Акционерное общество «Национальная платежная корпорация Национального Банка Республики Казахстан»

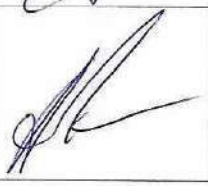
Утверждена
решением Совет директоров
АО «НПК»
от «21» 11 2023 года
(протокол № 3)

Политика информационной безопасности
Рег. № 11

г. Алматы

Должность, подразделение разработчика	ФИО	Подпись	Дата
Главный сотрудник отдела информационной безопасности	Курмалаев А.Т.		

ЛИСТ СОГЛАСОВАНИЯ

№ п/п	Должность	Ф.И.О. согласователя	Подпись	Дата
1	Начальник управления информационной безопасности	Муканов Т.Л.		
2	Управляющий директор – директор Департамента по развитию продуктов	Абдрашев Р.А.		
3	Директор Департамента Информационных технологий	Кандалов С.В.		
4	Начальник управления удостоверяющего центра	Третьяков П.С.		
5	Начальник управления правового обеспечения	Бабагалиева Б.К.		

Содержание

Глава 1. Общие положения

1. Политика информационной безопасности (далее - Политика) является основополагающим документом, отражающим основные взгляды и принципы в обеспечении информационной безопасности в Акционерном обществе «Национальная платежная корпорация Национального Банка Республики Казахстан» (далее – АО «НПК»).

2. Политика разработана в соответствии с законами Республики Казахстан «О Национальном Банке Республики Казахстан», «О национальной безопасности Республики Казахстан» и «Об информатизации», а также стандартом Республики Казахстан СТ РК ISO/IEC 27001.

3. Орган управления АО «НПК» осознает важность и необходимость создания, развития и постоянного совершенствования системы управления информационной безопасностью (далее – СУИБ) в контексте существующих рисков информационной безопасности и совершенствования законодательства.

Глава 2. Цели и задачи

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

5. Основными задачами для выполнения цели Политики являются:

1) обеспечение целостности, доступности информационных активов и защиты конфиденциальной информации АО «НПК» и третьих сторон, связанной с деятельностью АО «НПК»;

2) выявление, предупреждение и нейтрализация реальных и потенциальных угроз ИБ, а также установление причин и условий их возникновения;

3) минимизация и локализация последствий при воздействии угроз информационной безопасности, оценка и всесторонний анализ инцидентов для дальнейшего предотвращения;

4) анализ соответствия правовых аспектов деятельности в области информационной безопасности и постоянная актуализация требований внутренних нормативных документов;

5) повышение корпоративной культуры работников и их осведомленности в области обеспечения информационной безопасности;

6) контроль эффективности и достаточности применяемых мер защиты информации и средств ее обработки.

6. Основные направления по реализации Политики и соблюдению требования информационной безопасности в АО «НПК» осуществляются за счёт:

- реализации организационных и технических мер защиты;
- исполнения законодательных и регуляторных требований, а также применимых требований государственных и международных стандартов в области обеспечения информационной безопасности;
- разработки и соблюдения внутренних нормативных документов регулирующих различные аспекты обеспечения информационной безопасности,

включая, но не ограничиваясь, порядок наделения полномочиями доступа, работу с защищаемыми ресурсами, паролями, обращение с информацией и ее носителями, программным обеспечением и его обновлениями, резервным копированием, доступом к внутренним и внешним сетевым ресурсам, работу с системами анализа защищенности, обнаружения и предотвращения атак, антивирусной защиты, процесс анализа исходного кода, обеспечение пожарной безопасности, использование прочих средств защиты и обеспечения информационной безопасности.

Глава 3. Основные положения системы управления информационной безопасностью

7. Для достижения цели настоящей Политики АО «НПК» усовершенствует СУИБ.

8. Функционирование СУИБ должно осуществляться в соответствии со следующими основными принципами:

1) законность – любые действия, предпринимаемые для обеспечения информационной безопасности, осуществляются на основе действующего законодательства, с применением всех дозволенных законодательством методов обнаружения, предупреждения, локализации и пресечения негативных воздействий на объекты защиты АО «НПК»;

2) комплексность – обеспечение безопасности информационных ресурсов в течение всего их жизненного цикла, на всех технологических этапах их использования и во всех режимах функционирования;

3) персональная ответственность – руководители всех уровней и исполнители должны быть осведомлены о всех требованиях обеспечения информационной безопасности и несут персональную ответственность за выполнение этих требований и соблюдение установленных мер информационной безопасности;

4) взаимодействие и координация – меры информационной безопасности осуществляются на основе взаимосвязи соответствующих структурных подразделений АО «НПК», координации их усилий для достижения поставленных целей, а также установления необходимых связей с внешними организациями, профессиональными ассоциациями и сообществами, государственными органами.

9. В АО «НПК» выбор технических средств и организационных мер защиты информационных активов с целью минимизации возможных потерь строится на основе идентификации и оценке рисков информационной безопасности.

10. Область действия СУИБ распространяется на все самостоятельные структурные подразделения АО «НПК», а также на организации и учреждения, взаимодействующие с АО «НПК», в качестве поставщиков и (или) потребителей информационных ресурсов АО «НПК».

11. Работники АО «НПК», 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

12. Председатель Правления АО «НПК» принимает на себя ответственность за реализацию настоящей Политики, осуществляет контроль 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.

13. Управление информационной безопасностью в повседневной деятельности возлагается на начальника подразделения безопасности, который несет персональную ответственность за реализацию настоящей Политики.

14. Управление безопасности несет ответственность за поставленные руководством АО «НПК» цели и задачи, а также контроль выполнения требований, отраженных в документах СУИБ. Все исключения из этих требований в обязательном порядке согласовываются с ответственным структурным подразделением.

15. Руководители структурных подразделений и работники АО «НПК» несут ответственность за безусловное полное выполнение своих обязанностей по поддержанию деятельности по обеспечению и выполнению требований ИБ в соответствии с документами СУИБ, а представители третьих сторон, имеющие доступ к информационным ресурсам и конфиденциальной информации АО «НПК» - в соответствии с договорными обязательствами.

16. Все работники АО «НПК» несут персональную ответственность за нарушение и/или невыполнение установленных во внутренних документах АО «НПК» 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.

17. Внутренние документы АО «НПК», в том числе должностные инструкции всех работников должны содержать требования по обеспечению и соблюдению информационной безопасности.

Глава 5. Заключительные положения

18. Политика подлежит ежегодному пересмотру, а в случае существенных изменений в деятельности АО «НПК», а также требований законодательства Республики Казахстан или регулирующих органов, влияющих на СУИБ, незамедлительно.

19. Подразделение информационной безопасности доводит настоящую Политику до сведения всех работников АО «НПК».

20. Политика является общедоступным документом и размещается на официальном сайте АО «НПК».