Приложение
к приказу Генерального директора
АО «Кольская ГМК»
от 17.09.2020 № КГМК-_632-п_

УТВЕРЖДЕНЫ
распоряжением
Первого вице-президента
руководителя Блока
корпоративной защиты
ПАО «ГМК «Норильский никель»
от 13.08.2020 № ГМК-09/023-р

Методические указания

по допустимому использованию информационных активов в ПАО «ГМК «Норильский никель»

Обозначение документа: МУ ГК НН 167-004-2020
Введены впервые.
Дата введения:13.08.2020

Содержание

1. Область применения

1.1. Настоящие Методические указания по допустимому использованию информационных активов в ПАО «ГМК «Норильский никель» (далее – Методические указания) устанавливают правила допустимого использования информационных активов (далее – ИА) и требования информационной безопасности при работе с ИА, информационными системами (далее – ИС) и компонентами ИТ-инфраструктуры, обрабатывающими ИА ПАО «ГМК «Норильский никель» (далее – Компания) и российских организаций корпоративной структуры, входящих в Группу компаний «Норильский никель» (далее – РОКС НН).

1.2. Требования настоящих Методических указаний распространяются на работников Компании и РОКС НН, использующих ИА, ИС и компоненты ИТ-инфраструктуры, обрабатывающие ИА Компании/РОКС НН.

1.3. Методические указания не применяются при использовании работниками Компании/РОКС НН ИА, содержащих:

1.3.1. Инсайдерскую информацию, информацию, составляющую коммерческую тайну, персональные данные, общедоступную информацию. Требования к обработке указанных категорий ИА устанавливаются нормативно-методическими документами Компании/РОКС НН, нормативно-правовыми актами Российской Федерации.

1.3.2. Сведения, составляющие государственную тайну.

2. Нормативные ссылки

При разработке настоящих Методических указаний были использованы следующие регламентирующие документы Компании и иные нормативные акты:

от 30.11.1994 № 51-ФЗ	Гражданский кодекс Российской Федерации (часть первая)
от 30.12.2001 № 197-ФЗ	Трудовой кодекс Российской Федерации
от 26.07.2006 № 149-ФЗ	Федеральный закон «Об информации, информационных технологиях и о защите информации»
УП ГК НН 167-004-2018	Политика ПАО «ГМК «Норильский никель» в области информационной безопасности
Протокол Совета директоров ПАО «ГМК «Норильский никель» от 22.06.2020 № ГМК/17-пр-сд	Положение о порядке доступа к инсайдерской информации ПАО «ГМК «Норильский никель», правилах охраны ее конфиденциальности и контроля за соблюдением требований законодательства в сфере противодействия неправомерному использованию инсайдерской информации и манипулированию рынком
Протокол Совета директоров от 29.12.2012 № ГМК/62-пр-сд	Кодекс деловой этики ОАО «ГМК «Норильский никель»
СТО ГМК-НН 108-005-2016	Стандарт организации «Оснащение рабочих мест пользователей информационных систем ПАО «ГМК

	«Норильский никель» и российских организаций корпоративной структуры, входящих в Группу компаний «Норильский никель»
П ГМК-НН 167-003-2017	Положение «Управление доступом к информационным активам ПАО «ГМК «Норильский никель»
П ГО 165-001-2019	Положение о пропускном и внутриобъектовом режимах в помещениях Главного офиса ПАО «ГМК «Норильский никель», расположенных по адресам: г. Москва, 1-й Красногвардейский проезд, д. 15, ул. Тестовская, д. 8, ул. Тестовская, д. 10
Р ГК НН 167-007-2019	Регламент идентификации и классификации информационных активов ПАО «ГМК «Норильский никель»
Р ГК НН 167-003-2019	Регламент управления инцидентами информационной безопасности в ПАО «ГМК «Норильский никель»
Р ГК НН 23-002-2018	Регламент взаимодействия должностных лиц ПАО «ГМК «Норильский никель» с российскими и зарубежными средствами массовой информации

3. Термины, определения и сокращения

3.1. В настоящих Методических указаниях применены термины с соответствующими определениями:

3.1.1. **Административная учетная запись:** регистрационная запись субъекта доступа информационной системы, бизнес-приложения, инфраструктурного приложения или компонента ИТ-инфраструктуры, автоматизированной системы управления технологическим процессом с расширенными (административными) правами, позволяющая его идентифицировать и однозначно определяющая его права на доступ к информационной системе, бизнес-приложению, инфраструктурному приложению или компоненту ИТ-инфраструктуры, автоматизированной системе управления технологическим процессом.

3.1.2. **Бизнес-приложение**: специальное программное обеспечение, предназначенное для автоматизации бизнес-процессов и прикладных задач структурных подразделений.

3.1.3. **Доступ к информации**: возможность получения информации и ее использования.

3.1.4. **Инсайдерская информация**: точная и конкретная информация, которая не была распространена и распространение которой может оказать существенное влияние на цены финансовых инструментов Компании.

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

3.1.6. **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.

3.1.7. **Информация, составляющая коммерческую тайну (секрет производства)**: сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны.

3.1.8. **Инфраструктурное приложение:** специальное программное обеспечение, обеспечивающее коллективную работу пользователей и информационных систем.

3.1.9. **Инцидент информационной безопасности**: событие или комбинация событий, указывающая на свершившуюся, предпринимаемую или вероятную реализацию угрозы ИБ.

3.1.10. **Компоненты ИТ-инфраструктуры**: общесистемное программное обеспечение, аппаратные, телекоммуникационные средства, обеспечивающие функционирование бизнес-приложений и инфраструктурных-приложений.

3.1.11. **Конфиденциальная информация**: сведения (сообщения, данные) независимо от формы их представления, в отношении которых законодательством Российской Федерации, внутренними документами Компании или соглашениями между Компанией, ее контрагентами и иными лицами установлен режим конфиденциальности.

3.1.12. **Корпоративная сеть передачи данных**: информационно-телекоммуникационная вычислительная сеть (за исключением компонентов АСУ ТП), объединяющая в единое информационное пространство все структурные подразделения Компании и российских организаций корпоративной структуры, входящих в Группу компаний «Норильский никель.

3.1.13. **Логин**: идентификатор (имя) учетной записи пользователя, используемый, как правило, в паре с паролем для доступа к АРМ, ИС, инфраструктурному приложению или компоненту ИТ-инфраструктуры.

3.1.14. **Мобильное устройство**: портативное электронное устройство компактных размеров, используемое для приема, записи, хранения и переноса информации и оснащенное модулем беспроводной связи.

3.1.15. **Несанкционированный доступ к информационным активам**: доступ к информационным активам, бизнес-приложению, инфраструктурному приложению или компонентам ИТ-инфраструктуры, осуществляемый с нарушением установленных прав и (или) правил доступа.

3.1.16. **Обработка информации**: любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств

автоматизации или без использования таких средств с информацией, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение информации.

3.1.17. **Общедоступная информация**: общеизвестные сведения и иная информация, доступ к которой не ограничен.

3.1.18. **Пароль**: набор символов, предназначенный для подтверждения подлинности субъекта доступа.

3.1.19. **Персональные данные**: любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

3.1.20. **Пользователь информационной системы:** работник ПАО «ГМК «Норильский никель» либо российской организации корпоративной структуры, входящей в Группу компаний «Норильский никель», в силу своих функциональных обязанностей применяющий информационную систему в своей работе и получающий или вносящий информацию в информационную систему.

3.1.21. **Средство защиты информации**: техническое, программное, программно-техническое средство, предназначенные или используемые для защиты информации.

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

3.1.23. **Съемный носитель информации**: материальный носитель информации, предназначенный для ее автономного хранения и независимого от места ее записи или использования.

3.1.24. **Технические средства**: изделия, оборудование, аппаратура или их составные части, функционирование которых основано на законах электротехники, радиотехники и (или) электроники, содержащие электронные компоненты и (или) схемы.

3.1.25. **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.

3.1.26. **Учетная запись**: регистрационная запись субъекта доступа информационной системы, бизнес-приложения, инфраструктурного приложения или компонента ИТ-инфраструктуры, автоматизированной системы управления технологическим процессом, позволяющая его идентифицировать и однозначно определяющая его права на доступ к информационным активам, обрабатываемым с помощью данной информационной системы, инфраструктурного приложения или компонента ИТ-инфраструктуры.

3.1.27. **Штатные средства:** функциональные возможности программных и/или аппаратных средств, входящих в состав информационной системы и/или компонента ИТ–инфраструктуры и описанных в эксплуатационной документации.

3.2. В настоящих Методических указаниях применены следующие сокращения:

АРМ	Автоматизированное рабочее место
ДЗИиИТИ	Департамент защиты информации и IT инфраструктуры Главного офиса ПАО «ГМК «Норильский никель»
ДИТ	Департамент информационных технологий Главного офиса ПАО «ГМК «Норильский никель»
ИА	Информационный актив
ИБ	Информационная безопасность
ИС	Информационная система
Компания	ПАО «ГМК «Норильский никель»
КСПД	Корпоративная сеть передачи данных
КСЭП	Корпоративная система электронной почты
НМД	Нормативно-методический документ
Обособленные подразделения	Филиалы, представительство ПАО «ГМК «Норильский никель»
ОС	Операционная система
Персональные настройки АРМ	Набор изменяемых параметров ПО, позволяющих пользователю через специальный графический интерфейс штатно изменять настройки для удобства работы (разрешение, яркость и контрастность экрана, размер и тип шрифтов, уровень звука, заставка экрана и т.п.)
ПО	Программное обеспечение
Пропускной режим	Порядок, устанавливаемый в Компании/РОКС НН, не противоречащий законодательству Российской Федерации, доведенный до сведения работников и посетителей объектов охраны и обеспечиваемый совокупностью мероприятий и правил, исключающих возможность бесконтрольного входа (выхода) лиц, въезда (выезда) транспортных средств, вноса (выноса), ввоза (вывоза) имущества на объекты охраны (с объектов охраны)
Работник	Работник Компании/РОКС НН

РОКС НН	Российские организации корпоративной структуры, входящие в Группу компаний «Норильский никель»
СЗИ	Средство защиты информации
Системные настройки АРМ	Изменяемые параметры системного и прикладного ПО и оборудования, позволяющие менять режим их функционирования (в том числе параметры, относящиеся к обеспечению ИБ)
СКУД	Система контроля и управления доступом
СМИ	Средство массовой информации
Служба ИБ	Структурное подразделение ИБ или работники, ответственные за информационную безопасность в Обособленных подразделениях, РОКС НН
Стационарное оборудование	Оборудование, не относящееся к перемещаемому
VPN	Virtual Private Network, виртуальная частная сеть

4. Требования по допустимому использованию информационных активов

4.1. Общие сведения

4.1.1. Работники обеспечивают соблюдение требований и правил, установленных Политикой ПАО «ГМК «Норильский никель» в области информационной безопасности, а также настоящими Методическими указаниями.

4.1.2. Требования ИБ к ИА определяются в зависимости от класса критичности по свойствам безопасности ИА, установленного с учетом ценности ИА, в соответствии с Регламентом идентификации и классификации информационных активов ПАО «ГМК «Норильский никель», а также требований законодательства Российской Федерации.

4.1.3. Работникам предоставляется доступ к ИА, ИС и компонентам ИТ-инфраструктуры, обрабатывающим ИА Компании/РОКС НН, для осуществления ими своих трудовых обязанностей.

4.1.4. ИА, обрабатываемые в Компании/РОКС НН, являются собственностью Компании/РОКС НН, если иное не оговорено соответствующими соглашениями и/или нормативными и законодательными актами Российской Федерации.

4.1.5. В Компании/РОКС НН осуществляется контроль действий работников при использовании ИА, ИС и компонентов ИТ-инфраструктуры, обрабатывающих ИА Компании/РОКС НН, в объеме, необходимом и достаточном для выявления нарушений требований ИБ и/или при расследовании инцидентов ИБ.

4.2. Общие требования по ИБ

4.2.1. Доступ к ИА предоставляется работникам в рамках выполнения ими трудовых обязанностей. Предоставление доступа к ИА, обрабатываемым в ИС и

компонентах ИТ-инфраструктуры, осуществляется в соответствии с Положением «Управление доступом к информационным активам ПАО «ГМК «Норильский никель» Компании и соответствующими НМД РОКС НН, регламентирующими порядок управления доступом к ИА.

4.2.2. Создаваемые или передаваемые работниками ИА (в том числе, включаемые в сообщения КСЭП или передаваемые с помощью других средств коммуникации) являются:

– точными (не ложными, соответствующими действительности, не противоречащими официальным фактам);

– уместными (относящимися непосредственно к трудовым обязанностям и к обсуждаемому вопросу/теме, не содержащими сведений личного характера);

– этичными (соответствующими Кодексу деловой этики ОАО «ГМК «Норильский никель» и НМД РОКС НН в сфере регулирования деловой этики и правилам этики);

– полученными законным способом.

4.2.3. ИА передаются работникам только в случаях, обусловленных:

– трудовыми обязанностями работников;

– требованиями законодательства Российской Федерации;

– по согласованию руководителя структурного подразделения (для ИА на бумажных носителях).

4.2.4. Работники осуществляют обработку ИА в электронном виде только в ИС и компонентах ИТ-инфраструктуры Компании/РОКС НН, в т.ч.:

– КСЭП;

– бизнес-приложениях;

– инфраструктурных приложениях;

– файловых ресурсах (общих и личных корпоративных сетевых дисках);

– мобильных устройствах (планшетных компьютерах и мобильных телефонах) и ноутбуках[1], корпоративных съемных носителях информации.

4.2.5. Работники при выполнении своих трудовых обязанностей обеспечивают вывод на печать ИА в минимально необходимом объеме и количестве экземпляров.

4.2.6. Работники забирают выведенные на печать документы с печатающих устройств (принтеров и многофункциональных устройств) сразу после их печати.

4.2.7. Работники обеспечивают своевременное удаление (уничтожение) ИА, в том числе:

[1] Использование личных мобильных устройств и ноутбуков допускается при выполнении требований п.4.4.1, 4.4.2, 4.4.4 настоящих Методических указаний.

– неактуальных ИА в бумажной и электронной форме, если они более не требуются для дальнейшей работы и не подлежат дальнейшему хранению в соответствии со сроками, установленными законодательством Российской Федерации и НМД Компании/РОКС НН;

– избыточных копий ИА (не требующихся для выполнения трудовых обязанностей черновиков, дубликатов, записей, распечаток, копий) в электронной и бумажной формах.

4.2.8. Удаление ИА в электронной форме осуществляется путем использования штатных средств ОС, ИС Компании/РОКС НН.

4.2.9. Уничтожение бумажных носителей ИА осуществляется способом, препятствующим их восстановлению (например, с использованием шредеров).

4.3. Автоматизированное рабочее место работника

4.3.1. Покидая свое рабочее место, работники обеспечивают блокирование сеанса пользователя АРМ (например, используя сочетания клавиш «Win» + «L» для ОС семейства MS Windows).

4.3.2. Работникам запрещается самостоятельно открывать корпус АРМ и изменять его конфигурацию.

4.3.3. Работникам запрещается самостоятельное подключение к АРМ какого-либо оборудования, за исключением входящих в комплект рабочей станции устройств ввода-вывода (при наличии): монитор, мышь, клавиатура, микрофон, наушники, камера. Запрещается подключать к АРМ личные устройства (например, смартфоны, USB-модемы, мыши, клавиатуры и др.).

4.3.4. Работникам запрещается подключать оборудование к КСПД (в том числе посредством удаленного доступа) без согласования с ДЗИиИТИ/Службой ИБ.

4.3.5. Работникам запрещается обрабатывать на АРМ и в ИС Компании/РОКС НН информацию, не связанную с выполнением трудовых обязанностей.

4.3.6. Работникам запрещается вносить изменения в системные настройки корпоративных АРМ, за исключением случаев, когда это входит в их трудовые обязанности. Внесение изменений в персональные настройки корпоративных АРМ допускается.

4.3.7. Работникам запрещается осуществлять действия, направленные на:

– обход/взлом систем защиты АРМ, ИС и КСПД Компании/РОКС НН, анонимизацию действий;

– получение несанкционированного доступа к ИА Компании/РОКС НН посредством перехвата трафика, сканирования портов, неавторизованного доступа к серверам и данным, использования ошибок и недокументированных возможностей ПО;

– несанкционированное повышение привилегий в ОС или ИС;

– нарушение или прерывание работы компонентов ИТ-инфраструктуры, уничтожение, нарушение целостности ИА и оборудования;

– кражу, несанкционированный вынос оборудования.

4.3.8. Перемещение любого стационарного оборудования (например, стационарный компьютер, принтер, серверное оборудование) может осуществляться только по согласованию с работниками подразделения Компании/РОКС НН, в чьи обязанности входит установка и настройка технических средств. Ремонт технических средств и вскрытие корпусов оборудования (системных блоков, ноутбуков) выполняется исключительно работниками подразделения Компании/РОКС НН, в чьи обязанности входит выполнение ремонта технических средств.

4.4. Использование мобильных устройств и ноутбуков

4.4.1. Использование личных мобильных устройств (например, планшетных компьютеров и мобильных телефонов) и ноутбуков для работы с ИА, ИС и компонентами ИТ-инфраструктуры, обрабатывающими ИА, в целях выполнения трудовых обязанностей в офисных помещениях Компании/РОКС НН) осуществляется работниками только по согласованию с ДЗИиИТИ/Службой ИБ.

4.4.2. При использовании для подключения к КСПД Компании/РОКС НН мобильных устройств и ноутбуков, должны выполняться следующие требования ИБ:

– на мобильные устройства устанавливаются средства контроля мобильных устройств (MDM);

– доступ к ИА осуществляется с мобильных устройств и ноутбуков при использовании зарегистрированной учетной записи работника.

4.4.3. Для личных мобильных устройств и ноутбуков, используемых для подключения к КСПД Компании/РОКС НН, исключается возможность копирования/сохранения на них, а также на съемных носителях информации (оптических дисках, картах памяти, USB-флеш-накопителях, внешних дисках) ИА Компании/РОКС НН.

4.4.4. Работник при поддержке Единой службы поддержки сервисов обеспечивает наличие на личных мобильных устройствах и ноутбуках:

– средства защиты от вредоносного кода с актуальными сигнатурами;

– установленных актуальных версий ОС и прикладного ПО, патчей и обновлений безопасности, рекомендованных производителем (вендором).

4.4.5. Работники обеспечивают принятие следующих мер для предотвращения повреждения, утери/кражи личных и предоставленных им технических средств (ноутбуков, мобильных устройств):

– технические средства не оставляются без личного присмотра при их использовании в общедоступных помещениях Компании/РОКС НН (зоны ресепшн, переговорные комнаты, столовые комнаты), в публичных местах за пределами Компании/РОКС НН или в неохраняемых помещениях при удаленной работе (на встречах, в командировках и т.п.);

– во внерабочее время технические средства, используемые для работы с ИА, ИС и компонентами ИТ-инфраструктуры, обрабатывающими ИА, не оставляются без личного присмотра, при необходимости и наличии технической

возможности осуществляется их хранение в запираемых шкафах (тумбочках), сейфах, или используются механические замки (например, kensington lock).

4.4.6. Работникам запрещается фиксировать ИА Компании/РОКС НН, содержащиеся в ИС, компонентах ИТ-инфраструктуры Компании/РОКС НН и на бумажных носителях информации, встроенными в личные мобильные устройства фото-, видео-камеры, за исключением случаев использования для этих целей приложений, запускаемых из защищенной области, создаваемой клиентской частью средств контроля мобильных устройств (MDM).

4.5. Использование носителей информации

4.5.1. Работникам запрещается оставлять без личного присмотра в общедоступных местах Компании/РОКС НН, в публичных местах за пределами Компании/РОКС НН или в неохраняемых помещениях при удаленной работе:

– бумажные носители информации;

– съемные носители информации: оптические диски, карты памяти, USB-флеш-накопители, внешние диски.

4.5.2. В нерабочее время работники обеспечивают хранение всех носителей информации в запираемых шкафах (тумбочках).

4.5.3. Доступ (на чтение и запись) к съемным носителям информации (например, оптических дисков, карт памяти, USB-флеш-накопителей, внешних дисков) предоставляется только в рамках трудовых обязанностей при согласовании с ДЗИиИТИ/Службой ИБ.

4.5.4. Работникам запрещается использовать личные съемные носители информации (например, оптические диски, карты памяти, USB-флеш-накопители, внешние диски) для записи и хранения ИА Компании/РОКС НН.

4.6. Учетные записи и пароли

4.6.1. Для обработки ИА в электронном виде работнику создается учетная запись, с помощью которой предоставляется доступ к АРМ, ИС, компонентам ИТ-инфраструктуры.

4.6.2. Работникам запрещается использовать учетные записи других работников или третьих лиц.

4.6.3. Работникам запрещается сообщать или передавать другим работникам или третьим лицам персональные пароли и иные средства аутентификации[2].

4.6.4. Работникам, обладающим административными учетными записями, запрещается работа под административной учетной записью в случаях (например, работа с документами, КСЭП, ресурсами сети Интернет), когда для

[2] Использование коллективных (групповых/общих) учетных записей запрещается, за исключением случаев, когда их использование согласовано ДЗИиИТИ/Службой ИБ. Технические учетные записи применяются только для обеспечения работы программных интерфейсов и системных служб. Интерактивный вход в систему для технических учетных записей отключен.

выполнения такой работы использование административной учетной записи не требуется (достаточно пользовательской учетной записи).

4.6.5. В случае разглашения (либо подозрения на компрометацию) учетных данных (логина и пароля) работник незамедлительно осуществляет смену своего пароля и сообщает об этом в ДЗИиИТИ/Службу ИБ, в соответствии с п. 4.16 настоящих Методических указаний.

4.6.6. Работникам запрещается включать в пароли учетных записей очевидные слова и комбинации, повторяющиеся символы, сочетания символов (более трех), последовательно расположенных на клавиатуре, контекст (имя, фамилия пользователя, дата рождения, названия приложений и т.д.), использовать пароли, входящие в общедоступные словари часто используемых паролей. Примеры запрещенных к использованию паролей: дата рождения, имя, набор цифр, последовательность близко расположенных на клавиатуре букв и т.п.

4.6.7. Работники обеспечивают безопасное хранение и использование своих паролей и (или) средств аутентификации, исключающее их утерю или компрометацию. Для этого соблюдаются следующие правила:

– ввод пароля осуществляется непосредственно самим работником;

– при вводе пароля работник убеждается, что исключена возможность компрометации пароля (например, вводимый пароль не виден/не слышен другим работникам либо третьим лицам);

– работник при первом входе в ИС или на АРМ и регулярно (с установленной периодичностью) производит смену пароля от своей персональной учетной записи;

– работникам запрещается размещать записанные в каком-либо виде пароли в местах, где они могут быть легко получены (скомпрометированы) другими работниками или третьими лицами (например, на рабочем столе, мониторе, клавиатуре, в блокноте, черновиках и документах).

4.7. Использование сети Интернет

4.7.1. Работники обеспечивают использование предоставляемого Компанией/РОКС НН доступа к ресурсам сети Интернет только для выполнения своих трудовых обязанностей.

4.7.2. При доступе к ресурсам сети Интернет работники обеспечивают использование защищенных Интернет-соединений (адрес сайта начинается с https://, но не с http://).

4.7.3. При использовании сети Интернет, доступ к которой предоставлен Компанией / РОКС НН, либо в случае использования корпоративных мобильных устройств и ноутбуков для доступа в сеть Интернет, работникам запрещается:

– использовать для хранения и обработки ИА Компании/РОКС НН «облачные» сервисы (сервисы хранения и обработки информации, такие как Google Диск, Dropbox, Яндекс.Диск и т.п.);

– использовать для обработки ИА Компании/РОКС НН веб-сайты, не принадлежащие Компании/РОКС НН, и социальные сети, если это не входит в их

трудовые обязанности, или не предусмотрено договорами Компании/РОКС НН с третьими лицами;

– посещать ресурсы сети Интернет, содержащие материалы противозаконного, экстремистского, дискриминационного, неэтического, расистского или религиозного характера, а также получать (скачивать), хранить и распространять в КСПД или сети Интернет данные материалы;

– использовать доступ в сеть Интернет в личных и развлекательных целях;

– использовать браузеры, отличные от разрешенных к использованию в Компании/РОКС НН, в том числе браузеры с функциональностью сокрытия IP-адреса или поддерживающие функции VPN;

– использовать средства шифрования сетевого трафика и подключения к внешним сетям (VPN), отличные от разрешенных к использованию в Компании/РОКС НН;

– использовать прокси-серверы, не согласованные с ДЗИиИТИ/Службой ИБ;

– использовать средства для удаленного доступа и (или) общего доступа к рабочему столу, отличные от разрешенных к использованию в Компании/РОКС НН;

– подключаться к файлообменным ресурсам и сетям, не принадлежащим Компании/РОКС НН, и использовать их.

4.8. Использование беспроводных сетей (Wi-Fi)

4.8.1. Беспроводной доступ предоставляется только тем работникам, которым он необходим для выполнения трудовых обязанностей.

4.8.2. При использовании беспроводного доступа в офисах Компании/РОКС НН работники обеспечивают выполнение следующих требований ИБ:

– запрещается передавать свои учетные данные (логин/пароль) другим работникам или третьим лицам;

– беспроводная связь в мобильных устройствах и ноутбуках включается только при необходимости её использования (для исключения автоматического подключения к известным или злонамеренным общедоступным беспроводным сетям);

– при доступе к ресурсам сети Интернет соблюдаются ограничения, описанные в п. 4.7 настоящих Методических указаний.

4.8.3. Работникам при работе с ИА в помещениях Компании/РОКС НН запрещается использовать точки доступа в сеть Интернет, не принадлежащие корпоративной беспроводной сети.

4.8.4. При использовании общедоступных беспроводных сетей (например, в транспорте, в аэропорту, в кафе) для выполнения трудовых обязанностей работники обеспечивают выполнение следующих требований ИБ:

– беспроводная связь в корпоративных мобильных устройствах и корпоративных ноутбуках включается только при необходимости её

использования (для исключения автоматического подключения к известным или злонамеренным общедоступным беспроводным сетям);

– используются защищенные общедоступные беспроводные сети, которые в обязательном порядке требуют ввода учетных данных (логина/пароля или только пароля);

– перед подключением к общедоступным беспроводным сетям знакомятся с соглашением пользователя, предоставляемого провайдером сети (такие соглашения могут содержать подробные сведения о том, какие данные необходимо предоставить – запрещается предоставлять корпоративные адреса электронной почты и иные сведения о Компании/РОКС НН);

– при использовании личных или корпоративных ноутбуков – используется защищенное соединение.

4.9. Использование электронной почты

4.9.1. Работники для выполнения трудовых обязанностей используют только КСЭП. Использование иных почтовых систем, в том числе интернет-сервисов, запрещается.

4.9.2. Использование средств обмена мгновенными сообщениями (мессенджеров) для передачи ИА Компании/РОКС НН, содержащихся в ИС и компонентах ИТ-инфраструктуры Компании/РОКС НН, допускается в случае использования корпоративных средств обмена мгновенными сообщениями, включенными в реестр ИС ДИТ (Виртуальный помощник «Ника» (Viber) и корпоративная система объединенных коммуникаций Skype for Business).

4.9.3. Работникам запрещается в личных целях публиковать адрес КСЭП в сети Интернет (например, при заполнении анкет и электронных форм на веб-сайтах, при подписке на рассылки и уведомления).

4.9.4. При использовании КСЭП работникам запрещается:

– отправлять письма, содержащие информацию или материалы противозаконного, экстремистского, дискриминационного, неэтического, расистского или религиозного характера;

– пересылать другим работникам сообщения рекламного характера или другой спам;

– отправлять письма, содержащие информацию, не относящуюся к трудовым обязанностям;

– отправлять ИА на личную электронную почту;

– отвечать на подозрительные письма (от неизвестных отправителей, рекламного характера, спам) или пересылать их другим работникам, а также сообщать любые данные о себе, Компании/РОКС НН, третьих лицах Компании/РОКС НН или какую-либо иную информацию в ответ на эти письма.

4.9.5. Работники обеспечивают отправку письма только тем получателям (адресатам), которым предназначена информация, содержащаяся в этих письмах. Массовая рассылка писем может осуществляться только для выполнения своих трудовых обязанностей в том случае, если содержащаяся в них информация касается всех без исключения получателей (адресатов).

Возможность и сроки рассылки письма в адрес более 100 (ста) получателей согласовываются с администратором КСЭП. Работникам запрещается отвечать на массовую рассылку в режиме «Ответить всем» («Reply to all»).

4.9.6. Работники при отправке писем третьим лицам обеспечивают наличие в письме правовой оговорки (disclaimer) установленной формы в неизменном виде, предупреждающей о том, что содержимое данного письма является конфиденциальной информацией Компании/РОКС НН, неправомерное использование которой запрещено.

4.9.7. При получении электронных сообщений сомнительного содержания (рекламного характера, спам) и (или) от незнакомого отправителя работникам запрещается открывать вложенные файлы и ссылки в тексте таких сообщений, так как это может привести к запуску вредоносного ПО. О получении таких сообщений работник осуществляет незамедлительное информирование в соответствии с п. 4.16 настоящих Методических указаний.

4.9.8. При передаче информации по электронной почте за пределы Компании/РОКС НН в рамках трудовых обязанностей работник обеспечивает согласование с непосредственным руководителем возможности такой передачи. При этом информация передается в архиве, защищенном паролем. Передача пароля к такому архиву осуществляется с использованием канала, отличного от того, который использовался для передачи электронного сообщения, например, по телефону или посредством смс-сообщений.

4.10. Использование программного обеспечения

4.10.1. АРМ предоставляются работникам с предустановленным стандартным ПО, включающим в себя почтовую программу, офисный пакет, веб-браузер, архиватор и другое необходимое для выполнения трудовых обязанностей ПО в соответствии со Стандартом организации «Оснащение рабочих мест пользователей информационных систем ПАО «ГМК «Норильский никель» и российских организаций корпоративной структуры, входящих в Группу компаний «Норильский никель».

4.10.2. Работникам запрещается самостоятельно устанавливать ПО на АРМ Компании/РОКС НН.

4.10.3. В Компании/РОКС НН допускается использование только разрешенного ПО. При наличии обоснованной необходимости использования ПО, не включенного в перечень разрешенного, работник согласовывает такую возможность с ДЗИиИТИ/Службой ИБ.

4.10.4. При необходимости использования личного ноутбука работника для доступа к ИА Компании/РОКС НН состав ПО, разрешенного к установке на личные ноутбуки, может быть ограничен, а запрещенное ПО удалено по согласованию с ДЗИиИТИ/Службой ИБ.

4.11. Защита от вирусов и вредоносного программного обеспечения

4.11.1. Работникам запрещается отключать антивирусное ПО или другие средства защиты информации, а также изменять их режим работы.

4.11.2. При возникновении всплывающих сообщений на веб-сайтах или при получении сообщений по КСЭП, которые внешне напоминают сообщение об обнаружении вируса или другого вредоносного ПО, работникам запрещается:

– переходить по ссылкам, содержащимся в таких сообщениях;

– следовать указаниям, содержащимся в таких сообщениях;

– пересылать данные сообщения другим работникам.

4.12. Резервное копирование информации

4.12.1. Информация, хранимая локально на АРМ, не подлежит централизованному резервному копированию. Для надежного хранения информации, создаваемой или обрабатываемой на АРМ локально, работники обеспечивают хранение такой информации на сетевом диске.

4.12.2. Компания/РОКС НН может осуществлять принудительную перезагрузку АРМ с предварительным уведомлением работника (перезагрузка необходима в целях установки ПО, СЗИ, обновлений ОС, ПО и корпоративных политик) – в таком случае необходимо сохранить рабочие файлы до начала перезагрузки.

4.13. Удаленный доступ

4.13.1. Компания/РОКС НН предоставляет работникам удаленный доступ к ИА, обрабатываемым в ИС, компонентах ИТ-инфраструктуры только в случае необходимости выполнения ими своих трудовых обязанностей вне рабочего места.

4.13.2. Порядок предоставления удаленного доступа к ИА, обрабатываемым в ИС, компонентах ИТ-инфраструктуры, регламентируется Положением «Управление доступом к информационным активам ПАО «ГМК «Норильский никель» для Компании и соответствующими НМД РОКС НН, регламентирующими порядок управления доступом к ИА.

4.14. Пропускной режим и контроль физического доступа к ИА

4.14.1. В Компании/РОКС НН введен пропускной режим и контроль физического доступа к ИА и компонентам ИТ-инфраструктуры, который осуществляется с использованием СКУД.

4.14.2. Доступ на территорию Компании/РОКС НН и в помещения с ограниченным правом доступа предоставляется работникам и третьим лицам в соответствии с Положением «О пропускном и внутриобъектовом режимах в помещениях Главного офиса ПАО «ГМК «Норильский никель», расположенных по адресам: г. Москва, 1-й Красногвардейский проезд, д. 15, ул. Тестовская, д. 8, ул. Тестовская, д. 10» и соответствующими НМД обособленных подразделений Компании/ РОКС НН, регламентирующими порядок пропускного и внутриобъектового режимов.

4.15. Соблюдение правил информационной безопасности при коммуникациях

4.15.1. Работникам, использующим ИА Компании/РОКС НН, запрещается:

– обсуждать ставшую известной информацию, не являющуюся общедоступной, в публичных местах за пределами Компании/РОКС НН;

– доводить информацию другим работникам или третьим лицам, которым эта информация не требуется для выполнения трудовых/договорных обязанностей;

– комментировать информацию и принимать участие в дискуссиях (в т.ч. онлайн), если это может привести к репутационному ущербу для Компании/РОКС НН, ее брендов или работников.

4.15.2. Порядок взаимодействия работников со СМИ определяется Регламентом взаимодействия должностных лиц ПАО «ГМК «Норильский никель» с российскими и зарубежными средствами массовой информации.

4.16. Действия в случае возникновения инцидентов ИБ или подозрений на возникновение инцидентов ИБ

4.16.1. При обнаружении инцидентов ИБ или подозрений на инцидент ИБ работники осуществляют незамедлительное информирование по адресу: infosec@nornik.ru или путем регистрации обращения через Единую службу поддержки сервисов, в соответствии с Регламентом управления инцидентами информационной безопасности в ПАО «ГМК «Норильский никель». Примерами инцидентов ИБ (подозрений на инцидент ИБ) являются:

– подозрение на вирусное заражение АРМ или ИС;

– получение подозрительного электронного письма/телефонного звонка с запросом информации или выполнению действий, которые не были согласованы заранее;

– компрометация учетной записи (разглашение логина и пароля);

– нарушение требований ИБ, установленных в Компании/РОКС НН;

– нарушения установленного порядка и правил обращения с ИА;

– утрата АРМ, съемных носителей информации, мобильных устройств или другого ИТ-оборудования Компании/РОКС НН;

– попытка несанкционированного доступа к ИС;

– сбой в работе средств защиты информации;

– в любых других случаях, если, по мнению пользователя ИС, возникают риски нарушения ИБ Компании/РОКС НН.

4.16.2. При подозрении на вирусное заражение АРМ или ИС, работник обеспечивает прекращение работы на АРМ и в ИС (не вводит учетные данные, не отправляет почту, не переходит по ссылкам и т.п.) до выяснения причин работниками ДЗИиИТИ/Службой ИБ.

5. Ответственность

5.1. Все работники, использующие ИА, несут персональную ответственность за несоблюдение установленных требований к работе с ИА и допущение их несанкционированного использования или разглашения и могут привлекаться к дисциплинарной и материальной ответственности в порядке,

установленном Трудовым кодексом Российской Федерации и иными законодательными актами.

5.2. Ответственность за ненадлежащую организацию и неосуществление контроля исполнения требований настоящих Методических указаний несет директор ДЗИиИТИ.

5.3. Ответственность за несвоевременное внесение изменений и дополнений в настоящие Методические указания несет директор ДЗИиИТИ.