

Приложение
к Приказу АО «Казахтелеком»
от «__» _____ 2025 года
№ _____

Политика информационной безопасности
АО "Казахтелеком"

Алматы, 2025

Оглавление

Глава 1. Общие положения.....	3
Глава 2. Основные цели и задачи.....	3
Глава 3. Основные принципы обеспечения ИБ.....	5
Глава 4. Ответственность и намерения руководства	5
Глава 5. Заключительные положения	6

Глава 1. Общие положения

1. Политика информационной безопасности (далее – Политика) – комплекс превентивных мер по защите информации, в том числе информации с ограниченным распространением (служебная информация), информационных процессов и включает в себя требования в адрес пользователей информационных систем АО «Казахтелеком» (далее - Общество), его филиалов и структурных подразделений в своей деятельности.

2. Политика разработана с целью определения стратегических целей, задач и основных требований к комплексу мер в области информационной безопасности (далее – ИБ), как одному из критичных факторов успешной и стабильной работы Общества, обеспечению устойчивости функционирования информационных систем (далее - ИС) и сохранности информации, обеспечению всесторонней защиты интересов Общества, его работников, а также третьих лиц, контрагентов от угроз в сфере информационных технологий.

3. Политика является основополагающим документом, отражающим видение и намерения руководства Общества в области ИБ, устанавливает цели, задачи и принципы в области ИБ, которыми руководствуется Общество в своей деятельности. Служит руководством при разработке соответствующих документов системы управления информационной безопасностью (далее – СУИБ);

4. Нормативно-правовую основу Политики составляют требования положений законодательства Республики Казахстан (далее – РК) по вопросам использования ИС и ИБ, а также требования международных стандартов управления ИБ (ISO/IEC 27000, ITIL).

5. Под ИБ в рамках данного документа, Общество понимает состояние защищенности своих интересов (целей) от угроз в сфере информационных технологий (далее - ИТ). Защищенность достигается обеспечением совокупности свойств информационных активов: конфиденциальности, целостности и доступности.

6. Обеспечение ИБ Общества осуществляется в рамках циклической модели менеджмента ИБ: «планирование — реализация — проверка — совершенствование», отвечающей принципам и модели корпоративного менеджмента в Обществе.

7. Политика является общедоступным документом, который может предоставляться без ограничений всем заинтересованным сторонам.

Глава 2. Основные цели и задачи

8. Политика направлена на достижение основных целей:

- 1) обеспечение доступности информационных активов Общества для поддержки его бизнес-процессов;
- 2) защиту целостности информационных активов Общества в целях поддержки высокого качества бизнес-процессов;
- 3) сохранение конфиденциальности информации Общества и иных сторон;

4) обеспечение непрерывности основных бизнес-процессов, функционирующих в Обществе;

5) соответствие предпринимаемых мер по информационной безопасности, применяемых в Обществе, требованиям законодательства, а также требованиям регулирующих и надзорных органов.

9. Основные задачи по реализации Политики - планирование, реализация и контроль за выполнением комплекса организационных и технических мер по обеспечению ИБ на основе оценки рисков Общества в сфере ИТ, направленных на:

1) защиту информации от реальных и потенциальных современных киберугроз;

2) предупреждение, выявление и деактивацию различных современных киберугроз;

3) установление причин и условий возникновения киберугроз;

4) быстрое реагирование на воздействие современных угроз и их точная локализация;

5) минимизацию ущерба от событий, таящих угрозу безопасности информации, посредством их предотвращения или сведения их последствий к минимуму;

6) применение современных международных методологий и практик по совершенствованию механизмов оперативного реагирования и расследования киберугроз;

7) эффективное управление рисками ИБ;

8) обеспечение осведомленности работников о Политике, предпринимаемых мерах, требованиях по обеспечению ИБ, обязанностях и правилах поведения, возлагаемых на работников, а также обеспечение контроля за их надлежащим выполнением;

9) повышение уровня знаний и развитие корпоративной культуры в области ИБ;

10) совершенствование СУИБ;

11) обеспечение соблюдения требований законодательства РК в ходе деятельности по обеспечению ИБ Общества.

12) ведение практики дисциплинарного взыскания в случае нарушения Политики.

10. Для достижения указанных целей и решения перечисленных задач в Обществе строится СУИБ, соответствующая требованиям:

1) законодательства РК и стандартов в области ИБ;

2) международных стандартов ИСО/МЭК в области ИБ;

3) нормативно-регламентирующих документов регулятора;

4) нормативно-регламентирующих документов Общества, договорных обязательств и иных нормативных документов в области ИБ.

СУИБ, являясь частью общей системы управления Общества, документирована в настоящей Политике, а также других документах СУИБ (частные правила, требования, регламенты, руководства, стандарты, инструкции, положения, процедуры и т.п.), детализирующих, развивающих положения, изложенные в

настоящей Политике на уровне их практической реализации и являющихся обязательными для всех работников Общества, а также представителей третьих сторон, имеющих доступ к информационным ресурсам Общества.

Глава 3. Основные принципы обеспечения ИБ

11. В основу Политики заложены следующие базовые принципы:

- 1) законность обеспечения ИБ;
- 2) вовлеченность высшего руководства Общества в процесс обеспечения ИБ;
- 3) ориентированность на бизнес;
- 4) процессный подход;
- 5) комплексное использование способов, методов и средств защиты информации;
- 6) следование лучшим практикам;
- 7) разумная достаточность;
- 8) информированность и персональная ответственность.

Глава 4. Ответственность и намерения руководства

12. Обеспечение ИБ Общества достигается реализацией комплекса необходимых процессов и мер, поддерживаемых каждым СП и работником Общества в необходимой и определенной для него мере в соответствии с правилами и требованиями внутренних документов по обеспечению ИБ Общества.

13. Руководство Общества стремится обеспечить эффективную и стабильную работу Общества, а также поддержать уверенность всех заинтересованных сторон в надежности и стабильности работы Общества, в защищенности их интересов от воздействия различных неблагоприятных факторов.

14. К руководству Общества относятся:

- 1) Председатель Правления и члены Совета директоров;
- 2) Первый Заместитель Председателя Правления, Члены Правления;
- 3) Главные и Управляющие директора;
- 4) Генеральные директора Дивизионов - филиалов и структурных подразделений (далее – СП);
- 5) Руководители СП.

15. Руководство Общества принимает на себя ответственность за реализацию настоящей Политики.

16. Руководство стремится организовать деятельность по обеспечению ИБ в соответствии с законодательством Республики Казахстан, стандартами, такими как СТ РК ИСО/МЭК 27001, НРД Общества и лучшими практиками.

17. Руководство Общества стремится к достижению поставленной цели путем создания, поддержки, контроля и развития эффективной СУИБ, основывающейся на сбалансированном комплексе организационных и технических мер по обеспечению ИБ.

18. Руководители функциональных блоков, СП, работники Общества несут ответственность за выполнение своих обязанностей по обеспечению поддержания деятельности и исполнение требований ИБ в соответствии с документами СУИБ.

19. Ответственность Представителей третьих сторон, имеющих доступ к информационным ресурсам Общества, должна быть предусмотрена в договорных обязательствах сторон.

Глава 5. Заключительные положения

20. Положения настоящей Политики подлежат пересмотру по мере необходимости, согласно результатам проведения внешнего аудита, внутреннего анализа и оценки рисков ИБ для информационной системы Общества, в результате каких-либо изменений в деятельности Общества, изменений в законодательстве РК, но не реже одного раза в два года.

21. Если в результате изменения законодательства РК нормы настоящей Политики вступают в противоречие с действующим законодательством, эти нормы Политики утрачивают силу и до момента внесения изменений, дополнений в настоящую Политику необходимо руководствоваться действующим законодательством Республики Казахстан.

22. Вопросы, не предусмотренные в положениях Политики, разрешаются в соответствии с законодательством РК, внутренними документами и решениями Правления Общества (при этом законодательство РК имеет преваляющую силу).

23. Несоблюдение порядка и правил использования информационных ресурсов и принятых в Обществе мер ИБ влечет за собой ответственность в соответствии с действующим законодательством РК и внутренними нормативными документами Общества.

24. Содержание настоящей Политики должно быть доведено до сведения работников Общества в порядке, определенном нормативными документами и процедурами Общества.

25. Настоящая Политика ИБ вступает в силу с момента ее утверждения Председателем Правления Общества и действует до принятия новой Политики ИБ.

26. Ответственность за внесение изменений в Политику несет Управляющий директор по информационной безопасности.

27. Контроль за доведением требований пунктов данной Политики до руководителей СП Общества возлагается на Управляющего директора по информационной безопасности. Контроль за ознакомление работников Общества с данным документов лежит на руководителях филиалов и руководителях СП Общества.

28. Настоящая Политика размещается на официальном веб-сайте Общества.