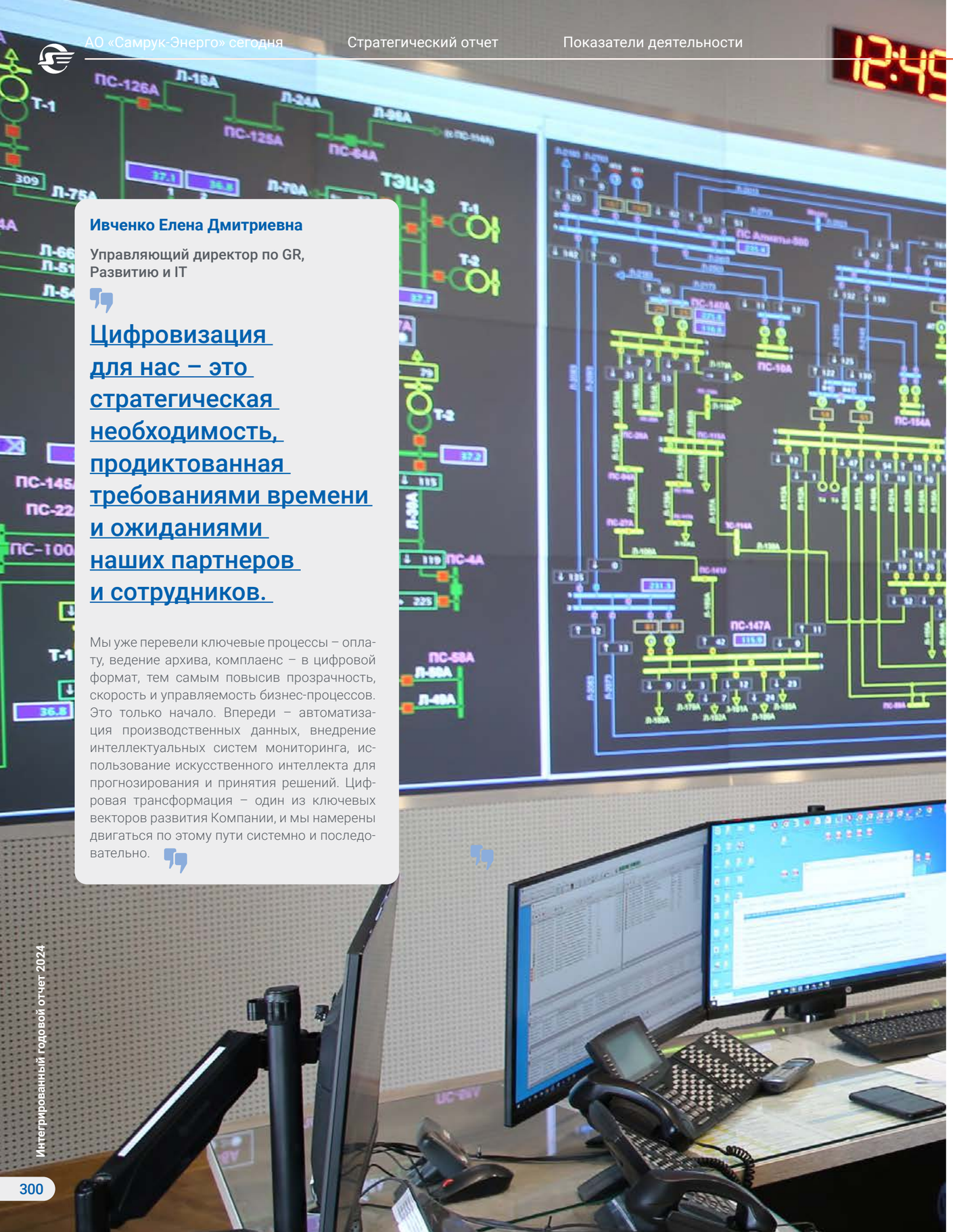

Ивченко Елена Дмитриевна

Управляющий директор по GR, Развитию и IT

Цифровизация для нас – это стратегическая необходимость, продиктованная требованиями времени и ожиданиями наших партнеров и сотрудников.

Мы уже перевели ключевые процессы – оплату, ведение архива, комплаенс – в цифровой формат, тем самым повысив прозрачность, скорость и управляемость бизнес-процессов. Это только начало. Впереди – автоматизация производственных данных, внедрение интеллектуальных систем мониторинга, использование искусственного интеллекта для прогнозирования и принятия решений. Цифровая трансформация – один из ключевых векторов развития Компании, и мы намерены двигаться по этому пути системно и последовательно.

Информационная безопасность

GRI 3-3

В соответствии с Политикой информационной безопасности АО «Самрук-Энерго», Компания нацелена на построение системы защиты информации, соответствующей международному стандарту СТ РК ISO 27001 «Информационные технологии. Методы и средства обеспечения безопасности. Системы управления информационной безопасностью». Для реализации этой цели были разработаны и утверждены внутренние нормативные документы, а также внедряются следующие ключевые мероприятия:

- Разработка и актуализация системы управления информационной безопасностью (СУИБ);
- Идентификация рисков информационной безопасности и определение владельцев информационных активов;
- Оценка и обработка рисков информационной безопасности;
- Координация разработки и внедрения контрольных мероприятий;
- Исполнение мероприятий по обеспечению информационной безопасности;
- Мониторинг рисков информационной безопасности и подготовка отчетности;
- Постоянное совершенствование системы управления информационной безопасностью.

Ответственность за обеспечение информационной безопасности в компании возложена на Департамент по безопасности, который является самостоятельным структурным подразделением и непосредственно подчиняется Председателю Правления АО «Самрук-Энерго». В рамках своей деятельности по обеспечению информационной безопасности, подразделение выполняет следующие ключевые функции:

- Разработка нормативно-распорядительной документации и требований по информационной безопасности;
- Обеспечение взаимодействия между бизнес-подразделениями по вопросам информационной безопасности;
- Контроль соблюдения требований информационной безопасности;
- Мониторинг деятельности ДЗО в области информационной безопасности;
- Взаимодействие с государственными органами по вопросам информационной безопасности Компании;
- Координация действий по управлению рисками информационной безопасности;
- Взаимодействие с Оперативным центром информационной безопасности.

В процессе обеспечения ИБ в Компании учитываются три основных направления:

- Управление информационной безопасностью;
- Техническое обеспечение информационной безопасности;
- Контроль и реагирование на инциденты информационной безопасности.

Управление информационной безопасностью

В рамках процесса управления информационной безопасностью в Компании разработаны ряд документов, которые регламентируют работу в этой области:

- 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».

Техническое обеспечение информационной безопасности

Функция технического обеспечения информационной безопасности осуществляется Департаментом по безопасности совместно со специалистами ТОО «Energy Solutions Center». Под техническим обеспечением подразумевается комплекс мероприятий,

направленных на защиту информационных активов Компании с использованием современных программно-технических средств.

Ключевые мероприятия, выполняемые в рамках данной функции:

- Обеспечение антивирусной защиты корпоративной сети и филиалов с применением специализированного программного обеспечения для защиты от вредоносного кода;
- Создание демилитаризованной зоны (ДМЗ) для повышения уровня информационной безопасности корпоративной сети и ресурсов с доступом в интернет. ДМЗ реализована на базе программно-аппаратного комплекса пакетных фильтров Firewall (брандмауэров), что обеспечивает дополнительную фильтрацию пакетов на уровне распределения;
- Контроль программного обеспечения для мониторинга отправляемых и получаемых электронных писем. Система позволяет блокировать спам-отправителей в периметре АО «Самрук-Энерго», анализировать электронные письма на наличие вредоносных программ и предотвращать утечку конфиденциальной информации за пределы корпоративной сети.

Контроль и реагирование на инциденты информационной безопасности

Функция контроля и реагирования на инциденты информационной безопасности выполняется работниками Департамента по безопасности совместно с специалистами ТОО «Energy Solutions Center». Все инциденты регистрируются и обрабатываются в Оперативном центре информационной безопасности (ОЦИБ) с использованием программно-аппаратного комплекса для обеспечения ИБ.

Ключевые мероприятия включают:

- Централизованный сбор, хранение и анализ журналов событий безопасности;
- Обнаружение инцидентов в реальном времени;
- Определение приоритетов инцидентов;
- Контроль над процессом исправления инцидентов и соблюдение времени реагирования;
- Создание отчетов о соблюдении нормативных требований.

Результаты контроля и реагирования на инциденты документируются в следующих отчетах:

- Ежемесячный аналитический отчет, содержащий анализ состояния инфраструктуры информационной безопасности АО «Самрук-Энерго» в рамках договора с Оперативным центром информационной безопасности;
- Ежеквартальный отчет по рискам информационной безопасности для Совета директоров АО «Самрук-Энерго»;
- Ежегодный отчет по обеспечению информационной безопасности (кибербезопасности), а также анализ и оценка достаточности внутренних контролей АО «Самрук-Энерго» для Комитета по аудиту и Совету директоров.

В течение отчетного периода проводились работы над повышением уровня осведомленности о системе управления информационной безопасностью. Ежегодно утверждается план работ, в рамках которого разрабатываются обучающие материалы, такие как памятки, скринсерверы и видеоролики, для всех сотрудников Компании. Также осуществляется рассылка о нововведениях, требованиях и превентивных мерах по информационной безопасности. Ежегодно все работники Компании проходят онлайн-тестирование на знание норм информационной безопасности, что подтверждает их компетентность в этой области.

При приеме на работу все новые сотрудники проходят «Адаптационный курс», включающий обучение по информационной безопасности. В 2024 году это обучение было проведено для всех вновь принятых сотрудников, что позволяет обеспечить высокую осведомленность и соблюдение стандартов информационной безопасности с самого начала их работы в компании.

GRI 418-1

За отчетный период в Компании не было зафиксировано ни одной обоснованной жалобы на нарушение конфиденциальности, утечку, кражу или потерю данных клиентов

Оперативный центр информационной безопасности

АО «Самрук-Энерго» подключено к Оперативному центру информационной безопасности (далее – ОЦИБ), который осуществляет мониторинг всех событий информационной безопасности в режиме 24/7. ОЦИБ предоставляется в рамках договора с ТОО «QazCloud», оказывающим следующие услуги:

- Круглосуточный мониторинг событий информационной безопасности, зафиксированных системами мониторинга и управления событиями информационной безопасности, а также системами защиты внешнего периметра;
- Круглосуточный мониторинг событий информационной безопасности, происходящих на серверном оборудовании и сетевых устройствах (далее – Зона мониторинга);
- Выявление инцидентов информационной безопасности, которые происходят в Зоне мониторинга;
- Регистрация выявленных инцидентах, а также методов реагирования на них и рекомендаций по их устранению;
- Предоставление экспертной поддержки в процессе реагирования на инциденты;
- Проведение расследований инцидентов информационной безопасности;
- Трехуровневая линия поддержки ОЦИБ, состоящая из командной работы по обеспечению мониторинга ИБ, включающей Red team и Blue team. Blue team занимается защитой инфраструктуры, осуществляя круглосуточный мониторинг событий и реагируя на киберугрозы. Red team, в свою очередь, профессионально выявляет уязвимости инфраструктуры;
- Защита веб-приложений и WEB трафика;
- Защита от DDOS-атак;
- Еженедельный дайджест по информационной безопасности;
- Аудит (penetration test), включающий внешнее тестирование на проникновение и выявление уязвимостей.