«ЗАТВЕРДЖЕНО»
Рішенням Наглядової ради
АТ «ПІРЕУС БАНК МКБ»
Протокол № 17_22
Від 08.12.2022

ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ
АТ «ПІРЕУС БАНК МКБ»

Загальна інформація про Документ

Назва	Політика інформаційної безпеки АТ «ПІРЕУС БАНК МКБ»
Автор	Управління інформаційної безпеки
Власник	Управління інформаційної безпеки
Код версії	553
Дата версії	08/12/2022

Історія документу

Код версії	Дата затвердження версії	Опис внесених змін	Автор версії
1.0	08.09.2011	Створення документу	Управління інформаційної безпеки
2.0	26.06.2016	Перегляд Політики згідно рекомендацій інспекції НБУ	Управління інформаційної безпеки
277ISD-PLC-05022019-3.0	05.02.2019	Перегляд Політики згідно рекомендацій Внутрішнього аудиту Групи за результатами перевірки ефективності впровадження та підтримки системи управління інформаційною безпекою (ISMS) та у зв'язку із набранням чинності Постанови № 95 від 28.09.2017.	Управління інформаційної безпеки
76	07.09.2021	Внесення змін відповідно до Стратегії розвитку інформаційних технологій та пов'язаних заходів інформаційної безпеки.	Управління інформаційної безпеки
553	08.12.2022	Внесення змін відповідно до імплементації вимог Постанови НБУ №178 від 12.08.2022 «Про затвердження Положення про організацію кіберзахисту в банківській системі України та внесення змін до Положення про визначення об'єктів критичної інфраструктури в банківській системі України» та рекомендацій Департаменту комплаєнс контролю.	Управління інформаційної безпеки

Пов’язані документи

Назва	Ким видано
Стратегія розвитку інформаційної безпеки АТ «ПІРЕУС БАНК МКБ»	Управління інформаційної безпеки

Зміст

1. Політика інформаційної безпеки

1.1. Вступ

Політика інформаційної безпеки АТ “ПІРЕУС БАНК МКБ” (далі – "Політика") є нормативним документом, який формулює й відображає позицію АТ «ПІРЕУС БАНК МКБ» (далі – "Банк") у сфері інформаційної безпеки. Він описує основні принципи, викладені Керівництвом Банку, що визначають побудову структури інформаційної безпеки.

Банківська інформація є важливим активом Банку. Вся банківська інформація підлягає захисту відповідно до її цінності, та у спосіб, що зміцнює довіру клієнтів, забезпечує відповідність регулятивним нормам та захищає конкурентоспроможність Банку.

У цьому документі описуються загальні вектори розвитку інформаційної безпеки та принципи, визначені Керівництвом, які використовуються для управління інформаційною безпекою Банку на шляху досягнення цілей бізнес-стратегії Банку. Інші, більш специфічні політики, процедури, стандарти, інструкції, регламенти тощо розробляються з урахування вимог даної Політики.

1.2. Сфера застосування

Вимоги Політики інформаційної безпеки поширюються на процеси Банку, його інформаційні системи та інфраструктуру та є обов’язковими до виконання всіма працівниками Банку, а також стосується взаємовідносин з постачальниками, провайдерами та партнерами, послуги яких пов’язані з використанням, обробкою чи доступом до інформації або інформаційних активів Банку, та які обробляють чи використовують банківську інформацію у своїй діяльності.

Будь-які випадки недотримання Політики інформаційної безпеки підлягають розслідуванню. У випадку виявлення порушень, до винних застосовуються заходи згідно чинного законодавства України.

1.3. Терміни та визначення

Банк – АТ «ПІРЕУС БАНК МКБ»

Банківська (корпоративна) інформація – сукупність інформації (в електронній, письмовій чи усній формі), яка обробляється у Банку, а також використовується для підтримки процесів Банку. Інформація, яка створюється третіми особами від імені Банку та інформація, на яку Банк має авторські права, також відноситься до банківської інформації.

Інформаційна система – комбінація апаратного, програмного забезпечення та даних, яка забезпечує функціонування процесів Банку.

Власник інформації – підрозділ Банку, який відповідає за процес, в якому виконується обробка інформації. Власник інформації відповідає за дотримання вимог інформаційної безпеки та визначає порядок використання інформації в процесі.

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

Доступність – властивість досяжності інформації або інформаційного активу, яка визначає можливість використання інформації або інформаційної системи на вимогу авторизованого об'єкта у мінімально необхідному обсязі.

Конфіденційність – властивість інформації (або інформаційного активу), яка полягає в тому, що доступ до неї не може бути отриманий неавторизованою особою, об'єктом та/або процесом, внаслідок адміністративних / правових обмежень, накладених її власником.

Цілісність – властивість інформації (або інформаційного активу), яка полягає у неможливості її модифікації несанкціоновано, без дозволу / відома її власника.

Система управління інформаційною безпекою (СУІБ) – частина загальної системи управління Банку, заснована на підході оцінки ризиків, призначена для створення, впровадження, експлуатації, контролю, аналізу, підтримки та покращення інформаційної безпеки Банку.

Критичні інформаційні активи (критична інформація) – сукупність інформації, в письмовому чи електронному вигляді, що представляє цінність для Банку та / або його клієнтів, а також несанкціоноване чи неконтрольоване розголошення або втрата якої може завдати шкоди Банку чи клієнтам. Критичність інформації визначається, виходячи із рівнів її класифікації щодо конфіденційності, цілісності та доступності.

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

Кіберзахист (як система в банківській системі України) – сукупність суб'єктів, упроваджених систем, комплексів та засобів забезпечення кіберзахисту, взаємопов'язаних заходів організаційного, технічного, інформаційного характеру щодо забезпечення належного рівня кібербезпеки та кіберстійкості банківської системи України.

Кібербезпека – це безпека IT систем (обладнання та програм). Кібербезпека є частиною інформаційної безпеки будь-якої організації.

1.4. Нормативні посилання

Дана Політика розроблена з урахуванням вимог:

- Національних стандартів України з питань ІБ:
  - ДСТУ ISO/IEC 27000:2019 "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";
  - ДСТУ ISO/IEC 27002:2015 "Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки";
- Постанови Правління НБУ №95 від 28.09.2017 року «Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України»;
- Постанови Правління НБУ №4 від 16.01.2021 року «Про затвердження Положення про здійснення контролю за дотриманням банками вимог законодавства з питань інформаційної безпеки, кіберзахисту та електронних довірчих послуг»;

- Постанови Правління НБУ №178 від 12.08.2022 «Про затвердження Положення про організацію кіберзахисту в банківській системі України та внесення змін до Положення про визначення об'єктів критичної інфраструктури в банківській системі України»;

1.5. Мета, завдання та цілі

Метою Політики є впровадження, підтримка та постійне вдосконалення СУІБ, яка має забезпечувати необхідний рівень інформаційної безпеки в умовах штатного функціонування та в умовах реалізації загроз, захист інформації та ресурсів Банку від зовнішніх і внутрішніх загроз та загроз, які пов'язані з навмисними та ненавмисними діями працівників Банку, визначення основних засад функціонування системи кіберзахисту в банківській системі України. Також загальною метою для Банку є захищеність інформації.

Завданнями та цілями Політики інформаційної безпеки Банку є:

- Підтримка завдань Банку за допомогою забезпечення конфіденційності, цілісності та доступності банківської інформації та інформаційних систем / інфраструктури;
- Зменшення ризику порушення конфіденційності, цілісності та доступності банківської інформації шляхом визначення правил використання банківської інформації та інформаційних систем;
- Поширення інформації щодо загальних правил інформаційної безпеки серед персоналу Банку та представників третіх осіб, визначаючи тим самим обов'язки, відповідальність та роль кожного працівника;
- Забезпечення відповідності регулятивним нормам та контрактним зобов'язанням;
- Забезпечення захисту ділової репутації та іміджу Банку;
- Забезпечення масштабування процесів Банку та зміцнення довіри клієнтів до продуктів й послуг Банку, створюючи таким шляхом конкурентні переваги;
- Управління інформаційної безпекою, зокрема визначення ролей та обов'язків у сфері ІБ;
- Класифікація інформаційних активів;
- Здійснення оцінки ризиків ІБ;
- Забезпечення безпеки інформаційних активів відповідно до категорії їх класифікації та оцінки ризиків;
- Моніторинг подій ІБ та управління інцидентами ІБ;
- Забезпечення безперервності діяльності Банку в частині, що стосується ІБ;
- Організація та контроль забезпечення безпечного управління життєвим циклом інформаційних систем Банку.

1.6. Основні вимоги, правила, принципи, ролі та відповідальність в частині забезпечення ІБ.

Принципи та правила:

- Публічні сервіси та внутрішні мережі Банку повинні відповідати вимогам стандартів з ІБ;

- Для зменшення ризиків виникнення інцидентів ІБ керівництво Банку повинно створювати всім працівникам Банку умови для систематичного навчання нормам та заходам ІБ;
- У Банку створюються, діють, систематично тестуються та оновлюються Плани безперебійного функціонування діяльності Банку на випадок непередбачуваних (критичних) ситуацій;
- Працівники Банку та представники третіх осіб, що мають доступ до інформації та/чи інфраструктури Банку, беруть участь у підтримці відповідного рівня ІБ в межах своїх посадових обов'язків та повноважень і несуть відповідальність за його порушення в межах, встановлених чинним законодавством України та внутрішніми нормативними документами Банку.

Банком застосовуються наступні заходи щодо забезпечення ІБ:

- Визначено перелік критичних процесів, інформаційних ресурсів (активів), які забезпечують їх функціонування, та заходів, необхідних для їх належного захисту;
- Створено та затверджено перелік відомостей, банківської, у. які відноситься до банківською комерційної таємниці та конфіденційної інформації Банк;
- Визначено оцінку критичності інформаційних активів;
- Встановлено правила доступу до інформаційних ресурсів та програмно-технічних комплексів;
- Забезпечується контроль фізичного та логічного доступу до всіх наявних ресурсів;
- Забезпечується антивірусний захист інформаційних ресурсів;
- Забезпечується захист мережі та захист віддаленого доступу до ресурсів мережі (локальної, мережі Інтернет, мереж інших організацій);
- Забезпечується ідентифікація та автентифікація всіх визначених ресурсів;
- Забезпечується криптографічний захист інформації;
- Банк розробляє вимоги з інформаційної безпеки (та, зокрема, з кібербезпеки) для третіх сторін, які надають Банку послуги з аутсорсингу, розробки, впровадження, аудиту інформаційних систем і ресурсів, а також отримують від Банку інформацію з обмеженим доступом. Ці вимоги, відповідальність та контроль за їх виконання вищезазначеними третіми сторонами визначаються в угодах (договорах) з цими сторонами.

Ролі та відповідальність:

- Ефективна ІБ Банку забезпечується шляхом безперервної участі працівників усіх підрозділів на всіх етапах діяльності;
- Кожен працівник Банку чи третьої сторони, що має доступ до інформації та/чи інфраструктури Банку, забезпечує підтримку відповідного рівня інформаційної безпеки;
- В межах своїх функціональних обов'язків та повноважень працівники виконують та відповідають за виконання вимог Політики, законодавчих, регуляторних і внутрішньобанківських норм та несуть відповідальність за їх порушення згідно із чинним законодавством України та внутрішньобанківськими нормативними документами;
- Функції із забезпечення кіберзахисту покладені на Управління інформаційної безпеки, що підпорядковується відповідальній особі за інформаційну безпеку банку (CISO)

- У Банку створений та постійно працює спеціальний Керівний орган з питань впровадження та функціонування СУІБ (далі – "Керівний орган СУІБ"), рішення та настанови якого є обов'язковими до виконання всіма працівниками Банку;
- Керівний орган СУІБ забезпечує процес розроблення, впровадження, функціонування, моніторингу, перегляду, підтримання та вдосконалення СУІБ;
- На Керівний орган СУІБ покладені завдання щодо визначення завдань інформаційної безпеки, їх відповідності вимогам чинного законодавства України, зокрема, нормативно-правовим актам Національного банку України, нормативним документам Банку, а також їх інтегрованості у процеси та банківські продукти;
- Керівний орган СУІБ затверджує та переглядає Політику, аналізує ефективність її реалізації та здійснює контроль за діяльністю будь-якого підрозділу Головного офісу та відділень Банку щодо виконання ними вимог нормативно-правових актів НБУ та нормативних документів Банку з питань інформаційної безпеки шляхом ініціювання перед Головою Правління Банку проведення перевірок підрозділів Головного офісу та відділень Банку з питань впровадження і функціонування СУІБ, виконання рішень Керівного органу СУІБ. Постійний контроль впровадження, виконання, вдосконалення та підтримки Політики в актуальному стані покладений на Керівний орган СУІБ;
- Для зменшення ризиків виникнення інцидентів інформаційної безпеки Керівництво Банку створює працівникам умови для систематичного навчання нормам та заходам інформаційної безпеки.

2. Загальні положення інформаційної безпеки.

Прихильність Керівництва Банку до управління інформаційною безпекою є очевидною і зрозумілою для всіх працівників Банку. Стратегія розвитку інформаційної безпеки відображає мету Керівництва Банку щодо побудови надійної системи інформаційної безпеки. З цією метою Керівництво Банку затверджує політики безпеки, процедури, стандарти та норми й забезпечує їх дотримання.

Цей документ визначає роль Керівництва Банку відносно інформаційної безпеки. Загальні принципи інформаційної безпеки визначають основні необхідні дії та заходи, виконання яких є обов'язковою умовою побудови захищеного робочого процесу. Такі принципи – це короткі характеристики положень Політики інформаційної безпеки, яких обов'язково дотримуються усі працівники Банку, а також інші особи, які мають доступ до банківської інформації чи інформаційних систем.

Загальні положення випливають із потреб інформаційної безпеки Банку, які визначаються шляхом оцінки ризиків у інформаційних системах, вивченням міжнародних стандартів з питань інформаційної безпеки та національних регулятивних норм.

Загальні положення встановлюють мінімальний рівень безпеки, визначений Керівництвом Банку, який відноситься до усіх працівників Банку та третіх осіб, які мають доступ до банківської інформації чи інформаційних систем. Загальні положення свідчать про важливість та необхідність захисту банківської інформації.

Усі рішення відносно інформаційної безпеки та безпеки інформаційних систем приймаються з урахуванням положень, описаних у цьому документі, як мінімальних вимог щодо інформаційної безпеки.

Загальні положення інформаційної безпеки, що застосовуються у кожній організації поділяються на базові та функціональні положення.

2.1. Базові положення

Базові положення є загальними директивами, які використовуються для встановлення та підтримки прийнятного рівня інформаційної безпеки Банку в цілому. Базові положення є основою для визначення функціональних принципів.

2.1.1. Відповідальною особою за інформаційну безпеку Банку (Chief information security officer, CISO) є Член Правління Банку (або особа, що виконує його повноваження) 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 процесів/банківських продуктів;
- контроль за впровадженням заходів безпеки інформації в Банку.

2.1.2. Підпорядкованість та / або підзвітність надає можливість перевірки дій сторін, залучених до обробки інформації, та забезпечує, що дії користувача (працівника чи працівника третьої сторони) однозначно можуть визначати такого користувача. Ролі та відповідальність визначаються відповідно до критичності інформації.

2.1.3. Відповідальність за контроль виконання вимог Політики та своєчасну поінформованість з питань інформаційної безпеки підлеглих працівників, несуть їх керівники за відповідним напрямком роботи. Кожен працівник повинен забезпечувати підтримку відповідного рівня інформаційної безпеки. В межах своїх функціональних обов'язків та повноважень працівники повинні виконувати та відповідати за виконання вимог Політики та нормативних документів, затверджених у Банку.

2.1.4. Усі правила та методи, які застосовуються для забезпечення прийнятного рівня інформаційної безпеки у Банку, не суперечать встановленим соціально-етичним нормам.

2.1.5. Рівень інформаційної безпеки досягається завдяки спільним діям власників інформації, користувачів інформаційних систем, адміністраторів інформаційних систем та спеціалістів з інформаційної безпеки. Рішення приймаються після детального розгляду й обговорення та оцінки усіх задіяних підрозділів Банку задля досягнення найвищого доцільного рівня інформаційної безпеки.

2.1.6. Механізми безпеки та контролю, що застосовуються до кожного інформаційного активу, є пропорційними цінності такого активу, загрозам, які можуть вплинути на цей актив та втратам, які можуть бути отримані у разі порушення інформаційної безпеки цього активу.

2.1.7. Запровадження принципу цілісності – застосування механізмів, впровадження політик, процедур та стандартів як цілісної системи інформаційної безпеки допомагає досягнути більш ефективної безпеки, а також зниження вартості та складності системи.

2.1.8. Створення порядку реагування на інциденти. При виникненні інциденту з інформаційної безпеки (та, зокрема, кібербезпеки) персонал Банку своєчасно та скоординовано реагує відповідно до затверджених процедур обробки інцидентів інформаційної безпеки. Зменшення чи попередження майбутніх загроз досягається за рахунок своєчасного використання відповідних адміністративних та технічних засобів безпеки.

2.1.9. У зв'язку із розвитком інформаційних технологій та потреб бізнесу у Банку зростає кількість загроз та вразливостей для інформації та інформаційних систем, що вимагає періодичної переоцінки становища. Переоцінка допомагає визначити відхилення відносно впроваджених механізмів та засобів безпеки та контролю, а також надлишковий ризик. Управління ризиками є досить важливим завданням для Банку так, як і питання прийняття рішень про приймання ризику чи зниження рівня ризику до прийнятного.

2.1.10. Політика інформаційної безпеки та контролі безпеки, які використовуються у Банку, враховують та не порушують права сторін, задіяних в обробці інформації.

2.2. Функціональні принципи

Функціональні принципи є похідними та визначаються із базових положень. Вони покривають специфічні тематичні області (політики, процедури, стандарти, інструкції, тощо з інформаційної безпеки) та визначають області застосування системи управління інформаційною безпекою Банку.

2.2.1. Дотримання Політики інформаційної безпеки

Усі працівники Банку повинні розуміти необхідність захисту банківської інформації, інформаційних систем та інфраструктури та дотримуються усіх вимог визначених у політиках, процедурах, технічних стандартах та методиках з інформаційної безпеки. Персонал Банку та представники третіх сторін, які мають доступ до банківської інформації чи інформаційних систем, повинні бути ознайомленими з Політикою інформаційної безпеки.

2.2.2. Призначення власника інформації

Для усіх видів банківської інформації повинен бути визначений її власник, який несе відповідальність за її функції. Власник інформації також відповідальний за захист інформації, навіть якщо відповідальність за обробку інформації була передана іншій, більш спеціалізованій стороні, чи якщо власник дозволив надання доступу до інформації третій стороні.

2.2.3. Класифікація та захист інформації

Уся банківська інформація класифікована відповідно до встановленої схеми класифікації. Віднесення інформації до певного класу здійснюється власником інформації відповідно до її конфіденційності, цілісності та доступності. Більш того, інформація захищається відповідним чином

при її зберіганні, обробці та передачі. Класифікація інформації передбачає, що інформація використовується та захищається належним чином.

2.2.4. Організаційна структура системи інформаційної безпеки

Для досягнення прийнятного рівня безпеки необхідна тісна взаємодія з боку усіх підрозділів Банку. З цією метою, задачі безпеки (ролі, завдання, відповідальності) так само, як і критичні процедури, повинні чітко визначатись для всього Банку для досягнення однозначності та взаєморозуміння при виборі та застосуванні адміністративних та технічних механізмів безпеки.

Для вирішення питань щодо управління системою інформаційної безпеки в Банку створено Керівний орган СУІБ, до складу якого входять представники підрозділів, які є власниками та учасниками критичних процесів, спеціалісти з інформаційної безпеки та, за необхідністю представники інших підрозділів Банку.

Банк має у складі підрозділ з інформаційної безпеки, який безпосередньо підпорядковується відповідальній особі за інформаційну безпеку Банку. Підрозділ з інформаційної безпеки контролює та координує призначених осіб щодо застосування Політики інформаційної безпеки Банку (Групи Піреус) у різних сферах, впровадження відповідного захисту та механізмів контролю та ефективне виконання завдань з інформаційної безпеки. Працівникам підрозділу з інформаційної безпеки заборонено розробляти, впроваджувати, супроводжувати чи експлуатувати інформаційні системи Банку, які не використовуються для забезпечення безпеки інформації.

2.2.5. Ефективність адміністративних та технічних засобів контролю інформаційної безпеки

Задля дотримання відповідності прийнятному рівню інформаційної безпеки у Банку необхідно впровадження та перегляд ефективності адміністративних та технічних засобів безпеки (контролів). Адміністративні та технічні засоби безпеки (контролі) є важливими, оскільки вони є взаємопов’язаними між собою та формують єдину систему управління інформаційною безпекою.

Адміністративні та технічні засоби безпеки (контролі), які використовуються у Банку, перевіряються на відповідність існуючим політикам, процедурам та стандартам, а також проводиться їх переоцінка щодо ефективності запобігання існуючим загрозам та актуалізація відповідно до вимог інформаційної безпеки.

2.2.6. Відповідальність за дотриманням працівниками вимог з інформаційної безпеки

Керівники структурних підрозділів Банку повинні вживати усіх необхідних заходів задля дотримання політик, процедур, стандартів, інструкцій, регламентів та методичних рекомендацій інформаційної безпеки у їхніх підрозділах. Відповідальність щодо загального рівня інформаційної безпеки, дотримання Політики інформаційної безпеки у Банку покладена на Керівництво Банку та поширюється на усіх працівників на всіх рівнях Банківської організаційної структури (top-down approach).

2.2.7. Аудит Політики інформаційної безпеки

Перевірка дотримання політик, процедур, стандартів, інструкцій, регламентів та методичних рекомендацій інформаційної безпеки працівниками Банку та третіми особами здійснюється

періодичними проведеннями незалежного аудиту інформаційної безпеки. Зовнішній аудит проводиться згідно з нормами законодавства України, національних стандартів та з урахуванням міжнародних стандартів аудиту. Програма аудиту формується, ураховуючи особливості діяльності Банку, характер та обсяг банківських, фінансових послуг та інші види діяльності.

2.2.8. Відповідність нормам інформаційної безпеки

Контролі та засоби, впроваджені для захищення банківської інформації, визначені та обрані на основі існуючих регулятивних норм та контрактних зобов'язань Банку, що забезпечують вільний обмін ідеями, вільний інформаційний потік, конфіденційність інформації та комунікацій, захист персональних даних та прозорість процесу.

Відповідно до вимог діючого законодавства України Голова Правління Банку (або особа, що його замінює, або відповідальний за інформаційну безпеку Член Правління) організовує проведення зовнішнього аудиту (з метою одержання Банком оцінки інформаційної безпеки) відповідно до законодавства в сфері захисту інформації та кібербезпеки. Така оцінка використовується Банком для забезпечення своєчасного моніторингу стану впровадження та ефективності функціонування СУІБ, визначення можливостей вдосконалення та потреби проведення коригувальних дій.

Також, Банк зобов'язаний проводити щорічну самооцінку стану інформаційної безпеки/кіберзахисту шляхом складання щорічного Звіту з питань оцінювання ризиків інформаційної безпеки/кіберризиків із урахуванням відомостей за результатами щорічного проведення:

1) оцінювання ризиків інформаційної безпеки/кіберзахисту відповідно до внутрішніх нормативних документів;

2) оцінювання результативності інформаційної безпеки та ефективності СУІБ;

3) зовнішнього аудиту інформаційної безпеки;

4) внутрішнього аудиту інформаційної безпеки/кіберзахисту (далі - "Внутрішній аудит").

Відповідальність за складання Звіту несе відповідальний підрозділ Банку за інформаційну безпеку.

2.2.9. Інформування та навчання щодо інформаційної безпеки

Для підвищення рівня обізнаності та відповідальності працівників Банку та третіх сторін у сфері інформаційної безпеки (та, зокрема, кібербезпеки), Банком розроблена відповідна програма навчання. Метою цієї програми є забезпечення того, що всі працівники, які мають доступ до банківської інформації та інформаційних систем, розуміють необхідність захисту такої інформації та приймають відповідальність, яку вони несуть. Більш того, програма націлена на роз'яснення загальних принципів інформаційної безпеки, яких повинні дотримуватись усі співробітники, та розвиток знань щодо інформаційної безпеки.

2.2.10. Належне використання інформації

Працівники Банку є відповідальними за використання належним чином банківської інформації та інформаційних систем/інфраструктури відповідно до існуючих політик, процедур, стандартів, інструкцій, регламентів та методичних рекомендацій інформаційної безпеки для забезпечення цілей та вимог бізнесу.

2.2.11. Безперервність бізнесу

Для забезпечення безперервності бізнесу та мінімізації шкоди, яка може бути завдана у випадку непередбачуваних ситуацій (стихійні лиха, відмова систем, тощо). Банком розробляється та застосовується Планування безперервності бізнесу (Business continuity plan) та План відновлення діяльності підрозділів (Disaster recovery plan). Керівництво Банку відповідає за прийняття відповідних заходів, що гарантуватимуть безперервність бізнесу у відповідності до потреб бізнесу.

Також забезпечується доступність та відмовостійкості об'єктів кіберзахисту ,здійснюється оперативне реагування на кібератаки та кіберінциденти відповідно до Плану реагування, інформування Центру кіберзахисту відповідно до базових сценаріїв реагування на кіберінциденти; наданням на запит CSIRT-NBU інформації, потрібної для здійснення реагування на кібератаки, кіберінциденти в банківській системі України в термін та обсязі, що зазначені в запиті,

2.2.12. Управління персоналом

Досягнення цілей інформаційної безпеки може бути здійснено шляхом включення спеціальних положень до договорів персоналу, впровадженням відповідних заходів у процес найму нових працівників, розподілом обов'язків, а також наявністю постійного процесу навчання персоналу щодо дотримання норм та вимог інформаційної безпеки. Навчання персоналу щодо питань інформаційної безпеки повинно здійснюватися не рідше одного разу на рік, а також при перегляді Політики інформаційної безпеки та при внесенні важливих змін у дану Політику чи інші політики та / або процедури, які супроводжують систему інформаційної безпеки Банку.

Політика інформаційної безпеки Банку поширюється на усі підрозділи Банку, а також на представників компаній, які мають доступ, обробляють чи використовують банківську інформацію у своїй діяльності. Будь-які випадки недотримання Політики інформаційної безпеки розслідуються та у випадку виявлення порушень можуть бути застосовані дисциплінарні санкції.

2.2.13. Контроль доступу

Власники інформації та інформаційних систем несуть відповідальність за визначення осіб, яким буде надано доступ до інформації та інформаційних систем згідно потреб бізнесу та ролям користувачів. Права доступу оновлюються та переглядаються відповідно до потреб бізнесу. Надання, зміна, скасування, блокування та тимчасова передача прав доступу до інформації / інформаційних систем відбувається згідно розроблених Банком регулятивних документів.

2.2.14. Моніторинг захищеності систем

Для визначення рівня безпеки критичних інформаційних активів періодично проводиться моніторинг за допомогою технічних засобів у наявності, згідно графіка проведення планових аудитів систем, задля дотримання захищеності систем. Результати перевірки критичних систем аналізуються та надаються Керівництву Банку.

2.2.15. Оцінка ризиків

Оцінка ризиків проводитися на регулярній основі (щорічно) для ідентифікації загроз та вразливостей, визначення прийнятного рівня ризику для Банку та обрання належних засобів захисту, адміністративних та технічних контролів для управління ризиками.

2.2.16. Вимоги інформаційної безпеки

Вимоги інформаційної безпеки Банку розроблені та впроваджені відповідно до цілей інформаційної безпеки Банку та результатів регулярного процесу оцінки ризиків. При впровадженні нової інформаційної системи, сервісу, служби чи проекту для Банку, дотримання вимог інформаційної безпеки є необхідною умовою.

2.2.17. Обробка інцидентів з інформаційної безпеки

Адміністративні та технічні контролі безпеки, які відносяться до інцидентів інформаційної безпеки Банку, ефективно забезпечують обробку таких інцидентів у разі їх виникнення. Користувачі інформаційних систем поінформовані щодо існуючих вимог з інформаційної безпеки та одразу повідомляти у разі виявлення їх порушення:

- Безпосереднього керівника свого структурного підрозділу;
- Управління інформаційної безпеки;
- Управління банківської безпеки;
- Департамент інформаційних технологій.

Інцидент інформаційної безпеки може бути попереджений або ідентифікований, проаналізований і оброблений.

2.2.18. Інформаційна безпека при придбанні, розробці та підтримці інформаційних систем та додатків

Інформаційна безпека має бути пріоритетним напрямком при придбанні та / або розробці й підтримці інформаційних систем. Інформаційні системи, які проектуються та / або розробляються та взаємодіють з іншими інформаційними системами, повинні відповідати затвердженим Банком політикам, процедурам, стандартам, інструкціям, регламентам та методичним рекомендаціям з інформаційної безпеки.

2.2.19. Фізична безпека

Будівлі та/чи приміщення Банку, які використовуються для зберігання важливого обладнання (центри обробки даних, мережеве обладнання, серверні/комутаційні кімнати тощо), а також критичні для процесів Банку приміщення підлягають належному фізичному захисту, відповідно до встановлених у Банку вимог з фізичної безпеки. Фізичний доступ до таких приміщень надається лише авторизованому персоналу.

2.2.20. Управління зв’язками із зовнішніми сторонами

Управління зв’язками Банку із зовнішніми сторонами відповідає визначеним нормам безпеки та впроваджується відповідно до затверджених політик, процедур, стандартів, інструкцій, регламентів та методичних рекомендацій з інформаційної безпеки.

2.2.21. Управління зв’язками із партнерами

Інформаційні системи Банк, можуть бути взаємопов’язаними з інформаційними системами та / або мережами третіх сторін, для швидкого пошуку несправностей чи інших потреб бізнесу. У разі

необхідності, для таких підключень впроваджуються належні заходи інформаційної безпеки для захисту банківської інформації та здійснення контролю дій третіх сторін.

2.2.22. Доступ третіх сторін до інформаційних систем Банку

Надання доступу третім сторонам до інформаційних систем Банку та / або банківської інформації, інформаційних систем / інфраструктури виконується за умов:

- Наявності укладених відповідних договорів, які описують юридичну сторону співпраці та підписаної угоди про нерозголошення конфіденційної інформації (наприклад non-disclosure Agreement, NDA);
- Чітко визначених необхідних та достатніх вимог та контролів інформаційної безпеки;
- Наявності технічної можливості для надання доступу.

Доступ до банківської інформації за наявності усіх необхідних контролів може бути надано лише авторизованим користувачам.

2.2.23. Мінімальний рівень повноважень

Для проведення будь-якої діяльності в інформаційних системах Банку надання повноважень та прав доступу відбувається згідно принципу мінімального рівня повноважень, а саме: повноваження та права доступу, які мають суб'єкти в інформаційній системі банку є мінімально необхідними для якісного виконання покладених задач.

3. Перегляд Політики інформаційної безпеки

Політика інформаційної безпеки переглядається за необхідності, але не рідше одного разу на рік. Позаплановий перегляд Політики інформаційної безпеки можливий у випадку внесення змін до інформаційної інфраструктури та / або впровадженні нових інформаційних технологій, а також змін в законодавчих, регуляторних та нормах тощо.

У разі змін у законодавстві України, у нормативно-правових актах Національного банку України та міжнародних вимог, ця Політика використовується в частинах, що не суперечить наведеним змінам, до її оновлення.

4. Структура ієрархії нормативної бази з інформаційної безпеки

Структура ієрархії нормативної бази з інформаційної безпеки складається з Політики інформаційної безпеки, Стратегії розвитку інформаційної безпеки, профільних Політик, Положень, Процедур, Регламентів, Методик та Інструкцій, що відображають застосування найкращих практик з інформаційної безпеки.

Політика інформаційної безпеки встановлює принципи щодо управління цілями інформаційної безпеки Банку та відповідає вимогам Стратегії розвитку інформаційної безпеки Банку, законодавства України та іншим нормативним і контрактним вимогам. Політика інформаційної безпеки включає цілі та принципи для забезпечення спрямованості всіх дій, пов'язаних з інформаційною безпекою, загальні та спеціальні зони відповідальності, обов'язки та сторони залучені до управління інформаційною безпекою.

Стратегія розвитку інформаційної безпеки – це стратегічний вектор розвитку інформаційної безпеки та принципи, визначені Керівництвом Банку, які використовуються для управління інформаційною безпекою Банку на шляху досягнення мети загальної стратегії розвитку Банку.

Профільні Політики включають:

- Спеціальні Політики, що охоплюють різні тематичні сфери для забезпечення належного рівня інформаційної безпеки в усіх напрямках діяльності Банку (наприклад, «Політика обробки інцидентів з інформаційної безпеки», «Політика криптографічного захисту інформації», тощо);
- Зони відповідальності, обов'язки та сторони, залучені до окремих сфер управління інформаційною безпекою.

Організаційна структура системи інформаційної безпеки включає підрозділи Банку, які охоплює Система управління інформаційною безпекою.

Положення у відповідності до **Профільних Політик** визначають норми, які враховуються у кожній окремій сфері забезпечення інформаційної безпеки та визначають, що та як необхідно здійснити для досягнення вимог інформаційної безпеки.

Процедури, Регламенти, Методики та Інструкції – це нормативні документи, що визначають яким чином, поетапно, в усіх можливих варіантах, виконуються вимоги інформаційної безпеки Банку

та включають в себе чіткі кроки, виконання яких є умовою ефективного управління інформаційною безпекою Банку.

5. Ознайомлення з вимогами Політики

Для забезпечення ознайомлення персоналу Банку та представників третіх сторін, що мають доступ (зокрема, віддалений) до інформації та/чи інформаційних систем/інфраструктури Банку, з Політикою, норми цієї Політики розміщуються зовнішньому сайті Банку для клієнтів та третіх сторін, та на внутрішньому сайті Банку для співробітників Банку у формі окремого електронного документу.

При оновленні вмісту Політики обов'язково здійснюється оновлення документу на зовнішньому та внутрішньому сайті Банку.

Відповідальність за визначення обсягу норм та вимог Політики, що публікується на зовнішньому та внутрішньому сайті Банку, покладається на Управління інформаційної безпеки .

Персонал Банку та представники третіх сторін, що мають доступ до інформації та/чи інформаційних систем Банку під час прийому на роботу (перед отриманням доступу до інформації / інформаційних систем для представників третіх сторін) зобов'язані ознайомитися з Політикою та надати зобов'язання про дотримання конфіденційності.