

## Вимоги політики інформаційної безпеки в АТ «КРЕДОБАНК»

### 1. ВСТУП

З метою забезпечення максимально можливого рівня безпеки банківських послуг та продуктів, що надаються Клієнтам Банку, а також внутрішніх процесів, інфраструктури, ІТС та інформації, що в них обробляється, Банк впровадив Систему Управління Інформаційною Безпекою (СУІБ), відповідно до вимог стандартів НБУ та міжнародного стандарту ISO/IEC 27001:2013. Шляхом впровадження, підтримання та розвитку СУІБ, Банк зобов'язується виконувати вимоги інформаційної безпеки та постійно вдосконалювати СУІБ.

Впроваджена в Банку СУІБ, враховує вимоги інформаційної безпеки, зазначені в нормативних актах, рекомендаціях установ банківського нагляду, внутрішньо-нормативних документах Банку, нормах і стандартах безпеки, а також вимог, що випливають з укладених договорів. Джерела цих вимог були виокремлені у вступі до Політики.

### 2. ЦІЛІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

2.1. Реалізовані Банком принципи, що впливають з Системи Управління Інформаційною Безпекою, повинні забезпечити досягнення наступних цілей інформаційної безпеки:

- ✓ **Відповідність до вимог законодавства.** Під час опрацювання інформації Банком, та зокрема організація її захисту, повинно відповідати чинному законодавству України.
- ✓ **Доступність інформації.** Інформація та засоби її опрацювання є доступні для уповноважених осіб. Банк забезпечує прийнятний рівень доступності інформації, враховуючи вимоги законодавства та операційної діяльності Банку.
- ✓ **Конфіденційність інформації.** Інформація є доступною виключно для осіб і процесів, що мають відповідні права доступу до них. Ці права впливають, зокрема, з приналежності інформації (інформація Клієнтів Банку), а також обов'язків і завдань, що виконуються на користь Банку, працівниками та Постачальниками послуг Банку.
- ✓ **Цілісність інформації.** Банк застосовує організаційні та технічні заходи, що забезпечують захист точності та повноти інформації, та захист коректної роботи механізмів, що опрацьовують інформацію. Зокрема, інформація захищена від несанкціонованої зміни.
- ✓ **Спостережність.** Забезпечення можливості встановлення визначення користувачів і процесів, а також фіксації дій користувачів і процесів над цією інформацією з метою запобігання та/або розслідування порушень політики безпеки.
- ✓ **Застосування принципів захищеної обробки інформації.** Обробка інформації та експлуатація засобів її обробки відбувається, відповідно до визначених принципів. Принципи, які є діючими для зовнішніх суб'єктів господарювання, виконуються на підставі договорів, укладених з Банком.

- ✓ **Нагляд за захистом інформації.** Банк контролює, чи спосіб обробки інформації відповідає вимогам щодо захисту інформації. У випадку підтвердження невідповідності, своєчасно приймаються заходи щодо їх виправлення.
- ✓ **Адекватний захист інформації і засобів її обробки щодо рівня ризику.** Підбір засобів захисту впливає з управління інформаційним ризиком в Банку. Такий підхід робить можливим забезпечення ефективності інформаційних процесів.
- ✓ **Адекватна оптимізація засобів захисту відповідно до поточних потреб Банку.** Шляхом управління ризиком, аудиту, перегляду та вимірювання ефективності, Банк визначає чи організаційні та технічні засоби захисту є оптимальними на вимоги безпеки та операційної діяльності Банку.
- ✓ **Забезпечення швидкої та ефективної реакції на порушення інформаційної безпеки.** Банк оперативно реагує на будь-які ознаки порушення інформаційної безпеки/кібербезпеки, що забезпечує мінімізацію ймовірних негативних наслідків події та прийняття негайних коригувальних дій.

### 3. ОСНОВНІ ПРИНЦИПИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

2.2. Організація інформаційної безпеки Банку базується на таких фундаментальних принципах :

- ✓ **Принцип мінімальності повноважень:** доступ працівників Банку та користувачів інформаційних систем до інформаційних ресурсів обчислювальної мережі Банку повинен бути організований таким чином, щоб надавати тільки ті повноваження, які необхідні для виконання службових завдань.
- ✓ **Принцип необхідних знань:** кожен працівник або особа, що співпрацює з Банком, володіє лише тією інформацією про інформаційні ресурси Банку, засоби їх обробки та способи їх захисту, яка є необхідною для виконання поставлених завдань та обов'язків. Сторонні особи мають доступ виключно до тієї інформації, яку Банк визначив як публічну (відкрити).
- ✓ **Принцип розподілу обов'язків:** виконання завдань, що є критичними з точки зору безпеки фінансових та інформаційних ресурсів Банку, інформаційно-телекомунікаційних систем та банківських послуг організовуються таким чином, щоб їх реалізація вимагала участі більше, ніж однієї особи («правило двох рук»).
- ✓ **Принцип санкціонування дій:** ті дії працівників Банку, які явно не дозволені законодавством, нормативними документами НБУ, внутрішніми розпорядчими або нормативними документами, є забороненими.
- ✓ **Принцип законності:** СУБ Банку враховує вимоги чинного законодавства України, а також вимоги міжнародних нормативних вимог в галузі інформаційної безпеки.
- ✓ **Принцип узгодженості та єдності:** цілі і завдання інформаційної безпеки відповідають стратегічним цілям та бізнес-завданням Банку, а управління інформаційною безпекою є невід'ємною частиною управління Банком.
- ✓ **Принцип адекватності і ефективності:** засоби захисту інформаційних ресурсів впроваджуються відповідно до їх критичності, тобто категорії класифікації та рівня ризику інформаційного ресурсу, ґрунтуючись на засадах оцінки ризику, прийнятого Банком.
- ✓ **Принцип практичності:** засоби захисту інформаційних ресурсів повинні бути практичними та підтримувати баланс між працездатністю та захищеністю інформаційних систем.

- ✓ **Принцип безперервності:** інформаційна безпека є безперервним процесом протистояння загрозам/кіберзагрозам та управління ризиками, характерними для сфери діяльності Банку.
- ✓ **Принцип відповідальності:** керівництво Банку всіх рівнів, працівники, постачальники та інші треті сторони, які мають доступ до інформаційних ресурсів Банку, повинні дотримуватися вимог внутрішніх документів Банку в області інформаційної безпеки та несуть персональну відповідальність за їх виконання.
- ✓ **Принцип постійного вдосконалення:** впроваджена у Банку Система управління інформаційною безпекою містить механізми та показники для вимірювання і контролю ефективності системи управління та впроваджених заходів для раціонального планування і реалізації дій для вдосконалення.
- ✓ **Принцип багаторівневого захисту:** організація інформаційної безпеки передбачає створення наступного ряду послідовних рівнів захисту інформаційних ресурсів та персоналу Банку від ймовірних загроз/кіберзагроз:
  - організаційно-правовий рівень, який визначає правові та нормативні вимоги та зобов'язання персоналу, користувачів інформаційних ресурсів та контрагентів Банку щодо інформаційної безпеки;
  - фізичний рівень захисту, який запобігає неавторизованому фізичному доступу, ушкодженню чи вторгненню до службових приміщень Банку з метою несанкціонованого доступу до інформації;
  - рівень прикладного програмного забезпечення, який відповідає за взаємодію з користувачем інформаційних ресурсів;
  - рівень системи управління базами даних, який відповідає за зберігання та опрацювання даних;
  - рівень операційної системи, який відповідає за безпечне та надійне обслуговування прикладного програмного забезпечення та систем управління базами даних;
  - рівень мережі, який відповідає за взаємодію вузлів інформаційної системи Банку.
- ✓ **Принцип комплексності і системності:** інформаційна безпека Банку будується комплексно, враховуючи всі аспекти захисту інформації, зокрема:
  - стратегії та цілі безпеки,
  - управління інформаційними ресурсами та носіями інформації,
  - безпека людських ресурсів,
  - управління фізичною безпекою та безпекою навколишнього середовища,
  - безпека відносин з Постачальниками,
  - безпека процесів внутрішніх та зовнішніх комунікацій,
  - управління відповідністю до правових, нормативних та договірних вимог,
  - управління інцидентами безпеки інформації,
  - управління безперервністю бізнесу,
  - безпека у процесах проектування, пошуку, розвитку, впровадження та підтримки ІТ систем,
  - безпека у процесах експлуатації ІТ систем
  - 100% виявлення ризику змін систем на безперервність та цілісність їх функціонування.

Прийнята Банком системність підходу до управління інформаційною безпекою, передбачає забезпечення узгодженості процесів та дій здійснених в області безпеки:

- з умовами середовища, у якому функціонує Банк,
- зі стратегією та бізнес-цілями Банку,
- з результатами оцінки ризиків та можливостей,
- з результатами оцінки ефективності системи управління та впровадження засобів захисту,
- зі всіма аспектами управління операційною діяльністю та інформаційними технологіями Банку.

2.3. Кожен працівник або особа, що співпрацює з Банком зобов'язаний сприяти діяльності щодо досягнення та підтримання відповідного рівня інформаційної безпеки в Банку в обсязі, що відповідає його службовим обов'язкам та наданим повноваженням.

2.4. Кожен працівник або особа, що співпрацює з Банком, зобов'язаний повідомляти про виникнення інциденту, пов'язаного з інформаційною безпекою.

2.5. Банк вимагає від Постачальників знань та дотримання вимог з інформаційної безпеки, зокрема, в договірних відносинах регулювати питання у сфері захисту активів Банку та гарантувати, що одержаний ним доступ до активів Банку буде використано виключно з метою надання послуг за окремим договором, укладеним між Банком та цим Постачальником, та Постачальник не чинитиме будь-яких спроб на доступ до таких активів або втручання в них у строки, формі, спосіб, що не визначено письмовими договірними відносинами між сторонами. Постачальник зобов'язаний надати перелік власних працівників, що допущені до надання послуг Банку та забезпечити виконання ними вимог з інформаційної безпеки. Після закінчення надання послуг Банку, Постачальник повинен знищити будь-яку інформацію, що має ознаки інформації з обмеженим доступом, не створювати та не зберігати будь-яку інформацію щодо функціонування інформаційних активів Банку, крім загальновідомої.

2.6. У Банку розроблено, діє, тестується та оновлюється план забезпечення безперервної діяльності, у якому враховано безперервність функціонування заходів інформаційної безпеки в рамках процесу управління безперервністю діяльності Банку, заходи відновлення інформаційних систем після збоїв.