Політика інформаційної безпеки АТ «Укрексімбанк»

Вступ

Політика інформаційної безпеки АТ «Укрексімбанк» (далі – Політика) описує та регламентує функціонування системи управління інформаційною безпекою (далі – СУІБ) та передбачає подальший розвиток заходів безпеки для зменшення інформаційних ризиків Банку.

Політика розроблена відповідно до вимог законодавства України, нормативно-правових актів Національного банку України, національних стандартах України з питань інформаційної безпеки ДСТУ ISO/IEC 27001:2015 "Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги" (далі - ДСТУ ISO/IEC 27001:2015), ДСТУ ISO/IEC 27002:2015 "Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки" (далі - ДСТУ ISO/IEC 27002:2015), які прийняті наказом Державного підприємства "Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості" від 18 грудня 2015 року N 193, Положенні про організацію заходів із забезпечення інформаційної безпеки в банківській системі України, що затверджене постановою Правління Національного банку України від 28.09.2017 №95, міжнародних промислових стандартів випуску платіжних карток (PSI DSS), а також нормативних документів міжнародних та національних платіжних систем та систем переказу коштів.

Терміни та скорочення

Інформаційна безпека – це захист інформації від широкого діапазону загроз з метою забезпечення безперервності бізнесу, мінімізації ризику бізнес-процесів і отримання максимальної рентабельності інвестицій і бізнес-можливостей.

Інформаційна безпека спрямована на збереження конфіденційності, цілісності та доступності інформації; забезпечує автентичність, спостережність, неспростовність для Банку та надійність автентифікації користувачів і інформаційних ресурсів.

Інформація з обмеженим доступом – це інформація, яка містить банківську, комерційну таємниці, конфіденційну інформацію, персональні дані, та інша інформація, яка віднесена до інформації з обмеженим доступом відповідно до чинного законодавства України, в тому числі нормативно-правових актів Національного банку України, а також внутрішніх нормативних документів Банку, угодами з клієнтами/контрагентами.

Інцидент інформаційної безпеки – одна або серія небажаних або непередбачуваних подій інформаційної безпеки, що мають значну ймовірність компрометації функціонування бізнесу і загрози інформаційній безпеці.

Критичний бізнес-процес – це процес, що обробляє Інформацію з обмеженим доступом, розголошення якої може нанести шкоду Банку.

Подія інформаційної безпеки – є ідентифікований стан інформаційного об‘єкту, системи, служби, мережі, який указує на можливе порушення політики інформаційної безпеки чи відмови засобів захисту або раніше невідому ситуацію, яка може мати відношення до безпеки.

Система управління інформаційною безпекою (СУІБ) – частина загальної системи управління, яка ґрунтується на підході, що враховує бізнес-ризики, призначена для розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та вдосконалення інформаційної безпеки.

Ціль документа

Ціллю Політики є впровадження та ефективне функціонування СУІБ, яка забезпечує захист інформації та ресурсів Банку від зовнішніх і внутрішніх загроз та загроз, які пов’язані з навмисними та ненавмисними діями працівників Банку, забезпечує безперервну роботу Банку, сприяє мінімізації ризиків операційної діяльності Банку та підтримання позитивної репутації Банку при роботі з клієнтами.

Сфера застосування

Політика розповсюджується на весь Банк у цілому та повинна використовуватися для всіх критичних бізнес-процесів/банківських продуктів Банку.

Предмет Політики

Основними принципами Політики є підтримання належного захисту інформації із забезпеченням цілісності, конфіденційності, доступності та спостережності. Це в першу чергу стосується Інформації з обмеженим доступом.

Банк підтримує ризик-орієнтовний підхід, який забезпечує розуміння, моніторинг та зменшення ризиків операційної діяльності. Деталі ризик-орієнтованого підходу описані в Політиці управління інформаційною безпекою., що затверджена в Банку.

Всі працівники Банку обізнані та виконують вимоги інформаційної безпеки в роботі. Під час розроблення, впровадження та функціонування програмно-технічних комплексів враховуються вимоги інформаційної безпеки.

Публічні сервіси та внутрішні мережі Банку відповідають вимогам стандартів з інформаційної безпеки.

Банк забезпечує виконання усіх вимог інформаційної безпеки, які наявні в угодах з третіми сторонами стосовно участі у міжнародних платіжних системах та системах переказу коштів.

У разі настання Інциденту інформаційної безпеки працівниками Банку здійснюються дії, що визначені Процедурою управління інцидентами інформаційної безпеки АТ «Укрексімбанк»., затвердженою в Банку.

Ролі та відповідальність

Керівництво Банку чітко розуміє, що інформаційна безпека є основою життєдіяльності Банку. У Банку створений постійно діючий колегіальний орган з питань інформаційної безпеки – Комітет з питань інформаційної безпеки (далі – Комітет), рішення якого є обов'язковими для виконання усіма працівниками Банку. Комітет забезпечує процес розроблення, впровадження, функціонування, моніторингу, перегляду, підтримання та вдосконалення СУІБ.

Комітет забезпечує визначення завдань інформаційної безпеки, їх відповідності вимогам чинного законодавства України, в тому числі нормативно-правовим актам Національного банку України, нормативним документам Банку, а також їх інтегрованості у бізнес-процеси та банківські продукти.

Комітет затверджує та переглядає Політику, аналізує ефективність її реалізації.

У своїй діяльності Комітет керується чинним законодавством України, у тому числі Законом України «Про банки і банківську діяльність», нормативно-правовими актами Національного банку України, Статутом Банку, а також внутрішніми нормативними документами, зокрема Положенням про комітет з питань інформаційної безпеки АТ «Укрексімбанк», та розпорядчими документами Банку.

Комітет здійснює контроль за діяльністю будь-яких самостійних структурних та відокремлених підрозділів Банку щодо виконання ними вимог чинного законодавства України, у тому числі нормативно-правових актів Національного банку України, а також внутрішніх нормативних та розпорядчих документів з питань інформаційної безпеки шляхом ініціювання перед Головою Правління Банку проведення перевірки самостійних структурних та відокремлених підрозділів Банку щодо дотримання ними вимог СУІБ.

Документи з питань інформаційної безпеки розробляються Управлінням захисту електронної інформації та іншими самостійними структурними підрозділами Банку, до функцій та завдань яких належать відповідне питання. Постійний контроль впровадження, виконання, вдосконалення та підтримки Політики в актуальному стані покладений на Комітет.

Керівництво Банку сприяє створенню, впровадженню, контролю та підтримці Політики.

Стратегія розвитку інформаційних технологій Банку, всі проекти, які пов'язані з інформаційними технологіями, узгоджуються з цією Політикою.

Кожен працівник Банку забезпечує підтримку відповідного рівня інформаційної безпеки Банку. Працівники Банку при виконанні своїх посадових обов'язків та повноважень повинні дотримуватись вимог законодавчих та підзаконних нормативно-правових актів, зокрема, Політики, і несуть відповідальність за не дотримання їх положень згідно із чинним законодавством України та нормативними документами Банку. Для зменшення ризиків виникнення Інцидентів інформаційної безпеки керівництво Банку створює умови для систематичного навчання працівників Банку нормам та заходам інформаційної безпеки.

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

Усі нормативні документи Банку з питань інформаційної безпеки доступні працівникам Банку у межах їх повноважень і призначені надавати допомогу працівникам Банку з метою дотримання ними вимог інформаційної безпеки АТ «Укрексімбанк».

Перегляд Політики

Політика підтримується в актуальному стані та переглядається за необхідності, але не менш ніж один раз на рік. Причинами внесення змін до Політики є зміни в інформаційній інфраструктурі та/або впровадження нових інформаційних технологій, а також зміни у чинному законодавстві України.