншого боку, слабкими сторонами є: відсутність інтегрованої стратегії кадрової безпеки; потреба в удосконаленні технічних засобів для кібербезпеки; недостатня ефективність системи внутрішнього контролю та аудиту.

Отже, першочергові завдання для посилення ефективності системи управління кадровою безпекою АТ «А-Банк» полягають у: розробці інтегрованої стратегії, орієнтованої на стратегічні цілі банку; покращені технічних засобів для захисту інформаційних ресурсів і даних клієнтів; забезпечені ефективності систем внутрішнього контролю та аудиту.

РОЗДІЛ 3
ПРОПОЗИЦІЇ ЩОДО УДОСКОНАЛЕННЯ СИСТЕМИ УПРАВЛІННЯ КАДРОВОЮ БЕЗПЕКОЮ БАНКІВСЬКОЇ УСТАНОВИ

3.1. Впровадження сучасних методів діагностики кадрової небезпеки в систему банківського менеджменту

Діагностика рівня кадрової небезпеки - це процес системного оцінювання та аналізу різних аспектів, які можуть становити ризики для безпеки персоналу та діяльності банківської установи в цілому. Цей процес дозволяє ідентифікувати потенційні загрози, виявляти слабкі місця в системі управління кадровою безпекою та розробляти ефективні стратегії їх подолання.

Серед великої кількості багатоаспектних підходів до діагностики рівня кадрової небезпеки, сфокусуємось на найбільш ефективних для впровадження в практику менеджменту АТ «А-Банк».

1. Кваліативний підхід, заснований на зборі якісної інформації через інтерв'ю, фокус-групи та аналіз документів. Дозволяє отримати глибоке розуміння проблем та сприяє розробці індивідуалізованих стратегій, проте характеризується незначною об'єктивністю та складністю кількісного вимірювання.

2. Кількісний підхід використовує числові дані та метрики для оцінки рівня кадрової небезпеки. Розрахунок конкретних числових оцінок полегшує порівняння та аналіз, проте кількісний підхід не враховує контекстуальні та якісні аспекти.

3. Комбінований підхід покликаний поєднувати якісні та кількісні методи для отримання всебічної характеристики ситуації. Об'єднує переваги кваліативного та кількісного підходів та надає комплексну інформацію, проте вимагає більше фінансово-технічних ресурсів та часу для здійснення.

4. Бенчмаркінг, в основі якого застосовується порівняння власних показників з аналогічними показниками інших організацій чи галузей. Дозволяє

визначити рівень ефективності та конкурентоспроможності у порівнянні з банківськими установами. Відчутний недолік криється у можливій обмеженості щодо доступності порівняльних даних.

5. Технологічний підхід передбачає застосування технологічних рішень, таких як аналіз Big Data, машинне навчання для обробки та аналізу великих обсягів даних. Дозволяє ефективно обробляти великі обсяги даних та виявляти конкретні патерни, проте вимагає високої технічної підготовки та відчутної фінансової підтримки.

Кожний із запропонованих підходів є доцільним для використання в практичні діяльності «А-Банку», оскільки враховує специфіку внутрішнього бізнес-середовища банківської установи, її стратегічні цілі та кадрову ситуацію. Проте найбільш ефективною для отримання повної та точної карти рівня кадрової небезпеки вважається комбінація різних методів.

Враховуючи цінності корпоративної культури, які притаманні «А-Банку» детальніше розглянемо напрямки побудови ефективного механізму діагностики рівня кадрової небезпеки банку.

Ефективний механізм діагностики має починатись з проведення аудиту персоналу, сутність якого полягає у перевірці відповідності працівників встановленим стандартам та кваліфікаційним вимогам.

Ґрунтовний аналіз компетенцій, дій та відповідальності працівників з метою визначення їхньої відповідності вимогам безпеки пропонується здійснювати шляхом систематичного спостереження та перевірки якості виконання посадових обов’язків, а також за допомогою аналізу результатів тренінгів та семінарів з питань безпеки.

Проведення аудиту персоналу дозволяє ідентифікувати компетенції та слабкі сторони працівників, які можуть негативно впливати на безпеку. Серед недоліків слід підкреслити залежність від добросовісності та дбайливості персоналу під час аудиту.

В результаті аудиту персоналу менеджмент банку має можливість виявити слабкі місця та ризикові зони в компетенціях працівників і на цій основі

розробити індивідуальні або групові тренінги для підвищення культури безпеки.

Отже, така складова механізму діагностики рівня кадрової небезпеки банку як аудит персоналу дозволяє не лише оцінити компетенції працівників, але й ідентифікувати їхні дії та відповідальність у сфері безпеки, що вкрай важливо для управління кадровою безпекою банківської установи.

Важливою складовою механізму діагностики є оцінка внутрішньої лояльності та задоволеності персоналу. Вивчення рівня залученості працівників, їхнього задоволення роботою та внутрішньою атмосферою доцільно здійснювати методами опитування, анкетування, фокус-групи, інтерв'ю та групових дискусій для деталізації відповідей персоналу.

Вивчення рівня задоволення та лояльності працівників щодо робочих умов, корпоративної культури та стратегії управління допомагає виявити фактори, які впливають на мораль та етику працівників. Проте, варто враховувати значний вплив суб'єктивізму в процесі індивідуальних оцінок працівників.

Результати оцінки внутрішньої лояльності та задоволеності персоналу будуть корисними для виявлення елементів робочого оточення, які можуть впливати на відданість та безпеку працівників з метою розробки стратегії поліпшення робочих умов та підвищення лояльності.

Отже, оцінка внутрішньої лояльності та задоволеності персоналу дозволяє зрозуміти, наскільки працівники віддані своїй установі та як це може впливати на їхню поведінку щодо безпеки.

Останнім часом все більшої актуальності набуває така складова механізму діагностики як моніторинг соціальних мереж та відкритих джерел. Цей процес включає в себе спостереження за активністю в Інтернеті, аналіз публічної інформації, та виявлення можливих загроз або ризиків, які можуть виникнути через дії співробітників чи зовнішні особи. Відстеження публікацій, систематичний аналіз публічної інформації та активностей працівників в соціальних мережах та інших відкритих джерелах дає можливість вчасно виявити можливі загрози та ризики.

На даному етапі корисним буде використання спеціалізованих програм для моніторингу соціальних мереж та відслідковування публічних профілів. Переваги таких методів полягають у виявлені небезпечних практик, які можуть виникнути через необережне ведення працівниками власних профілів, а також у можливості відстеження зовнішнього сприйняття банку через коментарі та обговорення працівників. Разом з тим, варто звернути увагу на певні обмеження у вигляді питань щодо приватності працівників.

Результати моніторингу доцільно використовувати для виявлення можливих порушень вимог безпеки, які можуть бути пов’язані з публічною активністю працівників, з метою розробки стратегії для підвищення усвідомленості працівників щодо віртуальної безпеки.

Отже, моніторинг соціальних мереж та відкритих джерел – це корисний інструмент для попередження можливих загроз та виявлення ризиків, пов’язаних з діяльністю працівників у віртуальному просторі.

Важливим аспектом управляння кадровою безпекою є оцінка цінностей, етики та норм поведінки в організації, що впливає на ступінь внутрішніх конфліктів, виникнення шахрайства та інші ризики. З цих позицій аналіз організаційної культури та ефективності внутрішніх процесів, як складова механізму діагностики виконує визначальну функцію.

Дослідження цінностей, норм, уявлень та способів взаємодії серед працівників в банківській установі доцільно здійснювати методами опитування, спостереження, аналізу документів. Аналіз організаційної культури дозволяє виявити особливості робочого середовища, які можуть впливати на кадрову безпеку; негативні аспекти культури, які можуть призводити до внутрішніх конфліктів чи погіршення моралі.

На етапі оцінки ефективності внутрішніх процесів визначають позитивні та негативні аспекти організаційної культури, які можуть впливати на кадрову безпеку з метою розробки стратегії поліпшення культурних аспектів та зменшення можливих загроз. При цьому важливо враховувати певний суб’єктивізм оцінок, оскільки вони спираються на сприйняття працівників.

Отже, аналіз організаційної культури допомагає розкрити психологічні та соціальні аспекти робочого середовища, що може впливати на кадрову безпеку. Результатом оцінки ефективності внутрішніх процесів може стати виявлення негативного ставлення до звітності про можливі порушення серед працівників, що може вказувати на проблеми внутрішнього контролю та збільшувати ризик фінансових махінацій.

Оцінка ефективності системи кібербезпеки як підхід до діагностики рівня кадрової небезпеки передбачає перевірку та аналіз існуючої системи кібербезпеки з метою виявлення слабких місць та потенційних загроз; виявлення недостатньої уваги до обов'язкових процедур аутентифікації та авторизації серед працівників, що може призвести до неправомірного доступу до системи.

Аналіз заходів, які прийняті для захисту інформації від кібератак та витоків даних слід здійснювати шляхом пентестування (тесту на проникнення), аудиту систем безпеки, моніторингу інцидентів для виявлення неправомірних дій працівників. Такі заходи дозволяють визначити рівень захищеності від кіберзагроз, які можуть виникати через працівників, а також виявити проблеми у кібербезпеці, які можуть бути викликані недбалістю персоналу. Проте, слід враховувати обмежений фокус лише на технічних аспектах безпеки, не враховуючи людського фактору повністю і особливі вимоги присутності експертів з кібербезпеки для аналізу та розробки рекомендацій.

У підсумку варто підкреслити, що оцінка ефективності системи кібербезпеки в контексті діагностики кадрової небезпеки допомагає ідентифікувати можливі загрози, які можуть виникнути через недостатню кібергігієну чи недбалість персоналу. Визначення рівня загрози, яку працівники можуть становити для кібербезпеки дає можливість вчасно розробити та впровадити заходи для підвищення свідомості працівників і поліпшення їхньої кібергігієни.

Характеристика складових елементів, методичні інструменти здійснення діагностики та напрями використання результатів діагностики систематизовано в таблиці 3.1.

Таблиця 3.1

Характеристика елементів ефективного механізму діагностики рівня кадрової небезпеки «А-Банку»

Елемент механізму	Сутність	Інструменти	Переваги	Недоліки	Використання результатів
Аудит персоналу	Оцінка знань, навичок та дій персоналу	Перевірка резюме, інтерв'ю, аналіз компетенцій та фахових навичок	Виявлення ризикових зон при виконані персоналом процедур та стандартів безпеки	Залежність від добросовісності персоналу Не враховує навмисні дії та недбалість працівників	Визначення слабких місць та розробка індивідуальних тренінгів з питань безпеки
Оцінка внутрішньої лояльності та задоволеності персоналу	Вивчення емоційного та морального стану працівників	Опитування та анкетування працівників	Виявлення факторів робочого оточення, що впливають на безпеку	Суб'єктивність оцінок та індивідуальні відмінності	Покращення робочих умов та стратегій для підвищення лояльності
Моніторинг соціальних мереж та відкритих джерел	Аналіз віртуального сліду працівників у соціальних мережах	Використання програм для моніторингу соціальних мереж	Виявлення небезпечних практик у віртуальному просторі	Збір та обробка великої кількості даних	Попередження можливих загроз та виявлення ризиків через інтернет
Аналіз організаційної культури та ефективності внутрішніх процесів	Визначення впливу корпоративної культури на безпеку	Групові дискусії, інтерв'ю, опитування та анкети для оцінки цінностей та уявлень працівників	Розуміння впливу корпоративної культури на безпеку	Суб'єктивність оцінок, залежність від індивідуальних вражень	Визначення ефективних стратегій для підвищення безпекової культури
Розрахунок показників та HR-метрик	Кількісне вимірювання рівня безпеки та ефективності політики безпеки	Порівняння ключових показників та метрик з нормативним значенням	Кількісне вимірювання рівня безпеки	Не враховує контекстуальних аспектів безпеки	Установлення об'єктивних метрик та оцінка ефективності політик безпеки
Оцінка ефективності системи кібербезпеки	Аналіз технічних параметрів системи кібербезпеки	Пентестування (тест на проникнення), аудит систем безпеки, моніторинг інцидентів	Визначення рівня захищеності від кіберзагроз	Не враховує соціальні та організаційні аспекти	Забезпечення оптимального рівня захисту від кіберзагроз

Джерело: складено автором

З метою побудови ефективного механізму діагностики кадрової небезпеки в системі менеджменту «А-Банку» доцільно здійснити процес реструктуризації служби безпеки, головним завданням якої сьогодні має бути кадрова стратегія збереження персоналу і гарантія безпеки.

В основу побудови системи охорони банку та управління кадровою безпекою варто покласти принцип забезпечення послідовних етапів безпеки, на яких своєчасно виявляються загрози, вони локалізуються і не мають можливості поширюватися, оскільки системою передбачені надійні перешкоди. Ефективність системи охорони банку оцінюється тривалістю часу з моменту виникнення загрози до початку її усунення.

З цією метою вкрай необхідно створити службу безпеки з централізованим організаційно-методичним управлінням та синхронізацією діяльності по однакових принципах і правилах (рис. 3.1).

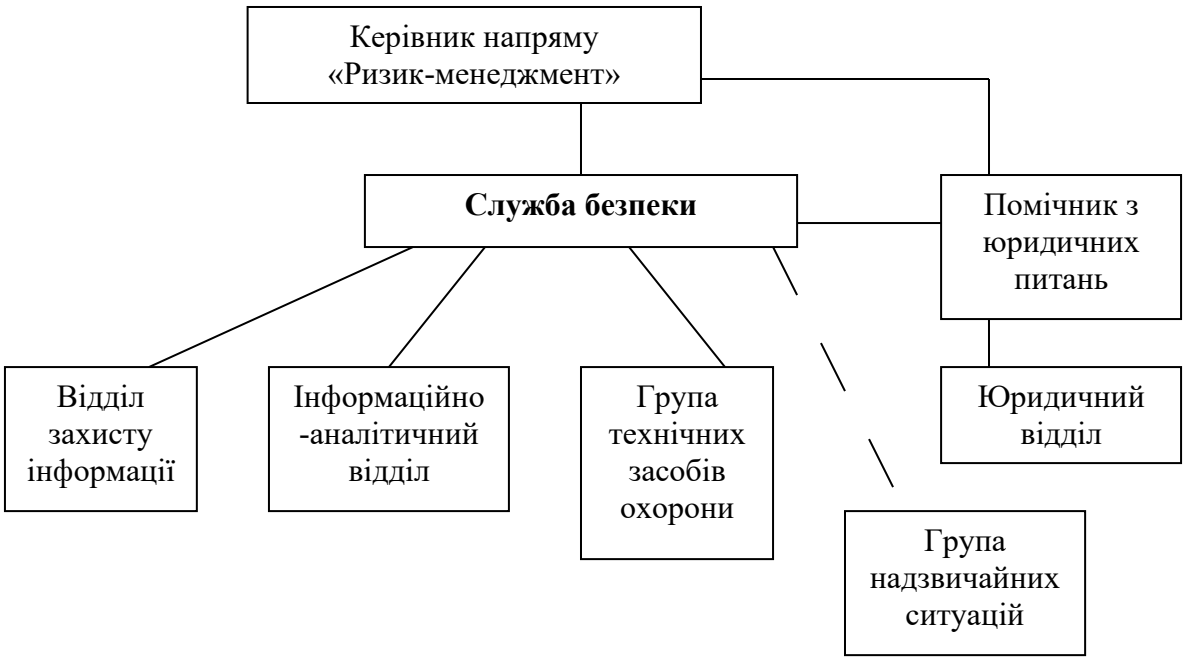

Рис. 3.1. Оновлена структура служби безпеки АТ «А-Банк»

Джерело: проілюстровано автором

Служба безпеки має підпорядковуватися безпосередньо члену Правління банку, керівнику напряму «Ризик-менеджменту». Питання безпеки банку повинні вирішуватися спільно із керівництвом і підрозділами.

Завдяки раціонально організованій роботі служби безпеки, АТ «А-Банк» може працювати в двох режимах – звичайному і надзвичайному.

За умов звичайного режиму, коли не виникає серйозних загроз інформаційній та кадровій безпеці, здійснюється профілактична робота щодо їх попередження, а діяльність всіх підрозділів відбувається у повсякденному режимі. Проблеми та загрози, що виникають, мають локальний характер і усуваються поточною роботою підрозділів банку, у тому числі службою безпеки. В умовах надзвичайного режиму виникають несподівані загрози з важкими наслідками. В такій ситуації керівник служби безпеки викликає команду з надзвичайних ситуацій (кризисну групу), в яку входять найбільш кваліфіковані і досвідчені в даній проблемі фахівці. Ця група працює не постійно, а за потреби.

Оновлена структура служби безпеки ґрунтується на розподілі функціональних обов'язків між співробітниками служби безпеки, що відповідають за безпосередній захист основних об'єктів погроз та, одночасно, взаємодіють з іншими функціональними підрозділами банку, від діяльності яких в значній мірі залежить забезпечення кадрової безпеки. Така розширена структура служби безпеки дає можливість забезпечити достатню безпеку банку та максимально зменшити загрози, що можуть виникати з боку власного персоналу, особливо тих категорії працівників, які мають доступ до комерційної та конфіденційної інформації. Такі посади розглядаються в системі управління кадровою безпекою як потенційні джерела неправомірних дій та розголошення банківських таємниць. До цих категорій відносяться працівники бухгалтерії, касири, особи, що мають право розпорядження друком, бланками, працівники комп'ютерних підрозділів.

3.2. Перспективи удосконалення системи управління кадровою безпекою банку в контексті технологічних інновацій

Ключову роль у забезпеченні кадрової безпеки в банківських установах відіграють новітні технології. Інтеграція штучного інтелекту, біометрії, IoT

(інтернету речей), блокчейну та інших інноваційних рішень може значно покращити систему безпеки і знизити ризики для працівників та інформаційних ресурсів банку. Однак важливо враховувати питання етичності та приватності, а також витрати на впровадження та підтримку новітніх технологій.

Найбільш актуальні технологічні інновації для удосконалення системи управління кадровою безпекою АТ «А-Банк» охарактеризовані нижче.

1. Штучний інтелект та аналітика.

Застосування алгоритмів машинного навчання для аналізу великої кількості даних допомагає виявляти аномалії та попереджувати про можливі загрози з боку персоналу. Впровадження систем моніторингу з використанням штучного інтелекту для раннього виявлення підозрілих дій та ідентифікації невідповідностей в поведінці працівників.

2. Інтернет речей (IoT).

Використання IoT-пристроїв для відстеження місцезнаходження та безпеки працівників у реальному часі. Впровадження IoT-рішень для моніторингу робочих умов та забезпечення безпеки в робочих приміщеннях.

3. Блокчейн.

Забезпечення безпеки та невідкладності в обміні конфіденційною інформацією, зокрема у сфері менеджменту персоналу. Використання технології блокчейн для зберігання та відстеження конфіденційної інформації про працівників.

4. Кіберфізичні системи.

Інтеграція кіберфізичних систем для автоматизації та контролю робочих процесів може зменшити ризики, пов’язані з людським фактором. Впровадження систем кіберфізичного контролю для автоматизації та моніторингу ключових аспектів безпеки працівників.

5. Віртуальна реальність (VR) та доповнена реальність (AR).

Використання віртуальної та доповненої реальності для проведення тренінгів та симуляцій небезпечних ситуацій. Розробка власних VR- та AR-програм для тренувань працівників із питань кадрової безпеки.

6. Мобільні додатки для безпеки.

Розробка мобільних додатків для швидкого сповіщення стосовно екстрених ситуацій та отримання рекомендацій щодо дій у випадку загрози. Впровадження мобільних додатків, спрямованих на підвищення безпеки та невідкладної допомоги працівникам.

7. Аналітика на основі даних профілю працівника.

Використання аналітики для оцінки профілю поведінки працівників та виявлення потенційних ризиків. Застосування аналітичних інструментів для вивчення патернів поведінки та ідентифікації аномальних ситуацій.

Впровадження запропонованих технологічних інновацій значно удосконалить систему управління кадровою безпекою, надасть можливість зменшити ризики та підвищити ефективність заходів безпеки в банківській установі.

Серед переваг впровадження технологічних інновацій в систему управління кадровою безпекою банку особливу увагу привертають наступні:

- ефективність та швидкість: автоматизовані системи та технології дозволяють проводити моніторинг та реагувати на інциденти в реальному часі, що підвищує ефективність управління кадровою безпекою;
- автоматизація процесів: технології дозволяють автоматизувати багато рутинних завдань, таких як ведення журналів, моніторинг доступу та аналіз потенційних загроз;
- прогностичний аналіз: використання штучного інтелекту та машинного навчання дозволяє проводити прогностичний аналіз та передбачати можливі загрози, допомагаючи уникнути інцидентів;
- ідентифікація та аутентифікація: використання біометричних технологій спрощує процес ідентифікації та аутентифікації працівників, забезпечуючи високий рівень безпеки;
- моніторинг умов праці: використання IoT дозволяє моніторити умови працівників та виявляти можливі ризики для їхнього здоров’я та безпеки;
- гнучкість та мобільність: мобільні додатки та віртуальні рішення

дозволяють здійснювати моніторинг та управління кадровою безпекою з будь-якого місця та пристрою;

- підвищення обізнаності працівників: використання навчальних технологій, таких як віртуальна реальність та доповнена реальність, дозволяє проводити ефективні тренінги та підвищує рівень обізнаності працівників стосовно правил та процедур безпеки;

- зниження ризику людського фактору: кіберфізичні системи та автоматизовані процеси допомагають знижувати ризик людських помилок та недбалості у справах безпеки;

- інтеграція та аналіз даних: використання технологій дозволяє інтегрувати та аналізувати великі обсяги даних, що сприяє вдосконаленню стратегій та процесів управління кадровою безпекою;

- зменшення ризику кібератак: використання захисту кібербезпеки та технологій блокчейну зменшує ризик кібератак та забезпечує безпеку конфіденційної інформації.

Отже, впровадження технологічних інновацій в управління кадровою безпекою не лише підвищує рівень безпеки, а й забезпечує більш ефективні та гнучкі стратегії управління ризиками та безпекою працівників.

Запропоновані пропозиції вдосконалення системи управління кадровою безпекою розкривають перед менеджментом АТ «А-Банк» низку перспектив.

1. Інтеграція інноваційних технологій.

Подальше використання та розвиток штучного інтелекту, блокчейну, IoT, біометрії та інших технологій для підвищення рівня кібербезпеки та контролю доступу.

2. Розвиток системи автоматизації.

Впровадження систем автоматизації управління кадровою безпекою для швидкого реагування на загрози та оптимізації рутинних завдань.

3. Ефективний моніторинг умов праці.

Розширення застосування IoT (інтернету речей) для забезпечення високоточного моніторингу умов праці та виявлення можливих небезпек.

4. Технологічні інновації у тренуванні та навчанні.

Використання віртуальної реальності та інших інновацій в тренуванні працівників, що дозволяє ефективно симулювати різні сценарії та ситуації.

5. Гнучкі та ефективні рішення.

Розробка та впровадження гнучких стратегій управління кадровою безпекою, які враховують форс-мажорні умови та загрози.

6. Вдосконалення культури безпеки.

Спрямовані заходи на вдосконалення корпоративної культури серед працівників, включаючи навчання та виховання.

7. Глобальний підхід до кібербезпеки.

Забезпечення глобальної координації та співпраці з іншими банківськими установами для обміну інформацією та спільної боротьби з кіберзагрозами.

8. Емоційна та соціальна інтелектуальність.

Розвиток технологій, спрямованих на виявлення та реагування на емоційний та соціальний стрес серед працівників, зокрема в умовах дистанційної роботи.

9. Посилення заходів протидії внутрішнім загрозам.

Вдосконалення систем внутрішньої безпеки та контролю, враховуючи потенційні внутрішні загрози та шахраїв.

10. Наголос на приватність та етику.

Розвиток та дотримання строгих стандартів щодо захисту приватності та етичного використання технологій в управлінні кадровою безпекою.

11. Аналіз та реакція на виклики сучасності.

Постійний моніторинг та аналіз нових викликів, таких як пандемія, природні катастрофи, воєнні дії та адаптація стратегій кадрової безпеки до сучасних реалій.

Врахування цих перспектив допоможе банківським установам підвищити рівень кадрової безпеки, стати більш адаптивними та готовими до змін у сучасному бізнес-середовищі.

Всебічний аналіз впровадження інноваційних змін в систему забезпечення

кадрової безпеки доводить, що поряд з перевагами новітніх технологій слід враховувати певні виклики. Характеристика переваг і викликів використання технологічних інновацій систематизована в таблиці 3.2.

Таблиця 3.2

Характеристика переваг і викликів впровадження технологічних інновацій в систему управління кадровою безпекою

Аспект	Переваги	Виклики
Автоматизація процесів	Збільшення ефективності та швидкості виконання рутинних завдань	Високі витрати на впровадження нових систем та навчання персоналу
Використання Big Data	Аналіз великих обсягів даних для прогнозування тенденцій та прийняття стратегічних рішень	Проблеми з конфіденційністю та захистом персональної інформації
Штучний інтелект	Автоматизація процесів відбору та аналізу кандидатів, що прискорює найм нового персоналу	Потенційна втрата робочих місць внаслідок автоматизації
Електронні системи навчання	Забезпечення доступу до навчальних матеріалів та тренінгів для персоналу з будь-якого місця та у будь-який час	Вимоги до великого обсягу інтернет-зв'язку для участі в електронних тренінгах
Віддалена робота	Збільшення гнучкості та робочого комфорту для працівників, особливо під час кризисних ситуацій	Виклики з підтримкою ефективного комунікаційного процесу між віддаленими робітниками та командами
Кібербезпека	Забезпечення високого рівня захисту конфіденційної інформації та персональних даних	Постійна зміна кіберзагроз та необхідність постійного оновлення захисту систем
Мобільність	Забезпечення можливості працювати з будь-якого місця та пристосування робочих процесів до мобільних потреб	Потреба в ефективному управлінні робочими процесами з різних місць роботи
Інтеграція з іншими системами	Можливість спільно використовувати дані та інформацію з іншими організаційними системами	Сумісність та інтеграція із застарілими та неоднорідними інформаційними технологіями

Джерело: складено автором

Враховуючи зазначені виклики (табл. 3.2) доцільно передбачити та запропонувати шляхи їх подолання в контексті удосконалення кадрової безпеки в банківській установі.

Шляхи подолання технічних перешкод та витрат:

- вивчення можливостей використання відкритих джерел та ресурсів для зменшення витрат на впровадження технологій;
- встановлення етапів впровадження та поетапного фінансування для зниження фінансового тиску.

Шляхи подолання ризику витоку та використання даних:

- впровадження механізмів блокування та моніторингу доступу до конфіденційної інформації;
- здійснення аудиту безпеки та періодична оцінка ризиків.

Опір технологічним змінам серед персоналу можна подолати шляхом:

- забезпечення ефективної комунікації та надання відповідної освіти персоналу щодо переваг та необхідності впровадження змін;
- залучення персоналу до процесу планування та виконання стратегій безпеки.

Дотримання приватності в процесі використання технологій:

- розробка та дотримання прозорих політик щодо використання технологій та захисту приватності;
- проведення незалежних аудитів щодо відповідності політикам та вимогам щодо приватності.

Шляхи подолання нехватки кваліфікованих кадрів у сфері кібербезпеки:

- сприяння навчанню та розвитку кібербезпекових навичок серед внутрішнього та зовнішнього персоналу;
- укладання партнерських угод із навчальними закладами та компаніями з профільною експертизою.

Комплексність та об’єм даних досягається шляхом:

- застосування аналітичних інструментів та штучного інтелекту для обробки та аналізу великих обсягів даних;

- розвиток системи фільтрації та попередження для фокусування на ключових показниках безпеки.

Важливою частиною розробки та прийняття рішення щодо впровадження новітніх технологій в систему управління кадровою безпекою є попереднє прогнозування результатів впровадження пропозицій. Отже основні прогнози виглядають наступним чином.

1. Підвищення рівня кібербезпеки.

Впровадження інноваційних технологій та стратегій допоможе підвищити рівень кібербезпеки, зменшуючи ризики кібератак та несанкціонованого доступу.

2. Ефективне управління інцидентами.

Автоматизація та розширення систем управління інцидентами дозволить швидше виявляти та реагувати на можливі загрози, зменшуючи час реакції та втрати.

3. Зниження кількості інцидентів та порушень.

Підвищення обізнаності працівників та вдосконалення процесів безпеки призведе до зменшення кількості інцидентів та порушень у банківській установі.

4. Покращення реакції на екстрені ситуації.

Використання віртуальної та доповненої реальності для тренувань та симуляцій дозволить працівникам краще реагувати на екстрені ситуації, зменшуючи можливі наслідки.

5. Підвищення продуктивності та ефективності.

Автоматизація та оптимізація процесів управління кадровою безпекою призведе до підвищення продуктивності та ефективності роботи персоналу.

6. Створення прозорої та доступної інформаційної середи.

Використання технологій для інтеграції та аналізу даних створить прозоре та доступне інформаційне середовище для прийняття обґрунтованих рішень.

7. Мінімізація внутрішніх загроз.

Посилення заходів протидії внутрішнім загрозам та вдосконалення систем внутрішньої безпеки допоможе мінімізувати ризики від дій працівників.

8. Посилення культури безпеки.

Вдосконалення стратегій та виведення корпоративної культури на новий рівень стане основою для забезпечення безпеки на всіх рівнях банківської установи.

9. Підвищення довіри клієнтів.

Забезпечення високого рівня безпеки та конфіденційності даних клієнтів призведе до збільшення довіри та лояльності клієнтів.

10. Адаптація до нових викликів.

Гнучкі та резилієнтні стратегії дозволять банківській установі ефективно адаптуватися до нових викликів та змін у бізнес-середовищі.

У підсумку прогнозується, що впровадження запропонованих інновацій та технологій сприятиме покращенню загального стану кадрової безпеки в банківській установі, забезпечуючи стабільність та конкурентоспроможність на ринку.

Системність і комплексність підходів до удосконалення системи управління кадровою безпекою дозволять визначити основні напрями та ключові кроки для досягнення поставлених цілей. Кожна складова системи має бути розглянута детальніше з метою розробки конкретного плану дій для гарантії високого рівня кадрової безпеки.

На етапі вибору першочергових заходів та інвестицій провести порівняльний аналіз ефективності кожного напрямку удосконалення та обрати найбільш пріоритетні, які спрямовані на створення комплексної та ефективної системи діагностики кадрової небезпеки в банківському менеджменті з метою забезпечення високого рівня безпеки та відповідність сучасним вимогам кадрової стратегії.

Складові елементи пріоритетних напрямів удосконалення системи управління кадровою безпекою з урахуванням етапу стратегічного розвитку, рівня технологічної готовності АТ «А-Банк», стану кадрового забезпечення, готовності персоналу до організаційних і технологічних змін, а також впливу форс-мажорних обставин, детально представлені на рис. 3.2.

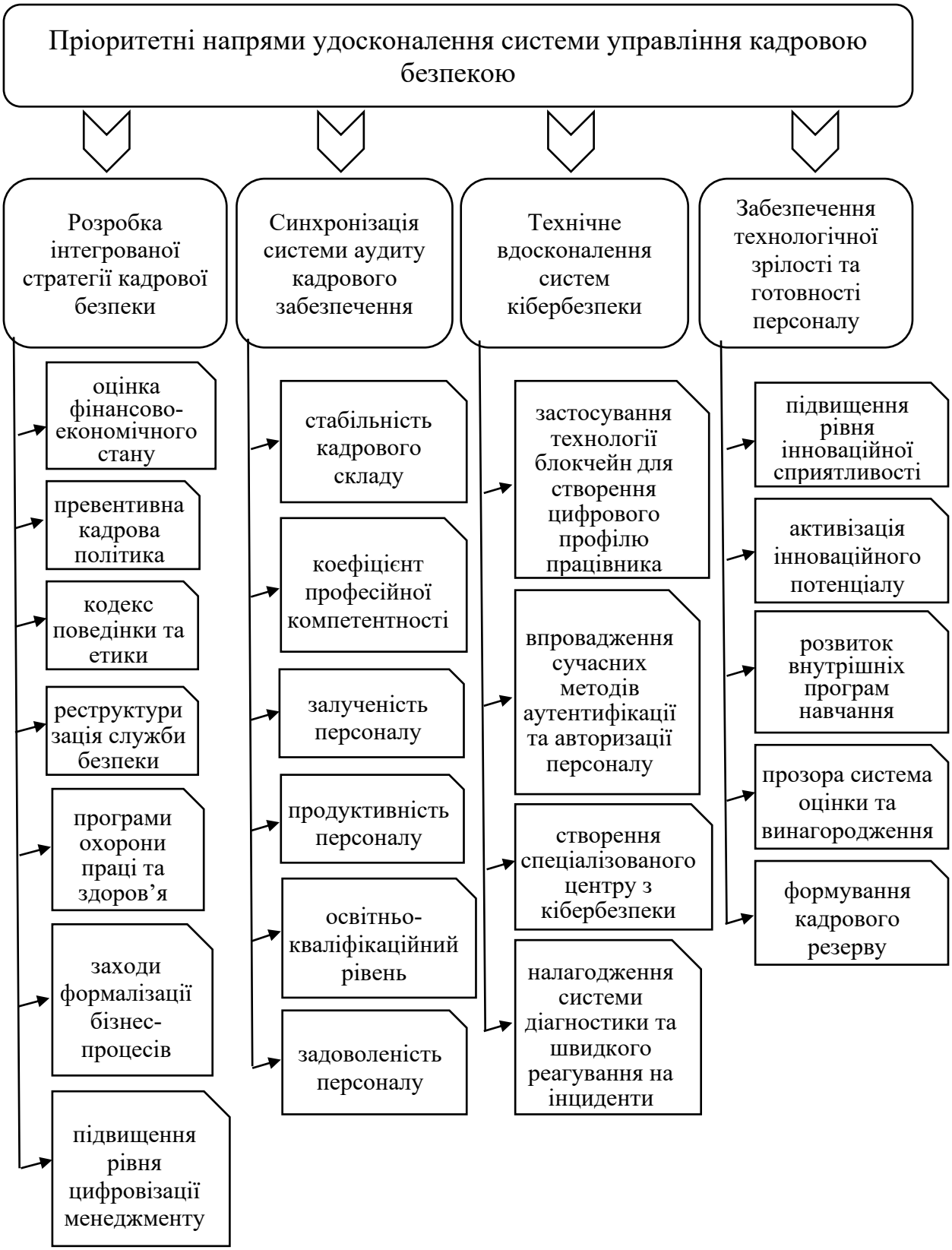

Рис. 3.2. Напрями удосконалення системи управління кадровою безпекою банку в контексті технологічних інновацій

Джерело: проілюстровано автором

Визначені напрями спрямовані на створення комплексної та ефективної системи діагностики кадрової небезпеки в банківському менеджменті, що забезпечить високий рівень безпеки та відповідність сучасним вимогам кібербезпеки АТ «А-Банк».

У підсумку зазначимо, що використання сучасних методів, таких як аналіз Big Data, штучний інтелект, моніторинг соціальних мереж, розрахунок показників рівня безпеки дозволить отримувати об'єктивні дані та оцінювати потенційні ризики в сфері кадрової безпеки «А-Банку». Результатами удосконалення системи управління кадровою безпекою є збільшення точності та об'єктивності діагностики, можливість вчасно реагувати на зміни в кадровому середовищі, автоматизація процесів та прискорення прийняття рішень.

АТ «А-Банк» отримає переваги технологічних інновацій, а саме: збільшення швидкості реакції на загрози та виклики, забезпечення високого рівня кібербезпеки та захисту персональних даних, автоматизація процесів та зменшення ризику людського фактору.

Отже, впровадження сучасних методів діагностики та технологічних інновацій в систему управління кадровою безпекою банку значно покращить ефективність та надійність цієї системи. Проте, для успішної реалізації цих змін, важливо передбачити і подолати виклики шляхом забезпечення надійності та безпеки обробки великих обсягів даних; підвищення кваліфікації персоналу для роботи з сучасними інструментами діагностики; технічного вдосконалення систем кібербезпеки.

Запропоновані рекомендації доцільно покласти в основу розробки конкретного плану дій та імплементації стратегії удосконалення системи управління кадровою безпекою в АТ «А-Банк».

ВИСНОВКИ

В результаті проведеного дослідження система управління кадровою безпекою банківської установи АТ «А-Банк» ми зробили наступні висновки:

1. Кадрова безпека є складовою економічної безпеки, яку доцільно досліджувати як сукупність певних умов, які дозволяють попереджати потенційно небезпечні дії чи обставини; а також зводити їх до такого рівня, за якого вони не спроможні заподіяти шкоди встановленому порядку функціонування банку. Ефективність системи управління кадровою безпекою проявляється у вигляді збереження й відтворення майна банківської установи, її інфраструктури та досягнення стратегічних цілей. Кадрова безпека визначається як система моніторингу та синхронізації трудових відносин у колективі, яка сприяє встановленню довірчих взаємин серед працівників, а у випадку потенційної загрози чітко і швидко усуває негативні прояви без шкоди для інших.

2. Менеджери успішних банків сьогодні озброєні сучасним арсеналом показників і HR метрик, які дозволяють банку отримати об’єктивні дані та відслідковувати ефективність стратегій з управління кадровою безпекою. Це допомагає визначати слабкі місця, вдосконалювати процеси та забезпечувати високий рівень безпеки в організації. Серед показників та HR метрик, які найбільш розповсюджені в практиці банківського менеджменту для вимірювання рівня кадрової безпеки особливу увагу привертають: число інцидентів безпеки; рівень успішності тренінгів та тестувань ; час виявлення та реакції на інцидент; рівень усвідомленості персоналу; аналіз доступів та привілеїв; відсоток вирішених конфліктів із залученням HR-менеджерів; показники кібербезпеки - кількість виявлених та зупинених кібератак; індекс задоволення персоналу та лояльності; витрати на безпеку та реакцію на інциденти. Ці показники і метрики надають банку засоби для оцінки ефективності стратегій кадрової безпеки, виявлення слабких місць та впровадження необхідних заходів для підвищення рівня безпеки організації.

3. Основою побудови системи управління кадровою безпекою «А-Банку» стали корпоративні цінності. Вони характеризують принципи ведення бізнесу, забезпечують реалізацію стратегії розвитку банку, створення та збереження його ділової репутації. Корпоративними цінностями «А-Банку» є: клієнти, працівники, технологічність, якість, ощадливість, відкритість до діалогу.

Умови воєнного стану значно вплинули на стратегію розвитку українських банків, АТ «А-Банк» не став виключенням. Важливим досягненням менеджменту банку стала доступність і безперервна робота відділень. Станом на 01.01.2023р. банківська мережа становила 200 відділень (16 відділень знаходяться на окупованих територіях та в зоні бойових дій). Характерною рисою воєнного періоду стала оптимізація 20% відділень діючої мережі, скорочення неефективних відділень у зв'язку зі зменшенням клієнтопотоку та переходом в on-line. Автономність функціонування досягається за рахунок формування мережі ефективних відділень з альтернативними джерелами енергії та резервними каналами зв'язку. 83 відділення «А-Банку» входять до державної об'єднаної мережі «Power banking» та забезпечені 100% альтернативним електроживленням, а також 57% із них вже підключено до альтернативних каналів зв'язку.

Аналіз організаційної структури управління «А-Банку» та оцінка розподілу відповідальності у сфері кадрової безпеки дозволяє зробити висновок, що характерною рисою ОСУ є чітка та зрозуміла ієрархічна структура, яка підтримує ефективність управління кадровою безпекою.

Головною цінністю банку є людський капітал і фокус на співробітниках став пріоритетним напрямком за останні два роки. Команда «А-Банку» швидко адаптувалася до страшних викликів, які супроводжувалися карантином у 2021 році та форс-мажорними обставинами, які спричинила війна. Першочерговим завданням менеджменту банку з лютого 2022 року стала розробка та здійснення програми релокації та збереження персоналу.

Протягом 2018-2022 років чисельність персоналу скоротилась з 2396 до 1912 осіб (484 особи або на 20%). Причинами такої плинності стали фактори

зовнішнього впливу. Отже в теперішніх умовах банк взяв курс на розвиток персоналу шляхом складання індивідуальних планів розвитку співробітників, виявлення потенціалу і формування кадрового резерву (особлива увага до позицій системних аналітиків). Важливою складовою менеджменту персоналу є система професійного розвитку персоналу. «А-Банк» систематично забезпечує своїх співробітників необхідним рівнем професійних знань, навичок та компетентностей. У системі HR-менеджменту здійснюються програми з підготовки кадрового резерву з метою оперативного закриття вакантних посад.

4. Діюча система управління кадровою безпекою банку, з одного боку характеризується позитивними аспектами, а саме високою лояльністю та підготовленістю персоналу, які варто зберегти та підтримувати. З іншого боку, слабкими сторонами є: відсутність інтегрованої стратегії кадрової безпеки; потреба в удосконаленні технічних засобів для кібербезпеки; недостатня ефективність системи внутрішнього контролю та аудиту.

Отже, першочергові завдання для посилення ефективності системи управління кадровою безпекою АТ «А-Банк» полягають у: розробці інтегрованої стратегії, орієнтованої на стратегічні цілі банку; покращені технічних засобів для захисту інформаційних ресурсів і даних клієнтів; забезпечені ефективності систем внутрішнього контролю та аудиту.

5. Використання сучасних методів, таких як аналіз Big Data, штучний інтелект, моніторинг соціальних мереж, розрахунок показників рівня безпеки дозволить отримувати об’єктивні дані та оцінювати потенційні ризики в сфері кадрової безпеки «А-Банку». Результатами удосконалення системи управління кадровою безпекою є збільшення точності та об’єктивності діагностики, можливість вчасно реагувати на зміни в кадровому середовищі, автоматизація процесів та прискорення прийняття рішень.

Запропоновані пропозиції дозволять АТ «А-Банк» отримати переваги технологічних інновацій, а саме: збільшення швидкості реакції на загрози та виклики, забезпечення високого рівня кібербезпеки та захисту персональних даних, автоматизація процесів та зменшення ризику людського фактору.

СПИСОК ВИКОРИСТАНИ[Х ДЖЕРЕЛ

1. Андрєєва Т. Є., Бутенко О. П., Гненна Є. В. Здійснення оцінки ефективності праці персоналу в банківській сфері. *Економіка. Управління. Інновації.* 2013. № 2 (10).

2. Балабанова Л. В. Управління персоналом: підручник для студ. вищ. навч. закл. / Л. В. Балабанова, О. В. Сардак. Київ: Центр учбової літератури, 2019. 468 с.

3. Бей Г.В., Середа Г.В. Трансформація HR-технологій під впливом цифровізації бізнес-процесів. Економіка і організація управління. 2019. № 2(34). С. 93–101.

4. Волянська-Савчук Л. В. Трансформація кадрової політики на підприємстві в період кризи. Вісник Хмельницького національного університету. Економічні науки. 2014. № 3. С. 137–141.

5. Воробйова Н. П., Познякова Т. В. Кадрова політика як основа формування інноваційної стратегії в системі менеджменту організації. Проблеми інноваційно-інвестиційного розвитку. 2021. № 26. С. 60–73.

6. Гавкалова Н. Л. Організаційно-економічне забезпечення ефективності менеджменту персоналу підприємства: монографія / Н. Л. Гавкалова, О. О. Болотова. Харків : ХНЕУ ім. С. Кузнеця, 2020. 251 с.

7. Гавриш О.А., Довгань Л.Є., Крейдич І.М., Семенченко Н.В. Технології управління персоналом: монографія. Київ: НТУУ «КПІ імені Ігоря Сікорського», 2017. 528 с.

8. Донець Л. І., Шепеленко О. В., Баранцева С. М., Сергєєва О. В., Веремейчик О. Ф. Обґрунтування господарських рішень та оцінювання ризиків: Навчальний посібник. К.: Центр учбової літератури, 2012. 472 с.

9. Дороніна О. А. Трансформація підходів до мотивування персоналу в умовах новітньої управлінської парадигми. Менеджмент та підприємництво: тренди розвитку. 2018. Вип. 3. С. 23-32. URL: http://nbuv.gov.ua/UJRN/mnnt_2018_3_5

10. Дороніна О.А. Кадрова політика як інструмент антикризового управління підприємством. Інвестиції: практика та досвід. 2015. № 20. С. 92–95.

11. Дребот Н., Грудзевич У. Інноваційна політика банків на ринку банківських послуг. Економіка та суспільство. (33). 2021. URL: https://doi.org/10.32782/2524-0072/2021-33-45

12. Дробязко А. Як працює банківська система України в умовах війни. URL: https://mind.ua/openmind/20239949-yak-pracyue-bankivska-sistema-ukrayini-v-umovah-vijni

13. Економіка праці та соціально-трудові відносини: підручник Л.М. Ільїч, О.В. Акіліна К.: Київський ун-т ім. Бориса Грінченка. 2020. 952 с.

14. Економіка праці: навчальний посібник. за заг. ред. Г. В. Назарової. Харків: ХНЕУ ім. С. Кузнеця, 2019. 330 с.

15. Економіка праці та соціально-трудові відносини. Підручник. 2-ге видання. Ведерніков М. Д., Чернушкіна О. О. 2023. 860 с.

16. Єкімова О. О. Типи кадрової політики та необхідність оцінки обраного типу управління людськими ресурсами. Теоретичні і практичні аспекти економіки та інтелектуальної власності. Том 3 № 1. 2012. С. 156-170.

17. Занора В., Зачосова Н., Поковба Д. Управління кадровою політикою суб'єкта господарювання: теоретичний базис. Економіка та суспільство, (38). 2022. URL: https://doi.org/10.32782/2524-0072/2022-38-3

18. Кодекс корпоративної етики та поведінки URL: https://a-bank.com.ua/static/korp_codex_ethics_2021.pdf

19. Корпоративні відносини в банківському секторі: фінансові механізми та маркетингові стратегії : моногр. / П. П. Гаврилко, М. О. Кужелєв, І. Г. Брітченко. Рівне: «Волинські обереги», 2016. 240 с.

20. Крушельницька О.В. Мельничук Д.П. Управління персоналом: Навчальний посібник. Видання друге, перероблене й доповнене. К., «Кондор». 2006. 308 с.

21. Лепейко Т.І. Управління персоналом підприємства в умовах невизначеності (поведінковий підхід): монографія Т.І. Лепейко, О.М. Миронова.

Х.: Вид. ХНЕУ. 2010. 236 с.

22. Мехеда Н. Г., Маренич А. І. Соціально-мотиваційні складові кадрової безпеки. *Фінансовий простір: міжнародний науково-практичний журнал*. 2012. № 2 (6). С. 38-45.

23. Назарова Г.В., Лобазов С.М. Удосконалення методики розрахунку інтегрального індексу кадрової безпеки підприємства. *Економіка: реалії часу.* 2015. №1(17). С. 134-139.

24. Назарова Г.В. Оцінка конкурентоспроможності системи управління персоналом підприємства: монографія / Г.В. Назарова, В.І. Лаптєв, Д.О. Корсаков. Х. ХНЕУ ім. С. Кузнеця. 2014. 188 с.

25. Назарова Г.В. Передумови створення системи кадрової безпеки підприємства. *Регіональні аспекти розвитку продуктивних сил України.* 2010. Вип.15. С. 34-37.

26. Новітні технології управління персоналом: навч. посіб. І. М. Сочинська-Сибірцева, О. В. Сторожук, А. О. Доренська. Кропивницький : ЦНТУ, 2023. 278 с. http://dspace.kntu.kr.ua/jspui/handle/123456789/13256

27. Особливості організації трудових відносин в умовах воєнного стану URL: https://wiki.legalaid.gov.ua/index.php/

28. Офіційний сайт АТ «А-Банк». URL: https://a-bank.com.ua/services/abank

29. Пластун О.І. Аналітика в управлінні персоналом: навчальний посібник. Рівне: Рівненський державний гуманітарний університет, 2020. 202с.

30. Принципи (кодекс) корпоративного управління АТ «А-Банк» URL: https://a-bank.com.ua/static/korp_codex_2021.pdf

31. Про схвалення основних (стратегічних) напрямів діяльності банків державного сектору на період воєнного стану та післявоєнного відновлення економіки. URL: https://zakon.rada.gov.ua/laws/show/356-2022-%D1%80#Text

32. Сибірцев В.В., Сочинська-Сибірцева І.М. Креативні технології адаптації персоналу в умовах форс-мажору. Центральноукраїнський науковий вісник. Економічні науки : зб. наук. пр. Кропивницький: ЦНТУ, 2022. Вип. 8 (41). с.49-55. URL: http://economics.kntu.kr.ua/archive/8(41)/41_Sybirtsev.html

33. Сочинська-Сибірцева І.М. Технологія управління надійністю персоналу в контексті кадрової безпеки. *Економіка і організація управління*. №3 (23), 2016. С. 302-308.

34. Статут АТ «А-Банк» URL: https://a-bank.com.ua/static/statut_2022.pdf

35. Стратегія АТ «А-Банк» на 2024 рік. URL: https://a-bank.com.ua/static/bank_strategy_ua.pdf

36. Управління персоналом : підручник / О. М. Шубалий, Н. Т. Рудь, А. І. Гордійчук, І. В. Шубала, М. І. Дзямулич, О. В. Потьомкіна, О. В. Середа; за заг. ред. О. М. Шубалого. Луцьк: ІВВ Луцького НТУ, 2018. 404 с.

37. Фінансова звітність АТ «А-Банк». URL: https://minfin.com.ua/ua/company/a-bank/rating/

38. Фонд гарантування вкладів фізичних осіб. URL: http://www.fg.gov.ua

39. Щокін Г.В. Соціальна теорія та кадрова політика. Монографія. К: МАУП, 2020. 576 с.

40. David Ulrich. Four HR Roles. URL: https://hrmhandbook.com/hro/model/dave-ulrich-four-roles/

41. EMA Partners International, executive search & leadership advisory : HR у час війни 2022 URL:https://www.ema-partners.com/europe/ukraine

42. Ferron D., Lomas F. (2020). Eight forces driving HR transformation right now. EY. URL: https://www.ey.com/en_gl/workforce/eight-forces-driving-hr-transformation-right-now

43. Global Human Capital Trends 2023 // *Deloitte Insights:* [Website]. 2023. URL: https://www2.deloitte.com/us/en/insights/focus/human-capital-trends.html

44. Global Economic Crime Survey 2022. *PricewaterhouseCoopers. URL:* https://www.pwc.com/gx/en/services/forensics/economic-crime-survey.html

45. HR Technology Strategy and Selection – Insights (2023). Gartner. URL: https://www.gartner.com/en/human-resources/insights/hr-technology-strategy

46. HR-менеджмент: навчальний посібник / І. М. Сочинська-Сибірцева, А.О. Доренська, Т. В. Тушевська. Кропивницький, 2022. 278 с. http://dspace.kntu.kr.ua/jspui/handle/123456789/12269