Информационная политика и безопасность

В 2023 ГОДУ АО «KEGOC» В ЦЕЛЯХ СОБЛЮДЕНИЯ ПРИНЦИПОВ РАВНОПРАВНОГО, ПОЛНОГО, ДОСТОВЕРНОГО И ОПЕРАТИВНОГО РАСКРЫТИЯ ИНФОРМАЦИИ ДЛЯ СТЕЙКХОЛДЕРОВ ПРОДОЛЖИЛО РЕАЛИЗАЦИЮ ИНФОРМАЦИОННОЙ ПОЛИТИКИ.

АО «KEGOC» успешно провело вторичное размещение акций (SPO) и в рамках информационной поддержки эмиссии Компания провела активную работу по взаимодействию с инвестиционным сообществом, а также широкой аудиторией потенциальных инвесторов. Так в отчетном периоде, помимо своевременного раскрытия информации, затрагивающей интересы акционеров и инвесторов, Компанией был проведен ряд мероприятий для СМИ: брифинги, интервью, «День эмитента» на площадке KASE, в ходе которых инвесторы, профессиональные участники рынка ценных бумаг и представители СМИ ознакомились с результатами деятельности Компании, ходом исполнения стратегических планов, реализации инвестиционных проектов.

В целях формирования положительного инвестиционного имиджа АО «KEGOC» продолжило работу по обеспечению информационно-аналитического обслуживания, формированию доверительных отношений между Компанией и экспертным сообществом, инвесторами и акционерами. Для обеспечения оперативности и доступности информации, существенно значимой для пользователей, АО «KEGOC» обеспечена публикация в СМИ, а также на корпоративном веб-сайте и страницах Компании в социальных сетях Facebook, Instagram, Telegram и Twitter материалов о производственно-финансовой деятельности, результатах и достижениях за 26 лет функционирования Системного оператора, в том числе о прошедшем форуме ветеранов-энергетиков, выпуске «зеленых» облигаций, досрочном погашении кредитных займов, включении новых линий 220 кВ в по проекту усиления электрических сетей Западной энергозоны, модернизации НЭС и результатах ежегодной ремонтной кампании. Также были организованы интервью и выступления топ-менеджмента, проведены общественные слушания с участием заинтересованных лиц для широкого освещения инвестиционной деятельности, реализации поставленных задач и достижений Компании по различным направлениям деятельности.

При раскрытии информации АО «KEGOC» руководствуется защитой сведений, составляющих коммерческую, служебную и иную охраняемую законодательством тайну, а также сведений ограниченного распространения.

Информационная безопасность

Основной целью деятельности по информационной безопасности (ИБ) является обеспечение и повышение защищенности информационных активов АО «KEGOC», а также координация, планирование и организация деятельности информационной безопасности, включая эффективное стратегическое управление ИБ и повышение уровня зрелости процессов ИБ.

В АО «KEGOC» ежегодно проходит внутренний и внешний аудит системы управления информационной безопасности (СУИБ) на предмет соответствия международному стандарту ISO 27001.

СУИБ разработана и внедрена на основе ISO/IEC 27001:2013 и является составной частью интегрированной системы менеджмента Компании.

Областью применения СУИБ в АО «KEGOC» является информационная система управления процессами финансово-экономического блока АО «KEGOC», обеспечивающая выполнение основных и вспомогательных бизнес-процессов.

Для соответствия требованиям и определения контекста Компании утверждена Политика информационной безопасности.

В соответствии с установленными в АО «KEGOC» регламентами информационной безопасности, проведены работы по анализу новых критериев для информационных активов, которые имеют ценность для АО «KEGOC». В 2023 году в АО «KEGOC» продолжено усиление мер по обеспечению безопасности информационных активов.

Основные достижения

По результатам внешнего аудита за 2023 год АО «KEGOC» получен сертификат соответствия международному стандарту ISO 27001, который подтверждает, что Компания соответствует высоким стандартам управления информационной безопасностью. Это значительный шаг в направлении обеспечения безопасности информационных систем и данных Компании.

По итогам 2023 года все системы ИБ работают исправно. Производится постоянный контроль над поддержанием работоспособности систем защиты Компании от кибер-атак. Ведется обновление политик систем ИБ (DLP, SIEM, CyberArk). Производится еженедельная проверка корпоративной сети при помощи антивирусного ПО. Системой защиты (Kaspersky) Компании успешно фиксируются и отражаются вредоносные ПО (вирусы-шифровальщики). Ведется анализ конфиденциальных данных, и блокируются фишинговые рассылки и спамы с помощью системы предотвращения утечек (DLP). На данный момент ведется работа по настройке политик антивирусного ПО и системы DLP.

Отделом информационной безопасности Департамента безопасности АО «KEGOC», совместно с работниками ТОО «QazCloud» проведены мероприятия по расширению зоны мониторинга ОЦИБ. На сегодняшний день корпоративная сеть Компании полностью подключена к ОЦИБ (Произведено полное подключение к Киберщиту АО «Самрук-Қазына). Проведен аудит разрешенных ПО в Компании в рамках утвержденного Реестра программных обеспечений, используемых в АО «KEGOC».

За 2023 год системой защиты (Kaspersky) Компании выявлены и успешно удалены вредоносные ПО связанные с вирусами червями и нелегитимными ПО. В связи с выполнениями мероприятий по выявлению и устранению вирусов, отсутствовала необходимость служебной проверки. Заблокированы фишинг письма, связанные с криптовалютами.

Повышение осведомленности

Согласно требованиям СУИБ в Компании утверждена единая корпоративная этика в вопросах ИБ, поддерживающая осведомленность работников.

АО «KEGOC» обеспечивает соответствующую компетентность (образование, подготовка, опыт) персонала, который несет ответственность за обеспечение ИБ, путем проведения технической учебы, специального обучения на курсах повышения квалификации, инструктажей, также внедрена система профессиональной подготовки и профессионального развития персонала.

В 2023 году проведены следующие обучения для работников Компании:

- Что такое ИБ;
- ИБ парольная защита;
- ИБ электронная почта;
- ИБ антивирусная защита;
- ИБ Обновления;
- Социальная инженерия.

Кроме того, в 2023 году в целях самообразования на портале Компании существует раздел «Информационная безопасность». В котором размещается информация по действующим угрозам, дайджесты по информационной безопасности и спам рассылкам. Так же направлены рассылка всем работникам ИД, филиалам, и ДО в которой сообщалось о возможности ознакомления с ВНД, и рекомендациями по ИБ в вышеуказанном разделе.

Разработан тест для повышения осведомленности ИБ. При приеме вновь принятого работника проводится вводный инструктаж по ИБ и заполняется контрольный лист инструктажа согласно Стандарт по управлению персоналом. За 2023 года инструктаж прошли более 100 человек.

В 2023 году для работников Компании занятых ИБ проведены следующие обучения:

- Обучение ключевых пользователей по программно-аппаратному комплексу межсетевые экраны нового поколения «Palo Alto Networks»;
- Обучение ключевых пользователей по системе контроля привилегированных пользователей PAM.

В АО «KEGOC» разработаны процессы по обучению пользователей по процедурам защиты и правильному обращению с информационными ресурсами. Выработаны процессы по направлению и получению необходимых сведении о правилах АО «KEGOC» и принятых в них процедурах, включая требования к безопасности и другим средствам контроля. Данные процессы также действуют в отношении пользователей информационных систем из сторонних организаций, имеющих постоянный или временный доступ к информационным ресурсам АО «KEGOC».

В целях повышения осведомленности работников АО «KEGOC» были подготовлены методические разработки по вопросам обеспечения ИБ. Данные материалы ежемесячно размещаются на едином портале АО «KEGOC» в разделе «Информационная безопасность».

Управление инцидентами

В Компании утверждены Правила по управлению инцидентами информационной безопасности, которые определяют основные меры, методы и средства сохранения (поддержания) работоспособности ИС Компании при возникновении различных инцидентов ИБ, а также способы и средства восстановления информации и процессов ее обработки в случае нарушения работоспособности ИС и компонентов. Основными целями процесса по управлению инцидентами ИБ являются минимизация ущерба, скорейшее восстановление исходного состояния ИС и разработка плана по недопущению подобных инцидентов в будущем.

Работники Компании, пользователи информационных систем должны без промедления сообщать по административным каналам о событиях, потенциально несущих угрозу безопасности. Перечень и состав таких событий должен быть доведен до сведения пользователей при их информировании об обеспечении ими информационной безопасности при выполнении служебных обязанностей, а также при обучении правилам использования информационных ресурсов и сервисов информационных систем.

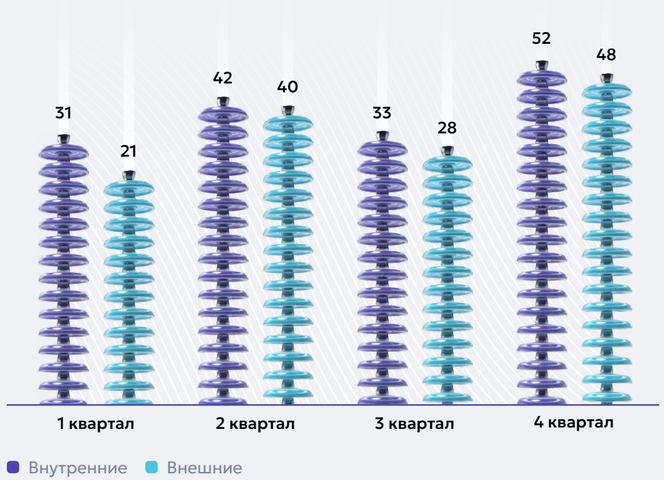
Пользователи информационных ресурсов АО «KEGOC» обязаны регистрировать любые наблюдаемые или предполагаемые слабости в системе безопасности и сообщать о них. Пользователи должны незамедлительно доводить подобные инциденты до уполномоченных работников. Ни при каких обстоятельствах они не должны пытаться проверять предполагаемые слабости в системе защиты информации.

Пользователи информационных ресурсов АО «KEGOC» обязаны регистрировать все случаи, когда функционирование программного обеспечения представляется им неправильным, т.е. не соответствующим спецификации, а о подозрениях, что сбой вызван вредоносной программой, например, компьютерным вирусом они должны сообщать уполномоченным работникам.

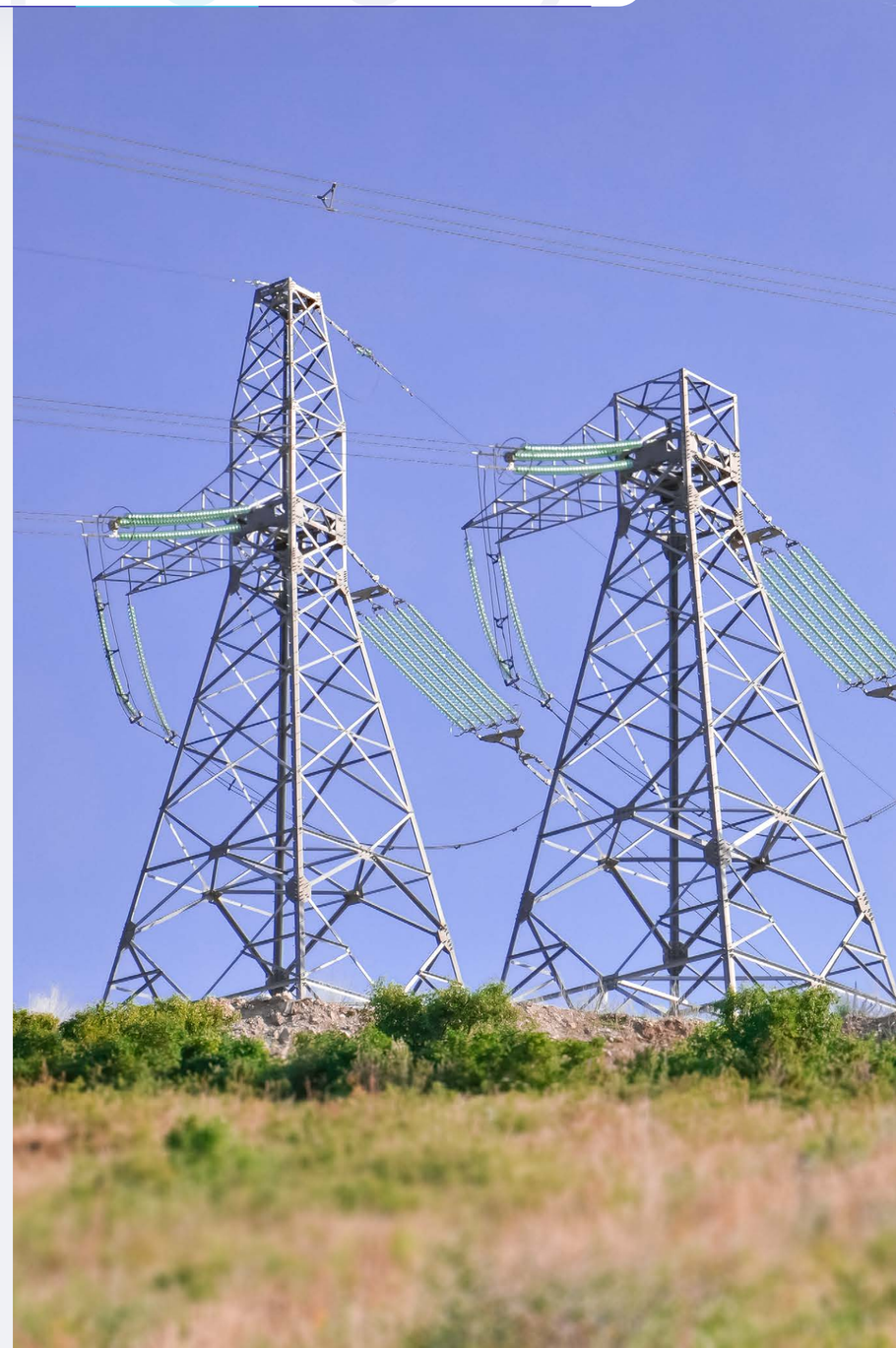
Пользователи не должны пытаться самостоятельно восстановить функционирование программного обеспечения путем удаления подозрительного программного обеспечения.

По итогам 2023 года было выявлено 290 инцидентов информационной безопасности, по которым были проведены соответствующие мероприятия, направленные на минимизацию рисков ИБ.

Распределение инцидентов по кварталам в 2023 году



Наибольшее количество внешних инцидентов было зарегистрировано по категории «вирусы», обнаруженных на съемных носителях. В соответствии Правилами по кадровому администрированию в АО «KEGOC» за совершение работником дисциплинарного проступка/инцидента информационной безопасности АО «KEGOC» были применены дисциплинарные взыскания.



Готовность к аварийным ситуациям

В Компании установлены процедуры обеспечения непрерывности деятельности направленные на ограничения степени воздействия внутренних и внешних негативных факторов на деятельность АО «KEGOC». В соответствии с Планом обеспечения непрерывности работы информационной инфраструктуры и информационных объектов при обнаружении инцидентов информационной безопасности АО «KEGOC» проводилось тестирование и плановое расследование кибер-инцидента в рамках плана ОНД. Данный План тестируется каждый год.

Результатом деятельности в 2023 году явилось недопущение инцидентов информационной безопасности, влекущих финансовые и репутационные потери в отношении информационных активов Компании.

Внешний и внутренний аудит

В АО «KEGOC» в соответствии с Планом аудита проводятся внешние и внутренние аудиты по СУИБ. Аудит проводится по всем процессам системы, устанавливая связь между целями процесса, ходом реализации и результатами процесса, выявляя слабые стороны и области для улучшения.

Во исполнения законодательных норм Компания ежегодно проводит внешнее тестирование на проникновение. Тестирование проводится с использованием различных методов и техник, которые были выбраны с учетом специфики Компании и информационных систем.

Риски и принятые меры

Управление рисками в области информационной безопасности является элементом корпоративной системы управления рисками АО «KEGOC».

Оценка рисков в области информационной безопасности осуществляется для всех активов АО «KEGOC», на основании которой формируется отчет об оценке и План обработки рисков в области ИБ.

Для управления выявленными рисками разработаны План контрольных мероприятий по внедрению мер безопасности СУИБ АО «KEGOC», План проведения тематических занятий по информационной безопасности для работников, а также план первоочередных мер информационной безопасности и мероприятия, направленные на повышение уровня информационной безопасности производственных систем.

Мы стремимся постоянно улучшать наши меры по обеспечению безопасности информационных систем и обеспечить надежность работы всей нашей Компании. Мы будем продолжать совершенствовать наши процессы и меры безопасности в соответствии с лучшими практиками и новыми технологиями.

Политика конфиденциальности

Обеспечение конфиденциальности информации является элементом корпоративной системы управления рисками АО «KEGOC». Работники Компании со дня приема на работу подписывают документ о неразглашении сведений, составляющих конфиденциальную информацию, в соответствии с требованиями внутренних документов и проходят соответствующий инструктаж. В договорах с поставщиками прописываются отдельным разделом условия обеспечения конфиденциальности данных Компаний.

О механизме информирования потребителей о защите конфиденциальности

В 2023 году разработаны и приняты Правила по обеспечению информационной безопасности при работе с поставщиками в АО «KEGOC».

Индикаторы реализации Цели 2

Наименование КПД	2019 факт	2020 факт	2021 факт	2022 факт	2023 план	2023 факт
LTIFR, коэффициент	0	0	0,15	0,45	0,65	0,15
ESG рейтинг				индикатор определен в 2022 году	30	51