Информационная безопасность

Согласно Политике информационной безопасности АО «Самрук-Энерго», Компания стремится организовать деятельность по обеспечению информационной безопасности (далее - ИБ) в соответствии со стандартом ISO/IEC 27001 «Информационная технология. Методы и средства обеспечения безопасности. Системы управления информационной безопасностью». В этой связи были утверждены внутренние нормативные документы и проводятся следующие мероприятия:

- Разработка и актуализация СУИБ;
- Идентификация рисков ИБ и владельцев информационных активов;
- Оценка и обработка рисков ИБ;
- Координация разработки/внедрения контрольных мероприятий;
- Исполнение мероприятий по ИБ;
- Мониторинг рисков ИБ, отчетность;
- Совершенствование СУИБ.

Функции обеспечения информационной безопасности возложены на Департамент «Безопасность», который является структурным подразделением, обособленным от остальных структурных подразделений, занимающихся созданием, сопровождением и развитием объектов информатизации. Согласно утвержденной организационной структуре, Департамент находится в прямом подчинении Председателя Правления АО «Самрук-Энерго». В части ИБ данное структурное подразделение отвечает за следующие функции:

- разработка нормативно-распорядительной документации и требований к ИБ;
- обеспечение взаимодействия между бизнес-подразделениями по вопросам обеспечения ИБ;
- контроль над исполнением требований по ИБ;
- мониторинг деятельности ДЗО в области обеспечения информационной безопасности;
- взаимодействие с государственными уполномоченными органами в области обеспечения информационной безопасности Общества;
- осуществление координации действий по рискам ИБ;
- взаимодействие с Оперативным центром информационной безопасности.

В рамках процесса по обеспечению ИБ, Компанией учитываются следующие основные направления:

- управление информационной безопасностью;
- техническое обеспечение информационной безопасности;
- контроль и реагирование на инциденты информационной безопасности.

В рамках процесса по управлению ИБ, Компанией разработаны следующие документы, регламентирующие работу ИБ:

- Политика информационной безопасности АО «Самрук-Энерго»;
- Правила обеспечения информационной безопасности информационных систем в АО «Самрук-Энерго»;
- Инструкция по обеспечению сохранности конфиденциальной информации в АО «Самрук-Энерго».

Функция технического обеспечения ИБ осуществляется Департаментом «Безопасность» и специалистами ТОО «Energy Solutions Center». Под данной функцией понимается процесс обеспечения ИБ посредством применения программно-технических механизмов защиты информационных активов Компании. Основными мероприятиями по обеспечению информационной безопасности Компании на данный момент являются:

- обеспечение антивирусной защиты корпоративной сети Компании и филиалов путем использования программного комплекса обеспечения защиты от вредоносного кода;
- демилитаризованная зона (ДМЗ), применяющаяся для повышения уровня информационной безопасности корпоративной сети Компании и ресурсов, имеющих доступ в сеть Интернет. ДМЗ реализовано на базе программно-аппаратного комплекса пакетных фильтров Firewall (брандмауэров), также для дополнительной фильтрации пакетов на уровне распределения программно-аппаратными средствами реализованы система предотвращения вторжения, контроль программного обеспечения, используемое для отслеживания отправляемых и получаемых электронных писем. При помощи данной системы производятся блокировка спам отправителей в периметре АО «Самрук-Энерго» и анализ электронных писем на наличие вредоносных программных обеспечений, и контроль программного обеспечения для предотвращения утечек конфиденциальной информации за пределы корпоративной сети.

Функция контроля и реагирования на инциденты ИБ осуществляется работниками Департамента «Безопасность» и специалистами ТОО «Energy Solutions Center» регистрируемых Оперативным центром информационной безопасности (ОЦИБ) и средствами программно-аппаратного комплекса по информационной безопасности:

- Централизованный сбор, хранение, анализ журналов событий безопасности;
- Обнаружение инцидентов в режиме реального времени;

- Определение приоритетов инцидентов;
- Контроля над процессом исправления инцидентов и соблюдения времени реагирования (SLA);
- Создание отчетов о соблюдении нормативных требований.

Результаты по контролю и реагированию на инциденты ИБ фиксируются в следующих отчетах:

- Ежемесячный аналитический отчет с анализом состояния инфраструктуры информационной безопасности АО «Самрук-Энерго» в рамках договора с ОЦИБ;
- Ежеквартальный отчет по рискам информационной безопасности для Совета директоров АО «Самрук-Энерго»;
- Формируется ежегодный отчет по обеспечению информационной безопасности (кибербезопасности), а также анализу и оценке достаточности внутренних контролей АО «Самрук-Энерго» в части защиты и поддержания ИТ-систем и инфраструктуры для Комитета по аудиту и Совету директоров АО «Самрук-Энерго».

В течение года проводится повышение осведомленности о СУИБ путем ежегодного утверждения Плана работ о разработках обучающих материалов по повышению осведомленности работников Компании (памятки, скринсерверы, видеоролики), осуществляется рассылка о нововведениях, требованиях и превентивных мерах по ИБ. На ежегодной основе работники Компании в установленном порядке проходят онлайн тестирование на знание норм информационной безопасности.

В 2023 году для всех вновь принятых работников при приеме был проведен «Адаптационный курс», который включает обучение по информационной безопасности.

GRI 418-1

В Компании в отчетный период не было зарегистрировано обоснованных жалоб на нарушение конфиденциальности, утечек, краж и/или потерю данных клиентов.

Оперативный центр информационной безопасности

АО «Самрук-Энерго» подключено к Оперативному центру информационной безопасности для мониторинга всех событий информационной безопасности в режиме 24/7, предоставляемый в рамках договора с ТОО «QazCloud», который оказывает следующие услуги:

- круглосуточный мониторинг событий ИБ, зафиксированных системами мониторинга и управления событиями информационной безопасности и системами защиты внешнего периметра;
- круглосуточный мониторинг событий ИБ, зафиксированных на серверном оборудовании и сетевых устройствах Заказчика (далее — Зона мониторинга);
- выявление инцидентов ИБ, произошедших в Зоне мониторинга;
- направление Заказчику информации о выявленных инцидентах и методах реагирования на них и предоставления рекомендаций по их устранению;
- предоставление экспертной поддержки в процессе реагирования на инциденты;
- реагирование на инциденты поступающих с внешней сети Интернет на периметр Заказчика;
- проведение расследования инцидентов ИБ;
- 3 уровневая линия поддержки ОЦИБ, состоящая из командной взаимодействии при обеспечении мониторинга ИБ (Red team и Blue team). Blue team обеспечивает защиту инфраструктуры путем мониторинга событий и реагирования на киберугрозы в режиме 24/7. Red team позволяет профессионально выявлять уязвимости инфраструктуры;
- защита веб-приложений и WEB трафик;
- защита от DDOS-атак;
- еженедельный дайджест ИБ;
- проведение аудита (penetration test), включающий внешнее тестирование на проникновение и выявление уязвимостей.

Инициативы Компании в области кибербезопасности утверждены в Стратегии информационных технологий и цифровизации АО «Самрук-Энерго» на 2023–2025 гг.