Службова інформація

«ЗАТВЕРДЖЕНО»
Рішенням Спостережної ради
ПАТ «БАНК ІНВЕСТИЦІЙ
ТА ЗАОЩАДЖЕНЬ»
від «__ »_____2017р. №
Голова Спостережної ради
_____ В.І. Зінченко

«ПОГОДЖЕНО»
Рішенням Правління
ПАТ «БАНК ІНВЕСТИЦІЙ
ТА ЗАОЩАДЖЕНЬ»
від «__» _____ 2017 р. № __/____
Голова Правління
_____ О.В. Омельченко

Політика
інформаційної безпеки
ПАТ «БАНК ІНВЕСТИЦІЙ ТА ЗАОЩАДЖЕНЬ»

Вступ

Політика інформаційної безпеки ПАТ «БАНК ІНВЕСТИЦІЙ ТА ЗАОЩАДЖЕНЬ» (далі - Політика) описує та регламентує функціонування системи управління інформаційною безпекою (далі – СУІБ) відповідно до стандартів Національного банку України СОУ Н НБУ 65.1 СУІБ 1.0:2010 та СОУ Н НБУ 65.1 СУІБ 2.0:2010, відповідає вимогам законодавства України та нормативно-правовим актам Національного банку України, вимогам міжнародних та внутрідержавних платіжних систем та систем переказу коштів, а також вимогам внутрішніх документів ПАТ «БАНК ІНВЕСТИЦІЙ ТА ЗАОЩАДЖЕНЬ» (далі – Банк).

Ціль політики

Ціллю Політики є впровадження та ефективне функціонування системи управління інформаційною безпекою, яка буде забезпечувати захист інформації та ресурсів Банку від зовнішніх і внутрішніх загроз та загроз, які пов'язані з навмисними та ненавмисними діями працівників Банку, забезпечувати безперервну роботу Банку, сприяти мінімізації ризиків операційної діяльності Банку та створювати позитивну репутацію Банку при роботі з клієнтами.

Основним завданням інформаційної безпеки є захист інформаційних ресурсів Банку від зовнішніх та внутрішніх, навмисних та ненавмисних загроз.

Сфера застосування

Політика розповсюджується на Банк у цілому та використовується 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, яка відноситься до "банківської таємниці", "комерційної таємниці", "персональних даних" та іншої конфіденційної інформації.

Банк підтримує ризик-орієнтовний підхід, який забезпечує розуміння, моніторинг та зменшення ризиків операційної діяльності. Деталі ризик-орієнтовного підходу описані в окремому внутрішньому документі.

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 банку та внутрішні мережі Банку відповідають вимогам стандартів з інформаційної безпеки.

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

Для зменшення ризиків виникнення інцидентів інформаційної безпеки Керівництво Банку створює працівникам умови для систематичного навчання нормам та заходам інформаційної безпеки.

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

Ролі та відповідальності

Керівництво Банку чітко розуміє, що інформаційна безпека Банку є основою життєдіяльності Банку та сприяє впровадженню, контролю та підтримці вимог прийнятої Політики.

У Банку створений та постійно працює колегіальний орган - Комісія з питань системи управління інформаційною безпекою (далі - Комісія) Публічного акціонерного товариства «БАНК ІНВЕСТИЦІЙ ТА ЗАОЩАДЖЕНЬ», рішення якої є обов'язковими для виконання усіма працівниками Банку.

Документи з питань системи управління інформаційною безпекою розробляються структурними підрозділами за відповідними напрямками діяльності та доступні працівникам Банку у межах їх повноважень і призначені надавати допомогу у виконанні вимог інформаційної безпеки.

Постійний контроль впровадження, виконання, вдосконалення та підтримки Політики в актуальному стані покладений на Комісію.

Кожен працівник Банку забезпечує підтримку відповідного рівня інформаційної безпеки Банку в межах своїх службових обов'язків та повноважень, несе відповідальність за їх порушення згідно із законодавством України та внутрішньобанківськими нормативними документами.

Перегляд документа

Виконується робота щодо підтримки Політики інформаційної безпеки в актуальному стані. Політика переглядається за необхідністю, але не менш ніж одного разу на рік. Причинами внесення змін до Політики є зміни в інформаційної інфраструктурі та/або впровадженні нових інформаційних технологій, а також змінах в законодавчих, регуляторних та інших нормах.