Приложение 1

УТВЕРЖДЕНА
приказом Президента
ПАО «ГМК «Норильский никель»
от 03.06.2025 № ГМК/049-п

Политика
в области информационной безопасности

Обозначение документа: УП ГК НН IS.1-2025
Введена взамен: УП ГК НН 167-004-2018
Дата введения: 03.06.2025

Содержание

1. Область применения

1.1. Настоящая Политика в области информационной безопасности (далее – Политика) определяет цели, основные принципы, правила, требования и ограничения деятельности ПАО «ГМК «Норильский никель» (далее – Компания) в области информационной безопасности (далее - ИБ).

1.2. Требования настоящей Политики распространяются на работников Компании и российских организаций корпоративной структуры, входящих в Группу компаний «Норильский никель» (далее – РОКС НН), а также рекомендованы для зарубежных организаций корпоративной структуры, входящих в Группу компаний «Норильский никель» (далее – ЗОКС НН), с учетом ограничений и требований применимого законодательства.

1.3. Политика является основополагающим документом для принятия управленческих решений в области ИБ в Группе компаний «Норильский никель» (далее – Группа) и разработки нормативно-методических документов (далее – НМД) в области ИБ, детализирующих положения настоящей Политики.

2. Цели и задачи

2.1. Основные цели и задачи деятельности в области ИБ представлены в Таблице 1.

Таблица 1 – Цели и задачи деятельности в области ИБ

№	Цель	Задачи
1	2	3
1	Защита информационных активов Группы посредством выполнения комплекса организационно–технических мер по снижению и поддержанию рисков ИБ на приемлемом уровне и минимизации ущерба, возникающего в результате инцидентов ИБ	Снижение рисков ИБ (в т.ч. связанных с возможными кибератаками на информационные активы) Компании и ОКС НН. Обеспечение выполнения требований законодательства Российской Федерации в области ИБ. Минимизация финансового и репутационного ущерба Компании и РОКС НН в случае инцидентов ИБ. Обеспечение надлежащего уровня ИБ при внедрении новых технологий. Обеспечение информированности Руководителей Компании по актуальным вопросам обеспечения ИБ Компании и ОКС НН, в т.ч. о текущем и прогнозируемом состоянии обеспечения ИБ Компании и ОКС НН

3. Принципы, требования и ограничения

3.1. Основные принципы деятельности в области ИБ представлены в Таблице 2.

Таблица 2 – Принципы деятельности в области ИБ

№	Описание принципов деятельности в области ИБ
1	2
1	*Ориентация на бизнес:* защита информационных активов, информационных систем и компонентов ИТ–инфраструктуры, систем управления производственными процессами (далее - MES), автоматизированных систем управления технологическими процессами (далее – АСУТП), используемых в Блоках и бизнес–процессах Группы и создающихся в результате реализации программ/проектов в соответствии с Корпоративной стратегией и целевой ИТ–архитектурой; создание добавленной стоимости и преимуществ для бизнеса от реализации программы ИБ; обеспечение соизмеримости затрат на ИБ с ценностью защищаемых информационных активов
2	*Защита бизнеса:* защита информационных активов посредством применения проактивного (управление рисками ИБ) и реактивного (управление инцидентами ИБ) подходов к управлению и обеспечению ИБ, интеграция деятельности в области ИБ в бизнес–процессы и операционную деятельность Группы
3	*Лидерство:* способность Руководителей Компании, Руководителей Обособленных подразделений, РОКС НН, ЗОКС НН оказывать влияние на подчиненных работников и направлять их усилия на достижение целей ИБ путем демонстрации приверженности и единства в следовании настоящей Политике, обязательств по рассмотрению и поддержке инициатив ИБ
4	*Инновации:* использование новых технологий и подходов, обеспечивающих повышение результативности и эффективности принимаемых организационно–технических мер ИБ
5	*Продвижение культуры ИБ:* повышение осведомленности работников Компании, РОКС НН, ЗОКС НН и третьих лиц в области ИБ, демонстрация профессионального и этичного отношения к деятельности в области ИБ
6	*Единая интегрированная методология:* разработка и применение в Группе стандартов, унифицированных подходов на базе лучших отечественных и международных практик в области ИБ, использование всех ресурсов и их взаимосвязей в комплексе для достижения целей ИБ
7	*Целостная структура:* эффективные коммуникации и обмен информацией между Главным офисом Компании, Обособленными подразделениями, РОКС НН, ЗОКС НН в области ИБ, следование единой Стратегии ИБ и настоящей Политике
8	*Ответственность:* каждый работник Компании, РОКС НН, ЗОКС НН несет ответственность за ненадлежащее использование информационных активов и управление рисками ИБ в рамках своих компетенций
9	*Социальная ответственность:* участие в общественных мероприятиях и профессиональных сообществах в области ИБ, внесение вклада в развитие ИБ и борьбу с киберпреступностью для обеспечения стабильности социально-экономического развития горно-металлургической отрасли
10	*Постоянное совершенствование:* построение деятельности и Бизнес-процессов в области ИБ, владельцем которых является директор Департамента защиты информации и IT инфраструктуры (далее – ДЗИиИТИ) в соответствии с Корпоративной процессной моделью (далее – Бизнес-процессы в области ИБ), в соответствии с подходом PDCA

3.2. Основные требования и ограничения деятельности в области ИБ представлены в Таблице 3.

Таблица 3 – Требования и ограничения деятельности в области ИБ

№	Описание требований и ограничений деятельности в области ИБ
1	2
1	Информационные активы, информационные системы/компоненты ИТ–инфраструктуры, MES, АСУТП применяются исключительно для выполнения бизнес–процессов и достижения целей деятельности Группы. Запрещается нецелевое использование информационных активов, информационных систем/компонентов ИТ–инфраструктуры, MES, АСУТП
2	Все действия с информационными активами (получение, сбор, ввод, обработка, хранение, вывод, уничтожение и др.) выполняются с соблюдением требований ИБ
3	Контроль выполнения требований ИБ осуществляется на всех стадиях жизненного цикла информационных активов, информационных систем/компонентов ИТ–инфраструктуры, MES, АСУТП. Запрещается ввод в эксплуатацию и эксплуатация информационных систем/компонентов ИТ–инфраструктуры, MES, АСУТП без выполнения требований ИБ, либо без согласования перечня компенсирующих мер ИБ с ДЗИиИТИ/Службами ИБ
4	Для управления рисками ИБ применяются предупредительные, обнаруживающие, корректирующие и компенсирующие организационно–технические меры ИБ
5	Планирование, выбор и обоснование применимости организационно–технических мер ИБ осуществляется на основании результатов идентификации/классификации информационных активов, информационных систем/компонентов ИТ–инфраструктуры, оценки рисков ИБ, требований законодательства и регуляторов
6	Стратегическое управление ИБ выполняется в Главном офисе Компании. Организация деятельности в области ИБ в Группе вне рамок Стратегического управления ИБ (Программы и Стратегии ИБ, настоящей Политики) допускается при условии предварительного согласования с Первым вице-президентом – Финансовым директором
7	Тактическое управление (менеджмент) ИБ выполняется в Главном офисе Компании, Обособленных подразделениях, РОКС НН, ЗОКС НН в соответствии со Стратегическим управлением ИБ (Программой и Стратегией ИБ, настоящей Политикой)
8	Операционная деятельность ИБ в Главном офисе Компании, Обособленных подразделениях, РОКС НН, ЗОКС НН выполняется в рамках Тактического управления ИБ и включает процессы ИБ операционного уровня в рамках Бизнес-процессов в области ИБ
9	В случае отсутствия Служб ИБ и необходимых ресурсов ИБ в Компании и РОКС НН реализация требований ИБ осуществляется структурными подразделениями ООО «Норникель Спутник», или внешними организациями на договорной

№	Описание требований и ограничений деятельности в области ИБ
1	2
	основе[1] по согласованию с ДЗИиИТИ и в соответствии с НМД Компании/РОКС НН в области закупочной деятельности, договорной работы, НМД Компании/РОКС НН, регламентирующими порядок передачи бизнес-процессов на аутсорсинг (если применимо)
10	В случае отсутствия Служб ИБ и необходимых ресурсов ИБ в ЗОКС НН реализация требований ИБ осуществляется на договорной основе внешними организациями по согласованию с ДЗИиИТИ
11	Выбор технических средств защиты Группы осуществляется в соответствии с требованиями Методики применяемых средств защиты информации ПАО «ГМК «Норильский никель»

4. Объекты Политики

4.1. Ключевыми объектами управления деятельности в области ИБ являются используемые в бизнес–процессах Группы:

- информационные активы;
- информационные системы/компоненты ИТ–инфраструктуры;
- MES;
- АСУТП.

5. Субъекты Политики

5.1. Субъекты управления деятельности в области ИБ представлены в Таблице 4.

Таблица 4 – Субъекты управления деятельности в области ИБ

№	Субъект	Ключевые принимаемые решения
1	2	3
1	Первый вице-президент – Финансовый директор	– определяет ключевые стратегические направления деятельности Группы в области ИБ; – осуществляет контроль выполнения требований законодательства Российской Федерации и НМД Компании, РОКС НН в области ИБ, обеспечение соответствия применяемых организационно-технических мер ИБ требованиям законодательства Российской Федерации и регуляторов, международным и российским стандартам в области ИБ; – контроль организации и осуществления деятельности по выявлению и реагированию на инциденты ИБ в

[1] В качестве подрядных организаций, предоставляющих (выполняющих, оказывающих) сервисы (работы, услуги) по обеспечению ИБ Компании и РОКС НН, являющимся субъектами критической информационной инфраструктуры, не могут привлекаться юридические лица, находящиеся под юрисдикцией иностранных государств, совершающих в отношении Российской Федерации, российских юридических лиц и физических лиц недружественные действия, прямо или косвенно подконтрольные таким организациям, либо аффилированные с ними.

№	Субъект	Ключевые принимаемые решения
1	2	3
		Компании и координирует деятельность по выявлению и реагированию на инциденты ИБ в РОКС НН
2	ДЗИиИТИ	– осуществляет разработку и актуализацию стратегии Компании и программ в области ИБ, политики ИБ, целевой Архитектуры ИБ в Компании и РОКС НН, стандартизацию и унификацию применяемых подходов и технических средств защиты информации в Компании и РОКС НН; – осуществляет контроль: • выполнения требований ИБ (в том числе в рамках деятельности Архитектурного подкомитета) на всех стадиях жизненного цикла информационных активов, информационных систем/компонентов ИТ–инфраструктуры, MES, АСУТП; • защищенности информационных систем и компонентов ИТ-инфраструктуры, MES, АСУТП; • предоставления доступа к информационным активам, информационным системам и компонентам ИТ-инфраструктуры, MES, АСУТП Компании и РОКС НН; • выполнения требований ИБ третьими лицами, привлекаемыми при эксплуатации, сопровождении информационных систем/компонентов ИТ–инфраструктуры, MES, АСУТП; – осуществляет управление рисками Компании и ОКС НН в области ИБ; – осуществляет выявление и реагирование на инциденты ИБ в Компании в порядке, установленном нормативными правовыми актами Российской Федерации и НМД Компании и РОКС НН в области ИБ, координирует выявление и реагирование на инциденты ИБ в РОКС НН, в том числе обнаружение, предупреждение и ликвидацию последствий компьютерных атак, и реагирование на компьютерные инциденты; – проводит разработку и актуализацию НМД Компании и РОКС НН в области ИБ по функциональным направлениям ИБ, описание Бизнес-процессов в области ИБ в Автоматизированной системе управления Корпоративной процессной моделью (далее - АСУ КПМ); – осуществляет деятельность по обеспечению соответствия применяемых организационно-технических мер ИБ в Компании, РОКС НН требованиям законодательства Российской Федерации, регуляторов, международным и российским стандартам в области ИБ, формирует предложения по обеспечению ИБ в ЗОКС НН; – осуществляет деятельность по разработке и реализации мероприятий по защите информационных активов, информационных систем и компонентов

№	Субъект	Ключевые принимаемые решения
1	2	3
		ИТ-инфраструктуры, MES, АСУТП Компании и ОКС НН, в т.ч. эксплуатацию систем и средств защиты информации в Компании и ОКС НН; – осуществляет управление комплаенсом в области ИБ в Компании и РОКС НН; – осуществляет деятельность по обеспечению непрерывности ИБ в Компании и РОКС НН; – осуществляет взаимодействие в установленном в Компании порядке с представителями уполномоченных органов государственной власти, регуляторов по вопросам, относящимся к области ИБ, контролирует исполнение их указаний; – разрабатывает, внедряет и осуществляет последующую поддержку методологии планирования бюджетов на деятельность в области ИБ, в том числе оказывает методическую помощь бизнес-единицам в соответствии с Бюджетным регламентом ПАО «ГМК «Норильский никель»
3	Службы ИБ	– участвуют в осуществлении контроля в Обособленных подразделениях/РОКС НН: • защищенности информационных систем и компонентов ИТ-инфраструктуры, MES, АСУТП в Обособленных подразделениях/РОКС НН; • предоставления доступа к информационным активам, информационным системам и компонентам ИТ-инфраструктуры, MES, АСУТП Компании и РОКС НН; • выполнения требований ИБ третьими лицами, привлекаемыми при эксплуатации, сопровождении информационных систем/компонентов ИТ–инфраструктуры, MES, АСУТП в Обособленных подразделениях/РОКС НН; – осуществляют выявление и реагирование на инциденты ИБ в РОКС НН в порядке, установленном нормативными правовыми актами Российской Федерации и НМД Компании и РОКС НН в области ИБ, в том числе обнаружение, предупреждение и ликвидацию последствий компьютерных атак, и реагирование на компьютерные инциденты; – разрабатывают и актуализируют НМД Обособленных подразделений/РОКС НН в области ИБ; - участвуют в деятельности Обособленных подразделений/РОКС НН по следующим вопросам: • управление рисками ИБ; • выявление и реагировании на инциденты ИБ в Обособленных подразделениях в порядке, установленном нормативными правовыми актами Российской Федерации и НМД Компании и РОКС НН

№	Субъект	Ключевые принимаемые решения
1	2	3
		в области ИБ, в том числе в обнаружение, предупреждение и ликвидация последствий компьютерных атак, и реагирование на компьютерные инциденты; • разработка и актуализация НМД Компании в области ИБ; • обеспечение соответствия применяемых организационно-технических мер ИБ требованиям законодательства Российской Федерации, регуляторов, международным и российским стандартам в области ИБ; • защита информационных активов, информационных систем и компонентов ИТ-инфраструктуры, MES, АСУТП, в т.ч. эксплуатация систем и средств защиты информации; • управление комплаенсом ИБ; • непрерывность ИБ
4	Департамент информационных технологий (далее – ДИТ)/Сервисные линии ООО «Норникель Спутник»/Службы ИТ	– обеспечивают выполнение требований ИБ: – при формировании/актуализации ИТ-стратегии и ИТ-архитектуры; – при формировании планов реализации, сопровождения и развития решений, обеспечивающих автоматизацию деятельности Блоков и бизнес–процессов Группы; – на стадиях ИТ-инициатив, ИТ-проектов, ИТ-программ, проектов с ИТ–составляющей, на стадиях жизненного цикла информационных систем/компонентов ИТ–инфраструктуры, MES; – при эксплуатации и сопровождении информационных систем/компонентов ИТ–инфраструктуры, MES; – при организации деятельности в рамках направлений ДИТ/Сервисных линий ООО «Норникель Спутник»/Служб ИТ; – обеспечивают доступность информационных активов, непрерывность работы информационных систем/компонентов ИТ–инфраструктуры, MES, восстановление после сбоев и чрезвычайных ситуаций; – формируют бюджеты мероприятий, направленных на снижение рисков ИБ, возникающих в рамках проектной и/или эксплуатационной деятельности в области ИТ, в соответствии с Бюджетным регламентом ПАО «ГМК «Норильский никель»
5	Департамент защиты государственной тайны, мобилизационной	– формирует требования по организации защиты информации, составляющей коммерческую тайну, и осуществляет контроль выполнения этих требований;

№	Субъект	Ключевые принимаемые решения
1	2	3
	подготовки и специальной связи	– осуществляет методическую поддержку ДЗИиИТИ в части формирования требований по технической защите информации, составляющей коммерческую тайну
6	Департамент корпоративных отношений	– формирует требования по организации защиты инсайдерской информации и осуществляет контроль выполнения этих требований; – осуществляет методическую поддержку ДЗИиИТИ в части формирования требований по технической защите инсайдерской информации
7	Департамент промышленных активов	– осуществляет оценку последствий для технологических и производственных процессов от нарушений ИБ АСУТП (нарушения целостности и доступности информации, обрабатываемой АСУТП); – осуществляет согласование планов мероприятий по управлению рисками ИБ АСУТП, разработанных ДЗИиИТИ, и формирует бюджеты на данные мероприятия; – выполняет требования ИБ: – при формировании/актуализации стратегии и планов развития промышленной автоматизации и АСУТП; – на стадиях ИТ-инициатив, ИТ-проектов, ИТ-программ, проектов с ИТ–составляющей, других проектов в области промышленной автоматизации, автоматизации деятельности Операционного блока и на стадиях жизненного цикла АСУТП; – при эксплуатации и сопровождении АСУТП; – контролирует выполнение требований ИБ третьими лицами, привлекаемыми при эксплуатации и сопровождении АСУТП и на стадиях программ и проектов по автоматизации деятельности Операционного блока, производственных и технологических процессов
8	Департамент расследований и экономической защиты	– проводит проверочные мероприятия и служебные расследования по инцидентам ИБ при получении соответствующей информации от ДЗИиИТИ, в том числе участвует во взаимодействии с правоохранительными органами по инцидентам ИБ; – формирует исходные данные для разработки требований ИБ для инженерно-технических средств безопасности (далее - ИТСБ); – реализует в Главном офисе Компании мероприятия и координирует деятельность подразделений и служб безопасности Обособленных подразделений Компании и РОКС НН по обеспечению ИБ ИТСБ с учетом требований ДЗИиИТИ в области ИБ
9	Подкомитет по управлению рисками ИБ в составе	– осуществляет принятие решений по вопросам:

№	Субъект	Ключевые принимаемые решения
1	2	3
	Профильного комитета по управлению рисками Блока экономики и финансов	– оценки ключевых/значимых рисков ИБ, связанных с отклонением от действующих требований ИБ; – отчетности по управлению ключевыми/значимыми рисками ИБ, согласования методических материалов для работников Служб ИБ, рассмотрения замечаний аудита в отношении управления рисками ИБ и статусов исполнения мероприятий по устранению замечаний; – управления рисками ИБ для вынесения вопросов на уровень Профильного Комитета по управлению рисками Блока экономики и финансов
10	Владельцы бизнес–процессов	– назначают Владельцев информационных активов; – организуют соблюдение требований настоящей Политики и НМД в области ИБ (паспортов Бизнес-процессов в области ИБ), разработанных в развитие настоящей Политики, участниками бизнес–процессов, включая работников третьих лиц, привлекаемых на договорной основе
11	Руководители Обособленных подразделений, РОКС НН, ЗОКС НН	– организуют соблюдение и исполнение принципов и требований настоящей Политики и НМД в области ИБ (паспортов Бизнес-процессов в области ИБ), разработанных в развитие настоящей Политики, в Обособленных подразделениях, РОКС НН, ЗОКС НН; – осуществляют обеспечение ресурсами, организацию и контроль деятельности по функциональным направлениям ИБ в Обособленных подразделениях, РОКС НН, ЗОКС НН в соответствии с требованиями настоящей Политики и НМД в области ИБ, разработанных в развитие настоящей Политики; – осуществляют организацию и контроль исполнения мероприятий в области ИБ в Обособленных подразделениях/РОКС НН (в том числе рассмотрение и, при необходимости, утверждение планов мероприятий и отчетов ИБ); – определяют работника, ответственного за осуществление деятельности в области ИБ в Обособленных подразделениях, РОКС НН, ЗОКС НН
12	Владельцы информационных активов	– проводят оценку ценности и последствий от нарушения конфиденциальности, целостности и доступности информационных активов; – осуществляют согласование результатов оценки рисков ИБ и планов мероприятий по управлению рисками ИБ

6. Ответственность

6.1. Ответственность за ненадлежащую организацию и неосуществление контроля исполнения требований настоящей Политики несет Первый вице-президент – Финансовый директор.

6.2. Ответственность за несвоевременное внесение изменений и дополнений в настоящую Политику несет Первый вице-президент – Финансовый директор.

Приложение А

Сокращения

PDCA	Plan-Do-Check-Act (Планирование - Выполнение - Контроль – Воздействие), цикл Деминга
Архитектурный подкомитет	Архитектурный подкомитет ИТ-комитета ПАО «ГМК «Норильский никель»
АСУТП	Автоматизированные системы управления технологическими процессами
Бизнес-процессы в области ИБ	Бизнес-процессы в области ИБ, владельцем которых является директор ДЗИиИТИ в соответствии с Корпоративной процессной моделью
Главный офис Компании	Главный офис ПАО «ГМК «Норильский никель»
Группа	Компания и совокупность организаций корпоративной структуры, входящих в Группу компаний «Норильский никель»
ДЗИиИТИ	Департамент защиты информации и IT инфраструктуры Главного офиса ПАО «ГМК «Норильский никель»
ДИТ	Департамент информационных технологий Главного офиса ПАО «ГМК «Норильский никель»
ЗОКС НН	Зарубежные организации корпоративной структуры, входящие в Группу компаний «Норильский никель»
ИБ	Информационная безопасность
ИТ	Информационные технологии
ИТСБ	Инженерно-технические средства безопасности
Компания	ПАО «ГМК «Норильский никель»
Корпоративная стратегия	Стратегия развития Компании
Непрерывность ИБ	Способность, в случае реализации нештатных ситуаций, обеспечить функционирование процессов ИБ и средств защиты информации, а также способность продолжать оказание услуг ИБ на заранее согласованном приемлемом уровне
НМД	Нормативно–методические документы Компании
Обособленные подразделения	Филиалы и представительство ПАО «ГМК «Норильский никель»
ОКС НН	Организации корпоративной структуры, входящие в Группу компаний «Норильский никель»
РОКС НН	Российские организации корпоративной структуры, входящие в Группу компаний «Норильский никель»

Руководитель РОКС НН	Единоличный исполнительный орган российской организации корпоративной структуры, входящей в Группу компаний «Норильский никель»
Служба ИБ	Структурное подразделение, отвечающее за обеспечение информационной безопасности в Обособленном подразделении Компании/РОКС НН/ЗОКС НН (или работник, на которого в Обособленном подразделении/РОКС НН/ЗОКС НН возложены соответствующие функции) или организация, оказывающая Компании/РОКС НН/ЗОКС НН услуги в области ИБ (в рамках заключенного договора)
Служба ИТ	Структурное подразделение Обособленного подразделения Компании/РОКС НН/ЗОКС НН, осуществляющее функции ИТ, или работник Обособленного подразделения Компании/РОКС НН/ЗОКС НН, ответственный за установку и обслуживание ИС/компонентов ИТ-инфраструктуры, обеспечивающих бесперебойное функционирование ИС/компонентов ИТ-инфраструктуры или организация, оказывающая Компании/РОКС НН/ЗОКС НН услуги в области ИТ (в рамках заключенного договора)

Приложение Б

Термины

Термины представлены в отдельном файле в формате Excel, являющимся неотъемлемой частью настоящей Политики.

Термины.xlsx