Витяг з Політики
інформаційної безпеки
АТ «ОТП БАНК»

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 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.

Мета

Метою документу 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**), а також вимогами стандартів України та міжнародних стандартів у галузі безпеки інформації, зокрема ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2015; Cor 1:2014, IDT) та Payment Card Industry Data Security Standard (**PCI DSS**).

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, електроні 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.

Терміни та скорочення, що використовуються в даному документі

Банк – АТ «ОТП БАНК»

ІБ – інформаційна безпека.

ІзОД – інформація з обмеженим доступом.

НБУ – Національний банк України.

СЗІ – система захисту інформації.

Система ІТ – система інформаційних технологій.

СУІБ – система управління інформаційною безпекою.

Основні принципи ІБ 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.

- Головним завданням ІБ є мінімізація інформаційних ризиків Банку, що пов'язані з банківською діяльністю, відповідно до вимог політики безпеки Банку.

  Визначення цілей, розробка та реалізація стратегії і основних напрямків ІБ Банку, контроль їх виконання належить до компетенції та є прерогативою Правління Банку.
- Функції з керування та забезпечення режиму ІБ, а також розробки та актуалізації політики ІБ покладаються Правлінням Банку на окремий структурний підрозділ ІБ.
- Всі співробітники Банку повинні бути ознайомлені, правильно розуміти та виконувати свої обов'язки та функції щодо забезпечення ІБ Банку.
- Режим безпеки розуміється та безумовно підтримується керівництвом Банку.

  Політика ІБ Банку будується виключно на підставі його виробничих інтересів у відповідності до вимог законодавства України, Політики безпеки Групи ОТП, до складу якої входить Банк, вимог договорів, зобов'язань, що мають виконуватись Банком.
  У випадку виникнення розбіжностей, вимоги законодавства України мають пріоритет щодо вимог інших нормативних актів.
  Банк створює та постійно удосконалює систему управління інформаційною безпекою (СУІБ) відповідно до вимог національних та міжнародних стандартів і рекомендацій з урахуванням змін, що плануються і впроваджуються у бізнес-процесах Банку.
- Вся інформація, що знаходиться у розпорядженні Банку у зв'язку з провадженням банківської діяльності, класифікується за категоріями обмеження доступу та критичністю щодо здійсненням цієї діяльності.
- Банк має забезпечити, 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» та «Інсайдерська інформація» відповідно.
- Банк має забезпечити 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 співробітникам 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.
- Поширення персональних даних можливе лише за згодою фізичної особи, стосовно якої відповідно до закону здійснюється обробка її персональних даних.
- 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.

Основні цілі ІБ:

- забезпечення діяльності Банку з припустимим рівнем конфіденційності, цілісності та доступності інформації, а також спостереженості та керованості процесів її обробки, згідно з вимогами, визначеними цією Політикою;
- забезпечення постійної придатності, адекватності та ефективності СУІБ;
- відповідність процесів ІБ технічним рішенням, що використовуються Банком;
- врахування результатів оцінки та управління інформаційними ризиками в рамках впровадження ризик-орієнтованого підходу до вжиття заходів ІБ;
- відповідність процесів ІБ встановленій політиці ІБ Банку;
- забезпечення вимірювальності процесів ІБ.

Система захисту інформації

ІБ забезпечується шляхом застосування системи захисту інформації (СЗІ), яка реалізує цілі та вимоги політики ІБ Банку.
СЗІ має забезпечувати:

- неможливість відключення або обходу СЗІ;
- цілісність та неперервність захисту на всіх етапах життєвого циклу інформації;
- оптимальність на мінімальну достатність ступеня захисту;
- розмежування доступу та повноважень виконавців до інформаційних активів Банку та процесів обробки інформації за принципом мінімальної достатності (принцип «need-to-know»);
- мінімізацію кількості шлюзів між внутрішніми середовищами обробки інформації, що контролюються Банком, та зовнішніми неконтрольованими середовищами;
- побудову систем автоматизації Банку із застосуванням сучасних технологій та криптографічних алгоритмів захисту інформації, захищених операційних систем та систем керування базами даних;
- максимальний рівень захисту ключової інформації СЗІ;
- мінімізацію «людського фактору» в процесі застосування засобів захисту інформації.

Моніторинг СЗІ

Банком, на постійній основі, здійснюється моніторинг роботи СЗІ та критичних систем обробки інформації.
Банком запроваджується механізм оповіщення та реагування щодо інцидентів ІБ.
Банк декларує своє право та здійснює у межах, передбачених законодавством України, моніторинг дій персоналу та сторонніх організацій щодо доступу до ІзОД, критичної інформації та інформаційних активів Банку.

Аналіз інформаційних ризиків

Стратегія ІБ Банку ґрунтується на процесі керування інформаційними ризиками. Керування інформаційними ризиками є безперервним процесом, що передбачає оцінку, обробку та контроль інформаційних ризиків.
Банком на постійній основі здійснюється аналіз інформаційних ризиків та рівень відповідності СЗІ цим ризикам. Політика ІБ Банку підлягає періодичному перегляду та корегуванню, з метою урахування та мінімізації поточного рівня інформаційних ризиків.

Оцінка та обробка інформаційних ризиків

Банк запроваджує процес оцінки та управління ризиками інформаційної безпеки в рамках системи управління ризиками Банку.

Забезпечення безперервності діяльності

Банк превентивно планує заходи забезпечення безперервності банківської діяльності щодо обробки інформації, збереження критичної інформації та інформаційних активів, недопущення розголошення ІзОД Банку в умовах надзвичайних ситуацій. Плани безперервної діяльності затверджуються у порядку, визначеному внутрішніми регулятивними документами Банку та передбачають проведення комплексу заходів щодо збереження критичної інформації (в тому числі комерційної та банківської таємниці).

Зобов'язання Керівництва Банку щодо забезпечення інформаційної безпеки

Правління Банку, згідно з Положенням про Правління АКЦІОНЕРНОГО ТОВАРИСТВА «ОТП БАНК», в цілому визначає цілі, розробляє та реалізує стратегію і основні напрямки забезпечення ІБ як невід'ємної умови забезпечення діяльності Банку, а також здійснює контроль їх виконання.
Керівництво Банку повинно сприяти створенню, впровадженню, контролю та при необхідності підтримці СУІБ шляхом затвердження Стратегії ІБ, політик ІБ, а також прав та обов'язків у цій сфері. Таким чином, керівництво Банку підтверджує, що цілі ІБ визначені, СУІБ впроваджена та постійно удосконалюється, вимоги ІБ інтегровані в усі організаційні процеси.
Керівництво Банку забезпечує виділення ресурсів, необхідних для управління інформаційною безпекою, шляхом затвердження окремого бюджету.

Стратегія ІБ

Стратегія ІБ є складовою Стратегії комплаєнсу та безпеки Банку і визначає:

- концептуальні цілі ІБ, обсяг їх застосувань;
- принципи оцінки ризиків ІБ;

- основні принципи інформаційної безпеки, які визначають порядок впровадження, функціонування та використання інформаційних систем Банку;
- поширення вимог ІБ на весь персонал Банку та треті сторони;
- наявність системи централізованого управління і аудиту ІБ;
- принципи комплаєнсу, навчання та підготовки персоналу з питань ІБ;
- принципи розподілу завдань ІБ;
- зобов'язання реалізації встановлених вимог ІБ та постійного удосконалення СУІБ;
- забезпечувати настанови щодо рівня та захищеності інформації щодо усіх складових інформаційних систем стосовно фізичних, логічних та організаційних засобів та заходів захисту.

Формування політики ІБ

Політика ІБ містить вимоги ІБ щодо інформаційних систем, ресурсів та сервісів Банку, які повинні забезпечуватися на етапах розробки, впровадження, експлуатації та внесення змін в їх роботу.

Угода щодо конфіденційності

З метою забезпечення виконання вимог законодавства України, вимог договорів та зобов'язань, власних інтересів щодо обмеження несанкціонованого доступу до інформації, Банк застосовує механізм угоди щодо конфіденційності.

Цей механізм передбачає можливість надання доступу до ІзОД юридичним та фізичним особам, що мають ділові відношення з Банком, а також співробітникам Банку лише за умов попереднього узяття ними юридично значущих зобов'язань стосовно захисту та нерозголошення цієї інформації.

Взаємодія з державними органами та сторонніми організаціями з питань ІБ

Порядок взаємодії Банку з питань захисту інформації, що відбувається на постійній основі у процесі банківської діяльності з НБУ, іншими державними організаціями, платіжними та депозитарними системами регламентується законодавством України, регулятивними та розпорядчими документами Банку, а також умовами договорів, укладених між Банком та цими організаціями.

Процедура ідентифікації застосовного законодавства

Правовою основою політики ІБ Банку є Конституція України, закони України, нормативно-правові акти Президента України і Кабінету Міністрів України, а також інші державні нормативно-правові акти, що стосуються питань ІБ та визначають порядок здійснення банківської діяльності. Додатково до вказаних нормативно-правових актів, політика ІБ ґрунтується на вимогах стандартів України та міжнародних стандартів у галузі ІБ, нормативних документів з питань захисту інформації окремих платіжних систем, фінансових організацій, інших суб'єктів господарювання тощо, якщо така відповідність визначена вимогами законодавства України або умовами договорів, укладеними між Банком та цими суб'єктами господарювання.

Захист організаційних записів

Всі важливі організаційні записи (журнали аудиту, описи активів тощо), що стосуються керування СЗІ Банку, підлягають захисту від втрати, знищення та несанкціонованої модифікації.

Захист даних та конфіденційність персональних даних.

Персональні дані, що надані Банку у зв'язку зі здійсненням банківської діяльності його персоналом, а також клієнтами або будь-якою Зовнішньою стороною, є ІзОД і підлягають захисту згідно з вимогами законодавства України

Запобігання зловживанню засобами оброблення інформації

Банк декларує власне право здійснювати та здійснює контроль умов належного використання систем ІТ, а також моніторинг інформаційних потоків, що обробляються засобами цих систем.
Контроль використання систем ІТ, а також моніторинг інформаційних потоків запроваджується Банком виключно з метою захисту власних інтересів та виконання зобов'язань щодо інших суб'єктів банківської діяльності і здійснюється відповідно до вимог законодавства України.