АО «Транстелеком»

УТВЕРЖДЕНА
Решением Правления
АО «Транстелеком»
«25» 09 2025 года
№ 15/2025

Политика информационной безопасности АО «Транстелеком»

П ISM-01-07/25

Астана, 2025 год

1. Общие положения

1.1. Настоящая Политика информационной безопасности (далее - Политика) представляет собой основной документ в области защиты информации в АО «Транстелеком» (далее - Общество) и определяет общие направления обеспечения информационной безопасности (далее - ИБ) во всех областях деятельности Общества и на всех участках его информационного и инфраструктурного информационно-технологического оборудования с учетом особенности деятельности Общества, его организационной структуры, размещения информационных систем и их структуры функционирования и характера выполняемых задач.

1.2. Политика разработана на основе следующих нормативных правовых актов и нормативных документов Республики Казахстан, международных и национальных стандартов:

- Закон Республики Казахстан от 24 ноября 2015 года № 418-V ЗРК «Об информатизации»;
- Закон Республики Казахстан от 21 мая 2013 года № 94-V «О персональных данных и их защите»;
- Закон Республики Казахстан от 7 января 2003 года № 370 «Об электронном документе и электронно-цифровой подписи»;
- Закон Республики Казахстан от 5 июля 2004 года № 567 «О связи»;
- Закон Республики Казахстан от 6 января 2012 года № 527-IV «О национальной безопасности Республики Казахстан»;
- Постановление Правительства Республики Казахстан от 20 декабря 2016 года №832 «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности»;
- Международный стандарт безопасности данных индустрии платежных карт (PCI DSS 4.0);
- Международный стандарт ISO/IEC 27001-2022 «Информационная безопасность, кибербезопасность и защита персональных данных – Системы менеджмента информационной безопасности – Требования»;
- Национальный стандарт СТ РК ISO/IEC 27002-2023 «Информационная безопасность, кибербезопасность и защита конфиденциальности. Средства управления информационной безопасностью».

2. Цели и принципы Политики

2.1. Политика определяет цели, принципы и основные направления обеспечения ИБ в Обществе.

2.2. Политика разрабатывается и применяется в целях реализации бизнес-стратегии и поддержки бизнес-процессов Общества.

2.3. Политика распространяется на все процессы, информационных систем, данные, информационные и телекоммуникационные технологии Общества и дочерних организаций, а также на всех работников Центрального аппарата и

филиалов Общества, подрядчиков и третьих лиц, имеющих доступ к информационным и инфраструктурному информационно-технологическому оборудованию Общества.

2.4. Общество рассматривает ИБ как стратегический фактор устойчивого развития, обеспечивая защиту данных, соответствие нормативным требованиям и сохранения доверия клиентов и партнеров.

2.5. Взаимосвязь ИБ с бизнес-стратегией Общества заключается в поддержке ключевых направлений бизнес-стратегии, включая:

- непрерывность бизнес-процессов – защита критически важных сервисов и минимизация простоев;
- доверие клиентов – обеспечение конфиденциальности и защиты персональных данных;
- соответствие требованиям рынка в области телекоммуникационных и отраслевых услуг;
- выполнение регуляторных требований, международных и национальных стандартов в сфере информатизации и обеспечения ИБ.

2.6. Политика основана на следующих принципах:

- системный подход – интеграция ИБ во все процессы Общества;
- конфиденциальность, целостность и доступность – обеспечение защиты данных от несанкционированного доступа, изменений и потерь;
- риск-ориентированное управление – непрерывный анализ и минимизация рисков;
- минимально необходимый доступ – ограничение доступа к данным и системам на основе бизнес-необходимости;
- непрерывное совершенствование – постоянное развитие мер защиты.

2.7. Действия системы управления ИБ охватывают следующие направления: «Управление информационной безопасностью при проектировании, разработке, строительстве, внедрении, эксплуатации, сервисном обслуживании инфраструктуры, мониторинге, анализе и оказании услуг в сфере телекоммуникаций и информационных технологий, включая услуги информационной безопасности».

2.8. Обеспечение системы управления ИБ (далее - СУИБ) Общества осуществляется в рамках циклической модели (цикл Деминга «PDCA Plan-Do-Check-Act») менеджмента информационной безопасности: «планирование - реализация - проверка - совершенствование», отвечающей принципам и модели корпоративного менеджмента в Обществе.

3. Ответственность и обязательства

3.1. Руководство Общества:

3.1.1. Определяет цели и приоритеты в области обеспечения ИБ.

3.1.2. Обеспечивает выделение необходимых ресурсов (финансовых, технологических, кадровых) для реализации мероприятий по ИБ.

3.1.3. Демонстрирует лидерство, приверженность целям и принципам обеспечения ИБ и оказывает необходимое содействие.

3.1.4. Обеспечивает определение и распространение в Обществе обязанностей и полномочий в области ИБ.

3.1.5. Инициирует идеи, планы и программы по поддержанию осведомленности по ИБ, определяет потребность в обучении по процедурам обеспечения ИБ.

3.2. Подразделение по информационной безопасности:

3.2.1. Разрабатывает, внедряет и актуализирует политику и нормативные документы в области ИБ.

3.2.2. Организует процессы управления СУИБ.

3.2.3. Взаимодействует с государственными регуляторами и отраслевыми организациями в сфере ИБ.

3.2.4. Осуществляет координацию работ по обеспечению ИБ и контролю за исполнением требований ИБ, определенных во внутренних нормативных документах ИБ.

3.2.5. Работники подразделения ИБ, проходят специализированные курсы в сфере обеспечения ИБ, не реже одного раза в три года с выдачей сертификата.

3.3. Подразделение по информационным технологиям (далее - ИТ):

3.3.1. Обеспечивает безопасную эксплуатацию, сопровождение и модернизацию ИТ-инфраструктуры.

3.3.2. Реализует технические меры защиты, включая управление доступом, резервное копирование, обновление программного обеспечения и устранение уязвимостей.

3.4. Оперативный центр информационной безопасности (далее – ОЦИБ):

3.4.1. Обеспечивает круглосуточный мониторинг событий информационной безопасности.

3.4.2. Реагирует на инциденты ИБ, проводит их классификацию и анализ причин возникновения.

3.4.3. Осуществляет мониторинг уязвимостей и анализ технической защищенности ИТ-инфраструктуры и информационных систем Общества.

3.4.4. Осуществляет взаимодействие с Национальным координационным центром информационной безопасности Республики Казахстан и регулирующими органами при обработке инцидентов и правоохранительными органами при расследовании кибератак.

3.5. Работники Общества обязаны:

- соблюдать Политику, внутренние регламенты и процедуры безопасности;
- немедленно сообщать в ОЦИБ и подразделению ИБ о подозрительных действиях, инцидентах и возможных нарушениях безопасности;
- соблюдать правила управления доступом, паролями и безопасного обращения с конфиденциальной информацией;

- использовать доступные в Обществе механизмы и средства для обеспечения защиты обрабатываемой и хранимой информации;
- выполнять процедуры, необходимые для предупреждения проникновения, обнаружения и уничтожения компьютерного вируса;
- соблюдать принцип «чистого стола» в отношении бумажных документов, съемных информационных носителей и электронных средств обработки информации.

3.5.1. Все работники Общества несут ответственность за разглашение сведений, составляющих служебную, коммерческую или иную охраняемую законом тайну, утрату документов, носителей информации, содержащих вышеуказанные сведения, в соответствии с законодательством Республики Казахстан.

3.5.2. Владельцы бизнес-процессов в Обществе, принимают участие в разработке, пересмотре и оценке документации по ИБ.

3.6. Ответственность подрядчиков и партнеров:

3.6.1. В соответствии с договорами и соглашениями с Обществом, подрядчики и партнеры обязаны:

- соблюдать требования ИБ по использованию защищенных каналов связи и безопасных методов передачи данных;
- уведомлять о выявленных инцидентах и уязвимостях в информационных системах и инфраструктурного ИТ оборудования, к которым имеют доступ;
- соблюдать обеспечение защиты информации при оказании услуг и выполнении работ в рамках договорных обязательств с Обществом.

3.7. Лица, нарушившие требования настоящей Политики или других документов по ИБ, следующих из положений Политики, привлекаются к дисциплинарной или иной ответственности в соответствии с действующим законодательством Республики Казахстан.

4. Безопасность облачных сервисов

4.1. Информационная безопасность облачной инфраструктуры строится на основе разделения зон ответственности между Обществом, оказывающим услуги хостинг-провайдера и клиентами.

4.2. Гарантия непрерывности предоставления услуг:

- Общество обязуется обеспечивать высокую доступность и отказоустойчивость облачных сервисов и хостинг-инфраструктуры;
- реализуются резервирование критически важных систем, регулярное тестирование планов и процедур восстановления;
- контролируются показатели производительности и нагрузки для предотвращения сбоев.

4.3. Обеспечение конфиденциальности клиентских данных:

- Общество не передает клиентские данные третьим лицам без их разрешения, за исключением случаев, предусмотренных законодательством и «Уведомлением о конфиденциальности» Общества;

- предусмотрены технологии шифрования каналов передачи данных;
- применяются механизмы управления доступом, обеспечивающие защиту от несанкционированного доступа.

4.4. Соответствие требованиям и сертификация:

- Общество стремится соответствовать международным требованиям обеспечения информационной безопасности и законодательству Республики Казахстан связанных с информационной безопасностью за счет поддержания и развития СУИБ;
- регулярно проводятся аудиты безопасности, тестирования на проникновение и независимые проверки на соответствия;
- обеспечивается мониторинг новых угроз и оперативное обновление мер защиты в соответствии с изменениями законодательства, стандартов и технологий.

5. Права на интеллектуальную собственность

5.1. Для обеспечения соответствия правовым, обязательным и договорным требованиям по использованию материалов, для которых предусмотрены права на интеллектуальную собственность, в Обществе внедряются соответствующие процедуры.

5.2. Требования к защите любого материала, являющегося интеллектуальной собственностью:

- строгое соблюдение требований авторского права, которое определяет законное использование программных и информационных продуктов;
- приобретение программного обеспечения (далее - ПО) у известных и имеющих хорошую репутацию источников;
- обеспечение контроля за соблюдением ограничений, определяемых законным использованием программных и/или информационных продуктов;
- выполнение условий соответствующих лицензионных соглашений;
- учет и надлежащее документальное подтверждение перехода прав на интеллектуальную собственность в случае их выкупа или безвозмездной передачи;
- соблюдение условий получения из общедоступных источников ПО и информации.

5.3. Права на интеллектуальную собственность включают авторское право на ПО или документ, право на конструкцию, торговые марки, патенты и лицензии исходных кодов.

5.4. Законодательные, регулирующие и договорные требования вводят ограничения на копирование материалов, являющихся предметом собственности. Эти ограничения содержат требования к использованию тех материалов, разработанных или лицензированных либо предоставляемых разработчиком.

6. Заключительные положения

6.1. Управление Политикой осуществляется в соответствии с Правилами разработки документов интегрированной системы менеджмента.

6.2. Пересмотр Политики осуществляется не реже одного раза в год, также могут быть инициированы внесения изменений подразделением ИБ, влияющие на положения настоящей Политики.

6.3. В случае противоречия требований Политики нормам законодательства Республики Казахстан, применяются нормы законодательства Республики Казахстан до внесения соответствующих изменений и дополнений в Политику.

6.4. Ознакомление с Политикой обязательно для всех работников, подрядчиков и партнеров Общества.