ПУБЛИЧНОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО
«МОСКОВСКАЯ ОБЪЕДИНЕННАЯ ЭНЕРГЕТИЧЕСКАЯ КОМПАНИЯ»

ПОЛИТИКА
информационной безопасности ПАО «МОЭК»

Москва, 2025 г.

Содержание

1. Общие положения

Политика информационной безопасности ПАО «МОЭК» определяет позицию руководства ПАО «МОЭК» в отношении информационной безопасности , основные направления и меры обеспечения ИБ, которыми Общество руководствуется в своей деятельности.

В рамках реализации настоящей Политики руководство Общества заявляет, что:

- информационные технологии играют важную роль в достижении бизнес-целей Общества;
- информация является ценным активом Общества, требующим защиты независимо от форм её представления;
- в своей деятельности Общество сталкивается с широким спектром угроз ИБ, 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 ИБ является обеспечение функционирования и использования информационных технологий с учетом принимаемых рисков получения возможного ущерба от реализации угроз ИБ;
- стратегической задачей в области ИБ является построение системы обеспечения информационной безопасности, основанной на методологии управления рисками, учитывающей бизнес-требования, а также правовые требования ИБ.

Политика ИБ, в том числе ИБ объектов КИИ, призвана обеспечить выполнение следующих основных принципов безопасности при эксплуатации информационных ресурсов Общества:

- использование технических и программных средств, а также информационных активов, принадлежащих Обществу, только в производственных целях;
- наделение работников минимально необходимыми правами на доступ к информационным ресурсам для выполнения ими своих должностных обязанностей;
- противодействие внутренним и внешним угрозам ИБ Общества;
- разделение информационной инфраструктуры по степени доступности к защищаемой информации на «контуры защиты»;
- формирование КСОИБ как гибкой многоуровневой системы противодействия угрозам ИБ.

Основными целями Политики ИБ Общества являются:

– обеспечение единых подходов к обеспечению ИБ в рамках Общества;
– создание методологической основы для разработки внутренних документов Общества по вопросам ИБ;
– определение форм участия руководства Общества в решении проблем ИБ.

Основными целями процесса обеспечения ИБ, в том числе в Обществе являются:

- создание условий для устойчивого функционирования информационной инфраструктуры Общества;

- поддержание необходимого уровня ИБ в Обществе, соответствующего требованиям действующего законодательства РФ, нормативных и организационно-распорядительных документов Общества.

Настоящая Политика определяет основные мероприятия и правила обеспечения ИБ Общества. Конкретная реализация положений настоящей Политики регламентируется соответствующими нормативными, организационно-распорядительными и информационно-методическими документами Общества в области ИБ.

Обеспечение ИБ, в том числе в Обществе осуществляется по следующим направлениям:

- управление ИБ;
- обеспечение ИБ при работе с внешними организациями;
- организация работы с персоналом по вопросам ИБ;
- идентификация и классификация объектов защиты;
- обеспечение непрерывности бизнес-процессов;
- обеспечение ИБ при эксплуатации средств обработки, хранения и передачи информации и использовании информационных ресурсов;
- управление инцидентами ИБ;
- обеспечение соответствия порядка эксплуатации информационной инфраструктуры требованиям ИБ.

Данные направления реализуются организационными и техническими мерами.

Соблюдение требований Политики является обязательным для всех структурных подразделений и работников Общества, а также сторонних организаций, участвующих в разработке, ремонте, обслуживании и эксплуатации информационных систем и систем управления Общества.

2. Нормативные ссылки

Настоящая Политика ИБ разработана с учётом требований действующего законодательства Российской Федерации и требований других нормативных и организационно-распорядительных документов Общества по вопросам обеспечения ИБ:

- Доктрина информационной безопасности Российской Федерации. Утверждена Указом Президента Российской Федерации от 5.12.2016 г. №646;
- Национальный стандарт Российской Федерации информационные технологии методы и средства обеспечения безопасности свод норм и правил применения мер обеспечения информационной безопасности ГОСТ Р ИСО/МЭК 27002-2021. Утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 20.05.2021 г. № 416-ст;
- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

– Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры»;

– Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;

– Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне»;

– Указ Президента Российской Федерации от 17.03.2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»;

– Приказ ФСТЭК России от 14.03.2014 № 31 «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды»;

– Приказ ФСТЭК России от 21.12.2017 № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования»;

– Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»;

Политика ИБ ПАО «МОЭК» базируется на открытой системе стандартов и рекомендаций ПАО «Газпром» «Система обеспечения информационной безопасности ПАО «Газпром», рекомендованных к использованию в компаниях группы Газпром».

3. Термины, определения и сокращения

В настоящей Политике использованы термины в соответствии с СТО Газпром 4.2-1-001 и следующие сокращения:

Пользователь – работник структурного подразделения Общества, имеющий в установленном порядке доступ к информационным ресурсам КАСУ в объеме, необходимом для надлежащего выполнения должностных обязанностей.

АРМ - автоматизированное рабочее место.

АСУТП - автоматизированная система управления технологическими процессами.

ИБ - информационная безопасность.

ОИБ УКЗ - отдел информационной безопасности Управления корпоративной защиты ПАО «МОЭК».

УКЗ - Управление корпоративной защиты ПАО «МОЭК».

КМС - корпоративная Мультисервисная сеть ПАО «МОЭК».

КТ - коммерческая тайна.

КАСУ - корпоративная автоматизированная система управления.

КИИ - критическая информационная инфраструктура.
ЛВС - локальная вычислительная сеть.
ОС - операционная система.
ПО - программное обеспечение.
РСПД - региональная сеть передачи данных.
КСОИБ - комплексная система обеспечения информационной безопасности.
ЭП - электронная подпись.
КИС **-** корпоративная информационная система.

4. Управление информационной безопасностью

Общее руководство обеспечением ИБ Общества осуществляет генеральный директор.

Координацию деятельности по реализации комплекса мер, предусмотренных настоящей Политикой и другими нормативными документами Общества в области ИБ, осуществляет директор по безопасности и режиму – заместитель управляющего директора Общества.

4.1. Принципы управления информационной безопасностью.

Обеспечение информационной безопасности объектов информатизации предполагает реализацию ряда управленческих задач.

В качестве основных из них следует выделить:

- администрирование встроенных механизмов использующегося системного и прикладного программного обеспечения;
- администрирование применяемых дополнительных средств защиты информации;
- установление полномочий работников в отношении защищаемых информационных ресурсов;
- контроль выполнения работниками требований в области информационной безопасности.

Каждая из задач решается с учетом особенностей обработки и передачи информации в конкретных автоматизированных системах и вычислительных сетях, что отражается в соответствующей политике информационной безопасности.

Работы по обеспечению информационной безопасности в автоматизированных системах и вычислительных сетях, эксплуатируемых в Обществе, непосредственно осуществляют:

– УКЗ ;
– ОИБ УКЗ ;
– администраторы информационной безопасности Общества;
– администраторы автоматизированных систем, информационных и коммуникационных систем, серверного оборудования, отдельных программных комплексов, а также вычислительных сетей, эксплуатируемых в Обществе;

– работники, ответственные за информационную безопасность в структурных подразделениях Общества.

4.2. Внутренняя организация.

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

В Обществе создается система обеспечения ИБ, предусматривающая организационную структуру управления ИБ, систему нормативных документов по обеспечению ИБ и техническую составляющую указанной системы.

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

4.3. УКЗ .

УКЗ обеспечивает выполнение требований, предъявляемых к информационной безопасности при эксплуатации в Обществе объектов информационной инфраструктуры.

На УКЗ Общества возлагается:

- обеспечение разработки и реализации в Обществе стратегии защиты объектов информационной инфраструктуры, в том числе отнесенных к критически важным;

- формирование и проведение единой научно-технической политики в области информационной безопасности;

- методическое руководство системой обеспечения информационной безопасности Общества, контроль эффективности предусмотренных мер защиты информации.

4.4. ОИБ УКЗ .

ОИБ УКЗ обеспечивает информационную безопасность при эксплуатации автоматизированных систем и вычислительных сетей.

Основной задачей ОИБ УКЗ является организация непрерывной, плановой и целенаправленной работы по осуществлению и контролю выполнения принимаемых в Обществе мер по обеспечению информационной безопасности.

Организация плановой работы по созданию и поддержанию системы обеспечения ИБ в Обществе.

На ОИБ УКЗ возложены следующие функции:

- планирование работ по ИБ;

- контроль эффективности реализуемых мер обеспечения ИБ и внесение рекомендаций по их совершенствованию;

- формирование предложений по совершенствованию системы обеспечения ИБ Общества;

- координация действий по обеспечению ИБ с представителями структурных подразделений Аппарата управления и филиалов (далее - структурные подразделения) Общества;

- контроль выполнения и своевременного пересмотра нормативных документов Общества в области ИБ.

4.5. Администратор информационной безопасности Общества.

Администрирование ИБ обеспечивает выполнение установленных правил разграничение доступа к элементам информационной инфраструктуры, порядка обращения с защищаемой информацией при ее обработке, хранении и передаче, которое достигается:

- обеспечением заданных настроек систем защиты информации, подсистем управления разграничением доступом, регистрации и учета автоматизированных систем и вычислительных сетей;

- контролем целостности программно-аппаратной среды, хранимой, обрабатываемой и передаваемой информации;

- контролем автоматизированных систем, вычислительных сетей и автономных ПК (ведением и своевременным анализом журнала учета событий, регистрируемых средствами защиты, операционными системами и т.д.), с целью выявления возможных нарушений установленных требований по обеспечению информационной безопасности.

Администратором ИБ назначается, как правило, работник структурного подразделения, эксплуатирующего защищаемые элементы информационной инфраструктуры.

На администратора ИБ возлагается ответственность по предотвращению несанкционированного доступа к защищаемой информации.

4.6. Администрирование информационной безопасности Общества.

С учётом особенностей конкретных объектов информационной инфраструктуры в Обществе осуществляется:

- определение полномочий работников в отношении защищаемых информационных ресурсов;

- администрирование и контроль средств и механизмов безопасности;

- контроль выполнения работниками требований в области ИБ.

Функции администрирования и контроля средств и механизмов безопасности в Обществе распределяются между подразделениями, эксплуатирующими объекты защиты информационной инфраструктуры, и ОИБ УКЗ:

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

- контроль функционирования и настройки механизмов безопасности, а также соблюдения требований по ИБ осуществляется работниками ОИБ УКЗ.

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

4.7. Администратор автоматизированной системы (вычислительной сети), эксплуатируемой в Обществе.

Администратором автоматизированной системы (информационной системы, серверного оборудования), а также вычислительной сети назначается работник структурного подразделения Общества, ответственный за обеспечение ее работоспособности.

Основными задачами администратора являются:

- непосредственное управление автоматизированной системой (элементами системы) или вычислительной сетью;
- поддержание заданных настроек систем защиты информации, подсистем управления доступом, регистрации и учета автоматизированной системы (элемента системы) или вычислительной сети;
- обеспечение доступа работников к ресурсам автоматизированной системы (элемента системы) или вычислительной сети;
- контроль целостности автоматизированной системы (элемента системы) или вычислительной сети;
- обеспечение безотказной работы и восстановление работоспособности автоматизированной системы (элемента системы) или вычислительной сети при возникновении нештатной ситуации.

4.8. Работники, ответственные за информационную безопасность в структурных подразделениях Общества.

В структурных подразделениях Аппарата управления и филиалах руководители подразделений отвечают или назначают работников, ответственных за обеспечение ИБ, перечень обязанностей которых разрабатывается с учётом специфики работы структурного подразделения.

Работник, ответственный за информационную безопасность, обеспечивает:

- контроль защищаемых информационных ресурсов, находящихся в ведении (управлении) подразделения;
- введение заявок в СЦУД и Service Desk на подключение новых работников подразделения к информационным ресурсам и к сети Интернет (другим сетям общего пользования);
- при необходимости, доведение до работников под подпись, по поручению руководителя структурного подразделения, нормативных и организационно-распорядительных документов, регламентирующих работу с защищаемыми информационными ресурсами и другие аспекты обеспечения ИБ Общества;

- контроль использования работниками подразделения паролей на доступ к ПК и ресурсам вычислительной сети, порядка их смены, хранения и использования;

- участие в проведении проверок и расследований, связанных с нарушением работниками установленных правил обеспечения информационной безопасности.

Вышеуказанные обязанности работника, ответственного за информационную безопасность в структурном подразделении, вносятся в его должностную инструкцию, с которой он должен быть ознакомлен под роспись.

4.9. Предотвращение утечки защищаемой информации по техническим каналам.

Основными задачами при обеспечении защиты информации от утечки по техническим каналам являются:

- выявление и пресечение возможных каналов утечки информации;
- организация противодействия утечке информации.

Противодействие утечке защищаемой информации по техническим каналам представляет собой систему мер, направленную на ее выявление и предотвращение. Противодействие планируется и носит непрерывный характер.

Применяются следующие организационно-технические меры противодействия утечке защищаемой информации по техническим каналам:

- проведение категорирования служебных помещений ПАО «МОЭК» и филиалов;
- регламентирование порядка проведения деловых встреч и переговоров, ведения телефонных разговоров;
- регламентирование порядка проведения обследований защищаемых помещений и технических средств на предмет установления каналов утечки;
- обеспечение режима доступа в служебные помещения;
- разработка требований по размещению пожарной и охранной сигнализации;
- звукоизоляция ограждающих конструкций защищаемых помещений для исключения прослушивания переговоров за их пределами;
- исключение возможности установки посторонних (внештатных) предметов на внешней стороне ограждающих конструкций защищаемых помещений и выходящих из них коммуникаций (систем отопления, вентиляции, кондиционирования);
- проведение специальных обследований защищаемых помещений и технических средств;
- проведение специальных обследований строящихся и ремонтируемых зданий и помещений;
- приобретение специальных технических средств обнаружения каналов утечки и их закрытия, организация учета и контроля их использования;

- оборудование категорированных помещений специальными средствами защиты от утечки информации;

- использование сертифицированных серийно выпускаемых в защищенном исполнении технических средств обработки, передачи и хранения информации;

- использование технических средств, удовлетворяющих требованиям стандартов по электромагнитной совместимости;

- размещение объектов защиты на максимально возможном расстоянии от границы контролируемой зоны;

- использование защищенных каналов связи;

- оборудование служебных помещений средствами разграничения доступа.

5. Обеспечение информационной безопасности при работе с внешними организациями

При необходимости предоставления доступа сторонним организациям к защищаемым информационным ресурсам в Обществе осуществляются мероприятия по обеспечению ИБ:

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

- формирование на основе оценки рисков перечня мероприятий по обеспечению ИБ при предоставлении доступа сторонней организации к конфиденциальной информации Общества и их реализация;

- заключение соглашения о конфиденциальности со сторонними организациями.

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

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

6. Организация работы с персоналом по вопросам информационной безопасности

6.1. Обеспечение информационной безопасности при заключении и во время действия трудового договора.

В целях повышения уровня обеспечения информационной безопасности при приёме на работу новых работников, руководитель подразделения доводит до них установленные в Обществе правила обеспечения ИБ и ответственность за их нарушение.

Обязанности работников по неразглашению конфиденциальной информации ограниченного доступа и соблюдению правил ИБ указываются в трудовом договоре работника с Обществом.

Обязанности работников Общества по обеспечению ИБ определяются нормативными и организационно-распорядительными документами Общества в области ИБ и конкретизируются должностными инструкциями.

С работниками, имеющими, в силу должностных обязанностей, доступ к информации ограниченного доступа, Общество заключает договор (соглашение) о конфиденциальности.

В Обществе обеспечивается сохранность заключенных договоров (соглашений) о конфиденциальности.

Работники Общества, при вступлении в должность, проходят первичный инструктаж, предусматривающий ознакомление с основными правилами и мерами ИБ. Порядок проведения первичного инструктажа устанавливается в соответствии с организационно-распорядительными документами Общества.

Для работников Общества реализуются мероприятия повышения осведомленности в области ИБ.

Работники, отвечающие за обеспечение ИБ, регулярно проходят повышение квалификации, знакомятся с изменениями в действующем законодательстве РФ, нормативных и организационно-распорядительных документах Общества в области ИБ.

Работники, допустившие разглашение, утрату, искажение подлежащей защите информации или нарушившие установленные в Обществе правила ИБ, несут ответственность в соответствии с действующим законодательством Российской Федерации.

6.2. Обеспечение безопасности при увольнении и при изменении условий трудового договора.

В целях обеспечения ИБ при увольнении и при 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.

Напоминание увольняемым работникам о принятых ими обязательствах по соблюдению тайны конфиденциальных сведений и доведение до них срока её сохранения возложено на работников УКЗ.

В Обществе определен порядок контроля возврата увольняемыми работниками, взятых во временное пользование технических средств.

При увольнении работника (изменении условий трудового договора) его права доступа к информационным ресурсам аннулируются (блокируются) со дня подписания соответствующего приказа.

Управление администрирования и развития кадрового потенциала своевременно проводит мероприятия в программных модулях КИС Общества об увольнениях и перемещениях работников Общества, а также о предстоящих увольнениях (изменениях условий трудового договора). Проведенные мероприятия об увольнениях и перемещениях работников Общества в программных модулях КИС Общества являются автоматическим

уведомлением ОИБ УКЗ об произошедших изменениях по работникам, допущенным к работе со сведениями, составляющими коммерческую тайну, и иной конфиденциальной информацией Общества.[1]

7. Идентификация и классификация объектов защиты

В целях обеспечения ИБ 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 с учётом требований СТО Газпром 4.2-3-004. Идентифицированные и классифицированные объекты защиты отражаются в инвентаризационной документации, маркируются и назначаются работники Общества, ответственные за их безопасную эксплуатацию.

Дополнительные процедуры идентификации и классификации объектов защиты выполняются в случае изменения состава объекта защиты, порядка его эксплуатации, либо внесения существенных изменений в информационную инфраструктуру Общества.

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 частными политиками ИБ, а также другими нормативными и организационно-распорядительными документами Общества в области ИБ.

8. Управление инцидентами информационной безопасности

8.1. Выявление инцидентов информационной безопасности.

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

Выявление инцидентов ИБ осуществляется:

- ОИБ - в процессе централизованного мониторинга систем защиты информации Общества, а также в ходе плановых (внеплановых) проверок состояния ИБ структурных подразделений 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 структурных подразделениях Общества - в процессе исполнения своих должностных обязанностей;

---

[1] В случае отсутствия возможности проведения мероприятий в программных модулях КИС Общества, Управление администрирования и развития кадрового потенциала своевременно информирует доступным способом ОИБ УКЗ об произошедших изменениях по работникам.

- работниками Общества - при обнаружении нарушений параметров ИБ в используемой в работе информации либо нарушений установленных правил ИБ со стороны других лиц.

8.2. Оповещение об инцидентах информационной безопасности.

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

Работники Общества обязаны сообщать в ОИБ УКЗ о любых замеченных фактических или предполагаемых нарушениях безопасности, а также выявленных уязвимостях информационных ресурсов, сетевых сервисов и персональных компьютеров.

Информация об инцидентах ИБ, составляющих потенциальную опасность причинения ущерба интересам Общества, незамедлительно доводится до сведения директора по безопасности и режиму – заместителя управляющего директора.

8.3. Реагирование на инциденты информационной безопасности.

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

Реагирование на инциденты ИБ осуществляется ОИБ УКЗ в соответствии с принятым в Обществе порядком.

9. Обеспечение непрерывности бизнес-процессов

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

Мероприятия по обеспечению бесперебойного функционирования информационной инфраструктуры Общества проводятся с учётом оценки рисков ИБ. Правила оценки рисков ИБ и перечень угроз ИБ регламентируются СТО Газпром 4.2-3-003 и СТО Газпром 4.2-0-004.

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

10. Порядок обеспечения информационной безопасности на этапах жизненного цикла объектов информационной инфраструктуры

ИБ информационной инфраструктуры Общества обеспечивается на всех стадиях жизненного цикла её объектов с участием 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:

- формирование требований к объекту;
- разработка (актуализация) методологии;

- разработка (модернизация) объекта;
- ввод объекта в действие;
- эксплуатация объекта;
- вывод объекта из эксплуатации.

ОИБ УКЗ в части сопровождения вопросов ИБ 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 Общества может разрабатываться программа сопровождения и обеспечения ИБ в течение их жизненного цикла.

При выводе объекта информационной инфраструктуры из эксплуатации, в случае необходимости, предусматривается перенос хранимой объектом информации с учетом возможного изменения формата хранения.

Информация с выводимых из эксплуатации накопителей удаляется способом, исключающим её последующее восстановление.

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

11.1. Физическая защита объектов информационной инфраструктуры.

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.

11.2. Защита территорий, зданий и помещений.

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

В Обществе устанавливается пропускной режим, препятствующий бесконтрольному посещению его охраняемых территорий и зданий.

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 частными политиками ИБ и регламентами эксплуатации объектов защиты информационной инфраструктуры.

Порядок допуска на территории, объекты и в помещения, подконтрольные Обществу, а также правила поведения на объектах регламентируются положениями о внутриобъектовом режиме.

11.3. Обеспечение ИБ при эксплуатации средств обработки, хранения и передачи информации.

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

Принимаются меры, обеспечивающие использование средств обработки, хранения и передачи информации только по целевому назначению.

Функции администрирования и контроля эксплуатации средств обработки, хранения и передачи информации разделяются и возлагаются на специально выделенных работников.

Правила эксплуатации средств обработки, хранения и передачи информации, используемых в Обществе, определяются частными политиками ИБ и регламентами эксплуатации объектов защиты.

11.3.1. Защита от вредоносного программного обеспечения.

В целях предотвращения проникновения, обнаружения и нейтрализации вредоносного ПО в Обществе создана централизованная система защиты информационной инфраструктуры Общества от вредоносного ПО.

В Обществе используются сертифицированные на соответствие требованиям безопасности информации средства защиты от вредоносного ПО.

Архитектура системы защиты от вредоносного ПО обеспечивает многоуровневую защиту.

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

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

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

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.

11.3.3. Обеспечение сетевой безопасности.

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

Обеспечение сетевой безопасности достигается защитой оборудования вычислительной сети и сетевых сервисов КМС, а также сетевой инфраструктуры КАСУ от неправомочных действий пользователей и посторонних лиц.

В рамках обеспечения сетевой безопасности принимаются меры по выявлению и фиксированию фактов несанкционированной активности, блокирование неправомочных действий и минимизация их возможных последствий.

11.3.4. Обеспечение информационной безопасности при обращении со съемными носителями информации.

В Обществе применение съёмных носителей информации на АРМ ограничено и допускается только для выполнения своих непосредственных функциональных обязанностей и по согласованию в установленном порядке с ОИБ УКЗ.

В целях предотвращения разглашения, утечки или утраты информации в Обществе применяются меры защиты съёмных носителей информации, осуществляется мониторинг использования съёмных носителей. Информация, хранящаяся на съемных носителях информации, подлежит обязательной проверке на отсутствие вредоносного ПО.

Подключать носители неизвестного происхождения, а также личные съёмных носителей информации в КАСУ запрещено.

Съёмные носители для работы с информацией ограниченного доступа учитываются в соответствии с правилами Положения об обработке персональных данных в Обществе и Положения о сохранении информации, составляющей коммерческую тайну Общества.

Утилизация неиспользуемых носителей осуществляется только с обеспечением гарантированного уничтожения содержащейся на них информации.

11.3.5. Защищённый обмен информацией.

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

В случае физического подключения АРМ к КМС обязательная защита распространяется на информационный обмен, содержащий сведения ограниченного доступа и иную критически важную информацию.

В случае удалённого или беспроводного доступа к ресурсам КМС, защите подлежит весь информационный обмен с подключаемым рабочим местом.

11.3.6. Обеспечение безопасности при обработке, обмене служебной информацией.

В целях защиты от несанкционированного доступа к сведениям о производственной деятельности, работникам Общества запрещен обмен служебной информацией с использованием личных и корпоративных устройств посредством мессенджеров зарубежной разработки (WhatsApp, Telegram, Viber, WeChat, Discord, Snapchat, Skype, Microsoft Teams, Threema), а также недопустима передача указанной информации на бесплатные почтовые серверы сети Интернет (mail.ru, yandex.ru, gmail.com и пр.).

Для проведения рабочих встреч, переговоров, совещаний, конференций и информационного обмена необходимо использовать исключительно применяемые в ГК Газпром телекоммуникационные технические решения.

11.3.7. Защита программного обеспечения.

В целях поддержания работоспособности ПО в Обществе осуществляются меры по выявлению и устранению уязвимостей используемого ПО, а также другие меры защиты.

Устранение уязвимостей ПО достигается регулярным централизованным получением и установкой обновлений, предоставляемых разработчиками ПО. Новое ПО и все обновления принимаются в эксплуатацию только после успешного прохождения тестирования. Задачи по своевременному обновлению ПО возлагается на работников подразделений, отвечающих за его эксплуатацию.

Контроль за работами по защите ПО возлагается на ОИБ УКЗ.

11.3.8. Регистрация и учет событий информационной безопасности.

В целях своевременного выявления нарушений ИБ в Обществе осуществляется контроль событий ИБ.

В Обществе осуществляется регистрация и учет в журналах событий технических средств обработки, хранения и передачи информации событий,

которые могут быть связаны с нарушениями ИБ. Журналы событий регулярно анализируются администраторами безопасности информационных систем, сервисов КМС и работниками ОИБ УКЗ. Результаты регистрации и учёта событий используются при проведении мероприятий по управлению инцидентами ИБ.

11.3.9. 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 защищённости осуществляется работниками ОИБ УКЗ с использованием специализированных аппаратно-программных средств.

Перечень объектов контроля защищённости, а также методы и способы контроля определяются по результатам идентификации и классификации объектов защиты.

11.3.10. 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 ЭП.

При передаче информации, содержащей сведения 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.

12. Контроль доступа

12.1. Управление доступом пользователей.

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

Необходимые права доступа и привилегии в отношении информационной инфраструктуры Общества для каждого работника (пользователя) определяются на основании его должностных обязанностей.

Пользователи наделяются минимальными правами доступа и привилегиями, необходимыми им для выполнения служебных задач.

Наделение пользователей правами доступа и привилегиями основывается на определённой для конкретного ресурса системе полномочий (прав, ролей и пр.) и осуществляется в соответствии с установленной в Обществе формализованной процедурой предоставления прав доступа. Права доступа и привилегии пользователей подлежат регулярному пересмотру и подтверждению.

Все реквизиты доступа к элементам информационной инфраструктуры Общества имеют однозначную персонификацию.

12.2. Ответственность пользователей.

В целях предотвращения несанкционированного доступа, а также компрометации или утраты информации и средств обработки информации, определяется ответственность пользователей за соблюдение правил доступа при использовании АРМ.

Пользователи несут ответственность за соблюдение установленных правил при выборе и использовании паролей, а также за сохранность аппаратных средств усиленной аутентификации.

Пользователям запрещено работать под чужими учётными записями, а также сообщать свои пароли и передавать аппаратные средства аутентификации другим лицам. При оставлении АРМ пользователями в обязательном порядке должны предприниматься меры по защите их от несанкционированного доступа.

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

12.3. Контроль доступа к операционной системе.

В целях предотвращения несанкционированного доступа к объектам защиты информационной инфраструктуры Общества осуществляется контроль доступа к ОС АРМ работников, серверов и других аппаратных средств КАСУ Общества.

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

Управление учётными записями пользователей домена, их принадлежностью к группам пользователей, правами и привилегиями, а также политикой парольной защиты осуществляется службой системных администраторов централизовано и контролируется ОИБ.

12.4. Контроль доступа к прикладным системам и информационным ресурсам.

В целях предотвращения несанкционированного доступа к информации и нарушения функционирования КАСУ 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.

Доступ к прикладным системам и информационным ресурсам определяются соответствующими политиками, а также другими нормативными и организационно-распорядительными документами Общества.

Для защиты информационных систем, содержащих сведения ограниченного доступа, применяются усиленные методы аутентификации.

12.5. Контроль доступа к сетевым сервисам.

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

Доступ к сетевым сервисам предоставляется пользователям только в случае служебной необходимости. Порядок разрешения и осуществления доступа пользователей к сетевым сервисам, меры контроля доступа определяются соответствующими политиками ИБ, а также другими нормативными и организационно-распорядительными документами Общества в области обеспечения ИБ.

12.6. Контроль сетевого доступа.

В целях предотвращения несанкционированного доступа в информационную инфраструктуру Общества и к её информационным ресурсам в Обществе осуществляется контроль сетевого доступа, который включает в себя:

- контроль информационных потоков внешнего взаимодействия КМС;
- контроль информационных потоков внешнего взаимодействия сегментов АСУ ТП;
- контроль внутренних информационных потоков КМС;
- контроль удаленного и беспроводного подключения к КМС.

12.7. Обеспечение безопасности при использовании сетей общего пользования.

При использовании сетей общего пользования (Internet и т.п.) применяются следующие первоочередные меры для защиты информации:

- организация взаимодействия с сетью общего пользования через единый шлюз ПАО «МОЭК»;
- обеспечение блокировки внешнего доступа к внутренним ресурсам рабочих мест и узлов, с которых осуществляется взаимодействие с сетью общего пользования;
- предпочтительное использование сертифицированных средств криптографической защиты информации;

- использование ресурсов сетей общего пользования доступа работниками ПАО «МОЭК» в строгом соответствии с производственной необходимостью.

Для ЛВС АСУТП, эксплуатируемых в филиалах Общества, КМС ПАО «МОЭК» рассматривается как сеть общего пользования и взаимодействие с ней осуществляется через выделенный шлюз в составе ЛВС АСУТП с функциями сетевого экрана.

12.8. Обеспечение безопасности при удалённом 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 в Обществе принимаются меры по обеспечению безопасности при осуществлении удалённого доступа и использовании мобильных устройств.

При удалённом подключении пользователей к объектам защиты осуществляется контроль удалённого подключения, включающий применение средств усиленной аутентификации и средств криптографической защиты информационного обмена (защищённых виртуальных сетей). Удалённое подключение к сетям АСУ ТП запрещено.

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

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

12.9. Обеспечение безопасности в беспроводных сетях.

В целях защиты от несанкционированного доступа к информационной инфраструктуре Общества 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 КМС при использовании беспроводного подключения;
- защита циркулирующей в беспроводных сетях информации с применением УКЗИ;
- учёт используемых устройств беспроводного доступа и контроль сетевых подключений.

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

Подключение пользовательских устройств к беспроводной сети Общества согласовывается с ОИБ УКЗ.

Меры обеспечения безопасности беспроводных сетей определяются частными политиками ИБ объектов защиты, рекомендациями Р Газпром 4.2-2-001-2009, а также другими нормативными и организационно-распорядительными документами Общества в области ИБ.

12.10. Контроль доступа к сетевому оборудованию.

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

В информационной инфраструктуре Общества обеспечивается защита физического и логического доступа к диагностическим и конфигурационным портам сетевого оборудования и сетевых средств защиты. Логический доступ к сетевому оборудованию предоставляется в пределах выделенной сети управления. 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 подразделений, ответственных за их эксплуатацию.

13. Обеспечение соответствия требованиям по информационной безопасности

13.1. Обеспечение соответствия правовым требованиям.

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

Защита информации ограниченного доступа в Обществе обеспечивается организацией:

- режима коммерческой тайны;
- защиты персональных данных действующих и бывших работников Общества, а также кандидатов на замещение вакантных должностей (далее - персональные данные).

При использовании ПО должны соблюдаться права Лицензиаров (Разработчиков) на данные объекты интеллектуальной собственности.

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 действующим законодательством Российской Федерации, используются сертифицированные по требованиям безопасности информации криптографические средства защиты.

13.2. Организация режима коммерческой тайны.

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

Защита коммерческой тайны организуется в соответствии с Федеральным законом от 29.07.2004 № 98-ФЗ «О коммерческой тайне». Перечень мер по защите КТ и иной конфиденциальной информации регламентируется Положением о сохранении информации, составляющей коммерческую тайну и иной конфиденциальной информации ПАО «МОЭК», а также иными нормативными и организационно-распорядительными документами Общества в области ИБ.

13.3. 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 в ПАО «МОЭК», а также иными нормативными и организационно-распорядительными документами Общества в области ИБ.

13.4. Обеспечение соответствия организационным и техническим требованиям.

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

К мерам контроля относятся:

- регулярный контроль руководителями структурных подразделений выполнения требований ИБ;
- внутренние проверки ОИБ УКЗ соответствия существующих процедур обеспечения ИБ предъявляемым требованиям;
- анализ выявленных несоответствий и установление причин их возникновения;
- реализация корректирующих мер и устранение выявленных несоответствий.

13.5. Контроль состояния информационной безопасности.

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

Контроль состояния ИБ осуществляется:

- проведением плановых (внеплановых) внешних проверок Департаментом корпоративной защиты ПАО «Газпром», а также сторонними организациями и специалистами на договорной основе;

- проведением внутренних плановых (внеплановых) проверок и постоянным мониторингом, осуществляемых ОИБ.

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

Результаты проведения контроля состояния ИБ документируются.

14. Обеспечения безопасности объектов КИИ

14.1. Цели и задачи обеспечения безопасности объектов КИИ

Целью обеспечения безопасности объектов КИИ Общества является обеспечение их устойчивого функционирования в штатных режимах работы в условиях реализации в отношении объектов КИИ угроз безопасности информации (в том числе компьютерных атак).

Задачами обеспечения безопасности объектов КИИ являются:

– предотвращение неправомерного доступа к информации, уничтожения информации, ее модифицирования, блокирования, копирования, предоставления и распространения, а также иных неправомерных действий в отношении информации;

– недопущение физического или информационного воздействия на программные и программно-аппаратные средства, в результате которого может быть нарушено и (или) прекращено функционирование объекта КИИ;

– обеспечение возможности восстановления функционирования объекта КИИ.

14.2. Организация обеспечения безопасности объектов КИИ

Общество, как субъект критической информационной инфраструктуры создает систему безопасности, организует и контролирует ее функционирование в соответствии с приказом ФСТЭК России от 21.12.2017 № 235.

Система безопасности создается в отношении всех значимых объектов КИИ Общества в соответствии с приказом ФСТЭК России от 25.12.2017 № 239 в рамках функционирования систем безопасности в ходе создания (модернизации, дооснащения) подсистем безопасности значимых объектов КИИ.

Система безопасности включает в себя силы обеспечения безопасности, используемые ими средства обеспечения безопасности и организационно – распорядительную документацию.

14.3. Силы обеспечения безопасности объектов КИИ

К силам обеспечения безопасности относятся:

- подразделения (работники) субъекта критической информационной инфраструктуры, ответственные за обеспечение безопасности значимых объектов критической информационной инфраструктуры;

- подразделения (работники), эксплуатирующие значимые объекты критической информационной инфраструктуры;
- подразделения (работники), обеспечивающие функционирование (сопровождение, обслуживание, ремонт) значимых объектов критической информационной инфраструктуры.

Координацию и контроль деятельности работников по вопросам обеспечения безопасности объектов КИИ Общества осуществляет УКЗ (штатный специалист ответственный за обеспечение безопасности КИИ).

14.4. Средства обеспечения безопасности объектов КИИ

К средствам обеспечения безопасности значимых объектов критической информационной инфраструктуры относятся программные и программно-аппаратные средства, применяемые для обеспечения безопасности значимых объектов критической информационной инфраструктуры.

Для обеспечения безопасности объектов критической КИИ применяются сертифицированные на соответствие требованиям по безопасности средства защиты информации или средства, прошедшие оценку соответствия в форме испытаний при приемке в эксплуатацию.

Параметры, характеристики и функции применяемых средств защиты информации должны обеспечивать реализацию технических мер по обеспечению безопасности объектов КИИ, на которых они применяются.
Применяемые средства защиты информации должны быть обеспечены технической поддержкой со стороны разработчиков (производителей).

Средства защиты информации применяются в соответствии с инструкциями (правилами) по эксплуатации от разработчиков (производителей) этих средств, и иной эксплуатационной документацией на средства защиты информации.

Оценка соответствия встроенных в общесистемное и прикладное программное обеспечение средств защиты информации функциям безопасности проводится на этапе испытаний (приемки в эксплуатацию) самостоятельно или с привлечением организаций-лицензиатов в области защиты информации.

15. Ответственность руководства и работников

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

Ответственность за обеспечение ИБ объектов защиты информационной инфраструктуры 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 ИБ, принятых в Обществе;

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

Работники Общества обязаны:

- соблюдать требования настоящей Политики ИБ и других нормативных и организационно-распорядительных документов Общества в области ИБ;

- использовать технические средства хранения, обработки и передачи информации только в служебных целях;

- осуществлять информирование ОИБ УКЗ о выявленных инцидентах ИБ.

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

Работники Общества, не выполняющие требования настоящей Политики или требования нормативных и организационно-распорядительных документов Общества в области ИБ, несут ответственность, установленную действующим законодательством РФ.

16. Порядок пересмотра Политики информационной безопасности

Политика ИБ Общества пересматривается с периодичностью не реже одного раза в 3 года. При пересмотре Политики ИБ учитываются результаты контроля эффективности обеспечения ИБ за предыдущий период.

Процедура пересмотра Политики ИБ Общества включает:

- анализ и выявление несоответствий действующей Политики ИБ текущим условиям функционирования КАСУ Общества;

- разработку предложений по совершенствованию Политики ИБ;

- утверждение новой редакции Политики ИБ генеральным директором Общества.

При пересмотре Политики ИБ учитываются:

- результаты контроля состояния ИБ и предложения структурных подразделений о совершенствовании мер и процедур обеспечения ИБ;

- изменения в организационно-штатной структуре Общества и в КАСУ;

- изменения в нормативно - правовой базе по ИБ, произошедшие с момента утверждения предыдущей редакции Политики ИБ;

- результаты анализа произошедших инцидентов ИБ, а также уязвимости и угрозы, выявленные в Обществе за время, прошедшее с момента утверждения предыдущей редакции Политики ИБ;

- изменения в управлении ИБ, включая изменения в распределении ресурсов и обязанностей работников Общества при обеспечении ИБ.