МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ОДЕСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ

Кафедра банківської справи

РЕФЕРАТ
кваліфікаційної роботи
на здобуття освітнього ступеня бакалавра
зі спеціальності 072 «Фінанси, банківська справа та страхування» за освітньо-професійною програмою
«Міжнародний банківський бізнес»
на тему:

«Організаційно – методичні засади інформаційної безпеки банку в умовах невизначеності»

Виконав: студент 4 курсу, групи 3
ФФБС
ГОЛИКОВ Андрій Олександрович
Науковий керівник: к.е.н., доцент
СЕРГЄЄВА Олена Степанівна

ОДЕСА - 2024 р

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Стрімкий розвиток інформаційних технологій, розширення глобального інформаційного середовища, широке застосування засобів обміну інформацією, всеохоплююча комп'ютеризація всіх сфер життєдіяльності зумовлюють актуальність дослідження питань безпеки інформаційної інфраструктури. Забезпечення ефективного захисту інформації є надзвичайно актуальним і для установ банківської сфери, де щоденно оброблюється великий обсяг інформації різного рівня конфіденційності.

На сьогодні банки відіграють надважливу роль у забезпеченні сталого розвитку економіки, адже саме вони є тими фінансовими посередниками, що забезпечують постачання ліквідності на фінансовий ринок та забезпечують кредитування реального сектору економіки. Банки належать до об'єктів критичної інфраструктури, що є стратегічно важливими для функціонування економіки та безпеки держави. Однією з нових загроз втрати стійкості банків в умовах переходу на шостий технологічний уклад та пов'язаного з цим застосування технологій Індустрії 4.0, таких як штучний інтелект, «хмарні» та «туманні» обчислення, IoT / IIoT, Big Data, Blockchain, VR / AR, є кіберзагрози, ландшафт який постійно трансформується та оновлюється. Зважаючи на це, банки мають формувати комплекс заходів, інструментів та механізмів для забезпечення інформаційної безпеки, кіберстійкості як здатності протистояти зовнішнім та внутрішнім загрозам, спричинених кіберризиками, адаптуватися до них та / або відновлюватися після них.

Вивченням питанням безпеки банків займалися такі науковці як М. Зубок М., Баранівський О., Букін С., Бланк І., Вовчак О., П. Гайдуцький П., Геєць В., Гіжевський В., Гриценко Р., Криклій О., Коваленко В. Проте питання розробки ефективної системи забезпечення банківської інформаційної безпеки ще потребують подальшого вивчення.

Визначені проблеми підвищують актуальність дослідження в напряму рекомендацій щодо удосконалення інформаційної безпеки банків в умовах невизначеності та кіберзагроз.

Метою кваліфікаційної роботи є теоретичне узагальнення, яке полягає у розгляді поняття «інформаційна безпека банку» та запропонуванні рекомендацій щодо підвищення її в умовах невизначеності (воєнного стану).

Для досягнення мети в роботі було поставлено наступні задачі:

- обґрунтувати поняття «інформаційна безпека» через визначення наукових підходів, функцій, видів та напрямів;
- надати характеристику загроз, що впливають на інформаційну безпеку банків та визначити правове регулювання, яке регламентує дотримання інформаційної безпеки в банках;
- провести оцінку діяльності АТ «А – БАНК» в українському інформаційному полі;
- проаналізувати дотримання безпеки інформаційних ресурсів АТ «А – БАНК»;

- оцінити дотримання безпеки інформаційної інфраструктури АТ «А – БАНК
- ознайомитися зі світовими викликами, які впливають на інформаційну безпеку банків;
- надати рекомендації щодо підвищення інформаційної безпеки банків України та АТ «А - БАНК» в умовах діючого воєнного стану.

Об'єктом дослідження є процес організації та дотримання інформаційної безпеки в Акціонерне товариство «АКЦЕНТ-БАНК» (далі АТ «А – БАНК»).

Предметом дослідження є теоретико-методичні засади організації процесів організація та дотримання інформаційної безпеки банку в умовах невизначеності.

Методи дослідження. Теоретичною основою кваліфікаційної роботи є положення економічної теорії банківської справи та фінансового менеджменту, дослідження вітчизняних науковців з питань організації та забезпечення інформаційної безпеки в банках. Результати кваліфікаційної роботи отримано з урахуванням сукупності загальнонаукових і спеціальних методів дослідження, а саме: системний – для визначення економічної сутності поняття «інформаційна безпека банку», джерел, особливостей та чинників його виникнення; угруповань і класифікацій – для систематизації чинників, які впливають на інформаційну безпеку; економіко-математичні методи – для аналізу впливу чинників на формування прибутку банку, які впливають на розмір його економічного результату; порівняльного – співставлення результатів діяльності АТ «А – БАНК» на 01.01.2020 – 2024 рр., дослідженню діючих інструментів та впровадження нових технологій щодо підвищення інформаційної безпеки банків в умовах цифровізації.

Інформаційну базу дослідження становили дослідження українських науковців, Закони та Постанова НБУ, офіційні відкриті статистичні бази Державної служби статистики України, Міністерства фінансів України, аналітичні матеріали Національного банку України, фінансова звітність АТ «А-БАНК», розрахунки автора.

Апробація результатів дослідження. По темі кваліфікаційної роботи була прийнята участь у VII Міжнародної науково-практичної Інтернет-конференції «ФІНАНСИ, БАНКІВСЬКА СИСТЕМА ТА СТРАХУВАННЯ В УКРАЇНІ: СТАН, ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ РОЗВИТКУ В КРИЗОВІЙ ЕКОНОМІЦІ» м. Дніпро, 4-5.03.2024 р. та опубліковані тези на тему «Удосконалення механізму фінансової стійкості банків в умовах воєнного стану».

Кваліфікаційна робота бакалавра складається зі вступу, трьох розділів, висновків, списку використаних джерел (73 найменування). Загальний обсяг роботи становить 96 сторінок. Основний зміст викладено на 83 сторінках. Робота містить 17 таблиць, 26 рисунка, 4 додатки.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У першому розділі **«Теоретичні основи організації інформаційної безпеки банку»** було визначено наступне: проведено аналіз поняття «інформаційна безпека банку» та визначено, що це поняття рекомендовано розглядати як стан інформаційної інфраструктури банку, за якого забезпечуються умови стабільного функціонування, максимізації прибутку, оптимального використання ресурсів банку, а також забезпечення захищеності клієнтів, співробітників і керівництва банку від зовнішніх і внутрішніх загроз.

Визначені базові елементи інформаційної безпеки банків, такі як мета, завдання, суб'єкт, об'єкт. Визначення функцій інформаційної безпеки: превентивна, детективна, реактивна, коректива.

З'ясовано, що в організації інформаційної безпеки сучасного банку необхідно відокремлювати наступні напрями безпеки як інформаційне поле, інформаційні ресурси, інформаційна інфраструктура.

У роботі запропоновано визначати, що система управління інформаційною безпекою це забезпечення захисту конфіденційності, цілісності та доступності інформаційних активів. Вона складається з безлічі різних процесів, кожен з яких спрямований на обробку певних загроз.

Проведена характеристика чинників впливу на інформаційну безпеку банку, які пропонується розглядати як зовнішні чинники: кібератаки, політичні, соціальні, економічні та правові чинники, конкуренти та внутрішні чинники: бізнес-модель банку, рівень діджиталізації, високий рівень професіонально персоналу. Завдяки чому, було визначено види загроз інформаційної безпеки банків, які запропоновано розглядати як випадкові та навмисні.

За результатами здійсненого аналізу чинного законодавства України можна зробити висновок, що нормативно – правові норми, які регулюють діяльність банків, постійно удосконалюються та адаптуються в залежно від політичних та економічних умов в яких функціонує країна.

У другому розділі **«Оцінка діяльності банку в інформаційно-цифровому просторі»** було проведена наступна робота: визначена бізнес – модель діяльності АТ «А – БАНК», яка вже протягом багато років направлена на роздрібний бізнес, не зважаючи на пандемію COVID-19 та понад два роки повномасштабної війни в Україні, й надалі підтримує прагнення населення зберігати кошти у надійному банку, займається впровадженням змін заради покращення клієнтського досвіду, розвиває новітні канали обслуговування і комунікації з клієнтами. На 01.01.2024 р. діяльність АТ «А – БАНК» відбувається через 201 фізичне відділення, інтернет – банкінг та мобільний додаток.

Проведена оцінка основних фінансових показників діяльності АТ «А – БАНК» в розрізі найбільш значущих складових які впливають на формування прибуткового результату.

Статутний капітал АТ «А – БАНК» за аналізований період збільшився до 1514594 тис. грн., практично у 3 рази, це відбулось за рахунок власних коштів акціонерів банків та капіталізації за рахунок прибутку, в результаті чого збільшився загальний показник власного капіталу АТ «А – БАНК» з 292 162 тис. грн. до 2 9997309 тис. грн. практично у 10 разів.

Зобов'язання за аналізований період АТ «А – БАНК» відображав постійне зростання, за виключенням 2022 року для коштів банків, своєю чергою кошти клієнтів мали постійну тенденцію до зростання та за 5 років виросли з 5 167 804 тис.грн. до 20 359 333 тис.грн, тому як результат усіх зобов'язання АТ «А – БАНК» теж збільшились та склав на 01.01.2024 р. 21 668 440 тис. Грн.

Активи АТ «А – БАНК» ситуація суттєво покращилась, за аналізований період загальні активи АТ «А – БАНК» збільшились на 19 958 855 тис. грн. чи на 243%.

За аналізований період АТ «А – БАНК» отримав прибуток у розмірі 254 801 тис. Грн., на початок 2021 року 299738 тис. грн., на початок 2022 року АТ «А – БАНК» збільшив прибутковість практично в чотири рази або 800 013 тис. грн, за перший воєнний рік, на 01.01.2023 р, АТ «А – БАНК» відзвітував про отримання прибутку 202 637 тис. грн, а вже на 01.01.2024 р. АТ «А – БАНК» 561 312 тис. грн.

Визначено, що АТ «А – БАНК» за п'ять років активно залучав кошти як від банківських установ, так від клієнтів юридичних та фізичних осіб. Збільшення усіх показників підтверджує, що протягом досліджуваного періоду до АТ «А – БАНК» дотримується усіх норм безпеки щодо інформаційних ресурсів, завдяки має високу довіру з боку клієнтів, що відображається в щорічному збільшенню клієнтської бази.

В напряму обслуговування поточних та строкових рахунків фізичних осіб за п'ять років мала тенденцію до постійного зростання, як в національній, так і в іноземній валюті. За два роки повномасштабного вторгнення кошти фізичних осіб виросли на 6 505 675 тис. грн., я яких кошти на вимогу на 4 183 810 тис. грн., строкові вклади на 2 321 865 тис. грн. В загальній сумі зобов'язань АТ «А – БАНК» у впродовж 2019 та 2020 років обслуговування фізичних осіб займало практично 80% усіх зобов'язань банку, то вже починаючи з 2021 року АТ «А – БАНК» зменшує цей показник до рівня 75%, а на 01.01.2024 р. до 72%,

Оцінка кредитного портфеля АТ «А – БАНК» за клієнтами фізичними та юридичними особами показала, що по юридичним особам АТ «А – БАНК» відбувається несуттєве збільшення до 1 440893 тис.грн.

За обсягами наданих кредитів фізичних осіб відбувається щорічне зростання, за 2022 рік зниження, а вже за результатами 2023 року кредитний портфель фізичних осіб склав 7 905 229 тис. грн, та перевищив показник довоєнного 2021 року.

Оцінювання дотримання інформаційної безпеки в напряму безпеки інформаційних ресурсів АТ «А – БАНК» показало, що АТ «А – БАНК» вже на ранніх стадіях інформаційної загрози визначає проблемні місця в

діяльності б та забезпечує захищеність фінансових інтересів банку, його клієнтів і акціонерів.

Зроблені висновки, що інформаційна інфраструктура є необхідною умовою в діяльності сучасних банків, оскільки вона забезпечує ефективне управління даними, оптимізацію процесів та підвищення безпеки. Інформаційні технології дозволяють банкам скорочувати витрати, підвищувати ефективність роботи, забезпечувати лояльність клієнтів та спрощувати надання послуг.

У третьому розділі **«Напрями удосконалення інформаційної безпеки банків України в умовах невизначеності»** зроблені висновки, щодо 1.

Розглянуто світові виклики одним із яких є безпека і співпраця в сучасному розрізненому світі та визначено, що за останні роки фінансовий сектор має дуже високий рівень вразливості до кіберзлочинів. Розглянутий досвід основних суттєвих подій ризику банків світу 1991 – 2017 рр, показує, що практично усі кіберризики на пряму, чи опосередковано пов'язані з недосконалістю, чи економії на інформаційній інфраструктурі, тому завданням управління кіберризиками повинно бути направлена на зниження їх виникнення та мінімізації розмірів втрат, а заходи щодо підвищення ефективності управління повинні бути спрямовані на поліпшення техніко-технологічних характеристик інформаційно-комп'ютерних систем, обладнання, програмного забезпечення та вдосконалення управління банком.

Найбільш розповсюдженими кіберзагрозами як для України, так і для зарубіжних країн є несанкціонований доступ до даних банку через злом комп'ютерних мереж банку. Найпоширенішим видом кіберзагроз є фішинг, виникнення якого відбувається через викрадення або пошкодження корпоративних і персональних даних, BEC/EAC-атаки.

Запропоновано про необхідність банкам на базовому рівні визначити універсальні міжнародні індикатори в забезпеченні кібербезпеки у вигляді єдиних стандартів доступу до даних, програмне забезпечення з вбудованими кодами.

Розглянуто досвід США в напряму впливу кібератак на фінансові установи та зазначено, що кожного року зростає вплив кіберзагроз на програмне забезпечення, що спонукає банки ще більш оптимізувати та удосконалювати свою інформаційну інфраструктуру.

Надані рекомендації що використання принципів планування реагування банків України впродовж воєнних дій в країні, а тощо: удосконалення інформаційної безпеки усіх видів діяльності банку, гнучкості при виборі захистів інформаційної та забезпеченні кіберстійкості банків.

Надані пропозиції основних напрямів щодо підвищення інформаційної безпеки банків в реаліях сьогодення до яких слід віднести: удосконалення системи контролю банків, через підвищення ролі контролінгу, через формування в працівниках банків професійної досконалості щодо прийняття правильних рішень та удосконалення підвищення фінансової грамотності населення України.

ВИСНОВКИ

У кваліфікаційній роботі наведено теоретичне узагальнення, яке полягає у розгляді сутності «інформаційна безпека банку» та запропонуванні рекомендацій щодо її підвищення в умовах невизначеності (воєнного стану).

За результатами виконаної кваліфікаційної роботи можемо зробити наступні висновки:

1. Визначено теоретичний аспект щодо сутності поняття «інформаційна безпека банку», базові елементи та функції. Залежно від підходів організації інформаційної безпеки банків запропоновано розглядати наступні напрями безпеки як інформаційне поле, інформаційні ресурси, інформаційна інфраструктура, які наддадуть можливості безризикової діяльності банку.

2. Розглянуто загрози, які впливають на інформаційну безпеку банків України в умовах невизначеності та зазначено, що їх необхідно розглядати в тісному взаємозв'язку одних з другими. Інформаційна безпека банків регулюється нормативно - правовими актами, які забезпечують оперативний контроль, регулювання інформаційної безпеки та відбувається корегування тактичних та стратегічних цілей для досягнення стратегій банків.

3. За результатами оцінка діяльності АТ «А – БАНК» в українському інформаційному полі визначено, що АТ «А – БАНК» не потрапляв під інформаційні атаки з боку конкурентів, персоналу, клієнтів, на офіційному сайті банку постійно оновлюється інформація. В інформаційному середовищі відсутня негативна інформація про його діяльність.

4. Оцінювання дотримання безпеки інформаційних ресурсів діяльності АТ «А – БАНК» через обслуговування клієнтів, як з боку залучення коштів (поточні, строкові), так і в напряму кредитування показала, що АТ «А – БАНК» дотримується усіх норм безпеки інформаційних ресурсів, завдяки чому має високу довіру з боку клієнтів.

5. З’ясовано, що основою для дотримання інформаційної безпеки банку первинним є захист його інформаційну (технологічну) інфраструктури. АТ «А – БАНК» контролює ефективність впроваджених заходів та засобів забезпечення інформаційної безпеки в інформаційних системах, які забезпечують їх функціонування.

6. Доведено, що міжнародний досвід підкреслює важливість комплексного підходу до інформаційної безпеки, який охоплює моніторинг, аналіз, прогнозування ризиків, розробку стратегій та заходів щодо захисту від інформаційних загроз.

7. У роботі були надані рекомендації підвищення інформаційної безпеки банків України в умовах діючого воєнного стану та під впливом кіберзагроз через удосконалення системи контролю банків, через підвищення ролі фінансового контролінгу, через формування в працівниках банків професійної досконалості щодо прийняття правильних рішень та удосконалення підвищення фінансової грамотності населення.