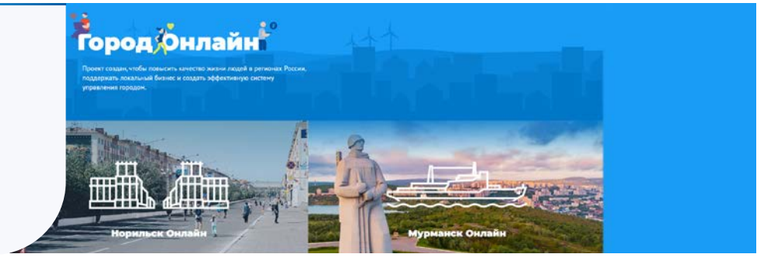
Цифровизация для регионов присутствия



GRI 203–1, 203–2

Проект «Город Онлайн» направлен на повышение качества жизни людей, проживающих в малых и средних городах Крайнего Севера и Дальнего Востока, за счет предоставления инфраструктурных и цифровых сервисов в различных сферах жизни, позволяющих сделать привычные услуги более доступными для удаленных районов.

Платформа доступна в веб-версии и мобильном приложении в пяти городах: Норильске, Дудинке, Мончегорске, Мурманске и Красноярске. На сегодняшний день в веб-версии представлено 28 сервисов, в мобильном приложении — 16. Наиболее востребованы из них «ГО.Медиа», «Афиша», «Трансляции» (только веб-версия), «Карта» и «Транспорт». В ближайшей перспективе запланировано развитие сервисов, которые позволят муниципальным служащим оперативно взаимодействовать друг с другом, с жителями города внутри единого информационного пространства.

Среди крупных инфраструктурных сервисов «Город Онлайн» можно выделить:

- программу мониторинга городского воздуха с моделью предиктивной оценки экологической ситуации в г. Норильске, г. Мончегорске, п. г. т. Никель и г. Заполярном, которая направлена на улучшение качества городской среды и комфорта жизни людей;
- систему мобильного школьного образования в Мурманской области. Система была развернута в 2022 году и уже позволила выйти на более качественный и равный для разных социальных групп уровень образования, минимизировать влияние активированных дней в период обучения.

Для обеспечения производственных потребностей Компании высокоскоростной связью и повышения качества жизни в Норильском промышленном районе за счет предоставления широкополосного доступа в интернет, улучшения качества сервисов и расширения спектра оказываемых услуг связи реализуется Проект строительства волоконно-оптической линии связи в г. Норильске. Проект предусматривает строительство волоконно-оптической линии связи протяженностью 956 км от г. Нового Уренгоя до г. Норильска.

В 2022 году с учетом растущей потребности населения в Норильском районе для улучшения качества связи были проведены работы по расширению полосы пропускания транспортной сети с 40 до 200 Гбит/с, что на сегодняшний день обеспечило возможность роста трафика на клиентский каналах связи до 85 Гбит/с, при этом трафик для потребностей Компании составляет менее 1%.

Учитывая, что мобильный и фиксированный доступ в интернет остается одними из ключевых условий высокого качества жизни людей в современном мире и является драйвером развития цифровых сервисов, для повышения доступности качественной связи в 2022 году проведена акция для операторов связи, предоставляющих услуги конечным потребителям, предполагающая снижение стоимости в среднем на 15%. Новая тарифная политика способствовала развитию в 2022 году высокоскоростных тарифных планов операторов в городе и привело к снижению стоимости в среднем в два раза. Также 15 школ в Норильском промышленном районе получили доступ в интернет на льготных условиях.

Более
180 тыс. пользователей
зарегистрировано на платформе

Почти
1,5 млн
уникальных пользователей посетили платформу

Около
55 тыс. раз
установлено мобильное приложение

Обеспечение корпоративной защиты

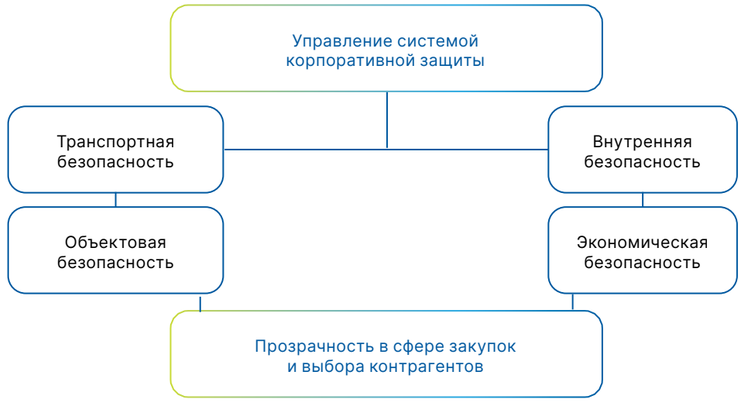
Одним из ключевых факторов устойчивости бизнес-процессов «Норникеля» является работа корпоративной системы безопасности. В Компании разработана комплексная система управления корпоративной защитой, включающая в себя пять основных блоков.

Для управления вопросами корпоративной защиты в Компании функционирует специализированный Блок корпоративной защиты. Помимо этого, в Компании организована и расширяется сеть ситуационно-аналитических центров безопасности. Регуляторные рамки в данном направлении определяются российским законодательством, применимыми международными нормами и внутрикорпоративными стандартами, и регламентами «Норникеля».

В процессы совершенствования и выработки нормативно-правовых документов, направленных на обеспечение корпоративной безопасности вовлечены все высшие руководители Компании, включая Совет директоров и Правление. В марте 2022 года Советом Директоров была утверждена Политика ПАО «ГМК «Норильский никель» в области противодействия корпоративному мошенничеству. Требования Политики соответствуют принципам честного и ответственного ведения бизнеса, подчеркивают стремление Компании к совершенствованию корпоративной культуры, следование лучшим практикам корпоративного управления и высоким этическим стандартам.

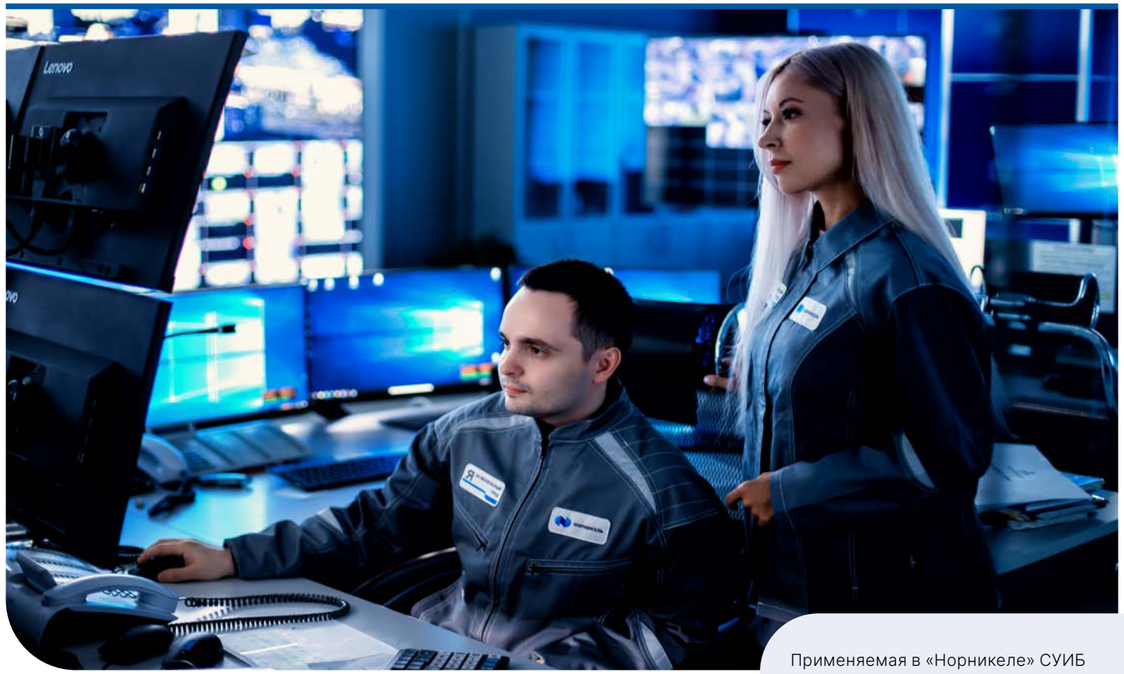
Данная Политика унифицировала комплекс системных мер по предупреждению, выявлению и противодействию злоупотреблениям и проявлениям корпоративного мошенничества.

Структура системы управления корпоративной защитой



Цели Политики в области противодействия корпоративному мошенничеству

1. Предотвращение, выявление и минимизация рисков корпоративного мошенничества. Защита законных интересов Компании, ее филиалов, их акционеров/участников, обеспечение сохранности активов.
2. Подтверждение приверженности принципу полного неприятия корпоративного мошенничества в любых формах и проявлениях.
3. Формирование у всех сотрудников единообразного понимания сути мошеннических действий, а также единого стандарта поведения для предотвращения и пресечения таких ситуаций.
4. Предотвращение нарушения Компанией или ее дочерними организациями, сотрудниками законодательства в сфере противодействия корпоративному мошенничеству.



Обеспечение информационной безопасности

«Норникель» обладает высоким уровнем интегрированности информационных систем во все направления деятельности. Информация является важным ресурсом для Компании, а информационная безопасность — залогом непрерывности ее работы. В «Норникеле» функционирует и развивается собственная Система управления информационной безопасностью (СУИБ). СУИБ распространяется на процессы оперативного управления производством, обеспечения сырьем и технологическими материалами, а также контроля выполнения плановых показателей по производству и отгрузке готовой продукции.

Ключевыми инструментами поддержания высокого уровня информационной безопасности в «Норникеле» являются регулярная организация внешних аудитов СУИБ на соответствие требованиям защиты персональных данных, защиты критической информационной инфраструктуры, соответствие требованиям международных стандартов в области управления процессами кибербезопасности, а также тестирование и анализ уровня защищенности, контроль обеспечения информационной безопасности в морском и речном судоходстве в результате веттинг-инспекций и т. д.

Применяемая в «Норникеле» СУИБ соответствует нормам и требованиям международного стандарта ISO/IEC 27001:2013. В 2022 году высокую эффективность процессов управления информационной безопасности подтвердили четыре площадки «Норникеля»:

1. Мурманский транспортный филиал;
2. Надеждинский металлургический завод;
3. Медный завод;
4. Талнахская обогатительная фабрика.

Внешний аудитор отметил высокую готовность предприятий реагировать на новые угрозы и вызовы. Компания продемонстрировала контроль над рисками и готовность к неожиданным изменениям, подтвердив свою способность достигать поставленных целей в области обеспечения защиты производственных процессов.

Наравне с ситуационно-аналитическими центрами безопасности в Компании функционирует Центр реагирования на инциденты информационной безопасности. В случае обнаружения пользователями подозрительного контента или активности информация направляется в Центр реагирования. В Центре происходит оценка возможного деструктивного влияния на информационные системы Компании и реализация мер, направленных на предотвращение и устранение последствий инцидентов. В своей работе Центр опирается на лучшие отечественные и мировые практики управления процессами кибербезопасности и передовые технологические решения.

В 2022 году отмечался значительный рост кибератак на российские компании. Для минимизации рисков были приняты дополнительные комплексные, в том числе проактивные меры по обеспечению безопасности информационной инфраструктуры «Норникеля». За отчетный год сотрудниками Центра реагирования было обработано более 20 тыс. событий информационной безопасности и более тысячи инцидентов.

Защита конфиденциальной информации в Компании обеспечивается специальными техническими средствами защиты, которые позволяют выявлять попытки несанкционированного вывода по основным каналам, включая электронную почту и файловый обмен. В случае выявления попыток несанкционированного вывода конфиденциальной информации инициируется процедура служебной проверки и расследования, в соответствии с действующими в Компании регламентами.

Компания признает существование риска наступления нештатных и чрезвычайных ситуаций, влияющих на устойчивость информационных систем «Норникеля». Для обеспечения бесперебойности работы Компании разработаны и документированы процессы и процедуры обеспечения непрерывности информационной безопасности. Данные процедуры тестируются не реже одного раза в квартал, что гарантирует их актуальность.

Для защиты персональных данных различных типов субъектов, включая защиту персональных данных третьих лиц, в Компании применяется комплекс организационно-технических мер. Техническая защита обеспечивается средствами антивирусной защиты, предотвращения утечек, контроля отчуждаемых устройств, анализа событий безопасности. Также в Компании действуют Политика в области обработки персональных данных и ряд внутрикорпоративных документов, регламентирующих обработку и защиту персональных данных.

Обучение по вопросам информационной безопасности

В соответствии с Регламентом повышения осведомленности в области информационной безопасности все сотрудники Компании проходят соответствующее обучение.

Все новые сотрудники «Норникеля» проходят ознакомление с внутренними нормативно-методическими документами, регламентирующими требования информационной безопасности, и дополнительный вводный инструктаж. В 2022 году около 7,4 тыс. вновь принятых сотрудников были ознакомлены с внутренними нормативно-методическими документами по информационной безопасности, около 4,3 тыс. новых сотрудников прошли дополнительные вводные инструктажи по информационной безопасности.

В «Норникеле» разрабатываются ежегодные планы обучения сотрудников, которые учитывают актуальные тенденции, вновь выявленные риски и киберугрозы. На регулярной основе организуются проверки знаний сотрудников как Главного офиса Компании, так и предприятий, расположенных в регионах присутствия. В 2022 году было проведено около 70 плановых и пяти внеплановых тренингов в формате электронных курсов, обучение прошли почти 18,5 тыс. сотрудников Группы.

В 2022 году обучение прошли почти
18,5 тыс. сотрудников

Полученные теоретические знания подкрепляются практическим опытом в условиях угроз информационной безопасности. Для этого проводятся тренинги и учения, включающие в том числе имитацию фишинговых атак и иных способов незаконного воздействия на корпоративную ИТ-инфраструктуру. Такие практики позволяют провести проверку качества функционирования систем кибербезопасности, отработать действия сотрудников в случае угрозы информационной безопасности, а также повысить общий уровень корпоративной системы информационной безопасности. После анализа результатов тренингов актуализируются существующие и разрабатываются новые инструкции для сотрудников. Обновленная после тренингов информация включается в ежеквартальный бюллетень, рассылаемый руководителям структурных подразделений Компании. Информирование сотрудников о действиях в случае обнаружения подозрительных активностей происходит через внутренние документы, касающиеся вопросов информационной безопасности.

Дополнительно для информирования сотрудников об актуальных угрозах информационной безопасности и правилах цифровой гигиены на регулярной основе организуются тематические информационные рассылки. В 2022 году было выполнено 27 тематических рассылок для всех сотрудников Группы.