Приложение № 1

к приказу ООО «ТСК Мосэнерго»

от «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20 \_\_ г.

№ АУ/ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**ПОЛИТИКА**

**информационной безопасности**

**ООО «ТСК Мосэнерго»**

Москва

2023

**Содержание**

[1. Общие положения 3](#_Toc119659688)

[2. Управление информационной безопасностью 4](#_Toc119659689)

[3. Идентификация и классификация объектов защиты 5](#_Toc119659690)

[4. Организация работы с работниками Общества по вопросам информационной безопасности 6](#_Toc119659691)

[5. Управление инцидентами информационной безопасности 7](#_Toc119659692)

[6. Обеспечение непрерывности бизнес-процессов 8](#_Toc119659693)

[7. Порядок обеспечения информационной безопасности на этапах жизненного цикла объектов информационной инфраструктуры 8](#_Toc119659694)

[8. Обеспечение информационной безопасности при эксплуатации средств обработки, хранения и передачи информации и использовании информационных ресурсов 9](#_Toc119659695)

[9. Контроль доступа 12](#_Toc119659696)

[10. Обеспечение соответствия требованиям по информационной безопасности 15](#_Toc119659697)

[11. Ответственность руководства и работников 17](#_Toc119659698)

[12. Порядок пересмотра Политики информационной безопасности 17](#_Toc119659699)

## Общие положения

Настоящая Политика информационной безопасности разработана с учетом требований федерального законодательства, и требований других нормативных и организационно-распорядительных документов ООО «ТСК Мосэнерго» (далее – Общество) по вопросам обеспечения информационной безопасности.

Политика информационной безопасности Общества базируется на открытой системе стандартов и рекомендаций ПАО «Газпром», входит в систему документов в области обеспечения информационной безопасности Общества.

Положения Политики информационной безопасности уточняются (дополняются) политиками информационной безопасности объектов защиты информационной инфраструктуры, учитывающих функциональные и иные особенности этих объектов.

Политика информационной безопасности определяет позицию руководства Общества в отношении информационной безопасности, основные цели, направления и меры обеспечения информационной безопасности, которыми Общество руководствуется в своей деятельности.

В рамках Политики информационной безопасности руководство Общества заявляет, что:

* информационные технологии играют важную роль в достижении бизнес-целей Общества;
* информация является ценным активом, требующим защиты независимо   
  от форм ее представления;

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.);

* стратегической целью Общества в области информационной безопасности является обеспечение функционирования и использования информационных технологий   
  с учетом принимаемых рисков получения возможного ущерба от реализации угроз;
* стратегической задачей Общества в области информационной безопасности является построение системы управления информационной безопасностью, основанной   
  на методологии управления рисками, учитывающей бизнес-требования, а также правовые требования информационной безопасности.

Исполнение положений настоящей Политики информационной безопасности является обязательным для всех работников Общества.

* 1. **Цели Политики информационной безопасности**

Основными целями Политики информационной безопасности Общества являются:

* обеспечение единых подходов к обеспечению информационной безопасности   
  в Обществе;
* создание методологической основы для разработки внутренних документов   
  по информационной безопасности в Обществе;
* участие руководства Общества в решении проблем информационной безопасности.

Основными целями процесса обеспечения информационной безопасности   
в Обществе являются:

* создание условий для устойчивого функционирования информационной инфраструктуры;
* поддержание необходимого уровня информационной безопасности, соответствующего требованиям федерального законодательства, нормативных и организационно-распорядительных документов Общества.
  1. **Направления обеспечения информационной безопасности**

Обеспечение информационной безопасности осуществляется по следующим направлениям:

* управление информационной безопасностью;
* идентификация и классификация объектов защиты;
* организация работы с работниками Общества по вопросам информационной безопасности;
* управление инцидентами информационной безопасности;
* обеспечение непрерывности бизнес-процессов;
* обеспечение информационной безопасности при эксплуатации средств обработки, хранения и передачи информации и использовании информационных ресурсов;
* обеспечение соответствия требованиям по информационной безопасности.

Данные направления реализуются организационными и техническими мерами.

## Управление информационной безопасностью

* 1. **Внутренняя организация**

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

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.

Полномочия по обеспечению информационной безопасности Общества, в том числе по обнаружению, предупреждению и ликвидации последствий компьютерных атак, и реагированию на компьютерные инциденты возложены на заместителя генерального директора по корпоративной защите Общества.

Организация плановой, непрерывной и целенаправленной работы по осуществлению мер обеспечения информационной безопасности и контролю их выполнения возлагается   
на управление корпоративной защиты и включает в себя:

* планирование работ по информационной безопасности;
* контроль эффективности реализуемых мер обеспечения информационной безопасности и внесение рекомендаций по их совершенствованию;
* координация действий по обеспечению информационной безопасности   
  с представителями различных подразделений Общества;
* контроль выполнения и пересмотр политик информационной безопасности объектов защиты.

С учетом особенностей конкретных объектов информационной инфраструктуры Общества управлением корпоративной защиты осуществляется:

* определение полномочий работников в отношении защищаемых информационных ресурсов;
* администрирование и контроль средств и механизмов безопасности;
* контроль выполнения работниками требований в области информационной безопасности.

Функции администрирования и контроля средств и механизмов безопасности   
в Обществе распределяются между обслуживающей организацией, эксплуатирующей объекты защиты информационной инфраструктуры, управлением информационных технологий и управлением корпоративной защиты:

* администрирование встроенных механизмов безопасности средств обработки, хранения и передачи информации, а также дополнительных средств защиты осуществляется работниками обслуживающей организации, отвечающей за их эксплуатацию;
* контроль функционирования и настройки механизмов безопасности, а также соблюдения требований по информационной безопасности работниками управления информационных технологий и управления корпоративной защиты;
* организация плановой работы по созданию и поддержанию стратегии защиты объектов информационной инфраструктуры, в том числе отнесенных к критически важным, формирование и проведение единой политики в области информационной безопасности, контроль эффективности предусмотренных мер защиты информации осуществляется работниками управления корпоративной защиты.

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.

На администратора информационной безопасности (обслуживающую организацию) возлагается ответственность по предотвращению несанкционированного доступа   
к защищаемой информации.

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

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

* 1. **Обеспечение информационной безопасности при работе с внешними организациями**

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

* определение рисков, связанных с предоставлением доступа сторонней организации к конфиденциальной информации;
* формирование на основе оценки рисков перечня мероприятий по обеспечению информационной безопасности при предоставлении доступа сторонней организации   
  к конфиденциальной информации Общества и их реализация;
* заключение соглашения о конфиденциальности со сторонними организациями, которым предоставляется доступ к конфиденциальной информации.

В Обществе установлен порядок представления информации органам государственной власти, контрагентам и средствам массовой информации.

Вопросы обеспечения информационной безопасности при допуске на объекты защиты Общества иностранных представителей регламентируются соответствующими нормативными, организационно-распорядительными документами в области обеспечения внутриобъектового режима.

## Идентификация и классификация объектов защиты

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

Идентификация объектов защиты, определение степени критичности и их классификация осуществляются в соответствии с требованиями СТО Газпром 4.2-3-004 (Система обеспечения информационной безопасности ОАО «Газпром». Классификация объектов защиты). Идентифицированные и классифицированные объекты защиты отражаются в инвентаризационной документации, маркируются и для них назначаются владельцы – работники Общества, ответственные за безопасную эксплуатацию объектов защиты.

Дополнительные процедуры идентификации и классификации объектов защиты выполняются в случае внесения существенных изменений в информационную инфраструктуру.

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 Общества в области информационной безопасности.

## Организация работы с работниками Общества по вопросам информационной безопасности

* 1. **Обеспечение безопасности при заключении и во время действия трудового договора**

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.

Обязанности работников по соблюдению правил информационной безопасности определяются должностными инструкциями и конкретизируются нормативными и организационно-распорядительными документами в области информационной безопасности.

В трудовые договоры со всеми работниками вне зависимости от наличия у них доступа к информации, составляющей коммерческую тайну, включается соответствующие пункты об обязанности не разглашать и ответственности за разглашение данного вида информации, ставшей им известной в процессе трудовой деятельности.

С работниками, имеющими в силу должностных обязанностей, доступ к информации, составляющей коммерческую тайну и иной конфиденциальной информации, заключается договор (соглашение) о конфиденциальности.

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

Для работников реализуются мероприятия повышения осведомленности в области информационной безопасности.

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

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

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.

* 1. **Обеспечение безопасности при увольнении и при изменении условий трудового договора**

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

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 управлением корпоративной защиты.

В Обществе определяется порядок контроля возврата увольняемыми взятых   
во временное пользование технических средств.

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

Управление по работе с персоналом уведомляет управление корпоративной защиты об увольнении (изменении условий трудового договора) работников, а также о предстоящих увольнениях (изменениях условий трудового договора) работников.

## Управление инцидентами информационной безопасности

* 1. **Выявление инцидентов информационной безопасности**

Под инцидентом информационной безопасности понимается событие, указывающее на свершившуюся, предпринимаемую или вероятную реализацию угрозы информационной безопасности, т.е. реализацию нарушения свойств информационной безопасности информационных активов Общества.

Выявление инцидентов информационной безопасности осуществляется:

* управлением корпоративной защиты – в процессе централизованного мониторинга систем защиты информации, а также в ходе плановых (внеплановых) проверок состояния информационной безопасности структурных подразделений, обособленных структурных подразделений и филиалов Общества;
* администраторами безопасности – в процессе эксплуатации систем и подсистем безопасности аппаратно-программных средств информационной инфраструктуры Общества;
* работниками, ответственными за информационную безопасность и конфиденциальное делопроизводство – в процессе исполнения своих должностных обязанностей;
* работниками Общества ‑ при обнаружении нарушений параметров информационной безопасности в используемой в работе информации либо нарушений установленных правил информационной безопасности со стороны других лиц.
  1. **Оповещение об инцидентах информационной безопасности**

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

Работники Общества обязаны незамедлительно сообщать в управление корпоративной защиты о любых замеченных или предполагаемых нарушениях безопасности, а также выявленных уязвимостях информационных ресурсов, сетевых сервисов и персональных компьютеров.

Информация об инцидентах информационной безопасности, составляющих потенциальную опасность причинения ущерба интересам Общества, незамедлительно доводится до сведения лица ответственного за обеспечение информационной безопасности Общества, в том числе по обнаружению, предупреждению и ликвидации последствий компьютерных атак, и реагированию на компьютерные инциденты в Обществе.

* 1. **Реагирование на инциденты информационной безопасности**

Реагирование на инциденты информационной безопасности осуществляется   
в соответствии с принятым в Обществе порядком.

В управлении корпоративной защиты назначаются работники, ответственные   
за реагирование на инциденты информационной безопасности и имеющие соответствующую подготовку. Данные работники осуществляют регистрацию и анализ произошедших инцидентов, а также принимают необходимые меры по исключению   
их повторения.

## Обеспечение непрерывности бизнес-процессов

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

Состав мероприятий по обеспечению бесперебойного функционирования информационной инфраструктуры 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.

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

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

Информационная безопасность информационной инфраструктуры 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).

Жизненный цикл объекта информационной инфраструктуры Общества включает   
в себя следующие этапы:

* обоснование требований к объекту;
* разработка (модернизация) объекта;
* ввод объекта в действие;
* эксплуатация объекта;
* вывод объекта из эксплуатации.

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

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 может разрабатываться программа сопровождения и обеспечения информационной безопасности в течение   
их жизненного цикла.

Порядок обеспечения информационной безопасности информационной инфраструктуры на всех этапах жизненного цикла ее объектов определяется их политиками информационной безопасности, а также другими нормативными и организационно-распорядительными документами Общества в области информационной безопасности.

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

* 1. **Физическая защита объектов информационной инфраструктуры Общества**

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

Принимаются меры, обеспечивающие ограничение доступа посторонних лиц   
к техническим средствам обработки, хранения и передачи информации.

* 1. **Защита территорий, зданий и помещений Общества**

В целях обеспечения защиты информации и технических средств обработки, хранения и передачи информации обеспечивается защита территорий, зданий и помещений Общества. Устанавливается пропускной режим, препятствующий бесконтрольному посещению охраняемых территорий и зданий Общества.

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

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

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

Порядок защиты помещений, в которых располагаются технические средства (серверы, централизованные хранилища данных, сетевое оборудование и средства защиты информации), определяются политиками информационной безопасности объектов защиты информационной инфраструктуры, а также другими нормативными и организационно-распорядительными документами Общества в области информационной безопасности.

* 1. **Организация безопасной эксплуатации средств обработки, хранения и передачи информации**

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

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

Функции по администрированию и контролю эксплуатации средств обработки, хранения и передачи информации разделяются и возлагаются на обслуживающую организацию.

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

* 1. **Защита от вредоносного программного обеспечения**

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

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.

Защита от вредоносного ПО обеспечивается на периметре корпоративной вычислительной сети, на всех серверах и рабочих станциях.

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

* 1. **Резервирование информационных ресурсов и технических средств обработки, хранения и передачи информации**
     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.

Меры, принимаемых по резервному копированию важных информационных активов Общества, подлежат регулярному тестированию.

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

* + 1. Резервирование средств обработки, хранения и передачи информации

В целях обеспечения бесперебойного функционирования информационной инфраструктуры Общества осуществляется резервирование 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 Общества   
в области информационной безопасности.

* 1. **Обеспечение сетевой безопасности**

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

Обеспечение сетевой безопасности достигается защитой корпоративной мультисервисной сети Общества, 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 Общества в области информационной безопасности.

* 1. **Обеспечение информационной безопасности при обращении со съемными носителями информации**

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

Разрешается применение только зарегистрированных установленным порядком съемных носителей информации. Применение персональных (в том числе зарегистрированных) съемных носителей информации в автоматизированной системе управления технологическими процессами запрещено.

Осуществляется мониторинг использования съемных носителей. Утилизация неиспользуемых носителей осуществляется только с обеспечением гарантированного уничтожения содержащейся на них информации.

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

* 1. **Защищенный обмен информацией**

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

Порядок защиты обмена информацией определяется политиками информационной безопасности объектов защиты, а также другими нормативными и организационно-распорядительными документами Обществе в области информационной безопасности.

* 1. **Защита программного обеспечения**

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

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 обслуживающую организацию, отвечающую за его эксплуатацию.

Порядок защиты программного обеспечения определяется политиками информационной безопасности объектов защиты, а также другими нормативными и организационно-распорядительными документами Общества в области информационной безопасности.

* 1. **Регистрация и учет событий информационной безопасности**

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

Регистрация и учет событий осуществляется в журналах событий технических средств обработки, хранения и передачи информации, которые могут быть связаны   
с нарушениями информационной безопасности. Журналы событий регулярно анализируются администраторами безопасности информационных систем, сервисов корпоративной мультисервисной сети и работниками управления корпоративной защиты. Результаты регистрации и учета событий используются при проведении мероприятий   
по управлению инцидентами информационной безопасности.

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

* 1. **Контроль защищенности**

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.

Контроль защищенности осуществляется работниками управления корпоративной защиты. Перечень объектов контроля защищенности определяется по результатам идентификации и классификации объектов защиты.

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

* 1. **Криптографическая защита**

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

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

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

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

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

## Контроль доступа

* 1. **Управление доступом пользователей**

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

Пользователи наделяются минимальными правами доступа и привилегиями, необходимыми им для выполнения служебных задач. Наделение пользователей правами доступа и привилегиями основывается на установленной формализованной процедуре предоставления прав доступа. Целесообразно при этом использовать принцип ролевого управления доступом. Права доступа и привилегии пользователей подлежат регулярному пересмотру.

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

* 1. **Ответственность пользователей**

В целях предотвращения несанкционированного доступа, а также компрометации или утраты информации и средств обработки информации, определяется ответственность пользователей по соблюдению правил доступа при использовании автоматизированных рабочих мест.

Пользователи несут ответственность за соблюдение установленных правил   
при выборе и использовании паролей. Парольная политика и правила использования паролей определяются нормативными и организационно-распорядительными документами Общества в области информационной безопасности.

Пользователям запрещено работать под чужими учетными записями, а также сообщать свои пароли и передавать средства аутентификации другим пользователям.   
При оставлении автоматизированных рабочих мест пользователями предпринимаются меры по защите их от несанкционированного доступа.

Каждый пользователь несет ответственность за действия, совершенные   
с использованием выделенных ему реквизитов доступа и средств аутентификации.

Порядок использования автоматизированных рабочих мест определяется политиками информационной безопасности объектов защиты, а также другими нормативными и организационно-распорядительными документами Общества в области информационной безопасности.

* 1. **Контроль доступа к операционной системе**

В целях предотвращения несанкционированного доступа к объектам защиты информационной инфраструктуры Общества осуществляется контроль доступа к ОС.

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

Управление учетными записями пользователей, их принадлежностью к группам пользователей, правами и привилегиями, а также политикой парольной защиты осуществляется работниками обслуживающей организации, ответственной за эксплуатацию объектов защиты, и согласовывается с управлением корпоративной защиты.

Меры контроля доступа к ОС определяются политиками информационной безопасности объектов защиты, а также другими нормативными и организационно-распорядительными документами Общества в области информационной безопасности.

* 1. **Контроль доступа к прикладным системам и информационным ресурсам**

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

Доступ к прикладным системам и информационным ресурсам предоставляется пользователям после прохождения ими процедур идентификации и аутентификации.   
При наличии технической возможности целесообразно осуществлять единую аутентификацию в прикладных системах и ОС.

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

* 1. **Контроль доступа к сетевым сервисам**

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

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 Общества в области обеспечения информационной безопасности.

* 1. **Контроль сетевого доступа**

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

Контроль сетевого доступа включает:

* контроль информационных потоков внешнего взаимодействия корпоративной мультисервисной сети Общества;
* контроль информационных потоков внешнего взаимодействия сегментов автоматизированной системы управления технологическими процессами;
* контроль внутренних информационных потоков корпоративной мультисервисной сети Общества;
* контроль удаленного и беспроводного подключения к корпоративной мультисервисной сети Общества.

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

* 1. **Обеспечение безопасности при удаленном доступе и использовании мобильных устройств**

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

При удаленном подключении пользователей к объектам защиты осуществляется контроль удаленного подключения, включающий применение средств усиленной аутентификации и средств криптографической защиты информационного обмена (защищенных виртуальных сетей). Удаленное подключение к сетям автоматизированных систем управления технологическими процессами запрещено.

Перед подключением к информационной инфраструктуре Общества все мобильные устройства в рамках групповых политик домена проверяются на наличие вредоносного программного обеспечения и необходимых обновлений системного программного обеспечения. При несоответствии групповым политикам домена доступ не предоставляется.

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

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

* 1. **Обеспечение безопасности в беспроводных сетях**

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

* использование минимально необходимого числа точек беспроводного доступа и радиуса их действия;
* ограничение доступа к сервисам и информационным ресурсам корпоративной мультисервисной сети Общества при использовании беспроводного подключения;
* защита циркулирующей в беспроводных сетях информации с применением средств криптографической защиты информации;
* учет используемых устройств беспроводного доступа и контроль сетевых подключений.

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

Подключение пользовательских устройств к беспроводной сети согласовывается   
с управлением корпоративной защиты.

Меры обеспечения безопасности беспроводных сетей определяются политиками информационной безопасности объектов защиты, Р Газпром 4.2-2-001-2009 «Технические требования к обеспечению информационной безопасности в беспроводных сетях, развертываемых на объектах ОАО «Газпром», его дочерних обществ и организаций»,   
а также другими нормативными и организационно-распорядительными документами Общества в области информационной безопасности.

* 1. **Контроль доступа к сетевому оборудованию**

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

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.

Доступ к управлению сетевым оборудованием и средствами защиты предоставляется только работникам обслуживающей организации, ответственной за их эксплуатацию.

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

## Обеспечение соответствия требованиям по информационной безопасности

* 1. **Обеспечение соответствия правовым требованиям**

В соответствии с законодательством Российской Федерации, требованиями нормативных и организационно-распорядительных документов Общества в области информационной безопасности осуществляются меры по защите информации ограниченного доступа.

Защита информации ограниченного доступа обеспечивается организацией:

* режима коммерческой тайны;
* защиты персональных данных.

Допускается использование только официально приобретенного лицензионного программного обеспечения.

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

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

* 1. **Организация режима коммерческой тайны**

В Обществе устанавливается порядок, предусматривающий правовые, организационные и технические меры по охране информации, содержащей коммерческую тайну, и иную конфиденциальную информацию.

Перечень мер по защите коммерческой тайны и иной конфиденциальной информации регламентируется Федеральным законом от 29.07.2004 № 98-ФЗ «О коммерческой тайне» и Положением о режиме коммерческой тайны, а также нормативными и организационно-распорядительными документами Общества в области информационной безопасности.

* 1. **Организация защиты персональных данных**

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

Перечень мер по защите персональных данных регламентируется Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Политикой обработки персональных данных, а также нормативными и организационно-распорядительными документами Общества в области информационной безопасности.

* 1. **Обеспечение соответствия организационным и техническим требованиям**

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

К числу мер контроля относятся:

* регулярный контроль руководителями структурных подразделений выполнения требований информационной безопасности;
* внутренние проверки управления корпоративной защиты соответствия существующих процедур обеспечения информационной безопасности предъявляемым требованиям;
* анализ выявленных несоответствий и установление причин их возникновения;
* реализация корректирующих мер и устранение выявленных несоответствий.
  1. **Контроль состояния информационной безопасности**

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.

Контроль состояния информационной безопасности осуществляется:

* проведением плановых (внеплановых) внешних проверок управлением корпоративной защиты ПАО «МОЭК», а также независимыми организациями и специалистами;
* проведением внутренних плановых (внеплановых) проверок и постоянным мониторингом, осуществляемых управлением корпоративной защиты Общества.

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

Результаты проведения контроля состояния информационной безопасности документируются.

## Ответственность руководства и работников

Руководство Общества отвечает за состояние информационной безопасности   
в Обществе и обеспечивает реализацию Политики информационной безопасности, включая регулярный контроль ее исполнения, актуализации и выделения необходимых   
для обеспечения информационной безопасности ресурсов, а также организацию мероприятий по повышению осведомленности и обучения работников в области обеспечения информационной безопасности.

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

На руководителей структурных подразделений Общества возлагается ответственность за:

- соблюдение режима коммерческой тайны в структурном подразделении;

- соблюдение работниками структурного подразделения норм информационной безопасности, принятых в Обществе;

- соответствие полномочий работников подчиненного структурного подразделения по доступу к конфиденциальной информации, информационным активам Общества, сетевым сервисам и ресурсам их должностным обязанностям.

Работники Общества обязаны выполнять следующие общие требования   
по информационной безопасности:

* соблюдать требования настоящей Политики информационной безопасности и других нормативных и организационно-распорядительных документов Общества в области информационной безопасности;
* использовать технические средства обработки информации только в служебных целях;
* информировать управление корпоративной защиты Общества о выявленных инцидентах информационной безопасности.

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

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

## Порядок пересмотра Политики информационной безопасности

Политика информационной безопасности пересматривается с периодичностью   
не реже одного раза в 5 лет. При пересмотре Политики информационной безопасности учитываются результаты контроля эффективности обеспечения информационной безопасности за предыдущий период.

Процедура пересмотра Политики информационной безопасности включает:

* анализ и выявление несоответствий действующей Политики информационной безопасности текущим условиям;
* разработку предложений по совершенствованию Политики информационной безопасности;
* утверждение новой редакции Политики информационной безопасности.

При осуществлении процедуры пересмотра учитываются:

* результаты контроля состояния информационной безопасности и предложения структурных подразделений о совершенствовании процедур обеспечения информационной безопасности;
* изменения в организационно-штатной структуре Общества и в его информационной инфраструктуре;
* изменения в законодательной и нормативной базе по информационной безопасности, произошедшие с момента утверждения предыдущей Политики информационной безопасности;
* результаты анализа произошедших инцидентов информационной безопасности,   
  а также уязвимости и угрозы, выявленные за время, прошедшее с момента утверждения предыдущей Политики информационной безопасности;
* изменения в управлении информационной безопасностью, включая изменения   
  в распределении ресурсов и обязанностей при обеспечении информационной безопасности.