ЗАТВЕРДЖЕНО
Рішенням Наглядової ради АТ «БТА БАНК»
Протокол №___ від «__» _____ 2025 р.

Голова Наглядової ради АТ «БТА БАНК»

_____Алібєк Мухамєд-Рахімов

СХВАЛЕНО
Рішенням Правління АТ «БТА БАНК»
Протокол № ___ від «__» _____ 2025 р.

Голова Правління АТ «БТА БАНК»

_____Євген БЕЗВУШКО

ПОЛІТИКА
ІНФОРМАЦІЙНОЇ БЕЗПЕКИ АТ «БТА БАНК»

Київ – 2025

ЗМІСТ

1. ТЕРМІНИ ТА СКОРОЧЕННЯ

1.1. Визначення та скорочення в цьому документі використовуються в таких значеннях:

- **Банк** — АКЦІОНЕРНЕ ТОВАРИСТВО «БТА БАНК» (АТ «БТА БАНК»).
- **Конфіденційність** — властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем та/або процесом.
- **Цілісність** — властивість інформації, яка полягає в тому, що інформація не може бути модифікована неавторизованим користувачем та/або процесом.
- **Доступність** — властивість ресурсу системи, яка полягає в гарантії своєчасного доступу авторизованих осіб і/або процесів до інформації, можливості використовувати ресурс відповідно до правил, встановлених політикою ІБ/кібербезпеки, відсутні простої в процесі обробки інформації, тобто коли інформація знаходиться у вигляді, необхідному користувачеві, в місці, необхідному користувачеві, і у той час, коли вона йому необхідна, а у випадку втрати інформації існує можливість своєчасного відновлення.
- **Спостережність** — властивість системи, що дозволяє фіксувати діяльність користувачів і процесів, використання пасивних об’єктів, а також однозначно установлювати ідентифікатори причетних до певних подій користувачів і процесів з метою запобігання порушення політики безпеки та/або забезпечення відповідальності за певні дії.
- **Політика** — Політика інформаційної безпеки.
- **Ризик** — імовірність виникнення збитків або додаткових втрат або недоотримання доходів, або невиконання стороною договірних зобов'язань унаслідок впливу негативних внутрішніх та зовнішніх факторів;
- **Ризик інформаційної безпеки (складова операційного ризику)** — ймовірність виникнення збитків або додаткових втрат, або недоотримання запланованих доходів внаслідок порушення конфіденційності, цілісності, доступності даних в інформаційних системах Банку, недоліків або помилок в організації внутрішніх процесів або настання зовнішніх подій, включаючи кібератаки або неадекватну фізичну безпеку. Ризик інформаційної безпеки включає кіберризик;
- **СУІБ** — система управління інформаційною безпекою.
- **Інформаційна безпека (ІБ)** — багаторівневий комплекс організаційних заходів Банку, програмних і технічних засобів, які забезпечують захист інформації від випадкових і навмисних загроз, у результаті реалізації яких можливе порушення доступності, цілісності, конфіденційності інформації, а також які забезпечують безперервність бізнес-процесів, зниження операційних ризиків і оптимізацію витрат Банку.
- **Інцидент інформаційної безпеки (інцидент ІБ)** — це поява одного або декількох небажаних або несподіваних подій інформаційної безпеки, які пов'язані з настанням або значною вірогідністю настання негативних наслідків для інформаційної безпеки, інформації, інформаційних активів, бізнес-процесів або завдати шкоди Банку та системі захисту.
- **Інцидент кібербезпеки (кіберінцидент)** – подія або ряд несприятливих подій ненавмисного характеру (природного, технічного, технологічного, помилкового, у тому числі внаслідок дії людського фактора) та/або таких, що мають ознаки можливої (потенційної) кібератаки, які становлять загрозу безпеці систем електронних комунікацій, систем управління технологічними процесами, створюють ймовірність порушення штатного режиму функціонування таких систем (у тому числі зриву та/або блокування роботи системи, та/або несанкціонованого управління її ресурсами), ставлять під загрозу безпеку (захищеність) електронних інформаційних ресурсів.
- **Інформаційний ресурс** — сукупність людських, апаратних та програмних ресурсів в інформаційних системах та процесах Банку.

- **Інформація з обмеженим доступом (ІзОД)** — це відомості які становлять банківську таємницю, комерційну таємницю, персональні дані та іншу конфіденційну інформацію Банку.
- **Кібербезпека** — захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі.
- Інші терміни, що вживаються в Політиці, використовуються в значеннях, визначених законами України, нормативно-правовими актами Національного банку та ДСТУ.

2. ЗАГАЛЬНІ ПОЛОЖЕННЯ

2.1. Політика інформаційної безпеки АТ «БТА БАНК» (далі – Політика) розроблена відповідно до внутрішніх документів Банку, вимог чинного законодавства України, у тому числі нормативно-правових актів Національного банку України, зокрема:

- Закону України “Про основні засади забезпечення кібербезпеки України”;
- Закону України “Про банки і банківську діяльність”;
- Закону України “Про захист персональних даних”;
- Закону України “Про хмарні послуги”;
- Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України, затверджене Постановою Правління Національного банку України (далі – НБУ) від 28.09.2017 № 95 (далі – Положення № 95) »;
- Положення про організацію кіберзахисту в банківській системі України та внесення змін до Положення про визначення об'єктів критичної інфраструктури в банківській системі України, затверджене постановою Правління НБУвід 12.08.2022 № 178;
- Положення про організацію системи управління ризиками в банках України та банківських групах, затверджене постановою Правління НБУ від 11.06.2018 №64, із змінами та доповненнями; (далі – Положення № 64)
- Положення про захист інформації та кіберзахист учасниками платіжного ринку (заголовок із змінами, внесеними згідно з постановою Правління НБУ від 13.06.2022. № 119), затверджене постановою Правління НБУ від 19.05.2021 № 43, із змінами та доповненнями;
- Положення про організацію системи внутрішнього контролю в банках України та банківських групах, затвердженим постановою Правління НБУ від 02.07.2019 № 88 (далі – Положення № 88);
- Національних стандартів України з питань інформаційної безпеки:

- ДСТУ ISO/IEC 27001:2023 (ISO/IEC 27001:2022, IDT) ”Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги”, прийнятий наказом Державного підприємства "Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості" від 17.08.2023 № 210;
- ДСТУ ISO/IEC 27002:2023 (ISO/IEC 27002:2022, IDT) “Інформаційна безпека, кібербезпека та захист конфіденційності. Засоби контролювання інформаційної безпеки”, прийнятий наказом Державного підприємства "Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості" від 17.08.2023 № 210.

- Статуту АТ “БТА Банк”,

та з урахуванням міжнародних стандартів з питань інформаційної безпеки, кібербезпеки та безпеки інформації у хмарних середовищах, загальноприйнятих у міжнародній практиці принципів забезпечення інформаційної безпеки та кіберзахисту.

2.2. Політика є внутрішнім документом АКЦІОНЕРНОГО ТОВАРИСТВА «БТА БАНК», що описує та регламентує функціонування системи управління інформаційною безпекою/кібербезпекою Банку відповідно до вимог законів України, нормативно-правових актів НБУ, міжнародних норм, стандартів і правил захисту інформації та інформаційних

систем. Складові процесу управління інформаційною безпекою, які не зазначені у Політиці, представлені в інших внутрішніх документах Банку (порядках, процедурах тощо).

2.3. Ціллю Політики є впровадження та ефективне функціонування системи управління інформаційною безпекою, яка забезпечує:

- захист інформаційних ресурсів Банку (у тому числі тих, що розташовані у хмарному середовищі) від реальних та потенційних зовнішніх і внутрішніх загроз, у тому числі пов'язаних з навмисними та ненавмисними діями працівників Банку;
- безперервну роботу Банку;
- зменшення ризиків операційної діяльності Банку;
- підтримання доброчесної ділової репутації і ділової корпоративної культури Банку.

2.4. Дія цієї Політики поширюється на всі підрозділи Банку. Зміст Політики доводиться до відома всього персоналу Банку, та, за необхідності, представникам третіх сторін. Під час прийому на роботу працівники ознайомлюються з Політикою під підпис із зобов'язанням про дотримання конфіденційності.

2.5. Відповідальність за ознайомлення працівників при прийомі на роботу з вимогами ІБ/кібербезпеки, нормативними та організаційно-розпорядчими документами з питань ІБ/кібербезпеки, навчання персоналу з питань ІБ/кібербезпеки несуть, в рамках компетенції Управління інформаційної безпеки (далі – УІБ) та Управління по роботі з персоналом.

2.6. Політика використовується для усіх критичних бізнес-процесів/банківських продуктів/програмно-технічних комплексів Банку, є обов’язковою до виконання всіма працівниками Банку, а також особами, які працюють з інформацією, що належить Банку, у межах укладених контрактів та договорів.

2.7. Сферою застосування СУІБ є Банк в цілому та всі критичні бізнес-процеси Банку.

3. ОРГАНІЗАЦІЙНА СТРУКТУРА ПРОЦЕСУ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

3.1. Банк забезпечує організацію системи управління інформаційної безпеки, дотримуючись моделі трьох ліній захисту:

- **перша лінія** – на рівні бізнес-підрозділів та підрозділів підтримки діяльності Банку;
- **друга лінія** – Служба управління ризиками, що координує в цілому систему управління операційним ризиком, виконує методологічні та контрольні функції з управління операційним ризиком з дотриманням вимог Політики управління операційним ризиком в АТ «БТА БАНК» (окрім комплаєнс та ризик у сфері ПВК\ФТ), Служба комплаєнс-контролю, яка забезпечує контроль дотриманням норм законодавства, та внутрішніх документів Банку;
- **третя лінія захисту** – внутрішній аудит, який здійснює оцінку ефективності системи управління операційним ризиком підрозділами першого та другого рівнів захисту, включаючи оцінку ефективності системи внутрішнього контролю.

Відповідно до застосовуваної в Банку моделі трьох ліній захисту – підрозділ інформаційної безпеки відноситься до першої лінії захисту. В рамках системи управління ризиками підрозділ з інформаційної безпеки несе відповідальність за ризики інформаційної безпеки та кіберризики (далі – ризики ІБ) та звітує Правлінню Банку щодо поточного стану управління такими ризиками та Системи управління інформаційною безпекою в цілому.

3.2. Банк при щорічному перегляді Політики інформаційної безпеки визначає зацікавлені сторони СУІБ, їх ролі, відповідальності та враховує їх вимоги.У процесі управління інформаційною безпекою, у межах визначених повноважень та відповідальності:

Наглядова рада Банку:

- здійснює контроль за забезпеченням інформаційної безпеки / кіберзахисту шляхом:

- затвердження документів з питань управління інформаційною безпекою та кіберзахистом, в тому числі, затверджує Стратегію розвитку інформаційної безпеки Банку, План забезпечення безперервності діяльності Банку, в якому враховано безперервність функціонування заходів інформаційної безпеки в рамках процесу управління безперервністю діяльності Банку;
- забезпечення фінансування (затвердження бюджету) щодо підтримання на належному рівні програмного та технічного забезпечення Банку;
- отримання регулярної звітності щодо управління ризиками, виконання бюджету, тощо;
- отримання аудиторських звітів про проведені Службою внутрішнього аудиту аудиторські перевірки;
- розгляду звітів ризиків ІБ;

- визначає перелік відомостей, що становлять інформацію з обмеженим доступом, в тому числі комерційну таємницю та конфіденційну інформацію про діяльність Банку, та порядок їх використання та охорони.

Правління Банку:

- забезпечує впровадження та функціонування СУІБ відповідно до нормативно-правових актів НБУ, в тому числі:

- впроваджує єдину методологію з організації управління ІБ/кібербезпеки, ідентифікації і оцінки ризиків ІБ;
- відповідає за призначення відповідальних осіб за забезпечення ІБ, кіберзахисту Банку;
- відповідає за розробку і підтримку заходів забезпечення безперервності діяльності Банку;
- впроваджує політики управління ризиками ІБ;
- затверджує процедури управління ризиком ІБ, процедури проведення операцій;
- здійснює контроль за управлінням ризиками ІБ.

- забезпечує безпеку інформаційних систем Банку і систем, що застосовуються для зберігання активів клієнтів.

Робоча група з питань системи управління інформаційної безпеки (далі – РГ СУІБ)

У Банку функціонує РГ СУІБ - є постійно діючим колегіальним органом Банку, який забезпечує процес розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та вдосконалення системи управління інформаційною безпекою (далі - СУІБ) шляхом прийняття відповідних рішень.

РГ СУІБ:

- переглядає та погоджує політику інформаційної безпеки, положення щодо застосовності та стратегії розвитку інформаційної безпеки Банку;
- узгоджує впровадження нових проектів, напрямів, стратегічних завдань з питань інформаційної безпеки Банку та заходів інформаційної безпеки;
- розглядає, затверджує та контролює виконання проектів щодо розроблення, упровадження, функціонування, моніторингу, перегляду, підтримання та вдосконалення СУІБ Банку;
- визначає необхідні оптимальні ресурси для впровадження заходів інформаційної безпеки;
- організовує практичні заходи щодо підвищення обізнаності/навчання персоналу Банку з питань інформаційної безпеки;
- забезпечує своєчасний моніторинг стану впровадження та ефективності функціонування СУІБ Банку з подальшою оцінкою можливостей удосконалення та потреби проведення коригувальних дій.

Відповідальний за інформаційну безпеку в Банку (Chief Information Security Officer):

- забезпечує стратегічне керівництво з питань інформаційної безпеки Банку;
- визначає напрямки розвитку інформаційної безпеки Банку, їх відповідність стратегії розвитку Банку;

- приймає рішення щодо внесення змін до стратегії розвитку ІБ в рамках її планового перегляду, або позапланового, через значні зміни, які впливають на державну діяльність або на діяльність Банку;
- забезпечує відповідність заходів безпеки інформації потребам бізнес-процесів/банківських продуктів;
- контролює впровадження заходів безпеки інформації в Банку;
- виносить питання щодо застосування заходів впливу до порушників вимог інформаційної безпеки;
- забезпечує виконання заходів щодо перегляду та підтримання в актуальному стані переліку об'єктів критичної інформаційної інфраструктури, надання актуального переліку об'єктів критичної інформаційної інфраструктури до НБУ;
- забезпечує виконання заходів щодо перегляду та підтримання в актуальному стані відомостей про об'єкти критичної інформаційної інфраструктури, надання актуальних відомостей до НБУ;
- забезпечує участь Банку у інформаційному обміну з НБУ та іншими банками України;
- забезпечує пріоритетну реалізацію заходів кіберзахисту критичної інформаційної інфраструктури Банку відповідно до розробленого Плану реагування на кіберзагрози, кібератаки та кіберінциденти відносно інформаційних систем АТ « БТА БАНК»;
- забезпечує надання інформації про аутсорсинг функції кіберзахисту Банку на запит НБУ в обсязі та в термін, що встановлені в такому запиті;
- забезпечує створення умов для підвищення кваліфікації працівників Управління інформаційної безпеки, навчання працівників Банку стосовно цифрових навичок, кіберобізнаності щодо сучасних кіберзагроз та протидії їм.

Управління інформаційної безпеки:

- забезпечує функціонування системи управління інформаційною безпекою у відповідності до вимог чинного законодавства, нормативно – правових актів НБУ, міжнародних платіжних систем, інших контрагентів Банку, регуляторних органів, стандартів PCI DSS, 3D Security тощо;
- здійснює управління ризиками інформаційної безпеки/кіберризиками Банку;
- здійснює розробку, актуалізацію та тестування планів безперервності діяльності бізнес-процесів та інформаційних систем Банку;
- здійснює управління рольовою моделлю та доступами до інформаційних ресурсів Банку;
- здійснює контроль за виконанням заходів щодо забезпечення безпеки інформації на всіх стадіях життєвого циклу інформаційних систем Банку;
- забезпечує організаційний та технічний захист інформації;
- здійснює управління вразливостями та інцидентами інформаційної безпеки/кіберінцидентами;
- контролює витік інформації з обмеженим доступом, здійснює управління захистом персональних даних, в тому числі проводить аналіз загроз безпеки персональних даних та забезпечує організацію та контроль дотримання норм законодавства України щодо захисту персональних даних у Банку;
- розробляє або бере участь у розробленні документів Банку щодо інформаційної безпеки та кіберзахисту;
- забезпечує надання до Служби управління ризиками даних щодо внутрішніх подій (інцидентів) інформаційної безпеки/кіберінцидентів.

Інші підрозділи, які залучаються до процесу управління інформаційною безпекою.

Департамент інформаційних технологій:

- співпрацює з Управлінням інформаційної безпеки з питань оцінки ризиків ІБ при впровадженні нових проектів;
- забезпечує усунення вразливостей в інформаційних системах, які були виявлені Управлінням інформаційної безпеки;
- забезпечує дотримання вимог ІБ під час розроблення, модернізації та придбання інформаційних ресурсів;
- забезпечує безпечне конфігурування серверних операційних систем, баз даних та мережевого обладнання;
- забезпечує належне користування хмарними технологіями з метою дотримання конфіденційності, цілісності та доступності інформації, яка циркулює в хмарному середовищі.

Департамент банківської безпеки:

- забезпечує проведення внутрішніх службових розслідувань з метою підтвердження фактів порушення вимог інформаційної безпеки;
- розглядає питання впровадження заходів зі збереження інформаційних ресурсів Банку від зовнішніх та внутрішніх загроз;
- протидіє кіберзлочинності та телефонному шахрайству, забезпечує високий рівень захисту електронних платежів та послуг;
- відповідає за забезпечення фізичного захисту інфраструктури Банку.

Управління по роботі з персоналом:

- виявляє кадрові ризики кандидатів та працівників Банку, які ґрунтуються на перевірці подій минулого або вчинків та зловживань;
- спільно з Управлінням інформаційної безпеки, в межах компетенції здійснює організацію проведення навчання та тестування працівників Банку з питань інформаційної безпеки/кібербезпеки.

Служба управління ризиками:

- розробляє, впроваджує та забезпечує постійний розвиток системи управління операційним ризиком;
- оцінює величину операційного ризику Банку.
- здійснює контроль за розробленням Плану забезпечення безперервної діяльності;
- розробляє разом з підрозділами першої лінії захисту перелік специфікацій ключових індикаторів операційного та ризику ІБ;
- забезпечує своєчасну ідентифікацію і попередження подій операційного ризику ІБ.

Служба комплаєнс-контролю:

- забезпечує організацію контролю за захистом персональних даних відповідно до законодавства України;
- забезпечує організацію контролю за дотриманням Банком норм законодавства, внутрішніх документів, в тому числі процедур, та відповідних стандартів професійних об'єднань, ринкових стандартів дія яких поширюється на Банк;
- забезпечує моніторинг змін у законодавстві та відповідних стандартах професійних об'єднань, дія яких поширюється на Банк, та здійснює оцінку впливу таких змін на процеси та процедури, запроваджені в Банку, а також забезпечує контроль за імплементацією відповідних змін у внутрішні документи;

Юридичний департамент:

- надає правову підтримку при визначенні заходів впливу в межа чинного законодавства України щодо порушників вимог інформаційної безпеки;
- відповідно до встановленого в Банку порядку погоджує проекти внутрішніх положень Банку з інформаційної безпеки та перевіряє їх відповідність статутним документам Банку, нормам чинного законодавства;

- забезпечує правову підтримку діяльності Банку для коректного тлумачення законодавства з метою відповідності вимогам з питань інформаційної безпеки.

Всі працівники Банку:

- відповідають за захист інформаційних ресурсів, до яких вони мають доступ. Їх обов'язки включають як захист комп'ютерної і некомп'ютерної інформації, так і інформаційних пристроїв, що знаходяться у них на зберіганні чи у володінні;
- повинні дотримуватись політик і процедур ІБ/кібербезпеки;
- мають використовувати інформаційні системи відповідно до цієї Політики, вимог до безпеки певних систем або прикладних програм;
- повинні використовувати наявні захисні механізми для забезпечення цілісності та конфіденційності інформації.

3.4. **Зовнішні зацікавлені сторони:Верховна Рада України:**

- приймає нові законодавчі акти, які впливають на подальшу роботу банківської системи та необхідність внесення змін до СУІБ.

Державні структури (КМУ, Мінфін, ДССЗЗІ, СБУ та інші державні органи):

- визначають умови функціонування Банку, як об'єкта критичної інфраструктури України;
- сприяють покращенню захисту інформаційних ресурсів та участі у центрах з інформаційної безпеки та координації.

Національний банк України:

- визначає умови роботи банківських систем;
- висуває вимоги щодо архітектури інформаційної безпеки;
- впроваджує нові або вносить зміни у поточні інформаційні системи НБУ;
- здійснює перевірку стану впровадження СУІБ Банку та повноту виконання заходів з безпеки інформації.

Надавачі хмарних послуг:

- надають хмарні послуги відповідно до визначеного рівня інформаційної безпеки/кібербезпеки;

Кримінальні структури, комп'ютерні злочинці, хакери, шахраї:

- прагнуть розкрити/викрасти інформацію з обмеженим доступом за допомогою технічних або програмних засобів, людського фактору, та вчинення спроб негативного впливу на репутацію Банку;
- підбурюють/залучають працівників Банку з метою отримання власної вигоди та сприяють на вчинення протиправних дій.

Конкурентні організації:

- сприяють/стимулюють на пошук та створення нових конкуренто спроможних рішень/продуктів, покращення діючих процесів та збільшення привабливості на ринку.

Клієнти:

- досвід використання продуктів клієнтами сприяє визначенню подальшого розвитку СУІБ, впровадженню заходів з безпеки інформації.

Держави-агресори, держави-спонсори тероризму (ворожі країни):

- такі країни як РФ, Республіка Білорусь та інші країни, які підтримують їх в збройній агресії проти України впливають на розвиток СУІБ через розгортання інформаційної війни у кіберпросторі, а також військових дій, актів тероризму на території України;
- виступають спонсорами кримінальних структур, комп'ютерних злочинців та хакерів.

4. ПІДХОДИ ЩОДО УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

4.1. Підходи до визначення цілей СУІБ.

Для підтримання належного захисту інформації (насамперед інформації з обмеженим доступом) із забезпеченням її цілісності, конфіденційності, доступності та спостережності

визначаються цілі інформаційної безпеки. Цілі інформаційної безпеки виражаються у вигляді характеристик і параметрів, для досягнення яких впроваджуються заходи інформаційної безпеки, та встановлюються якісні та кількісні показники в системі внутрішнього контролю процесів СУІБ.

Джерелами для формування цілей інформаційної безпеки є зовнішні та внутрішні фактори, що визначають діяльність Банку, а саме:

- закони України;
- стандарти інформаційної безпеки, в тому числі, міжнародні;
- нормативно-правові акти НБУ;
- правила платіжних систем та систем переказу коштів, учасником яких є Банк;
- угоди з третіми сторонами;
- результати оцінки ризиків, які враховують загальну бізнес-стратегію та цілі діяльності Банку;
- внутрішні документи Банку, що регламентують принципи обміну та обробки інформації відповідно до бізнес-потреб.

Цілі інформаційної безпеки затверджуються окремим розділом у внутрішньому документі Банку з управління СУІБ.

4.2. **Управління ризиками інформаційної безпеки.**

При управлінні ризиками інформаційної безпеки Банк керується основними принципами системи управління ризиком в Банку:

1. дотримання моделі трьох ліній захисту;
2. створення та впровадження процедури управління ризиком інформаційної безпеки з метою ефективного управління ризиком інформаційної безпеки/кіберризиком;
3. забезпечення своєчасного виявлення загроз інформаційної безпеки та усунення ризиків інформаційної безпеки;
4. виявлення і врахування факторів ризику, які загрожують доступності, цілісності, конфіденційності інформації в Банку;
5. забезпечення обізнаності працівників Банку щодо ризиків інформаційної безпеки.

4.3. **Управління інцидентами інформаційної безпеки.**

1. Виявлення і фіксація подій ІБ найбільш ефективним шляхом, підтвердження їх класифікації як інцидентів ІБ/кіберінцидентів;
2. Послідовна оцінка і безперервне реагування на виявлені інциденти ІБ/кіберінциденти найбільш сприятливим та ефективним чином;
3. Застосування ефективної системи управління інцидентами для зведення до мінімуму несприятливих наслідків для Банку;
4. Використання своєчасного інформування відповідальних осіб за інформаційну безпеку про інциденти ІБ/кіберінциденти;
5. Впровадження моніторингу, оцінки та усунення вразливостей ІБ для скорочення кількості інцидентів;
6. Отримання досвіду за результатами управління інцидентами ІБ.

4.4. **Підходи до управління та моніторингу ІБ.**

Для управління інформаційною безпекою в Банку використовується ефективне поєднання технічних та організаційних рішень, що дозволяє досягти високої якості моніторингу стану СУІБ.

Технічні рішення є сукупністю засобів для збору відомостей про стан елементів інформаційних систем, а також засобів впливу на їх поведінку. Зокрема засоби моніторингу шкідливого ПЗ, а також системи управління подіями і інцидентами інформаційної безпеки.

Організаційні рішення використовуються у вигляді налагодження процесів взаємодії людей (працівників), спрямованих на забезпечення необхідного рівня моніторингу ІТ-систем і підсистем ІБ.

5. ПРИНЦИПИ, ПРАВИЛА ТА ВИМОГИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ.

5.1. Основним принципом інформаційної безпеки є підтримання належного захисту інформації (насамперед інформації з обмеженим доступом) із забезпеченням її цілісності, конфіденційності, доступності та спостережності.

5.2. Принципами забезпечення інформаційної безпеки є:

- системний (комплексний) підхід до забезпечення інформаційної безпеки Банку;
- безперервність процесу удосконалення та розвитку інформаційної безпеки та його здійснення шляхом обґрунтування та реалізації раціональних засобів, методів, заходів із застосуванням найкращого міжнародного досвіду;
- своєчасність та адекватність заходів захисту від реальних та потенційних загроз інформаційній безпеці Банку;
- контроль та забезпечення підтримки належного рівня інформаційної безпеки з боку керівників Банку;
- забезпечення достатності ресурсів, у тому числі фінансових, для сталого розвитку систем інформаційної безпеки.

5.3. Управління інформаційної безпеки Банку безпосередньо підпорядковується відповідальній особі за інформаційну безпеку Банку (CISO).

5.4. Керівництво Банку всіляко підтримує впровадження інформаційної безпеки та забезпечує її фінансування на достатньому рівні.

5.5. Документи з питань інформаційної безпеки/кіберзахисту розробляються Управлінням інформаційної безпеки та іншими підрозділами за відповідними напрямками діяльності. Постійний контроль впровадження, виконання, вдосконалення та підтримки Політики в актуальному стані покладено на Управління інформаційної безпеки та РГ СУІБ.

5.6. Банк розробляє внутрішні документи, які визначають, зокрема:

- вимоги щодо використання, надання, скасування та контролю доступу до інформаційних систем Банку;
- вимоги щодо безпеки інформації під час використання змінних носіїв інформації;
- вимоги до забезпечення захисту від зловмисного коду та організації захисту від зловмисного коду;
- використання криптографічних засобів для захисту інформації;
- процес управління ключами;
- процес управління оновленнями;
- вимоги щодо безпеки інформації, технічного обслуговування, експлуатації факсимільних апаратів, багатофункціональних пристроїв, телефонів та/або телефонних систем;
- вимоги щодо використання електронної корпоративної пошти;
- вимоги щодо підбору, застосування або модернізації програмних та апаратних засобів обробки інформації або в разі придбання, а також порядок виведення з експлуатації обладнання інформаційних систем Банку;
- вимоги щодо процесу управління інцидентами інформаційної безпеки.

5.7. У Банку діє принцип надання мінімального рівня повноважень під час надання доступу до інформаційних систем Банку (включаючи доступ привілейованих користувачів).

5.8. В інформаційних системах Банку, які безпосередньо забезпечують автоматизацію банківської діяльності, забороняється суміщення в межах однієї функції (ролі) таких повноважень: розроблення та супроводження (адміністрування), розроблення та експлуатація, супроводження (адміністрування) та експлуатація, виконання операцій в таких системах та подальшого контролю за їх виконанням.

5.9. Під час розроблення, впровадження та функціонування програмно-технічних комплексів обов'язково враховуються вимоги інформаційної безпеки.

5.10. Публічні сервіси Банку та внутрішні мережі Банку мають відповідати вимогам стандартів з інформаційної безпеки.

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

5.12. Банк підтримує високий рівень безпеки інформації, яка обробляється, зберігається та передається за допомогою хмарних технологій зберігання даних.

5.13. У Банку розроблено та затверджено план забезпечення безперервності діяльності Банку, у якому враховано безперервність функціонування заходів інформаційної безпеки в рамках процесу управління безперервністю діяльності Банку.

5.14. Відповідальність структурних підрозділів Банку в частині інформаційної безпеки визначається внутрішніми документами Банку.

5.15. Кожен працівник Банку під час виконання своїх посадових обов'язків і повноважень повинен забезпечувати виконання вимог інформаційної безпеки Банку. Працівники Банку несуть відповідальність за невиконання вимог інформаційної безпеки, встановлених внутрішніми документами Банку та нормами чинного законодавства.

5.16. Банк підтримує програму підвищення обізнаності/навчання працівників Банку з питань безпеки інформації/кіберзахисту з урахуванням досвіду, отриманого за результатами вирішення інцидентів безпеки інформації.

5.17. Банк впроваджує заходи щодо дотримання законодавства про захист персональних даних, а також договірних умов, узгоджених з партнерами, підрядниками та відповідними третіми сторонами. Банк визнає свою відповідальність за захист приватності та конфіденційності персональних даних, а також за забезпечення безпечної обробки та зберігання таких даних.

6. ПЕРЕГЛЯД ПОЛІТИКИ

6.1. Банком забезпечується підтримка Політики в актуальному стані. Політика переглядається один раз на рік та/або за необхідністю.

6.2. Причинами внесення змін до Політики є зміни в актах чинного законодавства України, в тому числі нормативно-правових актах НБУ, та інших документах, що регламентують питання функціонування СУІБ.

7. ВНУТРІШНІЙ КОНТРОЛЬ

7.1. Внутрішній контроль у сфері інформаційної безпеки є невід’ємною частиною системи управління Банком та спрямований на забезпечення виконання вимог цієї Політики, нормативно-правових актів НБУ, чинного законодавства та договірних зобов’язань Банку. Контроль здійснюється на всіх етапах життєвого циклу бізнес-процесів, інформаційних активів і банківських продуктів.

7.2. Управління інформаційної безпеки відповідає за розробку, повноту та актуальність внутрішніх документів з інформаційної безпеки, координує впровадження організаційних, технологічних та технічних заходів, здійснює погодження істотних змін у системах та проводить оцінку їхнього впливу на інформаційну безпеку.

7.3. Департамент інформаційних технологій спільно з Управлінням інформаційної безпеки реалізує технологічні та технічні заходи з організації безпечних каналів обміну інформацією, забезпечує виконання регламентів, розподілу доступів і повноважень, впроваджує та супроводжує механізми захисту інформації в програмно-технічних комплексах Банку.

7.4. Керівництво Банку здійснює стратегічний контроль за реалізацією Політики, періодично затверджує звіти про стан інформаційної безпеки та управління ризиками, а також ініціює перегляд внутрішніх документів на відповідність вимогам НБУ, законодавства України, правил платіжних систем та договірних зобов’язань.

7.5. Виконання вимог цієї Політики контролюється Управлінням інформаційної безпеки та РГ СУІБ. Контроль включає перевірку виконання технічних, організаційних та

регламентних вимог, своєчасності оновлень, а також ефективності заходів захисту, а його результати оформлюються звітами, які подаються Правлінню Банку з пропозиціями щодо усунення виявлених невідповідностей.

7.6. Профільні підрозділи Банку, що беруть участь у розробці та узгодженні цієї Політики, несуть відповідальність за її зміст і актуальність положень у межах своєї компетенції.

8. ЗАКЛЮЧНІ ПОЛОЖЕННЯ

8.1 Політика набирає чинності з моменту її затвердження рішенням Наглядової ради та діє до її скасування чи до затвердження нового документа, з набранням чинності якого попередній втрачає силу.

8.2 Перегляд Політики здійснюється не рідше ніж 1 (один) раз на рік. Якщо за результатами перегляду зміни до Політики не вносяться, то повторне її затвердження не потрібно.

8.3 У разі невідповідності будь-якої частини Політики вимогам законодавства, нормативно-правових актів НБУ, в тому числі в зв'язку з прийняттям нових законодавчих та/або нормативно-правових актів або удосконалення чинних, Політика буде діяти лише в тій частині, що не суперечитиме законодавству та нормативно-правовим актам НБУ.

8.4 У випадку зміни найменування підрозділів Банку за умови збереження за ними відповідних функціональних обов’язків, дії цих підрозділів, що регламентуються Політикою, не змінюються.