ЗАТВЕРДЖЕНО

рішення Наглядової Ради
АКЦІОНЕРНОГО ТОВАРИСТВА «БАНК ІНВЕСТИЦІЙ ТА ЗАОЩАДЖЕНЬ»

від «27» серпня 2025 р. № 27/08-4

ПОГОДЖЕНО

рішення Правління
АКЦІОНЕРНОГО ТОВАРИСТВА «БАНК ІНВЕСТИЦІЙ ТА ЗАОЩАДЖЕНЬ»

від «04» листопада 2024 р. № 04/11-1

ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ АТ «БАНК ІНВЕСТИЦІЙ ТА ЗАОЩАДЖЕНЬ»

м. Київ

ЗМІСТ

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1. Політика інформаційної безпеки АКЦІОНЕРНОГО ТОВАРИСТВА «БАНК ІНВЕСТИЦІЙ ТА ЗАОЩАДЖЕНЬ» (далі – Політика) визначає основні цілі, принципи та вимоги щодо інформаційної безпеки, описує функціонування системи управління інформаційною безпекою та її сферу застосування, а також ролі та відповідальності за забезпечення інформаційної безпеки.

1.2. Політика розроблена відповідно до вимог законодавчих актів та національних стандартів України, нормативно-правових актів Національного банку України (далі – НБУ) з питань інформаційної безпеки, а саме:

- Закону України «Про основні засади забезпечення кібербезпеки України»;
- ДСТУ ISO/IEC 27000:2019 "Інформаційні технології. Методи захисту. Система керування інформаційною безпекою. Огляд і словник термінів";
- ДСТУ ISO/IEC 27001:2023 "Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги";
- ДСТУ ISO/IEC 27002:2023 "Інформаційна безпека, кібербезпека та захист конфіденційності. Засоби контролювання інформаційної безпеки";
- Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України затвердженого постановою Правління НБУ від 28.09.2017 р. № 95;
- Положення про організацію кіберзахисту в банківській системі України затвердженого постановою Правління НБУ від 12.08.2022 р. № 178.

А також Політика розроблена з урахуванням вимог міжнародних стандартів з питань інформаційної безпеки, загальноприйнятих у міжнародній практиці принципів забезпечення інформаційної безпеки і кіберзахисту; вимог міжнародних та внутрішньодержавних платіжних систем та систем переказу коштів, вимог внутрішніх нормативних документів АТ «БІЗБАНК» (далі – Банк).

1.3. В Політиці використані наступні терміни та скорочення:

Загроза – потенційна причина небажаного інциденту, який може призвести до шкоди для системи або Банку.

Інформаційний актив – інформація в електронному та паперовому вигляді (що представляє цінність для Банку та/або його клієнтів, ділових партнерів і працівників), системне та прикладне програмне забезпечення, у тому числі інформаційні системи та бази даних, апаратне обладнання, що необхідні для оброблення, обміну або фізичного зберігання інформації в рамках бізнес-процесів Банку.

Інформаційна безпека – це сукупність організаційно-технічних заходів і засобів, спрямованих на захист інформації від широкого діапазону загроз з метою збереження таких властивостей інформації як конфіденційність, цілісність, доступність, а також забезпечення безперервності бізнес-процесів, мінімізації бізнес-ризику і отримання максимальної рентабельності інвестицій і бізнес-можливостей Банку.

Інформація з обмеженим доступом - відомості, що містять банківську, комерційну таємницю, конфіденційну та інсайдерську інформацію, персональні дані, службову інформацію, інформацію, що стосується здійснення Банком фінансового моніторингу, власником яких є Банк, або які є предметом професійного, ділового, виробничого, комерційного та інших інтересів Банку.

Інцидент інформаційної безпеки – це одинична подія або ряд небажаних та непередбачених подій безпеки, через які існує ймовірність компрометації бізнес-інформації і загрози інформаційній безпеці.

Подія інформаційної безпеки – це явище, яке відбулося, або відбувається в інформаційних системах і мережах за певних умов і може вплинути на інформаційну безпеку (спричиняти загрози, збій, втрату даних тощо).

Ризик інформаційної безпеки (складова операційного ризику) - імовірність виникнення збитків або додаткових втрат, або недоотримання запланованих доходів унаслідок порушення конфіденційності, цілісності, доступності даних в інформаційних системах Банку, недоліків або помилок в організації внутрішніх процесів або настання зовнішніх подій, уключаючи кібератаки або неадекватну фізичну безпеку. Ризик інформаційної безпеки включає кіберризик.

Система управління інформаційною безпекою (далі - СУІБ) – частина загальної системи управління Банку, заснована на підході впровадження заходів/засобів/ процесів/процедур інформаційної безпеки із застосуванням ризик-орієнтованого підходу при прийнятті рішень із метою досягнення визначеного рівня захищеності.

Третя сторона – особа (фізична або юридична), яка перебуває у будь-яких договірних відносинах з Банком і є стороною таких відносин.

Інші терміни та скорочення, що вживаються в цій Політиці, застосовуються у значеннях, визначених чинним законодавством України, у тому числі нормативно-правовими актами НБУ та внутрішніми нормативними документами Банку.

2. ОСНОВНІ ЦІЛІ ПОЛІТИКИ

2.1. Цілями Політики є впровадження та ефективне функціонування СУІБ, яка забезпечує:

- захист інформаційних ресурсів Банку від реальних та потенційних зовнішніх і внутрішніх загроз, та загроз, які пов’язані з навмисними та ненавмисними діями працівників Банку;
- безперервну роботу інформаційних систем Банку;
- мінімізацію ризиків інформаційної безпеки, як складової частини операційних ризиків, які властиві операційній діяльності Банку;
- мінімізацію впливу внутрішніх та зовнішніх негативних факторів на діяльність Банку;
- створення позитивної репутації Банку при роботі з клієнтами Банку та третіми сторонами.

2.2. Шляхи досягнення вищезазначених цілей:

- інвентаризація інформаційних активів Банку, регулярна оцінка та обробка ризиків інформаційної безпеки;
- документування та регламентація процедур, досягнення належного рівня інформаційної безпеки у відповідності до вимог п.1.1. Політики;
- регулярне проведення внутрішнього аудиту інформаційних технологій та/або інформаційної безпеки (в т.ч. СУІБ) і вимірювання ефективності процесів СУІБ;
- впровадження заходів щодо забезпечення безперервної діяльності інформаційних систем Банку у випадках настання (реалізації впливу) негативних факторів;
- підвищення обізнаності працівників Банку процедурам забезпечення інформаційної безпеки;
- реалізація положень «Стратегії розвитку інформаційної безпеки Банку в горизонті 2024-2026рр.».

3. СФЕРА ЗАСТОСУВАННЯ ПОЛІТИКИ

3.1. Вимоги визначені Політикою поширюються на Банк у цілому та охоплюють всі

аспекти діяльності Банку, включаючи всі підрозділи та процеси. Дія Політики також поширюється на треті сторони, які мають доступ до інформації з обмеженим доступом Банку.

3.2. Всі працівники Банку та треті сторони, незалежно від рівнів доступу до інформації та ресурсів інформаційно-комунікаційної системи, мають дотримуватись вимог цієї Політики.

4. СФЕРА ЗАСТОСУВАННЯ СУІБ

4.1. Мінімальною сферою застосування СУІБ є всі критичні бізнес-процеси Банку, а також підрозділи, інформаційні активи та технології, що забезпечують ці процеси. До сфери застосування можуть додаватися інші бізнес-процеси та активи, якщо вони стають критичними або Банк прагне підвищити загальний рівень інформаційної безпеки. Питання розширення сфери застосування розглядається на засіданні Комісії з питань СУІБ.

5. ПРИНЦИПИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

5.1. Політика інформаційної безпеки Банку ґрунтується на таких основних принципах:

- ***Законність.*** Забезпечення інформаційної безпеки здійснюється з дотриманням вимог законодавства України, нормативно-правових актів НБУ, а також інших регуляторних і контролюючих державних органів.
- ***Відповідність та адекватність до існуючих загроз, та економічна обґрунтованість.*** Організаційні контролі та технічні механізми захисту обираються та застосовуються відповідно до потреб бізнесу, та на основі оцінки ризиків інформаційної безпеки, зокрема аналізу актуальних загроз і вразливостей, а також витрат на впровадження та підтримку цих механізмів. Проводиться регулярна оцінка ефективності впроваджених заходів та механізмів захисту.
- ***Перспективність та орієнтація на національні та міжнародні відкриті стандарти.*** Організаційні заходи та технічні засоби СУІБ впроваджуються з урахуванням світових тенденцій у сфері інформаційної безпеки. Орієнтація на відкриті стандарти забезпечує використання накопиченого досвіду щодо захисту інформації.
- ***Безперервність функціонування.*** Забезпечується відмовостійкість, надійність, доступність та коректність функціонування інформаційних систем, процедур та засобів безпеки.
- ***Безперервність вдосконалення.*** Для забезпечення ефективної протидії загрозам інформаційної безпеки в умовах постійних змін внутрішнього та зовнішнього середовища реалізується безперервний цикл розвитку та вдосконалення СУІБ.
- ***Персональна відповідальність.*** Кожен працівник Банку несе персональну відповідальність за виконання функцій та обов'язків, покладених на нього в рамках СУІБ. У разі порушення вимог з інформаційної безпеки працівник може бути притягнутий до дисциплінарної, матеріальної, адміністративної або кримінальної відповідальності відповідно до законодавства України.
- ***Контроль.*** Здійснюється постійний контроль за виконанням працівниками Банку вимог з інформаційної безпеки.

6. ВИМОГИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

6.1. Для реалізації та подальшого вдосконалення СУІБ Банк чітко визначає нормативно-правові та регуляторні вимоги, що стосуються інформаційної безпеки. Перелік таких

вимог і правил, які становлять правову основу цієї Політики, наведено в Політиці управління інформаційною безпекою Банку.

6.2. Банк використовує ризик-орієнтований підхід, який забезпечує розуміння, моніторинг та зменшення ризиків інформаційної безпеки. Деталі управління ризиками інформаційної безпеки викладені в окремій методології.

6.3. Всі працівники Банку обізнані та виконують вимоги інформаційної безпеки в роботі. Банк сприяє створенню належного інформаційного поля для підвищення обізнаності працівників.

6.4. Під час розроблення, впровадження та функціонування програмно-технічних комплексів враховуються вимоги інформаційної безпеки.

6.5. Публічні сервіси та внутрішні мережі Банку відповідають вимогам стандартів з інформаційної безпеки. Банк сприяє проведенню модернізації обладнання та програмного забезпечення.

6.6. Банк забезпечує виконання усіх вимог з інформаційної безпеки, які наявні в угодах з третіми сторонами, у тому числі стосовно участі у міжнародних платіжних системах та системах переказу коштів.

6.7. Банк контролює дотримання вимог цієї Політики при наданні послуг третім сторонам, які в процесі надання послуг одержують доступ до інформації з обмеженим доступом Банку. Представники (користувачі) третіх сторін мають негайно повідомляти Банк про події безпеки та/або слабкі місця інформаційної безпеки.

6.8. Банк вимагає від третіх сторін знання і дотримання вимог з інформаційної безпеки, зокрема, укладає окремі угоди або включає застереження в договори про те, що третя сторона гарантує, що одержаний доступ до інформації з обмеженим доступом Банку буде використано виключно з метою надання послуг. Третя сторона на вимогу Банку зобов'язана надати перелік власних працівників, що допущені до надання послуг Банку та забезпечити виконання ними вимог з інформаційної безпеки. Банк в угодах (договорах) про нерозголошення інформації попереджає про відповідальність за порушення вимог з інформаційної безпеки.

6.9. Всі працівники Банку зобов'язані негайно сповістити про підозрілі події та інциденти інформаційної безпеки свого безпосереднього керівника та Управління інформаційної безпеки для аналізу та реакції (в тому числі на рівні комунікації). За результатами аналізу вживаються заходи, направлені на недопущення повторення подібних інцидентів в майбутньому.

6.10. Для зменшення ризиків виникнення інцидентів інформаційної безпеки, керівництво Банку створює умови для систематичного навчання працівників нормам та заходам інформаційної безпеки. Банк регулярно перевіряє рівень знань працівників з різних питань інформаційної безпеки.

6.11. Банк вимагає дотримання вимог з інформаційної безпеки під час обміну інформацією з використанням всіх засобів комунікацій. Обмін інформацією з обмеженим доступом Банку, по незахищеним каналам зв'язку не допускається. Усне обговорення питань з використанням інформації з обмеженим доступом має здійснюватися таким чином, щоб сторонні особи не були присутні під час такого обговорення (випадково чи навмисно).

6.12. У Банку складаються, діють, тестуються та оновлюються плани забезпечення безперервної діяльності на випадок непередбачених критичних ситуацій, таких як технічні або інфраструктурні аварії, а також кіберінциденти. Ці плани враховують пріоритети Банку щодо забезпечення безперервної діяльності критично важливих інформаційних систем. Оновлення планів узгоджуються з цією Політикою та сценаріями реагування на кіберінциденти, шляхом:

- зміни до планів забезпечення безперервної діяльності обговорюються та затверджуються Правлінням Банку, при цьому аналізується вплив змін на Політику та сценарії реагування. За потреби, ці зміни також вносяться до супутніх документів;
- плани регулярно тестуються для перевірки їх ефективності та відповідності актуальним загрозам і вимогам. Результати тестів документуються, розглядаються на засіданнях відповідних робочих груп і використовуються для вдосконалення планів.

7. РОЛІ ТА ВІДПОВІДАЛЬНОСТІ

7.1. Керівництво Банку чітко розуміє, що інформаційна безпека є основою життєдіяльності Банку та сприяє впровадженню, контролю та підтримці даної Політики.

7.2. У Банку створений та постійно діє колегіальний орган – Комісія з питань СУІБ, рішення якої є обов'язковими для виконання усіма працівниками Банку.

7.3. Документи з питань СУІБ розробляються структурними підрозділами за відповідними напрямками діяльності, доступні працівникам Банку у межах їх повноважень і призначені надавати допомогу у виконанні вимог інформаційної безпеки. Матриця RACI визначає ролі, обов'язки та відповідальності працівників Банку в процесах СУІБ та міститься в Додатку 2 до Політики управління інформаційною безпекою Банку.

7.4. Підрозділ інформаційної безпеки здійснює постійний моніторинг та поточний контроль дотримання вимог цієї Політики, виявляє потенційні загрози та реагує на інциденти. Підтримка Політики в актуальному стані покладена на керівника підрозділу з інформаційної безпеки.

7.5. Кожен працівник Банку здійснює самостійний контроль та перевірку своїх дій на відповідність вимогам інформаційної безпеки, забезпечує підтримку відповідного рівня інформаційної безпеки Банку в межах своїх посадових обов'язків та несе відповідальність за їх порушення згідно із законодавством України та внутрішньо-нормативними документами Банку.

7.6. Керівники Банку та структурних підрозділів Банку здійснюють попередній і поточний контроль за дотриманням підлеглими працівниками вимог з інформаційної безпеки.

7.7. Поточний та подальший контроль за загальним впровадженням, виконанням та вдосконаленням Політики здійснює Комісія з питань СУІБ.

7.8. Відповідальність за оперативний поточний та подальший контроль за впровадженням заходів безпеки інформації в усіх підрозділах Банку, а також за їх відповідність бізнес-потребам покладається на відповідальну особу за інформаційну безпеку (CISO). До основних завдань CISO належить стратегічне керівництво інформаційною безпекою, зокрема розробка та впровадження стратегії інформаційної безпеки, яка узгоджується із загальною стратегією розвитку Банку.

8. ПРИКІНЦЕВІ ПОЛОЖЕННЯ

8.1. Політика набирає чинності з дати її затвердження і діє до моменту скасування (втрати чинності) або затвердження нової редакції Політики.

8.2. Політика переглядається за необхідністю, але не менш ніж один раз на рік.

8.3. Причинами внесення змін до Політики, є зміни в інформаційній інфраструктурі та/або впровадження нових інформаційних технологій, зміни в законодавчих, регуляторних актах та внутрішніх документах Банку, які стосуються інформаційної безпеки.

8.4. У разі невідповідності будь-якої частини цієї Політики чинному законодавству

України, або нормативно-правовим актам Національного банку України, в тому числі у зв'язку з прийняттям нових актів законодавства України, або нормативних актів Національного банку України, ця Політика буде діяти лише у тій частині, яка не суперечитиме чинному законодавству України та нормативним актам НБУ. До внесення відповідних змін в Політику, працівники Банку в своїй роботі зобов'язані керуватись чинним законодавством України та нормативними вимогами НБУ.

8.5. Електронна версія затвердженої Політики доступна для ознайомлення у Електронній базі внутрішніх нормативних документів.

8.6. Управління ризиками в процесі забезпечення інформаційної безпеки Банку здійснюється на 3-х лініях захисту та з урахуванням вимог Положення про організацію системи внутрішнього контролю в банках України та банківських групах, затвердженого постановою Правління НБУ від 02.07.2019 № 88, Політики системи внутрішнього контролю Банку та Положення про внутрішній контроль у Банку.