ВВЕДЕНО В ДІЮ

Наказом Т.в.о. Голови Правління
АТ «ТАСКОМБАНК»
№ 338 від «18» травня 2016 р.

ЗАТВЕРДЖЕНО

Рішенням Спостережної Ради
АТ «ТАСКОМБАНК»
Протокол
від «17» травня 2016 р.

Голова Спостережної Ради
АТ «ТАСКОМБАНК»

_____ . . _____

ПОГОДЖЕНО

Рішенням Правління
АТ «ТАСКОМБАНК»
Протокол
від «06» травня 2016 р.

Т.в.о. Голови Правління
АТ «ТАСКОМБАНК»

_____ В.В. Дубєй

ПОЛІТИКА
ІНФОРМАЦІЙНОЇ БЕЗПЕКИ
ПУБЛІЧНОГО АКЦІОНЕРНОГО ТОВАРИСТВА «ТАСКОМБАНК»

м. Київ – 2016 р.

ЗМІСТ

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1. Політика інформаційної безпеки АТ «ТАСКОМБАНК» (далі — Політика) визначає цілі та основні принципи забезпечення безпеки інформації, що представлена в електронному вигляді та обробляється за допомогою інформаційно-телекомунікаційної системи АТ «ТАСКОМБАНК» (далі — Банк).

1.2. Положення даної Політики ґрунтуються на вимогах галузевих стандартів (стандарти Національного банку України з управління інформаційною безпекою в банківській системі України, стандарт захисту інформації в індустрії платіжних карт (PCI DSS), стандарти Міжнародної Організації зі Стандартизації (ISO)) та рекомендаціях кращих міжнародних практик в галузі захисту інформації.

1.3. Під забезпеченням інформаційної безпеки розуміється встановлення та підтримання належного рівня її властивостей.

1.4. Доступність — властивість інформації, яка гарантує те, що забезпечується своєчасний доступ авторизованих осіб і/або процесів до інформації, відсутні простої в процесі її обробки, тобто коли вона знаходиться у вигляді, необхідному користувачеві, в місці, необхідному користувачеві, і в той час, коли вона йому необхідна, а у випадку втрати інформації існує можливість своєчасного відновлення.

1.5. Цілісність — властивість інформації, яка гарантує те, що інформація не містить помилок, є актуальною, вичерпною, будь-які зміни інформації здійснюються авторизованими особами і/або процесами.

1.6. Конфіденційність — властивість інформації, яка гарантує те, що доступ до інформації можуть одержати тільки авторизовані особи і/або процеси.

1.7. Спостережність - властивість системи, що дозволяє фіксувати діяльність користувачів і процесів, використання пасивних об’єктів, а також однозначно установлювати ідентифікатори причетних до певних подій користувачів і процесів з метою запобігання порушення політики безпеки і/або забезпечення відповідальності за певні дії.

1.8. Вимоги Політики поширюються на всі підрозділи Банку, всі бізнес-процеси Банку і є обов'язковими для всіх співробітників Банку. Дотримання вимог Політики є важливим аспектом для досягнення Банком його стратегічних цілей і завдань.

1.9. Політика інформаційної безпеки Банку відповідає вимогам міжнародних галузевих стандартів та стандартів Національного банку України СОУ Н НБУ 65.1 СУІБ 1.0:2010 та СОУ Н НБУ 65.1 СУІБ 2.0:2010, Положенню про забезпечення безперервного функціонування інформаційних систем Національного банку України та банків України.

2. ЦІЛЬ ДОКУМЕНТА

2.1. Метою Політики є впровадження та ефективне функціонування системи управління інформаційною безпекою (далі — СУІБ).

2.2. СУІБ — комплекс організаційних, програмних, технічних і фізичних заходів, спрямованих на управління ризиками, що пов'язані з використанням в Банку інформації та інформаційних технологій.

2.3. Основними задачами СУІБ є:

- забезпечення захисту інформації та ресурсів Банку від зовнішніх і внутрішніх загроз;
- забезпечення надійності бізнес-процесів/банківських продуктів/програмно-технічних комплексів та безперервної роботи Банку;
- сприяння мінімізації ризиків операційної діяльності Банку;
- створення позитивної репутації Банку при роботі з клієнтами.

2.4. Необхідність забезпечення інформаційної безпеки обумовлена тим, що інформація є стратегічно важливим ресурсом Банку.

2.5. Політика спрямована на:

- забезпечення захисту інформаційних активів Банку від зовнішніх і внутрішніх загроз, а також загроз, пов'язаних з навмисними і ненавмисними діями співробітників Банку;
- забезпечення ефективного функціонування СУІБ, яка є основоположною ланкою забезпечення інформаційної безпеки (далі — ІБ);
- забезпечення цілісності, доступності, конфіденційності та спостережності інформації;
- забезпечення безперервності роботи Банку;
- мінімізацію операційних ризиків і ризиків ІБ, впровадження необхідних заходів для запобігання виникненню інцидентів в майбутньому;
- створення позитивної репутації Банку.

2.6. Політикою декларується позиція керівництва Банку щодо забезпечення ІБ та забезпечення з його боку всієї необхідної підтримки при формуванні, прийнятті, впровадженні і супроводі даної Політики і СУІБ Банку. Керівництво Банку виконує ті ж вимоги ІБ, що і всі співробітники Банку.

3. СФЕРА ЗАСТОСУВАННЯ

3.1. Сферою застосування СУІБ є Банк в цілому.

3.2. Дія Політики поширюється на всі підрозділи Банку. Політика використовується для усіх критичних бізнес-процесів/банківських продуктів/програмно-технічних комплексів Банку, є обов'язковою до виконання всіма співробітниками Банку, а також особами, які працюють з інформацією, що належить Банку, в межах укладених контрактів та договорів.

3.3. Забезпечення ІБ здійснюється на постійній основі і є завданням усіх підрозділів Банку. Заходи забезпечення ІБ здійснюються на засадах розподілу сфер відповідальності між підрозділами Банку та узгоджені між собою за цілями, завданнями, принципами, методами і засобами. Організація виконання заходів щодо забезпечення ІБ здійснюється відділом захисту інформаційних систем Департаменту безпеки Банку.

3.4. Всі співробітники Банку, незалежно від займаної посади, несуть персональну відповідальність за дотримання вимог ІБ відповідно до чинного законодавства України та внутрішнім нормативним документам Банку. Керівники підрозділів Банку додатково несуть відповідальність за порушення вимог ІБ і інші неправомірні дії підлеглих співробітників.

3.5. Внутрішні нормативні документи ІБ доводяться до відома всіх співробітників Банку в частині що їх стосується. Банк здійснює на регулярній основі інформування та навчання співробітників Банку з питань забезпечення інформаційної безпеки.

4. ПРЕДМЕТ ПОЛІТИКИ

4.1. Основними принципами Політики є підтримання належного захисту інформації із забезпеченням її цілісності, конфіденційності, доступності та спостережності.

4.2. Об'єктами захисту в Банку є інформаційні активи - матеріальні та нематеріальні об'єкти, які є інформацією або містять інформацію, служать для обробки, зберігання або передачі інформації і мають цінність для Банку.У загальному випадку до інформаційних активів відносяться:

- інформація в електронному вигляді, яка циркулює в ІС на всіх етапах їх життєвого циклу (створення, обробка, зберігання, передача, знищення);
- інформація на паперових носіях;
- інформаційні системи, включаючи апаратні, апаратно-програмні та програмні засоби, системи і комплекси;
- приміщення Банку;
- персонал Банку.

4.3. Вся інформація, що представлена в електронному вигляді та обробляється за допомогою ІТ системи Банку повинна мати визначеного власника. За кожним інформаційним активом, розпорядчим документом Банку призначається власник - структурний підрозділ банку в особі його начальника, який ініціював його створення або використовує для виконання бізнес завдань. Власник інформаційного активу приймає рішення про необхідність його зміни / модернізації, оцінює інформаційні ризики щодо активів, приймає рішення щодо їх мінімізації, прийняття або передачі, розглядає і організовує виконання вимог ІБ, погоджує доступ до інформаційного активу, приймає рішення про знищення інформаційного активу або виведення з експлуатації.

4.4. Забезпечення ІБ здійснюється СУІБ, яка є основоположною у процесах захисту інформації. Етапи ефективного функціонування СУІБ є циклічними за схемою «Планування-Впровадження-Перевірка-Корегування». Основними етапами організації СУІБ є:

- підготовка до впровадження;
- опис існуючої інфраструктури та заходів безпеки;
- оцінка ризиків інформаційної безпеки;
- планування комплексу заходів щодо мінімізації ризиків;
- затвердження та впровадження комплексу заходів;
- навчання співробітників;
- складання звітів про стан інформаційної безпеки.

4.5. СУІБ висуває вимоги щодо забезпечення інформаційної безпеки до ІТ системи Банку, процесів, які обробляються в ІТ системі, і до процесів управління ІТ системою.

4.6. Протягом життєвого циклу СУІБ не рідше ніж один раз на рік проводиться аудит інформаційної безпеки — незалежна оцінка стану системи інформаційної безпеки, що встановлює рівень її відповідності певним критеріям.

4.7. При забезпеченні інформаційної безпеки Банк керується ризик-орієнтованим підходом, який забезпечує розуміння, моніторинг та зменшення ризиків операційної діяльності та ІТ ризиків.

4.8. Заходи щодо захисту інформації в Банку відповідають потребам бізнесу та вимогам законодавства України, нормативно-правових документів Національного банку України, внутрішніх нормативних документів Банку.

4.9. Організація будь-якого процесу, що має оброблятись в ІТ системі, або внесення змін в існуючі процеси здійснюється з урахуванням забезпечення інформаційної безпеки.

4.10. СУІБ постійно розвивається і вчасно реагує на зміни бізнес-процесів і ІТ системи банку.

4.11. Оцінка ефективності функціонування СУІБ здійснюється на регулярній основі.

4.12. Для зменшення ризиків виникнення інцидентів інформаційної безпеки керівництво Банку створює умови для систематичного навчання працівників нормам та заходам інформаційної безпеки.

4.13. Відділ захисту інформаційних систем Департаменту безпеки відповідає за визначення вимог інформаційної безпеки та здійснює контроль за їх виконанням в Банку.

4.14. Процеси інформаційної безпеки описані, формально визначені та затверджені керівництвом Банку у вигляді стандартів, політик, положень та інших внутрішніх нормативних документів.

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

4.16. Заходи та засоби захисту інформаційних активів обираються за результатами аналізу ризиків для інформаційних активів. Витрати на ІБ повинні бути адекватними існуючим ризикам з урахуванням витрат на їх реалізацію і можливих втрат від реалізації загроз.

4.17. Банк виявляє, враховує і оперативно реагує на дійсні і ймовірні порушення ІБ. Всі інциденти ІБ фіксуються, аналізуються та враховуються при розробці заходів забезпечення захисту інформаційних активів. Внутрішніх нормативних документах.

4.18. Фінансування заходів щодо забезпечення ІБ передбачається в щорічному бюджеті Банку.

4.19. Ефективність реалізації Політики ІБ щорічно оцінюється підрозділом безпеки і керівництвом Банку.

5. РОЛІ ТА ВІДПОВІДАЛЬНІСТЬ

5.1. Керівництво Банку чітко розуміє, що інформаційна безпека Банку є основою життєдіяльності Банку.

5.2. Керівництво Банку сприяє створенню, впровадженню, контролю та підтримці Політики інформаційної безпеки.

5.3. Документи Політики інформаційної безпеки розробляються Відділом захисту інформаційних систем Департаменту безпеки та іншими підрозділами за відповідними напрямками діяльності.

5.4. Будь-які дії співробітників банку в ІТ системі, які не дозволені явно та не затверджені нормативними або інструктивними документами, є забороненими.

6. КОНТРОЛЬ ТА ВІДПОВІДАЛЬНІСТЬ

6.1. Контроль за виконанням вимог Політики інформаційної безпеки АТ «ТАСКОМБАНК» покласти на Відділ захисту інформаційних систем Департаменту безпеки.

6.2. Кожен співробітник Банку забезпечує підтримку відповідного рівня інформаційної безпеки Банку. В своїй роботі всі підрозділи та працівники дотримуються вимог Політики інформаційної безпеки.

6.3. Відділ захисту інформаційних систем Департаменту безпеки забезпечує моніторинг дотримання вимог Політики інформаційної безпеки.

6.4. Відповідальність за виконання працівниками вимог Політики інформаційної безпеки несуть керівники працівників всіх підрозділів.

6.5. Відповідальність за ознайомлення персоналу з вимогами ІБ, нормативними та розпорядчими документами з питань ІБ, навчання персоналу з питань ІБ несуть, в рамках компетенції, відділ захисту інформаційних систем Департаменту безпеки, загальний відділ, учбовий центр.

6.6. За порушення вимог Політики, законодавчих, регуляторних і внутрішньобанківських норм кожен співробітник несе відповідальність згідно із законодавством України і внутрішніми нормативними документами Банку.

6.7. Відповідальність за підтримання Політики в актуальному стані, своєчасне внесення змін та доповнень до неї, несе Відділ захисту інформаційних систем.

7. УПРАВЛІННЯ РИЗИКАМИ

7.1 Процес управління ризиками інформаційної безпеки здійснюється для банку в цілому.

7.2 Процес управління ризиками інформаційної безпеки стосується всіх підрозділів банку, у першу чергу, керівників підрозділів – власників бізнес-процесів/банківських продуктів. Банк керується ризик-орієнтованим підходом при плануванні та впровадженні СУІБ.

7.3 Затвердження, управління, обробка та прийняття залишкових ризиків здійснюється Керівництвом Банку.

7.4 Зниження ризиків можливо забезпечити шляхом застосування належних заходів безпеки з урахуванням всіх вимог законодавства України, нормативно-правових актів Національного банку України, внутрішніх документів, політики та стратегії банку.

8. ЗАКЛЮЧНІ ПОЛОЖЕННЯ

8.1. Дана Політика затверджується рішенням Спостережної Ради Банку та набирає чинності з дати введення його в дію Наказом Голови Правління Банку.

8.2. Політика переглядається за необхідністю, але не менш ніж один раз на три роки.

8.3. Причинами внесення змін до Політики є зміни в інформаційній інфраструктурі та/або впровадженні в Банку нових інформаційних технологій, а також змінах в законодавчих, регуляторних та інших нормах.

8.4. Відповідальність за підтримання Політики в актуальному стані, за своєчасне внесення змін та доповнень до них несе Відділ захисту інформаційних систем.

8.5. Дана Політика розроблена з урахуванням вимог:

— Стандартів Національного банку України: СОУ Н НБУ 65.1 СУІБ 1.0:2010 «Методи захисту в банківській діяльності. Система управління інформаційною безпекою. Вимоги" (ISO/IES 27001:2005, MOD) та СОУ Н НБУ 65.1 СУІБ 2.0:2010 "Методи захисту в банківській діяльності. Звід правил для управління інформаційною безпекою" (ISO/IES 27002:2005, MOD), які набрали чинності згідно Постанови Правління Національного банку України від 28.10.2010 №474.