Информационная безопасность и защита данных

GRI 418-1 Мы стремимся развивать надежную систему управления информационной безопасностью, которая охватывает стратегии, методы и процессы защиты информации и ИТ-активов от несанкционированного доступа и рисков, которые могут нарушить конфиденциальность, целостность или доступность информации.

Ключевыми стратегическими целями Фонда в сфере информационной безопасности являются обеспечение доступности, целостности, конфиденциальности и отказоустойчивости информационных систем.

Наши принципы для минимизации рисков в информационной безопасности:

- быстрое выявление, анализ и прогноз развития угроз в информационных технологиях, способных негативно повлиять на стабильность и надежность работы Фонда;
- оценка влияния неблагоприятных факторов;
- приоритетность требований по информационной безопасности;
- непрерывность обеспечения информационной безопасности;
- контролируемость и эффективность мер.

В Фонде функционирует Комитет по информационной безопасности, который отвечает за выработку рекомендаций, направленных на повышение уровня информационной безопасности, и поддерживает постоянное взаимодействие с государственными органами и другими заинтересованными сторонами для более эффективного решения данных вопросов.

GRI 3-3 GRI 418-1 Для системного подхода в этой сфере мы разработали и внедрили «Основные правила политики информационной безопасности», которые включают в себя методики, инструкции и правила. Эти документы направлены на обеспечение соблюдения требований безопасности как специалистами в сфере информационных технологий, так и всеми другими работниками Фонда.

В некоторых портфельных компаниях внедрены Политики информационной безопасности, которые разработаны с учетом специфики их деятельности и ориентированы на лучшие международные практики в сфере обеспечения информационной безопасности. Так, например, для обеспечения информационной безопасности и защиты персональных данных клиентов АО «Казахтелеком», оказывающий услуги связи тысячам казахстанцев, придерживается комплексного подхода: ведет круглосуточный контроль данных на всех этапах их жизненного цикла, начиная с момента их поступления в инфраструктуру компании и заканчивая их архивацией или безвозвратным уничтожением. Кроме того, компания использует такие элементы безопасности, как встраивание в государственную систему кибербезопасности ЕШДИ (единый шлюз доступа к Интернету), безопасность Интернета вещей, использование ловушек Honeypot (позволяет изучить стратегию злоумышленника и определить перечень средств, с помощью которых могут быть нанесены удары по реально существующим объекты безопасности), использование технологий Machine Learning и ряд других инструментов.

GRI 3-3 В рамках совершенствования системы информационной безопасности мы внедрили Корпоративный стандарт информационной безопасности, который охватывает все основные принципы и правила, направленные на защиту данных и координацию действий внутри Группы Фонда. Корпоративный стандарт является обязательным для исполнения при осуществлении процессов информационной безопасности для Фонда и его портфельных компаний.

В 2024 году мы продолжили системную работу по укреплению информационной безопасности:

- начата подготовка к внедрению лучших практики в управлении информационной безопасностью международного стандарта ISO 27001;
- повышена надежность и эффективность ИТ-инфраструктуры. Внедрены технические и организационные меры, обеспечивающие стабильную и безопасную работу информационных ресурсов в соответствии с современными требованиями информационной безопасности;
- реализован комплекс решений по защите от внешних и внутренних угроз, включая внедрение современных программных продуктов и инструментов для предотвращения утечек информации, средств сканирования уязвимостей и анализа угроз в режиме реального времени;
- в рамках контроля и повышения уровня киберустойчивости проведены аудиты информационной безопасности в двух портфельных компаниях (АО «НГК «Тау-Кен Самрук» и АО «Samruk Kazyna Construction»). По итогам проверок даны рекомендации по устранению выявленных рисков;
- проведены обучающие мероприятия и курсы по вопросам информационной безопасности для работников, направленные на формирование культуры безопасного поведения при работе с ИТ-системами и корпоративными данными.

GRI 418-1 Общее количество зарегистрированных инцидентов, связанных с информационной безопасностью в отчетном году, составило 25 240 случаев, что на 57% больше, чем в 2023 году (в 2023 году – 16 094). Около 60% случаев приходится на обнаружение вредоносного программного обеспечения и попытки несанкционированного доступа/взлома. В отчетном периоде в портфельных компаниях не было выявлено фактов утечки данных клиентов.