

4.4.4. Рынки и конкуренция

4.4.4.1. Подход к управлению

GRI 3-3

Подход к управлению антиконкурентным поведением в Компании включает комбинацию правовых, этических и стратегических мер. Одним из основополагающих законодательных актов Республики Казахстан, которым руководствуется АО «Казахтелеком», является Закон «О естественных монополиях».

Компания включена в республиканский раздел Государственного регистра субъектов естественных монополий и осуществляет функции оператора «универсальных услуг», в связи с чем ее деятельность подлежит регулированию со стороны государства.

Деятельность АО «Казахтелеком» в сфере тарифного регулирования и соблюдения законодательства о естественных монополиях

осуществляется под контролем Агентства по защите и развитию конкуренции Республики Казахстан как уполномоченного органа в сфере регулирования естественных монополий и защиты конкуренции. Полномочия в сфере антимонопольного регулирования и защиты конкуренции в отношении Компании также реализуются Агентством по защите и развитию конкуренции Республики Казахстан.

Отраслевое регулирование деятельности в сфере связи, включая лицензирование, распределение радиочастотного спектра и технический надзор, осуществляет Министерство искусственного интеллекта и цифрового развития Республики Казахстан через Комитет телекоммуникаций. Вопросы кибер- и информационной безопасности курируются Комитетом информационной безопасности при министерстве.

GRI 2-27, GRI 206-1

За отчетный период в Компании не зафиксировано случаев, связанных с нарушением антимонопольного законодательства и иных правовых действий в отношении Компании в связи с препятствием конкуренции.

Таблица 76. Случаи нарушений антимонопольного и конкурентного законодательства в 2025 году, шт. А

Область фокуса	2025
Общее количество подтвержденных случаев антиконкурентного поведения	0
Общее количество нарушений антимонопольного и конкурентного законодательства	0

4.4.5. Информационная безопасность и защита данных

По результатам анализа существенности, раскрытого в разделе [«Анализ существенности»](#), информационная безопасность и защита данных признаны одной из существенных тем АО «Казахтелеком». При определении существенности Компания учитывала ожидания заинтересованных сторон, результаты анкетирования, внутреннюю экспертизу, а также влияние темы на устойчивость цифровой инфраструктуры, качество услуг, доверие клиентов, регуляторное соответствие и долгосрочное создание стоимости.

Для АО «Казахтелеком» данная тема имеет существенное значение с учетом роли Компании как национального оператора связи, масштабов обработки клиентских и корпоративных данных, развития цифровых сервисов, ИИ-решений, центров обработки данных и сетевой инфраструктуры. Недостаточный уровень информационной безопасности может привести к нарушению непрерывности услуг, утечке данных, регуляторным последствиям, репутационным потерям и снижению доверия клиентов, партнеров и государственных органов. Поэтому Компания рассматривает информационную безопасность и защиту данных как один из ключевых факторов устойчивости бизнеса и долгосрочного создания стоимости.

4.4.5.1. Подход к управлению

GRI 3-3, 418-1

Служба информационной безопасности находится в непосредственном подчинении Управляющего директора по информационной безопасности, которому подотчетен Руководитель Службы информационной безопасности, что обеспечивает контроль вопросов информационной безопасности на стратегическом и операционном уровнях.

Вопросы функционирования системы информационной безопасности выносятся на рассмотрение Комитета по аудиту и устойчивому развитию при Совете директоров. Комитет рассматривает ключевые вопросы, связанные с управлением рисками информационной безопасности, защитой персональных данных, результатами мониторинга и проверок, выполнением мероприятий по развитию системы информационной безопасности, а также соответствием требованиям законодательства и ВНД Компании. Рассмотрение этих вопросов на уровне Комитета усиливает надзор со стороны Совета директоров и позволяет учитывать риски информационной безопасности при принятии управленческих решений. Отчетность по ключевым рискам, инцидентам в сфере ИБ и реализации мероприятий представляется Комитету по аудиту и устойчивому развитию на регулярной основе в соответствии с внутренними процедурами Компании.

Основными внутренними документами, регулирующими вопросы в области информационной безопасности, являются:

- Политика информационной безопасности.
- Политика по защите персональных данных в АО «Казахтелеком».
- Концепция по информационной безопасности.

С документами Компании, регулирующими вопросы в области информационной безопасности, можно ознакомиться на сайте компании в разделе «Устойчивое развитие», подраздел «Информационная безопасность» и защита данных.

Основные принципы обеспечения информационной безопасности:

- исполнение законодательных норм;
- вовлеченность высшего руководства Компании в процесс обеспечения ИБ;

4. Отчет об устойчивом развитии

- ориентированность на бизнес;
- процессный подход;
- комплексное использование организационных и технических мер защиты;
- следование лучшим практикам;
- разумная достаточность;
- информированность и персональная ответственность.

Для обеспечения информационной безопасности АО «Казакхтелеком» применяет системный подход. Одним из важных аспектов является круглосуточный контроль данных на всех этапах их жизненного цикла, начиная с момента их поступления в инфраструктуру Компании и заканчивая их архивацией или безвозвратным уничтожением.

В Компании применяются международные практики обеспечения информационной безопасности. Наши внутренние системы защищены с помощью таких решений, как безопасный удаленный доступ к информационным ресурсам, безопасное использование интернета, контроль привилегированных пользователей (PAM), сканеры уязвимостей, защита баз данных и другие. Компания стремится противостоять как внешним, так и внутренним угрозам и внедряет новые решения и методы работы с ресурсами, включая создание необходимой инфраструктуры в Компании, обучение квалифицированных специалистов, формирование оперативного центра информационной безопасности и внедрение концепции ZeroTrust.

Также в Компании используются такие важные элементы безопасности, как встраивание в государственную систему кибербезопасности ЕШДИ, безопасность Интернета вещей, использование ловушек Honeypot и технологии машинного обучения (Machine Learning). Кроме того, на постоянной основе проводится обучение и повышение ИБ-осведомленности сотрудников Компании. В программе Корпоративного университета предусмотрен курс, знакомящий сотрудников с Политикой информационной безопасности АО «Казакхтелеком»,

разработанной в целях определения стратегических целей, задач и основных требований к комплексу мер в области информационной безопасности. Эти меры позволяют поддерживать культуру ответственного обращения с информацией и минимизировать риски человеческого фактора.

В Компании действует сертификат соответствия стандарту ISO 20000–1 «Система менеджмента услуг», который подтверждает наличие процессов управления ИТ-услугами, включая требования к надежности, непрерывности и безопасности предоставляемых сервисов.

В октябре 2025 года (28–29 октября) проведен инспекционный аудит Дивизиона по корпоративному бизнесу (филиал г. Алматы) на соответствие требованиям стандарта СТ РК ISO/IEC 27001–2023 «Информационная безопасность, кибербезопасность и защита конфиденциальности. Системы менеджмента информационной безопасности. Требования». По результатам аудита, проведенного ТОО «Казакхстанский центр качества», подтверждено соответствие системы менеджмента информационной безопасности установленным требованиям.

31 октября 2025 года выдан
Сертификат соответствия стандарту
СТ РК ISO/IEC 27001–2023.

Планы на 2026:

Завершение внедрения и прохождение сертификации системы менеджмента информационной безопасности в филиале Дивизиона информационных технологий с получением сертификата соответствия стандарту ISO/IEC 27001 (планируемый срок — март 2026 года).

4.4.5.2. Защита персональных данных

GRI 418-1

В Компании разработана и внедрена «Политика защиты персональных данных», утвержденная приказом Председателя Правления Компании от 06.10.2023 № 313, в которой определены основные принципы обработки персональных данных клиентов, поставщиков, деловых партнеров, работников и других лиц, а также определены основные действия по сбору, хранению и обработке персональных данных, а также меры по их защите.

На основании Закона Республики Казакхстан от 17 ноября 2025 года № 231-VIII «О внесении изменений и дополнений в некоторые законодательные акты Республики Казакхстан по вопросам искусственного интеллекта и цифровизации», в Закон Республики Казакхстан «О персональных данных и их защите» были внесены изменения. В этой связи в Политику внесены изменения по следующим направлениям:

- актуализация перечня терминов, сокращений и определений;
- усовершенствование процесса получения согласий на сбор и обработку персональных данных;
- унификация подходов к порядку получения согласий на сбор и обработку персональных данных;
- внедрение порядка утверждения перечня лиц, осуществляющих сбор и обработку персональных данных либо имеющих к ним доступ, а также назначения лица (лиц), ответственного(-ных) за организацию обработки персональных данных;
- совершенствование процессов блокирования и хранения персональных данных;
- корректировка процессов предоставления доступа к персональным данным.

Политика является основополагающим документом в области защиты персональных данных, устанавливает цели, задачи и принципы в области защиты ПД, которыми руководствуется Компания в своей деятельности. Служит руководством

при разработке соответствующих документов защиты персональных данных.

Основные принципы обеспечения защиты персональных данных:

- соблюдение конституционных прав и свобод человека и гражданина;
- законность обеспечения защиты персональных данных;
- конфиденциальность персональных данных ограниченного доступа;
- вовлеченность руководства Компании в процесс обеспечения защиты персональных данных;
- ориентированность на бизнес;
- процессный подход;
- комплексное использование способов, методов и средств защиты;
- следование лучшим практикам;
- разумная достаточность;
- информированность и персональная ответственность.

Для оценки эффективности реализации этих принципов и контроля рисков нарушения конфиденциальности применяется метрика «Число инцидентов, которые привели к утечке персональных данных абонентов Общества». Этот показатель напрямую связан с правом абонентов на конфиденциальность и защиту персональной информации. Данный показатель отражает интересы внешних заинтересованных сторон и демонстрирует стремление Компании обеспечивать высокий уровень информационной безопасности.

Данная метрика является частью системы управления рисками и включена в Ключевые показатели деятельности (КПД) Генерального директора Департамента информационных технологий. Для нее установлен целевой ориентир — 0% инцидентов, что соответствует политике нулевой терпимости к утечкам персональных данных.

4. Отчет об устойчивом развитии

В дополнение к этому, в системе КПД Генерального директора Департамента информационных технологий используются и другие показатели, отражающие подход Компании к управлению рисками в области информационной безопасности и клиентского опыта, в том числе:

- Индекс клиентской лояльности (Net Promoter Score, NPS);
- Реализация мероприятий по дооснащению ядра ZeroTrust;
- Доля своевременно устраненных инцидентов информационной безопасности;
- Другие метрики, направленные на защиту интересов пользователей и укрепление доверия к цифровым сервисам Компании.

4.4.5.3. Основные результаты за отчетный период

В области информационной безопасности в 2025 году в Компании проведен комплекс мероприятий для обеспечения защиты корпоративных информационных систем, персональных данных, служебной информации и сетей передачи данных.

Сотрудниками информационной безопасности на регулярной основе проводятся учения по действиям пользователей при получении подозрительных писем. Работа Оперативного центра информационной безопасности (ОЦИБ) с режимом функционирования 24/7 постоянно совершенствуется. В основные обязанности входит:

- Защита корпоративного периметра Компании;
- Мониторинг событий информационной безопасности (ИБ);
- Реагирование на инциденты ИБ;
- Расследование инцидентов ИБ;
- Поиск уязвимостей в информационных системах Компании;
- Выдача рекомендаций по устранению инцидентов информационной безопасности;
- Контроль средств защиты информации (СЗИ).

Мониторинг и контроль указанных показателей осуществляются постоянно в рамках внутренних регламентов по информационной безопасности Компании.

В мае 2025 года Комитетом информационной безопасности Министерства цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан проведена проверка соблюдения требований законодательства в сфере информационной безопасности. По итогам проверки нарушений в части защиты персональных данных не выявлено.

В 2025 году реализован третий этап перехода Компании к модели ZeroTrust, произведено внедрение ряда программно-аппаратных средств защиты информации (СЗИ), что позволило усилить имеющуюся защиту корпоративной инфраструктуры Компании.

Общее количество обоснованных жалоб, полученных относительно нарушения конфиденциальности клиентов, равно нулю. В том числе:

- Жалоб, полученных от сторонних лиц и обоснованных организаций — 0;
- Жалоб, полученных от контролирующих органов — 0;
- Выявленных утечек, краж или потерь данных клиентов — 0.

Данные показатели свидетельствуют об отсутствии зарегистрированных инцидентов, связанных с нарушением конфиденциальности клиентов за отчетный период.

Результаты работы корпоративного ОЦИБ:

Отражено порядка **9 000** DDoS-атак на ресурсы клиентов (пиковая величина более 400 Гбит/сек), общим трафиком свыше 1 230 Тбит.

Развернуто порядка **80 ловушек** (Honeypot — полностью имитирующих информационные системы/ресурсы компании), которые позволили выявить более **50 408 зловредных запросов** внутри корпоративной сети компании.

Антивирусным решением выявлено **около 260 тыс. случаев** выявления вредоносной активности и подозрительных объектов.

Сканированием уязвимостей веб-приложений и ПО выявлено порядка **60,9 тыс. активных уязвимостей** на 98,8 тыс. активов Компании; устранено ответственными администраторами свыше 55,6 тыс. уязвимостей (61.66% от общего количества).

В рамках функционирования системы SIEM осуществляется централизованный прием и корреляция данных от **567 источников логов**, что позволило выявить и обработать более **4 873 критических и высоко рискованных событий** внутри корпоративной сети компании.

С помощью WAF было зафиксировано порядка **27,3 млн веб-запросов** к Интернет-ресурсам. Из них 1,75 млн вредоносных попыток успешно отражены.

При помощи системы контроля привилегированных пользователей РАМ более **305 привилегированных пользователей** (администраторов информационных систем, внешних пользователей и подрядчиков) имеют доступ на более 420 IP-адресов терминальных серверов корпоративных информационных систем.

Системой DLP зарегистрировано около **1,5 млн событий**. Основная активность приходилась на каналы USB, File Share и Clipboard.

Совместно с Отделом по противодействию мошенничеству ФРОД проводится работа по выявлению источников фрод-трафика, находящихся за рубежом, заблокировано свыше **7 млн мошеннических звонков**.

4.4.5.4. Информирование и обучение сотрудников по вопросам информационной безопасности

GRI 418-1

В Компании реализуется системная программа повышения осведомленности работников в области информационной безопасности, направленная на обеспечение конфиденциальности, целостности и доступности данных.

Информационные материалы по вопросам информационной безопасности регулярно направляются сотрудникам через систему электронного документооборота. Все организационно-распорядительные документы Компании, включая документы в области информационной безопасности, доводятся до сведения работников Группой по качеству с обязательной фиксацией факта ознакомления.

Проводятся обучающие тренинги по вопросам информационной безопасности и защиты персональных данных с последующим тестированием для проверки уровня понимания и усвоения требований. В отчетном году Департамент информационных технологий (ДИТ) инициировал дополнительный формат обучения сотрудников с использованием презентационных материалов и практико-ориентированных кейсов, направленных на разбор типовых инцидентов и формирование навыков безопасного поведения при работе с информационными ресурсами. В целях оценки устойчивости к социальным инженерным атакам организуются фишинговые учения: сотрудникам направляются имитационные фишинговые письма с вложениями, фиксируются факты открытия писем, вложений и заполнения форм, а результаты используются для проведения дополнительной разъяснительной работы.

Информационная безопасность обеспечивается как на административном уровне — каждый сотрудник обязан ознакомиться и исполнять требования регламентов, правил, политик Компании в области информационной безопасности, так и на техническом и физическом уровне — в компании используются различные аппаратно-программные комплексы, средства криптографической защиты информации и прочее.

Кроме того, специалисты Дивизиона ИБ регулярно проходят различные курсы повышения квалификации по информационной безопасности, кибербезопасности, рискам и угрозам ИБ. Для сотрудников подразделений по работе с клиентами и по работе с персоналом, где риск неправомерного использования данных достаточно высокий, проводится общее обучение/тестирование по повышению уровня гигиены.

Таблица 77. Показатели по существенной теме, влияющей на долгосрочное создание стоимости Компании

Показатель	Цель на 2025 год	Результат 2025
Число инцидентов, которые привели к утечке персональных данных абонентов	0 инцидентов	0 инцидентов ^A
Доля своевременно устраненных инцидентов ИБ	100%	100%
Выявление и устранение уязвимостей	Своевременное устранение критичных и высокорисковых уязвимостей	выявлено 60,9 тыс. уязвимостей, устранено 55,6 тыс.
Защита данных и противодействие фрод-трафику	Выявление и блокировка мошеннического трафика	около 9 000 отраженных DDoS-атак свыше 1 230 Тбит DDoS-трафика заблокировано свыше 7 млн мошеннических звонков

Показатели в области информационной безопасности и защиты данных, включая метрики «Число инцидентов, которые привели к утечке персональных данных абонентов Общества» и «Доля своевременно устраненных инцидентов ИБ», включены в КПД Управляющего директора по информационной безопасности и Руководителя службы информационной безопасности. Выполнение КПД учитывается в переменной части их вознаграждения в порядке, установленном внутренними документами Компании.