



**ЗАТВЕРДЖЕНО**  
Рішенням Наглядової Ради  
АТ «ТАСКОМБАНК»  
Протокол 24122020/8  
від «24» грудня 2020 р.  
Голова Наглядової Ради  
АТ «ТАСКОМБАНК»

\_\_\_\_\_ С.П. Попенко  
«\_\_» \_\_\_\_\_ 2020 р.

**ПОГОДЖЕНО**  
Рішенням Правління  
АТ «ТАСКОМБАНК»  
Протокол №50-6  
від «08» грудня 2020 р.  
Голова Правління  
АТ «ТАСКОМБАНК»

\_\_\_\_\_ В.В. Дубей  
«\_\_» \_\_\_\_\_ 2020 р.

**ПОЛІТИКА**  
**ІНФОРМАЦІЙНОЇ БЕЗПЕКИ**  
**АКЦІОНЕРНОГО ТОВАРИСТВА «ТАСКОМБАНК»**

## ПАСПОРТ

### внутрішнього документа нормативного характеру «Політика інформаційної безпеки АКЦІОНЕРНОГО ТОВАРИСТВА «ТАСКОМБАНК»»

#### I. Загальна інформація щодо внутрішнього документа нормативного характеру

Назва внутрішнього документа нормативного характеру	Політика інформаційної безпеки АКЦІОНЕРНОГО ТОВАРИСТВА «ТАСКОМБАНК»
Вид внутрішнього документа нормативного характеру	<b>Політика</b>
Орган, що затверджує внутрішній документа нормативного характеру	<b>Наглядова рада</b>
Основна мета розробки внутрішнього документа нормативного характеру	Визначення засад забезпечення інформаційної безпеки Банку та розподіл сфер відповідальності між підрозділами за дотримання вимог законодавства України та нормативних актів НБУ з інформаційної безпеки
Перелік актів законодавства України та нормативно-правових актів НБУ, на виконання яких розроблено внутрішній документ нормативного характеру	<p><b>Закони України:</b></p> <ul style="list-style-type: none"> <li>Закон України «Про банки і банківську діяльність»</li> </ul> <p><b>Нормативні акти Національного банку України:</b></p> <ul style="list-style-type: none"> <li>Положення про забезпечення безперервного функціонування інформаційних систем Національного банку та банків України, затверджене постановою Правління Національного банку України від 17.06.2004 № 265;</li> <li>Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України» затверджене постановою Правління Національного банку України від 28.09.2017 № 95;</li> <li>Положення про організацію системи управління ризиками в банках України та банківських групах, затвердженого Постановою Правління НБУ від 11.06.2018. №64.</li> <li>Положення про застосування електронного підпису в банківській системі України, затверджене постановою Правління Національного банку України від 14.08.2017 року №78;</li> <li>Положення про функціонування інформаційних систем Національного банку України та банків в особливий період, затвердженого Постановою Правління Національного банку від 21.04.2004 №175;</li> </ul> <p><b>Національних стандартів України з питань інформаційної безпеки:</b></p> <ul style="list-style-type: none"> <li>ДСТУ ISO/IEC 27000:2019 "Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Огляд і словник термінів".</li> <li>ДСТУ ISO/IEC 27001:2015 "Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги"</li> <li>ДСТУ ISO/IEC 27002:2015 "Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки".</li> </ul>
Документи, що втратили чинність у зв'язку із затвердженням внутрішнього документа нормативного характеру	Політика інформаційної безпеки АКЦІОНЕРНОГО ТОВАРИСТВА «ТАСКОМБАНК», погоджена рішенням Правління, протокол від 01.10.2019 №40-2, затверджена рішенням Наглядової ради, протокол №11102019 від 11.10.2019
Підрозділ розробник (власник) внутрішнього документа нормативного характеру	Департамент інформаційної безпеки
Контактні дані особи підрозділу Банку – розробника внутрішнього документа нормативного характеру	ПІБ: Палюх Валерій Миколайович Номер телефону: 2632

#### II. Регламентация процесів

Основні процеси I та II рівнів, які регламентуються внутрішнім документом нормативного характеру	I рівень – Банківська безпека II рівень – Забезпечення інформаційної безпеки
Категорії працівників, що мають бути ознайомлені з внутрішнім документом нормативного характеру	Усі посадові особи Банку
Перелік структурних підрозділів, на діяльність яких матиме вплив внутрішній документ нормативного характеру	Усі структурні підрозділи Банку

#### III. Внутрішній контроль

№ з/п	Зміст/короткий опис процедур контролю	Періодичність здійснення процедури контролю	I рівень контролю				II рівень контролю
			самостійний контроль	подвійний контроль	автоматизований контроль	колегіальний контроль	
1	Контроль відповідності реальних	Постійно	Власник процесу		Здійснюється програмно-технічними		Служба внутр. Аудиту в
2							

3	процесів вимогам Політики				засобами контролю процесів у інформаційно-телекомунікаційній мережі Банку		межах своїх планів внутрішніх перевірок
4		Щорічно		Директор Департаменту ІБ		Робоча група з питань ІБ в рамках оцінки ризиків	Служба внутр. аудиту

#### IV. Управління ризиками та комплаєнс-контроль.

Перелік ризиків, які притаманні процесам, регламентованим внутрішнім документом нормативного характеру	<p><b>Ризик персоналу.</b> Невиконання/несумлінне виконання посадових обов'язків, правил, регламентів, процедур тощо), внутрішнє шахрайство — управління ризиком будується шляхом впровадження принципу «чотирьох очей» та шляхом оперативного контролю дотримання вимог Політики, забезпечення здійснення повсякденної діяльності у відповідності з розробленими правилами.</p> <p><b>Ризик технологій.</b> Збої Програмного забезпечення та обладнання — управління ризиком здійснюється шляхом ретельного аналізу та планування змін. Для змін, впровадження яких пов'язане з високим ступенем ризику, обов'язково готується План комунікацій та ескалації. Під час виконання зміни Директором з інформаційних технологій забезпечується здійснення наскрізного контролю ходу виконання робіт і дотримання строків і якості виконаних робіт. Процес управління змінами обов'язково передбачає оцінку успішності зміни.</p> <p><b>Ризик процесу.</b> Основними заходами по управлінню ризиками процесу є: побудова технологічного процесу виконання заходів і робіт таким чином, щоб виключити/мінімізувати можливість виникнення факторів операційного ризику, регламентація процесів на всіх рівнях бізнес-процесу від планування до фактичного здійснення заходів і робіт тощо.</p> <p><b>Інформаційний ризик.</b> Імовірність виникнення збитків або додаткових втрат або недоотримання запланованих доходів унаслідок виникнення внутрішніх і зовнішніх подій щодо інформаційних систем Банку та інших інформаційних ресурсів, що використовуються для досягнення цілей Банку, недостатності внутрішнього контролю чи неадекватних або помилкових внутрішніх процесів Банку у сфері інформаційно-комунікаційних технологій. Інформаційний ризик є складовою операційного ризику.</p> <p><b>Комплаєнс-ризик.</b> Імовірність виникнення збитків/санкцій, додаткових втрат або недоотримання запланованих доходів або втрати репутації внаслідок невиконання Банком вимог законодавства, нормативно-правових актів, ринкових стандартів, правил добросовісної конкуренції, правил корпоративної етики, виникнення конфлікту інтересів, а також внутрішньобанківських документів Банку.</p> <p><b>Ризик середовища.</b> Правовий ризик (зовнішній). Зазначений перелік не є вичерпним та може доповнюватися за результатами проведення додаткової оцінки ризиків згідно встановленого в Банку порядку.</p> <p>Управління всіма видами операційних ризиків притаманних процесам, що регламентує це Політика, будується відповідно до Політик управління ризиками та процедур управління ризиками Банку.</p> <p>З метою ефективного управління та мінімізації ризиків, зазначених в цій Політиці, здійснюється комплекс заходів, спрямованих на зниження ймовірності настання подій та обставин, що призводять до збитків, та/або на зменшення розмірів потенційних збитків.</p> <p>Управління комплаєнс-ризиками здійснюється відповідно до Політики управління комплаєнс-ризиками Банку та Порядку здійснення процедур управління комплаєнс-ризиками Банку.</p> <p>Функція управління операційними та інформаційними ризиками покладається на керівників структурних підрозділів Банку, задіяних у виконанні своїх процесів.</p> <p>Загальний контроль за управлінням операційними та інформаційними ризиками покладається на Правління</p>
Відповідальні за актуалізацію внутрішнього документу нормативного характеру та імплементацію нових вимог	Департамент інформаційної безпеки; Департамент супроводження інформаційних систем АТ «ТАСКОМБАНК»
Відповідальні за контроль за дотриманням вимог внутрішнього документу нормативного характеру	Департамент інформаційної безпеки

## ЗМІСТ

<b>1. ЗАГАЛЬНІ ПОЛОЖЕННЯ .....</b>	<b>3</b>
2. ГЛОСАРІЙ .....	3
3. ЦІЛІ ТА ЗАВДАННЯ ПОЛІТИКИ .....	4
4. МЕЖІ ЗАСТОСУВАННЯ ПОЛІТИКИ.....	4
5. ЗАСАДИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ .....	5
6. ПРИНЦИПИ ОРГАНІЗАЦІЇ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ .....	7
7. ВІДПОВІДАЛЬНІСТЬ ЗА РЕАЛІЗАЦІЮ ПОЛІТИКИ.....	8
8. ЗАКЛЮЧНІ ПОЛОЖЕННЯ .....	9

## 1 ЗАГАЛЬНІ ПОЛОЖЕННЯ

- 1.1. Політика інформаційної безпеки АКЦІОНЕРНОГО ТОВАРИСТВА «ТАСКОМБАНК» (далі — Політика) визначає засади забезпечення інформаційної безпеки АКЦІОНЕРНОГО ТОВАРИСТВА «ТАСКОМБАНК» (далі — Банк).
- 1.2. Політика інформаційної безпеки публікується на внутрішньому та зовнішньому сайтах Банку та доступна для всіх.
- 1.3. Належний рівень інформаційної безпеки, це такий стан інформаційних ресурсів Банку, який гарантує конфіденційність, доступність, цілісність інформації Банку та спостережність/контрольованість системи в якій інформація циркулює.
- 1.4. Належний рівень захищеності банківської інформації досягається за допомогою застосування комплексу програмних/технічних засобів і організаційних заходів, спрямованих на забезпечення захищеності інформації від зловмисного використання, несанкціонованого оприлюднення, руйнування, несанкціонованих змін, знищення, недоступності.

## 2 ГЛОСАРІЙ

2.1. У цій Політиці вживаються терміни та поняття у наступному значенні:

**Актив (або ресурс)** – матеріальні або нематеріальні об'єкти або інформація, що мають цінність для Банку.

**Доступність інформації** — властивість, яка гарантує те, що забезпечується своєчасний доступ авторизованих осіб і/або процесів до інформації, відсутні простої в процесі її обробки, тобто коли вона 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.

**Інформаційна безпека (ІБ)** – процес, який забезпечує збереження визначених Політикою безпеки властивостей інформації та спрямований на запобігання несанкціонованим діям в інформаційній системі, що включає сукупність організаційно-технічних заходів і правових норм для запобігання заподіяння шкоди інтересам власника інформації чи інформаційної системи.

**Інформаційна система (ІС)** - організаційно-технічна система, у якій реалізується технологія обробки інформації з використанням технічних і програмних засобів.

**Конфіденційність інформації** — властивість, яка гарантує те, що доступ до інформації можуть одержати тільки авторизовані особи або процеси.

**НБУ** – Національний банк України.

**Персонал** – усі працівники Банку, які використовують інформаційні ресурси Банку, комп'ютерне, телекомунікаційне і офісне обладнання відповідно до своїх посадових обов'язків.

**Робоча група** – Робоча група з управління інформаційною безпекою, колективний керівний орган Системи управління інформаційною безпекою.

**Система управління інформаційною безпекою (СУІБ)** — комплекс організаційних, програмних, технічних і фізичних заходів, спрямованих на управління ризиками, що пов'язані з використанням у Банку інформації та інформаційних технологій.

**Спостережність системи** – властивість, що дозволяє фіксувати діяльність користувачів і процесів, а також однозначно установлювати ідентифікатори причетних до певних подій користувачів і процесів з метою запобігання порушення політики безпеки або забезпечення відповідальності за певні дії.

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

**Цілісність інформації** — властивість, яка гарантує те, що інформація не містить помилок, є актуальною, вичерпною, будь-які зміни інформації здійснюються авторизованими особами або процесами.

2.2. Інші терміни, що вживаються у цій Політиці, застосовуються в значеннях, визначених чинним законодавством України, нормативно-правовими актами Національного банку України та внутрішніми документами Банку.

### 3 ЦІЛІ ТА ЗАВДАННЯ ПОЛІТИКИ

3.1. Метою Політики є визначення засад забезпечення інформаційної безпеки Банку та розподіл сфер відповідальності між підрозділами за дотриманням вимог законодавства України та нормативних актів НБУ з інформаційної безпеки.

3.2. Політика спрямована на виконання наступних цілей:

- забезпечення захисту інформаційних активів Банку від зовнішніх загроз і загроз, пов'язаних з навмисними або ненавмисними діями працівників Банку;
- забезпечення ефективного функціонування СУІБ, яка є інструментом забезпечення інформаційної безпеки;
- забезпечення цілісності, доступності, конфіденційності та спостережності інформації;
- забезпечення безперервності роботи Банку;
- забезпечення відповідності Банку вимогам Законів України та нормативно-правовим актам НБУ;
- мінімізацію операційних ризиків, впровадження необхідних заходів для запобігання виникненню інцидентів у майбутньому;
- забезпечення рівня репутації Банку достатнього для конкурентних переваг на ринку.

3.3. Основними задачами Політики є встановлення:

- засад захисту інформації та ресурсів Банку від зовнішніх і внутрішніх загроз;
- засад забезпечення надійності бізнес-процесів/банківських продуктів/програмно-технічних комплексів та безперервної роботи Банку;
- впровадження ризик-орієнтованого підходу до забезпечення інформаційної безпеки банку;
- впровадження процесного підходу до забезпечення інформаційної безпеки Банку;
- засад мінімізації ризиків операційної діяльності Банку;
- засад створення позитивної репутації Банку при роботі з клієнтами.

### 4 МЕЖІ ЗАСТОСУВАННЯ ПОЛІТИКИ

4.1. Сферою застосування СУІБ є Банк в цілому.

4.2. Дія Політики поширюється на всі підрозділи Банку. Політика застосовується до усіх процесів, банківських продуктів, програмно-технічних комплексів, проектів, організаційних рішень. Політика є обов'язковою до виконання усіма працівниками Банку, а також Третіми сторонами, залученими до роботи з інформаційними ресурсами Банку, у межах укладених з Третіми особами угод/контрактів/договорів.

4.3. Об'єкти регулятивного впливу.

Об'єктами, на які розповсюджується дія і регулятивний вплив Політики, є:

**• Інформаційні ресурси:**

Інформація та дані у будь-якому вигляді, що отримуються, зберігаються, оброблюються, передаються, оголошуються, у тому числі інформація про Персонал і контрагентів, бази даних та файли, нормативна документація, електронні архіви тощо.

**• Програмне забезпечення:**

Прикладне/системне/сервісне програмне забезпечення та будь-яке інше, незалежно від форми отримання (придбання, власної розробки, безкоштовне), яке використовується у Банку працівниками та системами для роботи та взаємодії з клієнтами та іншими та зовнішніми системами.

**• Фізичні ресурси:**

Виробничі приміщення, усі технічні засоби роботи з інформацією, зокрема: сервери, робочі станції, міжмережеві екрани, принтери, копіювальні апарати, телекомунікаційне обладнання, маршрутизатори тощо.

**• Сервісні ресурси:**

Обчислювальні та комунікаційні сервіси, зокрема: доступ до мережі Інтернет, електронної пошти, телефонного зв'язку. Технічні сервіси забезпечення належних санітарних умов для персоналу, зокрема: опалення, освітлення, енергозбереження, кондиціювання повітря, системи сигналізації та моніторингу, усі послуги, пов'язані з отриманням, наданням, використанням, передачею та знищенням активів, усі юридичні та фізичні особи, організації, установи та підприємства (їх працівники), послугами яких користується Банк для отримання, використання, передачі та знищення активів.

**• Кадровий ресурс:**

Персонал Банку.

**• Треті сторони:**

Фізичні та юридичні особи, які перебувають у фінансових або будь-яких договірних відносинах з Банком і є сторонами таких відносин.

4.4. Інформаційними активами Банку, як одним з об'єктів захисту вважаються матеріальні та нематеріальні об'єкти, які є інформацією або містять інформацію, використовуються для обробки, зберігання або передачі інформації і мають цінність для Банку:

- інформація в електронному вигляді, яка циркулює в ІС на всіх етапах їх життєвого циклу (створення, обробка, зберігання, передача, знищення);
- інформація на паперових носіях;
- інформаційні системи, включаючи апаратні, апаратно-програмні та програмні засоби, системи і комплекси;
- приміщення Банку;
- персонал Банку.

4.5. Вся інформація, що представлена в електронному вигляді та обробляється за допомогою Інформаційної системи Банку повинна мати визначеного власника. За кожним інформаційним активом, розпорядчим документом Банку призначається власник - структурний підрозділ Банку в особі його начальника, який ініціював його створення або використовує його для виконання бізнес завдань. При цьому власник активу не має матеріальних/авторських або інших прав на актив.

4.6. Власник інформаційного активу приймає рішення щодо його зміни/модернізації, оцінює інформаційні ризики щодо активів, приймає рішення щодо їх мінімізації, прийняття або передачі, розглядає і організовує виконання вимог ІБ, погоджує доступ до інформаційного активу, приймає рішення про знищення інформаційного активу або виведення з експлуатації.

## 5 ЗАСАДИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

- 5.1. Управління інформаційною безпекою організовується у спосіб консолідації людських, методологічних, інтелектуальних та програмно-технічних ресурсів в єдину систему - Систему управління інформаційною безпекою.
- 5.2. Задачі Системи управління інформаційною безпекою:
  - Забезпечення захисту інформації та ресурсів Банку від зовнішніх і внутрішніх загроз.
  - Забезпечення надійності бізнес-процесів/ програмно-технічних комплексів та безперервної роботи.
  - Сприяння мінімізації операційних ризиків.
  - Створення позитивної репутації Банку при роботі з клієнтами та партнерами.
  - Необхідність забезпечення інформаційної безпеки обумовлена тим, що інформація є стратегічно важливим ресурсом Банку.
- 5.3. СУІБ встановлює вимоги щодо забезпечення інформаційної безпеки до ІТ-систем, процесів, які обробляються в ІТ-системі, і до процесів управління ІТ-системою.
- 5.4. Заходи щодо захисту інформації в Банку відповідають потребам бізнесу та вимогам законодавства України, нормативно-правових документів НБУ, внутрішніх нормативних документів Банку.
- 5.5. Організація будь-якого процесу, що має оброблятися в ІТ-системі, або внесення змін в існуючі процеси здійснюється з урахуванням потреб забезпечення інформаційної безпеки.
- 5.6. СУІБ слід постійно розвивати враховуючи зміни у процесах та ІТ-системах.
- 5.7. Процеси забезпечення інформаційної безпеки повинні бути описані, формально визначені та затверджені у стандартах, політиках, положеннях та інших внутрішніх документах.
- 5.8. Відповідальні працівники Банку складають, тестують та оновлюють плани забезпечення безперебійного функціонування та відновлення діяльності на випадок непередбачених надзвичайних ситуацій які можуть призвести до зупинки діяльності.
- 5.9. Заходи та засоби захисту інформаційних активів обираються за результатами аналізу ризиків для інформаційних активів. Витрати на ІБ повинні відповідати існуючим ризикам з урахуванням витрат на їх реалізацію і можливих втрат від реалізації загроз.
- 5.10. Працівники Банку виявляють, враховують і оперативно реагують на дійсні і ймовірні порушення ІБ. Всі інциденти ІБ фіксуються, аналізуються, надаються на розгляд Робочої групи, та враховуються при розробці заходів забезпечення захисту інформаційних активів.
- 5.11. Внутрішні документи нормативного характеру з ІБ доводяться до відома працівників Банку в частині, що їх стосується. У Банку на регулярній основі забезпечується інформування та навчання працівників Банку з питань забезпечення інформаційної безпеки.
- 5.12. Вимоги ІБ щодо забезпечення захисту інформаційних активів визначаються у внутрішніх документах нормативного характеру і внутрішніх розпорядчих документах Банку. При розробці вимог ІБ враховуються вимоги викладені в Законах України і нормативно-правових актах НБУ. Вимоги ІБ враховуються при реалізації всіх бізнес - процесів Банку та протягом життєвого циклу ІС Банку. Вимоги ІБ також враховуються у відносинах з контрагентами та Третіми сторонами.



- 5.13. Організація будь-якого процесу, що має оброблятися в інформаційній системі, або внесення змін в існуючі процеси здійснюється з урахуванням забезпечення інформаційної безпеки.
- 5.14. Оцінка ефективності функціонування СУІБ здійснюється на регулярній основі.
- 5.15. Для зменшення ризиків виникнення інцидентів інформаційної безпеки керівництво Банку створює умови для систематичного навчання працівників нормам та заходам інформаційної безпеки.
- 5.16. Процеси інформаційної безпеки описані, формально визначені та затверджені керівництвом Банку у вигляді стандартів, політик, положень та інших внутрішніх нормативних документів.
- 5.17. У Банку складаються, діють, тестуються та оновлюються плани забезпечення безперебійного функціонування на випадок непередбачених критичних ситуацій.
- 5.18. Відповідальні працівники Банку виявляють, враховують і оперативно реагують на дійсні і ймовірні порушення ІБ. Всі інциденти ІБ фіксуються, аналізуються та враховуються при розробці заходів забезпечення захисту інформаційних активів у внутрішніх нормативних документах.
- 5.19. Фінансування заходів щодо забезпечення ІБ передбачається в щорічному бюджеті Банку.
- 5.20. Ефективність реалізації Політики ІБ щорічно оцінюється підрозділом безпеки, робочою групою з питань інформаційної безпеки АТ «ТАСКОМБАНК» і керівництвом Банку.

## **6 ПРИНЦИПИ ОРГАНІЗАЦІЇ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ**

6.1. Система управління інформаційною безпекою організовується з дотриманням наступних принципів:

- **Належності ресурсів.**

Для кожного інформаційного ресурсу призначається Власник.

- **Персональної відповідальності.**

За реалізацію та виконання визначених заходів забезпечення інформаційної безпеки передбачена відповідальність. У договірних документах з Третіми особами зазначаються умови взаємних перевірок дотримання вимог інформаційної безпеки.

- **Колегіальної участі.**

У межах своїх повноважень і відповідальності всі працівників Банку беруть участь у захисті інформації в Інформаційній системі Банку. Функцію загального управління виконує CISO Банку (Відповідальна особа за інформаційну безпеку). Функцію колегіального управління виконує Робоча група.

- **Виправданості витрат.**

Об'єм ресурсів, залучених для захисту інформаційних активів, має відповідати наявним загрозам і не перевищувати обсяг збитків, що можуть виникнути внаслідок реалізації загроз.

- **Достатньої компетенції.**

Персонал та Треті сторони повинні мати рівень обізнаності, достатній для адекватного реагування на інциденти, ефективної протидії загрозам інформаційної безпеки та дотримання вимог інформаційної безпеки. В Банку організовується навчання з інформаційної безпеки та контроль рівня знань персоналу. Достатній рівень обізнаності з інформаційної безпеки представників Третіх сторін є обов'язковою умовою співпраці з Банком та зазначається у договірних умовах.

- **Системної діяльності.**

Діяльність із забезпечення належного рівня інформаційної безпеки провадиться у спосіб організації Системи управління інформаційною безпекою в основі якої організується колегіальний орган управління – Робоча група. Така діяльність є системною та проводиться в рамках моделі Демінга – «плануй-виконуй-перевір-впливай».

• **Розподілу прав доступу.**

Персонал може мати тільки такі права доступу до приміщень та інформаційних/технологічних ресурсів, які достатні для виконання посадових обов'язків згідно посадових інструкцій. Третя сторона може мати тільки такі права доступу до приміщень та інформаційних/технологічних ресурсів, які достатні для виконання нею договірних зобов'язань згідно діючих договірних умов визначених в договорах. До ресурсів, що не стосуються посадових обов'язків персоналу або виконання договірних умов Третьою стороною, права доступу не надаються, або надаються як виняток з обов'язковим визначенням посадових осіб, які приймають ризики, обумовлені застосованим винятком.

• **Забезпечення безперервності.**

У Банку організується управління безперервністю бізнесу, яке забезпечує безперебійне надання послуг споживачам та виконання зобов'язань Банку перед контрагентами і Національним банком у спосіб застосування комплексу організаційних заходів та програмно-технічних засобів. Такий комплекс забезпечує надійність роботи Банку, виявлення загроз, причин, передумов кризових/надзвичайних ситуацій, усунення негативних наслідків реалізації загроз та відновлення нормального режиму роботи Банку.

6.2. Основні правила та вимоги Інформаційної безпеки:

- Банк забезпечує постійний контроль ефективності впроваджених заходів інформаційної безпеки та механізмів забезпечення безпеки в інформаційних системах, визначає перелік критичних бізнес-процесів, інформаційних ресурсів, які забезпечують їх функціонування, та заходів, необхідних для їх належного захисту; забезпечує відповідний рівень захисту інформації, яка належить до "банківської таємниці", персональних даних клієнтів, "комерційної таємниці" та іншої конфіденційної інформації.
- Банк розробляє вимоги з інформаційної безпеки для третіх сторін, які надають Банку послуги з ІТ аутсорсингу, розробки, впровадження, аудиту інформаційних систем і ресурсів, а також отримують від Банку інформацію з обмеженим доступом, тощо.

## 7 ВІДПОВІДАЛЬНІСТЬ ЗА РЕАЛІЗАЦІЮ ПОЛІТИКИ

- 7.1. Цією Політикою визначається позиція керівництва Банку щодо забезпечення ІБ та забезпечення з його боку всієї необхідної підтримки при формуванні, прийнятті, впровадженні і супроводі даної Політики і СУІБ Банку. Керівники та Органи управління Банку виконують ті ж вимоги ІБ, що і всі працівників Банку.
- 7.2. Правління Банку відповідає за забезпечення необхідної підтримки для впровадження цієї Політики та функціонування СУІБ Банку.
- 7.3. Робоча група з управління інформаційною безпекою є постійним колективним керівним органом Правління Банку, колективним керівним органом СУІБ, частиною Системи управління ризиками Банку. Увесь склад Робочої групи відповідальний за повноту та своєчасність належного виконання покладених на кожного обов'язків.
- 7.4. Забезпечення ІБ здійснюється на постійній основі і є завданням усіх підрозділів Банку. Заходи забезпечення ІБ здійснюються на засадах розподілу сфер відповідальності між підрозділами Банку та узгоджені між собою за цілями, завданнями, принципами, методами і засобами. Організація виконання заходів щодо забезпечення ІБ здійснюється Департаментом інформаційної безпеки Банку.

- 7.5. Усі працівники Банку, незалежно від займаної посади, є персонально відповідальними за дотриманням вимог ІБ відповідно до чинного законодавства України, вимог НБУ та внутрішніх документів нормативного характеру. Керівники підрозділів Банку додатково є відповідальними за порушення вимог ІБ і неправомірні дії підлеглих їм працівників в межах обов'язків з контролю за підлеглими, згідно посадових інструкцій.
- 7.6. Кожен працівник Банку забезпечує підтримку відповідного рівня інформаційної безпеки Банку. В своїй роботі всі підрозділи та працівники дотримуються вимог Політики інформаційної безпеки.
- 7.7. Департамент інформаційної безпеки визначає та впроваджує вимоги з інформаційної безпеки Банку, забезпечує функціонування та використання засобів інформаційної безпеки, організовує належне навчання з питань інформаційної безпеки для працівників Банку, а також забезпечує контроль дотримання вимог Політики інформаційної безпеки.
- 7.8. Працівники усіх підрозділів Банку є відповідальними за виконання вимог Політики інформаційної безпеки, законодавчих, регуляторних і внутрішньобанківських норм інформаційної безпеки. Усі працівники під час прийому на роботу повинні бути ознайомлені з цією Політикою. Працівник банку зобов'язаний ознайомитися з політикою інформаційної безпеки банку під підпис та надати зобов'язання про дотримання конфіденційності.
- 7.9. Відповідальними за ознайомлення персоналу з вимогами ІБ, нормативними та розпорядчими документами з питань ІБ, навчання персоналу з питань ІБ, є, в рамках компетенції, Департамент інформаційної безпеки, Управління документаційного забезпечення, Учебний центр та Управління по роботі з персоналом.
- 7.10. За порушення вимог Політики, законодавчих, регуляторних і внутрішньобанківських норм інформаційної безпеки кожен працівник відповідатиме згідно із законодавством України і внутрішніми нормативними документами Банку.
- 7.11. Відповідальним за підтримання Політики в актуальному стані, своєчасне внесення змін та доповнень до неї, є Департамент інформаційної безпеки.
- 7.12. **Власник процесу.** Відповідальність за розробку вимог ІБ, управління інформаційним ризиком, організацію виконання заходів ІБ, а також перегляд і актуалізацію даної Політики покладено на Департамент інформаційної безпеки, який є власником процесу.

## 8 ЗАКЛЮЧНІ ПОЛОЖЕННЯ

- 8.1. Ця Політика затверджується рішенням Наглядової Ради Банку та набирає чинності з дати затвердження.
- 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 впровадженні в Банку нових інформаційних технологій, а також змін в законодавстві чи нормативно-правових актах НБУ.
- 8.4. Підрозділом, відповідальним за підтримання Політики в актуальному стані, за своєчасне внесення змін та доповнень до них є Департамент інформаційної безпеки.