АТ «ЮНЕКС БАНК»
вул. Васильківська, буд. 14, м. Київ, 03040, Україна
Ліцензія НБУ №56 від 28 жовтня 2011 р.
0 800 3 111 33 | www.unexbank.ua

Unex Bank

Політика інформаційної безпеки АТ «ЮНЕКС БАНК» (версія 4.0)

1. Загальні положення

1.1.Політика інформаційної безпеки описує та регламентує функціонування системи управління інформаційною безпекою відповідно до вимог:

- стандарту України з питань інформаційної безпеки ДСТУ ISO/IEC 27001:2015 “Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги”;
- стандарту України з питань інформаційної безпеки ДСТУ ISO/IEC 27002:2015 “Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки”;
- постанови Правління Національного банку України №95 від 28.09.2017 «Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України»;
- Методичних рекомендацій щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків відповідно до стандартів Національного банку України, визначених листом Національного банку України від 01.03.2011 N 24-112/365;
- інших законодавчих та нормативно-правових актів України, а також внутрішніх нормативних документів Банку, а також міжнародних та внутрідержавних платіжних систем та систем переказу коштів (визначених Додатком 1 до цієї Політики).

1.2.Політика інформаційної безпеки стоїть на верхньому рівні ієрархії усіх інших нормативних документів, вимог, правил та інструкцій, які стосуються питань інформаційної безпеки Банку.

2. Визначення та скорочення

Банк - АТ «ЮНЕКС БАНК».

Бізнес-процес – структурована послідовність дій з виконання певного виду діяльності на всіх етапах життєвого циклу банківської діяльності, метою якої є отримання результату, що має цінність для Банку.

Загроза – потенційна причина інциденту інформаційної безпеки, яка може призвести до шкоди для системи або організації.

Інцидент інформаційної безпеки (інцидент ІБ) – це поява одного або декількох небажаних або несподіваних подій інформаційної безпеки, які пов’язані з настанням або значною вірогідністю настання негативних наслідків для інформаційної безпеки, інформації, інформаційних активів, бізнес-процесів або завдати шкоди Банку та системі захисту.

Інформаційна безпека (ІБ) – сукупність процесів та заходів, які мають на

меті збереження цілісності, конфіденційності, та доступності інформації.

Інформація з обмеженим доступом (ІзОД) – це відомості, які становлять банківську таємницю, комерційну таємницю, персональні дані та іншу конфіденційну інформацію Банку.

Політика інформаційної безпеки (політика) – сукупність правил, обмежень і рекомендацій, прийнятих керівництвом банку, які спрямовані на захист інформації від внутрішніх та зовнішніх загроз.

Система управління інформаційною безпекою (СУІБ) – комплекс організаційних, програмних, технічних і фізичних заходів, спрямованих на управління ризиками, що пов'язані з використанням у Банку інформації та інформаційних технологій.

CISO – (Chief information security officer) відповідальна особа за інформаційну

безпеку банку яка має повноваження, достатні для прийняття управлінських рішень

3. Цілі інформаційної безпеки АТ «ЮНЕКС БАНК»

3.1. Цілі інформаційної безпеки АТ «ЮНЕКС БАНК» (надалі – Банк) є складовою частиною загальних цілей Банку, визначених Стратегією та бізнес-планом розвитку Банку. Зокрема, безпосередньою ціллю інформаційної безпеки є впровадження та ефективне функціонування системи управління інформаційної безпеки, високий рівень розвитку якої дозволить:

- забезпечувати надійний захист інформаційних ресурсів Банку від зовнішніх і внутрішніх загроз, пов'язаних з навмисними або ненавмисними діями працівників банку та сторонніх осіб;
- забезпечувати надійність бізнес-процесів, банківських продуктів, програмно-технічних комплексів;
- сприяти мінімізації ризиків операційної діяльності Банку;
- попереджувати та мінімізувати ризики інформаційної безпеки, впроваджувати необхідні заходи для запобігання виникненню інцидентів;
- забезпечувати процесний підхід до діяльності Банку;
- впроваджувати ризик-орієнтований підхід до забезпечення інформаційної безпеки Банку;
- забезпечувати безперервну роботу Банку;
- забезпечувати позитивну репутацію Банку при роботі з клієнтами, партнерами для підтримання довірчих відносин та конкурентного іміджу Банку.

4. Сфера застосування

4.1.Сфера застосування інформаційної безпеки розповсюджується на функціонування всіх критичних бізнес-процесів Банку на всіх етапах їх життєвого циклу.

4.2.Вимоги інформаційної безпеки застосовуються в процесі проектування, тестування та експлуатування програмно-технічних комплексів.

4.3.Дотримання цієї Політики є обов'язковим для всіх співробітників Банку (як постійних, так і тимчасових).

4.4.У договорах з третіми сторонами, які отримують доступ до інформації Банку, повинно бути визначено зобов'язання третьої сторони щодо дотримання вимог цієї Політики.

5. Предмет інформаційної безпеки

5.1.Загальні принципи

5.1.1. **Комплексність та системність.** Діяльність із забезпечення інформаційної безпеки суворо і всебічно регламентується. Формування політики, як сукупності норм, вимог, положень та інструкцій, здійснюється на підставі системного методологічно обґрунтованого підходу і враховує усі найбільш слабкі та вразливі місця інформаційних систем.

5.1.2. **Забезпечення цілісності, конфіденційності, доступності та спостережності інформації.** Банк забезпечує цілісність і доступність інформації, що обробляється, зберігається, в системах та комп'ютерних мережах банку. Банк здійснює захист інформації з обмеженим доступом, яка відноситься до «банківської таємниці», «комерційної таємниці» та іншої конфіденційної інформації від несанкціонованого розповсюдження, використання і порушення її конфіденційності (таємності).

5.1.3. **Пріоритетність цілей.** Інформаційна безпека повинна впроваджуватись у відповідності цілей, Стратегії та бізнес-плану розвитку Банку.

5.1.4. **Ефективність.** Банк підтримує ризик-орієнтовний підхід, який забезпечує розуміння, моніторинг та зменшення ризиків операційної діяльності. Прийняття рішення щодо застосування заходів захисту повинно бути обґрунтовано процесом аналізу інформаційних ризиків, пов'язаних з ресурсами СУІБ і бізнес процесами Банку. Деталі ризик-орієнтовного підходу описані в Політиці управління інформаційною безпекою.

5.1.5. **Безперервність.** Безперервність процесу удосконалення та розвитку інформаційної безпеки, адаптація до нових інформаційних систем та рішень із застосуванням міжнародного досвіду.

5.1.6. **Адекватність заходів захисту.** Своєчасність та адекватність заходів захисту від реальних та потенційних загроз інформаційній безпеці.

5.1.7. **Мінімізація повноважень.** Надання користувачам мінімальних прав доступу до бізнес-процесів та інформаційних систем, відповідно до службових обов'язків, визначених посадовими інструкціями та іншими внутрішніми нормативними документами Банку.

5.1.8. **Взаємодія з керівництвом.** Підтримка та контроль за впровадженням, функціонуванням та розвитком СУІБ з боку Наглядової Ради та Правління Банку.

5.1.9. **Дотримання національних та міжнародних стандартів у сфері інформаційної безпеки.** Публічні сервіси банку та внутрішні мережі банку

повинні відповідати вимогам стандартів України та нормативних документів Національного банку України 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.

5.2.Обізнаність (компетентність) з питань інформаційної безпеки

5.2.1. Наглядова Рада Банку та Правління Банку усвідомлюють, що інформаційна безпека є важливою складовою життєдіяльності Банку і надають свою повну підтримку впровадженню СУІБ в Банку.

5.2.2. Керівники та працівники Банку всіляко підтримують та виконують принципи інформаційної безпеки завдяки своїй високій компетенції з питань інформаційної безпеки.

5.2.3. Кожний працівник задіяний у питаннях інформаційної безпеки у рамках своєї компетенції та відповідальності за напрямком діяльності.

5.2.4. Передумовою досягнення належної відповідності стандартам інформаційної безпеки є інформованість працівників з питань вимог та принципів інформаційної безпеки з боку керівництва, а також проведення тренінгів з питань інформаційної безпеки для працівників.

5.2.5. Банк очікує від усіх працівників високий рівень знань вимог та принципів інформаційної безпеки, які базуються на опублікованих правилах, інших документах та інформації з питань безпеки, а також на тренінгах.

5.2.6. Вразливості та порушення інформаційної безпеки, які виявлено працівниками Банку повинні бути зафіксовані та пройти через процедуру управління інцидентами.

5.3.Правове зобов'язання

5.3.1. Банк зобов'язаний відповідати вимогам Законів, стандартів України та нормативним документам Національного банку України.

5.3.2. З цією метою повинні проводитись Відділом інформаційної безпеки наступні заходи:

- відстеження усіх змін у нормативних актах, що пов'язані з питаннями інформаційної безпеки, проведення оцінки їх впливу на відповідні бізнес-процеси та процедури Банку;
- у разі необхідності вносити Відділом інформаційної безпеки зміни до нормативних документів Банку та виконувати відповідні дії задля приведення Банку у відповідність до актуальних нормативних документів.

5.3.3. Всі працівники і відповідні треті особи, які співпрацюють з Банком, зобов'язані захищати паперову і електронну інформацію від несанкціонованого доступу, використання, модифікації, розкриття інформації, знищення, втрати чи передачі.

5.4.Захист даних

5.4.1. Банк цінує довіру своїх клієнтів та гарантує захист даних усіх клієнтів. Працівники Банку зобов'язуються використовувати інформацію про клієнтів тільки у службових цілях та належно зберігати конфіденційні дані клієнта.

5.4.2. ***Захист активів***

5.4.3. Банк визнає пріоритетним захист матеріальних та нематеріальних активів, а також права своїх клієнтів, працівників та ділових партнерів.

5.4.4. З метою забезпечення захисту інформаційних активів клієнтів, працівників та ділових партнерів в їх спільній діяльності з Банком повинні бути впроваджені Відділом інформаційної безпеки адекватні організаційні та технічні міри та засоби безпеки.

5.4.5. Дані міри та засоби повинні бути сумісними з ризиками, розміром потенційних втрат та імовірністю виникнення даних втрат.

5.4.6. Інтелектуальна власність Банку, а також інтелектуальна власність клієнтів та ділових партнерів, повинна бути захищена.

5.5.Правила та вимоги інформаційної безпеки

5.5.1. Політика інформаційної безпеки є складовою системи управління інформаційною безпекою.

5.5.2. Як невід'ємна частина бізнес-процесів, система управління інформаційною безпекою гарантує, що управління ризиками інформаційної безпеки узаконено, контролюється та постійно адаптується до актуального стану.

5.5.3. Система управління інформаційною безпекою забезпечує безперервну адаптацію Політики, стандартів безпеки, а також розпоряджень та вимог з питань інформаційної безпеки.

5.5.4. Система управління інформаційною безпекою включає усі аспекти інформаційної безпеки, які повинні враховуватись при проектуванні та управлінні важливих процесів Банку.

5.5.5. Банк контролює ефективність впроваджених заходів та засобів забезпечення інформаційної безпеки в інформаційних системах, визначає перелік усіх бізнес-процесів та інформаційних ресурсів, які забезпечують їх функціонування.

5.5.6. Банк здійснює належний захист інформації обмеженого доступу, яка належить до категорій «банківська таємниця», «персональні дані», «комерційна таємниця» та іншу конфіденційну інформацію.

5.5.7. Банк здійснює ефективний моніторинг функціонування СУІБ, реєстрація та опрацювання інцидентів СУІБ.

5.5.8. Банк здійснює прогнозування потенційних загроз і забезпечення готовності до їх виникнення через усунення, навчання фахівців, складання конкретних планів забезпечення безперервної діяльності Банку в разі виникнення надзвичайної ситуації.

5.6.Модель життєвого циклу бізнесу

5.6.1. У Банку всі бізнес-рішення впроваджуються у відповідності до моделі життєвого циклу бізнесу з врахуванням вимог інформаційної безпеки.

5.6.2. Інформаційна безпека, як невід'ємна частина всіх процесів, гарантує, що Банк може забезпечити сервіси високого класу, які мають гарантований рівень безпеки.

5.6.3. Вимоги з інформаційної безпеки застосовуються до усіх етапів життєвого циклу: розробка та впровадження систем та сервісів, придбання ресурсів, оцінка продуктів, операційна діяльність, експлуатація та обслуговування, виведення з експлуатації.

5.7.Управління безперервністю бізнесу

5.7.1. Банк забезпечує безперервність бізнесу.

5.7.2. У Банку діє Робоча група з відновлення діяльності Банку, яка складається з працівників Банку, що призначаються наказом Голови Правління. Робоча група з відновлення діяльності Банку враховує усі можливі переривання у бізнес процесах та організовує дії, що направлені на захист критичних для Банку процесів від наслідків стихійних лих, а також навмисного чи ненавмисного збитку.

5.7.3. Базовими вимогами для управління безперервністю бізнесу є захист людських ресурсів, забезпечення альтернативних середовищ для роботи, збереження інфраструктури, інформаційних технологій і активів та гарантія безпеки збереження даних за межами Банку.

5.7.4. Вимоги управління безперервністю бізнесу повинні постійно контролюватись та адаптуватись.

5.7.5. Кожний партнер Банку, постачальник та підрядчик повинні надавати такі послуги, які гарантують безперервність діяльності Банку в межах наданих послуг.

6. Ролі та відповідальності

6.1.Керівництво Банку забезпечує своєчасний моніторинг та удосконалення системи управління інформаційною безпекою.

6.2.У Банку створений та постійно працює Комітет з управління інформаційною безпекою, відповідальний за планування, впровадження та перегляд СУІБ.

6.3.Політики, положення та інші нормативні документи з питань інформаційної безпеки розробляються Відділом інформаційної безпеки та іншими підрозділами за відповідними напрямками діяльності.

6.4.Постійний контроль впровадження, виконання, вдосконалення та підтримки Політики в актуальному стані покладено на CISO Банку.

6.5.Всі проекти, які пов'язані з інформаційними технологіями, мають узгоджуватись з вимогами Політики.

6.6.Кожен працівник Банку забезпечує підтримку відповідного рівня інформаційної безпеки Банку. В межах своїх службових обов'язків та повноважень працівники повинні виконувати та відповідати за виконання вимог Політики, законодавчих, регуляторних і внутрішньобанківських норм і несуть відповідальність за їх порушення згідно із законодавством України та внутрішньобанківськими нормативними документами.

6.7.Документи, які регламентують інформаційну безпеку, доступні працівникам Банку у межах їх повноважень і призначені надавати допомогу у виконанні вимог інформаційної безпеки.

6.8.Для зменшення ризиків виникнення інцидентів інформаційної безпеки, керівництво Банку створює працівникам умови для систематичного навчання нормам та заходам інформаційної безпеки.

6.9.У Банку складаються, діють, тестуються та оновляються плани забезпечення безперебійного функціонування на випадок непередбачених критичних ситуацій.

7. Прикінцеві положення

7.1.Політика ІБ розміщується на мережевому ресурсі Банку в порядку, визначеному Положенням про порядок ведення внутрішніх документів на порталі АТ «ЮНЕКС БАНК» .

7.2.Політика набирає чинності з дня затвердження її Комітетом з управління інформаційною безпекою Банку.

7.3.Зміни та доповнення до Політики затверджуються Комітетом з управління інформаційною безпекою Банку та оформлюються або змінами до Положення, або викладенням його в новій редакції. Прийняття нової редакції Положення автоматично призводить до припинення дії попереднього документа

7.4. Політика ІБ повинна переглядатися і оновлюватися з періодичністю, що буде забезпечувати її відповідність вимогам законодавства та бізнес-процесам, але не рідше як один раз на рік.

7.5. При перегляді Політики ІБ до уваги повинно братися наступне:

- Ефективність і достатність поточної політики;
- Вартість і вплив на ефективність бізнесу;
- Ідентифікація нових вразливостей;
- Зміни в організаційній структурі;
- Нові бізнес-ініціативи та ринки;
- Інциденти ІБ;
- Зміни в законодавстві.

7.6. Відповідальним за перегляд та актуалізацію даної Політики є керівник Відділу ІБ.

7.7. У разі зміни організаційної структури Банку виконання функцій, визначених цим внутрішнім нормативним актом, здійснюватиметься структурними підрозділами Банку, на які буде покладено вищезазначені функції в порядку, визначеному іншими внутрішніми процедурами Банку

7.8. У випадку змін вимог нормативно-правових актів в частині, що регламентуються цією Політикою, вона вважається чинною в частині вимог, які не суперечать новим вимогам.

7.9. Відповідальність за організацію, забезпечення та контроль виконання вимог Політики покладено на Відділ інформаційної безпеки, який є власником процесу.

7.10. Відповідальність за контроль організації, забезпечення виконання вимог Політики та результату процесу покладається на CISO.

АТ «ЮНЕКС БАНК»
вул. Васильківська, буд. 14, м. Київ, 03040, Україна
Ліцензія НБУ №56 від 28 жовтня 2011 р.
0 800 3 111 33 | www.unexbank.ua

Unex Bank

Додаток 1.

Нормативно-правова база

Закони України:

- «Про Національний банк України» № 679-XIV від 20.05.1999, зі змінами та доповненнями;
- «Про банки і банківську діяльність» № 2121-III від 07.12.2000, зі змінами та доповненнями;
- «Про інформацію» № 2657-XII від 02.10.1992, зі змінами та доповненнями;
- «Про захист персональних даних» № 2297-VI від 01.06.2010, зі змінами та доповненнями;
- «Про захист інформації в інформаційно-телекомунікаційних системах» № 80/94-ВР від 05.07.1994, зі змінами та доповненнями;
- «Про електронні документи та електронний документообіг» № 851-IV від 22.05.2003, зі змінами та доповненнями;
- «Про електронну ідентифікацію та електронні довірчі послуги» № 2155-VIII від 05.10.2017 (зі змінами та доповненнями);
- «Про платіжні послуги» № 1591-IX від 30.06.2021, зі змінами та доповненнями;
- «Про електронні комунікації» № 1089-IX від 16.12.2020, зі змінами та доповненнями;

Постанови Національного банку України:

- «Положення про організацію бухгалтерського обліку, бухгалтерського контролю під час здійснення операційної діяльності в банках України», затвердженого Постановою Правління НБУ № 75 від 04.07.2018;
- «Положення про забезпечення безперервного функціонування інформаційних систем Національного банку та банків України», затвердженого Постановою Правління НБУ № 265 від 17.06.2004;
- «Правил технічного захисту приміщень банків, у яких обробляються електронні банківські документи», затверджених Постановою Правління НБУ № 243 від 04.07.2007;
- «Інструкції про безготівкові розрахунки в національній валюті користувачів платіжних послуг», затвердженої Постановою Правління НБУ № 163 від 29.07.2022;
- «Положення про порядок формування, зберігання та знищення відокремлених електронних даних отриманих за результатами роботи інформаційних систем у Національному банку України і банках України», затвердженого Постановою Правління НБУ № 99 від 14.09.2018;

- «Положення про функціонування інформаційних систем Національного банку України та банків в особливий період», затверджене постановою Правління НБУ № 175 від 21.04.2004;

- «Правила зберігання, захисту, використання та розкриття банківської таємниці», затверджених Постановою Правління НБУ № 267 від 14.07.2006;

- «Регламент роботи Засвідчувального центру Національного банку України», затверджений Постановою Правління НБУ № 553 від 08.09.2014;

- «Правила застосування переліку документів, що утворюються в діяльності Національного банку України та банків України», затвердженого постановою Правління НБУ № 130 від 27.11.2018;

- «Положення про використання засобів криптографічного захисту інформації Національного банку України», затвердженого Постановою Правління НБУ № 49 від 14.04.2023;

- «Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України», затвердженого Постановою Правління НБУ № 95 від 28.09.2017;

- «Положення про використання електронного підпису та електронної печатки в банківській системі України» затвердженого Постановою Правління НБУ №172 від 20.12.2023;

Інші нормативні документи:

- Міжнародний стандарт безпеки даних індустрії платіжних карт (PCI DSS) версія 4.0 (березень 2022 року);

- Стандарт України з питань інформаційної безпеки ДСТУ ISO/IEC 27001:2015 “Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги”;

- Стандарт України з питань інформаційної безпеки ДСТУ ISO/IEC 27002:2015 “Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки”;