ЗАТВЕРДЖЕНО
Рішенням Наглядової Ради
№40/2024 від 22.03.2024р.
Вводиться в дію з 22.03.2024р.
Схвалено Рішенням Правління
№229 від 04.03.2024р.
Нова редакція!

Вимоги Політики інформаційної безпеки в АКЦІОНЕРНОМУ ТОВАРИСТВІ «КРЕДОБАНК»

З метою забезпечення максимально можливого рівня безпеки банківських послуг та продуктів, що надаються Клієнтам Банку, а також внутрішніх процесів, інфраструктури, ІСТ та інформації, що в них обробляється, в Банку впроваджено Систему Управління Інформаційною Безпекою (СУІБ), з врахуванням вимог:
- нормативно-правових актів Національного Банку України;
- стандартів ДСТУ ISO/IEC 27001:2023 (ISO/IEC 27001:2022, IDT) Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги; ДСТУ ISO/IEC 27002:2023 (ISO/IEC 27002:2022, IDT) Інформаційна безпека, кібербезпека та захист конфіденційності. Засоби контролювання інформаційної безпеки;
- вимог, передбачених діючим законодавством та внутрішніми нормативними документами АКЦІОНЕРНОГО ТОВАРИСТВА «КРЕДОБАНК» (далі - Банк);
- вимог карткових організацій та платіжних систем, учасником, яких є Банк;
- міжнародних стандартів з питань інформаційної безпеки, кібербезпеки та безпеки інформації у хмарних середовищах, загальноприйнятих у міжнародній практиці принципів забезпечення інформаційної безпеки і кіберзахисту;
- вимог, що випливають з укладених договорів.

Шляхом впровадження, підтримання та розвитку СУІБ, Банк зобов'язується виконувати вимоги інформаційної безпеки та постійно вдосконалювати СУІБ.

1. Правління Банку усвідомлює, що теперішня та майбутня позиція Банку на фінансовому ринку залежить від:
- швидкості, ефективності та точності ідентифікації загроз\кіберзагроз та сприятливих умов для діяльності Банку;
- оцінки ймовірності їх виникнення;
- оцінки їх впливу на безперервність, якість та відповідність законодавству бізнес-процесів Банку, а також впливу на ринкову позицію та імідж Банку;
- ефективності вибору та впровадження відповідних заходів запобігання загрозам\кіберзагрозам чи зменшення їх негативних наслідків;
- точності вибору та впровадження рішень, що збільшують ймовірність використання можливостей;
- глибокої цифрової трансформації у всіх аспектах діяльності, сміливих змін операційної моделі та моделі дистрибуції;
- диверсифікації та дисципліни в сфері управління ризиками та кібербезпеки, стійкості до ринкових потрясінь.
2. З огляду на те, що характер загроз у банківській діяльності змінюється в напрямку кіберзагроз, Правління Банку, особливу увагу приділяє забезпеченню інформаційної безпеки та кіберзахисту ІСТ Банку та даних, що в ній обробляються, а також розуміє необхідність прийняття цілісного, системного підходу до управління інформаційною безпекою в Банку.
3. Функціонування системи кіберзахисту ґрунтується на принципах:
   1) пропорційності та адекватності заходів кіберзахисту, що впроваджуються, реальним та потенційним кіберзагрозам;
   2) пріоритетності запобіжних заходів;
   3) мінімізації кіберризиків у діяльності банку;

4) дотримання вимог нормативно-правових актів Національного банку з питань інформаційної безпеки та кіберзахисту, рекомендацій Національного банку, уключаючи такі, що можуть бути надані Національним банком за результатами контролю;

5) постійної підтримки з боку Правління Банку кіберстійкості банку шляхом організації ефективного управління кіберризиками.

4. Цілі інформаційної безпеки

Реалізовані Банком принципи, що випливають 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 випливають, 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 випливає 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\кібербезпеки, що забезпечує мінімізацію ймовірних негативних наслідків події та прийняття негайних коригувальних дій.

5. Основні принципи забезпечення інформаційної безпеки

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 (відкриту).

– **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:** СУІБ 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 забезпечень 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 інформаційної безпеки,
- 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.

6. Програмне забезпечення Банку повинно відповідати вимогам з інформаційної безпеки законодавства України, документів та стандартів НБУ, а також міжнародних стандартів ISO 2700X і відповідати наступним вимогам:

- наявність вбудованої системи захисту інформації, яку не можна відключити і неможливо здійснити опрацювання інформації без її використання;
- наявність вбудованих механізмів належного захисту інформації під час її передавання між різними підсистемами, у яких обробляється інформація;
- для автоматизованих систем, які функціонують у режимі "клієнт-сервер", доступ користувачів до бази даних має відбуватися лише через додаткове програмне забезпечення, за допомогою якого здійснюється аутентифікація та авторизація осіб, яким дозволено користуватися цією базою даних;
- застосування посиленої автентифікації користувача платіжної послуги;
- наявність вбудованих механізмів, що забезпечують однозначну та незаперечну ідентифікацію користувача на кожному пристрої доступу до системи, в кожному модулі або елементі системи, до якого користувач має доступ, а також під час здійснення будь-яких операцій у системі;
- забезпечення можливості автоматичного блокування облікового запису в системі після перевищення кількості дозволених невдалих спроб введення паролю на будь-якому пристрої доступу до системи забезпечення безперервного технологічного контролю за цілісністю інформації та накладання/перевіряння цифрового підпису на всіх платіжних банківських документах на кожному етапі технологічного циклу їх опрацювання; забезпечення шифрування електронних банківських документів, що містять конфіденційну інформацію, під час передавання на зовнішніх носіях або відповідними каналами зв'язку в режимі on-line з відповідним підтвердженням про їх отримання забезпечити обов’язкову реєстрацію всіх спроб доступу, всіх операцій та інших дій в системі, а також записування їх у автоматизованій системі, у захищеному від модифікації електронному реєстрі, з постійним контролем його повноти та цілісності.

7.Вищезазначені вимоги повинні застосовуватись як до готового, придбаного Банком програмного забезпечення (COTS – Commercial Off-The-Shelf), так і програмного забезпечення, розробленого Банком самостійно або зовнішніми постачальниками відповідно до замовлення Банку.

8. Банк використовує стандарти, документи та настанови відкритого проекту захисту додатків "Open web application security project" (OWASP) для розроблення безпечних додатків.

9. Банк підтримує високий рівень безпеки інформації, яка обробляється, зберігається та передається за допомогою хмарних технологій зберігання даних.

10. У Банку діє принцип надання мінімального рівня повноважень під час надання доступу до інформаційних систем банку (включаючи доступ привілейованих користувачів).

11.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.

12.Для зменшення ризиків виникнення інцидентів інформаційної безпеки, у Банку виконуються систематичні дії, з метою підняття рівня обізнаності персоналу щодо інформаційної безпеки, а саме:

- повідомлення працівників Банку про впровадження (нових або змін) внутрішніх нормативних документів, що визначають принципи забезпечення безпеки (зокрема, цієї Політики) та зобов’язання працівників ознайомитись з ними та дотримуватись вимог цих документів;
- проведення тренінгів та навчань для працівників у галузі інформаційної безпеки;
- проведення внутрішніх кампаній та заходів (активностей), зокрема після виникнення серйозного інциденту безпеки та у випадку виявлення інформації щодо нових методів атак на Банки та їх Клієнтів;
- проведення тестів та аудитів безпеки (в тому числі соціотехнічних тестів), тестування планів безперервної діяльності Банку та обговорення їх результатів з відповідальними особами відповідних структурних підрозділів.

13.Кожен працівник Банку зобов’язаний повідомити про виникнення інциденту інформаційної безпеки. Принципи та порядок інформування та контактні дані осіб, що мають бути поінформовані, є визначені у окремому документі, який детально описує процедуру реагування на інциденти інформаційної безпеки.

14.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.

15.Всі працівники Банку при вступі на роботу підписують зобов'язання про нерозголошення інформації з обмеженим доступом, в тому числі банківської таємниці та персональних даних. Працівники Банку зобов'язані не розголошувати та не використовувати з вигодою для себе чи для третіх осіб інформацію з обмеженим доступом, яка стала відома їм при виконанні своїх службових обов'язків.