Приложение № 1 к приказу от «13» мая 2012 № 279

Открытое
акционерное общество
«ГОРНО-МЕТАЛЛУРГИЧЕСКАЯ КОМПАНИЯ
«НОРИЛЬСКИЙ НИКЕЛЬ»

кольская ГМК

Открытое
акционерное общество
«Кольская горно -
металлургическая компания»

Россия, 184507,Мурманская обл, г.Мончегорск – 7, тел.(815-36) 7-72-01, факс: (815-36) 7-99-86

ПОЛОЖЕНИЕ

об информационной безопасности

ОАО «Кольская горно-металлургическая компания»

П-3-7900-03-2012

Введено взамен приказа от 21.10.2009 года №501 «Об утверждении Положения об информационной безопасности в ОАО «Кольская горно-металлургическая компания»

Дата введения: 2012-06-01

г. Мончегорск

СОДЕРЖАНИЕ

1. Общие положения.

1.1. Информационная безопасность является составляющей экономической безопасности и обязательным условием деятельности ОАО «Кольская горно-металлургическая компания» (Компания).

1.2. Целью защиты информации является предотвращение (сведение к минимуму) возможности нанесения материального, физического, морального или иного ущерба Компании посредством случайного или преднамеренного несанкционированного вмешательства в процесс функционирования ее информационной среды, а также обеспечение использования технологий обработки информации на уровне приемлемых для Компании рисков.

1.3. Деятельность по защите информации осуществляется на основе законодательства Российской Федерации, распорядительных и нормативно-методических документов уполномоченных государственных органов и Компании.

1.4. Настоящее Положение определяет систему обеспечения информационной безопасности, ее структуру, задачи и функции, основы организации защиты сведений, составляющих коммерческую тайну и другого рода информации, подлежащей защите в соответствии с действующим законодательством Российской Федерации. Конкретные мероприятия по защите коммерческой тайны и принципы организации ее защиты должны быть определены в дополнительно разрабатываемых нормативно-методических документах. Таких, как:

- Руководством по защите коммерческой тайны – в части выработки порядка обеспечения безопасности информации в структурных (СП), внутренних структурных (ВСП) подразделениях и Управлении Компании;
- Инструкцией по конфиденциальному делопроизводству – в части организации и ведения конфиденциального делопроизводства в Компании;
- Положением об организации работ по защите информации в автоматизированных системах – в части определения порядка организации и проведения работ, по защите информации в автоматизированных системах (АС) и распределения функций между СП (ВСП) и должностными лицами по защите информации в АС Компании.
- Приказами, регламентами, специальными инструкциями – в части определения конкретных действий при обращении с конфиденциальной информацией.

1.5. **Настоящее Положение не распространяется на деятельность по защите сведений, составляющих государственную тайну.**

2. Термины, и определения.

информация – сведения о лицах, предметах, фактах, событиях, явлениях и процессах, независимо от формы их представления (может существовать в различных формах, в том числе в виде машинописного или рукописного текста на бумажном носителе, может храниться в электронном виде, передаваться по почте или с использованием электронных средств связи, демонстрироваться на пленке или быть выражена устно);

информационные процессы – процессы сбора, обработки, накопления, хранения, поиска и распространения информации;

информационная система – организационно упорядоченная совокупность документов и информационных массивов во взаимосвязи с информационными технологиями, реализующими информационные процессы;

информационные ресурсы – отдельные документы и части информационных массивов в информационных системах;

информационная среда – информационная система во взаимосвязи с территориальной распределенностью, степенью развития информационных технологий и с учетом уровня подготовки обслуживающего и эксплуатирующего персонала;

ИТ-профсервис – совокупность производственных объектов, активов и подразделений, которые предоставляют Компании услуги в области информационных технологий и рассматриваются, как отдельный единый субъект управления.

информационная безопасность - состояние защищенности информационной среды, обеспечивающее ее формирование, использование и развитие в интересах Компании.

конфиденциальная информация - информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации и которая включает:

- сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях;
- сведения, составляющие тайну следствия и судопроизводства;
- служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна);
- сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее);
- сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (коммерческая тайна);
- сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

конфиденциальное делопроизводство – деятельность, обеспечивающая документирование и организацию работы с документами и другими носителями информации, содержащими информацию, составляющую коммерческую тайну.

конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

коммерческая тайна – режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.

информация, составляющая коммерческую тайну, - 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.

передача информации, составляющей коммерческую тайну, – передача информации, составляющей коммерческую тайну и зафиксированной на материальном носителе, ее обладателем контрагенту на основании договора в объеме и на условиях, которые

предусмотрены договором, включая условие о принятии контрагентом установленных договором мер по охране ее конфиденциальности.

предоставление информации, составляющей коммерческую тайну, – передача информации, составляющей коммерческую тайну и зафиксированной на материальном носителе, ее обладателем органам государственной власти, иным государственным органам, органам местного самоуправления в целях выполнения их функций.

разглашение информации, составляющей коммерческую тайну, – действие или бездействие, в результате которых информация, составляющая коммерческую тайну, в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя такой информации либо вопреки трудовому или гражданско-правовому договору.

режим коммерческой тайны – правовые, организационные, технические и иные принимаемые обладателем информации, составляющей коммерческую тайну, меры по охране ее конфиденциальности.

3. Использованные нормативные документы.

Гражданский кодекс Российской Федерации. Часть четвертая, №230-ФЗ от 18.12.2006 года.

Трудовой кодекс Российской Федерации, №197-ФЗ от 30.12.2001 года

Федеральный Закон Российской Федерации «О коммерческой тайне» №98-ФЗ от 29.07.2004 года.

Федеральный Закон Российской Федерации «Об информации, информационных технологиях и о защите информации» №149-ФЗ от 27.07.2006 года.

Федеральный Закон Российской Федерации «О персональных данных» №152-ФЗ от 27.07.2006 года.

ГОСТ ИСО/МЭК 17799-2005 «Практические правила управления информационной безопасностью».

Концепция информационной безопасности ОАО «Кольская ГМК» (К 3-79-01-2007) .

4. Основные задачи в области информационной безопасности

- обеспечение конфиденциальности информации, защищаемой в соответствии с законодательством Российской Федерации;
- обеспечение достоверности, полноты и целостности обрабатываемой информации;
- защита от навязывания ложной информации;
- обеспечение своевременного законного доступа к информации, обрабатываемой в информационной системе Компании;
- разграничение ответственности участников информационных процессов за нарушение установленных правил обращения с информацией и нарушение законных прав субъектов информационных отношений;
- создание системы обеспечения информационной безопасности Компании;
- осуществление непрерывного контроля и управления процессами обработки и передачи информации.

5. Система обеспечения информационной безопасности.

5.1. Систему обеспечения информационной безопасности составляет скоординированная деятельность СП (ВСП) по поддержанию безопасности информационной среды на уровне

приемлемых для Компании рисков.

5.2. Общее руководство системой обеспечения информационной безопасности в Компании осуществляет Генеральный директор Компании через Директора Департамента безопасности.

5.3. На всех этапах создания информационных систем (проектирование, разработка, изготовление, монтаж, испытания, подготовка к эксплуатации и эксплуатация) соответствующие проектные, нормативные, организационно-распорядительные документы, договоры на поставку оборудования и т.д. в обязательном порядке согласовываются с Департаментом безопасности.

5.4. В интересах обеспечения информационной безопасности Компании защите подлежат:

- информационные ресурсы, содержащие конфиденциальную информацию и персональные данные работников Компании, а также информационные процессы их обслуживающие;
- информационные системы, обслуживающие информационные процессы, связанные с конфиденциальной информацией и персональными данными работников Компании (программные средства, средства вычислительной техники, связи, приема и передачи данных, эксплуатационная и сопроводительная документация к ним);
- помещения, транспортные средства и т.д. (со всей совокупность установленных в них технических средств), предназначенные для ведения закрытых совещаний и переговоров.

5.5. Защита информации достигается:

- тщательным подбором и подготовкой персонала;
- проверкой его благонадежности при приеме на работу;
- исключением несанкционированного доступа к информационным ресурсам;
- четкой организацией конфиденциального делопроизводства;
- строгой регламентацией информационных процессов;
- специальной организацией проведения закрытых совещаний и переговоров;
- предотвращением утечки информации по техническим каналам;
- предотвращением воздействий, вызывающих разрушение, уничтожение, искажение информации или сбои в информационных процессах;
- организацией пропускного и внутри объектового режима в Компании;
- эффективным контролем информационной безопасности;
- соблюдением правил и норм поведения, определенных корпоративной этикой, поддержанием здоровой морально-психологической атмосферы в коллективе, исключающей возникновение конфликтных ситуаций и негативных последствий.

5.6. Структурно в систему обеспечения информационной безопасности в Компании входят:

- Департамент безопасности - в части организации, координации и контроля всей деятельности по защите информации, составляющей коммерческую тайну, или защищаемой в режиме коммерческой тайны в соответствии с действующим законодательством Российской Федерации;
- Постоянно действующая техническая комиссия - в части выполнения дополнительных функций по вопросам обеспечения защиты коммерческой тайны Компании и иной конфиденциальной информации;

- Правовое управление - в части определения правомочности мер, предпринимаемых для защиты информации и законности ее передачи другим потребителям;
- ИТ-профсервис - в части организации эксплуатации технических средств, обеспечивающих защиту информации при ее обработке в автоматизированных информационных системах и в автоматизированных системах управления технологическим процессом Компании, обеспечения антивирусной защиты этих систем и целостности данных, используемых в них, а также в части соблюдения элементарных требований к обеспечению информационной безопасности, определяемых в соответствии с Федеральным законодательством и ГОСТ РФ для обработки информации с использованием ИТ-технологий;
- Департамент персонала - в части организации обработки и обеспечения сохранности персональных данных работников при их использовании в текущей деятельности Компании;
- Управление делами - в части обеспечения сохранности персональных данных действующих и бывших работников Компании при их хранении в архиве, а также в части организации работы по обеспечению сохранности документов, образующихся в текущей деятельности Компании;
- Мобилизационно-режимный отдел – в части определения порядка обращения с «коммерческой тайной (1 категории)» и обеспечения контроля за сохранностью информации, подпадающей под действие данного ограничительного грифа;
- руководители СП и ВСП Компании, в которых организовано конфиденциальное делопроизводство или (и) обрабатывается с использованием информационных технологий информация, подлежащая защите – в части организации и поддержания в СП (ВСП) режима коммерческой тайны;
- экспертные комиссии СП и ВСП Компании – в части контроля соблюдения режима коммерческой тайны при работе с документами, содержащими коммерческую тайну, и уничтожения этих документов по истечении срока хранения;
- администраторы безопасности локальных вычислительных сетей и лица, ответственные за ведение конфиденциального делопроизводства – в части надлежащего исполнения требований своих должностных инструкций и личной ответственности за соблюдение режима коммерческой тайны;
- должностные лица и исполнители, участвующие в информационных процессах – в части личной ответственности за соблюдение режима коммерческой тайны;
- применяемые в Компании активные и пассивные технические средства защиты информации;
- внешние специализированные организации, имеющие лицензии на деятельность в области защиты информации и проводящие работы по обеспечению информационной безопасности Компании на договорной основе.

5.7. Департамент безопасности осуществляет непосредственное руководство системой управления информационной безопасности. С этой целью:

- накапливает и анализирует сведения о попытках преодоления системы защиты информации и используемых в этих целях методах и средствах;
- организует проверку работников СП и ВСП, работающих с коммерческой тайной, а также осуществляет систематический контроль соблюдения ими требований режима коммерческой тайны;
- участвует в проведении служебных расследований по фактам незаконного получения и разглашения коммерческой тайны, организует проведение оценки размера экономического ущерба, причиненного Компании в результате несанкционированного доступа к защищаемым информационным ресурсам;

- разрабатывает и осуществляет организационные и инженерно-технические мероприятия по защите информационной системы Компании;
- разрабатывает и представляет на утверждение руководства Компании проекты распорядительных и нормативно-методических документов по вопросам защиты информации;
- осуществляет методическое обеспечение работ по защите информации в дочерних и зависимых обществах;
- организует аудит автоматизированных информационных систем Компании на предмет соблюдения установленных правил и технических норм по обеспечению информационной безопасности;
- проводит анализ обоснованности запросов сторонних организаций на предоставление информации о производственной и иной деятельности Компании и готовит предложения по ограничению внешнего документооборота;
- в пределах своей компетенции во взаимодействии с правоохранительными органами организует и проводит мероприятия по выявлению технических и иных каналов утечки информации из Компании;
- взаимодействует по вопросам информационной безопасности с государственными и иными организациями, а также подразделениями защиты информации ОАО «ГМК «Норильский никель»;
- организует тестирование, выбор сертифицированных средств защиты информации и подготовку заключений о возможности проведения работ с конфиденциальной информацией;
- осуществляет контроль информационной безопасности в СП (ВСП) Компании и разрабатывает предложения по ее совершенствованию;
- участвует в организации профессиональной подготовки работников СП (ВСП) Компании, ответственных за защиту информации и оказывает им методическую и практическую помощь;
- организует пропускной и внутри объектовый режим в Компании;
- организует охрану зданий, помещений, транспорта и т.д., функционирование которых связано с использованием информационной системы Компании.

5.8. Постоянно действующая техническая комиссия (ПДТК) Компании по защите государственной тайны руководствуется в своей деятельности Конституцией Российской Федерации, Федеральными Законами, Указами и Распоряжениями Президента Российской Федерации, Постановлениями и Распоряжениями Правительства Российской Федерации, нормативными и правовыми актами уполномоченных государственных органов, ОАО «ГМК «Норильский никель», ОАО «Кольская ГМК», регламентирующими вопросы защиты коммерческой тайны, а также Уставом Компании. К компетенции ПДТК по обеспечению защиты коммерческой тайны относится решение следующих вопросов:

- выработка предложений о дополнении и изменении Перечня информации, составляющей коммерческую тайну Компании (к работе по формированию Перечня привлекаются руководители и наиболее квалифицированные специалисты заинтересованных СП и ВСП);
- подготовка решений об отнесении работ, выполняемых в Компании и ее ДЗО, к коммерческой тайне;
- выработка рекомендаций по обеспечению защиты коммерческой тайны Компании при осуществлении научно-технического и экономического сотрудничества с зарубежными партнерами и проведении переговоров с ними, при заключении и выполнении международных договоров, при организации деятельности СП (ВСП) по выполнению обязательств Компании, вытекающих из международных договоров;
- организация и проведение научно-исследовательских и опытно-конструкторских

работ по разработке, производству и испытанию создаваемых в интересах Компании систем защиты информации, составляющей коммерческую тайну, или специализированного оборудования для защиты этой информации;
- согласование (разработка) проектов основных направлений работ по комплексной защите информации, целевых программ и соответствующих отраслевых планов работ в этой области.

5.9. Правовое управление:
- определяет правомочность запросов на предоставление информации, поступающих от других юридических лиц, государственных органов власти и самоуправления;
- подает в Департамент безопасности предложения по ограничению внешнего документооборота;
- по решению руководства Компании участвует в проведении служебных расследований по фактам незаконного получения и разглашения конфиденциальной информации.

5.10. ИТ-профсервис:
- через функционально подчиненные подразделения организует сопровождение и эксплуатацию всех типов автоматизированных информационных систем с соблюдением элементарных требований к обеспечению информационной безопасности, определяемых в соответствии с Федеральным законодательством и ГОСТ РФ для обработки информации с использованием ИТ-технологий;
- через функционально подчиненные подразделения осуществляет весь комплекс мероприятий по обеспечению эксплуатации подсистем информационной безопасности во всех типах автоматизированных информационных систем;
- обеспечивает целостность и доступность данных во всех типах автоматизированных информационных систем и антивирусную защиту этих систем;
- участвует в выработке Концепции обеспечения информационной безопасности Компании;
- участвует в выборе сертифицированных средств защиты информации и их тестировании.

5.11. Департамент персонала:
- в соответствии с действующим законодательством Российской Федерации и нормативно-распорядительными документами Компании организует мероприятия по обеспечению сохранности персональных данных работников;
- организует работу по передаче на хранение в Архивное бюро Управления делами персональных данных работников и бывших работников Компании.

5.12. Управление делами (во взаимодействии с заинтересованными структурными подразделениями), в строгом соответствии с законодательством Российской Федерации и действующими нормативно-распорядительными документами уполномоченных государственных органов и Компании:
- обеспечивает сохранность персональных данных действующих и бывших работников Компании при их хранении в архиве;
- обеспечивает секретарям Управления делами условия для соблюдения требований режима коммерческой тайны при работе с конфиденциальной информацией;
- организует работу по обеспечению сохранности документов, образующихся в текущей деятельности Компании.

5.13. Мобилизационно-режимный отдел осуществляет руководство деятельностью по обращению с информацией Компании, отнесенной к «коммерческой тайне (1 категории)». С

этой целью:

- разрабатывает и представляет на утверждение руководства Компании проекты распорядительных и нормативно-методических документов по вопросам защиты «коммерческой тайны (1 категории)»;
- участвует в проведении служебных расследований по фактам незаконного получения и разглашения информации, отнесенной к «коммерческой тайне (1 категории)», организует проведение оценки размера ущерба, причиненного Компании в результате несанкционированного доступа к защищаемым информационным ресурсам;
- проводит анализ обоснованности запросов сторонних организаций на предоставление информации, имеющей ограничительный гриф «коммерческая тайна (1 категории)» и готовит предложения по ограничению внешнего документооборота;
- организует проведение инженерно-технических мероприятий по защите «коммерческой тайны (1 категории)» Компании;
- взаимодействует по вопросам защиты «коммерческой тайны (1 категории)» с государственными и иными организациями, а также с УЗГТиМП ОАО «ГМК «Норильский никель».

5.14. Руководители СП и ВСП Компании, в которых организовано конфиденциальное делопроизводство или (и) обрабатывается с использованием информационных технологий информация, подлежащая защите:

- организуют проведение мероприятий по защите информации в своих подразделениях в соответствии с требованиями распорядительных и нормативно-методических документов;
- обеспечивают секретарям своего СП (ВСП) условия для соблюдения требований режима коммерческой тайны при работе с конфиденциальной информацией;
- оказывают содействие специалистам Департамента безопасности Компании в проведении специальных проверок и специальных исследований информационных систем;
- незамедлительно сообщают в Департамент безопасности Компании о всех попытках несанкционированного доступа к информационным ресурсам подразделения и принятых мерах по их пресечению;
- участвуют в осуществлении контроля информационной безопасности в своем подразделении, содействуют в проведении расследований фактов ее нарушений;
- участвуют в осуществлении оценки ущерба Компании, причиненного в результате несанкционированного доступа к защищаемым информационным ресурсам, кураторами которых они являются.

5.15. Специальные обязанности администраторов безопасности локальных вычислительных сетей, лиц, ответственных за ведение конфиденциального делопроизводства, должностных лиц и исполнителей, участвующих в информационных процессах определяются специальными инструкциями, разработанными в СП (ВСП) и согласованными с Департаментом безопасности Компании.

6. Организация контроля информационной безопасности.

6.1. Контроль заключается в проверке выполнения требований законодательства Российской Федерации, нормативно-распорядительных документов уполномоченных государственных органов, руководства Компании по вопросам информационной безопасности.

6.2. Контроль информационной безопасности осуществляется с целью:

- своевременного выявления и предотвращения каналов утечки информации;
- выявления условий, способствующих хищению, утрате и искажению

информационных ресурсов;
- выявлению нарушений в ведении конфиденциального делопроизводства;
- выявления недостатков в системе инженерно-технической защиты информационной системы;
- оценки обоснованности и эффективности мер, предпринимаемых для защиты конфиденциальной информации и персональных данных работников Компании;
- оценки информационной безопасности и выработки предложений, направленных на ее совершенствование.

6.3. Для проведения анализа достаточности мер, предпринимаемых для защиты информационной системы, получения консультаций или выполнения работ, связанных с созданием подсистем информационной безопасности, на договорной основе могут привлекаться специализированные организации, имеющие государственные лицензии на данный вид деятельности.

6.4. Повседневный контроль информационной безопасности в Компании организуется руководителями СП (ВСП), входящими в систему обеспечения информационной безопасности, в пределах компетенции, определенной в разделе 5 настоящего Положения, в объемах, определяемых специальными инструкциями.

6.5. Периодичность и объем контрольных мероприятий, осуществляемых сотрудниками Департамента безопасности Компании устанавливаются отдельными планами.

6.6. Сотрудники отдела информационной безопасности Департамента безопасности при выполнении своих служебных обязанностей имеют право доступа ко всем информационным ресурсам и системам Компании, не содержащим сведений, составляющих государственную тайну[1]. Указанные работники имеют право:

- посещать все здания и помещения Компании, в которых осуществляются информационные процессы;
- требовать устных и письменных объяснений и справок от любых работников Компании, за исключением Генерального директора Компании и его заместителей;
- проводить беседы и консультации с работниками специализированных организаций, имеющих государственные лицензии на деятельность в сфере обеспечения информационной безопасности;
- запрещать выполнение работ при нарушении требований распорядительных и нормативных документов по информационной безопасности.

6.7. Результаты контроля информационной безопасности, предложения и рекомендации по устранению выявленных нарушений докладываются Директору Департамента безопасности Компании и в виде предписания доводятся руководителю проверенного СП (ВСП). Требования, изложенные в предписании обязательны для исполнения.

7. Категорирование нарушений информационной безопасности.

7.1. Нарушения информационной безопасности по степени важности делятся на три категории:

I категория - невыполнение требований и норм по защите информации, в результате чего:

a) имеются признаки преступлений, предусмотренных УК РФ (преступления в сфере компьютерной информации, защиты коммерческой тайны, тайны переписки, телефонных переговоров, и т.д.);
b) имеется угроза личной безопасности работников Компании и членов их семей;

[1] допуск к сведениям, составляющим государственную тайну и в помещения, в которых эти сведения обрабатываются, осуществляется с учетом требований законодательства РФ и руководящих документов Компании

с) имеются нарушения конфиденциальности, целостности или доступности информации, приведшие к нарушению управления деятельностью Компании или прямому материальному ущербу.

II категория - невыполнение требований по защите информации, в результате чего создаются реальные предпосылки к нарушениям I категории.

III категория – другие нарушения требований по защите информации.

7.2. В случаях, когда выявленные нарушения требуют принятия незамедлительных мер (относятся к I-II категории), сотрудник Департамента безопасности Компании, осуществляющий проверку СП (ВСП), может потребовать немедленного устранения выявленных недостатков. В этом случае требования проверяющего (в том числе устные) обязательны для исполнения всеми работниками СП (ВСП) и доводятся до руководителя СП (ВСП) в 3-дневный срок в письменной форме.

7.3. Расследование нарушений информационной безопасности производятся сотрудниками Департамента безопасности Компании. По решению Директора Департамента безопасности может быть назначена комиссия из состава сотрудников Департамента, работников СП (ВСП), в котором обнаружены нарушения и других работников Компании.

7.4. В ходе расследования:

- выясняются обстоятельства и причины возникновения нарушения;
- определяется категория нарушения;
- рассчитывается размер причиненного (возможного) материального и иного ущерба;
- вырабатываются предложения по нейтрализации (уменьшению) последствий и причин возникновения подобных нарушений.

8. Ответственность за нарушение информационной безопасности.

8.1. В случае незаконного получения и разглашения сведений, составляющих коммерческую тайну, утраты документов, содержащих конфиденциальную информацию и иных нарушений при работе с информационными ресурсами, виновные лица могут быть привлечены к дисциплинарной, гражданско-правовой или уголовной ответственности в соответствии с действующими законодательством Российской Федерации.

9. Финансирование мероприятий по обеспечению информационной безопасности.

9.1. Финансирование мероприятий по обеспечению информационной безопасности производится:

- в автоматизированных информационных системах – в рамках бюджета ИТ-профсервиса;
- по отдельным проектам СП и ВСП – в рамках финансирования проектов;
- по оснащению информационных систем техническими средствами защиты информации, требующими капитальных вложений – в рамках инвестиционных проектов;
- мероприятия общего характера по обеспечению информационной безопасности:
  - для СП Управления Компании – в рамках бюджета Управления делами, сформированного по заявкам СП Управления, представленным на момент планирования бюджета;
  - для ВСП Компании – за счет собственных лимитов ВСП в рамках заявочной компании.

ЛИСТ ВИЗИРОВАНИЯ

Положение об информационной безопасности

ОАО «Кольская горно-металлургическая компания»

Должность, фамилия, инициалы	**Дата**	**Подпись**
Первый заместитель Генерального директора – главный инженер, председатель ПДТК по защите гостайны С.Г. Беседовский	18.05.12	
Директор Департамента безопасности А.И. Коломиец	18.04.12.	
Директор Департамента персонала Р.Д. Эльканов	15.05.12	
Управляющий делами ~~А.С. Федорцова~~ Л.И. Муравьева	04.05.12	
Директор Департамента информационных технологий Е.В. Навильников	15.05.12	
Начальник Правового управления А.А. Шестаков	16.05.12	
Начальник Мобилизационно-режимного отдела К.М. Сергиенко	19.04.12.	