УТВЕРЖДЕНА
приказом
ООО «Газпром добыча Ноябрьск»
от «18» декабря 2023 г. № 1832

ПОЛИТИКА
информационной безопасности
ООО «Газпром добыча Ноябрьск»

694-02-2023

Содержание

1. Общие положения

1.1 Настоящая Политика информационной безопасности ООО «Газпром добыча Ноябрьск» (далее - Политика) разработана с учетом требований федерального законодательства, Политики информационной безопасности ПАО «Газпром», утвержденной приказом ПАО «Газпром» от 15.02.2008 № 48, Положения настоящей Политики служат основой для разработки организационно-распорядительных документов ООО «Газпром добыча Ноябрьск» (далее - Общество), регламентирующих нормы и правила обеспечения защиты информации.

1.2 Политика определяет позицию руководства Общества в отношении информационной безопасности, основные цели и направления.

1.3 В рамках Политики определено, что:

1) информационные технологии играют важную роль в достижении бизнес-целей Общества;

2) информация является ценным активом Общества, требующим защиты независимо от форм ее представления;

3) в своей деятельности Общество сталкивается с широким спектром угроз информационной безопасности как внутреннего, так и внешнего характера, реализация которых может привести к ущербу (финансовые потери, юридические взыскания, потеря репутации, дезорганизация и т.д.);

4) стратегической целью Общества в области информационной безопасности является обеспечение функционирования и использования информационных технологий с учетом принимаемых рисков получения возможного ущерба от реализации угроз информационной безопасности;

5) стратегической задачей в области информационной безопасности является построение системы управления информационной безопасностью, основанной на методологии управления рисками, учитывающей бизнес-требования, а также правовые требования информационной безопасности.

1.4 Исполнение положений настоящей Политики является обязательным для всех работников Общества.

2. Цели Политики информационной безопасности

2.1. Основными целями Политики являются:

1) обеспечение единых с Политикой информационной безопасности ПАО «Газпром» подходов к организации информационной безопасности в Обществе;

2) обеспечение единых подходов к обеспечению информационной безопасности в рамках Общества;

3) создание методологической основы для разработки внутренних документов по информационной безопасности в Обществе;

4) определение форм участия руководства Общества в решении проблем информационной безопасности.

2.2. Основными целями процесса обеспечения информационной

безопасности в Обществе являются:

1) создание условий для устойчивого функционирования информационной инфраструктуры Общества;

2) поддержание необходимого уровня информационной безопасности в Обществе, соответствующего требованиям федерального законодательства, нормативных и организационно-распорядительных документов ПАО «Газпром».

3. Направления обеспечения информационной безопасности

3.1 Обеспечение информационной безопасности в Обществе осуществляется по следующим направлениям:

1) управление информационной безопасностью;

2) идентификация и классификация объектов защиты;

3) организация работы по осведомленности работников Общества в вопросах информационной безопасности;

4) управление инцидентами информационной безопасности;

5) обеспечение непрерывности бизнес-процессов;

6) обеспечение информационной безопасности при эксплуатации средств обработки, хранения и передачи информации и использовании информационных ресурсов;

7) обеспечение соответствия требованиям информационной безопасности, установленных в Обществе.

3.2 Данные направления реализуются организационными и техническими мерами.

4. Управление информационной безопасностью

4.1 Внутренняя организация

4.1.1 Организация и обеспечение управления информационной безопасностью в Обществе осуществляется его руководителем.

4.1.2 Руководство Общества постоянно поддерживает необходимый уровень информационной безопасности путем внедрения системы обеспечения информационной безопасности, а также распределения обязанностей и ответственности работников Общества за ее внедрение и осуществление.

4.1.3 Организация плановой, непрерывной и целенаправленной работы по осуществлению мер обеспечения информационной безопасности и контролю их выполнения в Обществе возлагается на отдел информационной безопасности Службы корпоративной защиты Общества (далее - Служба корпоративной защиты, СКЗ).

4.1.4 На Службу корпоративной защиты возложены функции:

1) планирование работ по информационной безопасности;

2) контроль эффективности реализуемых мер обеспечения

информационной безопасности и внесение рекомендаций по их совершенствованию;

3) координация действий по обеспечению информационной безопасности с представителями различных структурных подразделений Общества;

4) контроль выполнения и пересмотр политик информационной безопасности объектов защиты.

4.1.5 С учетом особенностей объектов информационной инфраструктуры в Обществе осуществляется:

1) определение полномочий работников в отношении защищаемых информационный ресурсов;

2) администрирование и контроль средств и механизмов безопасности;

3) контроль выполнения работниками требований в области информационной безопасности.

4.1.6 Функции администрирования и контроля средств и механизмов безопасности распределяются между подразделениями, эксплуатирующими объекты защиты информационной инфраструктуры, и Службой корпоративной защиты:

1) администрирование встроенных механизмов безопасности средств обработки, хранения и передачи информации, а также дополнительных средств защиты осуществляется работниками подразделений, отвечающих за их эксплуатацию;

2) контроль функционирования и настройки механизмов безопасности, определение полномочий работников в отношении защищаемых информационных ресурсов, а также соблюдения требований по информационной безопасности возлагается на Службу корпоративной защиты.

4.1.7 В Обществе организуется администрирование информационной безопасности, направленное на обеспечение установленных правил доступа к объектам информационной инфраструктуры, порядка обращения с защищаемой информацией при ее обработке, хранении и передаче.

4.1.8 Администратором информационной безопасности назначается, как правило, работник структурного подразделения, эксплуатирующего защищаемые объекты информационной инфраструктуры.

4.1.9 На администратора информационной безопасности возлагается ответственность по предотвращению несанкционированного доступа к защищаемой информации.

4.1.10 Обязанности работников Общества по обеспечению информационной безопасности зависят от занимаемой должности и определяются их должностными инструкциями.

4.1.11 В каждом структурном подразделении назначается работник, ответственный за обеспечение информационной безопасности, перечень обязанностей которого разрабатывается с учетом специфики работы подразделения.

4.1.12 В Обществе ежегодно разрабатывается план мероприятий по обеспечению информационной безопасности на будущий год, в том числе

мероприятий по контролю состояния информационной безопасности.

4.2 Обеспечение информационной безопасности при работе с внешними организациями

4.2.1 При организации доступа сторонних организаций к защищаемым информационным ресурсам в Обществе осуществляются мероприятия по обеспечению информационной безопасности:

1) определение рисков, связанных с предоставлением доступа сторонней организации к конфиденциальной информации;

2) формирование на основе оценки рисков перечня мероприятий по обеспечению информационной безопасности при предоставлении доступа сторонней организации к конфиденциальной информации Общества и их реализация;

3) заключение соглашения о конфиденциальности со сторонними организациями, которым предоставляется доступ к конфиденциальной информации Общества.

4.2.2 Порядок представления информации органам государственной власти, а также передачи материалов средствам массовой информации, вопросы обеспечения информационной безопасности при допуске на объекты защиты Общества иностранных представителей регламентируются нормативными и организационно-распорядительными документами ПАО «Газпром» и Общества в области информационной безопасности.

4.3 Идентификация и классификация объектов защиты

4.3.1 В целях обеспечения информационной безопасности в Обществе осуществляется идентификация и классификация объектов защиты информационной инфраструктуры, определение степени их критичности, классификация и назначение ответственных за их безопасную эксплуатацию.

4.3.2 Идентификация и классификация объектов защиты, определение степени критичности осуществляются в соответствии с требованиями СТО Газпром 4.2-3-004. Идентифицированные и классифицированные объекты защиты отражаются в инвентаризационной документации, маркируются и для них назначаются владельцы - работники Общества, ответственные за безопасную эксплуатацию объектов защиты.

4.3.3 Процедуры повторяются регулярно. Внеплановые процедуры идентификации и классификации объектов защиты выполняются в случае внесения существенных изменений в информационную инфраструктуру Общества.

4.3.4 На основе классификации объектов защиты информационной инфраструктуры определяются применяемые по отношению к ним меры безопасности. Процедуры обработки информации и правила безопасного использования объектов защиты определяются их политиками информационной

безопасности, а также другими нормативными и организационно-распорядительными документами ПАО «Газпром» и Общества в области информационной безопасности.

4.4 Организация работы с персоналом по вопросам информационной безопасности

4.4.1 Обеспечение безопасности при заключении и во время действия трудового договора

4.4.1.1 В целях повышения уровня обеспечения информационной безопасности при приеме на работу новых работников осуществляется доведение до них правил обеспечения информационной безопасности и устанавливается ответственность за их нарушение.

4.4.1.2 Обязанности работников Общества по соблюдению правил информационной безопасности определяются должностными инструкциями и конкретизируются нормативными и организационно-распорядительными документами ПАО «Газпром» и Общества в области информационной безопасности.

4.4.1.3 При приеме на работу Общество заключает с работником договор о конфиденциальности.

4.4.1.4 В Обществе обеспечивается сохранность заключенных соглашений о конфиденциальности.

4.4.1.5 Все работники Общества при вступлении в должность проходят вводный инструктаж, предусматривающий ознакомление с правилами и мерами информационной безопасности.

4.4.1.6 Для работников Общества реализуются мероприятия повышения осведомленности в области информационной безопасности.

4.4.1.7 Работники, отвечающие за обеспечение информационной безопасности, регулярно проходят повышение квалификации, знакомятся с изменениями в федеральном законодательстве, нормативных и организационно-распорядительных документах ПАО «Газпром» и Общества в области информационной безопасности.

4.4.1.8 Работники Общества, имеющие доступ к информации, подлежащей защите, несут ответственность за ее разглашение и утрату, а также за нарушение установленного порядка обеспечения информационной безопасности.

4.4.1.9 Работники, разгласившие подлежащую защите информацию или нарушившие установленный порядок обращения с ней, а также работники, по вине которых произошла ее утрата или искажение, несут ответственность в соответствии с действующим законодательством Российской Федерации.

4.4.2 Обеспечение безопасности при увольнении и изменении условий трудового договора

4.4.2.1 В целях обеспечения информационной безопасности при увольнении и изменении условий трудового договора в Обществе осуществляется контроль возврата технических средств обработки, хранения и передачи информации, своевременного прекращения прав доступа работников к объектам защиты Общества.

4.4.2.2 Напоминание увольняемым работникам о принятых ими обязательствах по соблюдению в тайне конфиденциальных сведений и доведение до них срока сохранения в тайне сведений, с которыми они были ознакомлены, выполняются группой по организации режима коммерческой тайны отдела информационной безопасности Службы корпоративной защиты.

4.4.2.3 При увольнении работника (изменении условий трудового договора) его права доступа к информационным ресурсам незамедлительно аннулируются (приводятся в соответствие с новыми условиями).

4.4.2.4 Служба корпоративной защиты осуществляет контроль своевременного прекращения доступа уволенных работников (также при изменении условий трудового договора) к объектам защиты.

4.4.2.5 Отдел кадров и трудовых отношений своевременно уведомляет Службу корпоративной защиты об увольнении (изменении условий трудового договора) работников.

4.5 Управление инцидентами информационной безопасности

4.5.1 Оповещение об инцидентах информационной безопасности

4.5.1.1 В целях предотвращения нарушений информационной безопасности в Обществе принимаются меры по оповещению об инцидентах информационной безопасности.

4.5.1.2 Работники Общества обязаны сообщать в Службу корпоративной защиты о любых замеченных или предполагаемых нарушениях безопасности, а также выявленных уязвимостях в соответствии с организационно-распорядительными документами Общества в области информационной безопасности.

4.5.2 Реагирование на инциденты информационной безопасности

4.5.2.1 В целях реагирования на инциденты информационной безопасности осуществляется их регистрация и анализ, а также принятие необходимых мер по исключению их повторения.

4.5.2.2 В Обществе действует рабочая группа реагирования на инциденты информационной безопасности, в которую на основе совмещения обязанностей назначаются работники, ответственные за реагирование на инциденты информационной безопасности, имеющие соответствующую подготовку.

4.5.2.3 Реагирование на инциденты информационной безопасности осуществляется в соответствии с организационно-распорядительными

документами Общества в области информационной безопасности.

4.6 Обеспечение непрерывности бизнес-процессов

4.6.1 В целях обеспечения поддержки и восстановления бизнес-процессов осуществляются профилактические и восстановительные мероприятия по обеспечению бесперебойного функционирования информационной инфраструктуры Общества.

4.6.2 Состав мероприятий по обеспечению бесперебойного функционирования информационной инфраструктуры Общества определяется с учетом оценки рисков информационной безопасности. Правила оценки рисков информационной безопасности регламентированы в СТО Газпром 4.2-3-003. Перечень угроз информационной безопасности формируется в соответствии с СТО Газпром 4.2-0-004.

4.6.3 Мероприятия по обеспечению бесперебойного функционирования информационной инфраструктуры Общества подвергаются тестированию и регулярному пересмотру.

4.7 Порядок обеспечения информационной безопасности на этапах жизненного цикла объектов информационной инфраструктуры

4.7.1 Информационная безопасность информационной инфраструктуры Общества обеспечивается на всех стадиях жизненного цикла ее объектов с учетом ролей всех вовлеченных в этот процесс сторон (разработчиков, заказчиков, поставщиков продуктов и услуг, эксплуатирующих организаций и надзорных органов).

4.7.2 Жизненный цикл объекта информационной инфраструктуры Общества включает следующие этапы:

1) обоснование требований к объекту;
2) разработка (модернизация) объекта;
3) ввод объекта в эксплуатацию;
4) эксплуатация объекта;
5) вывод объекта из эксплуатации.

4.7.3 Служба корпоративной защиты в части сопровождения вопросов информационной безопасности участвует во всех этапах жизненного цикла объектов информационной инфраструктуры Общества.

4.7.4 Порядок разработки требований к информационной инфраструктуре Общества регламентируется СТО Газпром 4.2-3-001. В соответствии с СТО Газпром 4.2-0-001 для наиболее важных объектов информационной инфраструктуры Общества может разрабатываться программа сопровождения и обеспечения информационной безопасности в течение их жизненного цикла.

4.7.5 Порядок обеспечения информационной безопасности технической инфраструктуры Общества на всех этапах жизненного цикла ее объектов определяется их политиками информационной безопасности, а также другими

нормативными и организационно-распорядительными документами ПАО «Газпром» и Общества в области информационной безопасности.

4.8 Обеспечение информационной безопасности при эксплуатации средств обработки, хранения и передачи информации и использовании информационных ресурсов

4.8.1 Физическая защита объектов информационной инфраструктуры

4.8.1.1 В целях предотвращения несанкционированного доступа к объектам защиты информационной инфраструктуры Общества обеспечивается физическая защита мест их эксплуатации (размещения).

4.8.1.2 Технические средства обработки, хранения и передачи информации (серверы, централизованные хранилища данных, сетевое оборудование и технические средства защиты информации) размещаются в запираемых шкафах в помещениях, доступ посторонних лиц в которые ограничивается. В обязательном порядке должен вестись учет доступа в такие помещения с указанием перечня проводимых работ.

4.8.1.3 Порядок обеспечения физической защиты мест эксплуатации (размещения) объектов защиты определяется их политиками информационной безопасности.

4.8.2 Защита территорий, зданий и помещений

4.8.2.1 В целях обеспечения защиты информации и технических средств обработки, хранения и передачи информации обеспечивается защита территорий, зданий и помещений Общества.

4.8.2.2 В Обществе устанавливается пропускной и внутриобъектовый режим, препятствующий бесконтрольному посещению его охраняемых территорий и зданий. Порядок посещения и поведения в зданиях, территориях и помещениях Общества регламентируется нормативными и организационно-распорядительными документами Общества в области информационной безопасности.

4.8.2.3 Здания и помещения Общества обеспечиваются техническими средствами охраны, системами контроля доступа и пожарной безопасности.

4.8.2.4 Для защиты информации ограниченного доступа во время проведения переговоров и иных мероприятий конфиденциального характера в Обществе выделяются отдельные защищаемые помещения, в которых обеспечивается защита информации от несанкционированного прослушивания и утечки по техническим каналам. Доступ в защищаемые помещения строго контролируются.

4.8.2.5 При проведении работ на охраняемых территориях Общества, в его зданиях и защищаемых помещениях третьими лицами обеспечивается контроль их деятельности.

4.8.2.6 Порядок защиты помещений, в которых располагаются технические средства (серверы, централизованные хранилища данных, сетевое оборудование и технические средства защиты информации), определяется политиками информационной безопасности объектов защиты и другими нормативными и организационно-распорядительными документами ПАО «Газпром» и Общества в области информационной безопасности.

4.8.3 Организация безопасной эксплуатации средств обработки, хранения и передачи информации

4.8.3.1 В целях обеспечения информационной безопасности объектов информационной инфраструктуры в Обществе устанавливаются правила безопасной эксплуатации средств обработки, хранения и передачи информации.

4.8.3.2 Принимаются организационные и технические меры по обеспечению использования средств обработки, хранения и передачи информации только по целевому назначению.

4.8.3.3 Функции по администрированию и контролю эксплуатации средств обработки, хранения и передачи информации разделяются и возлагаются на работников структурных подразделений Общества, в чьи должностные обязанности входит данный функционал.

4.8.3.4 Правила эксплуатации средств обработки, хранения и передачи информации, используемые в Обществе, определяются политиками информационной безопасности объектов защиты.

4.8.4 Защита от вредоносного программного обеспечения

4.8.4.1 В целях предотвращения проникновения, обнаружения и нейтрализации вредоносного программного обеспечения в Обществе создается система защиты информационной инфраструктуры Общества от вредоносного программного обеспечения.

4.8.4.2 В Обществе используются сертифицированные на соответствие требованиям безопасности информации средства защиты от вредоносного программного обеспечения. Архитектура системы защиты от вредоносного программного обеспечения обеспечивает многоуровневую (эшелонированную) защиту.

4.8.4.3 Порядок организации защиты информационной инфраструктуры Общества от вредоносного программного обеспечения определяется политиками информационной безопасности объектов защиты, а также другими нормативными и организационно-распорядительными документами ПАО «Газпром» и Общества в области информационной безопасности.

4.8.5 Резервирование информационных ресурсов и технических средств обработки, хранения и передачи информации

4.8.5.1 Резервное копирование информационных ресурсов

В целях обеспечения возможности восстановления информационных ресурсов в случае их утраты или нарушения целостности в Обществе осуществляется их резервное копирование.

Способ и периодичность резервного копирования, сроки хранения резервных копий определяются в зависимости от назначения и особенностей системы, в которой информация обрабатывается, а также от ценности информации.

Порядок резервного копирования информационных ресурсов определяется политиками информационной безопасности объектов защиты, а также другими нормативными и организационно-распорядительными документами ПАО «Газпром» и Общества в области информационной безопасности.

4.8.5.2 Резервирование средств обработки, хранения и передачи информации

В целях обеспечения бесперебойного функционирования информационной инфраструктуры Общества осуществляется резервирование сервисов критически важных средств обработки, хранения и передачи информации.

Перечень критически важных средств обработки, хранения и передачи информации формируется в результате проведения идентификации и классификации объектов защиты, проводимых в соответствии с СТО Газпром 4.2-3-004.

Порядок резервирования средств обработки, хранения и передачи информации определяется политиками информационной безопасности объектов защиты, а также другими нормативными и организационно-распорядительными документами ПАО «Газпром» и Общества в области информационной безопасности.

4.8.6 Обеспечение сетевой безопасности

4.8.6.1 В целях обеспечения защиты информации, непрерывного и устойчивого функционирования информационной инфраструктуры в Обществе осуществляются мероприятия по обеспечению сетевой безопасности.

4.8.6.2 Обеспечение сетевой безопасности достигается защитой распределенной сети передачи данных, сетевых сервисов информационно-управляющей системы производственно-хозяйственной деятельности и сетевой инфраструктуры автоматизированной системы управления технологическими процессами. Порядок обеспечения сетевой безопасности определяется соответствующими политиками информационной безопасности, а также другими нормативными и организационно-распорядительными документами ПАО «Газпром» и Общества в области информационной безопасности.

4.8.7 Обеспечение информационной безопасности при обращении со съемными носителями информации

4.8.7.1 В целях предотвращения разглашения, утечки или утраты информации в Обществе применяются меры защиты съемных носителей информации.

4.8.7.2 В Обществе разрешается применение только зарегистрированных установленным порядком съемных носителей информации. Применение съемных носителей информации в автоматизированной системе управления технологическими процессами определяется соответствующей политикой.

4.8.7.3 Осуществляется мониторинг использования съемных носителей. Утилизация неиспользуемых носителей, содержащих конфиденциальную информацию осуществляется только с обеспечением гарантированного уничтожения содержащейся на них информации.

4.8.7.4 Порядок обеспечения информационной безопасности при обращении со съемными носителями информации определяется соответствующими политиками информационной безопасности, а также другими организационно-распорядительными документами ПАО «Газпром» и Общества в области информационной безопасности.

4.8.8 Защищенный обмен информацией

4.8.8.1 В целях предотвращения разглашения, утечки или утраты информации в Обществе применяются меры по защите информации при ее передаче различными методами.

4.8.8.2 Порядок защиты обмена информацией определяется политиками информационной безопасности объектов защиты, а также другими нормативными и организационно-распорядительными документами ПАО «Газпром» и Общества в области информационной безопасности.

4.8.9 Защита программного обеспечения

4.8.9.1 В целях поддержания работоспособности программного обеспечения в Обществе осуществляются меры по устранению уязвимостей программного обеспечения, а также другие меры защиты.

4.8.9.2 Устранение уязвимостей программного обеспечения достигается регулярным централизованным получением и установкой обновлений, предоставляемых разработчиками программного обеспечения. Новое программное обеспечение и все обновления принимаются в эксплуатацию только после успешного прохождения тестирования. Обновление программного обеспечения возлагается на работников подразделений, отвечающих за его эксплуатацию.

4.8.9.3 Порядок защиты программного обеспечения определяется политиками информационной безопасности объектов защиты, а также другими

нормативными и организационно-распорядительными документами ПАО «Газпром» и Общества в области информационной безопасности.

4.8.10 Регистрация и учет событий информационной безопасности

4.8.10.1 В целях своевременного выявления нарушений информационной безопасности в Обществе осуществляется контроль событий информационной безопасности.

4.8.10.2 В Обществе осуществляется регистрация и учет в журналах событий технических средств обработки, хранения и передачи информации событий, которые могут быть связаны с нарушениями информационной безопасности. Журналы событий регулярно анализируются Службой корпоративной защиты. Результаты регистрации и учета событий используются при проведении мероприятий по управлению инцидентами информационной безопасности.

4.8.10.3 Порядок осуществления контроля событий информационной безопасности определяется политиками информационной безопасности объектов защиты, а также другими нормативными и организационно-распорядительными документами ПАО «Газпром» и Общества в области информационной безопасности.

4.8.11 Контроль защищенности

4.8.11.1 В целях своевременного и эффективного реагирования на опубликованные и выявленные уязвимости, а также устранения недостатков в конфигурации технических средств обработки, хранения и передачи информации в информационной инфраструктуре Общества принимаются меры контроля защищенности.

4.8.11.2 Контроль защищенности осуществляется Службой корпоративной защиты. Перечень объектов контроля защищенности определяется по результатам идентификации и классификации объектов защиты.

4.8.11.3 Порядок осуществления контроля защищенности определяется политиками информационной безопасности объектов защиты, а также другими нормативными и организационно-распорядительными документами ПАО «Газпром» и Общества в области информационной безопасности.

4.8.12 Обеспечение информационной безопасности при использовании средств виртуализации операционных систем и приложений

В целях повышения уровня защищенности при использовании средств виртуализации должна обеспечиваться информационная безопасность в соответствии с нормативными и организационно-распорядительными документами ПАО «Газпром» и Общества, в том числе за счет:

1) учета средств виртуализации и развернутых с их помощью

операционных систем и сервисов;

2) управления доступом к средствам виртуализации;

3) регистрации и учета действий при работе со средствами виртуализации;

4) обеспечения целостности средств виртуализации;

5) обеспечения сетевой безопасности средств виртуализации;

6) обеспечения криптографической защиты при управлении средствами виртуализации.

4.8.13 Криптографическая защита

4.8.13.1 В целях обеспечения конфиденциальности, целостности и аутентичности обрабатываемой, хранимой и передаваемой информации в информационной инфраструктуре Общества применяются сертифицированные установленным порядком криптографические средства защиты.

4.8.13.2 Электронные документы, для которых необходимо обеспечить целостность и аутентичность защищаются с помощью цифровой подписи.

4.8.13.3 При передаче информации ограниченного доступа вне контролируемых зон, в том числе при использовании беспроводных сетей, применяются средства криптографической защиты информации.

4.8.13.4 При использовании мобильных устройств информация ограниченного доступа, хранимая на них, защищается с использованием криптографических средств.

4.8.13.5 Порядок применения средств криптографической защиты определяются политиками информационной безопасности объектов защиты, а также другими нормативными и организационно-распорядительными документами ПАО «Газпром» и Общества в области информационной безопасности.

4.9 Контроль доступа

4.9.1 Управление доступом пользователей

4.9.1.1 В целях обеспечения безопасности и устойчивого функционирования информационной инфраструктуры в Обществе осуществляется управление доступом пользователей к ее информационным ресурсам, прикладным системам и соответствующим техническим средствам объектов защиты.

4.9.1.2 Пользователи наделяются минимальными правами доступа и привилегиями, необходимыми им для выполнения служебных задач. Наделение пользователей правами доступа и привилегиями определяется процедурой предоставления прав доступа, установленной в Обществе. Целесообразно при этом использовать принцип ролевого управления доступом. Права доступа и привилегии пользователей подлежат регулярному пересмотру.

4.9.1.3 Управление учетными записями пользователей, их

принадлежностью к группам пользователей, правами и привилегиями, а также политикой парольной защиты осуществляется назначенными сотрудниками подразделений, ответственными за эксплуатацию объектов защиты и ведению каталога учётных записей.

4.9.1.4 Предоставление прав и привилегий через изменение атрибутов и членства групп учётных записей согласовывается со Службой корпоративной защиты.

4.9.1.5 Порядок управления доступом пользователей определяется политиками информационной безопасности объектов защиты, а также другими нормативными и организационно-распорядительными документами ПАО «Газпром» и Общества в области информационной безопасности.

4.9.2 Ответственность пользователей

4.9.2.1 В целях предотвращения несанкционированного доступа, а также компрометации или утраты информации определяется ответственность пользователей за соблюдение правил доступа при эксплуатации объектов защиты и технических средств обработки информации.

4.9.2.2 Пользователи несут персональную ответственность за соблюдение установленных правил при выборе и использовании паролей. Парольная политика и правила использования паролей определяется нормативными и организационно-распорядительными документами ПАО «Газпром» и Общества в области информационной безопасности.

4.9.2.3 Пользователям запрещено работать под чужими учетными записями, а также сообщать свои пароли и передавать средства аутентификации третьим лицам. При оставлении автоматизированного рабочего места пользователями предпринимаются меры по защите их от несанкционированного доступа.

4.9.2.4 Порядок использования автоматизированного рабочего места определяется политиками информационной безопасности объектов защиты, а также другими нормативными и организационно-распорядительными документами ПАО «Газпром» и Общества в области информационной безопасности.

4.9.3 Контроль доступа к операционной системе

4.9.3.1 В целях предотвращения несанкционированного доступа к объектам защиты информационной инфраструктуры Общества осуществляется контроль доступа к операционной системе.

4.9.3.2 Работа пользователей в операционной системе осуществляется под учетными записями с ограниченными правами. Доступ к операционной системе предоставляется пользователям только после прохождения процедур идентификации и аутентификации.

4.9.3.3 Управление учетными записями пользователей, их принадлежностью к группам пользователей, правами и привилегиями, а также

политикой парольной защиты осуществляется работниками подразделений, ответственных за эксплуатацию объектов защиты и согласовывается со Службой корпоративной защиты.

4.9.3.4 Меры контроля доступа к операционной системе определяются политиками информационной безопасности объектов защиты, а также другими нормативными и организационно-распорядительными документами ПАО «Газпром» и Общества в области информационной безопасности.

4.9.4 Контроль доступа к прикладным системам и информационным ресурсам

4.9.4.1 В целях предотвращения несанкционированного доступа к информации и нарушения функционирования информационной инфраструктуры в Обществе обеспечивается контроль доступа к прикладным системам и информационным ресурсам.

4.9.4.2 Доступ к прикладным системам и информационным ресурсам предоставляется пользователям после прохождения ими процедур идентификации и аутентификации, в том числе с использованием двухфакторной идентификации. При наличии технической возможности целесообразно осуществлять единую аутентификацию в прикладных системах и операционной системы.

4.9.4.3 Меры контроля доступа определяются политиками информационной безопасности объектов защиты, а также другими нормативными и организационно-распорядительными документами ПАО «Газпром» и Общества в области информационной безопасности.

4.9.5 Контроль сетевого доступа и сетевых сервисов

4.9.5.1 В целях предотвращения несанкционированного сетевого доступа и использования сетевых сервисов в информационной инфраструктуре Общества осуществляется контроль доступа к сетевым сервисам.

4.9.5.2 Доступ к сетевым сервисам предоставляется пользователям объектов защиты только ввиду служебной необходимости. Порядок разрешения и осуществления доступа пользователей к сетевым сервисам, меры контроля доступа определяются соответствующими политиками информационной безопасности, а также другими нормативными и организационно-распорядительными документами ПАО «Газпром» и Общества в области информационной безопасности.

4.9.5.3 В целях предотвращения несанкционированного доступа в информационную инфраструктуру Общества и к ее информационным ресурсам в Обществе осуществляется контроль сетевого доступа.

4.9.5.4 Контроль сетевого доступа включает:

1) контроль информационных потоков внешнего взаимодействия региональной сети передачи данных (локальной вычислительной сети);

2) контроль информационных потоков внешнего взаимодействия

автоматизированной системы управления технологическими процессами;

3) контроль внутренних информационных потоков локальной вычислительной сети;

4) контроль удаленного подключения к локальной вычислительной сети.

4.9.5.5 Меры контроля сетевого доступа определяются политиками информационной безопасности объектов защиты, а также другими нормативными и организационно-распорядительными документами ПАО «Газпром» и Общества в области информационной безопасности.

4.9.6 Контроль доступа к сетевому оборудованию

4.9.6.1 В целях обеспечения безопасности сетевой инфраструктуры Общества осуществляется управление доступом администраторов к сетевому оборудованию.

4.9.6.2 В информационной инфраструктуре Общества обеспечивается защита физического и логического доступа к диагностическим и конфигурационным портам сетевого оборудования и сетевых средств защиты. Создается выделенная сеть управления сетевым оборудованием. При осуществлении управления сетевым оборудованием и средствами защиты без использования выделенной сети управления осуществляется криптографическая защита каналов управления.

4.9.6.3 Доступ к управлению сетевым оборудованием и средствами защиты предоставляется только сотрудникам подразделений, ответственных за их эксплуатацию.

4.9.6.4 Меры контроля доступа определяются политиками информационной безопасности объектов защиты, а также другими нормативными и организационно-распорядительными документами ПАО «Газпром» и Общества в области информационной безопасности.

4.9.7 Обеспечение безопасности при удаленном доступе и использовании мобильных устройств

4.9.7.1 В целях защиты от несанкционированного доступа в информационную инфраструктуру Общества и к защищаемым информационным ресурсам, а также от ее утечки в Обществе принимаются меры по обеспечению безопасности при осуществлении удаленного доступа и использовании мобильных устройств.

4.9.7.2 При удаленном подключении пользователей к объектам защиты осуществляется контроль подключения, предусматривающий применение средств мониторинга, усиленной аутентификации и криптографической защиты информационного обмена (защищенных виртуальных сетей). Удаленное подключение к АСУ ТП запрещено.

4.9.7.3 Перед подключением к информационной инфраструктуре Общества все мобильные устройства проверяются на наличие вредоносного программного обеспечения и необходимых обновлений системного

программного обеспечения.

4.9.7.4 При использовании беспроводных подключений к объектам защиты применяются меры защиты беспроводных сетей.

4.9.7.5 Меры обеспечения безопасности при использовании мобильных устройств и осуществлении удаленного доступа определяются политиками информационной безопасности объектов защиты, а также другими нормативными и организационно-распорядительными документами ПАО «Газпром» и Общества в области информационной безопасности.

4.9.8 Обеспечение безопасности в беспроводных сетях

4.9.8.1 В целях защиты от несанкционированного доступа к информационной инфраструктуре Общества и информации в Обществе принимаются меры по обеспечению безопасности беспроводных сетей.

4.9.8.2 Целесообразность применения беспроводных сетей обосновывается проведением оценки рисков с учетом возможных угроз информационной безопасности, связанных с использованием беспроводных сетей.

4.9.8.3 Подключение устройств к беспроводной сети Общества согласовывается со Службой корпоративной защиты.

4.9.8.4 Меры обеспечения безопасности беспроводных сетей определяются политиками информационной безопасности объектов защиты, Р 4.2-2-001-2009 ПАО «Газпром», а также другими нормативными и организационно-распорядительными документами ПАО «Газпром» и Общества в области информационной безопасности.

4.10 Обеспечение соответствия требованиям по информационной безопасности

4.10.1 Обеспечение соответствия правовым требованиям

4.10.1.1 В соответствии с законодательством Российской Федерации, требованиями нормативных и организационно-распорядительных документов ПАО «Газпром» в области информационной безопасности в Обществе осуществляются меры по защите информации ограниченного доступа.

4.10.1.2 Защита информации ограниченного доступа в Обществе обеспечивается организацией:

1) режима коммерческой тайны;

2) защиты персональных данных работников Общества.

4.10.1.3 Допускается использование только официально приобретенного лицензионного программного обеспечения.

4.10.1.4 В составе объектов информационной инфраструктуры используются сертифицированные по требованиям безопасности информации или разрешенные к применению средства защиты информации.

4.10.1.5 Для защиты информации ограниченного доступа

криптографическими методами в соответствии с законодательством Российской Федерации используются сертифицированные по требованиям безопасности информации криптографические средства защиты.

4.10.2 Организация режима коммерческой тайны

4.10.2.1 В Обществе устанавливается порядок, предусматривающий правовые, организационные и технические меры по охране информации, содержащей коммерческую тайну, и иной конфиденциальной информации.

4.10.2.2 Перечень мер по защите коммерческой тайны и иной конфиденциальной информации регламентируется федеральными нормативными правовыми актами, а также нормативными и организационно-распорядительными документами ПАО «Газпром» и Общества в области информационной безопасности.

4.10.3 Организация защиты персональных данных

4.10.3.1 В Обществе устанавливается порядок защиты персональных данных работников, предусматривающий правовые, организационные и технические меры по их охране.

4.10.3.2 Перечень мер по защите персональных данных регламентируется федеральными нормативными правовыми актами, а также нормативными и организационно-распорядительными документами ПАО «Газпром» и Общества в области информационной безопасности.

4.10.4 Обеспечение соответствия организационным и техническим требованиям

4.10.4.1 В целях предотвращения нарушений информационной безопасности осуществляется контроль выполнения требований нормативных и организационно-распорядительных документов ПАО «Газпром» и Общества в области информационной безопасности.

4.10.4.2 К числу мер контроля относятся:

1) регулярный контроль руководителями структурных подразделений выполнения требований информационной безопасности;

2) регулярный контроль выполнения требований информационной безопасности сотрудниками структурных подразделений, назначенными ответственными по информационной безопасности и администраторами информационной безопасности;

3) внутренние проверки Службой корпоративной защиты соответствия существующих процедур обеспечения информационной безопасности предъявляемым требованиям;

4) анализ выявленных несоответствий и установление причин их возникновения;

5) реализация корректирующих мер и устранение выявленных несоответствий.

4.10.5 Контроль состояния информационной безопасности

4.10.5.1 В целях определения соответствия принимаемых мер безопасности внутренним документам Общества по информационной безопасности, выявления угроз информационной безопасности и принятия мер по противодействию им в Обществе осуществляется контроль состояния информационной безопасности.

4.10.5.2 Контроль состояния информационной безопасности осуществляется:

1) проведением плановых (внеплановых) внешних проверок Службой корпоративной защиты ПАО «Газпром», а также независимыми организациями и специалистами;

2) проведением внутренних плановых (внеплановых) проверок и постоянным мониторингом, осуществляемыми Службой корпоративной защиты.

4.10.5.3 Контроль состояния информационной безопасности осуществляется путем интервьюирования руководителей и работников структурных подразделений, анализа документации, осуществления инструментальных проверок.

4.10.5.4 Результаты проведения контроля состояния информационной безопасностью документируются.

4.11 Ответственность руководства и работников

4.11.1 Руководство Общества отвечает за состояние информационной безопасности в Обществе и обеспечивает реализацию Политики информационной безопасности Общества, включая регулярный контроль ее исполнения, актуализацию и выделение необходимых для обеспечения информационной безопасности ресурсов, а также организацию осведомленности и обучения работников в области обеспечения информационной безопасности.

4.11.2 Ответственность за обеспечение информационной безопасности объектов защиты Общества возлагается на работников подразделений, ответственных за их эксплуатацию.

4.11.3 Работники Общества обязаны выполнять следующие общие требования по информационной безопасности:

1) соблюдать требования настоящей Политики и других нормативных и организационно-распорядительных документов ПАО «Газпром» и Общества в области информационной безопасности;

2) использовать технические средства обработки информации только в служебных целях;

3) осуществлять информирование своего непосредственного руководителя, администратора информационной безопасности своего

структурного подразделения, руководителя отдела информационной безопасности Службы корпоративной защиты о выявленных инцидентах информационной безопасности.

4.11.4 Работникам Общества запрещается нарушать установленные правила обеспечения информационной безопасностью и скрывать факты возникновения инцидентов информационной безопасности.

4.11.5 Работники Общества, не выполняющие требования настоящей Политики информационной безопасности или требования нормативных и организационно-распорядительных документов ПАО «Газпром» и Общества в области информационной безопасности, могут быть привлечены к ответственности установленным порядком.

4.12 Порядок внесения изменений в Политику информационной безопасности

4.12.1 Анализ и выявление несоответствия действующей Политики информационной безопасности Общества текущим условиям должны проводиться с периодичностью не реже чем 1 раз в 2 года. При проведении анализа Политики информационной безопасности Общества должны учитываться результаты контроля эффективности обеспечения информационной безопасности за предыдущий период.

4.12.2 При осуществлении процедуры анализа должны учитываться:

1) результаты контроля состояния информационной безопасности и предложения структурных подразделений о совершенствовании процедур обеспечения информационной безопасности;

2) изменения в организационно-штатной структуре Общества и в его информационной инфраструктуре;

3) изменения в законодательной и нормативной базе по информационной безопасности, произошедшие с момента утверждения предыдущей Политики информационной безопасности Общества;

4) результаты анализа произошедших инцидентов информационной безопасности, а также уязвимости и угрозы, выявленные в Обществе за время, прошедшее с момента утверждения предыдущей Политики информационной безопасности Общества;

5) изменения в управлении информационной безопасности, включая изменения в распределении ресурсов и обязанностей при обеспечении информационной безопасности.

4.12.3 Результаты проведения анализа Политики информационной безопасности Общества оформляются документально.

4.12.4 В случае выявления несоответствия действующей Политики информационной безопасности Общества текущим условиям проводится процедура внесения изменений в действующую редакцию Политики информационной безопасности Общества, которая должна включать:

1) разработку предложений по совершенствованию Политики информационной безопасности Общества;

2) утверждение новой редакции Политики ИБ Общества.

Разработана:

Ведущий специалист по защите информации

Согласовано:

Заместитель генерального директора
по корпоративной защите

Начальник СКЗ

Начальник ИТЦ

Начальник ЮО

Лист регистрации изменений

Номер изменения	Дата введения в действие	Разделы, в которые внесены изменения	И.О. Фамилия, подпись лица, внесшего изменение	Дата внесения изменений

Проект приказа ООО «Газпром добыча Ноябрьск» «Об утверждении и введении в действие «Политики информационной безопасности ООО «Газпром добыча Ноябрьск» 694-02-2023 подготовлен отделом информационной безопасности Службы корпоративной защиты.

Начальник отдела

СОГЛАСОВАНО:

Главный инженер – первый заместитель
генерального директора

Заместитель генерального директора
по производству

Заместитель генерального
директора – главный геолог

Заместитель генерального директора
по перспективному развитию

Заместитель генерального директора
по экономике и финансам

Заместитель генерального директора
по управлению персоналом

Заместитель генерального директора
по общим вопросам

Заместитель генерального директора
по ремонту и капитальному строительству

Заместитель генерального директора
по корпоративной защите

Главный бухгалтер

Начальника СКЗ

Начальник ИТЦ

Начальник ОДОУ

Начальник ЮО