ComInBank
Комерційний Індустріальний Банк

ЗАТВЕРДЖЕНО
Наглядова рада Акціонерного товариства
«Комерційний Індустріальний Банк»
протокол № 05/04-1 від 05 квітня 2019 року

ПОГОДЖЕНО
Правління Акціонерного товариства «Комерційний Індустріальний Банк»
протокол № 05/04-2 від 05 квітня 2019 року

Політика інформаційної безпеки Акціонерного товариства «Комерційний Індустріальний Банк»

(Версія 2.0)

Київ – 2019

ЗМІСТ

1. Загальні положення

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

1.2. Мета впровадження Політики інформаційної безпеки Банку – це визначення і використання в діяльності Банку нормативних вимог, організаційних і технічних заходів, що направлені на захист інформаційних активів; запобігання і зниження збитків, що можуть наступити в наслідок 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. Політика інформаційної безпеки встановлює обов'язкові вимоги до змісту і організації заходів інформаційної безпеки Банку згідно з вимогами чинного законодавства України, нормативно-правових актів Національного банку України з питань інформаційної безпеки та з урахуванням міжнародних стандартів і загальноприйнятих у міжнародній практиці принципів забезпечення інформаційної безпеки і кіберзахисту.

1.4. Банк розробляє, затверджує та постійно переглядає, з метою актуалізації, стратегію розвитку інформаційної безпеки, відповідно до потреб бізнесу та стратегії розвитку Банку.

1.5. 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.

1.6. Банк, згідно з вимогами державних стандартів з інформаційної безпеки ДСТУ ISO/IEC 27001:2015, ДСТУ ISO/IEC 27002:2015, регламентує, впроваджує та використовує 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 та кіберзахисту.

1.7. Банк визначає організаційну структуру управління, використання та контролю за впровадженням та функціонуванням інформаційної безпеки. Відповідальність за реалізацію Політики покладається на Наглядову Раду та Правління Банку, спеціальний колективний керівний орган з інформаційної безпеки, підрозділ інформаційної безпеки та керівників усіх структурних підрозділів Банку, відповідно до повноважень.

1.8. Складовими Політики є нормативні, організаційно-розпорядчі, експлуатаційні та технічні документи, які встановлюють цілі, вимоги і правила заходів безпеки за визначеними Банком напрямами інформаційної безпеки та кіберзахисту.

1.9. Вимоги і правила Політики є обов'язковими для виконання всіма підрозділами та працівниками Банку.

1.10. Політика інформаційної безпеки Банку є відкритою та визначає принципи і заходи безпеки, виконання яких гарантується Банком для захисту обміну інформацією з використанням усіх видів комунікації з усіма зацікавленими організаціями та фізичними особами.

2. Нормативне забезпечення

2.1. Перелік законодавчих і нормативних документів, які використовувалися при розробці Політики (у тому числі, нормативних, організаційно-розпорядчих, експлуатаційних та технічних документів за різними напрямами заходів Політики) зазначений у Додатку 1 до цієї Політики.

3. Терміни та визначення

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 та спостережності, - 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 та спостережності.

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.

Кіберзахист - сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання інцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування ІТ-інфраструктури Банку.

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.

Спостережність – властивість інформації, яка дозволяє однозначно встановлювати користувачів і процеси, а також фіксувати дії користувачів і процесів з цією інформацією з метою запобігання та/або розслідування порушень політики 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. У Банку створюється єдина комплексна система інформаційної безпеки, сфера застосування якої охоплює всі бізнес-процеси, банківські продукти, технологічні процеси, інформаційні системи та інформаційні ресурси Банку, в межах яких здійснюється зберігання, обробка або передавання інформації, незалежно від її змісту, конфіденційності та застосованих інформаційних технологій.

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

4.2.1. 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.

4.2.2. 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.

4.2.3. 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.

4.2.4. 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.

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

4.2.6. 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.

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

4.2.8. 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 правила використання привілейованих повноважень. Розподіл відповідальності працівників Банку та третіх сторін за дотриманням правил безпеки роботи з інформаційними ресурсами Банку.

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

4.2.10. 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.

4.2.11. 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.

4.2.12. 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 всіх системах та автоматизованих робочих місцях працівників Банку.

4.2.13. Резервне копіювання. Впровадження політики та засобів резервного копіювання та відновлення важливих і критичних інформаційних ресурсів і систем.

4.2.14. 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.

4.2.15. 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.

4.2.16. 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.

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

4.2.18. 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.

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

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

4.2.21. 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.

4.2.22. 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 та спостережності, - для захисту інформації, ресурсів IT-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 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:

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

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

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

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

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

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

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 Банку має взаємовідносини, клієнтам і контрагентам Банку, а також оприлюднюється на зовнішніх інформаційних ресурсах Банку.

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.

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.

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.

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

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

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

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

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

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.

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. Система управління інформаційною безпекою

7.1. Сукупність організаційних та виробничих процесів Банку, які стосуються розробки, впровадження і застосування заходів інформаційної безпеки, а також процеси, пов'язані з управлінням, моніторингом, оцінкою ефективності, переглядом, підтримуванням та вдосконаленням роботи підрозділів та Банку в цілому в галузі інформаційної безпеки, складають зміст системи управління інформаційною безпекою - СУІБ.

7.2. Організаційні засади, принципи планування, виконання, оцінки ефективності, перегляду і розвитку СУІБ, як процесу, що є складовою загальної системи управління Банку, визначаються у нормативному документі Банку - Політиці управління інформаційною безпекою.

8. Відповідальність та контроль

8.1. Керівництво Банку розуміє, що інформаційна безпека є важливою складовою успішної та безперервної діяльності Банку. У Банку створений та постійно працює керівний орган з питань інформаційної безпеки, обов'язки відповідальної особи за інформаційну безпеку Банку покладено на заступника Голови Правління з операційної діяльності Банку.

8.2. Наглядова Рада та Правління Банку сприяють і забезпечують впровадження та реалізацію Політики інформаційної безпеки, контролюють її виконання, затверджують звіти та стратегію розвитку.

8.3. На керівний орган з інформаційної безпеки Банку покладаються обов'язки з виконання таких завдань:

– погодження та перегляд: політики інформаційної безпеки, положення щодо застосовності та стратегії розвитку інформаційної безпеки 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.

8.4. Відповідальна особа за інформаційну безпеку Банку (Chief information security officer, CISO) має повноваження, достатні для прийняття управлінських рішень, та забезпечує:

– стратегічне керівництво з питань інформаційної безпеки Банку;

– визначення напрямів розвитку інформаційної безпеки Банку, їх відповідність стратегії розвитку Банку;

– відповідність заходів безпеки інформації потребам бізнес-процесів/банківських продуктів;

– контроль за впровадженням заходів безпеки інформації в Банку.

8.5. Підрозділ з інформаційної безпеки Банку здійснює:

– розроблення вимог щодо налаштувань безпеки інформаційних систем Банку;

– розроблення або участь у розробленні внутрішніх нормативних документів Банку щодо інформаційної безпеки;

– контроль за виконанням заходів щодо забезпечення безпеки інформації на всіх стадіях життєвого циклу інформаційних систем Банку;

– розслідування інцидентів безпеки інформації;

– спільно з підрозділами інформаційних технологій (інформатизації, автоматизації) Банку відновлення функціонування інформаційних систем Банку після збоїв у роботі внаслідок інцидентів безпеки інформації. Стратегія розвитку інформаційних технологій Банку, всі проекти, які пов'язані з інформаційними технологіями, узгоджуються з Політикою інформаційної безпеки та Політикою СУІБ.

8.6. 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.

8.7. Документи Політики доступні працівникам Банку у межах їх повноважень та функціональних обов'язків. У Банку створюються умови та проводяться навчання працівників з питань інформаційної безпеки та СУІБ. Здійснюється контроль знань і виконання норм та заходів інформаційної безпеки та СУІБ.

9. Прикінцеві положення

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

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

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

9.4. 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.

9.5. 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.

Додаток 1
до Політики інформаційної безпеки АТ «КІБ»

Перелік законодавчих і нормативних документів, які були використані при розробці нормативних документів Банку з питань інформаційної безпеки

Закони України:

- «Про інформацію» від 02.10.1992 № 2657-XII, в редакції від 01.01.2017.
- «Про банки і банківську діяльність» від 07.12.2000 № 2121-III, в редакції від 09.02.2019.
- «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII , в редакції від 08.07.2018.
- «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.94 № 80/94-ВР, в редакції від 19.04.2014.
- «Про електронні документи та електронний документообіг» від 22.05.2003 № 851-IV, в редакції від 07.11.2018.
- «Про електронні довірчі послуги» від 05.10.2017 № 2155-VIII.
- «Про захист персональних даних» від 01.06.2010 № 2297-VI, в редакції від 30.01.2018.
- «Про платіжні системи та переказ коштів в Україні» від 05.04.2001 № 2346-III, в редакції від 07.02.2019.

Нормативно-правові акти Національного банку України:

- Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України, затверджене постановою Правління Національного банку України від 28.09.2017 № 95.
- Положення про організацію бухгалтерського обліку, бухгалтерського контролю під час здійснення операційної діяльності в банках України, затверджене постановою Правління Національного банку України від 04.07.2018 № 75.
- Положення про застосування електронного підпису в банківській системі України, затверджене постановою Правління Національного банку України від 14.08.2017 № 78, в редакції від 25.02.2019.
- Положення про забезпечення безперервного функціонування інформаційних систем Національного банку та банків України, затверджене постановою Правління Національного банку України від 17.06.2004 № 265, в редакції від 18.12.2015.
- Положення про організацію системи управління ризиками в банках України та банківських групах, затверджене постановою Правління НБУ від 11.06.2018 № 64, в редакції від 01.01.2019.
- Правила зберігання, захисту, використання та розкриття банківської таємниці, затверджені постановою Правління Національного банку України від 14.07.2006 № 267, в редакції від 07.02.2019.
- Правила організації захисту електронних банківських документів, з використанням засобів захисту інформації Національного банку України, затверджені постановою Правління Національного банку України від 26.11.2015 № 829, в редакції від 31.03.2019.
- Правила з технічного захисту інформації для приміщень банків, у яких обробляються електронні банківські документи, затверджені постановою Правління Національного банку України від 04.07.2007 № 243, в редакції від 19.02.2008.
- Правила з організації захисту приміщень банків України, затверджені постановою Правління Національного банку України від 10.02.2016 № 63, в редакції від 22.08.2018.

Національні стандарти України з питань інформаційної безпеки:

- ДСТУ ISO/IEC 27000:2015 "Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Огляд і словник".
- 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".

Міжнародні стандарти з питань інформаційної безпеки:

- Серія міжнародних стандартів ISO/IEC 27000 Міжнародної Організації зі стандартизації (ISO) та Міжнародної електротехнічної Комісії (IEC), яка включає стандарти інформаційної безпеки та кібербезпеки.
- Payment Card Industry Data Security Standard (PCI DSS) — стандарт безпеки даних індустрії банківських платіжних карток, розроблений Радою зі стандартів безпеки індустрії платіжних карток (Payment Card Industry Security Standards Council, PCI SSC), заснованою міжнародними платіжними системами Visa, MasterCard, American Express, JCB і Discover.