НОРНИКЕЛЬ

КОЛЬСКАЯ ГМК

ПРИКАЗ

«03» мая 2018г. №КГМК-270-п

г. Мончегорск

**О применении Политики
ПАО «ГМК «Норильский никель»
в области информационной безопасности**

В целях защиты информационных активов АО «Кольская ГМК» от угроз информационной безопасности,

ПРИКАЗЫВАЮ:

1. Принять к применению в АО «Кольская ГМК» Политику ПАО «ГМК «Норильский никель» в области информационной безопасности УП ГК НН 167-004-2018 (далее - Политика), утвержденную приказом президента ПАО «ГМК «Норильский никель» от 05.04.2018 № ГМК/34-п (Приложение к приказу).

2. Главному инженеру – техническому директору, заместителям генерального директора и руководителям СП по направлениям деятельности довести до сведения подчиненного персонала и обеспечить исполнение требований Политики.

3. Заместителю генерального директора - директору департамента безопасности А.В. Вершинину разместить электронную версию Политики и настоящего приказа в информационной системе электронного архива нормативной документации «Алее Архив» в разделе Департамент безопасности.

Срок – 3 дня с даты подписания настоящего приказа.

4. Считать утратившей силу и изъять из обращения «Политику ОАО «Кольская ГМК» в области информационной безопасности», введенную в действие приказом от 10.11.2014г. №695.

5. Контроль за исполнением настоящего приказа возложить на Заместителя генерального директора - директора Департамента безопасности А.В. Вершинина.

Генеральный директор **Е.В. Борзенко**

И.С. Матвеев
(81536)77768

Приложение

К приказу генерального директора АО «Кольская ГМК» от «03» апреля 2018г. №КГМК-270-п

УТВЕРЖДЕНА
приказом Президента
ПАО «ГМК «Норильский никель»
от 05.04.2018 № ГМК/34-п

Политика

ПАО «ГМК «Норильский никель» в области информационной безопасности

Обозначение документа: УП ГК НН 167-004-2018
Введена впервые.
Дата введения: 05.04.2018

Содержание

1. Область и границы применения Политики 3
2. Нормативные ссылки 3
3. Термины, определения и сокращения 5
4. Принципы деятельности в области информационной безопасности 11
5. Объекты и субъекты Политики 12
6. Правила, требования и ограничения деятельности 18
7. Ответственность 19

1. Область и границы применения Политики

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

1.2. Целью разработки и реализации настоящей Политики является защита информационных активов Группы компаний «Норильский никель» (далее – Группа) посредством выполнения комплекса организационно–технических мер по снижению и поддержанию рисков информационной безопасности на приемлемом уровне и минимизации ущерба, возникающего в результате инцидентов информационной безопасности.

1.3. 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.

1.4. Требования настоящей Политики не распространяются на информацию, составляющую государственную тайну.

1.5. Политика является основополагающим документом для принятия управленческих решений в области информационной безопасности в Группе компаний и разработки нормативно-методических документов (далее – НМД), детализирующих положения настоящей Политики.

1.6. Политика разработана в соответствии с действующим законодательством Российской Федерации, Уставом и иными внутренними документами Компании.

2. Нормативные ссылки

При разработке Политики были использованы следующие нормативные документы:

от 27.07.2006 №149-ФЗ	Федеральный закон «Об информации, информационных технологиях и о защите информации»
от 27.07.2006 № 152-ФЗ	Федеральный закон «О персональных данных»
от 29.07.2004 № 98-ФЗ	Федеральный закон «О коммерческой тайне»
от 27.07.2010 № 224-ФЗ	Федеральный закон «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации»
от 26.07.2017 № 187-ФЗ	Федеральный закон «О безопасности критической информационной инфраструктуры Российской

	Федерации»
ГОСТ Р ИСО/МЭК 15408-1-2012	Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель
ГОСТ Р ИСО/МЭК 27001-2006	Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования
ГОСТ Р ИСО/МЭК 27002-2012	Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности
ГОСТ Р ИСО/МЭК 13335-1-2006	Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий
ГОСТ 34.601-90	Национальный стандарт Российской Федерации. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания
С НН 42-003-2017	Стандарт разработки нормативно-методических и организационно-правовых документов ПАО «ГМК «Норильский никель»
С НН 42-004-2017	Стандарт организации Системы управления бизнес-процессами ПАО «ГМК «Норильский никель»
СТО ГМК-НН 167-005-2017	Стандарт организации «Обеспечение техническими средствами защиты ИТ-инфраструктуры ПАО «ГМК «Норильский никель»
П ГМК-ГО 147-001-2015	Положение о стратегическом планировании ПАО «ГМК «Норильский никель»
П ГМК-НН 165-008-2014	Положение об организации работ по защите информации в автоматизированных системах ОАО «ГМК «Норильский никель»

П ГМК-ГО 44-001 2012	Положение о порядке обращения в Главном офисе ОАО «ГМК «Норильский никель» с информацией, составляющей коммерческую тайну
П ГМК-НН 167-008-2017	Положение об обработке и обеспечении безопасности персональных данных в ПАО «ГМК «Норильский никель»
Р ГМК-НН 112-003-2017	Регламент взаимодействия структурных подразделений и должностных лиц ПАО «ГМК «Норильский никель» при исполнении Регламента № 596/2014 Европейского парламента и Совета Европейского Союза «О злоупотреблениях на рынке» в части противодействия неправомерному использованию инсайдерской информации

3. Термины, определения и сокращения

3.1. В настоящей Политике применены термины с соответствующими определениями:

3.1.1. **Архитектура ИБ:** модель, описывающая множество взаимосвязанных информационных технологий, организационных мер и средств защиты информации совместимых друг с другом и интегрированных с ИТ–архитектурой, комплексная и совместная работа которых обеспечивает достижение цели информационной безопасности.

3.1.2. **Архитектурный подкомитет ИТ-комитета ПАО «ГМК «Норильский никель»:** коллегиальный совещательный орган, обеспечивающий выработку и принятие архитектурных решений для ИТ-комитета, Старшего вице-президента – Финансового директора, Президента, Правления, кураторов ИТ-проектов, руководителей ИТ-проектов, заинтересованных подразделений Компании в отношении: ключевых принципов, стандартов и планов в области развития и эксплуатации информационных систем с учетом задач и приоритетов развития по основным направлениям деятельности Компании и российских организаций корпоративной структуры, входящих в Группу компаний «Норильский никель».

3.1.3. **Бизнес-процесс:** повторяющаяся совокупность упорядоченных и взаимосвязанных действий, создающих ожидаемый результат, представляющий ценность для потребителя.

3.1.4. **Блок (Бизнес–направление):** объединение структурных подразделений Главного офиса Компании по родственным направлениям деятельности, подчиненных Первому вице-президенту, Старшему вице-президенту, Вице-президенту, руководителю прямого подчинения Президенту Компании (в соответствии с утвержденным в Компании распределением функций между Первыми вице-президентами, Старшими вице-президентами, Вице-президентами, руководителями прямого подчинения Президенту Компании).

3.1.5. **Бюджетный процесс:** регламентированная внутренними документами ПАО «ГМК «Норильский никель» деятельность по составлению, рассмотрению, утверждению, контролю и анализу исполнения планов и бюджетов Группы компаний «Норильский никель».

3.1.6. **Владелец бизнес–процесса:** Руководитель Компании или руководитель структурного подразделения Компании, устанавливающий иерархическую структуру, характеристики и правила выполнения бизнес-процесса, отвечающий за достижение целевых значений ключевых показателей эффективности бизнес-процесса, своевременное выявление и анализ рисков бизнес-процесса, внедрение и эффективное функционирование контрольных процедур, направленных на снижение рисков бизнес-процессов, и обладающий ресурсами и полномочиями по управлению и улучшению (оптимизации) бизнес-процесса.

3.1.7. **Владелец информационного актива:** должностное лицо, назначенное владельцем бизнес-процесса, для обеспечения результативности и эффективности которого применяется информационный актив, и для автоматизации которого используется информационная система, обрабатывающая информационный актив.

3.1.8. **Группа компаний «Норильский никель»:** Компания и совокупность Организаций корпоративной структуры, входящих в Группу компаний «Норильский никель».

3.1.9. **Идентификация информационных активов:** процесс определения принадлежности информационного актива, информационной системы, компонента ИТ–инфраструктуры Блоку, структурному подразделению, бизнес–процессу, для повышения эффективности и результативности которых они применяются.

3.1.10. **Информационный актив:** информация с реквизитами, позволяющими ее идентифицировать; имеющая ценность для организации; находящаяся в распоряжении организации и представленная на любом материальном носителе в пригодной для ее обработки, хранения или передачи форме.

3.1.11. **Информационная система:** совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

3.1.12. **Инцидент информационной безопасности:** одно или несколько нежелательных, или неожиданных событий информационной безопасности, которые со значительной степенью вероятности приводят к компрометации операций бизнеса и создают угрозы для информационной безопасности.

3.1.13. **ИТ-архитектура:** описание (модель) основного устройства (структуры) и связей частей информационной системы (физического или концептуального объекта, или сущности), необходимая для обеспечения комплексного подхода при развертывании новых и поддержке существующих информационных систем.

3.1.14. **ИТ-инфраструктура:** совокупность систем сбора, обработки, хранения и передачи данных. Включает в себя:

– инженерные системы обеспечения жизнедеятельности центров обработки данных, серверных и кроссовых помещений (системы кондиционирования, охлаждения, электропитания и т.д.);

– средства централизованного хранения и обработки данных (серверное оборудование, системы резервного копирования, дисковые и ленточные массивы);

– системное и системообразующее программное обеспечение, системы виртуализации;

– системные каталоги (включая Active Directory);

– системы управления базами данных;

– средства вычислительной техники (рабочие станции, мониторы и периферийное оборудование, включая типовой комплект ПО рабочих мест пользователей;

– программно-аппаратный комплекс «киоски самообслуживания»;

– сети хранения данных;

– структурированные кабельные сети и системы управления коммутацией;

– локальные вычислительные сети (активное и пассивное оборудование);

– системы передачи данных и управления технологическим процессом;

– копировально-множительную аппаратуру (коллективного, группового и персонального пользования);

– средства связи (учрежденческие автоматические телефонные станции и их компоненты, стационарные телефоны и факсимильные аппараты, мобильные средства связи и др.) и видеосвязи;

– средства телекоммуникаций (каналы связи, телекоммуникационное оборудование);

– средства корпоративных коммуникаций (электронная почта и т.п.);

– системы управления и мониторинга компонентов инфраструктуры, ИТ-систем и ИТ-персонала;

– техническую и организационную документацию, связанную с эксплуатацией, поддержкой и сопровождением ИТ-систем и инженерных систем.

3.1.15. **Классификация информационных активов:** присвоение существующим информационным активам типа в зависимости от степени тяжести последствий от потери их значимых свойств информационной безопасности.

3.1.16. **Корпоративная система управления рисками (риск-менеджмент):** систематический процесс выявления, оценки и воздействия на риски, базирующийся на инфраструктуре управления рисками и единых принципах, осуществляемый во всех сферах деятельности и на всех организационных уровнях Компании, для:

– повышения вероятности достижения поставленных целей;

– повышения эффективности распределения ресурсов;

– повышения инвестиционной привлекательности и акционерной стоимости Компании.

3.1.17. **Метрика информационной безопасности:** количественная мера, которая позволяет измерить результативность, эффективность, степень

достижения цели и другие качества деятельности в области информационной безопасности.

3.1.18. **Меры (обеспечения) информационной безопасности**: совокупность действий, направленных на разработку и/или практическое применение способов и средств защиты информации.

3.1.19. **Общий центр обслуживания:** ООО «Норникель – общий центр обслуживания», в которое переносится часть вспомогательных бизнес-процессов Компании и РОКС НН в целях повышения эффективности, снижения затрат и улучшения качества вспомогательных бизнес-процессов Компании и РОКС НН, в том числе, но не ограничиваясь, следующих вспомогательных бизнес-процессов: информационное-технологическое обслуживание и телекоммуникации (ИТ-функция), управление ИТ-проектами, бухгалтерский учёт, налоговый учет, казначейские функции, управление персоналом.

3.1.20. **Приемлемый уровень риска:** допустимый и обоснованный уровень исходя из анализа причин риска бизнес-процессов, последствий риска, затрат и полученных результатов от снижения риска, а также реальных возможностей его снижения с помощью действий по устранению недостатков для достижения целей процесса.

3.1.21. **Программа информационной безопасности:** совокупность взаимосвязанных проектов и другой деятельности в области информационной безопасности, направленных на достижение целей информационной безопасности и реализуемых в условиях существующих возможностей и ограничений.

3.1.22. **Работники Компании:** физические лица, которые находятся с ПАО «ГМК «Норильский никель» в трудовых отношениях, оформленных в соответствии с законодательством Российской Федерации.

3.1.23. **Ресурсы информационной безопасности:** персонал и компетенции, организационные структуры, информация, процессы, технологии, бюджеты, программно–аппаратные средства, услуги информационной безопасности, используемые для защиты информационных активов.

3.1.24. **Руководитель Компании:** Президент, Первые вице-президенты, Старшие вице-президенты, Вице-президенты, руководители прямого подчинения Президенту Компании.

3.1.25. **Сервисные линии ОЦО:** Подразделения ОЦО по направлениям бизнес-приложений, промышленной и производственной автоматизации и методологии, ИТ-инфраструктуры, ответственные за формирование проектных решений, реализацию проектов, эксплуатацию ИТ-решений в рамках своего направления, решение инцидентов и проблем (Вторая линия поддержки), управление ИТ-активами в рамках своей области (НМА, Оборудование), формирование и описание потребности в ИТ-закупках.

3.1.26. **Система управления (менеджмента) информационной безопасностью:** совокупность взаимосвязанных ресурсов информационной безопасности и формализованный порядок их применения для управления информационной безопасностью.

3.1.27. **Средства защиты информации:** технические, программные, программно-технические средства, предназначенные или используемые для защиты информации.

3.1.28. **Стратегическое управление информационной безопасностью:** вид деятельности, обеспечивающий уверенность в достижении целей информационной безопасности путём:

– сбалансированной оценки потребностей бизнеса, существующих условий и возможностей;

– установления направления развития информационной безопасности через приоритизацию и принятие решений;

– мониторинга соответствия фактических результатов и степени выполнения требований установленным направлению и целям информационной безопасности.

3.1.29. **Стратегия информационной безопасности:** заданное направление и долгосрочный план перехода от текущего к целевому состоянию информационной безопасности.

3.1.30. **Стратегия развития Компании (Стратегия):** концепция развития Компании на долгосрочную перспективу в виде важнейших управленческих решений и программы конкретных действий для реализации данной концепции, и обеспечения достижения стратегических целей и задач.

3.1.31. **Структурное подразделение:** подразделение Компании, являющееся исполнителем отдельных процессов, функций, работ, участвующее в хозяйственной деятельности Компании, но не имеющее хозяйственной самостоятельности в рамках Компании.

3.1.32. **Тактическое управление (менеджмент) информационной безопасностью:** вид деятельности, заключающийся в планировании, выполнении, контроле и совершенствовании деятельности в области информационной безопасности, в соответствии с направлением, заданным на уровне Стратегического управления информационной безопасностью, для достижения целей информационной безопасности.

3.1.33. **Третьи лица:** любые физические лица, не являющиеся Работниками Компании, любые юридические лица, их объединения, должностные лица, органы государственной власти и местного самоуправления, иные лица, с которыми Компания вступает в какие-либо правоотношения.

3.1.34. **Функциональное направление ИБ:** вид деятельности в области ИБ, выделяемый по определенному признаку, назначению, уровню ответственности, применяемым технологиям, методам, ресурсам ИБ.

3.1.35. **Цикл Деминга**: циклически повторяющийся процесс принятия решения, используемый в управлении. Цикл включает в себя следующие этапы: планирование, выполнение, контроль, воздействие (управление, корректировка).

3.2. В настоящей Политике применены следующие сокращения:

PDCA	Plan-Do-Check-Act (Планирование - Выполнение - Контроль – Воздействие), цикл Деминга

Архитектурный комитет	Архитектурный подкомитет ИТ-комитета ПАО «ГМК «Норильский никель»
АСУТП	Автоматизированные системы управления технологическими процессами
Группа	Группа компаний «Норильский никель»
ДЗГТМПиСС	Департамент защиты государственной тайны, мобилизационной подготовки и специальной связи Главного офиса ПАО «ГМК «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»
ДКБ	Департамент (Дирекция) корпоративной безопасности Главного офиса ПАО «ГМК «Норильский никель»
ДКО	Департамент корпоративных отношений Главного офиса ПАО «ГМК «Норильский никель»
ДКП	Департамент кадровой политики Главного офиса ПАО «ГМК «Норильский никель»
ДПА	Департамент промышленных активов Главного офиса ПАО «ГМК «Норильский никель»
ЗОКС НН	Зарубежные организации корпоративной структуры, входящие в Группу компаний «Норильский никель»
ИБ	Информационная безопасность
ИТ	Информационные технологии
Кадровые службы	Кадровые службы или работники, ответственные за управление кадрами, в обособленных подразделениях, РОКС НН, ЗОКС НН
Компания	ПАО «ГМК «Норильский никель»
Корпоративная стратегия	Стратегия развития Компании
КСУР	Корпоративная система управления рисками
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»

ОЦО	ООО «Норникель – Общий центр обслуживания»
ПД	Правовой департамент Главного офиса ПАО «ГМК «Норильский никель»
Политика	Политика ПАО «ГМК «Норильский никель» в области информационной безопасности
Правовые службы	Подразделения или работники, ответственные за правовое обеспечение, в обособленных подразделениях, РОКС НН, ЗОКС НН
Процессы ИБ	Бизнес-процессы информационной безопасности
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».
Службы безопасности	Подразделения по безопасности и режиму или работники, ответственные за безопасность (в том числе заместители/советники руководителей/начальники отделов/главные специалисты), в обособленных подразделениях, РОКС НН, ЗОКС НН
Службы ИБ	Подразделения информационной безопасности или работники, ответственные за информационную безопасность, в обособленных подразделениях, РОКС НН, ЗОКС НН
Службы ИТ	Подразделения информационных технологий или работники, ответственные за информационные технологии, в обособленных подразделениях, РОКС НН, ЗОКС НН
СУИБ	Система управления (менеджмента) информационной безопасностью
СРМ	Служба риск-менеджмента Главного офиса ПАО «ГМК «Норильский никель»

4. Принципы деятельности в области информационной безопасности

4.1. Деятельность Компании в области ИБ осуществляется в соответствии со следующими принципами:

4.1.1. *Ориентация на бизнес:* защита информационных активов, информационных систем и компонентов ИТ–инфраструктуры, 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.

4.1.2. *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.

4.1.3. *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.

4.1.4. *Инновации:* использование новых технологий и подходов, обеспечивающих повышение результативности и эффективности принимаемых организационно–технических мер ИБ.

4.1.5. *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.

4.1.6. *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.

4.1.7. *Целостная структура:* эффективные коммуникации и обмен информацией между Главным офисом, обособленными подразделениями, РОКС НН, ЗОКС НН в области ИБ, следование единой Стратегии ИБ и настоящей Политике.

4.1.8. *Ответственность:* каждый работник Компании, РОКС НН, ЗОКС НН несет ответственность за ненадлежащее использование информационных активов и управление рисками ИБ в рамках своих компетенций.

4.1.9. *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.

4.1.10. *Постоянное совершенствование:* построение деятельности и бизнес-процессов в области ИБ в соответствии с подходом PDCA.

5. Объекты и субъекты Политики

5.1. Объектами настоящей Политики являются информационные активы, информационные системы/компоненты ИТ–инфраструктуры, АСУТП, объекты информатизации и автоматизации, используемые в бизнес–процессах Группы.

5.2. Управление объектами настоящей Политики осуществляется для обеспечения надлежащего уровня защищенности информационных активов, информационных систем/компонентов ИТ–инфраструктуры, АСУТП, объектов информатизации и автоматизации Группы на всех стадиях жизненного цикла

путем создания, внедрения и эффективного применения организационно–технических мер ИБ.

5.3. Субъектами Политики являются:

- Совет директоров;
- Правление Компании;
- Вице-президент–руководитель Блока корпоративной защиты;
- Владельцы бизнес–процессов;
- Директор ДЗИиИТИ;
- Руководители обособленных подразделений, РОКС НН, ЗОКС НН;
- Владельцы информационных активов;
- ДЗИиИТИ/Службы ИБ;
- ДКБ/Службы безопасности;
- ДЗГТМПиСС;
- ДКО;
- ДИТ/Сервисные линии ОЦО/Службы ИТ;
- ДПА;
- ДКП/Кадровые службы;
- СРМ;
- ПД/Правовые службы.

5.4. К функциям **Совета директоров** как субъекта управления в области ИБ относятся:

– определение приоритетных направлений деятельности Компании, концепции и стратегии развития Компании, а также способов их реализации, утверждение планов и бюджетов Компании (включая бюджеты в области ИБ), а также утверждение изменений планов и бюджетов Компании;

– определение принципов и подходов к организации системы управления рисками (включая риски ИБ) и внутреннего контроля в Компании, обеспечение надзора за функционированием системы управления рисками и внутреннего контроля.

5.5. К функциям **Правления Компании** как субъекта управления в области ИБ относятся:

– реализация мероприятий и процедур по управлению рисками (включая риски ИБ) и внутреннему контролю;

– анализ и оценка результатов финансово-хозяйственной деятельности, а также рассмотрение отчетов и иной информации о деятельности Компании (включая деятельность в области ИБ) его дочерних обществ, филиалов и представительства.

5.6. К функциям **Вице-президента–руководителя Блока корпоративной защиты** как субъекта управления в области ИБ относятся:

– определение ключевых стратегических направлений деятельности Группы в области ИБ, приоритизация инициатив и проектов в области ИБ, утверждение Программы и Стратегии ИБ;

– контроль соответствия Программы и Стратегии ИБ Корпоративной стратегии и приоритетным направлениям деятельности Компании;

– контроль за проведением оценки и анализа основных рисков ИБ Группы;

– контроль соответствия применяемых в Группе организационно–технических мер ИБ требованиям законодательства Российской Федерации и регуляторов, международным и российским стандартам в области ИБ;

– координация и контроль реализации программ сотрудничества в области ИБ с ведущими добывающими и перерабатывающими компаниями;

– контроль и координация проведения аудитов состояния ИБ в информационных системах/компонентах ИТ–инфраструктуры Компании, РОКС НН, ЗОКС НН, разработки и реализации мер, нацеленных на повышение уровня ИБ.

5.7. К функциям **Владельцев бизнес-процессов** как субъектов управления в области ИБ относятся:

– назначение владельцев информационных активов;

– рассмотрение и согласование оценок ценности и последствий от нарушения конфиденциальности, целостности и доступности информационных активов, предоставленных владельцами информационных активов;

– контроль предоставления владельцами информационных активов информации об используемых и планируемых информационных активах в ДЗИиИТИ/Службы ИБ;

– организация соблюдения требований настоящей Политики и НМД в области ИБ, разработанных в развитие настоящей Политики, участниками бизнес–процессов, включая работников третьих лиц, привлекаемых на договорной основе;

– организация прохождения участниками бизнес–процессов обучения и проверок знаний в области ИБ.

5.8. К функциям **Директора ДЗИиИТИ** как субъекта управления в области ИБ относятся:

– организация разработки и актуализации Программы и Стратегии ИБ, целевой Архитектуры ИБ, настоящей Политики;

– организация внедрения и функционирования СУИБ;

– организация методической поддержки в области ИБ Руководителям Компани, Вице-президенту-руководителю Блока корпоративной защиты, Владельцам бизнес-процессов, Руководителям и работникам обособленных подразделений, РОКС НН, ЗОКС НН, Владельцам информационных активов;

– обеспечение соответствия применяемых организационно–технических мер ИБ требованиям законодательства Российской Федерации и регуляторов, международным и российским стандартам в области ИБ;

– управление рисками ИБ, в том числе утверждение отчетов об оценке рисков ИБ, планов мероприятий по управлению рисками ИБ, контроль реализации мероприятий по управлению рисками ИБ;

– определение и развитие необходимых компетенций ИБ, формирование организационной структуры ДЗИиИТИ;

– организация и контроль бюджетного процесса, исполнения инвестиционных проектов в области ИБ;

– обеспечение ресурсами, организация и контроль деятельности по функциональным направлениям ИБ, в том числе:

– назначение работников ДЗИиИТИ, ответственных за функциональные направления ИБ;

– рассмотрение и утверждение планов мероприятий и отчетов ИБ;

– рассмотрение и утверждение системы метрик ИБ;

– контроль совершенствования и повышения уровня зрелости процессов ИБ.

5.9. К функциям **Руководителей обособленных подразделений, РОКС НН, ЗОКС НН** как субъектов управления в области ИБ относятся:

– организация соблюдения и исполнения принципов и требований настоящей Политики и НМД в области ИБ, разработанных в развитие настоящей Политики, в обособленных подразделениях, РОКС НН, ЗОКС НН;

– обеспечение ресурсами, организация 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;

– определение работника, ответственного за осуществление деятельности в области ИБ в обособленных подразделениях, РОКС НН, ЗОКС НН;

– управление рисками ИБ, в том числе утверждение отчетов об оценке рисков ИБ и планов мероприятий по управлению рисками ИБ, контроль реализации мероприятий по управлению рисками ИБ в обособленных подразделениях, РОКС НН, ЗОКС НН;

– организация прохождения работниками обособленных подразделений, РОКС НН, ЗОКС НН обучения и проверок знаний в области ИБ.

5.10. К функциям **Владельцев информационных активов** как субъектов управления в области ИБ относятся:

– предоставление в ДЗИиИТИ/Службы ИБ информации об используемых и планируемых информационных активах, информационных системах/компонентах ИТ–инфраструктуры;

– оценка ценности и последствий от нарушения конфиденциальности, целостности и доступности информационных активов;

– согласование результатов оценки рисков ИБ и планов мероприятий по управлению рисками ИБ;

– участие в процессах ИБ по управлению доступом (рассмотрение и согласование запросов на доступ) к информационным активам.

5.11. К функциям **ДЗИиИТИ/Служб ИБ** как субъекта управления в области ИБ относятся:

– разработка целевой Архитектуры ИБ Группы, стандартизация и унификация применяемых подходов и технических средств защиты информации в Группе;

– контроль выполнения требований ИБ в рамках деятельности Архитектурного комитета, на всех стадиях жизненного цикла информационных активов, информационных систем/компонентов ИТ–инфраструктуры, АСУТП;

– осуществление операционной деятельности ИБ, оценка и мониторинг уровня рисков ИБ;

– управление и выполнение проектов в области ИБ;

– повышение уровня осведомленности работников Компании, РОКС НН, ЗОКС НН для снижения рисков ИБ, связанных с человеческим фактором;

– разработка и совершенствование НМД в области ИБ по функциональным направлениям ИБ;

– осуществление методической поддержки по функциональным направлениям ИБ работникам обособленных подразделений, РОКС НН, ЗОКС НН;

– разработка метрик по функциональным направлениям ИБ.

5.12. К функциям **ДКБ/Служб безопасности** как субъекта управления в области ИБ относятся:

– организация физической безопасности оборудования средств защиты информации, информационных систем/компонентов ИТ–инфраструктуры, обрабатывающих информационные активы;

– участие в расследованиях инцидентов ИБ;

– организация проведения служебных расследований по сообщениям о нарушениях ИБ;

– взаимодействие с правоохранительными органами по вопросам, связанным с нарушением ИБ.

5.13. К функциям **ДЗГТМПиСС** как субъекта управления в области ИБ относятся:

– формирование требований по организации защиты информации, составляющей коммерческую тайну, и контроль выполнения этих требований;

– методическая поддержка ДЗИиИТИ в части формирования требований по технической защите информации, составляющей коммерческую тайну;

– участие в процессах ИБ по управлению доступом к информации, составляющей коммерческую тайну;

– участие в расследованиях инцидентов ИБ в части информации, составляющей коммерческую тайну.

5.14. К функциям **ДКО** как субъекта управления в области ИБ относится:

– формирование требований по организации защиты инсайдерской информации и контроль выполнения этих требований;

– методическая поддержка ДЗИиИТИ в части формирования требований по технической защите инсайдерской информации;

– участие в процессах ИБ по управлению доступом к инсайдерской информации (формирование и ведение списка инсайдеров);

– участие в расследованиях инцидентов ИБ в части инсайдерской информации.

5.15. К функциям **ДИТ/Сервисных линии ОЦО/Служб ИТ** как субъекта управления в области ИБ относятся:

5.15.1. 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;

– при эксплуатации и сопровождении информационных систем/компонентов ИТ–инфраструктуры;

– при организации деятельности в рамках направлений ДИТ/сервисных линий ОЦО/Служб ИТ.

5.15.2. Формирование бюджетов мероприятий по управлению рисками ИБ, возникающими при автоматизации деятельности Блоков и бизнес–процессов Группы.

5.15.3. Контроль выполнения требований ИБ третьими лицами, привлекаемыми при эксплуатации, сопровождении информационных систем/компонентов ИТ–инфраструктуры, на стадиях ИТ-программ, ИТ-проектов, проектов с ИТ–составляющей.

5.15.4. Обеспечение доступности информационных активов, непрерывности работы информационных систем/компонентов ИТ–инфраструктуры, восстановление после сбоев и чрезвычайных ситуаций.

5.15.5. Предоставление в ДЗИиИТИ/Службы ИБ следующей информации:

– характеристики, конфигурации, взаимосвязи информационных систем/компонентов ИТ–инфраструктуры;
– администраторы, ответственные за эксплуатацию и сопровождение информационных систем/компонентов ИТ–инфраструктуры (включая представителей третьих лиц);
– ИТ-инициативы, ИТ-проекты, ИТ-программы, проекты с ИТ–составляющей, другие мероприятия, связанные с развитием/изменением ИТ–архитектуры;
– привлекаемые третьи лица (договор, участники, роли, сроки работ).

5.16. К функциям **ДПА** как субъекта управления в области ИБ относятся:

5.16.1. Оценка последствий для технологических и производственных процессов от нарушений ИБ АСУТП (нарушения целостности и доступности информации, обрабатываемой АСУТП);

5.16.2. Согласование планов мероприятий по управлению рисками ИБ АСУТП, разработанных ДЗИиИТИ, и формирование бюджетов на данные мероприятия;

5.16.3. Выполнение требований 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.

5.16.4. Контроль выполнения 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.

5.17. К функциям **ДКП/Кадровых служб** как субъекта управления в области ИБ относятся:

– ознакомление работников Компании, РОКС НН, ЗОКС НН при трудоустройстве с НМД в области ИБ;

– предоставление в ДЗИиИТИ/Службы ИБ актуальной информации о статусе работников Компании, РОКС НН, ЗОКС НН (прием на работу, увольнение, перевод с должности на должность/перевод в другое структурное подразделение).

5.18. К функциям **СРМ** как субъекта управления в области ИБ относятся:

– разработка общекорпоративных правил идентификации, анализа и управления рисками в Компании (в том числе рисков ИБ);

– формирование предложений по приемлемому уровню риска;

– методическая поддержка в области интеграции процессов управления рисками ИБ в КСУР.

5.19. К функциям **ПД/Правовых служб** как субъекта управления в области ИБ относятся:

– экспертиза НМД в области ИБ и договоров Компании с третьими лицами на предмет их соответствия законодательным требованиям в области ИБ;

– мониторинг изменений законодательства Российской Федерации в области ИБ;

– подготовка заключений по правовым вопросам в области ИБ, в рамках компетенции ПД/Правовой службы.

6. Правила, требования и ограничения деятельности

6.1. Информационные активы, информационные системы/компоненты ИТ–инфраструктуры применяются исключительно для выполнения бизнес–процессов и достижения целей деятельности Группы. Запрещается нецелевое использование информационных активов, информационных систем/компонентов ИТ–инфраструктуры.

6.2. Все действия с информационными активами (получение, сбор, ввод, обработка, хранение, вывод, уничтожение и др.) выполняются с соблюдением требований ИБ.

6.3. Контроль выполнения требований ИБ осуществляется на всех стадиях жизненного цикла информационных активов, информационных систем/компонентов ИТ–инфраструктуры, АСУТП. Запрещается ввод в эксплуатацию и эксплуатация информационных систем/компонентов ИТ–инфраструктуры, АСУТП без выполнения требований ИБ, либо без согласования перечня компенсирующих мер ИБ с ДЗИиИТИ/Службами ИБ.

6.4. Для управления рисками ИБ применяются предупредительные, обнаруживающие, корректирующие и компенсирующие организационно–технические меры ИБ.

6.5. Планирование, выбор и обоснование применимости организационно–технических мер ИБ осуществляется на основании результатов идентификации/классификации информационных активов, информационных систем/компонентов ИТ–инфраструктуры, АСУТП, оценки рисков ИБ, требований законодательства и регуляторов.

6.6. 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 Вице-президентом-руководителем Блока корпоративной защиты.

6.7. 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).

6.8. 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 (как минимум, но не ограничивает) по следующим функциональным направлениям ИБ:

6.8.1. «Классификация информационных активов и оценка рисков ИБ».
6.8.2. «Управление требованиями ИБ на стадиях жизненного цикла».
6.8.3. «Обеспечение соответствия требованиям законодательства и регуляторов в области ИБ».
6.8.4. «Управление архитектурой ИБ».
6.8.5. «Защита активов техническими средствами ИБ».
6.8.6. «Повышение осведомленности в области ИБ».
6.8.7. «Управление доступом».
6.8.8. «Управление инцидентами ИБ».
6.8.9. «Обеспечение ИБ АСУТП».
6.8.10. «Оценка и отчетность ИБ».

6.9. Требования и процессы ИБ по каждому функциональному направлению ИБ регламентируются НМД в области ИБ, разработанными в развитие настоящей Политики.

6.10. В случае отсутствия Служб ИБ и необходимых ресурсов ИБ в обособленных подразделениях и РОКС НН реализация требований ИБ осуществляется структурными подразделениями ОЦО, Службами ИТ или Службами безопасности.

6.11. 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.

6.12. Выбор технических средств защиты Группы осуществляется в соответствии с требованиями документа Стандарт организации «Обеспечение техническими средствами защиты ИТ-инфраструктуры ПАО «ГМК «Норильский никель».

7. Ответственность

7.1. Ответственность за ненадлежащую организацию и неосуществление контроля исполнения требований настоящей Политики несет Вице-президент – руководитель Блока корпоративной защиты.

7.2. Ответственность за ненадлежащую организацию исполнения требований настоящей Политики по функциональным направлениям ИБ несет Директор ДЗИиИТИ.

7.3. Ответственность за ненадлежащую организацию деятельности в области ИБ и выполнение требований настоящей Политики в обособленных подразделениях, РОКС НН, ЗОКС НН несут руководители обособленных подразделений, РОКС НН, ЗОКС НН.

7.4. Работники Компании, РОКС НН, ЗОКС НН несут ответственность за ненадлежащее соблюдение требований настоящей Политики.

7.5. Ответственность за несвоевременное внесение изменений и дополнений в настоящую Политику несет Вице-президент – руководитель Блока корпоративной защиты.