**«ЗАТВЕРДЖЕНО»**
**Рішенням Наглядової Ради**
**ПАТ «БАНК ІНВЕСТИЦІЙ**
**ТА ЗАОЩАДЖЕНЬ»**
**від «17» 04 2019р. № 5619**
**Голова Наглядової Ради**
**В.І. Зінченко**

**«ПОГОДЖЕНО»**
**Рішенням Правління**
**ПАТ «БАНК ІНВЕСТИЦІЙ**
**ТА ЗАОЩАДЖЕНЬ»**
**від «27» березня 2019 р. №2703-1**
**в.о. Голови Правління**
**В.О.Зінніков**

# Політика
# інформаційної безпеки
# ПАТ «БАНК ІНВЕСТИЦІЙ ТА ЗАОЩАДЖЕНЬ»
(нова редакція)

## Вступ

Політика інформаційної безпеки ПАТ «БАНК ІНВЕСТИЦІЙ ТА ЗАОЩАДЖЕНЬ» (далі - Політика) описує та регламентує функціонування системи управління інформаційною безпекою (далі – СУІБ) відповідно до національних стандартів 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", ДСТУ ISO/IEC 27002:2015 "Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки", міжнародних стандартів з питань інформаційної безпеки, загальноприйнятих у міжнародній практиці принципів забезпечення інформаційної безпеки і кіберзахисту, вимог законодавства України та нормативно-правових актів Національного банку України, вимог міжнародних та внутрішньодержавних платіжних систем та систем переказу коштів, а також вимог внутрішніх нормативних документів ПАТ «БАНК ІНВЕСТИЦІЙ ТА ЗАОЩАДЖЕНЬ» (далі – Банк).

## Ціль політики

Метою Політики є впровадження та ефективне функціонування СУІБ, яка буде забезпечувати створення та постійну підтримку умов, при яких ризики, пов'язані з забезпеченням безпеки інформаційних активів Банку, постійно контролюються та знаходяться на прийнятному рівні.

Досягнення цілей Політики дозволить:

- захистити інформаційні ресурси Банку від зовнішніх і внутрішніх загроз, та загроз, які пов'язані з навмисними та ненавмисними діями працівників Банку;
- забезпечити безперервну роботу інформаційних систем Банку;
- мінімізувати ризики інформаційної безпеки (далі - ІБ), як складової частини операційних ризиків, які властиві операційній діяльності Банку;
- створити позитивну репутацію Банку при роботі з клієнтами та контрагентами Банку.

Шляхи досягнення вищезазначених цілей:

- інвентаризація інформаційних активів Банку, регулярна оцінка та обробка ризиків інформаційної безпеки;
- документування та регламентація процедур досягнення ІБ у відповідності до вимог національних стандартів України з питань ІБ ДСТУ ISO/IEC 27001:2015, вимог законодавства України та нормативно-правових актів Національного банку України;
- регулярне проведення внутрішнього аудиту інформаційних технологій, інформаційної безпеки (в т.ч.СУІБ) та забезпечення безперервної діяльності у відповідності з внутрішніми нормативними документами Банку та стандартом ISO/IEC 27001:2015;
- навчання працівників Банку процедурам забезпечення ІБ.

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

## Принципи політики

В процесі забезпечення ІБ Банк повинен дотримуватися наступних принципів:

- Законність.

При забезпеченні ІБ дотримуватися вимог законодавства України, нормативно-правових актів Національного банку України та інших регуляторних та контролюючих державних органів.

- Відповідність та адекватність до існуючих загроз та економічна обґрунтованість.

Організаційні міри та технічні механізми захисту обираються та застосовуються виходячи з потреб бізнесу та базуються на аналізі ризиків ІБ, зокрема на аналізі актуальних загроз та витрат на впровадження та підтримку цих механізмів. Проводиться періодична оцінка ефективності впроваджених заходів та механізмів захисту.

- Перспективність та орієнтація на національні та міжнародні відкриті стандарти.

Організаційні заходи та технічні засоби СУІБ впроваджуються з урахуванням світових тенденцій в області ІБ. Орієнтація на відкриті стандарти дозволяє використовувати накопичений світовий досвід в області захисту інформації.

- Безперервність функціонування.

Забезпечується відмовостійкість, надійність, доступність та коректність функціонування організаційних заходів та технічних засобів СУІБ.

- Безперервність вдосконалення.

Для забезпечення протидії загрозам ІБ за умов постійної зміни внутрішнього та зовнішнього оточення реалізується безперервний цикл розвитку та вдосконалення СУІБ.

- Персональна відповідальність.

Кожний працівник Банку несе персональну відповідальність за виконання функцій та вимог, що покладені на нього в рамках функціонування СУІБ. У разі порушення вимог ІБ працівник може бути притягнутий до дисциплінарної, матеріальної, адміністративної , кримінальної відповідальності у відповідності до законодавства України.

- Контроль.

Здійснюється постійний контроль виконання працівниками Банку вимог ІБ.

## Сфера застосування

Політика розповсюджується на Банк у цілому та використовується для всіх критичних бізнес-процесів, а також до застосованих у їх функціонуванні інформаційних активів Банку.

## Предмет політики

Основними принципами Політики є підтримання належного захисту інформації із забезпеченням цілісності, конфіденційності, доступності та спостережності.

Це в першу чергу стосується інформації з обмеженим доступом, яка відноситься до "банківської таємниці", "комерційної таємниці", "персональних даних" та іншої конфіденційної інформації.

Банк підтримує ризик-орієнтовний підхід, який забезпечує розуміння, моніторинг та зменшення ризиків операційної діяльності. Деталі ризик-орієнтовного підходу описані в окремому внутрішньому документі.

Всі працівники 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 з інформаційної безпеки, які наявні в угодах з третіми сторонами стосовно участі у міжнародних платіжних системах та системах переказу коштів.

Для зменшення ризиків виникнення інцидентів інформаційної безпеки Керівництво Банку створює працівникам умови для систематичного навчання з інформаційної безпеки.

У Банку складаються, діють, тестуються та оновлюються плани забезпечення безперервного функціонування на випадок непередбачених критичних ситуацій.

## Ролі та відповідальності

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

У Банку створений та постійно працює колегіальний орган - Комісія з питань системи управління інформаційною безпекою (далі - Комісія) Публічного акціонерного товариства «БАНК ІНВЕСТИЦІЙ ТА ЗАОЩАДЖЕНЬ», рішення якої є обов'язковими для виконання усіма працівниками Банку.

Документи з питань СУІБ розробляються структурними підрозділами за відповідними напрямками діяльності та доступні працівникам Банку у межах їх повноважень і призначені надавати допомогу у виконанні вимог інформаційної безпеки.

Постійний контроль за впровадженням, виконанням та вдосконаленням Політики покладений на Комісію.

Підтримка Політики в актуальному стані покладена на керівника підрозділу з інформаційної безпеки.

Кожен працівник Банку забезпечує підтримку відповідного рівня інформаційної безпеки Банку в межах своїх службових обов'язків та повноважень, несе відповідальність за їх порушення згідно із законодавством України та внутрішньобанківськими нормативними документами.

## Перегляд документа

Політика переглядається за необхідності, але не менш ніж одного разу на рік. Причинами внесення змін до Політики є зміни в законодавчих, регуляторних та інших нормах.