ЗАТВЕРДЖЕНО
Наглядова рада Акціонерного товариства
«Комерційний Індустріальний Банк»
протокол № 05/07-1 від 05.07.2021 року

ПОГОДЖЕНО
Правління Акціонерного товариства «Комерційний Індустріальний Банк»
протокол № 05/07-1 від 05.07.2021 року

Політика інформаційної безпеки Акціонерного товариства «Комерційний Індустріальний Банк»

(Версія 4.0)

Київ – 2021

ОБЛІКОВА КАРТА ВНУТРІШНЬОГО НОРМАТИВНОГО ДОКУМЕНТА

Назва документа	Політика інформаційної безпеки Акціонерного товариства «Комерційний Індустріальний Банк» (версія 4.0)	
Реєстраційний номер та дата реєстрації	№05/07-1 від 05.07.2021	
Рішення про затвердження документа	Протокол Наглядової ради Банку №05/07-1 від 05.07.2021 року	
Дата набрання чинності	**05 липня 2021 року**	
Необхідність подання документа до регулюючих та контролюючих органів	ні	Найменування органів
Підрозділ - розробник документа	Управління інформаційної безпеки	
Рівень доступу	Публічний (для усіх юридичних та фізичних осіб, у т.ч. клієнтів, контрагентів Банку), розміщується на сайті Банку	
Назва та номер процесу		
Перелік документів, що втрачають чинність із вступом в дію даного ВНД	Політика інформаційної безпеки Акціонерного товариства «Комерційний Індустріальний Банк» (версія 3.0, затверджена протоколом Наглядової ради АТ «КІБ» від 27.12.2019)	
Історія документа	**Версія**	**Дата**
Політика інформаційної безпеки Акціонерного товариства «Комерційний Індустріальний Банк»	1.0	15.05.2015
Політика інформаційної безпеки Акціонерного товариства «Комерційний Індустріальний Банк»	2.0	05.04.2019
Політика інформаційної безпеки Акціонерного товариства «Комерційний Індустріальний Банк»	3.0	27.12.2019
Політика інформаційної безпеки Акціонерного товариства «Комерційний Індустріальний Банк»	4.0	05.07.2021

Політика інформаційної безпеки Акціонерного товариства «Комерційний Індустріальний Банк» (версія 4.0)

АРКУШ ПОГОДЖЕННЯ:

Посада	Прізвище, Ініціали	Підпис	Дата погодження
Директор Департаменту інформаційних технологій	Шостик А.О.		
Заступник директора Юридичного департаменту	Овчинніков М.В.		
Директор Департаменту ризик-менеджменту	Кухарук І.М.		
Начальник Служби комплаєнс-контролю	Дещенко Г.В.		
Начальник Управління загальнобанківської методології	Ірклієнко Г.М.		
Заступник директора Департаменту банківської безпеки	Шарий С.С.		
Директор Департаменту по роботі з персоналом	Чисникова Д.М.		
Директор Департаменту операційної діяльності	Попова М.В.		

Підрозділ – розробник	Посада - Ініціали, Прізвище	Підпис	Дата
Начальник Управління інформаційної безпеки	Крохін О.О.		

ЗМІСТ

1. Загальні положення

1.1. Політика інформаційної безпеки Акціонерного товариства «Комерційний Індустріальний Банк» (далі – Політика) визначає правові та організаційні засади, сферу застосування, напрями і цілі заходів, а також принципи діяльності у галузі інформаційної безпеки Акціонерного товариства «Комерційний Індустріальний Банк» (далі - Банк).

1.2. Мета впровадження Політики Банку – це визначення і використання в діяльності Банку нормативних вимог, організаційних і технічних заходів, що направлені на захист інформаційних ресурсів (або активів); запобігання і зниження збитків, що можуть наступити внаслідок реалізації подій та інцидентів інформаційної безпеки; забезпечення стабільного та безперервного функціонування засобів інформаційних технологій та безпеки; підвищення репутації Банку та довіри з боку клієнтів, акціонерів Банку і ділових партнерів.

1.3. Для планування та здійснення заходів інформаційної безпеки Банк застосовує ризик-орієнтований підхід, який полягає у прийнятті Керівництвом Банку управлінських рішень з питань інформаційної безпеки на підставі аналізу, оцінки і порівняння існуючих ризиків інформаційної безпеки. Банк запроваджує процес управління ризиками інформаційної безпеки в рамках загальної системи управління ризиками.

1.4. Банк, згідно з вимогами державних стандартів з інформаційної безпеки ДСТУ ISO/IEC 27001:2015, ДСТУ ISO/IEC 27002:2015, регламентує, впроваджує, підтримує та розвиває систему управління інформаційною безпекою (далі - СУІБ), яка є складовою загальної системи управління Банку, базується на процесному підході до організації і управління діяльністю і спрямована на постійне підвищення ефективності заходів інформаційної безпеки.

1.5. Політика публікується на внутрішніх ресурсах Банку та доступна для використання всіма співробітниками Банку. Положення Політики враховуються при розробці внутрішніх нормативних та розпорядчих документів Банку, а також при укладенні договорів.

1.6. Порушення вимог Політики тягне за собою дисциплінарну та іншу відповідальність згідно з Кодексом поведінки і внутрішнім дисциплінарним порядком Банку та чинним законодавством України.

1.7. Вимоги Політики поширюються на всі підрозділи Банку і є обов'язковими для всіх співробітників Банку. Дотримання вимог Політики є найважливішим аспектом для досягнення Банком його стратегічних цілей та завдань.

2. Нормативне забезпечення

№	Найменування документа:
1.	Закон України «Про інформацію» від 02.10.1992 № 2658-XII, в редакції від 16.06.2020.
2.	Закон України Про банки і банківську діяльність» від 07.12.2000 № 2121-III, в редакції від 17.06.2020.
3.	Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII, в редакції від 17.09.2020.
4.	Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.94 № 80/94-ВР, в редакції від 04.06.2020.
5.	Закон України «Про електронні документи та електронний документообіг» від 22.05.2003 № 851-IV, в редакції від 05.10.2017.
6.	Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI, в редакції від 30.03.2021.
7.	Закон України «Про електронні довірчі послуги» від 05.10.2017 № 2155-VIII, в редакції від 14.01.2020.
8.	Постанова Правління Національного банку України від 14.08.2017 № 78, Положення про застосування електронного підпису в банківській системі України, із змінами, внесеними згідно з Постановою № 42 від 25.02.2019

9.	Постанова Правління Національного банку України від 14.07.2006 № 267, Правила зберігання, захисту, використання та розкриття банківської таємниці, в редакції від 12.02.2021
10.	Постанова Правління Національного банку України від 17.06.2004 № 265, Положення про забезпечення безперервного функціонування інформаційних систем Національного банку та банків України, в редакції від 18.12.2015.
11.	Постанова Правління Національного банку України від 26.11.2015 № 829, Правила організації захисту електронних банківських документів, з використанням засобів захисту інформації Національного банку України, в редакції від 13.02.2019.
12.	Постанова Правління Національного банку України від 04.07.2007 № 243, Правила з технічного захисту інформації для приміщень банків, у яких обробляються електронні банківські документи, в редакції від 19.12.2007.
13.	Постанова Правління Національного банку України від 10.02.2016 № 63, Правила з організації захисту приміщень банків України, в редакції від 28.12.2019.
14.	Постанова Правління Національного банку України «Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України», від 28.09.2017 № 95
15.	Національні стандарти України з питань інформаційної безпеки: ДСТУ ISO/IEC 27001:2015 "Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги" (далі - ДСТУ ISO/IEC 27001:2015). ДСТУ ISO/IEC 27002:2015 "Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки".
16.	Payment Card Industry Data Security Standard (PCI DSS) — стандарт безпеки даних індустрії банківських платіжних карток, розроблений Радою зі стандартів безпеки індустрії платіжних карток
17.	Положення про організацію системи управління ризиками в банках України та банківських групах, затверджене постановою Правління НБУ від 11.06.2018 № 64 (зі змінами)
18.	Положення про організацію системи внутрішнього контролю в банках України та банківських групах, затверджене постановою Правління НБУ від 02.07.2019 № 88

3. Терміни та визначення

3.1. Терміни та визначення, що використовуються в Політиці, вживаються в таких значеннях:

Автоматизована (інформаційна) система (АС, АІС) - організаційно-технічна система, в якій реалізується певна технологія обробки інформації з використанням технічних і програмних засобів.

Бізнес-процес - сукупність взаємопов'язаних або взаємодіючих видів діяльності, спрямованих на створення певного продукту або послуги.

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

Доступність – властивість інформації, яка полягає в тому, що користувач або процес, який володіє відповідними повноваженнями, може використовувати інформацію відповідно до повноважень, коли ця інформація йому необхідна.

Загроза - будь-які обставини або події, які можуть бути причиною порушення сервісів інформаційної безпеки: доступності, цілісності, конфіденційності - стосовно інформаційних ресурсів або нанесення збитків інформаційній системі.

Захист інформації в інформаційній системі - діяльність, яка спрямована на забезпечення безпеки інформації, яка обробляється в інформаційній системі, та інформаційної системи в цілому, і дозволяє запобігти або ускладнити можливість реалізації загроз, а також знизити величину потенційних збитків внаслідок реалізації загроз.

Інформаційно-технологічна інфраструктура (ІТ-інфраструктура) Банку - програмно-технічні засоби обчислень, інформаційні ресурси і системи, засоби комунікацій, інформаційної безпеки та

технологічного забезпечення, що належать Банку, поєднані в єдину організаційно-технічну систему і забезпечують комплексну автоматизацію всіх виробничих, технологічних та бізнес-процесів Банку.

Інформаційна безпека (ІБ) - багаторівневий комплекс нормативних вимог, організаційних заходів, програмних і технічних засобів, що забезпечують захист інформації від дії випадкових і навмисних загроз, у результаті реалізації яких можливе порушення сервісів безпеки: доступності, цілісності, конфіденційності.

Інцидент інформаційної безпеки - небажана чи непередбачувана подія інформаційної безпеки, яка має значну ймовірність компрометації бізнес-процесів і загрози інформаційній безпеці.

Конфіденційність – властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем або процесом.

Подія інформаційної безпеки - це ідентифікована подія інформаційної системи, організаційного або технологічного процесу, інформаційної служби або телекомунікаційної мережі, яка вказує на можливе порушення політики інформаційної безпеки або відмову засобів захисту чи раніше невідому ситуацію, яка може мати відношення до безпеки.

Система управління інформаційною безпекою (СУІБ) - частина загальної системи управління, яка ґрунтується на підході, що враховує бізнес-ризики, призначена для розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування і вдосконалення інформаційної безпеки.

Спеціальний керівний орган з інформаційної безпеки - Комітет з інформаційної безпеки Банку.

Цілісність – властивість інформації, яка полягає в тому, що інформація не може бути модифікована неавторизованим користувачем або процесом.

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

4. Сфера застосування та напрями заходів інформаційної безпеки Банку

4.1.1. У Банку створюється єдина комплексна система інформаційної безпеки, сфера застосування якої охоплює критичні бізнес-процеси (список критичних бізнес процесів наведено у Положенні про визначення критичних бізнес-процесів, програмно-технічних комплексів (які забезпечують їх функціонування) в Публічному акціонерному товаристві «Комерційний Індустріальний Банк» та їх опис, № 14/04-1 від 14.04.2017 або прийнятому йому на зміну).

4.1.2. Відповідно до ДСТУ ISO/IEC 27001:2015 Банк визначає наступні основні напрями заходів інформаційної безпеки:

4.1.2.1. Політики безпеки. Нормативні документи Банку (політики, положення, правила, процедури тощо) щодо заходів інформаційної безпеки визначаються, затверджуються і доводяться до відома працівникам Банку та зацікавленим зовнішнім сторонам в межах, необхідних для виконання відповідних задач. Документи інформаційної безпеки переглядаються Банком в заплановані інтервали часу або за появи істотних змін, для забезпечення їх постійної придатності, адекватності й ефективності.

4.1.2.2. Організація інформаційної безпеки. Визначення сфер відповідальності та запровадження регламентованих правил і процедур розподілу ролей і обов’язків в організаційній структурі СУІБ з урахуванням можливих конфліктів інтересів, у тому числі для організації контактів з повноважними органами і сторонніми організаціями.

4.1.2.3. Мобільне обладнання та віддалена робота. Впровадження політики та заходів безпеки щодо використання мобільного обладнання, а також захисту інформації, яка доступна, обробляється або зберігається в місцях віддаленої роботи.

4.1.2.4. Безпека людських ресурсів. Впровадження регламентованих процедур підбору кандидатів та підрядників, атестації та навчання працівників Банку з метою перевірки розуміння, здатності виконувати та виконання ними вимог і функціональних обов’язків стосовно заходів безпеки.

4.1.2.5. Управління активами СУІБ. Класифікація та ідентифікація активів СУІБ, підтримка в актуальному стані їх переліків та описів. Нормативне регламентування сфер допустимого використання. Затвердження розподілу власників, розпорядників та користувачів ресурсів СУІБ.

4.1.2.6. Класифікація інформації. Забезпечення належного рівня захисту інформації відповідно до її важливості для Банку. Інформація має бути класифікована і промаркована в термінах правових вимог, цінності, критичності й чутливості для неавторизованого розкриття чи модифікації. Визначення та регламентування процедур поводження з ресурсами СУІБ відповідно до системи класифікації інформації.

4.1.2.7. Поводження з носіями. Застосування регламентованих процедур щодо запобігання несанкціонованому розголошенню, модифікації, вилученню або знищенню інформації, яка зберігається на носіях.

4.1.2.8. Контроль доступу. Обмеження доступу до інформації та засобів оброблення інформації в межах необхідних мінімальних потреб. Забезпечення контролю за повноваженнями користувачів і запобігання несанкціонованому доступу до систем та послуг IT-інфраструктури. Визначення правил використання привілейованих повноважень. Розподіл відповідальності працівників Банку та третіх сторін за дотримання правил безпеки роботи з інформаційними ресурсами Банку.

4.1.2.9. Криптографічні засоби захисту. Впровадження політики та забезпечення використання криптографічних засобів для захисту конфіденційності, автентичності та/або цілісності інформації.

4.1.2.10. Фізична безпека та безпека інфраструктури. Запобігання несанкціонованому фізичному доступу, пошкодженню та втручанню в засоби оброблення інформації. Запровадження заходів безпеки приміщень та обладнання, у тому числі від інфраструктурних загроз.

4.1.2.11. Безпека експлуатації. Забезпечення коректного та безпечного функціонування засобів оброблення інформації. Процедури експлуатації мають бути задокументовані та доступними для всіх користувачів. Зміни в бізнес-процесах і засобах оброблення інформації, які впливають на інформаційну безпеку, мають бути контрольованими.

4.1.2.12. Захист від зловмисного коду. Впровадження спеціальних заходів та засобів безпеки щодо виявлення зловмисного коду та запобігання від ураження програмного забезпечення та інформаційних ресурсів Банку внаслідок його дії. Застосування регламентованих процедур захисту від зловмисного коду в усіх системах та автоматизованих робочих місцях працівників Банку.

4.1.2.13. Резервне копіювання. Впровадження політики та засобів резервного копіювання та відновлення важливих і критичних інформаційних ресурсів і систем в необхідний узгоджений проміжок часу та об‘єму відновлення.

4.1.2.14. Ведення журналів аудиту та моніторинг. Застосування регламентованих засобів збору, безпечного зберігання і аналізу інформації з системних журналів та журналів аудиту дій користувачів і адміністраторів інформаційних систем з метою моніторингу і виявлення проблем і тенденцій негативного розвитку подій та попередження інцидентів інформаційної безпеки.

4.1.2.15. Безпека комунікацій. Забезпечення захисту інформації в мережах передачі даних та засобів, що підтримують їх роботу. Політики, процедури та заходи безпеки для захисту обміну інформацією з використанням усіх видів комунікацій мають бути регламентовані та затверджені. Характеристики безпеки, рівні послуг, а також вимоги до управління послугами комунікацій мають бути ідентифіковані і регламентовані у внутрішніх нормативних документах та угодах з третіми сторонами.

4.1.2.16. Придбання, розроблення та підтримка інформаційних систем. Застосування регламентованих процедур та вимог щодо заходів безпеки інформації на всіх етапах життєвого

циклу інформаційних систем Банку: розробки, придбання, підтримки, використання та припинення експлуатації.

4.1.2.17. Взаємовідносини з постачальниками. Регламентування, моніторинг та перегляд вимог щодо інформаційної безпеки та розподілу ризиків між Банком та постачальниками, що пов'язані з безпосереднім доступом постачальників до ресурсів ІТ-інфраструктури Банку в процесах надання послуг або постачання товарів і робіт.

4.1.2.18. Управління інцидентами інформаційної безпеки. Застосування регламентованих процедур збору, поширення, накопичення та обробки інформації про події та інциденти інформаційної безпеки. Забезпечення реагування на інциденти інформаційної безпеки згідно з нормативно визначеними процедурами.

4.1.2.19. Безперервність інформаційної безпеки. Впровадження та виконання плану забезпечення безперервної діяльності ІТ систем в рамках процесу управління безперервністю діяльності Банку. Забезпечення безперервності заходів безпеки інформації на всіх етапах реалізації плану безперервної діяльності.

4.1.2.20. Безпека банківських операцій. Забезпечення заходів безпеки інформації згідно з вимогами для систем автоматизації банківської діяльності, платіжних систем та систем переказу коштів.

4.1.2.21. Відповідність. Впровадження регламентованої процедури моніторингу змін у законодавстві, нормативно-правових актах Національного банку України, правилах платіжних систем та інших нормативних документах, виконання яких передбачено договірними зобов'язаннями, з метою забезпечення правової відповідності нормативних документів і угод Банку. Забезпечення захисту всіх важливих записів від несанкціонованих змін.

4.1.2.22. Перевірки інформаційної безпеки. Впровадження регламентованих періодичних процедур перевірки відповідності реалізації заходів безпеки вимогам чинного законодавства, нормативно-правових актів Національного Банку України та внутрішніх нормативних документів Банку.

5. Цілі заходів та вимоги інформаційної безпеки

5.1. Для організації діяльності із розробки та застосування заходів інформаційної безпеки за напрямами інформаційної безпеки Банком розробляються та затверджуються цілі заходів та вимоги інформаційної безпеки.

5.2. Цілі заходів та вимоги інформаційної безпеки визначають застосовність сервісів безпеки: доступності, цілісності, конфіденційності - для захисту інформації, ресурсів ІТ-інфраструктури та бізнес-процесів Банку. Вимоги інформаційної безпеки виражаються у вигляді характеристик і параметрів, яким мають задовольняти заходи інформаційної безпеки, та встановлюють якісні та кількісні показники в системі внутрішнього контролю процесів СУІБ, які мають бути забезпечені за результатами реалізації заходів інформаційної безпеки.

5.3. Джерелами для формування цілей заходів та вимог інформаційної безпеки є зовнішні та внутрішні фактори, що визначають діяльність Банку, а саме: закони України, стандарти інформаційної безпеки та нормативно-правові акти Національного банку України, 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 нормативні документи Банку, що регламентують принципи обміну та обробки інформації відповідно до потреб бізнесу.

5.4. Перелік цілей заходів і вимог інформаційної безпеки складається за участю власників бізнес-процесів та інформаційних активів і затверджується Правлінням Банку у вигляді внутрішнього нормативного документу.

5.5. Перелік вимог інформаційної безпеки не є незмінним і має відповідати дійсному рівню зовнішніх і внутрішніх загроз, стану розвитку інформаційної інфраструктури, толерантності Банку до

ризиків. Спеціальний керівний орган з інформаційної безпеки та підрозділ інформаційної безпеки організовують процеси підготовки, періодичного перегляду та затвердження переліку цілей заходів і вимог інформаційної безпеки. Перегляд переліку здійснюється щорічно за результатами оцінки ефективності інформаційної безпеки і використовується для планування і визначення стратегії розвитку СУІБ. Перегляд цілей заходів і вимог інформаційної безпеки має здійснюватися, також, у разі появи чинників, що можуть суттєво вплинути на безпеку діяльності Банку.

6. Принципи інформаційної безпеки

6.1. Інформаційна безпека Банку ґрунтується на принципах:

6.1.1. Пріоритет цілей. Управління і діяльність щодо забезпечення інформаційної безпеки здійснюється з урахуванням цілей, стратегії і політики Банку.

6.1.2. Персональна відповідальність за порушення вимог ІБ. Усі співробітники Банку, незалежно від займаної посади, несуть персональну відповідальність за дотримання вимог ІБ згідно з чинним законодавством України та внутрішніми нормативними документами Банку. Керівники підрозділів Банку додатково несуть відповідальність за порушення вимог ІБ та інші неправомірні дії підлеглих співробітників.

6.1.3. Залучення керівництва. Керівництво Банку безпосередньо бере участь в управлінні інформаційною безпекою Банку.

6.1.4. Законність. Діяльність із забезпечення інформаційної безпеки здійснюється у суворій відповідності до вимог чинного законодавства України.

6.1.5. Дотримання стандартів у галузі інформаційної безпеки. Під час здійснення захисних заходів враховуються вимоги національних та міжнародних стандартів у галузі інформаційної безпеки.

6.1.6. Відповідальність. Керівництво підрозділів Банку безпосередньо відповідає за дотримання заходів інформаційної безпеки щодо інформаційних ресурсів, власниками яких вони є.

6.1.7. Зобов’язання. Забезпечується виконання зобов’язань Банку перед третіми сторонами в галузі інформаційної безпеки і в управлінні ризиками.

6.1.8. Публічність інформаційної безпеки. Правила і вимоги інформаційної безпеки є відкритими і доводяться до відома працівникам Банку, стороннім організаціям та суб’єктам господарської діяльності, з якими Банк має взаємовідносини, клієнтам і контрагентам Банку, а також оприлюднюється на зовнішніх інформаційних ресурсах Банку.

6.1.9. Системність і комплексність. Діяльність із забезпечення інформаційної безпеки суворо і всебічно регламентується. Формування політики, як сукупності норм, вимог, положень та інструкцій, здійснюється на підставі системного методологічно обґрунтованого підходу і враховує усі найбільш слабкі та вразливі місця інформаційних систем.

6.1.10. Адекватність захисних заходів. Ресурси захищаються шляхом впровадження відповідних засобів і заходів інформаційної безпеки. Захисні заходи є адекватними загрозам і можливим втратам від негативного впливу цих загроз.

6.1.11. Безперервність. Забезпечення інформаційної безпеки є безперервним, цілеспрямованим процесом з реалізації засобів і методів захисту інформаційних ресурсів Банку. Забезпечується впровадження відповідних заходів протягом усього життєвого циклу автоматизованих систем і технологічних процесів, які їм відповідають.

6.1.12. Удосконалення і розвиток (циклічність). Управління інформаційною безпекою є реалізацією циклічної послідовності процесів: «планування» – «реалізація планів» – «перевірка та оцінка стану системи» – «удосконалення».

6.1.13. Мінімізація повноважень. Надання доступу до інформації здійснюється на основі мінімально необхідного для виконання службових обов’язків обсягу.

6.1.14. Виключення конфлікту інтересів. Передбачає чіткий розподіл обов'язків працівників Банку і виключення ситуацій, коли сфера відповідальності працівників Банку допускає конфлікт інтересів.

6.1.15. Внутрішній контроль. Впровадження системи внутрішнього контролю СУІБ на основі показників виконання заходів інформаційної безпеки.

6.1.16. Корпоративна етика. Дотримання політики інформаційної безпеки є елементом корпоративної етики.

6.1.17. Проектування засобів забезпечення інформаційної безпеки на ранніх стадіях розробки систем. Заходи інформаційної безпеки повинні розглядатися на стадіях визначення вимог до систем і проектів, на етапах проектування і розробки.

6.1.18. Необхідність запобігання проблемам та інцидентам інформаційної безпеки. Забезпечення інформаційної безпеки на основі аналізу виявлених порушень (інцидентів) не є ефективним. Необхідно забезпечити попередження та усунення інцидентів.

7. Об'єкти захисту

7.1. Об'єктами захисту в Банку є інформаційні активи - матеріальні чи нематеріальні об'єкти, які є інформацією або містять інформацію, служать для обробки, зберігання або передачі інформації і мають цінність для Банку.

7.2. За кожним інформаційним активом розпорядчим документом Банку призначається власник - структурний підрозділ банку в особі його начальника, який ініціював його створення або використовує для виконання бізнес завдань. Власник інформаційного активу приймає рішення про необхідність його зміни / модернізації, оцінює інформаційні ризики щодо активів, приймає рішення щодо їх мінімізації, прийняття або передачі, розглядає та організовує виконання вимог ІБ, погоджує доступ до інформаційного активу, приймає рішення про знищення інформаційного активу або виведення з експлуатації.

7.3. Порядок призначення власників інформаційних активів, категорювання інформаційних активів визначається окремим внутрішнім нормативним документом.

8. Управління інформаційними ризиками

8.1. Управління інформаційними ризиками є безперервним процесом і включає:

- ідентифікацію загроз і вразливостей для інформаційних активів;
- аналіз та оцінку ризиків з точки зору їх впливу на інформаційний актив, ймовірності їх реалізації;
- інформування власників інформаційних активів і керівництва Банку про ймовірність реалізації ризиків і можливі наслідки;
- обробку ризиків з метою зменшення їх впливу;
- ефективний моніторинг і регулярний перегляд ризиків і заходів щодо управління ними.

8.2. Управління інформаційними ризиками здійснюється відповідно до Методики оцінки та обробки ризиків інформаційної безпеки Акціонерного товариства «Комерційний Індустріальний Банк.

8.3. Результати оцінки ризиків беруться до уваги при прийнятті керівництвом Банку управлінських рішень з метою адекватного реагування на виявлені проблеми та визначення конкретних заходів щодо їх вирішення.

9. Відповідальність та контроль

9.1. У відповідності до вимог Положення про організацію системи внутрішнього контролю в банках України та банківських групах, затвердженого постановою Правління НБУ від 02.07.2019 №88, Положення про організацію системи управління ризиками в банках України та банківських групах, затвердженого постановою Правління НБУ від 11.06.2018 №64 (зі змінами) та внутрішніх

нормативних документів у Банку впроваджена система внутрішнього контролю під час виконання процесів інформаційної безпеки, що ґрунтується на розподілі обов'язків між підрозділами Банку із застосуванням моделі трьох ліній захисту, а саме:

9.2. **Перша лінія захисту** - на рівні бізнес-підрозділів та підрозділів підтримки, що задіяні в процесах інформаційної безпеки, зокрема: Управління інформаційної безпеки АТ, Департамент інформаційних технологій, Департамент банківської безпеки, Департамент по роботі з персоналом, Управління загальнобанківської методології та інші підрозділи Банку, що задіяні в процесах інформаційної безпеки, побудови та розвитку СУІБ. Зазначені структурні підрозділи здійснюють функції, визначені цією Політикою, приймають ризики в процесі своєї діяльності та несуть відповідальність за поточне управління цими ризиками, здійснюють заходи контролю у порядку, визначеному цією Політикою та іншими внутрішніми нормативними документами Банку.

На цій лінії захисту внутрішній контроль здійснюється за наступними видами контролів: попередній, поточний та подальший.

Попередній контроль передує процесам інформаційної безпеки, зокрема, наявність підтримки Керівництвом Банку процесів, наявність необхідного забезпечення процесів фінансовими та кадровими ресурсами.

Поточний контроль здійснюється під час виконання процесів інформаційної безпеки та полягає в контролі за виконанням вимог цієї Політики; своєчасному інформуванні Керівництва Банку про порушення Політики.

Подальший контроль здійснюється у відповідності до вимог нормативно-правових актів НБУ та внутрішніх документів Банку і полягає у виявленні причин порушень і недоліків та визначенні заходів щодо їх усунення; перевірці наявності відповідних документів, що оформлюються під час дотримання процесів з питань інформаційної безпеки. Подальший контроль здійснюється відповідальними працівниками Департаменту банківської безпеки, Департаменту ІТ, Управління інформаційної безпеки із залученням за необхідності працівників інших структурних підрозділів Головного офісу Банку.

9.3. **Друга лінія захисту** - на рівні Департаменту ризик-менеджменту та Служби комплаєнс-контролю, мінімальні вимоги щодо діяльності яких встановлені в Положенні про організацію системи управління ризиками в банках України та банківських групах, затвердженому постановою Правління НБУ від 11.06.2018 №64 (зі змінами) та Положенні про організацію системи внутрішнього контролю в банках України та банківських групах, затвердженому постановою Правління НБУ від 02.07.2019 №88, зокрема: контроль за виявленням, вимірюванням та оцінкою інформаційного ризику, який є складовою операційного ризику, та інших ризиків, що виникають в процесах інформаційної безпеки; контроль за дотриманням норм законодавства та внутрішніх нормативних документів Банку (Служба комплаєнс-контролю) та виконання інших функцій контролю у відповідності до функцій Департаменту ризик-менеджменту та Служби фінансового моніторингу і комплаєнс-контролю, визначених внутрішніми нормативними документами з питань управління ризиками.

На другій лінії захисту Департамент ризик-менеджменту та Служба комплаєнс-контролю аналізують, оцінюють, узагальнюють, складають звітність щодо результатів моніторингу ефективності системи внутрішнього контролю (СВК), проведеного бізнес-підрозділами та підрозділами підтримки на першій лінії захисту, з наданням відповідних рекомендацій. Моніторинг ефективності СВК, документальне оформлення його результатів, строки подання на засідання Правління Банку та Наглядової ради на розгляд та погодження звіту про результати моніторингу СВК здійснюється у порядку, визначеному внутрішньою Процедурою здійснення моніторингу ефективності системи внутрішнього контролю в АТ «КІБ».

9.4. **Третя лінія захисту** - на рівні Служби внутрішнього аудиту, яка здійснює незалежну оцінку ефективності діяльності першої та другої ліній захисту та загальну оцінку ефективності системи внутрішнього контролю з урахуванням вимог, установлених Положенням про організацію внутрішнього аудиту в банках України, затвердженим постановою Правління НБУ від 10.05.2016 №311 (зі змінами), Положенням про організацію системи управління ризиками в банках України та банківських групах, затвердженим постановою Правління НБУ від 11.06.2018 №64 (зі змінами),

Положенням про організацію системи внутрішнього контролю в банках України та банківських групах, затвердженим постановою Правління НБУ від 02.07.2019 №88.

9.5. Наглядова Рада та Правління Банку сприяють і підтримують впровадження та реалізацію Політики, затверджують звіти та стратегію розвитку інформаційної безпеки.

9.6. Відповідальність за дотримання Політики покладається на всіх співробітників і підрозділи Банку.

9.7. Відповідальність за ознайомлення персоналу з Політикою, в межах компетенції, покладається на Управління інформаційної безпеки, Управління загальнобанківської методології та Департамент по роботі з персоналом.

9.8. Відповідальність за класифікацію інформаційних активів, узгодження прав доступу користувачів ІС та участь у процесі оцінки ризиків ІБ несуть власники інформаційних активів та бізнес процесів.

9.9. Відповідальність за організацію та проведення спільно з власниками інформації класифікації інформаційних активів, спільно з власниками ІС оцінки ризиків ІБ, вибір організаційних та технічних засобів безпеки, розробку, впровадження та контроль за виконанням організаційних заходів безпеки, періодичний аналіз вразливостей ІС, узгодження, контроль за наданням та періодичний перегляд прав доступу користувачів ІС, моніторинг подій ІБ; управління інцидентами ІБ; аналіз змін в ІС з точки зору ІБ; розроблення вимог щодо налаштувань безпеки інформаційних систем Банку, розроблення або участь у розробленні внутрішніх нормативних документів Банку щодо інформаційної безпеки, моніторинг національних та міжнародних технологічних рішень та аналіз трендів з інформаційної безпеки, аналіз ефективності СУІБ та формування рекомендацій для Наглядової Ради та Правління Банку несе Управління інформаційної безпеки.

9.10. Відповідальність за участь в процесі класифікації інформаційних активів, участь в процесі оцінки ризиків ІБ, вибір організаційних та технічних засобів безпеки, впровадження та адміністрування технічних засобів безпеки, узгодження привілейованих прав доступу користувачів ІС, активацію та деактивацію прав доступу в ІС, участь у процесі розслідування інцидентів ІБ, управління змінами та життєвим циклом ІС несе Департамент інформаційних технологій.

9.11. Профільні підрозділи Банку, що беруть участь у розробці та погодженні даної Політики, несуть відповідальність за зміст Політики, відповідно до їх компетенції.

9.12. Кожний працівник Банку забезпечує підтримку відповідного рівня інформаційної безпеки Банку. В межах своїх службових обов'язків та повноважень працівники виконують та відповідають за виконання вимог Політики, законодавчих, регуляторних і внутрішньобанківських норм і несуть відповідальність за їх порушення згідно із законодавством України та внутрішніми нормативними документами Банку.

9.13. Контроль за виконанням даної Політики покладається на відповідальну особу за інформаційну безпеку Банку.

10. Управління ризиками

10.1. Процесам інформаційної безпеки, що регламентуються цією Політики, притаманні наступні види ризиків:

- Операційні ризики - управління даним видом ризиків будується на принципах контролю в частині інформаційних ризиків, здійснення аналізу та оцінки операційного інциденту за фактом: невчасного інформування щодо виникнення інцидентів пов’язаних з інформаційною безпекою, порушення цілісності інформаційних активів, порушення безперервності інформаційної безпеки, невиконання співробітниками Банку вимог цієї Політики тощо.
- Комплаєнс-ризики – управління даним видом ризиків здійснюється шляхом дотримання вимог законодавства, враховуючи вимоги нормативно-правових актів НБУ, відповідних стандартів професійних об’єднань, дія яких поширюється на Банк, та внутрішніх нормативних документів Банку; управління конфліктами інтересів тощо.
  Дотримання вимог законодавства, враховуючи вимоги нормативно-правових актів НБУ,

відповідних стандартів професійних об'єднань, дія яких поширюється на Банк, здійснюється шляхом:

- розробки внутрішніх нормативних документів, які регламентують процес управління інформаційною безпекою;
- розподілу в межах організаційної структури Банку повноважень, обов'язків та відповідальності між підрозділами, задіяними в процесі управління інформаційною безпекою;
- регламентації та забезпечення контролю за дотриманням відповідальними працівниками підрозділів, задіяних в процесі управління інформаційною безпекою, вимог, встановлених цією Політикою; інформуванням керівників Банку відповідного рівня, підрозділу комплаєнс-контролю про виявлені порушення, помилки і недоліки;
- контролю за інформаційними системами та технологіями Банку під час їх придбання, розроблення або супроводження та здійснення інших процедур контролю, запроваджених внутрішніми нормативними документами Банку згідно з вимогами Положення про організацію системи внутрішнього контролю в банках України та банківських групах, затвердженого постановою Правління НБУ від 02.07.2019 №88.

10.2. Управління ризиками, притаманними процесам інформаційної безпеки, які регламентує ця Політика, здійснюється відповідно до внутрішніх нормативних документів Банку, зокрема: Стратегії управління ризиками АТ «КІБ», Кодексу поведінки (етики) АТ «КІБ», Політики з управління операційним ризиком (в тому числі інформаційним ризиком) Акціонерного товариства «Комерційний Індустріальний Банк», Політики з управління комплаєнс-ризиком Акціонерного товариства «Комерційний Індустріальний Банк», Політики запобігання конфліктам інтересів в Акціонерному товаристві «Комерційний Індустріальний Банк», Методики управління операційним ризиком АТ «КІБ», Порядком управління комплаєнс-ризиком в АТ «КІБ» та іншими документами, що регламентують питання управління ризиками, у т.ч. комплаєнс-ризику.

10.3. З метою ефективного управління та мінімізації ризиків, зазначених в даному розділі цієї Політики, здійснюється комплекс заходів, спрямованих на зниження ймовірності настання подій та обставин, що призводять до операційних збитків, та/або на зменшення розмірів потенційних операційних збитків.

11. Прикінцеві положення

11.1. Політика набирає чинності з дати затвердження Наглядовою радою Банку.

11.2. Перегляд цієї Політики відбувається не рідше одного разу на рік на відповідність чинному законодавству України, нормативно-правовим актам НБУ, внутрішнім нормативним документам Банку.

11.3. Зміни та доповнення до Політики погоджуються рішенням Правління Банку та затверджуються Наглядовою радою Банку.

11.4. У разі невідповідності будь-якої частини цієї 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 буде діяти лише в тій частині, яка не суперечитиме чинному законодавству України або нормативно-правовим актам Національного банку України. До внесення відповідних змін до Політики відповідальні працівники Банку в своїй роботі повинні керуватися нормами чинного законодавства України.

11.5. У разі зміни назв структурних підрозділів, які задіяні в процедурах, що описані в Політиці, при незмінності функцій, дана Політика вважається дійсною щодо їх нової назви.