# ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ АТ «ПЕРШИЙ ІНВЕСТИЦІЙНИЙ БАНК»

**ЗМІСТ:**



## 1. ВСТУП

Політика інформаційної безпеки АТ «ПЕРШИЙ ІНВЕСТИЦІЙНИЙ БАНК» (надалі - Політика) є внутрішнім нормативним документом АТ «ПЕРШИЙ ІНВЕСТИЦІЙНИЙ БАНК» (далі - Банк).

Політика розроблена відповідно до вимог:

- чинного законодавства України, зокрема:
  - національного стандарту України ДСТУ ISO/IEC 27001:2015 «Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги.» (ISO/IEC 27001:2013; Cor 1:2014, IDT);
  - національного стандарту України, ДСТУ ISO/IEC 27002:2015 «Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки.» (ISO/IEC 27002:2013; Cor 1:2014, IDT);
- «Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України», затвердженого постановою Правління НБУ від 28.09.2017 № 95;
- інших нормативно-правових актів Національного банку України;
- внутрішніх документів щодо регулювання діяльності Банку.

Інформація є ресурсом, який, як і інші важливі бізнес-ресурси, має певну цінність для Банку а, отже, потребує відповідного захисту.

Інформаційна безпека передбачає захист інформації від різноманітних загроз для підтримки безперервності бізнесу, скорочення збитків, збільшення прибутку на інвестований капітал і розширення можливостей бізнесу.

Яку б форму не обрала інформація, і які б кошти не використовувалися для її передачі та зберігання, необхідно завжди забезпечувати відповідний рівень її захисту.

В рамках даної Політики під інформаційною безпекою мається на увазі забезпечення наступних характеристик інформації:

- ***конфіденційність:*** надання доступу до інформації тільки тим, у кого є на це право;
- ***цілісність:*** захист точності і повноти інформації і методів її обробки;
- ***доступність:*** забезпечення доступу до інформації і пов'язаних з нею ресурсів авторизованими користувачами по мірі необхідності.

Інформаційна безпека досягається шляхом впровадження сукупності необхідних засобів захисту, в число яких можуть входити політики, рекомендації, інструкції, організаційні структури та програмні функції.

У разі невідповідності будь-якої частини цієї Політики чинному законодавству України, нормативно-правовим актам Національного банку України, у т.ч. у зв'язку із

внесенням до них змін та доповнень, прийняттям нових законодавчих актів України, підрозділи Банку керуються даною Політикою у частині, що не суперечить чинному законодавству.

Політика описує прийняту та впроваджену Банком політику щодо захисту інформаційної безпеки.

Політика інформаційної безпеки Банку є обов'язковою для використання всіма підрозділами Банку.

## 2. ТЕРМІНИ ТА СКОРОЧЕННЯ

**Банк** - АТ «ПЕРШИЙ ІНВЕСТИЦІЙНИЙ БАНК».

**Бізнес-процес -** структурована послідовність дій з виконання певного виду діяльності на всіх етапах життєвого циклу банківської діяльності, метою якої є отримання заданого результату, що має цінність для банку.

**Загроза-** потенційна причина небажаного інциденту, яка може призвести до шкоди для системи або організації.

**Інформаційна безпека -** захист інформації від широкого діапазону загроз з метою забезпечення безперервності бізнесу, мінімізації ризику бізнес-процесів і отримання максимальної рентабельності інвестицій і бізнес-можливостей.

**КУІБ -** спеціальний колегіальний орган Банку з питань інформаційної безпеки.

**Несанкціонована особа, об'єкт або процес** - особа, об'єкт або процес, які не контролюються банком та/або не задовольняють вимоги, які до них висуваються.

**ПТК** – програмно-технічний комплекс.

**РЕСУРСИ СУІБ -** ресурси (ресурси користувачів – людські, інформаційні; технологічні ресурси - та засоби їх підтримки, автоматизовані робочі місця ПТК та зовнішніх систем), які використовуються в рамках критичних бізнес-процесів, та ресурси забезпечення роботи інформаційних технологій (мережеве обладнання, засоби антивірусного захисту тощо).

**САНКЦІОНОВАНИЙ ОБ'ЄКТ** - об'єкт, який контролюється банком та/або задовольняє вимоги, які до нього висуваються.

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

## 3. ЦІЛЬ ПОЛІТИКИ

Ціллю Політики є впровадження та ефективне функціонування системи управління інформаційною безпекою, яка буде забезпечувати безпечність та надійність функціонування бізнес-процесів, захист інформації та ресурсів Банку від зовнішніх та внутрішніх загроз та загроз, які пов'язані з навмисними та ненавмисними діями співробітників Банку, забезпечувати безперервну роботу Банку, сприяти мінімізації ризиків операційної діяльності Банку та створювати позитивну репутацію Банку при роботі з Клієнтами.

Основним завданням інформаційної безпеки є захист інформаційних ресурсів Банку від зовнішніх та внутрішніх, навмисних та ненавмисних загроз.

## 4. СФЕРА ЗАСТОСУВАННЯ

Дія Політики розповсюджується на весь Банк у цілому та використовується для всіх бізнес-процесів Банку, які можуть негативно впливати на результати діяльності Банку своєю відсутністю або функціонуванням з помилками.

## 5. ПРЕДМЕТ ПОЛІТИКИ ТА ОПИС ДІЙ

Дана політика визначає основні принципи і заходи щодо забезпечення та розвитку інформаційної безпеки в усіх підрозділах АТ «ПЕРШИЙ ІНВЕСТИЦІЙНИЙ БАНК», що дозволяють гарантувати захист інформаційних ресурсів для забезпечення ефективності та безперервності бізнес-діяльності відповідно до рекомендацій серії стандартів інформаційної безпеки ISO 27000, а також відповідає вимогам законодавства України та рекомендаціям стандартів України ДСТУ ISO/IEC 27001:2015 «Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги.» (ISO/IEC 27001:2013; Cor 1:2014, IDT) та ДСТУ ISO/IEC 27002:2015 «Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки.» (ISO/IEC 27002:2013; Cor 1:2014, IDT).
Основними принципами інформаційної безпеки, яких дотримується Банк, є підтримання належного захисту інформації із забезпеченням її:

- **Цілісності** - властивість захищеності, безпомилковості та повноти ресурсів СУІБ.
- **Конфіденційності** - властивість інформації не ставати доступною та розкритою для несанкціонованих осіб, об'єктів або процесів.
- **Доступності** - властивість доступності та можливості використання ресурсів СУІБ на вимогу санкціонованого об'єкта.
- **Спостережності** - властивість системи (автоматизованої, контролю доступу, моніторингу тощо) фіксувати діяльність ідентифікованих користувачів і процесів.

Це в першу чергу стосується інформації з обмеженим доступом, до якої відносяться відомості що становлять банківську та комерційну таємницю, персональні дані та іншу конфіденційну інформацію.
Серед основних об'єктів на які розповсюджується дія інформаційної безпеки Банку розглядаються наступні види ресурсів:

- **інформаційні ресурси** - інформація та дані у будь-якому вигляді, що отримуються, зберігаються, обробляються, передаються, оголошуються, у тому числі знання співробітників, партнерів Банку, бази даних та файли, документація, посібники користувача, навчальні матеріали, описи процедур, архівована інформація тощо;
- **програмне забезпечення** - прикладне програмне забезпечення, системне програмне забезпечення, сервісне програмне забезпечення та будь-яке інше програмне забезпечення, незалежно від форми отримання (придбання, власної розробки, таке, що вільно розповсюджується), яке використовується у Банку співробітниками та системами для роботи та взаємодії з клієнтами та іншими внутрішніми та зовнішніми системами тощо;
- **фізичні ресурси** - співробітники, апаратні засоби IT (сервери, робочі станції, міжмережеві екрани, принтери, копіювальні апарати, телекомунікаційне обладнання, обладнання зв'язку, маршрутизатори, АТС, факси, модеми тощо), носії даних (стрічки, диски тощо), меблі, приміщення, виробниче обладнання, інші технічні засоби тощо;
- **сервісні ресурси** - обчислювальні та комунікаційні сервіси (Інтернет, електронна пошта, канали зв'язку тощо), інші технічні сервіси (опалення, освітлення, енергозбереження, кондиціювання повітря, системи сигналізації та моніторингу), усі послуги, пов'язані з отриманням, наданням, використанням, передачею та знищенням ресурсів, усі юридичні та фізичні особи, організації, установи та

підприємства (а також їх співробітники), послугами яких користується Банк для отримання, використання, передачі та знищення ресурсів.

Для кожного ресурсу визначаються можливі ризики інформаційної безпеки та шляхи їх мінімізації, тобто Банк використовує ризик-орієнтований підхід, який забезпечує розуміння, моніторинг та зменшення ризиків операційної діяльності.

Політика базується на вимогах законодавчих, регуляторних та нормативних документів з інформаційної безпеки.

Банком використовуються наступні підходи щодо забезпечення інформаційної безпеки:

- створено та затверджено перелік відомостей, що містять інформацію з обмеженим доступом;
- створено та затверджено перелік критичних бізнес-процесів;
- встановлено правила доступу до інформаційних ресурсів та програмно-технічних комплексів;
- забезпечується контроль фізичного та логічного доступу до всіх визначених ресурсів;
- забезпечується парольний захист програмних та сервісних ресурсів;
- забезпечується антивірусний захист програмних та сервісних ресурсів;
- забезпечується захист мережі;
- забезпечується віддалений доступ до ресурсів мережі (локальної, мережі Інтернет, мереж інших організацій);
- забезпечується ідентифікація та автентифікація всіх визначених ресурсів;
- забезпечується криптографічний захист інформації.

Всі співробітники Банку обізнані та виконують вимоги інформаційної безпеки в роботі.

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

Публічні сервіси Банку та внутрішні мережі Банку відповідають вимогам стандартів з інформаційної безпеки.

Банк забезпечує виконання усіх вимог інформаційної безпеки, які наявні в угодах з третіми сторонами стосовно участі у міжнародних платіжних системах, системах переказу коштів та впровадженні нових ПТК.

Для зменшення ризиків виникнення інцидентів інформаційної безпеки Керівництво Банку створює співробітникам Банку умови для систематичного навчання нормам та заходам інформаційної безпеки.

У Банку складаються, діють, систематично тестуються та оновлюються плани безперебійного функціонування діяльності Банку на випадок різних непередбачуваних критичних ситуацій.

## 6. РОЛІ ТА ВІДПОВІДАЛЬНІСТЬ

Керівництво Банку чітко розуміє, що інформаційна безпека Банку є основою життєдіяльності Банку та сприяє (організаційно та фінансово) впровадженню, контролю та підтримці вимог прийнятої Політики.

У Банку створений та постійно працює Комітет з управління інформаційною безпекою АТ «ПЕРШИЙ ІНВЕСТИЦІЙНИЙ БАНК» (далі – КУІБ), рішення якого є обов'язковими для виконання усіма співробітниками Банку.

Документи системи управління інформаційною безпекою розробляються відділом інформаційної безпеки служби безпеки та іншими структурними підрозділами Банку за відповідними напрямками діяльності.

Документи системи управління інформаційною безпекою доступні співробітникам Банку у межах їх повноважень і призначені надавати допомогу у виконанні вимог інформаційної безпеки.

Постійний контроль впровадження, виконання, вдосконалення та підтримки Політики в актуальному стані покладається на відділ інформаційної безпеки служби безпеки.

Кожний співробітник Банку бере участь у підтримці відповідного рівня інформаційної безпеки Банку в межах своїх обов'язків та повноважень, несе відповідальність за їх порушення в межах, встановлених чинним законодавством України та внутрішньобанківськими нормативними документами.

## 7. ПЕРЕГЛЯД ДОКУМЕНТУ

Перегляд даної Політики повинен проводитися щорічно.
Внесення змін/доповнень до Політики інформаційної безпеки здійснюється відповідальною особою у наступних випадках:

- при змінах в документах, на підставі яких розроблено Політику;
- при впровадженні нових документів, що змінюють/впливають на процеси, описані в Політиці;
- при зміні ролей, відповідальності та процесів, що встановлює дана Політика;
- щорічно, за необхідності актуалізації найменувань документів, на які посилається дана Політика;
- у разі прийняття відповідного рішення колегіальним органом Банку.

Цей документ набуває чинності на наступний робочий день з дня затвердження, якщо інше не зазначено у рішенні Колегіального органу, яким документ затверджується.
Зміни та доповнення до цього документу набувають чинності на наступний робочий день з дня затвердження, якщо інше не зазначено у рішенні Колегіального органу, яким документ затверджується. Усі зміни та доповнення до цього документу є його невід'ємною частиною.
Дана редакція цього документу втрачає свою чинність з дати набрання чинності наступної/ нової редакції цього документу або на підставі рішення Колегіального органу.

## 8. ПЕРЕЛІК ВЗАЄМОПОВ'ЯЗАНИХ ДОКУМЕНТІВ

Ця Політика пов'язана з наступними документами (розроблена на підставі та посилається):

- Національний стандарт України ДСТУ ISO/IEC 27001:2015 «Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги.» (ISO/IEC 27001:2013; Cor 1:2014, IDT), прийнятий наказом ДП «УкрНДНЦ» від 18.12.2015 №193;
- Національний стандарт України ДСТУ ISO/IEC 27002:2015 «Інформаційні технології. Методи захисту. Звід для практик щодо заходів інформаційної безпеки.» (ISO/IEC 27002:2013; Cor 1:2014, IDT), прийнятий наказом ДП «УкрНДНЦ» від 18.12.2015 №193;
- «Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України», затвердженого постановою Правління НБУ від 28.09.2017 № 95.