Информационная безопасность и защита данных

Информационная безопасность и защита данных поддерживают устойчивость бизнеса и непрерывность деятельности Фонда. В условиях цифровизации и роста киберугроз Фонд управляет защитой информационных активов на основе единого Корпоративного стандарта информационной безопасности, который устанавливает требования к архитектуре защиты, управлению рисками, внутреннему аудиту и разграничению прав доступа.

В 2025 году мы продолжили развитие системы на основе риск-ориентированного подхода с учетом требований ISO 27001. Проведены анализ и оптимизация ИТ-инфраструктуры, а также оценка уровня защищенности и зрелости процессов. По результатам подтверждены формализованные процессы, распределение ответственности и функционирование системы информирования руководства по ключевым вопросам информационной безопасности.

В части обеспечения защищенности инфраструктуры проведено обследование ИТ-систем, выявлены потенциальные точки отказа и уязвимости, оптимизированы внешние веб-ресурсы с использованием OSINT-анализа. Проведено тестирование защищенности по модели «черного ящика», включая внутреннюю инфраструктуру, смежные системы и устойчивость работников к социально-инженерным воздействиям.

Выявленные уязвимости средней критичности устранены; существенные сценарии компрометации, способные привести к нарушению контроля над инфраструктурой, не выявлены. Для повышения отказоустойчивости оптимизировано размещение серверного и сетевого оборудования, для критической инфраструктуры обеспечено георезервирование, внедрены современные решения для мониторинга событий информационной безопасности, предотвращения утечек и сканирования уязвимостей.

Важным элементом системы киберустойчивости является централизованный мониторинг и реагирование на инциденты. Для противодействия кибератакам в Группе Фонда реализуется проект «Киберщит» на базе ТОО «QazCloud», обеспечивающий круглосуточный мониторинг инцидентов информационной безопасности в Фонде и портфельных компаниях.

Фонд регулярно сканирует инфраструктуру с использованием специализированного лицензионного программного обеспечения, формирует перечни источников риска и событий кибербезопасности, а также готовит регулярные отчеты по рискам.

В рамках корпоративного стандарта портфельные компании ежеквартально направляют информацию об инцидентах, которая анализируется как на уровне самих компаний, так и на уровне Фонда. Это обеспечивает централизованный контроль и своевременное принятие мер по минимизации угроз для конфиденциальности, целостности и доступности информационных систем.

По итогам 2025 года в Группе зафиксировано 27 164 инцидента, что на 8,05% больше по сравнению с 2024 годом. Рост показателя обусловлен, прежде всего, расширением охвата мониторинга и повышением чувствительности систем выявления. По уровню критичности преобладают инциденты низкого и среднего уровней, что свидетельствует о высокой доле событий, выявляемых на ранней стадии.

Основная концентрация инцидентов наблюдалась в ряде крупных организаций Группы, в том числе в АО «НК «Қазақстан темір жолы», АО «НК «QazaqGaz», АО НК «КазМунайГаз», а также в отдельных ИТ-компаниях Группы.

В отчетном периоде обучение в области безопасности данных прошли 9 194 работника, при этом более 40% из них обучались по программам, превышающим обязательные требования законодательства Республики Казахстан. Суммарный объем образовательных мероприятий составил 17 077 часов в рамках 113 тренингов, что соответствует в среднем 0,54 часа на одного работника. Такой подход позволил не только выполнить нормативные требования, но и существенно повысить уровень культуры информационной безопасности за счет внедрения передовых практик кибербезопасности.

Количество инцидентов по информационной безопасности в 2025 г.

3 153
Несанкционированный доступ/ взлом

8 605
Вредоносное программное обеспечение

15 406
Прочие

9 194 РАБОТНИКА

прошли обучение в области безопасности за отчетный период

17 077 ЧАСОВ

суммарный объем образовательных мероприятий

~0,54 часа на одного работника

GRI 3-3