«ЗАТВЕРДЖЕНО»
Рішенням Наглядової ради
АТ «БАНК ІНВЕСТИЦІЙ
ТА ЗАОЩАДЖЕНЬ»
від «__» _____ 2021р. №
в.о. Голови Наглядової Ради
О.М.Пєнов

«ПОГОДЖЕНО»
Рішенням Правління
АТ «БАНК ІНВЕСТИЦІЙ
ТА ЗАОЩАДЖЕНЬ»
від «18» 03 2021 р. №18/03-1
Голова Правління
В.О. Зінніков

ПОЛІТИКА
ІНФОРМАЦІЙНОЇ БЕЗПЕКИ
АТ «БАНК ІНВЕСТИЦІЙ ТА ЗАОЩАДЖЕНЬ»

(нова редакція)

м. Київ

Загальна інформація про документ:

Відповідальний за документ:	Начальник відділу інформаційної безпеки Богданов О.В.
Розробник:	Начальник відділу інформаційної безпеки Богданов О.В.
Дія документа поширюється:	Підрозділи Головного банку Відділення

ЗМІСТ

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1. Політика інформаційної безпеки АТ «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 27000:2019 "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", 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 АТ «БАНК ІНВЕСТИЦІЙ ТА ЗАОЩАДЖЕНЬ» (далі – Банк).

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

2. ЦІЛЬ ПОЛІТИКИ

2.1. Цілями 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.

2.2. 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, як складової частини операційних ризиків, які властиві операційній діяльності Банку;
- мінімізувати вплив внутрішніх та зовнішніх негативних факторів, що можуть вплинути на діяльність Банку;
- створити позитивну репутацію Банку при роботі з клієнтами та контрагентами Банку.

2.3. Шляхи досягнення вищезазначених цілей:

- інвентаризація інформаційних активів Банку, регулярна оцінка та обробка ризиків інформаційної безпеки;
- документування та регламентація процедур, досягнення належного рівня ІБ у відповідності до вимог національних стандартів України з питань інформаційної безпеки (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 ДСТУ ISO/IEC 27001:2015;
- впровадження заходів щодо забезпечення безперервної діяльності інформаційних систем Банку у випадках настання (реалізації впливу) негативних факторів;
- навчання працівників Банку процедурам забезпечення інформаційної безпеки;

• реалізація положень "Стратегії розвитку Банку" в частині вимог до стратегії розвитку інформаційної безпеки.

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

3. ПРИНЦИПИ ПОЛІТИКИ

3.1. В процесі забезпечення інформаційної безпеки Банк дотримується наступних принципів:

• ***Законність.*** При забезпеченні інформаційної безпеки 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 інформаційної безпеки, 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 інформаційної безпеки. 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 інформаційної безпеки 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/не виконання функцій та вимог, що покладені на нього в рамках функціонування СУІБ. У разі порушення вимог інформаційної безпеки працівник може бути притягнутий до дисциплінарної, матеріальної, адміністративної, кримінальної відповідальності у відповідності до законодавства України.

• ***Контроль.*** Здійснюється постійний контроль виконання працівниками Банку вимог інформаційної безпеки.

4. ВИМОГИ ПОЛІТИКИ

4.1. Основними вимогами Політики є підтримання Банком належного рівня захисту інформації із забезпеченням цілісності, конфіденційності, доступності та спостережності, відповідно до вимог діючих нормативних та регуляторних актів у всіх аспектах своєї діяльності. Це в першу чергу стосується інформації з обмеженим доступом, яка відноситься до "банківської таємниці", "комерційної таємниці", "персональних даних" та іншої інформації з обмеженим доступом.

4.2. Для впровадження і подальшого вдосконалення СУІБ, Банк чітко визначає нормативно-правові та регуляторні вимоги щодо інформаційної безпеки Банку. Перелік зовнішніх та внутрішніх нормативно-правових, регуляторних вимог та правил з інформаційної безпеки, що є правовою основою політики інформаційної безпеки Банку, визначено в "Політиці управління інформаційною безпекою".

4.3. Банк підтримує ризик-орієнтований підхід, який забезпечує розуміння, моніторинг та зменшення ризиків операційної діяльності. Деталі ризик-орієнтованого підходу описані в

окремому внутрішньому документі.

4.4. Всі працівники Банку обізнані та виконують вимоги інформаційної безпеки в роботі.

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

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

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

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

4.9. Банк забезпечує регулярну перевірку знань працівників з питань інформаційної безпеки за результатами проведеного навчання.

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

5. РОЛІ ТА ВІДПОВІДАЛЬНОСТІ

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

5.2. У Банку створений та постійно діє колегіальний орган – Комісія з питань СУІБ, рішення якої є обов'язковими для виконання усіма працівниками Банку.

5.3. 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.

5.4. Постійний контроль за впровадженням, виконанням та вдосконаленням Політики покладений на Комісію з питань системи управління інформаційною безпекою Банку.

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

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

6. ПРИКІНЦЕВІ ПОЛОЖЕННЯ

6.1. Політика набирає чинності з дати її затвердження і діє до моменту скасування (втрати чинності) або затвердження нової редакції Політики.

6.2. Політика переглядається за необхідністю, але не менш ніж один раз на рік.

6.3. Причинами внесення змін до Політики, є зміни в інформаційній інфраструктурі та/або впровадження нових інформаційних технологій, зміни в законодавчих, регуляторних актах та внутрішніх документах Банку.

6.4. У разі невідповідності будь-якої частини цієї Політики чинному законодавству України, або нормативно-правовим актам Національного банку України, в тому числі у зв'язку з прийняттям нових актів законодавства України, або нормативних актів Національного банку України, ця Політика буде діяти лише у тій частині, яка не суперечитиме чинному законодавству України та нормативним актам Національного банку України.

ЛИСТ ПОГОДЖЕННЯ
до ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ
АТ «БАНК ІНВЕСТИЦІЙ ТА ЗАОЩАДЖЕНЬ»

Розроблено:

Начальник Відділу інформаційної безпеки — О.В.Богданов

Погоджено:

т.в.о. Директора з ризиків — А.Г.Василевський

Начальник Департаменту інформаційних технологій — А.С.Баланда

Начальник Відділу комплаєнс - контролю — В.В.Базюк

Начальник юридичного управління — С.О.Войтович

Начальник Управління методології, ревізій та контролю — М.В.Ламандзія