Республиканское государственное предприятие «Казахстанский центр межбанковских расчетов Национального Банка Республики Казахстан»

Утверждена
Приказом РГП «КЦМР»
от «15» декабря 2017 года
№ 164-П

ПОЛИТИКА
информационной безопасности

Рег. № 4675-8/77

г. Алматы

Глава 1. Общие положения и область применения

1. «Казахстанский центр межбанковских расчетов Национального Банка Республики Казахстан» (далее – КЦМР) является юридическим лицом, организацией государственного учреждения Национальный Банк Республики Казахстан в форме республиканского государственного предприятия на праве хозяйственного ведения, основной целью деятельности которого является проведение межбанковских платежей и переводов денег, межбанковского клиринга в соответствии с законодательством Республики Казахстан. Деятельность КЦМР заключается в предоставлении услуг, связана с обработкой и хранением информации, являющейся важным информационным активом, и требует обеспечения информационной безопасности, под которой понимается обеспечение доступности, целостности и конфиденциальности информации.

2. Настоящая Политика информационной безопасности КЦМР (далее – Политика) разработана в соответствии с Политикой информационной безопасности Национального Банка Республики Казахстан, законодательством Республики Казахстан в области информационной безопасности и международным стандартом ISO/IEC 27001[1].

3. Руководство КЦМР осознает важность и осуществляет управление информационной безопасностью, обеспечивая необходимые условия развития, совершенствования мер и средств защиты информационных активов в контексте угроз информационной безопасности, развития законодательства и норм регулирования деятельности КЦМР.

Глава 2. Цель

4. Целью настоящей Политики является определение единого подхода в обеспечении информационной безопасности в КЦМР, направленного на организацию защиты информации вне зависимости от формы и места ее обработки и хранения, средств ее обработки.

Глава 3. Основные положения

5. Для достижения цели настоящей Политики в КЦМР внедряется система управления информационной безопасностью (далее – СУИБ), которая позволит:

- гарантировать достаточность мер и непрерывность защиты информационных активов КЦМР от угроз информационной безопасности;
- поддерживать структурированную и всестороннюю систему идентификации и оценки рисков информационной безопасности,

[1] Международный стандарт ISO/IEC 27001 Информационная технология. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.

выбора и применения соответствующих средств защиты, управления, измерения и улучшения их эффективности;

- непрерывно улучшать среду контроля;
- соответствовать юридическим и регулирующим требованиям.

6. В КЦМР выбор средств и мер защиты информационных активов с целью минимизации возможных потерь строится на основе идентификации и оценке рисков информационной безопасности.

7. Работники КЦМР, ответственные за организацию и осуществление мероприятий по обеспечению информационной безопасности и процессов обработки и хранения информации, регулярно проходят соответствующее обучение в области информационной безопасности.

Глава 4. Ответственность и контроль

8. Руководство КЦМР осуществляет общий контроль и несет персональную ответственность за выполнение целей и основных положений настоящей Политики, в т.ч. за предоставление необходимых условий и ресурсов для достижения целей настоящей Политики, а также принимает на себя обязательства по постоянному улучшению и выполнению применимых требований СУИБ.

9. Управление информационной безопасностью в повседневной деятельности возлагается на начальника управления безопасности, который несет персональную ответственность за реализацию настоящей Политики, а также за непрерывный контроль выполнения установленных в КЦМР требований и мероприятий информационной безопасности.

10.Все работники КЦМР несут персональную ответственность за нарушение и/или невыполнение установленных требований и мероприятий по защите информации и средств ее обработки, и обязаны сообщать обо всех выявленных нарушениях и инцидентах в ответственное за обеспечение безопасности подразделение.

11.Должностные инструкции всех работников КЦМР должны содержать требования по обеспечению и соблюдению информационной безопасности.

Глава 5. Другие положения

12. Политика подлежит ежегодному пересмотру, в случае существенных изменений в деятельности КЦМР, а так же требований законодательства Республики Казахстан или регулирующих органов, влияющих на СУИБ, незамедлительно.

13.Политика является общедоступным документом и размещается на официальном сайте КЦМР.