ЗАТВЕРДЖЕНО
Рішенням наглядової ради
АТ «Полтава-банк»
(протокол засідання наглядової ради
№ 39 від 23.06.2020 року)
Голова наглядової ради
АТ «Полтава-банк»

_____О.В. Некрасов

«23» червня 2020 року

ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ
АТ «Полтава-банк»
(нова редакція)

2020

Вступ

Діяльність та розвиток АТ «Полтава-банк» (далі - Банк) вимагає використання розподіленого бізнес-середовища для обміну інформацією, використання послуг сторонніх компаній і багато в чому покладається на інформаційні технології, які включають в себе різні рівні загроз і вразливостей.

Широке використання інформаційних систем і зовнішніх мереж, швидкі зміни в технологіях, випадки комп'ютерного шахрайства, крадіжки інформації, промислове шпигунство, саботаж, злом, пожежа і необережне поводження з інформацією становлять значний ризик інформаційної безпеки на всіх етапах її обробки.

Правління підкреслює важливість і необхідність у використанні та впровадженні заходів безпеки та заявляє про свою повну підтримку в побудові інформаційної безпеки в Банку і в роботі з корпоративними та іншими сторонами.

Інформаційну безпеку можна забезпечити шляхом проведення окремих відповідних технічних заходів, які можуть підтримуватися менеджментом відповідним чином, на основі відповідних бізнес-процесів і процедур.

Банк визначає політику Інформаційної безпеки як засіб збереження конфіденційності, цілісності та доступності інформації та інформаційних систем.

- **Конфіденційність:**
  забезпечення того, щоб інформація була доступна тільки тим особам, які мають повноваження для розгляду інформації;
- **Цілісність:**
  забезпечення точності, повноти та своєчасності інформації та методів обробки;
- **Доступність:**
  забезпечення того, щоб уповноважені користувачі мали доступ до інформації і пов'язаних з ними активів в строк і в разі потреби.

Конфіденційність, цілісність і доступність є основними принципами підтримки конкурентоспроможності, юридичної відповідності та відповідності іміджу.

Політика інформаційної безпеки АТ «Полтава-банк» розроблена у відповідності до: Закону України «Про інформацію», Закону України «Про банки і банківську діяльність», Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України, затвердженого Постановою Правління Національного банку УКраїни № 95 від 28.09.2017 року, ДСТУ ISO/IEC 27002: 2015 «Методи захисту. Звід практик щодо заходів інформаційної безпеки (ISO/IEC 27002:2013; Cor 1:2014, IDT), ДСТУ ISO/IEC 27001: 2015 «Методи захисту. Система управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT), Правил з технічного захисту інформації для приміщень банків, у яких обробляються електронні банківські документи Постанови Правління

Національного банку України, затверджених Постановою Правління Національного банку України №243 від 04.07.2007 року.

1. Основні терміни та скорочення

У цьому документі застосовано такі терміни та скорочення:

Інформаційний актив - це сукупність відомостей (інформації), що представляє цінність для компанії та / або її клієнтів, ділових партнерів і співробітників, а також будь-яка система обробки, обміну або фізичного місця зберігання інформації.

Інформаційна безпека - це сукупність організаційно-технічних заходів і засобів, спрямованих на захист інформації від загроз з метою забезпечення безперервності бізнес-процесів, зниження бізнес ризиків і оптимізації витрат.

Інформаційний інцидент - подія або послідовність подій, які ставлять під загрозу конфіденційність, цілісність і доступність інформаційних активів.

Заходи захисту - сукупність організаційних та / або технічних дій, спрямованих на управління ризиком.

Доступність - властивість інформації або інформаційного активу, яка визначає можливість її / його використання за призначенням в необхідний момент часу.

Конфіденційність - властивість інформації (або інформаційного активу), яке полягає в тому, що доступ до неї не може бути отриманий неавторизованим особою, об'єктом і / або процесом, внаслідок правових обмежень, накладених її власником.

Цілісність - властивість інформації (або інформаційного активу), яке полягає у неможливості її модифікації несанкціоновано, без дозволу її власника.

Ризик - це ймовірність шкідливого впливу на бізнес в результаті порушення конфіденційності, цілісності та доступності інформації.

Вразливість - брак або пролом в системі безпеки, які збільшують імовірність здійснення загрози порушення конфіденційності, цілісності та доступності інформації.

Загроза - спосіб, за допомогою якого може бути порушено конфіденційність, цілісність і доступність інформації.

Аналіз загроз - це процес вивчення джерел загроз по вразливостей в системі, щоб визначити загрози для конкретної системи в конкретній оперативній обстановці.

Управління ризиками - це процес, метою якого є зменшити ризики до прийнятного рівня, визначивши заходи захисту та мінімізувавши вплив від невизначених подій.

Аналіз інформаційних ризиків - процес оцінки потенційного впливу реалізації загроз на бізнес, визначення загроз і вразливостей і вибір відповідних контрзаходів.

Зниження ризиків - процес проведення заходів з безпеки для зменшення виявлених ризиків до прийнятного рівня.

Вплив на бізнес - це рейтинг шкоди, який свідчить про характер і рівень шкоди, заподіяної компанії в результаті порушення конфіденційності, цілісності та доступності інформації.
Керівництво - документ, який вказує що треба зробити і як для того, щоб досягти цілей поставлених політикою.
Політика - документ, що визначає загальні принципи та напрям, визначені керівництвом компанії.
Третя сторона - особа або організація, які вважаються незалежними від задіяних сторін, у випадках виникнення будь-яких питань.
У цьому Документі застосовано такі познаки та скорочення:
ІС - інформаційна система.
ІБ - інформаційна безпека.
СУІБ - Система управління інформаційною безпекою.
ПЗ – програмне забезпечення.

2. Ціль політики

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

3. Сфера застосування

Політика Інформаційної безпеки застосовується щодо всіх організаційних одиниць Банку. Політика інформаційної безпеки стосується ділових партнерів, постачальників і провайдерів послуг, при використанні інформаційних активів (ресурсів СУІБ), Банку.

4. Предмет політики

Стратегія Банку полягає у підвищенні інтеграційних процесів між відділеннями і системами. Завдяки інтеграції та швидкому розвитку бізнес-середовища зростає потреба в захисті інформаційних активів.

Банк ставить за мету створення гнучкої структури, в якій інформаційна безпека є одним з основних принципів ведення бізнесу (основних видів діяльності) та корпоративної поведінки. Для побудови такої структури, окрім впровадження основних заходів безпеки, необхідно розробляти відповідні бізнес-процеси та проводити навчання персоналу.

Міжнародні стандарти ДСТУ ISO/IEC 27002: 2015 «Методи захисту . Звід практик щодо заходів інформаційної безпеки (ISO/IEC 27002:2013; Cor 1:2014, IDT), ДСТУ ISO/IEC 27001: 2015 «Методи захисту. Система

управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT),є керівництвом для впровадження Системи управління інформаційною безпекою в Банку.

Політика інформаційної безпеки визначає план дій і є основним керуючим документом з управління інформаційною безпекою в Банку.

Також Політика інформаційної безпеки забезпечує підтримку інформаційної безпеки відповідно до вимог бізнесу та відповідних законів України.

4.1. Організація інформаційної безпеки

Правління Банку зобов'язується підтримувати систему управління інформаційною безпекою, визначати та розподіляти відповідні функції та обов'язки управління, обговорювати і затверджувати питання, що стосуються інформаційної безпеки.

Для координації питань інформаційної безпеки в Банку має бути затверджене Положення про Систему управління інформаційною безпекою.

4.2. Управління ризиками

Банк повинен визначати, оцінювати та визначати пріоритети щодо загроз інформаційних ризиків.

Політика інформаційної безпеки з метою управління інформаційними ризиками повинна ґрунтуватися більшою мірою на основі ризик-орієнтованого підходу для попередження, виявлення та усунення загроз, а не на обмеженнях і забороні.

Застосування заходів захисту повинно бути обґрунтовано на основі процесу аналізу інформаційних ризиків, пов'язаних з інформаційними активами (ресурсами СУІБ) і бізнес процесами Банку.

Для визначення рівнів ризику і зменшення його до прийнятного рівня має проводитися процес аналізу інформаційних ризиків на періодичній основі.

4.3. Управління інформаційними активами

Банк повинен забезпечувати і підтримувати належний захист інформаційних активів Банку за допомогою заходів, що включають інвентаризацію інформаційних активів, призначення власників інформаційних активів, належну класифікацію та маркування інформації, що обробляється в цих активах.

4.4. Безпека людських ресурсів

4.4.1. Ролі та обов'язки, пов'язані з інформаційною безпекою

Банк повинен визначити і документально забезпечити ролі і обов'язки співробітників Банку, підрядників і користувачів третьої сторони в їх посадових інструкціях або договорах, включаючи оцінку критичності інформаційних активів та інформування про інциденти.

Визначення відповідальностей співробітників за інформаційну безпеку має бути визначено по можливості на основі принципу поділу обов'язків для того, щоб запобігти залежності від однієї особи, а також запобігти неправильному використанню або зловживанню інформаційними активами та системами Банку

4.4.2. Скринінг (Перевірка)

Всі співробітники Банку при прийнятті на роботу, яка вимагає права привілейованого доступу до критично важливих систем або процесів, а також конфіденційних даних Банку, повинні пройти процес скринінгу, на скільки це дозволяє законодавство України. (Це включає в себе також тимчасових співробітників і третіх осіб, які запрошуються для співпраці).

4.4.3. Підвищення обізнаності користувачів

Всі співробітники Банку та у відповідних випадках, підрядники та користувачі третьої сторони, повинні отримати відповідну підготовку з питань безпеки, тренінги, навчання і регулярні оновлення в організаційних політиках і процедурах, залежно від функціональних обов'язків.

4.4.4. Дисциплінарний процес

В Банку повинен бути визначений чіткий дисциплінарний процес.

4.5. Фізична безпека та безпека навколишнього середовища

Для запобігання несанкціонованого фізичного доступу, пошкодження та втручання в приміщення організації та інформації, Банк вживає відповідних заходів безпеки відповідно до рівня класифікації інформації, яка зберігається і оброблятися в приміщеннях.

Захист обладнання необхідний для зменшення ризиків несанкціонованого доступу до інформації та захисту інформаційних активів від втрати або пошкодження.

4.6. Управління комунікаціями

Банк повинен створити необхідні процедури для безпечного і правильного використання систем обробки інформації та забезпечити запобігання порушень роботи об'єктів обробки інформації.

Повинен бути забезпечений захист комп'ютерних мереж, що належать Банку, а також забезпечене резервне копіювання інформації для підвищення її доступності.

Повинна бути впроваджена система моніторингу інформаційної безпеки для виявлення несанкціонованих дій, також журнали подій повинні бути належним чином зібрані й захищені для розслідування інцидентів інформаційної безпеки.

Банк повинен забезпечити заходи виявлення, профілактики та відновлення для захисту від шкідливого коду, а також запровадити відповідні процедури обізнаності користувачів.

Політика допустимого використання інформаційних активів повинна включати рекомендації та список заходів захисту для прийнятного використання Інтернету, електронної пошти та аналогічних послуг і ресурсів в рамках Банку.

4.7. Управління доступом

Банк використовує як логічний, так і фізичний контроль доступу, де обробляється і зберігається інформація. Права доступу, включаючи мережеві ресурси, повинні бути призначені відповідно до принципу «need-to-know»'(необхідно знати), і ці права повинні періодично переглядатися.

Всі користувачі повинні бути інформовані і навчені для запобігання несанкціонованого доступу та витоку інформації.

Доступ третіх сторін до систем Банку, а також віддалена робота співробітників, повинні бути обмеженими і контрольованими.

4.8. Придбання, розробка і використання інформаційних систем

Банк повинен розглянути питання про визначення вимог безпеки на етапі розробки або придбання програмного забезпечення, а також встановити критерії встановлення системи у робоче середовище для нових інформаційних систем і програмного забезпечення.

Банк повинен підтримувати безпеку при застосуванні системного програмного забезпечення та інформації. Проект і підтримка середовища (тестування, розробка та виробництво) повинні суворо контролюватися. Процеси управління змінами та управління конфігураціями повинні використовуватися для введення нових версій і оновлень програмного забезпечення.

Інформація, яка проходить через мережу, повинна бути захищена від шахрайської діяльності, і від будь-якого несанкціонованого доступу або модифікації.

4.9. Управління інцидентами

Банк повинен визначити Політику управління інцидентами інформаційної безпеки для ефективного реагування на інциденти, а також визначити для всіх співробітників порядок повідомлення про інциденти та вразливості. Інциденти повинні реєструватися і оброблятися.

4.10. Управління безперервністю бізнесу

Банк повинен створювати Політику забезпечення безперервності бізнес-процесів Банку.

Ця політика повинна визначати план, який в свою чергу, забезпечує належний захист і відновлення критично важливих бізнес-процесів Банку. Цей план повинен періодично тестуватися та утримуватися відповідно до змін.

4.11 Відповідність вимогам (Compliance)

Банк повинні відповідати всім законодавчим, нормативним, договірним вимогам і мати організаційні підходи до задоволення вимог.

Всі працівники Банку повинні діяти згідно з відповідними законами, положеннями, правами інтелектуальної власності, ліцензійними угодами, а також політиками і процедурами, які застосовуються в Банку. Вони повинні також нести відповідальність за захист інформації Банку відповідно до рівнів конфіденційності.

5. Ролі та відповідальності

Дотримання, а також забезпечення своєчасної реалізації Політики інформаційної безпеки є обов'язком всіх співробітників Банку.

Недисципліновані вчинки, які є результатом грубої недбалості, класифікуються як серйозні інциденти в області безпеки. Наступні категорії визначаються як серйозні порушення, якщо вони підпадають під одну або більше таких категорій:

- Якщо поведінка або дія стосується використання корпоративної інформації та активів у протиправних цілях;
- Якщо поведінка або дія стосується несанкціонованого доступу до інформації;
- Якщо поведінка або дія стосується несанкціонованої модифікації інформації;
- Якщо поведінка або дія завдає шкоди репутації Банку;
- Якщо поведінка або дія завдає шкоди людям, а Банк буде схильний до ризику;
- Якщо поведінка або дія завдає реальний чи потенційний збиток Банку або якщо буде знижена можливість збереження даних і ділової інформації, щоб представлятиме ризик.

Порушення цієї політики інформаційної безпеки може призвести до таких

заходів, але не обмежуватися ними:

- Дисциплінарні заходи, аж до припинення трудових або службових угод;
- Заходи за трудовим і / або цивільного законодавства;
- Відшкодування збитків.

Будь-яку інформацію про порушення безпеки слід негайно повідомляти в управління інформаційної безпеки Банку.

Правління Банку відповідає за управління інформаційними ризиками в Банку, за актуалізацію, впровадження та моніторинг Політики інформаційної безпеки.

6. Перегляд Політики

Політика переглядається за необхідністю, але не менш ніж одного разу на рік. Причинами внесення змін до Політики є зміни в інформаційної інфраструктурі та/або впровадженні нових інформаційних технологій, а також змінах в законодавчих, регуляторних та інших нормах.

Голова правління АТ «Полтава-банк» В.С. Переверзев

Начальник управління інформаційної
Безпеки АТ «Полтава-банк» Т.А. Бондар

Начальник юридичного відділу
АТ «Полтава-банк» О.М. Каспір

Начальник відділу комплаєнс
АТ «Полтава-банк» А.А. Комеліна