ЗАТВЕРДЖЕНО
Рішенням Наглядової ради
АТ “БАНК “УКРАЇНСЬКИЙ КАПІТАЛ”
Протокол від 02.10.2025 року, № 72

ПОГОДЖЕНО
Рішенням Правління
АТ “БАНК “УКРАЇНСЬКИЙ КАПІТАЛ”
Протокол від 29.09.2025 року, № 89

ПОЛІТИКА
ІНФОРМАЦІЙНОЇ БЕЗПЕКИ
АКЦІОНЕРНОГО ТОВАРИСТВА
«БАНК «УКРАЇНСЬКИЙ КАПІТАЛ»

Зареєстровано в реєстрі
внутрішніх нормативних документів
АТ “БАНК “УКРАЇНСЬКИЙ КАПІТАЛ”
№ 1995

м. Київ - 2025

ЗМІСТ

ГЛОСАРІЙ **3**

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ **7**

2. МЕТА ТА ЦІЛІ ДОКУМЕНТА **8**

3. СФЕРА ЗАСТОСУВАННЯ **8**

4. ПРИНЦИПИ ТА РЕСУРСИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ **8**

5. ПІДХОДИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ **9**

6. РОЛІ, ВІДПОВІДАЛЬНІСТЬ ТА ВНУТРІШНІЙ КОНТРОЛЬ **11**

7. СИСТЕМА ВНУТРІШНЬОГО КОНТРОЛЮ ТА ВІДПОВІДАЛЬНІСТЬ **13**

8. ПРИКІНЦЕВІ ПОЛОЖЕННЯ **18**

ГЛОСАРІЙ

У цій Політиці терміни та скорочення вживаються в такому значенні:

Банк	АКЦІОНЕРНЕ ТОВАРИСТВО “БАНК “УКРАЇНСЬКИЙ КАПІТАЛ”
Безпека ІТС	стан конфіденційності, доступності, цілісності ресурсів.
Відповідальний за ресурси ІТС	працівник Банку, що діє за дорученням Власника ІТС та за посадою відповідає за ввірені йому ресурси ІТС або їх частину
Відповідальний за ресурси ІТС	працівник Банку, що діє за дорученням Власника ІТС та за посадою відповідає за ввірені йому ресурси ІТС або їх частину
Власник інформаційного ресурсу	підрозділ/його керівник, відповідальний за своїм функціоналом за створення, редагування, видалення інформаційних ресурсів
Власник ІТС	Банк, як юридична особа
Власник процесу / бізнес- процесу	підрозділ/його керівник, який має персонал, інфраструктуру, програмне забезпечення, інформацію про процес, здійснює його управляння, несе відповідальність за результати і ефективність процесу, наділений повноваженнями вимагати від працівників/підрозділів Банку здійснення всіх дій, необхідних для ефективного виконання бізнес-процесу
Власник технологічного ресурсу	Управління інформаційних технологій, яке відповідає за технологічні ресурси ІТС
Інформаційна безпека (ІБ)	захист інформації від загроз з метою забезпечення безперервності бізнесу, мінімізації ризику зупинки бізнес-процесів і отримання максимальної рентабельності інвестицій і бізнес-можливостей. ІБ спрямована на забезпечення конфіденційності, цілісності та доступності інформації
Інформаційна система	організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів
Інформаційні технології (ІТ)	технології пошуку, збору, передачі, збереження, накопичення, тиражування, захисту інформації та забезпечення функціонування ІТС
Інформаційний ресурс	інформація та дані в інформаційних системах, що отримуються, зберігаються, оброблюються, оприлюднюються, передаються, у тому числі інформація про Персонал і Постачальників, бази даних та файли, нормативна документація, електронні архіви тощо
Інформаційний ризик	ризик ІСТ та ризик інформаційної безпеки
Інформація з обмеженим доступом	це інформація, яка містить банківську таємницю, конфіденційну інформацію та персональні дані, а також інша інформація, режим використання якої визначений законами України, нормативно-правовими актами НБУ, нормативними документами Банка, угодами з клієнтами та контрагентами

Інформаційна інфраструктура Банку	комплекс програмно-технічних засобів, організаційних систем та нормативних актів, який забезпечує доступність, використання і взаємодію інформаційних потоків, функціонування та розвиток засобів інформаційної технологій для створення єдиного інформаційного простору Банку
Інформаційно-телекомунікаційна система (далі - ІТС)	програмно-апаратні засоби об'єднані в мережу, системи вводу, зберігання, обробки інформації для автоматизації бізнес- процесів та взаємодії із зовнішніми інформаційними системами
Інцидент інформаційної безпеки	- одна або серія небажаних або непередбачуваних подій інформаційної безпеки, що мають значну ймовірність компрометації функціонування бізнес-процесу та загрози інформаційній безпеці; - випадок, коли через Вразливості ІТС, реалізувалася Загроза ІТС, яка вплинула або може вплинути на ІТС або плинність бізнес-процесів
Загроза ІТС	- спосіб чи засіб використання вразливостей ІТС для завдання шкоди: руйнування, розкриття, зміни або відмови в обслуговуванні
Вразливість ІТС	- незахищене місце в ІТС, що може призвести до порушення безпеки, становить Загрозу і може спричинити її реалізацію
Доступність	властивість доступності та можливості використання ресурсів СУІБ на запит авторизованого користувача та/або процесу
Цілісність	властивість інформації, яка полягає в тому, що інформація не може бути модифікована неавторизованим користувачем і/або процесом
Конфіденційність	властивість інформації, яка полягає в доступності та розкриттю тільки авторизованому користувачу та/або процесу.
Спостережність	властивість системи, що дозволяє фіксувати діяльність користувачів і процесів, однозначно встановлювати ідентифікатори причетних до певних подій користувачів і процесів з метою запобігання порушення політики безпеки і/або забезпечення відповідальності за певні дії
Користувач ІТС	працівник Банку, який відповідно до наданих йому прав доступу, користується інформаційними ресурсами
Критичний процес / бізнес- процес	- процес/бізнес-процес діяльності Банку, визначений критичними щодо інформаційної безпеки за результатом їх оцінювання Банком за такими критеріями: конфіденційність, цілісність, доступність; процес/бізнес-процес Банку , неналежне виконання або зупинка якого становить фактичну/потенційну небезпеку для задоволення вимог регулятора та для забезпечення заявленої Банком якості банківських продуктів/послуг
Моніторинг інформаційної безпеки	постійне спостереження за подіями інформаційної безпеки, збір, аналіз і узагальнення результатів спостереження
Персонал	працівник/и, які є суб'єктами кадрових відносин, використовують інформаційні ресурси, комп'ютерне, телекомунікаційне та офісне обладнання Банку

Подія інформаційної безпеки	це ідентифікований стан інформаційного об‘єкту, системи, служби, мережі, який вказує на можливе порушення політики інформаційної безпеки чи відмови засобів захисту або раніше невідому ситуацію, яка може мати відношення до безпеки
Пом’якшення ризиків	комплекс заходів спрямованих на зменшення ймовірності виникнення ризику та/або зменшення впливу ризику на результати діяльності банку.
Постачальник (Третя сторона)	особа (фізична або юридична), яка перебуває у фінансових або будь-яких договірних відносинах з Банком і є стороною таких відносин
Процес / Бізнес-процес	структурована послідовність дій з виконання певного виду діяльності, яка реалізує визначену задачу діяльності/бізнесу
Ресурси ІТС	обладнання, програмне забезпечення, бази даних, телекомунікаційна мережа, персонал що її обслуговує
Ризик інформаційно-комунікаційних технологій (далі – ризик ІСТ)	ризик інформаційно-комунікаційних технологій (складова операційного ризику) – імовірність виникнення збитків або додаткових втрат або недоотримання запланованих доходів унаслідок несправності або невідповідності інформаційно-комунікаційних технологій бізнес-потребам банку, що може призвести до порушення їх сталого функціонування, або недоліків в організації управління такими технологіями
Ризик інформаційної безпеки	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)	система управління інформаційною безпекою - перелік цілей, принципів керування, методів, заходів з захисту інформації та забезпечення стійкості процесів/бізнес-процесів в інформаційній інфраструктурі Банку частина системи управління Банку. Ґрунтується на врахуванні інформаційних ризиків, як складової операційних ризиків. Призначена для розроблення, впровадження, та підтримки функціонування процесів забезпечення належного рівня інформаційної безпеки в Банку, за напрямками їх моніторингу, перегляду, підтримки та вдосконалення
Технологічні ресурси	складова частина ІТС, яка містить в собі системні та призначені для користувача файли, комп'ютери, комп'ютерні мережі, апаратуру та інше обладнання, яке забезпечує діяльність ІТС
Управління інформаційної безпеки	підрозділ, який організаційно забезпечує належний рівень інформаційної безпеки та управління інформаційною безпекою

Управління інформаційною безпекою	(як процес) - комплекс системних дій, що містить: організаційні процедури, положення, регламенти, інструкції, вказівки, розпорядження та рішення керівних органів, створені для забезпечення досягнення цілей Банку, своєчасного усунення небажаних факторів і дій, недопущення їх повтору, забезпечення безперервності бізнесу і усунення наслідків реалізації загроз.
Стейкхолдер	Будь-яка особа або група осіб, що є об'єктом або суб'єктом діяльності Банку через його послуги, політику або процеси. // Будь-яка особа або група осіб, що впливає на діяльність Банку/ або відчуває на собі вплив цієї діяльності; основними стейкхолдерами Банку є: інвестори, що вкладають у Банк свій капітал з визначеною часткою ризику з метою одержання доходу на нього; кредитори, які тимчасово владують кошти в Банк в обмін на деякий заздалегідь встановлений дохід і які зацікавлені в інформації, що дозволяє їм визначити, чи будуть вчасно здійснені виплати по депозитах, ТОП менеджери Банку , оскільки фінансова інформація дозволяє здійснити найбільш достовірне оцінювання ефективності керування Банком ; працівники Банку , зацікавлені в одержанні інформації про здатність Банку вчасно виплачувати зарплату, здійснювати пенсійні та інші виплати; постачальники, зацікавлені в інформації, що дозволяє їм визначити, чи будуть вчасно виплачені належні ним суми; споживачі (клієнти Банку), зацікавлені в стабільності отримання кредитів/гарантій; суспільні і державні організації, оскільки від успішного функціонування Банку залежить добробут економічної інфраструктури регіону, НБУ, ФГВФО тощо
Інші терміни та поняття	які вживаються в цій Політиці, застосовуються в значеннях, визначених Законом України «Про банки і банківську діяльність», іншими Законами України, нормативно-правовими актами Національного банку України та внутрішніми нормативними документами Банку

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1. Політика інформаційної безпеки АКЦІОНЕРНОГО ТОВАРИСТВА “БАНК “УКРАЇНСЬКИЙ КАПІТАЛ” (далі — Політика) є загальнодоступним внутрішнім нормативним документом, який визначає основні методи, заходи та принципи побудови системи управління інформаційною безпекою АКЦІОНЕРНОГО ТОВАРИСТВА “БАНК “УКРАЇНСЬКИЙ КАПІТАЛ” (далі - Банк), що дозволяють гарантувати захист інформаційних ресурсів для забезпечення ефективності та безперервності бізнес діяльності.

1.2. Політика розроблена з урахуванням вимог законодавства та нормативних документів:

– Закон України «Про банки і банківську діяльність» зі змінами;

– Закон України «Про захист інформації в інформаційно-комунікаційних системах» зі змінами;

– Положення «Про організацію заходів із забезпечення інформаційної безпеки в банківській системі України» затвердженої Постановою Національного банку України №95 від 28.09.2017 року;

– Положення «Про забезпечення безперервного функціонування інформаційних систем Національного банку України та банків України» затвердженої Постановою Національного банку України №265 від 17.06.2004 року зі змінами;

– Положення про захист інформації та кіберзахист учасниками платіжного ринку, затверджене постановою Правління Національного банку України від 19.05.2021 № 43 зі змінами;

– Положення про організацію кіберзахисту в банківській системі України, затверджене постановою Правління Національного банку України від 12.08.2022 № 178, зі змінами;

– Положення про організацію системи управління ризиками в банках України та банківських групах, затвердженого постановою Правління Національного банку України від 11.06.2018 № 64 зі змінами;

– Положення про організацію системи внутрішнього контролю в банках України та банківських групах від 02 липня 2019 року №88;

– Інших нормативно-правових актів Національного банку України.

1.3. Політика є основою для розробки нормативних документів Банку в галузі інформаційної безпеки. Будь-які внутрішні документи не можуть суперечити вимогам цієї Політики.

1.4. Метою Політики є забезпечення ефективного функціонування системи управління інформаційною безпекою (далі – СУІБ) в Банку, яка забезпечує безпечність, надійність та безперервність функціонування бізнес-процесів, захист інформаційних ресурсів Банку від зовнішніх та внутрішніх загроз, мінімізацію ризиків операційної діяльності та спрямована на створення позитивної репутації Банку при роботі з Постачальниками.

1.5. Політика Банку будується виключно на підставі його виробничих інтересів у відповідності до вимог законодавства України, політики безпеки Банку, вимог договорів, зобов’язань, що мають виконуватись Банком.

1.6. Політика доводиться до всього Персоналу Банку через розміщення на внутрішньому веб-порталі Банку та під підпис при прийому на роботу.

1.7. Політика доводиться до Постачальників публікацією на сайті Банку (https://ukrcapital.com.ua/). Зобов'язання щодо ознайомлення з Політикою, та дій у межах її вимог, зазначаються у договірних документах з Постачальниками та внутрішніх нормативних документах Банку.

2. МЕТА ТА ЦІЛІ ДОКУМЕНТА

2.1. Метою цієї Політики є ефективне впровадження і функціонування системи управління інформаційною безпекою (далі – СУІБ) в Банку, яка забезпечує безпечність, надійність, та безперервність функціонування бізнес – процесів, захист інформаційних ресурсів Банку від зовнішніх та внутрішніх загроз, сприяння мінімізації інформаційних ризиків Банку та створення позитивної репутації Банку при роботі з Постачальниками.

2.2. Основними цілями Політики є підвищення довіри до Банку з боку клієнтів, партнерів та стейкхолдерів, забезпечення стабільного функціонування Банку, виконання необхідних і оперативних дій при виникненні реальних загроз безпеці інформації, запобігання та/або мінімізація збитку при виникненні інцидентів інформаційної безпеки.

2.3. Основними завданням інформаційної безпеки є захист інформаційних ресурсів Банку від зовнішніх і внутрішніх загроз, встановлення оптимальних вимог щодо забезпечення інформаційної безпеки та підвищення ефективності заходів щодо забезпечення й підтримки інформаційної безпеки Банку.

3. СФЕРА ЗАСТОСУВАННЯ

Мінімальною сферою застосування Політики є усі визначені Банком критичні процеси / бізнес-процеси, інформаційні ресурси та програмно-технологічні комплекси, які забезпечують їх функціонування, персонал Банку, задіяний у їх виконанні, та Постачальники, які мають/або можуть мати доступ до інформаційних ресурсів Банку.

Банк має право розширити сферу застосування Політики Банку відповідно до особливостей діяльності, характеру та обсягу банківських, фінансових послуг та інших видів діяльності.

4. ПРИНЦИПИ ТА РЕСУРСИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

4.1. Основними принципами функціонування системи управління інформаційної безпеки Банку, яких дотримується Банк, є підтримання належного рівня захисту інформації із забезпеченням:

- *Цілісності* - властивість інформації, яка полягає в тому, що інформація не може бути модифікована неавторизованим користувачем і/або процесом;
- *Конфіденційності* – властивість інформації, яка полягає в доступності та розкриттю тільки авторизованому користувачу та/або процесу.
- *Доступності* – властивість доступності та можливості використання ресурсів СУІБ на запит авторизованого користувача та/або процесу.
- *Спостережності* - властивість системи, що дозволяє фіксувати діяльність користувачів і процесів, однозначно встановлювати ідентифікатори причетних до певних подій користувачів і процесів з метою запобігання порушення політики безпеки і/або забезпечення відповідальності за певні дії

Основними об'єктами на які розповсюджується дія інформаційної безпеки Банку є такі ресурси:

- *Інформаційні ресурси* – Інформація та дані, що отримуються, зберігаються, оброблюються, оприлюднюються, передаються, у тому числі інформація про Персонал і Постачальників, бази даних та файли, нормативна документація, електронні архіви тощо;
- *Програмні ресурси* – прикладне/системне/сервісне програмне забезпечення та будь-яке інше, незалежно від форми отримання (придбання, власної розробки, безкоштовне), яке використовується в Банку Персоналом та ІТС для роботи і взаємодії з Клієнтами або іншими зовнішніми інформаційними системами;
- *Фізичні ресурси* – приміщення Головного офісу Банку та територіально віддалених підрозділів, виробниче обладнання та всі технічні засоби роботи з інформацією: сервери, робочі станції, мережеві екрани, принтери, копіювальні апарати, телекомунікаційне обладнання, маршрутизатори, носії даних (як паперові так і електронні, магнітні) та інше;
- *Сервісні ресурси* – обчислювальні та комунікаційні сервіси, конфігурації обладнання, доступ до Інтернет, електронної пошти та зв'язку, інші технічні сервіси: опалення, освітлення, енергозбереження, кондиціювання повітря, системи сигналізації та моніторингу, усі послуги, пов'язані з отриманням, наданням, використанням, передачею та знищенням активів/інформації, усі юридичні та фізичні особи, організації, установи та підприємства (їх працівники), послугами яких користується Банк для отримання, обробки, використання, передачі та знищення активів;
- *Людські ресурси* – Персонал Банку, Постачальники, фізичні та юридичні особи, які перебувають у фінансових або будь-яких договірних відносинах з Банком і є стороною таких відносин.

4.2. Банк використовує ризик–орієнтовний підхід, який забезпечує розуміння, моніторинг та зменшення ризиків операційної діяльності. Для цього визначаються можливі інформаційні ризики та шляхи їх мінімізації для кожного ресурсу.

5. ПІДХОДИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

5.1. Банком використовуються наступні підходи щодо забезпечення інформаційної безпеки:

- створення та затвердження переліку відомостей, що містять інформацію з обмеженим доступом;
- створення та затвердження переліку критичних бізнес–процесів Банку;
- встановлення правил доступу до інформаційних ресурсів та програмно–технічних комплексів;
- забезпечення контролю фізичного та логічного доступу до визначених ресурсів;
- забезпечення парольного захисту програмних та сервісних ресурсів;
- забезпечення антивірусного захисту програмних та сервісних ресурсів;
- забезпечення захисту мережі;
- забезпечення віддаленого доступу до ресурсів мережі (локальної, мережі Інтернет, мереж інших організацій);

- забезпечення надійної ідентифікації , автентифікації та авторизації для всіх визначених інформаційних ресурсів;
- забезпечення надійного криптографічного захисту інформації;
- забезпечення моніторингу, оцінювання та вдосконалення СУІБ;
- регулярне проведення моніторингу та перегляду СУІБ з боку керівництва Банку.

5.2. Всі працівники Банка ознайомлені з вимогами інформаційної безпеки та зобов'язані дотримуватись їх в роботі.

5.3. Під час розроблення, впровадження, та функціонування програмно–технічних комплексів враховуються вимоги інформаційної безпеки.

5.4. Банк забезпечує виконання усіх вимог інформаційної безпеки, які наявні в угодах з Постачальниками, в т.ч. стосовно участі у міжнародних платіжних системах та системах переказу коштів.

5.5. У Банку розроблюються, діють, систематично тестуються та оновлюються плани забезпечення безперервної діяльності Банку (BCP - business continuity plan) на випадок надзвичайних ситуацій, складовою яких є план відновлення діяльності (Recovery Plan).

5.6. Інформаційна безпека забезпечується шляхом застосування комплексу заходів її контролю (системи захисту інформації – СЗІ), який реалізує вимоги цієї Політики Банку.

СЗІ має забезпечувати:

- неможливість відключення або ігнорування СЗІ;
- цілісність та безперервність захисту на всіх етапах життєвого циклу інформації;
- оптимальність та мінімальну достатність ступеня захисту;
- обмеження доступу до інформації та ресурсів обробки інформації в обсязі, необхідному для виконання обов'язків даного користувача (принцип «need-to-know»);
- розмежування доступу та повноважень до інформаційних активів Банку та процесів обробки інформації за принципом надання користувачам мінімально необхідних повноважень (принцип «least-privilege»);
- мінімізацію кількості шлюзів між внутрішніми середовищами обробки інформації та зовнішніми неконтрольованими середовищами, та їх повну контрольованість;
- побудову систем автоматизації Банку із застосуванням сучасних технологій та криптографічних алгоритмів захисту інформації, захищених операційних систем та систем керування базами даних;
- максимальний рівень захисту ключової інформації СЗІ;
- мінімізацію «людського фактора» в процесі застосування засобів захисту інформації.

5.7. Банком запроваджується механізм оповіщення та реагування щодо інцидентів інформаційної безпеки.

5.8. Персонал Банку є важливою і невід'ємною складовою СЗІ.

- Банк встановлює рівень вимог щодо професійного рівня та репутації персоналу, що виконує ключові ролі стосовно забезпечення ІБ.
- Банк вживає заходів щодо доведення вимог політики ІБ, підвищення свідомості та кваліфікації співробітників Банку у галузі ІБ.

6. РОЛІ, ВІДПОВІДАЛЬНІСТЬ ТА ВНУТРІШНІЙ КОНТРОЛЬ

6.1. В цілях виконання завдань по забезпеченню інформаційної безпеки Банку відповідно до рекомендацій міжнародних і українських стандартів по інформаційній безпеці в Банку визначені наступні ролі:

- Наглядова рада;
- Служба управління ризиками;
- Служба комплаєнсу;
- Служба внутрішнього аудиту;
- Правління;
- Керівний орган СУІБ;
- Управління інформаційної безпеки;
- Працівник Банку.

При необхідності можуть бути визначені додаткові ролі.

6.2. Банк забезпечує організацію системи управління інформаційної безпеки, управління інформаційним ризиком та впроваджує систему внутрішнього контролю щодо інформаційної безпеки дотримуючись моделі трьох ліній захисту.

До першої лінії захисту належать усі структурні підрозділи Банку, які під час здійснення своєї діяльності повинні забезпечувати дотримання вимог політики, процедур та використання інструментів управління інформаційним ризиком відповідальні працівники за управління інформаційним ризиком, призначаються зі складу підрозділів першої лінії захисту, функції яких полягають в управлінні інформаційною безпекою або інформаційними технологіями та внутрішнього контролю.

До другої та третьої ліній захисту належать підрозділ з управління ризиками, підрозділ комплаєнс та підрозділ внутрішнього аудиту відповідно, які забезпечують виконання функцій, визначених внутрішніми нормативними документами у відповідності до нормативно-правових актів Національного банку України щодо дотримання трьох ліній захисту під час управління операційним ризиком та побудови системи внутрішнього контролю.

6.3. Оперативна діяльність і планування діяльності по забезпеченню інформаційної безпеки Банку здійснюються і координуються Комітетом банківських інформаційних технологій (далі – КБІТ) та Управлінням інформаційної безпеки.

6.4. **Завданнями Управління інформаційної безпеки** у рамках забезпечення інформаційної безпеки є:

- розробка і перегляд внутрішніх нормативних документів по забезпеченню інформаційної безпеки Банку, включаючи плани, політики, положення, методики, переліки відомостей і інші види внутрішніх нормативних документів;
- навчання, контроль і безпосередня робота з персоналом Банку в області забезпечення інформаційної безпеки;
- планування, застосування, участь в постачанні і експлуатації засобів забезпечення інформаційної безпеки на ресурси ІТС та інформаційні системи Банку;
- виявлення і запобігання реалізації загроз інформаційної безпеки;
- виявлення і реагування на інциденти інформаційної безпеки;
- інформування в установленому порядку відповідальних осіб про погрози і ризикові події інформаційної безпеки;

- прогнозування і попередження інцидентів інформаційної безпеки;
- припинення несанкціонованих дій порушників інформаційної безпеки;
- підтримка бази інцидентів інформаційної безпеки, аналіз, розробка оптимальних процедур реагування на інциденти і навчання персоналу;
- моніторинг і оцінка інформаційної безпеки, включаючи оцінку повноти і достатності захисних заходів і видів діяльності по забезпеченню інформаційної безпеки Банку;
- контроль забезпечення інформаційної безпеки Банку, у тому числі на базі інформації про інциденти інформаційної безпеки, результати моніторингу оцінки і аудиту інформаційної безпеки;

6.5. У Банку створений та постійно працює Комітет банківських інформаційних технологій (далі – КБІТ) – колегіальний орган, підпорядкований Правлінню Банку, на який покладено функції в галузі впровадження, розвитку, підтримки функціонування СУІБ. Рішення КБІТ є обов'язковими для виконання усіма працівниками Банку.

Основними функціями КБІТ є:

- координація і впровадження інформаційної безпеки у Банку;
- узгодження впровадження нових проектів, напрямів, стратегічних завдань з питань інформаційної безпеки банку та заходів інформаційної безпеки;
- розгляд, затвердження та контроль за виконанням проектів щодо розроблення, упровадження, функціонування, моніторингу, перегляду, підтримання та вдосконалення СУІБ банку;
- визначення необхідних оптимальних ресурсів для впровадження заходів інформаційної безпеки;
- організація практичних заходів щодо підвищення обізнаності/ навчання персоналу банку з питань інформаційної безпеки;
- забезпечення своєчасного моніторингу стану впровадження та ефективності функціонування СУІБ банку з подальшою оцінкою можливостей вдосконалення та потреби проведення коригувальних дій.
- отримання та погодження звітів щодо оцінки ризиків та звіти про інциденти інформаційної безпеки;
- здійснює аналіз інцидентів інформаційної безпеки;
- запроваджує та контролює плани заходів по зниженню рівня ризиків;
- визначає запобіжні та корегуючи дії;
- розробляє та постійно вдосконалює систему управління інформаційною безпекою Банку.

6.6. **Основними завданнями працівників Банку** при виконанні покладених на них обов'язків і у рамках їх участі в оперативній діяльності по забезпеченню інформаційної безпеки Банку є:

- дотримання вимог інформаційної безпеки, що встановлюються нормативними документами Банку;
- виявлення і запобігання реалізації загроз інформаційної безпеки в межах своєї компетенції;
- виявлення і реагування на інциденти інформаційної безпеки;

- інформування в установленому порядку відповідальних осіб про виявлені загрози і ризикові події інформаційної безпеки;
- прогнозування і попередження інцидентів інформаційної безпеки в межах своєї компетенції;
- моніторинг і оцінка інформаційної безпеки у рамках своєї ділянки роботи і в межах своєї компетенції;
- інформування свого керівництва і Управління інформаційної безпеки про виявлені загрози в інформаційному середовищі Банку.

Кожен працівник Банку бере участь у підтримці відповідного рівня інформаційної безпеки Банку в межах своїх обов'язків та повноважень. Несе відповідальність за її порушення в межах, встановлених чинним законодавством України та внутрішніми нормативними документами.

6.7. **Служба управління ризиками** бере участь у розробці політики, методик, положень, регламентів і процедур Банку щодо управління інформаційним ризиком в частини операційного ризику Банку

6.8. **Служба комплаєнсу** забезпечує організацію контролю за дотриманням Банком норм законодавства, внутрішньобанківських документів та відповідних стандартів професійних об'єднань, дія яких поширюється на Банк, забезпечує організацію контролю за захистом персональних даних відповідно до законодавства України.

6.9. **Служба внутрішнього аудиту** забезпечує аудит щодо впровадження та функціонування системи управління інформаційної безпеки відповідно до норм законодавства, внутрішньобанківських документів та відповідних стандартів професійних об'єднань, дія яких поширюється на Банк, а також контроль за впровадженням рекомендацій наданих СВА під час планових та позапланових перевірок.

6.10. **Керівництво Банку** сприяє (організаційно та фінансово) впровадженню, контролю та підтримці вимог прийнятої Політики.

6.11. **Правління Банку** визначає стратегію і програму забезпечення інформаційної безпеки Банку, затверджує положення і процедури інформаційної безпеки, забезпечує провадження процедур ідентифікації, вимірювання, контролю, мінімізації та моніторингу ризиків.

6.12. **Наглядова рада Банку** затверджує Стратегію розвитку інформаційної безпеки, Політику інформаційної безпеки, Політику управління інформаційною безпекою та Політику управління ризиком інформаційно-комунікаційних технологій / ризиком інформаційної безпеки.

7. СИСТЕМА ВНУТРІШНЬОГО КОНТРОЛЮ ТА ВІДПОВІДАЛЬНІСТЬ

7.1. Банк розробляє та впроваджує заходи з контролю під час комунікації з зовнішніми користувачами. Такі заходи включають цю Політику та процедури отримання інформації від зовнішніх користувачів та передавання цієї інформації в межах організаційної структури Банку, що дає змогу керівникам банку визначати тенденції, події або обставини, які можуть вплинути на досягнення цілей Банку.

7.2. Власники бізнес-процесів/банківських продуктів, банківських операцій та інформаційних ресурсів Банку несуть відповідальність за організацію та супроводження, покладених на них бізнес задач та функціонування процесів обміну інформацією, згідно з основними принципами цієї Політики.

7.3. КБІТ та Управління інформаційної безпеки відповідають за повноту та актуальність внутрішніх нормативних документів, що регулюють виконання організаційних, технологічних та технічних вимог Політики.

7.4. Департамент інформаційних технологій та Управління інформаційної безпеки відповідають за реалізацію та впровадження технологічних та технічних заходів, які забезпечують виконання вимог Політики щодо організації каналів обміну, виконання регламентів, розподілу доступів і повноважень, захисту інформації в програмно-технічних комплексах Банку.

7.5. Департамент забезпечення діяльності Банку забезпечує процеси санкціонування, здійснює реєстрацію та поточний контроль за виконанням підрозділами та працівниками Банку вхідних та вихідних документів під час обміну із зовнішніми кореспондентами.

7.6. Всі працівники Банку несуть відповідальність за дотримання цієї Політики під час виконання операцій та дій, що пов’язані з реалізацією процесів обміну інформацією. Працівники Банку зобов'язані інформувати в системі моніторингу ризикових подій Банку про виявлені інциденти та порушення вимог Політики.

7.7. Служба внутрішнього аудиту Банку контролює виконання Політики шляхом включення до програм аудиту питань безпеки обміну інформацією та безпеки комунікацій.

7.8. Керівництво Банку здійснює контроль за реалізацією Політики шляхом періодичного затвердження звітів про реалізацію інформаційних ризиків, перегляду внутрішніх нормативних документів, що регулюють питання реалізації Політики, а також вимог Політики на їх відповідність зовнішнім вимогам: нормативно-правових актів Національного банку, законодавства України, правилам платіжних систем, договірним зобов’язанням Банку тощо.

8. ПРИКІНЦЕВІ ПОЛОЖЕННЯ

8.1. Ця Політика набуває чинності з моменту затвердження її Наглядовою радою.

8.2. Зміни та доповнення до Політики оформлюються додатком або шляхом підготовки нової редакції та затверджуються відповідно до встановленого у Банку порядку. Прийняття нової редакції Політики автоматично призводить до припинення дії попереднього документа.

8.3. У разі невідповідності будь-якої частини цієї Політики чинному законодавству України, нормативно-правовим актам Національного банку України, зокрема у зв'язку з прийняттям нових нормативно-правових актів, ця Політика буде діяти лише у тій частині, яка не суперечитиме чинному законодавству України.

8.4. Всі питання, не врегульовані цією Політикою, вирішуються у формах, що не суперечать здоровому глузду, в порядку, передбаченому іншими внутрішніми документами Банку та на підставі законодавства України.

8.5. Вимоги цієї Політики можуть розкриватися іншими внутрішніми нормативними документами Банку, які доповнюють і уточнюють її.

8.6. Відповідальність за актуалізацію цієї Політики покладається на начальника Управління інформаційної безпеки. Документ повинен переглядатися за необхідності, але не рідше ніж один раз на рік.

8.7. Пропозиції щодо змін та доповнень до цієї Політики підрозділи Банку направляють на адресу Управління інформаційної безпеки.

8.8. Ця Політика публікується у формі, яка не може бути легко змінена, але до якої має вільний доступ відповідний читач. Політика зберігається і надається таким чином, щоб бути доступною для працівників Банку та Постачальникам, які надалі будуть мати право користуватися нею.

8.9. Політика публікується в системі електронного документообігу, внутрішньому веб-порталі Банку та офіційному сайті Банку.

8.10. За консультаціями або роз'ясненнями щодо цієї Політики працівники Банку мають звертатися до працівників Управління інформаційної безпеки.