ЗАТВЕРДЖЕНО:
рішенням Спостережної ради
ПАТ «АП БАНК»
від 10.04.2018, протокол №8

Голова Спостережної ради
ПАТ «АП БАНК»

А.І. Кутова

ПОЛІТИКА

ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

ПАТ «АП БАНК»

м. Київ, 2018

Розділ І. Призначення та сфера застосування

1.1. Ця Політика інформаційної безпеки (далі - Політика) є внутрішнім нормативним документом, що формулює та висловлює позицію ПАТ «АП БАНК» (надалі — Банк) щодо інформаційної безпеки (далі — ІБ), а також визначає основні принципи та завдання системи управління інформаційною безпекою (далі — СУІБ) Банку. Політика є нормативною основою для захисту інформаційних активів Банку з метою забезпечення:

- **конфіденційності** – забезпечення доступності інформації, активів тільки для авторизованих осіб, користувачів, процесів в мінімально необхідному обсязі;
- **цілісності** – захисту точності, коректності та повноти активів і методів обробки інформації;
- **доступності** – забезпечення безперервного доступу до інформаційних і супутніх активів і сервісів Банку, згідно з наданими користувачам повноваженням і правами у мінімально необхідному обсязі;
- **спостережності** – забезпечення можливості визначення користувачів, процесів, що працюють з тим чи іншим інформаційним активом Банку, час та дату такої роботи, а також забезпечення принципу неможливості відмови від виконаних дій.

1.2. Політика базується на вимогах законодавчих, регуляторних та нормативних документів з інформаційної безпеки.
1.3. Дія Політики поширюється на весь Банк та всі треті сторони, які мають доступ до інформаційних активів Банку.

Розділ ІІ. Нормативна база

2.1. Політика розроблена у відповідності до вимог чинного законодавства України, а саме:
- Законів України «Про банки і банківську діяльність», «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про захист персональних даних»;
- нормативно-правових актів з інформаційної безпеки Національного банку України (НБУ), а також стандартів ДСТУ ISO/IEC 2700x:2015;
- інших нормативних документів, що регламентують вимоги до інформаційної безпеки.

2.2. В цій Політиці терміни та скорочення вживаються в такому значенні:

Керівництво Банку (керівництво) – Голова та Члени Правління Банку, Голова та Члени Спостережної Ради.

Інформаційні активи – всі комп'ютерні системи, програмне забезпечення та інше периферійне обладнання, яке використовується для обробки або зберігання даних, а також інформація, що обробляється за їх допомогою.

Інформаційна безпека (ІБ) – сукупність процесів та заходів, які мають на меті забезпечення цілісності, конфіденційності, доступності та спостережності інформації.

Інформаційні системи (ІС) - комп'ютерні системи, програмне забезпечення, телекомунікаційне та периферійне обладнання.

Власник інформаційної системи (далі – власник ІС) - підрозділ Банку, що використовує цю систему для забезпечення процесів підрозділу та має ухвалену керівництвом Банку відповідальність щодо контролювання впровадження, розвитку, підтримування, використання та безпеки цієї системи.

Заходи безпеки – засоби керування ризиком, включаючи політики, процедури, інструкції, практики та організаційну структуру, які можуть носити адміністративний, технічний, управлінський чи юридичний характер.

Загроза - будь-які обставини чи події, що можуть спричинити порушення політики ІБ та нанесення збитку Банку.

Вразливість - нездатність протистояти реалізації певної загрози або ж сукупності загроз.

Ризик ІБ (ризик) – ймовірність того, що визначена загроза, впливаючи на вразливості системи або групи систем, може спричинити шкоду Банку.

Система управління інформаційною безпекою (СУІБ) – частина загальної системи управління Банку, заснована на підході оцінки ризиків, призначена для створення,

впровадження, експлуатації, контролю, аналізу, підтримки і покращення інформаційної безпеки Банку.

Розділ ІІІ. Принципи та цілі ІБ

3.1. Забезпечення ІБ та СУІБ Банку ґрунтуються на таких фундаментальних принципах:

- **Принцип законності:** СУІБ Банку виконує вимоги чинного законодавства України, а також застосовує міжнародні норми в галузі ІБ.
- **Принцип узгодженості:** цілі та завдання ІБ відповідають стратегічним цілям та завданням Банку.
- **Принцип єдності:** управління інформаційної безпекою є невід'ємною частиною управління Банком.
- **Принцип ефективності:** засоби захисту інформаційних активів впроваджуються відповідно до їхньої критичності, тобто категорії класифікації та рівня ризику інформаційного активу.
- **Принцип практичності:** засоби захисту інформаційних активів повинні бути практичними та підтримувати баланс між працездатністю і захищеністю ІС.
- **Принцип безперервності:** ІБ є постійним процесом протистояння загрозам та управління ризиками, характерними для сфери діяльності Банку.
- **Принцип відповідальності:** керівництво Банку всіх рівнів, працівники, бізнес-партнери та інші треті сторони, які мають доступ до інформаційних активів Банку, повинні дотримуватися вимог нормативних документів Банку в області ІБ та нести персональну відповідальність за їхнє невиконання.
- **Принцип комплексності та системності:** ІБ Банку забезпечується на правовому, адміністративному, організаційному та програмно-технічному рівнях, а також на підставі комплексного застосування засобів захисту інформації та взаємодії всіх підрозділів Банку.

3.2. Принципи ІБ інтегровані в усі аспекти управління процесами та інформаційними технологіями Банку.

3.3. Основними цілями ІБ Банку є:

- забезпечення безпеки персоналу та клієнтів Банку;
- управління інформаційної безпекою, у тому числі визначення ролей та обов'язків у галузі ІБ, створення і підтримка системи управління ІБ (СУІБ) Банку;
- класифікація інформаційних активів;
- здійснення оцінки ризиків ІБ;
- забезпечення безпеки інформаційних активів відповідно до категорії їх класифікації та оцінки ризиків;
- моніторинг подій ІБ та управління інцидентами ІБ;
- забезпечення безперервності бізнес-діяльності Банку;
- безпечне управління життєвим циклом ІС.

3.4. Банк дотримується наступних правил в частині забезпечення ІБ та безперебійної діяльності:

- публічні сервіси Банку та внутрішні мережі Банку відповідають вимогам стандартів з інформаційної безпеки;
- для зменшення ризиків виникнення інцидентів інформаційної безпеки керівництво Банку створює працівникам Банку умови для систематичного навчання нормам та заходам ІБ;
- у Банку складаються, діють, систематично тестуються та оновлюються плани безперебійного функціонування діяльності Банку на випадок непередбачуваних (критичних) ситуацій.
- Працівники Банку (третіх сторін) беруть участь у підтримці відповідного рівня ІБ в межах своїх обов’язків та повноважень і несуть відповідальність за його порушення в межах, встановлених чинним законодавством України та внутрішніми нормативними документами Банку.

3.5. Банком використовуються наступні вимоги щодо забезпечення інформаційної безпеки:

- створено та затверджено перелік відомостей, що містять інформацію (в тому числі, з обмеженим доступом);
- визначено перелік критичних процесів;
- встановлено правила доступу до інформаційних ресурсів та програмно-технічних комплексів;
- забезпечується контроль фізичного та логічного доступу до всіх наявних ресурсів;
- забезпечується парольний захист програмних та сервісних ресурсів;
- забезпечується антивірусний захист програмних та сервісних ресурсів;
- забезпечується захист мережі;
- забезпечується захист віддаленого доступу до ресурсів мережі (локальної, мережі Інтернет, мереж інших організацій);
- забезпечується ідентифікація та автентифікація всіх визначених ресурсів;
- забезпечується криптографічний захист інформації.

Розділ IV. Ролі та обов'язки

4.1. Ефективна ІБ Банку забезпечується шляхом безперервної участі працівників всіх підрозділів на всіх рівнях діяльності. Кожен підрозділ несе відповідальність за виконання нормативних документів Банку з ІБ як частини своїх службових завдань. Представники третіх сторін несуть відповідальність за виконання покладених на них функцій.

4.2. Керівництво активно підтримує безпеку в межах Банку шляхом чіткого регулювання, підтверджених зобов’язань, чітких призначень та визнання відповідальності за ІБ.

4.3 У Банку створений та постійно працює Керівний орган з питань інформаційної безпеки, рішення якого є обов’язковими для виконання усіма працівниками Банку. Головою Керівного органу наказом призначено Члена Правління, який відповідає за питання інформаційної безпеки Банку. До складу Керівного органу включено спеціаліста з питань інформаційної безпеки.

4.4. Увесь найманий персонал Банку, підрядники та користувачі третьої сторони (за необхідності) проходять належне навчання для поінформованості та регулярно отримують оновлені дані щодо політик і процедур Банку, суттєвих для їх посадових функцій (виконання покладених на них зобов’язань відповідно до укладених договорів).

4.5. Найманий персонал, підрядники та користувачі третьої сторони погоджують і підписують документи щодо термінів та умов з найму, які встановлюють взаємні відповідальності щодо інформаційної безпеки.

4.6. Банк описує та захищає наступні види ресурсів:

- **інформаційні ресурси** - інформація та дані у будь-якому вигляді, що отримуються, зберігаються, обробляються, передаються, оголошуються, у тому числі знання працівників, партнерів Банку, бази даних та вміст файлових ресурсів, документація, навчальні матеріали, описи процедур, архіви тощо;
- **програмне забезпечення** - прикладне програмне забезпечення та системне програмне забезпечення, незалежно від форми отримання (придбання, власної розробки, таке, що вільно розповсюджується), яке використовується у Банку працівниками та системами для роботи та взаємодії з клієнтами та іншими системами тощо;
- **фізичні ресурси** - працівники, апаратні засоби інфраструктури (сервери, робочі станції, міжмережеві екрани, багатофункціональні пристрої, телекомунікаційне обладнання, мережеве обладнання тощо), носії даних (диски, накопичувачі тощо), меблі, приміщення, виробниче обладнання, інші технічні засоби тощо;
- **сервісні ресурси** - обчислювальні та комунікаційні сервіси (Інтернет, електронна пошта, канали зв'язку тощо), інші технічні сервіси (опалення, освітлення, енергозабезпечення, кондиціювання повітря, системи сигналізації та моніторингу), усі послуги, пов'язані з отриманням, наданням, використанням, передачею та знищенням ресурсів, усі юридичні та фізичні особи, організації, установи та підприємства (а також їх працівники), послугами яких користується Банк для отримання, використання, передачі та знищення ресурсів.

4.7. Для кожного ресурсу Банк визначає можливі ризики інформаційної безпеки та шляхи їх мінімізації, тобто Банк використовує ризик-орієнтований підхід, що забезпечує розуміння, моніторинг та зменшення ризиків операційної діяльності.

4.8. Увесь найманий персонал, підрядники та користувачі третьої сторони повертають всі отримані від Банку ресурси, що перебувають у їх розпорядженні, після припинення їх найму, контракту чи угоди.

Розділ V. Прикінцеві положення

5.1. Зміст Політики розміщується на корпоративному сайті Банку після її затвердження належним чином.

5.2. Перегляд Політики здійснюється за потреби, але не менш ніж раз на рік, під час перегляду СУІБ керівництвом Банку.

5.3. Ця Політика набирає чинності з дати затвердження рішенням Спостережною радою.

5.4. Дана редакція Політики втрачає свою чинність з дати набрання чинності наступної / нової редакції або на підставі рішення Спостережної Ради.

5.5. У разі невідповідності будь-якої частини Політики чинному законодавству України або нормативно-правовим актам Національного банку України, у тому числі у зв’язку з прийняттям нових актів законодавства України або нормативно-правових актів Національного банку України, ця Політика діє лише в тій частині, яка не суперечить нормативно-правовим актам Національного банку України та чинному законодавству України.