В 2024 году Data Platform и ML Platform запущены в промышленную эксплуатацию.

В краткосрочной перспективе (2025–2026 годы) планируется ввести в промышленную эксплуатацию ML-кластеры. Это позволит сократить время реализации цифровых производственных инициатив за счет отсутствия необходимости многократно проектировать и реализовывать интеграционную инфраструктуру, а также снижать аналитическую нагрузку на системы управления/диспетчеризации производства.

Видеоаналитика

В течение отчетного года было расширено применение видеоаналитики (компьютерного зрения) в производственных процессах «Норникеля» в целом и задачах охраны труда и промышленной безопасности в частности, в том числе:

- выполнен тираж разработанной внутренней командой автоматизированной системы контроля использования СИЗ (АС СИЗ) на производственном предприятии Норильской площадки;
- расширен спектр детекций соблюдения правил промышленной безопасности сотрудниками (работа на высоте, вход в опасные зоны работающего оборудования, перевозка людей на технике, не предназначенной для транспортных целей);
- собран мобильный комплекс компьютерного зрения для контроля безопасности выполнения различных работ в отсутствие стационарных камер наблюдения и каналов связи (испытания запланированы на 2025 год);
- введена в промышленную эксплуатацию оптическая идентификация качества никелевых катодов в Цехе электролиза никеля на горно-металлургическом предприятии Кольской площадки, что позволяет в автоматизированном режиме разделять товарный никель по маркам, обеспечивать соответствующую премию за качество и снижать коммерческие потери вследствие влияния человеческого фактора;
- продолжена разработка решения для контроля работы техники в рудниках по видеопотоку с бортовых регистраторов: были созданы модули по распознаванию действий анкероустановщиков, стреловых и веерных буровых машин, что позволяет определить загрузку машин и оборудования, улучшить контроль выполнения наряд-заданий и повысить эффективность диспетчеризации в рудниках.

Взаимодействие с вузами

«Норникель» совместно с Центральным университетом (далее – ЦУ) запустил магистерскую программу «AI в промышленности». С 1 сентября 2024 года студентами направлений Data Science и Data Engineering стали 10 человек. За два года очного обучения они приобретут необходимые компетенции для работы на проектах по внедрению решений на базе искусственного интеллекта. Преподавателями программы являются эксперты ЦУ и сотрудники «Норникеля». Обучение проходит очно в московском кампусе ЦУ в вечернее время.

За время обучения студенты познакомятся с основами программирования, освоят фундаментальную базу в Machine Learning, Deep Learning, Data Engineering, MLOps, а также узнают об автоматизации бизнес-процессов, о базовой автоматизации и об управлении цехами и производством с помощью искусственного интеллекта.

Первый семестр, уровень Start

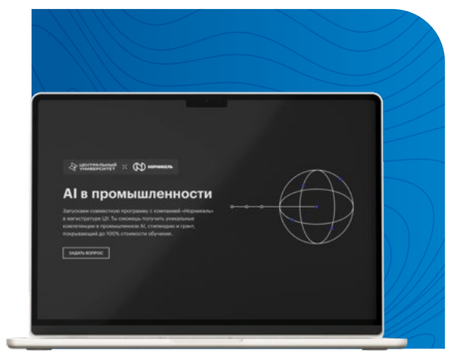
Грант на обучение от ЦУ, стипендия – 30 тыс. руб.

Второй семестр, уровень Medium

Возможность пройти оплачиваемую стажировку в «Норникеле» и получить грант на +50% к гранту, выданному ЦУ

Уровень Pro

Предложение о трудоустройстве в «Норникель» и 100%-ный грант на обучение от Компании



Информационная безопасность

Вклад «Норникеля» в национальный проект «Экономика данных и цифровая трансформация государства» и национальную цель «Цифровая трансформация государственного и муниципального управления, экономики и социальной сферы»

Целевые показатели и задачи:

л) обеспечение сетевого суверенитета и информационной безопасности в информационно-телекоммуникационной сети «Интернет»

Подход Компании к вопросам обеспечения информационной безопасности (ИБ)

Для «Норникеля» предотвращение угроз информационной безопасности – большая ответственность и один из ключевых приоритетов в силу существенного влияния потенциальных рисков ИБ на все сферы жизни, необходимости защиты критической информационной инфраструктуры и новых вызовов современности в области киберустойчивости.

Релевантные ЦУР ООН

9 ИНДУСТРИАЛИЗАЦИЯ, ИННОВАЦИИ И ИНФРАСТРУКТУРА

Связанные федеральные проекты

- «Отечественные решения»
- «Инфраструктура кибербезопасности»

Ключевые инициативы и направления деятельности

- Защита информационных систем и инфраструктуры Компании
- Импортозамещение и поддержка отечественных решений
- Вклад в развитие рынка через создание и развитие стратегических партнерств
- Вклад в нормотворчество и лучшие практики
- Развитие культуры ИБ среди сотрудников

В перспективе Компания планирует продолжить работу в рамках намеченных векторов с акцентом на усиление партнерств, развитие диалога между заказчиками и подрядчиками для минимизации рисков третьих сторон и развитие культуры ИБ в том числе за пределами Компании как вклад в безопасность российского общества

Задачи «Норникеля» в области ИБ в контексте повестки устойчивого развития

- Защита территорий присутствия через непрерывность производственных процессов, устойчивый рост Компании и недопущение аварий с экологическими последствиями
- Положительное влияние на общество через культуру ИБ, формирование партнерств, развитие законодательства
- Управление рисками ИБ в целях повышения защищенности Компании и государства, вклад в развитие рынка ИБ и нормотворчество

Функционирование системы управления информационной безопасностью регламентировано внутрикорпоративными документами. Политика информационной безопасности ПАО «ГМК «Норильский никель» распространяется на всех сотрудников и определяет цели, принципы, правила, требования и ограничения, связанные с осуществлением деятельности в области ИБ, в том числе участие и ответственность Совета директоров и Правления в данной области. К компетенции топ-менеджмента, в частности Первого вице-президента – Финансового директора, относятся вопросы определения и актуализации ключевых стратегических направлений в сфере ИБ, рассмотрения рисков информационной безопасности, а также бюджетов программ и проектов в области ИБ. Регулярный мониторинг рисков ИБ осуществляется в формате профильных комитетов и корпоративной отчетности. Профильным подразделением, обеспечивающим информационную безопасность «Норникеля», является Департамент защиты информации и ИТ-инфраструктуры.

В 2024 году «Норникель» совершенствовал существующие подходы к управлению информационной безопасностью. Для обеспечения планомерного развития функция ИБ идет по пути развития сервисной модели, адаптируя свои подходы под лучшие практики рынка. Повышение эффективности существующих процессов обеспечения ИБ является одной из ключевых целей функции на 2025 год.

При формировании стратегии информационной защиты Компании учитываются как растущие риски информационной безопасности[1], так и поддерживаемый на уровне государства курс на импортозамещение информационных технологий и решений ИБ. Так, в 2024 году был завершен процесс импортозамещения средств защиты информации для систем промышленной автоматизации в технологической инфраструктуре Компании.

Компания делится своей экспертизой с производителями продуктов ИБ и вовлекается в доработку решений, которые затем тиражируются на весь рынок, что оказывает влияние на развитие отрасли ИБ в России.

В Компании принимаются дополнительные меры по защите периметров технологической инфраструктуры предприятий и снижению рисков прерывания и остановки производственных процессов.

С учетом сохранения гибридного режима работы для офисных сотрудников Компании завершен первый этап их перевода на систему двухфакторной аутентификации, которая позволит минимизировать риски, связанные с несанкционированным удаленным доступом к корпоративным ресурсам. Ведется постоянный мониторинг уровня защищенности корпоративных систем, результаты которого позволяют своевременно выявлять и устранять уязвимости, а также принимать необходимые меры для противодействия кибервторжениям.

[1] Риски, связанные с актами киберпреступности в отношении процессов и систем Компании, а также нарушениям законодательства в области персональных данных, зарегистрированы в корпоративной системе управления рисками. Владельцем данных рисков является Департамент защиты информации и ИТ-инфраструктуры. Факторы рисков ИБ, их оценка и основные принимаемые «Норникелем» меры для снижения этих рисков представлены в Отчете об устойчивом развитии «Норникеля» за 2023 год и Годовом отчете «Норникеля» за 2024 год.

В 2024 году с целью улучшения системы управления информационной безопасности в Компании была разработана и утверждена модель корпоративных процессов ИБ, а также внедрена система управления ИБ-процессами, позволяющая агрегировать информацию о ключевых результатах работы и обеспечить высокий уровень доступности ИБ-услуг для внутренних заказчиков в рамках сервисной модели, в том числе посредством дополнительных мероприятий, повышающих уровень защищенности в отношении внешних киберугроз.

Сертификация

Система управления информационной безопасностью «Норникеля» (СУИБ) выстроена в соответствии с требованиями международного стандарта ISO/IEC 27001. Пять предприятий Группы получили сертификат в соответствии с ISO/IEC 27001.

В 2024 году в целях поддержания высокого уровня зрелости процессов обеспечения киберзащиты были реализованы мероприятия по переходу СУИБ-площадок на версию стандарта ISO/IEC 27001:2022. По итогам проведенных проверок площадки подтвердили эффективность процессов управления ИБ. Независимый аудитор отметил высокий уровень вовлеченности руководства в процессы СУИБ, готовность предприятий Группы реагировать на угрозы и вызовы внешней среды. Сотрудники СУИБ продемонстрировали высокий уровень знаний в области информационной безопасности.

Защита и управление уязвимостями

С целью повышения общего уровня защищенности автоматизированных систем управления технологическими процессами (АСУТП) и выполнения рекомендаций, полученных по итогам аудита в 2023 году, все мероприятия, запланированные на 2024 год, выполнены.

Согласно плану по внедрению базовых мер защиты технологических процессов, завершены работы на производственных предприятиях Энергетического дивизиона, что способствует снижению рисков ИБ на предприятиях, обеспечивающих энергобезопасность предприятий Группы и городов Крайнего Севера. В тесном сотрудничестве с ключевыми партнерами по рынку ИБ был доработан и приведен в соответствие требованиям информационной безопасности «Норникеля» ряд отечественных решений, которые предлагаются ведущими производителями систем в области автоматизации технологических и производственных процессов.

В отчетном году Компания развивала подходы к управлению уязвимостями и анализу защищенности корпоративных систем, уделив особое внимание тестированию АСУТП. Были выявлены слабые места в эксплуатируемых системах, приняты своевременные меры по укреплению ИБ. Регулярные мероприятия по анализу защищенности и отработка взаимодействия с командой центра реагирования также позволяют выявлять и устранять узкие места в системах защиты.

Компания совершенствует процессы обеспечения ИБ в рамках жизненного цикла разработки ПО. Внедрение платформы DevSecOps позволяет автоматизировать ключевые элементы контроля безопасности, интегрируя их непосредственно в процессы разработки. Для повышения устойчивости к атакам на цепочку поставок внедрен корпоративный репозиторий программного обеспечения, через который производится установка и обновление стороннего ПО.

>20 тыс.
событий ИБ было отработано сотрудниками центра в 2024 году (>18 тыс. годом ранее)

>1 тыс.
киберинцидентов было проанализировано сотрудниками центра в 2024 году

0
компьютерных инцидентов зафиксировано на объектах критической инфраструктуры «Норникеля» в 2024 году

6 тыс.
проверок по обращениям сотрудников «Норникеля» проведено в 2024 году

Система реагирования на киберинциденты

В «Норникеле» действует Центр мониторинга и реагирования на киберинциденты, в котором используются передовые технические решения и лучшие практики управления процессами киберзащиты. Сотрудники центра регулярно подтверждают высокий уровень компетенций — в 2024 году команда «Норникеля» продемонстрировала уникальные знания и навыки в трех соревнованиях.

Центр осуществляет постоянный мониторинг событий в сфере ИБ и организует обмен опытом с коллегами из других компаний и партнерами по рынку, что позволяет предпринимать упреждающие действия по блокировке действий злоумышленников.

Несмотря на значительный рост компьютерных атак, Компания успешно отразила все попытки злоумышленников нанести ущерб инфраструктуре «Норникеля».

Любой сотрудник «Норникеля» в случае обнаружения подозрительного контента или активности на корпоративных устройствах может направить эту информацию для проверки в функцию ИБ. Специалисты проводят оценку возможного деструктивного влияния на информационные системы Компании и принимают меры, направленные на предотвращение и устранение последствий инцидентов.

Требования к контрагентам

В 2024 году были выявлены факты компрометации информационной инфраструктуры ряда подрядных организаций, в результате которых были приняты меры по блокировке доступа подрядчиков к инфраструктуре «Норникеля» и предотвращены возможные негативные последствия.

Компания разработала раздел договора, устанавливающий требования в области ИБ и ответственность за их невыполнение для контрагентов, которые в рамках договоров получают доступ к информационным активам Компании. Указанный раздел уже в 2024 году включен в общие условия договоров. Кроме этого, внесены изменения в типовое соглашение о конфиденциальности – добавлена обязанность контрагента обеспечить выполнение мер ИБ и предоставлять по запросу Компании сведения о выполнении таких мер. Также были внедрены процесс использования двухфакторной аутентификации для всех сотрудников внешних организаций и ряд ограничительных мер для контрагентов, имеющих привилегированные права в информационных системах.

«Норникель» ведет разработку методики оценки контрагентов Компании на предмет достаточности мер обеспечения ИБ, которая позволит реализовать дополнительную защиту корпоративных информационных активов.

Защита персональных данных

В «Норникеле» реализуется комплекс правовых, организационных и технических мер по обеспечению безопасности персональных данных (ПДн). Техническая защита ПДн обеспечивается средствами антивирусной защиты, предотвращения утечек, контроля отчуждаемых устройств, анализа событий безопасности.

Особое внимание в Компании уделяется обеспечению соответствия процессов обработки ПДн требованиям законодательства, в рамках которых в течение 2024 года профильный департамент Компании разрабатывал и реализовывал на практике корпоративные методические указания.

8 предприятий Группы привели процессы обработки ПДн в полное соответствие требованиям законодательства и внутрикорпоративным документам

11 предприятий Группы провели оценку соответствия сайтов требованиям законодательства в области обработки ПДн

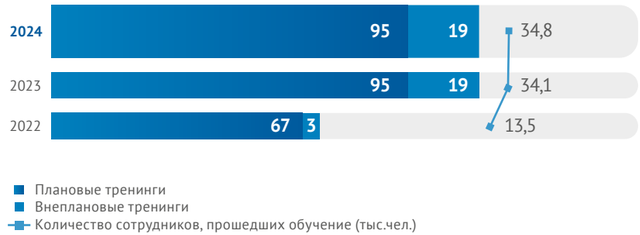
В Компании разработана методика бережной обработки ПДн, направленная на снижение риска утечки ПДн путем минимизации обработки ПДн в рамках бизнес-процессов.

Обучение и информирование в области информационной безопасности

В соответствии с поставленной целью по развитию культуры информационной безопасности в рамках всей Группы и снижению роли человеческого фактора в инцидентах ИБ «Норникель» уделяет особое внимание повышению осведомленности всех категорий сотрудников о требованиях ИБ и правилах цифровой гигиены.

Тематика ИБ включена в массовые корпоративные мероприятия и стратегические сессии. Информирование сотрудников осуществляется через внутренние каналы коммуникации: публикации на корпоративном портале, почтовые рассылки, корпоративный мессенджер, размещение сведений на информационных досках, трансляция видеоматериалов на экранах в общих зонах.

На регулярной основе проводится обучение сотрудников по релевантным темам ИБ, включая онлайн-курсы и тренинги, которые обновляются в ответ на изменяющийся ландшафт угроз и законодательства.



Для повышения бдительности сотрудников и отработки порядка действий в случае инцидентов ИБ регулярно проводятся учения, включающие имитацию фишинговых рассылок и иных актуальных способов незаконного воздействия на пользователей. По итогам учений актуализируются инструкции для сотрудников.

Наряду с этим «Норникель» заботится о личной информационной безопасности сотрудников и членов их семей, проводятся мероприятия для детей сотрудников Компании (игры по кибербезопасности, встречи с экспертами, видеоролики об основах ИБ).

Культура кибербезопасности – часть корпоративного культурного кода, который не ограничивается стенами Компании и способствует повышению уровня защищенности бизнеса и страны в целом.

Партнерство и обмен опытом в области информационной безопасности

Созданный по инициативе «Норникеля» клуб «Безопасность информации в промышленности» (БИП-Клуб) объединяет руководителей и специалистов в области ИБ для обмена опытом, государственно-частного диалога, разработки универсальных требований по ИБ, поиска инновационных решений и развития взаимовыгодных партнерств в целом.

В 2024 году БИП-Клуб продолжил работу и впервые в рамках открытой встречи для рынка объединил на своей площадке одновременно вендоров, интеграторов, заказчиков, а также регуляторов рынка для диалога на тему подходов, требований, ожиданий от партнеров и перспектив эффективного сотрудничества в рамках программы импортозамещения.

Наряду с этим на площадке БИП-Клуба «Норникель» предложил ИБ-сообществу «Кодекс этики для рынка информационной безопасности» – набор принципов, которые помогут повысить зрелость рынка, сделать сотрудничество между заказчиком и подрядчиком более эффективным.

С ключевыми игроками рынка «Норникель» заключает стратегические партнерства, направленные на разработку и внедрение решений для повышения киберустойчивости горно-металлургической отрасли.

Также Компания сотрудничает с рядом крупных российских вузов, с целью реализации совместных проектов и стимулирования молодых специалистов на работу в сфере информационной безопасности в промышленности.

> **Соглашение с «Норникелем» направлено на продолжение и расширение нашего взаимодействия, консолидацию экспертиз, усилий и ресурсов для обеспечения информационной безопасности в горно-металлургической промышленности. Наши эксперты отмечают резкий рост интереса киберпреступников к критической информационной инфраструктуре и прогнозируют увеличение деструктивных атак на российские компании. Вместе с «Норникелем» мы можем внести весомый вклад в обеспечение информационной безопасности отрасли, повышая ее готовность к растущим угрозам и вызовам.**
>
> **Михаил Осеевский,**
> президент «Ростелекома»