Витяг з Політики
інформаційної безпеки АТ «ОТП БАНК»
затвердженої РП № 73 від 10.03.2026

Вступ

Інформація, яка створюється, обробляється або знаходиться у розпорядженні АТ «ОТП БАНК» (далі – **Банк**) у зв'язку з провадженням банківської діяльності, а також процеси обробки інформації та інформаційні активи, які використовуються цими процесами, є важливими бізнес-ресурсами, що мають цінність для Банку.

Сукупність законів, правил, обмежень, рекомендацій, інструкцій тощо, які регламентують порядок обробки інформації у Банку, у широкому розумінні складає політику інформаційної безпеки (**ІБ**) Банку.

Стан інформації, в якому забезпечується збереження конфіденційності, цілісності та доступності інформації, а також цілісності, спостережності та керованості процесів її обробки згідно з вимогами, визначеними політикою ІБ Банку, є безпечним і визначається терміном «інформаційна безпека Банку».

Головним завданням ІБ є мінімізація інформаційних ризиків Банку, що пов'язані з банківською діяльністю.

Система управління інформаційною безпекою Банку (**СУІБ**) є складовою системи управління Банком. Вимоги інформаційної безпеки враховуються в усіх процесах та видах діяльності Банку.

Мета

Метою Політики ІБ Банку є:

Запровадження загальних принципів та правил ІБ Банку згідно з вимогами законодавства України, нормативно-правових актів Національного банку України (**НБУ**), Адміністрації Державної служби спеціального зв'язку та захисту інформації України (**ДССЗЗІ**), міжнародної банківської Групи OTP Bank Group (надалі – **МБГ**), міжнародної платіжної системи SWIFT та стандартів України та міжнародних стандартів у галузі безпеки інформації (ДСТУ ISO/IEC 27001:2023 Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги; ISO/IEC 27001:2022; PCI DSS).

Досягнення максимально можливого рівня захищеності інформації при раціональному використанні ресурсів, збалансованому дотриманні бізнес-інтересів Банку та обмежень ІБ, що визначені вище вказаними вимогами.

Область дії

Дія цієї Політики поширюється на суб'єкти:

- персонал Банку (штатний, позаштатний, тимчасовий);
- окремі фізичні та юридичні особи, що перебувають у ділових або інших легітимних відносинах з Банком і мають доступ до інформаційних активів або можуть впливати на виконання процедур обробки інформації, що здійснюються Банком.

Дія цієї Політики поширюється на об'єкти, що є інформаційними активами Банку, зокрема:

- системи, обладнання, програмне забезпечення (**ПЗ**), засоби комунікацій, носії інформації, електронні дані, що мають для Банку цінність і впливають на властивості та рівень захисту інформації;
- процедури обробки, збереження, передачі інформації, власником яких є Банк, або які є предметом професійного, ділового, виробничого, комерційного та інших інтересів Банку.

Основні принципи ІБ Банку

Відповідність ІБ національному законодавству та регулятивним документам

Дотримання вимог законодавства України, нормативно-правових актів НБУ, ДССЗЗІ, МБГ, міжнародної платіжної системи SWIFT та стандартів України та міжнародних стандартів у галузі безпеки інформації.

Вимоги національних нормативно-правових актів мають пріоритет, водночас враховується необхідність гармонізації з вимогами європейського законодавства у сфері інформаційної та кібербезпеки;

Захист інформації та інформаційних активів Банку

Інформація, яка створюється, обробляється або знаходиться у розпорядженні Банку у зв'язку з провадженням банківської діяльності, а також процеси обробки інформації та інформаційні активи, що використовуються цими процесами, є важливими бізнес-ресурсами, що мають цінність для Банку.

Банк здійснює заходи щодо захисту інформації та інформаційних активів від загроз несанкціонованого використання, модифікації, знищення, блокування доступу, а також щодо забезпечення цілісності, керованості та спостереженості процесів обробки інформації.

Банк забезпечує, згідно з вимогами законодавства України, обмеження доступу до відомостей, що стосуються діяльності та фінансового стану клієнтів, а також неоприлюдненої інформації стосовно емітентів та їх цінних паперів, якщо ці відомості віднесено до категорії «банківська таємниця», «професійна таємниця» та «Інсайдерська інформація» відповідно.

Банк забезпечує, згідно з вимогами законодавства України, обмеження доступу до персональних даних, які обробляються у базах персональних даних Банку, стосовно яких він виступає у якості власника або розпорядника, за винятком персональних даних певних категорій громадян чи їх вичерпного переліку, віднесення яких до інформації з обмеженим доступом заборонено законодавством України.

Банк використовує право щодо обмеження доступу до відомостей, пов'язаних з його діяльністю, та оголошення їх комерційною таємницею або конфіденційною інформацію, якщо розголошення цих відомостей може завдати шкоди інтересам Банку, за винятком тих відомостей, які відповідно до законодавства України не можуть бути віднесені до комерційної таємниці, конфіденційної інформації або відомостей, доступ до якої не може бути обмежено.

Доступ до ІзОД працівникам Банку та працівникам–аутстаферам надається тільки за умов підписання ними зобов'язань щодо нерозголошення цієї інформації.

Доступ до ІзОД та іншої критичної інформації стороннім організаціям, що мають ділові відношення з Банком, надається тільки за умов наявності юридично значущих документів, які визначають вимоги ІБ та зобов'язання сторін стосовно захисту цієї інформації.

Вимоги ІБ щодо взаємодії Банку з іншими учасниками у складі платіжних систем будуються на підставі моделі взаємної недовіри.

Банк має право та зобов'язаний, у визначених законодавством України випадках, відстоювати із застосуванням всіх необхідних для цього легітимних заходів свої права та права власних клієнтів у випадках несанкціонованого розголошення ІзОД або інших несанкціонованих дій щодо критичної інформації або інформаційних активів, що знаходяться у розпорядженні Банку у зв'язку з провадженням банківської діяльності.

Банк дотримується принципу всеосяжного захисту. Цей принцип застосовується до всіх систем і врахований у фізичних, логічних і адміністративних заходах безпеки.

ІБ інформаційних систем та ІТ сервісів Банку

Комплексність та всебічність заходів захисту стосується усіх компонент ІТ систем і передбачає застосування превентивних, детективних, коригуючих заходів та засобів (принцип PreDeCo);

Принцип безперервного захисту означає, що здатність захисту, реалізована під час розгортання ІТ-систем, повинна підтримуватися та вдосконалюватися протягом усього її життєвого циклу.

Банк визнає пріоритетом при впровадженні ІТ сервісів та додатків, їхню відповідність вимогам інформаційної та кібербезпеки для підвищення кіберстійкості.

Банк створює та впроваджує інформаційні системи виходячі з принципу «security by design» та «security by default» у тому числі під час використання сервісів третіх сторін. Постачальники ІТ сервісів та систем мають продемонструвати відповідність цим принципам в рамках процедур вибору рішень, та звітувати в рамках співпраці. Банк залишає за собою право аудиту постачальників ІТ сервісів та систем в частині, що стосується безпеки інформаційної взаємодії та мінімізації ризиків третіх сторін при протидії кібератакам за ланцюжком постачальників. Відповідні положення повинні бути включені в договори про надання послуг та співробітництво з урахуванням ризик-орієнтованого підходу.

Принцип ізоляції гарантує, що застосовуються усі існуючі заходи захисту від усіх відомих і передбачуваних загроз.

Керування та забезпечення режиму ІБ Банку

Режим безпеки розуміється та безумовно підтримується керівництвом Банку.

Політика ІБ будується виключно на підставі виробничих інтересів Банку у відповідності до вимог законодавства України, нормативно-правових актів НБУ, ДССЗЗІ, МБГ, стандартів України та міжнародних стандартів у галузі безпеки інформації, вимог договорів, зобов'язань, що мають виконуватись Банком.

У Банку побудовано, підтримується та постійно вдосконалюється СУІБ у відповідності до вимог «ДСТУ ISO/IEC 27001:2023 Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою» та міжнародного стандарту ISO/IEC 27001:2022.

Питання ІБ є обов'язковим аспектом в роботі колегіальних та дорадчих органів Банку з питань впровадження інформаційних технологій та управління ризиками. Для цього до складу відповідних комітетів включаються представники підрозділу ІБ Банку.

Управління ризиками інформаційної безпеки та кіберризиками

Банк запроваджує і підтримує процеси збору інформації про актуальні кіберзагрози з аналітичних джерел та сервісів партнерів, визнає це першочерговим завдання щодо забезпечення належного рівня кіберстійкості.

Оцінка та оброблення ризиків інформаційної безпеки здійснюється, як у складі операційних ризиків, так і виходячи з впливу на такі властивості інформації як:

- конфіденційність;
- цілісність;
- доступність;
- спостережність.

Вартість заходів захисту має бути пропорційна існуючим ризикам для досягнення максимального захисту при раціональному використанні наявних ресурсів.

Усі ідентифіковані загрози мають бути покриті відповідними заходами захисту.

Застосування проактивного, agile-орієнтованого підходу, спрямоване на якнайшвидше вирішення проблем. Пріоритет віддається превентивним заходам захисту, які повинні доповнюватись потужними детектуючими можливостями щодо потенційних інцидентів (в рамках реалізації принципу PreDeCo).

Застосування проактивного і орієнтованого на вирішення проблем підходу щодо виявлення та управління проблемами на рівні МБГ за рахунок співпраці, прозорого обміну інформацією та ефективної комунікації на основі партнерства членів МБГ.

Обізнаність персоналу з питань ІБ

Всі працівники Банку повинні бути ознайомлені з вимогами ІБ, правильно розуміти та виконувати свої обов'язки та функції щодо забезпечення ІБ Банку.

Банк запроваджує програму розвитку обізнаності персоналу Банку, а також партнерів, що перебувають з Банком у договірних відносинах, щодо проблематики інформаційної та кібербезпеки. Основним напрямом підвищення обізнаності має бути впровадження спеціалізованих тренінгових програм, курсів для високо ризикованих категорій користувачів та партнерів.