КОНТРОЛЬНИЙ ПРИМІРНИК

ЗАТВЕРДЖЕНО
Протокол Наглядової ради
АТ «ТАСКОМБАНК»
06.02.2025 №06022025/31

ПОГОДЖЕНО
Протокол Правління
АТ «ТАСКОМБАНК»
21.01.2025 №04-3

ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ АКЦІОНЕРНОГО ТОВАРИСТВА «ТАСКОМБАНК»

Київ – 2025

ЗМІСТ

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1. У Політиці інформаційної безпеки АКЦІОНЕРНОГО ТОВАРИСТВА «ТАСКОМБАНК» (далі — Політика) визначаються засади забезпечення інформаційної безпеки АКЦІОНЕРНОГО ТОВАРИСТВА «ТАСКОМБАНК» (далі — Банк).

1.2. Забезпечення інформаційної безпеки (далі по тексту – ІБ) у Банку повинно здійснюватися з використанням процесного підходу і формалізовано в процес «Забезпечення ІБ», який, в свою чергу, розділено на окремі процеси: «Методологія», «Кіберзахист» і «Криптозахист». Підтримку процесів нормативно врегульовано і описано у відповідних внутрішніх нормативних документах». Відповідальні особи, терміни виконання заходів захисту, показники ефективності – призначаються і визначаються розпорядчими документами Банку.

1.3. Належний рівень ІБ – це стан інформаційних ресурсів Банку, який гарантує конфіденційність, доступність, цілісність інформації Банку, а також спостережність та контрольованість системи, в якій інформація циркулює.

1.4. Належний рівень ІБ повинен досягатися застосуванням комплексу програмних та технічних і організаційних заходів, спрямованих на забезпечення захищеності інформації від зловмисного використання, руйнування, несанкціонованого оприлюднення, несанкціонованих змін, знищення, недоступності.

1.5. АТ «ТАСКОМБАНК» визначено системно-важливим банком, надано статус «об’єкт критичної інфраструктури в банківській системі України».

1.6. Політику розроблено відповідно до вимог чинного законодавства України, нормативно-правових актів Національного банку України, міжнародних стандартів та рекомендацій, зокрема:
Закону України «Про банки і банківську діяльність»;
Закону України «Про основні засади забезпечення кібербезпеки України»
Нормативних актів Національного банку України:

- Положення про забезпечення безперервного функціонування інформаційних систем Національного банку та банків України, затверджене постановою Правління Національного банку України від 17.06.2004 № 265.
- Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України затверджене постановою Правління Національного банку України від 28.09.2017 № 95.
- Положення про організацію системи управління ризиками в банках України та банківських групах, затвердженого Постановою Правління НБУ від 11.06.2018 №64.
- Положення про використання електронного підпису та електронної печатки, затверджене постановою Правління Національного банку України 20.12.2023 №172.
- Положення про здійснення контролю за дотриманням банками вимог законодавства з питань інформаційної безпеки, кіберзахисту та електронних довірчих послуг затверджене Постановою Правління Національного банку України 16 січня 2021 №4.
- Положення про захист інформації та кіберзахист у платіжних системах, затверджене постановою Правління Національного банку України від 19.05.2021 №43.
- Положення про використання засобів криптографічного захисту інформації Національного банку України, затверджене постановою Правління Національного банку України №49 від 14.04.2023.
- Положення про організацію системи внутрішнього контролю в банках України та банківських групах затверджене постановою Правління Національного банку України від 02.07.2019 №88.
- Положення про визначення об'єктів критичної інфраструктури в банківській системі України» затверджене постановою Правління Національного банку України від 20.08.2022 № 151.

- Про затвердження Положення про організацію кіберзахисту в банківській системі України та внесення змін до Положення про визначення об'єктів критичної інфраструктури в банківській системі України затверджене постановою Правління Національного банку України від 12.08.2022 № 178.

Національних стандартів України з питань інформаційної безпеки:

- ДСТУ ISO/IEC 27000:2019 «Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Огляд і словник термінів».
- ДСТУ ISO/IEC 27001:2022 «Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги».
- ДСТУ ISO/IEC 27002:2023 «Інформаційна безпека, кібербезпека та захист конфіденційності. Засоби контролювання інформаційної безпеки».
- ДСТУ ISO/IEC 27010:2018 «Інформаційні технології. Методи захисту. Керування інформаційною безпекою для міжгалузевих та міжорганізаційних комунікацій».

1.7. Політика публікується на зовнішньому сайті Банку та доступна для всіх.

2. ГЛОСАРІЙ

2.1. У цій Політиці вживаються терміни та поняття у наступному значенні:

Аутсорсер – організація будь-якої форми власності, фізична особа-підприємець або особа, яка провадить незалежну професійну діяльність, обрана Банком для виконання на умовах аутсорсингу окремих робіт/функцій Банку.

ЄДБО – Єдиний договір банківського обслуговування та надання інших послуг Національним банком України

ДІБ – Департамент інформаційної безпеки.

Доступність інформації — це гарантія своєчасного доступу авторизованих осіб і/або процесів до інформації, відсутні простої в процесі її обробки, тобто коли інформація знаходиться у вигляді, необхідному користувачеві, в місці, необхідному користувачеві, і у той час, коли вона йому необхідна, а у випадку втрати інформації існує можливість своєчасного відновлення.

Життєвий цикл інформаційної системи — це послідовність етапів, через які проходить інформаційна система від її створення до виведення з експлуатації.

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

Інформаційна безпека (ІБ) – процес, який забезпечує збереження визначених Політикою властивостей інформації та спрямований на запобігання несанкціонованим діям в інформаційній системі, що включає сукупність організаційно-технічних заходів і правових норм для запобігання заподіянню шкоди інтересам власника інформації чи інформаційної системи.

Інформаційна система (ІС) - організаційно-технічна система, у якій реалізується технологія обробки інформації з використанням технічних і програмних засобів.

ІКС – Інформаційно-комунікаційна система – сукупність інформаційних та комунікаційних систем, які у процесі обробки інформації діють як єдине ціле.

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

НБУ – Національний банк України.

Об'єкт критичної інфраструктури в банківській системі України (ОКІ) - банки України, стале функціонування яких забезпечує стабільність банківської системи, має суттєве значення для економіки та безпеки держави, функціонування суспільства та які становлять значний суспільний інтерес

Персонал – усі працівники Банку, які використовують інформаційні ресурси Банку, комп'ютерне, телекомунікаційне і офісне обладнання відповідно до посадових обов'язків.

Ризик інформаційної безпеки (складова операційного ризику) - ймовірність виникнення збитків або додаткових втрат, або недоотримання запланованих доходів

унаслідок порушення конфіденційності, цілісності, доступності даних в інформаційних системах банку, недоліків або помилок в організації внутрішніх процесів або настання зовнішніх подій, уключаючи кібератаки або неадекватну фізичну безпеку. Ризик інформаційної безпеки включає кіберризик.

Робоча група – Робоча група з управління інформаційною безпекою, колективний керівний орган Системи управління інформаційною безпекою (далі - СУІБ), з питань впровадження та функціонування СУІБ. До його складу входять Заступник Голови Правління Банку, що відповідає за ІБ, керівники підрозділів - власників критичних бізнес-процесів та керівник підрозділу з управління ризиками. Банк має право вводити до складу керівного органу СУІБ інших працівників відповідно до потреб, що обумовлені особливостями діяльності банку

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.

Соціальна інженерія – механізм психологічної маніпуляції, тобто нав’язування мотивації працівникам Банку з боку зловмисника з метою підштовхнути скоїти певні дії від власного імені.

Спостережність системи – властивість, що дозволяє фіксувати діяльність користувачів і процесів, а також однозначно установлювати ідентифікатори причетних до певних подій користувачів і процесів з метою запобігання порушення Політики або забезпечення відповідальності за певні дії.

Третя сторона (Третя особа) - особа (фізична або юридична), яка перебуває у фінансових або будь-яких договірних відносинах з Банком, являється стороною таких відносин але не є клієнтом Банку. Зокрема Третіми особами є організації будь-якої форми власності (та їх представники), самозайняті особи або фізичні особи, які провадять незалежну професійну діяльність) і надають послуги Банку (за винятком аутсорсерів).

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

MISP-NBU Центру кіберзахисту (англійською мовою Malware Information Sharing Platform of the National Bank of Ukraine) - спеціалізований сайт НБУ побудований на базі платформи з відкритим програмним кодом MISP і доступний за посиланням https://misp.bank.gov.ua/, призначений для організації доступу банків до системи збору, обробки, зберігання і обміну інформацією загального організаційного та технічного характеру в режимі реального часу з урахуванням вимог конфіденційності (далі - MISP-NBU).

CISO (англ. Chief information security officer) - відповідальна особа за ІБ Банку уповноважена Головою Правління приймати управлінські рішення та забезпечувати:

1) стратегічне керівництво з питань ІБ;
2) визначення напрямів розвитку ІБ, їх відповідність стратегії розвитку Банку;
3) відповідність заходів безпеки потребам бізнес-процесів/банківських продуктів;
4) контроль за впровадженням заходів безпеки інформації в Банку.

WAF (Web Application Firewall) – міжмережевий екран для веб-застосунків. Це інструмент для фільтрації трафіку, що працює на прикладному рівні та захищає веб-додатки методом аналізу трафіку HTTP/HTTPS та семантики XML/SOAP. WAF може встановлюватися на фізичний або віртуальний сервер та виявляє найрізноманітніші види атак.

2.2. Інші терміни, що вживаються у цій Політиці, застосовуються в значеннях, визначених чинним законодавством України, нормативно-правовими актами НБУ та внутрішніми нормативними документами Банку.

3. МЕТА ТА ЗАВДАННЯ ПОЛІТИКИ

3.1. Метою Політики є:
- визначення засад забезпечення ІБ Банку та розподіл сфер відповідальності між підрозділами Банку за дотримання вимог законодавства України та нормативних актів НБУ з ІБ;
- визначення принципів управління ІБ;
- визначення вимог до ІКС Банку, що взаємодіють з інформаційними системами НБУ, з урахуванням напрямів розвитку криптографічного захисту інформації в інформаційних системах НБУ.

3.2. Основними завданнями Політики є:
- визначення засад захисту інформації та ресурсів Банку від зовнішніх і внутрішніх кіберзагроз;
- визначення засад кіберзахисту бізнес-процесів, банківських продуктів, програмно-технічних комплексів;
- впровадження ризик-орієнтованого підходу до забезпечення ІБ;
- впровадження процесного підходу до забезпечення ІБ Банку;
- визначення засад попередження та мінімізації ризиків ІБ та ІСТ.

4. СФЕРА ЗАСТОСУВАННЯ ПОЛІТИКИ

4.1. Дія Політики поширюється на всі підрозділи та працівників Банку, усі процеси, банківські продукти, програмно-технічні комплекси, проекти, організаційні рішення. Політика є обов`язковою до виконання усіма працівниками Банку, а також Третіми сторонами, залученими до роботи з інформаційними ресурсами Банку, у межах укладених з Третіми особами угод/контрактів/договорів.

4.2. Об’єкти регулятивного впливу.

Об’єктами, на які розповсюджується дія і регулятивний вплив Політики, є:

- **Інформаційні ресурси:**

Інформація та дані у будь-якому вигляді, що отримуються, зберігаються, оброблюються, передаються, оголошуються, у тому числі інформація про Персонал і контрагентів, бази даних та файли, нормативна документація, електронні архіви тощо.

- **Програмне забезпечення:**

Прикладне, системне, сервісне програмне забезпечення та будь-яке інше, незалежно від форми отримання (придбання, власної розробки, безкоштовне), яке використовується у Банку працівниками та системами для роботи та взаємодії з клієнтами та іншими зовнішніми системами.

- **Фізичні ресурси:**

Виробничі приміщення, усі технічні засоби роботи з інформацією, зокрема, сервери, робочі станції, міжмережеві екрани, принтери, копіювальні апарати, телекомунікаційне обладнання, маршрутизатори тощо.

- **Сервісні ресурси:**

Обчислювальні та комунікаційні сервіси, зокрема, доступ до мережі Інтернет, електронної пошти, телефонного зв’язку. Технічні сервіси забезпечення належних санітарних умов для персоналу, зокрема, опалення, освітлення, енергозбереження, кондиціювання повітря, системи сигналізації та моніторингу, усі послуги, пов’язані з отриманням, наданням, використанням, передачею та знищенням активів, усі юридичні та фізичні особи, організації, установи та підприємства (їх працівники), послугами яких користується Банк для отримання, використання, передачі та знищення активів.

- **Кадровий ресурс:**

Персонал Банку (діючий, мобілізований та кадровий резерв).

- **Треті сторони:**

Фізичні та юридичні особи, які перебувають у фінансових або будь-яких договірних відносинах з Банком і є сторонами таких відносин.

4.3. Інформаційними активами Банку, як одним з об’єктів захисту, вважаються матеріальні та нематеріальні об'єкти, які є інформацією або містять інформацію, використовуються для обробки інформації і мають цінність для Банку:
- інформація в електронному вигляді, яка зберігається в ІС на всіх етапах їх життєвого циклу (створення, обробка, зберігання, передача, знищення);
- інформація на паперових носіях;
- ІС, включаючи апаратні, апаратно-програмні та програмні засоби;
- приміщення Банку;
- персонал Банку.

4.4. Вся інформація, що представлена в електронному вигляді та обробляється за допомогою ІС 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 його для виконання бізнес завдань. При цьому, власник активу не має матеріальних/авторських або інших прав на актив. Усі права на усі інформаційні активи належать тільки Банку.

4.5. Власник інформаційного активу надає на розгляд рішення щодо його зміни, модернізації, оцінює інформаційні ризики щодо своїх активів, надає на розгляд рішення щодо їх мінімізації, прийняття або передачі, усіляко сприяє виконанню вимог ІБ, погоджує доступ до свого інформаційного активу, виносить на розгляд рішення про знищення інформаційного активу або виведення його з експлуатації.

4.6. Рішення щодо зміни, модернізації, мінімізації, прийняття або передачі ризиків ІБ знищення інформаційного активу або виведення його з експлуатації приймаються уповноваженими колегіальними органами управління Банку, залежно від належності і важливості/критичності активу.

5. ЗАСАДИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

5.1. Управління ІБ організовано у спосіб консолідації людських, методологічних, інтелектуальних та програмно-технічних ресурсів в єдину систему - СУІБ.

5.2. Задачі СУІБ:
- захист інформації та ресурсів Банку від зовнішніх і внутрішніх загроз;
- забезпечення надійності роботи бізнес-процесів/програмно-технічних комплексів;
- сприяння мінімізації ризиків ІБ;
- створення позитивної репутації Банку при роботі з клієнтами та партнерами;
- реалізація системного підходу до управління ІБ.

5.3. СУІБ встановлює вимоги щодо забезпечення ІБ до ІКС, процесів, які автоматизовано в ІКС, і процесів з управління ІКС.

5.4. Заходи із захисту інформації в Банку відповідають потребам бізнесу та вимогам законодавства України, нормативно-правових актів НБУ, внутрішніх нормативних документів Банку.

5.5. Організація будь-якого процесу, що має оброблятись в ІКС, або внесення змін в існуючі процеси здійснюється з урахуванням вимог ІБ.

5.6. СУІБ постійно повинна розвиватися, враховуючи зміни у процесах та в ІКС.

5.7. Процеси забезпечення ІБ описані, формально визначені та затверджені у реєстрі бізнес-процесів та внутрішніх нормативних документах Банку.

5.8. В Банку складаються, тестуються та оновлюються плани забезпечення безперебійного функціонування та відновлення діяльності на випадок непередбачених надзвичайних ситуацій, які можуть призвести до зупинки діяльності. В даному процесі, ДІБ відповідає за складання, тестування та оновлення плану

відновлення ІС Банку, що використовуються для забезпечення безпеки електронної інформації.

5.9. Для забезпечення ІБ в Банку впроваджено ризик-орієнтований підхід. Заходи та засоби захисту обираються за результатами оцінки ризиків ІБ. Витрати на впровадження засобів захисту відповідають існуючим ризикам з урахуванням можливих втрат від реалізації ризиків.

5.10. Працівники Банку виявляють, враховують і реагують на дійсні і ймовірні порушення ІБ. Всі інциденти ІБ фіксуються у журналах обліку інцидентів ІБ, аналізуються ДІБ, надаються на розгляд Робочої групи, та враховуються при розробці заходів захисту інформаційних активів.

5.11. Внутрішні нормативні документи СУІБ доводяться до відома працівників Банку в частині, що їх стосується.

5.12. Вимоги ІБ щодо забезпечення захисту інформаційних активів визначаються у внутрішніх нормативних документах і внутрішніх розпорядчих документах Банку. При розробці вимог ІБ враховуються вимоги Законів України і нормативно-правових актів НБУ. Вимоги ІБ враховуються при реалізації всіх бізнес - процесів Банку та протягом життєвого циклу інформаційних систем. Вимоги ІБ також враховуються у відносинах з контрагентами та Третіми сторонами.

5.13. Організація будь-якого бізнес-процесу, що автоматизується і має оброблятись в ІС, або внесення змін в існуючі процеси здійснюється з урахуванням вимог забезпечення ІБ.

5.14. Для зниження ризиків ІБ в Банку проводиться систематичне навчання працівників нормам та заходам ІБ, такі навчання проводяться відповідно до річних планів навчання та організаційно інтегровані в загальну систему навчання Банку.

5.15. Процеси ІБ описані, формально визначені та затверджені керівництвом Банку.

5.16. ДІБ 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.

5.17. Фінансування заходів забезпечення ІБ передбачається в бюджеті Банку.

5.18. Оцінка ефективності функціонування СУІБ та ефективність реалізації Політики ІБ щорічно оцінюються в рамках процесу перегляду СУІБ Робочою групою і Правлінням Банку.

6. ПРИНЦИПИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

6.1. СУІБ організовується з дотриманням наступних принципів:

- **Приналежності ресурсів.**

Для кожного інформаційного ресурсу призначається Власник.

- **Персональної відповідальності.**

За реалізацію та виконання визначених заходів забезпечення ІБ передбачена відповідальність. У договірних документах з Третіми особами зазначаються умови взаємних перевірок дотримання вимог ІБ.

- **Колегіальної участі.**

У межах своїх повноважень і відповідальності всі працівників Банку беруть участь у захисті інформації в ІС Банку. Функцію загального управління виконує CISO Банку. Функцію колегіального органу управління виконує Робоча група.

- **Виправданості витрат.**

Об’єм ресурсів, залучених для захисту інформаційних активів, має відповідати наявним загрозам і не перевищувати обсяг збитків, що можуть виникнути внаслідок реалізації загроз.

- **Достатньої компетенції.**

Персонал та Треті особи повинні мати рівень обізнаності, достатній для адекватного реагування на інциденти, ефективної протидії загрозам ІБ та дотримання вимог ІБ. В Банку організовується навчання з ІБ та контроль рівня знань персоналу. Достатній рівень обізнаності з ІБ представників Третіх сторін є обов'язковою умовою співпраці з Банком та зазначається у договірних умовах.

- **Системної діяльності.**

Діяльність із забезпечення належного рівня ІБ провадиться у спосіб організації СУІБ, якою керує колегіальний орган управління – Робоча група. Така діяльність є системною та проводиться в рамках моделі Демінга – «плануй-виконуй-перевіряй-впливай».

- **Розподілу прав доступу.**

Персонал може мати тільки такі права доступу до приміщень та інформаційних/технологічних ресурсів, які достатні для виконання посадових обов'язків згідно посадових інструкцій. Третя сторона може мати тільки такі права доступу до приміщень та інформаційних/технологічних ресурсів, які достатні для виконання нею договірних зобов'язань згідно діючих договірних умов визначених в договорах. До ресурсів, що не стосуються посадових обов'язків персоналу або виконання договірних умов Третьою стороною, права доступу не надаються, або надаються як виняток з обов'язковим визначенням посадових осіб, які приймають ризики, обумовлені застосованим винятком.

- **Забезпечення безперервності.**

У Банку організовується управління безперервністю бізнесу, яке забезпечує безперебійне надання послуг споживачам та виконання зобов'язань Банку перед контрагентами і регуляторами ринку у спосіб застосування комплексу організаційних заходів та програмно-технічних засобів. Такий комплекс забезпечує надійність роботи Банку, виявлення загроз, причин, передумов кризових/надзвичайних ситуацій, усунення негативних наслідків реалізації загроз та відновлення нормального режиму роботи Банку.

6.2. Банк, для ефективного функціонування СУІБ, вивчає кращі світові практики у сфері управління ІБ та застосовує сучасні технології кіберзахисту.

6.3. Основні **правила та вимоги ІБ:**

- В Банку контролюється ефективність впроваджених заходів та засобів забезпечення ІБ в інформаційних системах, визначено перелік усіх бізнес-процесів та інформаційних ресурсів, які забезпечують їх функціонування.
- В Банку організовано захист інформації обмеженого доступу, яка належить до категорій: «банківська таємниця», «персональні дані», «комерційна таємниця», «таємниця страхування».
- В Банку розроблено вимоги з ІБ для третіх сторін, які надають Банку послуги з ІТ, розробки, впровадження, аудиту інформаційних систем і ресурсів, отримують від Банку інформацію з обмеженим доступом.

6.3.1. Передача функцій на аутсорсинг здійснюється відповідно до Порядку управління ризиками та здійснення контролю при запровадженні співпраці з аутсорсерами в АТ «ТАСКОМБАНК».

7. МОДЕЛЬ ЗАГРОЗ ТА МОДЕЛЬ ПОРУШНИКА

7.1. В Банку діє модель загроз інформаційній безпеці. Модель загроз використовується у оцінці ризиків ІБ. Перелік загроз визначається у Методиці оцінки інформаційних ризиків АТ «ТАСКОМБАНК».

7.2. В Банку діє модель порушника, описано вірогідні дії порушника. Складається на основі аналізу типу зловмисника, рівня його повноважень, знань, теоретичних та практичних можливостей. Порушники можуть бути зовнішні або внутрішні.

7.3. До внутрішніх порушників потенційно належать:

- працівники, користувачі інформаційної системи, які можуть завдавати навмисної чи ненавмисної шкоди інформаційним ресурсам;
- технічний персонал, який обслуговує будівлі, приміщення, технічні засоби які не є елементами інформаційної системи (електрики, сантехніки, інженери, техніки).

7.4. Зовнішні порушники – це сторонні особи, які знаходяться поза периметром інформаційно-телекомунікаційної системи Банку або її неавторизовані користувачі. Це означає, що вони не мають в ІКС Банку облікового запису і не мають повноважень працювати в даній системі.

Таблиця 7.1.

КАТЕГОРІЇ ПОРУШНИКІВ

№	Визначення категорії	Тип порушника по відношенню до Банку	Рівень загрози
1	Технічний персонал (електрики, прибиральники, тощо)	Внутрішній	Середній
2	Персонал, що обслуговує технічні засоби ІС	Внутрішній	Дуже високий
3	Користувачі ІС	Внутрішній	Середній
4	Адміністратори ІС, працівники ДІБ	Внутрішній	Дуже високий
5	Керівники підрозділів з розширеними повноваженнями в тому числі в інформаційних системах	Внутрішній	Дуже високий
6	Клієнти, відвідувачі Банку	Зовнішній	Низький
7	Представники обслуговуючих організацій (енергопостачання, газова служба, водопостачання, тощо)	Зовнішній	Низький
8	Хакери	Зовнішній	Дуже високий
9	Агенти конкурентів та спецслужб	Зовнішній	Дуже високий

Таблиця 7.2.

МОТИВИ ЗДІЙСНЕННЯ ПОРУШЕННЯ

№	Мотив	Рівень загрози
1	Безвідповідальність (ненавмисне порушення)	Низький
2	Самоствердження	Середній
3	Корисливий інтерес	Високий
4	Вираження незадоволення або нелояльності	Високий
5	Дії в інтересах конкурентів	Високий

Таблиця 7.3.

РІВНІ КВАЛІФІКАЦІЇ ПОРУШНИКА

№	Рівень кваліфікації порушника	Рівень загрози
1	Низький рівень знань; використовує ІС на рівні користувача.	Низький
2	Середній рівень знань, має навики використання ІС та їх обслуговування.	Середній
3	Високий рівень знань у галузі програмування та обчислювальної техніки, проектування та експлуатації ІС.	Високий
4	Високий рівень знань, знає структуру, функції та механізми дії систем захисту інформації в ІС, їх недоліки та можливості.	Дуже високий

Таблиця 7.4.

КЛАСИФІКАЦІЯ МОЖЛИВОСТЕЙ ПОРУШНИКА ЗА ВИКОРИСТАННЯМ ЗАСОБІВ ПОДОЛАННЯ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

№	Опис можливостей порушника	Рівень загрози
1	Може підслуховувати розмови у приміщеннях та читати документи на чужих робочих місцях.	Низький
2	Використовує пасивні технічні засоби перехвату без можливості модифікації інформації та компонентів ІС.	Середній
3	Використовує методи соціальної інженерії.	Високий
4	Використовує лише штатні засоби та недоліки системи захисту інформації для її подолання (несанкціоновані дії з використанням дозволених та доступних засобів), а також компактні носії інформації, які може приховано проносити повз пости охорони Банку.	Високий
5	Використовує високотехнологічні технічні засоби активного впливу з метою модифікації інформації та компонентів ІС, дезорганізації систем обробки/резервування інформації.	Дуже високий

Таблиця 7.5.

КЛАСИФІКАЦІЯ МОЖЛИВОСТЕЙ ПОРУШНИКА ЗА ДОСТУПОМ

№	Опис можливостей порушника	Рівень загрози
1	Ззовні приміщень Банку; всередині приміщень, але без доступу до технічних засобів ІКС.	Низький/середній
2	З робочих місць користувачів ІКС.	Середній/високий
3	З доступом у зону зберігання баз даних, архівів, серверну чи комутаційну кімнати, тощо.	Дуже високий
4	З доступом у зону керування засобами безпеки ІКС.	Дуже високий

8. КІБЕРЗАХИСТ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

8.1. До об'єктів критичної інформаційної інфраструктури Банк відносить інформаційні системи, що безпосередньо забезпечують автоматизацію банківської діяльності (надання банківських послуг) та відповідають двом критеріям:
- порушення функціонування інформаційної системи внаслідок кіберінциденту може вплинути на стале функціонування Банку та безперервність роботи Банку;
- якщо в Банку немає альтернативних за функціональними можливостями інформаційних систем для надання аналогічних відповідних послуг.

8.2. В Банку створено перелік об'єктів критичної інформаційної інфраструктури, який підтримується в актуальному стані.

8.3. Перелік об'єктів критичної інформаційної інфраструктури щороку переглядається Робочою групою з управління інформаційною безпекою.

8.4. Зв'язок технологічної платформи критичної інформаційної інфраструктури Банку з мережею Інтернет здійснюється з використанням двох або більше комунікаційних каналів, що надаються різними операторами, провайдерами телекомунікацій через захищені вузли доступу з мережі Інтернет.

8.5. Інформація аналізується засобами WAF.

8.6. Відомості про об'єкти критичної інформаційної інфраструктури Банку є інформацією з обмеженим доступом.

8.7. Організація інформаційного обміну з центром кіберзахисту НБУ.

8.7.1. Інформаційний обмін здійснюється з метою:
- вжиття спільних заходів щодо своєчасного виявлення, запобігання, нейтралізації кіберзагроз та попередження про можливі кібератаки, забезпечення кіберстійкості;
- мінімізації ризиків реалізації кібератак, наслідків реалізованих кібератак;
- підвищення обізнаності працівників організацій-учасників інформаційного обміну.

8.7.2. Підключення до MISP-NBU здійснюється шляхом приєднання Банку до ЄДБО Національного банку.

8.7.3. Функції щодо здійснення інформаційного обміну з MISP-NBU входять до компетенції відділу кіберзахисту ДІБ.

8.7.4. Банк, як учасник інформаційного обміну, маркує електронні повідомлення, що поширюються під час інформаційного обміну, спеціальними мітками з урахуванням протоколу «Світлофор», визначеного в додатку С до Національного стандарту України ДСТУ ISO/IEC 27010:2018 (англійською мовою Traffic Light Protocol).

8.7.5. Поширення інформації між учасниками інформаційного обміну здійснюється виключно на основі міток TLP відповідно до порядку інформаційного обміну. Оприлюднення цієї інформації в засобах масової інформації, поширення в мережі Інтернет, соціальних мережах не допускається.

8.7.6. У процесі здійснення інформаційного обміну заборонено:
- редагувати (модифікувати) інформацію, що отримана з довірених джерел інформації, під час надання її іншим учасникам інформаційного обміну;
- використовувати інформацію, отриману під час інформаційного обміну, з іншою метою, ніж зазначена в пункті 8.6.1 Політики, якщо інше не передбачено законодавством України.

9. АУДИТ СТАНУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

9.1. В Банку регулярно проводиться незалежний аудит ІБ (далі - зовнішній аудит). Зовнішній аудит проводиться згідно з нормами законодавства України, національних стандартів та з урахуванням вимог Національного Банку. Програма аудиту формується враховуючи особливості діяльності Банку, характер та обсяг банківських, фінансових послуг та інших видів діяльності.

9.2. Зовнішній аудит критичної інформаційної інфраструктури здійснюється відповідно до вимог Національного банку.

9.3. Допускається проведення зовнішнього аудиту аудиторською фірмою в межах аудиту щорічної перевірки фінансової звітності, консолідованої фінансової звітності та іншої інформації щодо фінансово-господарської діяльності.

9.4. ДІБ за результатами зовнішнього аудиту надає Національному банку відомості про результати зовнішнього аудиту (узагальнені результати оцінок стану захищеності об'єктів кіберзахисту та рівня відповідності СУІБ банку Національному стандарту України ДСТУ ISO/IEC 27001:2015), а також затверджений План заходів з усунення виявлених недоліків.

10. ВІДПОВІДАЛЬНІСТЬ ЗА РЕАЛІЗАЦІЮ ПОЛІТИКИ

10.1. Цією Політикою визначається позиція керівництва Банку щодо забезпечення ІБ, готовності до забезпечення необхідної підтримки при формуванні, прийнятті, впровадженні і супроводі даної Політики і СУІБ Банку.

10.2. Правління Банку відповідає за забезпечення необхідної підтримки для впровадження цієї Політики та функціонування СУІБ Банку.

10.3. Робоча група з управління ІБ є постійним колективним керівним органом Правління Банку, колективним керівним органом СУІБ, частиною Системи управління ризиками Банку. Увесь склад Робочої групи відповідальний за повноту та своєчасність належного виконання покладених на кожного обов’язків. Завдання, повноваження та відповідальність Робочої групи описано у Положенні про Робочу групу із захисту інформації АТ «ТАСКОМБАНК».

10.4. 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 ДІБ Банку.

10.5. Усі працівники Банку, незалежно від займаної посади, персонально відповідають за дотриманням вимог ІБ відповідно до чинного законодавства України, вимог НБУ та внутрішніх нормативних документів. Керівники підрозділів Банку додатково є відповідальними за порушення вимог ІБ і неправомірні дії підлеглих їм працівників в межах обов'язків з контролю за підлеглими, згідно посадових інструкцій. Кожен працівник Банку забезпечує підтримку належного рівня ІБ.

10.6. ДІБ відповідає за виконання наступних функцій:
- визначення вимог щодо налаштувань безпеки інформаційних систем банку;
- визначення внутрішніх нормативних вимог з ІБ;
- контроль за виконанням заходів із забезпечення безпеки інформації на всіх стадіях життєвого циклу інформаційних систем банку;
- розслідування інцидентів безпеки інформації;
- спільно з підрозділами інформаційних технологій (інформатизації, автоматизації) банку відповідає за відновлення функціонування інформаційних систем банку після збоїв у роботі внаслідок інцидентів безпеки інформації;
- методологічне забезпечення навчання з питань ІБ працівників Банку;
- забезпечення функціонування та використання засобів ІБ.

10.7. Працівники усіх підрозділів Банку є відповідальними за виконання і за порушення вимог Політики, законодавчих, регуляторних і внутрішньобанківських норм ІБ. Усі працівники під час прийому на роботу знайомляться з Політикою під підпис та дають зобов'язання про дотримання конфіденційності і таємниці страхування.

10.8. Підрозділом, відповідальним за ознайомлення персоналу з вимогами ІБ є ДІБ.

10.9. Підрозділом, відповідальним за ознайомлення персоналу з нормативними та розпорядчими документами з питань ІБ є Управління документаційного забезпечення та Управління по роботі з персоналом.

10.10. Підрозділом, відповідальним за навчання персоналу з питань ІБ є ДІБ та Навчальний центр.

10.11. Власник процесу. Відповідальність за розробку вимог ІБ, управління ризиком ІБ (в т.ч. кіберризиком), організацію виконання заходів ІБ, а також перегляд і актуалізацію даної Політики покладено на ДІБ, який є власником процесу.

10.12. Контроль процесу. Відповідальним за загальний контроль дотримання вимог цієї політики покладено на CISO.

11. ЗАКЛЮЧНІ І ПЕРЕХІДНІ ПОЛОЖЕННЯ

11.1. Політика погоджується Правлінням Банку, затверджується Наглядовою Радою Банку та набирає чинності з дати набуття чинності, зазначеної в протоколі Наглядової Ради.

11.2. Політика переглядається за необхідністю, але не рідше ніж один раз на рік. Позаплановий перегляд здійснюється у разі змін в інформаційній інфраструктурі та/або впровадженні в Банку нових інформаційних технологій, а також змін в законодавстві України чи нормативно-правових актах НБУ, які стосуються ІБ.

11.3. Підрозділом, відповідальним за підтримання Політики в актуальному стані, за своєчасне внесення змін та доповнень до Політики є ДІБ.

11.4. У разі зміни організаційної структури Банку Політика буде чинна з врахуванням зміни назв посад та зміни назв структурних підрозділів.

11.5. У разі невідповідності будь-якої частини Політики вимогам чинного законодавства України, в тому числі в зв'язку з прийняттям нових актів законодавства України та зміною чинних, Політика буде діяти лише в тій частині, що не суперечить чинному законодавству та чинним нормативним вимогам НБУ. До внесення відповідних змін в Політику, працівники Банку в своїй роботі повинні керуватися чинним законодавством України та нормативними вимогами НБУ.