АКЦИОНЕРНОЕ ОБЩЕСТВО «ГИПРОСПЕЦГАЗ»

(АО «Гипроспецгаз»)

ПРИКАЗ

«14» апреля 2025 г. Санкт-Петербург № 9

О введении в действие Политики информационной безопасности АО «Гипроспецгаз»

В целях совершенствования подходов к обеспечению информационной безопасности в АО «Гипроспецгаз»,

ПРИКАЗЫВАЮ:

1. Ввести в действие «Политику информационной безопасности АО «Гипроспецгаз» (далее – Политика).

2. Руководителям структурных и обособленных подразделений АО «Гипроспецгаз» обеспечить ознакомление с Политикой работников подчиненных подразделений и выполнение ее требований.

3. Инженеру 2 категории группы управления персоналом и корпоративной защиты Я.Ю. Рябовой обеспечить хранение подлинника документа в установленном порядке, главному специалисту службы по эксплуатации зданий и сооружений Д.Г. Князеву обеспечить размещение файла, содержащего документ, на внутреннем портале АО «Гипроспецгаз».

4. Отменить действие документа «Политика информационной безопасности АО «Гипроспецгаз», введенного в действие приказом от 18.10.2016 № 103.

5. Контроль исполнения настоящего приказа оставляю за собой.

Генеральный директор **А.М. Пароменко**

Введена в действие приказом
генерального директора
АО «Гипроспецгаз»

от 14.04.2025 № 9

ПОЛИТИКА
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АО «ГИПРОСПЕЦГАЗ»

Санкт-Петербург

РАЗРАБОТАНО

Должность	Подразделение	И.О. Фамилия	Подпись	Дата
Главный специалист	ГУП и КЗ	А.С. Смирнова		

СОГЛАСОВАНО

Должность	Подразделение	И.О. Фамилия	Подпись	Дата
Заместитель генерального директора по корпоративной защите и управлению персоналом	Руководство	А.З. Юринов		
Главный юрисконсульт	Аппарат при руководстве	Т.В. Лизогуб		
Главный специалист	ГУП и КЗ	Д.Г. Попов		

Содержание

1 НАЗНАЧЕНИЕ И ОБЛАСТЬ ПРИМЕНЕНИЯ

1.1 Политика информационной безопасности АО "Гипроспецгаз" (далее – Политика) разработана с учётом требований:

– Р Газпром 4.2-0-001-2009 «Система обеспечения информационной безопасности ОАО «Газпром». Типовая политика информационной безопасности дочернего общества (организации)» (далее – Рекомендации 4.2-0-001);

– Политики информационной безопасности ОАО «Газпром», утверждённой приказом ОАО «Газпром» от 15.02.2008 № 48.

1.2 Настоящая Политика определяет позицию руководства АО "Гипроспецгаз" (далее – Общество) в отношении информационной безопасности, основные цели, направления и меры обеспечения информационной безопасности, которыми Общество руководствуется в своей деятельности.

1.3 В рамках Политики руководство Общества заявляет, что:

– информационные технологии играют важную роль в достижении целей деятельности Общества;

– информация является ценным активом Общества, требующая защиты независимо от форм её представления;

– в своей деятельности Общество сталкивается с широким спектром угроз в отношении информационной безопасности как внутреннего, так и внешнего характера, реализация которых может привести к ущербу (финансовым потерям, штрафным санкциям, претензиям, потере репутации, дезорганизации и т.д.);

– стратегической целью Общества в области информационной безопасности является обеспечение функционирования и использования информационных технологий с учётом возможного ущерба от реализации угроз в отношении информационной безопасности;

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

1.4 Положения Политики являются обязательными для исполнения всеми работниками Общества.

2 НОРМАТИВНЫЕ ССЫЛКИ

Настоящая Политика разработана с учётом требований следующих документов[1]:

Федеральный закон Российской Федерации от 29.07.2004 № 98-ФЗ «О коммерческой тайне»

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

Федеральный закон Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных»

[1] Перечень нормативных документов приведен в действующей редакции на момент создания документа, перед началом работ пользователю необходимо проверить действие ссылочных нормативных документов, в случае если документ заменен (изменен), то следует руководствоваться замененным (измененным) нормативным документом.

Федеральный закон Российской Федерации от 06.04.2011 № 63-ФЗ «Об электронной подписи»

Методика оценки угроз безопасности информации, утверждённая Федеральной службой по техническому и экспортному контролю России 05.02.2021

Приказ ОАО «Газпром» от 24.02.2005 № 12 «Об утверждении положения о режиме коммерческой тайны в ОАО «Газпром»

Приказ ОАО «Газпром» от 15.02.2008 № 48 «Об обеспечении информационной безопасности ОАО «Газпром»

Приказ ОАО «Газпром» от 09.02.2015 № 45 «Об утверждении положения об обработке персональных данных в ПАО «Газпром»

Приказ ОАО «Газпром» от 16.02.2015 № 65 «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных ОАО «Газпром», его дочерних обществ и организаций»

СТО Газпром 4.2-0-004-2009 Система обеспечения информационной безопасности ОАО «Газпром». Базовая модель информационной безопасности корпоративных информационно-управляющих систем

СТО Газпром 4.2-0-003-2021 Система обеспечения информационной безопасности ПАО «Газпром». Общие положения, термины и определения

СТО Газпром 4.2-3-001-2009 Система обеспечения информационной безопасности ОАО «Газпром». Руководство по разработке требований к объектам защиты»

СТО Газпром 4.2-3-003-2009 Система обеспечения информационной безопасности ОАО «Газпром». Анализ и оценка рисков

СТО Газпром 4.2-3-004-2009 Система обеспечения информационной безопасности ОАО «Газпром». Классификация объектов защиты

Р Газпром 4.2-2-001-2009 Система обеспечения информационной безопасности ОАО «Газпром». Технические требования к обеспечению информационной безопасности в беспроводных сетях, развертываемых на объектах ОАО «Газпром», его дочерних обществ и организаций

Р Газпром 4.2-0-001-2009 Типовая политика информационной безопасности дочернего общества (организации)

3 ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ

3.1 В настоящей Политике использованы термины и определения в соответствии со СТО Газпром 4.2-0-003.

3.2 В настоящей Политике используются следующие сокращения:

АРМ – автоматизированное рабочее место Общества;

ВПО – вредоносное программное обеспечение, компьютерные вирусы и программные закладки;

ИБ – информационная безопасность;

ИР – информационный ресурс Общества;

ИУС – информационно-управляющая система;

ИУС ПХД – ИУС производственно-хозяйственной деятельности Общества;

ИУС САД – ИУС «Система административного документооборота» Общества;

ЛВС – локальная вычислительная сеть Общества;

Общество – АО "Гипроспецгаз";

ОС – операционная система;

ПД – персональные данные;

ГУП и КЗ – группе управления персоналом и корпоративной защиты;

ПО – программное обеспечение;

РСПД – региональная сеть передачи данных Общества;

СЗИ – средство защиты информации;

СКЗИ – средство криптографической защиты информации;

Администратор ИБ – сотрудник ответственный за управление системно-технической инфраструктурой и информационно –управляющими системами,назначается приказом генерального директора АО «Гипроспецгаз» при согласовании с ГУП и КЗ.

4 ЦЕЛИ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

4.1 Основными целями Политики являются:

– обеспечение единых методов к обеспечению ИБ Общества, изложенных в Политике информационной безопасности ОАО «Газпром», утверждённой приказом ОАО «Газпром» от 15.02.2008 № 48»;

– обеспечение единых подходов к обеспечению ИБ в рамках Общества;

– создание методологической основы для разработки нормативных и организационно-распорядительных документов по обеспечению ИБ в Обществе;

– определение форм участия руководства Общества в решении проблем ИБ.

4.2 Основными целями процесса обеспечения ИБ в Обществе являются:

– создание условий для устойчивого функционирования информационной инфраструктуры Общества;

– поддержание необходимого уровня ИБ в Обществе, соответствующего требованиям законодательства Российской Федерации, нормативно-правовых актов Правительства Российской Федерации, Федеральной службы безопасности России и Федеральной службы по техническому и экспортному контролю России, а также нормативных документов и организационно-распорядительных актов ПАО «Газпром».

5 НАПРАВЛЕНИЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

5.1 Обеспечение ИБ в Обществе осуществляется по следующим направлениям:

– управление ИБ;

– идентификация и классификация объектов защиты;

– организация работы с персоналом по вопросам ИБ;

– управление инцидентами ИБ;

– обеспечение непрерывности бизнес-процессов;

– обеспечение ИБ при эксплуатации средств обработки, хранения и передачи информации и использовании ИР;

– обеспечение соответствия требованиям по ИБ.

Данные направления реализуются организационными и техническими мерами.

6 УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

6.1 Внутренняя организация информационной безопасности

Организация и обеспечение управления ИБ в Обществе осуществляется заместителем генерального директора по корпоративной защите и управлению персоналом.

Руководство Общества постоянно поддерживает необходимый уровень ИБ путем внедрения системы обеспечения ИБ, а также распределения обязанностей и ответственности между работниками Общества за ее внедрение и осуществление.

Организация плановой, непрерывной и целенаправленной работы по осуществлению мер обеспечения ИБ и контролю их выполнения в структурных подразделениях Общества возлагается на группу управления персоналом и корпоративной защиты Общества.

На ГУП и КЗ возложены следующие функции:

– планирование работ по ИБ;

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

– координация действий по обеспечению ИБ в структурных подразделениях Общества;

– контроль соблюдения режима коммерческой тайны и порядка обработки персональных данных;

– контроль выполнения и пересмотр настоящей Политики, политик ИБ Общества, нормативных и организационно-распорядительных документов Общества, определяющих меры защиты информации в Обществе.

С учетом особенностей конкретных объектов информационной инфраструктуры в Обществе осуществляется:

– определение прав доступа и полномочий пользователей в отношении (защищаемых) ИР;

– эксплуатация и контроль эксплуатации средств, механизмов и методов безопасности информации;

– контроль выполнения работниками Общества требований в области ИБ.

Функции по администрированию и контролю средств, механизмов (техник) и методов безопасности информации в Обществе распределяются между и Администратором ИБ группой управления персоналом и корпоративной защиты :

– администрирование СЗИ, СКЗИ, встроенных механизмов безопасности средств обработки, хранения и передачи информации осуществляется работниками Общества, ответственными за их эксплуатацию;

– контроль функционирования и настройки механизмов безопасности, а также соблюдения требований по ИБ осуществляется работниками ГУП и КЗ.

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.

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

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

Обязанности Администраторов ИБ определяются приказом по Обществу, содержащему перечень обязанностей:

– контроль заданных настроек систем защиты информации, подсистем управления доступом, регистрации и учета автоматизированных систем и вычислительных сетей;

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

– организация аудита автоматизированных систем, вычислительных сетей и автономных АРМ (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.

На начальников структурных подразделений Общества возлагается ответственность за обеспечение ИБ во вверенном структурном подразделении, при этом данную ответственность возможно возложить на подчинённого работника, которая включает:

– учёт АРМ и ИР, владельцем которых является структурное подразделение;

– учёт и хранение копий заявок на подключение к информационным ресурсам и к другим ресурсам;

– доведение до подчинённых работников нормативных и организационно-распорядительных документов Общества по защите информации;

– контроль соблюдения подчинёнными работниками парольной политики и доступа к информационным ресурсам Общества;

– участие в проведении проверок и расследований, связанных с нарушениями во вверенном структурном подразделении режима коммерческой тайны, порядка обработки персональных данных и несанкционированного доступа к информации Общества.

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

6.2 Обеспечение информационной безопасности при работе с юридическими и физическими лицами.

При организации доступа к ИР осуществляются мероприятия по обеспечению ИБ:

– определение рисков, связанных с предоставлением прав доступа к конфиденциальной информации Общества;

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

– заключение соглашения (договора) о конфиденциальности, на основании которого предоставляется доступ к конфиденциальной информации Общества.

Порядок представления информации юридическим и физическим лицам, органам государственной власти, а также передачи материалов средствам массовой информации,

вопросы обеспечения ИБ при допуске на объекты защиты Общества иностранных представителей должно регламентироваться в нормативных и организационно-распорядительных документах Общества.

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 в соответствии со СТО Газпром 4.2-3-004.

Идентифицированные и классифицированные объекты защиты отражаются в инвентаризационной документации, маркируются и для них назначаются владельцы – работники Общества, ответственные за безопасную эксплуатацию объектов защиты.

Процедуры повторяются ежегодно. Внеплановые процедуры идентификации и классификации объектов защиты выполняются в случае 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 нормативными и организационно-распорядительными документами Общества.

8 ОРГАНИЗАЦИЯ РАБОТЫ С ПЕРСОНАЛОМ ПО ВОПРОСАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

8.1 Обеспечение безопасности при заключении и во время действия трудового договора

В целях повышения уровня обеспечения ИБ при приеме на работу новых работников Общества осуществляется доведение до них требований обеспечения ИБ и устанавливается ответственность за их нарушение.

Обязанность работников Общества по соблюдению требований обеспечения ИБ определяется в должностных инструкциях и конкретизируется в нормативных и организационно-распорядительных документах Общества.

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

В Обществе обеспечивается сохранность заключенных договоров о конфиденциальности, учёт которых осуществляется в ГУП и КЗ.

Все работники Общества при вступлении в должность проходят первичный инструктаж в ГУП и КЗ, предусматривающий ознакомление с правилами и мерами ИБ.

Для работников Общества реализуются мероприятия по повышению осведомленности в области ИБ.

Работники, отвечающие за обеспечение ИБ могут проходить повышение квалификации, знакомятся с изменениями в законодательстве Российской Федерации, нормативных и организационно-распорядительных документах в области ИБ Общества

Работники Общества, имеющие доступ к информации, подлежащей защите, несут ответственность за её разглашение или утрату, а также за нарушение установленного порядка обеспечения ИБ.

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

8.2 Обеспечение безопасности при увольнении работника или изменении условий трудового договора

В целях обеспечения ИБ при прекращении или изменении условий трудового договора между работником и Обществом определяется порядок и осуществляется контроль возврата технических средств обработки, хранения и передачи информации, своевременного прекращения прав доступа к объектам защиты (информационным ресурсам) Общества.

Уведомление увольняемым работникам структурных подразделений Общества о принятых ими обязательствах по соблюдению договора о конфиденциальности, выполняется ГУП и КЗ.

При увольнении работника или изменении должностных обязанностей, его права доступа к ИР незамедлительно аннулируются или приводятся в соответствие с новыми должностными обязанностями.

Процедуры уведомления работников ГУП и КЗ и Администратора ИБ об увольнении работников структурных подразделений Общества и других кадровых движениях в отношении работников Общества определяются нормативными и организационно-распорядительными документами в области ИБ Общества.

9 УПРАВЛЕНИЕ ИНЦИДЕНТАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

9.1 Оповещение об инцидентах информационной безопасности

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

Работники структурных подразделений Общества обязаны сообщать в ГУП и КЗ о любых замеченных или предполагаемых нарушениях режима коммерческой тайны, порядка обработки ПД и обеспечения ИБ, а также выявленных уязвимостях в соответствии с установленными в Обществе порядком.

9.2 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.

Администратор ИБ является ответственным за реагирование на инциденты ИБ и имеет соответствующую подготовку.

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

10 ОБЕСПЕЧЕНИЕ НЕПРЕРЫВНОСТИ БИЗНЕС-ПРОЦЕССОВ

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

Состав мероприятий по обеспечению бесперебойного функционирования информационной инфраструктуры Общества определяется с учётом оценки рисков ИБ. Правила оценки рисков ИБ регламентированы в СТО Газпром 4.2-3-003.

Перечень угроз ИБ формируется в соответствии с методическим документом «Методика оценки угроз безопасности информации», утверждённым Федеральной службой по техническому и экспортному контролю России 05.02.2021, с учётом СТО Газпром 4.2-0-004.

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

11 ПОРЯДОК ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ЭТАПАХ ЖИЗНЕННОГО ЦИКЛА ОБЪЕКТОВ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

ИБ информационной инфраструктуры Общества обеспечивается на всех этапах жизненного цикла её объектов с учётом 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 следующие этапы:

- обоснование требований к объекту;
- создание (модернизация) объекта;
- ввод объекта в эксплуатацию;
- эксплуатация объекта;
- вывод объекта из эксплуатации.

ГУП и КЗ в части сопровождения вопросов режима коммерческой тайны, обработки ПД и обеспечения ИБ участвуют во всех этапах жизненного цикла объектов информационной инфраструктуры Общества.

Порядок разработки требований к информационной инфраструктуре Общества регламентируется СТО Газпром 4.2-3-001.

Порядок обеспечения ИБ информационной инфраструктуры Общества на всех этапах жизненного цикла её объектов определяется нормативными и организационно-распорядительными документами Общества. Возможны отдельные политики ИБ для отдельных объектов.

12 ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ЭКСПЛУАТАЦИИ СРЕДСТВ ОБРАБОТКИ, ХРАНЕНИЯ И ПЕРЕДАЧИ ИНФОРМАЦИИ И ИСПОЛЬЗОВАНИИ ИНФОРМАЦИОННЫХ РЕСУРСОВ ОБЩЕСТВА

12.1 Физическая защита объектов информационной инфраструктуры Общества

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

Технические средства обработки, хранения и передачи информации размещаются в запираемых шкафах, располагаемых в помещениях, доступ к которым физически ограничивается.

Порядок обеспечения физической защиты мест эксплуатации (размещения) объектов защиты Общества определяется нормативными и организационно-распорядительными

документами Общества.

12.2 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, включая используемых на договорных основаниях.

В Обществе устанавливаются пропускной и внутриобъектовый режимы, препятствующие бесконтрольному посещению территорий и помещений зданий Общества. Порядок посещения и поведения в зданиях и помещениях Общества регламентируется нормативными и организационно-распорядительными документами Общества.

Совещания, переговоры и иные мероприятия по повестке вопросов, содержащих информацию, составляющей коммерческую тайну, и иной конфиденциальной информации, проводятся исключительно в защищаемых помещениях, аттестованных в соответствии с требованиями законодательства Российской Федерации.

Проведение работ на охраняемых территориях Общества, в его зданиях и защищаемых помещениях третьими лицами обеспечивается контроль их деятельности работниками структурных подразделений Общества, в компетенции которых выполняемые работы.

Порядок защиты помещений, в которых располагаются технические средства (серверы, централизованные хранилища данных, сетевое оборудование и средства защиты информации), определяется нормативными и организационно-распорядительными документами Общества.

12.3 Организация безопасной эксплуатации средств обработки, хранения и передачи информации

В целях обеспечения ИБ объектов защиты 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 возлагаются на Администратора ИБ.

Правила эксплуатации средств обработки, хранения и передачи информации, используемых в Общества, определяются политиками ИБ, нормативными и организационно-распорядительными документами Общества.

12.4 Защита от вредоносного программного обеспечения

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

В Обществе используются средства защиты информации от ВПО, обеспечивающие многоуровневую (эшелонированную) защиту.

Порядок организации защиты информационной инфраструктуры Общества от ВПО определяется нормативными и организационно-распорядительными документами Общества.

12.5 Резервное копирование информационных ресурсов

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

Способ и периодичность резервного копирования, сроки хранения резервных копий определяются в зависимости от назначения и особенностей системы, в которой информация

обрабатывается, а также от ценности информации.

Порядок резервного копирования ИР определяется нормативными и организационно-распорядительными документами Общества.

12.6 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 со СТО Газпром 4.2-3-004.

Порядок резервирования средств обработки, хранения и передачи информации определяется нормативными и организационно-распорядительными документами Общества.

12.7 Обеспечение сетевой безопасности

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

Обеспечение сетевой безопасности достигается защитой РСПД (ЛВС) и сетевых информационных ресурсов ИУС ПХД Общества. Порядок обеспечения сетевой безопасности определяется соответствующими нормативными и организационно-распорядительными документами Общества.

12.8 Обеспечение информационной безопасности при обращении со съёмными носителями информации

В целях предотвращения несанкционированной передачи информации в Обществе применяются меры защиты съёмных носителей информации.

В Обществе разрешается применение только зарегистрированных в соответствии с установленным порядком съёмных носителей информации.

Осуществляется мониторинг использования носителей информации. Утилизация неиспользуемых носителей осуществляется только с обеспечением гарантированного уничтожения содержащейся на них информации, составляющей коммерческую тайну, и иной конфиденциальной информации.

Порядок обеспечения ИБ при обращении со съёмными носителями информации определяется соответствующими нормативными и организационно-распорядительными документами в области ИБ Общества.

12.9 Защищенный обмен информацией

В целях предотвращения нарушения конфиденциальности или/и целостности информации в Обществе применяются меры по защите информации при ее передаче различными методами.

В Обществе используются СЗИ, соответствующие задаваемым требованиям по безопасности информации.

Порядок эксплуатации и использования СЗИ определяется эксплуатационной документацией к ним, нормативными и организационно-распорядительными документами Общества.

12.10 Защита программного обеспечения

В целях поддержания работоспособности ПО в Обществе осуществляются меры по устранению уязвимостей 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. Обновление ПО возлагается на Администратора ИБ, отвечающего за его эксплуатацию.

Порядок защиты ПО определяется нормативными и организационно-распорядительными документами в области ИБ Общества.

12.11 Регистрация и учёт событий информационной безопасности

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

В Обществе осуществляется сбор, обнаружение, обработка, анализ, оценка, регистрация и учёт в информационной системе событий, произошедших в технических средствах обработки, хранения и передачи информации событий, которые могут быть связаны с нарушениями режима коммерческой тайны, обработки персональных данных и требований по обеспечению ИБ.

Журналы событий регулярно анализируются работниками,Администратором ИБ, находящихся в зоне их ответственности.

Порядок осуществления контроля (регистрации, учёта и реагирования) событий ИБ определяется нормативными и организационно-распорядительными документами Общества.

12.12 Контроль защищенности

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

Контроль защищенности информации, обрабатываемой в технических средствах структурного подразделения Общества, осуществляется соответствующими работниками Общества. Перечень объектов контроля определяется по результатам идентификации и классификации объектов защиты.

Порядок осуществления контроля защищенности определяется нормативными и организационно-распорядительными документами Общества.

12.13 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 квалифицированного сертификата ключа проверки электронной подписи или/и неквалифицированного сертификата ключа проверки электронной подписи, выданного удостоверяющим центром, аккредитованным в Сети удостоверяющих центров Группы Газпром.

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

При использовании мобильных устройств информация ограниченного доступа,

хранимая на них, защищается с использованием СКЗИ.

Порядок эксплуатации и использования СКЗИ определяется нормативными и организационно-распорядительными документами в области Общества.

13 КОНТРОЛЬ ДОСТУПА

13.1 Управление доступом пользователей

В целях обеспечения безопасности и устойчивого функционирования информационной инфраструктуры в Обществе осуществляется управление доступом пользователей к информационным ресурсам Общества, включая системы и технические средства, осуществляющие обработку, хранения и передачу информации.

Пользователи наделяются минимальными правами доступа и привилегиями, необходимыми им для выполнения должностных обязанностей, определяемыми структурными подразделениями Общества – владельцами информационных ресурсов Общества в соответствующих матрицах распределения прав доступа пользователей к информационным ресурсам Общества.

Наделение пользователей правами доступа и привилегиями основывается на установленной в Обществе формализованной процедуре предоставления прав доступа. При этом требуется использовать принцип ролевого или/и мандатного управления доступом. Права доступа и привилегии пользователей подлежат регулярному пересмотру владельцами информационных ресурсов Общества.

Порядок управления доступом пользователей определяется, нормативными и организационно-распорядительными документами Общества.

13.2 Ответственность пользователей

В целях предотвращения несанкционированного доступа, компрометации, утраты информации и средств обработки информации, в Обществе определяется ответственность пользователей за соблюдение правил доступа при работе на АРМ и в информационных ресурсах Общества.

Пользователи несут ответственность за соблюдение установленных требований по сложности паролей и хранении в тайне пароля. Требования к паролям определяются нормативными и организационно-распорядительными документами Общества.

Пользователям запрещено использовать учётные записи других пользователей, сообщать свои пароли или/и передавать средства аутентификации другим пользователям. При оставлении АРМ из поля видимости, пользователями выполняются меры по защите от несанкционированного доступа к интерактивному сеансу работы в ОС.

Порядок эксплуатации и правила использования АРМ определяется, нормативными и организационно-распорядительными документами Общества.

13.3 Контроль доступа к операционной системе

В целях предотвращения несанкционированного доступа к объектам защиты информационной инфраструктуры Общества осуществляется контроль доступа к интерактивному сеансу работы в ОС.

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

Управление учётными записями пользователей, их принадлежностью к группам пользователей, правами доступа и привилегиями, а также политикой парольной защиты

осуществляется Администратором ИБ.

Порядок управления и контроля учётных записей, их принадлежностью к группам пользователей, правам доступа и привилегий к операционной системе определяются нормативными и организационно-распорядительными документами Общества.

13.4 Контроль доступа к прикладным системам и информационным ресурсам

В целях предотвращения несанкционированного доступа к информации и нарушения функционирования информационной инфраструктуры в Обществе обеспечивается контроль доступа к системам и ИР.

Доступ к системам и ИР предоставляется пользователям после прохождения ими процедур идентификации и аутентификации. Требуется осуществлять единую аутентификацию в ИУС и ОС, при наличии технической возможности.

Меры контроля доступа определяются нормативными и организационно-распорядительными документами в области ИБ Общества.

13.5 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 исключительно для выполнения должностных обязанностей. Порядок разрешения и осуществления доступа пользователей к сетевым сервисам, меры контроля доступа определяются соответствующими нормативными и организационно-распорядительными документами Общества.

13.6 Контроль сетевого доступа

В целях предотвращения несанкционированного доступа в информационную инфраструктуру Общества и к ИР в Обществе осуществляется контроль сетевого доступа.

Меры контроля сетевого доступа определяются политикой ИБ РСПД (ЛВС), нормативными и организационно-распорядительными документами в области ИБ ПАО «Газпром» и Общества.

13.7 Обеспечение информационной безопасности при удаленном доступе и использовании мобильных устройств.

В целях защиты от несанкционированного доступа в информационную инфраструктуру Общества и к защищаемым ИР, а также сохранения конфиденциальности, целостности и доступности информации, в Обществе принимаются меры по обеспечению безопасности при осуществлении удаленного доступа и использовании мобильных устройств.

При удаленном подключении пользователей к объектам защиты осуществляется контроль подключения, предусматривающий применение средств усиленной аутентификации, средств межсетевого экранирования и СЗИ, включая СКЗИ.

Целесообразность применения мобильных устройств или/и удалённого доступа обосновывается проведением оценки рисков с учётом возможных угроз ИБ, связанных с использованием мобильных устройств и удалённого доступа.

Меры обеспечения безопасности при использовании мобильных устройств и при осуществлении удаленного доступа определяются нормативными и организационно-распорядительными документами Общества.

13.8 Обеспечение безопасности в беспроводных сетях

В целях защиты от несанкционированного доступа к информационной инфраструктуре

Общества и информации в Обществе принимаются меры по обеспечению безопасности беспроводных сетей.

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

Подключение пользовательских устройств к беспроводной сети Общества согласовывается с ГУП и КЗ.

Меры обеспечения безопасности беспроводных сетей определяются политиками ИБ, нормативными документами и организационно-распорядительными актами Общества, с учётом рекомендации Р Газпром 4.2-2-001.

13.9 Контроль доступа к сетевому оборудованию

В целях обеспечения безопасности сетевой инфраструктуры Общества осуществляется управление доступом эксплуатационного персонала (администраторов) к сетевому оборудованию.

В информационной инфраструктуре Общества обеспечивается защита физического и логического доступа к диагностическим и конфигурационным портам сетевого оборудования, межсетевых экранов, систем обнаружения вторжений, систем предотвращения вторжений и других сетевых (аппаратно-программных) СЗИ.

Создается выделенный сегмент сети управления сетевым оборудованием. При осуществлении управления сетевым оборудованием и средствами защиты без использования выделенного сегмента сети управления осуществляется криптографическая защита каналов управления.

Осуществляется сбор, обнаружение, обработка, анализ, оценка, регистрация и учёт в информационной системе событий, произошедших в сетевом оборудовании и средствах защиты, которые могут связаны с нарушениями режима коммерческой тайны, обработки персональных данных и требований по обеспечению ИБ.

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

Меры контроля доступа определяются политикой ИБ РСПД (ЛВС) Общества, нормативными и организационно-распорядительными документами Общества.

14 ОБЕСПЕЧЕНИЕ СООТВЕТСТВИЯ ТРЕБОВАНИЯМ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

14.1 Обеспечение соответствия правовым требованиям

В соответствии с законодательством Российской Федерации, требований нормативных и организационно-распорядительных актов ПАО «Газпром» и Общества осуществляются меры по защите информации ограниченного доступа.

Защита информации в Обществе обеспечивается организацией:

– режима коммерческой тайны;

– защиты персональных данных.

В Обществе используется только официально приобретенное лицензионное ПО, при этом допускается использование свободно распространяемого ПО.

В составе объектов информационной инфраструктуры используются сертифицированные по требованиям безопасности информации или разрешенные к

применению СЗИ.

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

14.2 Организация режима коммерческой тайны

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

Перечень мер регламентируется Федеральным законом Российской Федерации от 29.07.2004 № 98-ФЗ «О коммерческой тайне», приказом ОАО «Газпром» от 24.02.2005 № 12 «Об утверждении положения о режиме коммерческой тайны в ОАО «Газпром», а также другими нормативными и организационно-распорядительными документами Общества.

14.3 Организация защиты персональных данных

В Обществе устанавливается порядок защиты персональных данных, предусматривающий правовые, организационные по обеспечению их целостности, доступности и конфиденциальности.

Перечень мер по защите персональных данных регламентируется Федеральным законом Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных», приказом ОАО «Газпром» от 16.02.2015 № 65 «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных ОАО «Газпром», его дочерних обществ и организаций», политикой обработки ПД Общества, а также другими нормативными и организационно-распорядительными документами Общества.

14.4 Обеспечение соответствия организационным и техническим требованиям

В целях предотвращения нарушений ИБ осуществляется контроль выполнения требований нормативных и организационно-распорядительных актов в области ИБ ПАО «Газпром» и Общества.

К числу мер контроля относятся:

– регулярный контроль руководителями структурных подразделений Общества выполнения требований ИБ;

– анализ выявленных несоответствий требованиями ИБ и установление причин их возникновения;

– реализация корректирующих мер и устранение выявленных несоответствий.

14.5 Контроль состояния информационной безопасности

В целях определения соответствия принимаемых мер безопасности нормативным и организационно-распорядительным документам Общества по ИБ, выявления угроз ИБ и принятия мер по противодействию им в Обществе осуществляется контроль состояния ИБ.

Контроль состояния ИБ осуществляется путем:

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

– проведения внутренних плановых (внеплановых) проверок и постоянным контролем в структурных подразделениях Общества, осуществляемыми ГУП и КЗ Общества.

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

Порядок контроля состояния ИБ определяется нормативными и организационно-распорядительными документами Общества.

Результаты проведения контроля состояния ИБ документируются.

15 ОТВЕТСТВЕННОСТЬ РУКОВОДСТВА И РАБОТНИКОВ

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

Ответственность за обеспечение ИБ объектов защиты Общества возлагается на Администратора ИБ и ответственных за их эксплуатацию.

Работники Общества обязаны:

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

– использовать технические средства обработки, хранения и передачи информации Общества исключительно в целях выполнения должностных обязанностей;

– осуществлять информирование непосредственного руководителя об обнаруженных инцидентах ИБ.

Работникам Общества запрещается нарушать установленные требования обеспечения ИБ, скрывать факты возникновения и обнаружения инцидентов ИБ.

Работники Общества, не выполняющие требования настоящей Политики, требования нормативных и организационно-распорядительных документов Общества в области ИБ, по решению генерального директора Общества привлекаются к ответственности, предусмотренной законодательством Российской Федерации.

16 ПОРЯДОК ПЕРЕСМОТРА

Настоящая Политика пересматривается не реже одного раза в два года либо досрочно с учётом: результатов анализа и выявления несоответствий в действующей редакции Политики текущим условиям; результатов контроля эффективности обеспечения ИБ за предыдущий период; изменений в законодательстве Российской Федерации; изменений в нормативных документах или организационно-распорядительных актах ПАО «Газпром»; результатов анализа произошедших инцидентов ИБ, уязвимостей и угроз, выявленных в информационной инфраструктуре Общества; другими обстоятельствами, требующими внесения изменений, и разрабатывается управлением корпоративной защиты администрации Общества.

Таблица регистрации версий

Версия №	№ разделов/пунктов документа СМ (измененных, новых, удаленных)	Сведения о пересмотре документа СМ	Примечание