**СОГЛАШЕНИЕ**

**о внедрении системы**

**дистанционного контроля промышленной безопасности**

«\_\_\_\_»\_\_\_\_\_\_\_\_\_ \_\_\_\_\_ г. № \_\_\_\_\_\_\_\_\_\_\_\_\_

Федеральная служба по экологическому, технологическому и атомному надзору в лице заместителя руководителя Корчивого Станислава Анатольевича, действующего на основании доверенности от 23.12.2024 № Д-29, с одной стороны, и *[организация, индивидуальный предприниматель]* (далее – Организация) в лице *[ФИО]*, действующего на основании *[документ]*, с другой стороны, совместно именуемые «Стороны», в рамках проводимого эксперимента по внедрению системы дистанционного контроля промышленной безопасности на опасных производственных объектах, предусмотренного постановлением Правительства Российской Федерации от 31.12.2020 № 2415 «О проведении эксперимента по внедрению системы дистанционного контроля промышленной безопасности», заключили настоящее Соглашение о нижеследующем.

1. **Предмет соглашения**

1.1. Предметом настоящего Соглашения является экспериментальное внедрение на опасном производственном объекте Организации системы дистанционного контроля промышленной безопасности (далее – СДК ПБ), обеспечивающей:

* передачу информации о показателях промышленной безопасности
на основе сведений, в т.ч. о состоянии технологического процесса, полученных от автоматизированных систем;
* оперативную оценку рисков возникновения аварий;
* передачу сведений об авариях и инцидентах;
* передачу иной информации, предусмотренной настоящим Соглашением,
в информационный ресурс Ростехнадзора.

1.2. Эксперимент по внедрению СДК ПБ проводится в соответствии
с постановлением Правительства Российской Федерации от 31.12.2020 № 2415
«О проведении эксперимента по внедрению системы дистанционного контроля промышленной безопасности».

1.3. Эксперимент проводится на эксплуатируемом Организацией опасном производственном объекте, указанном в приложении № 1 к настоящему Соглашению, с использованием СДК ПБ.

1.4. Целями эксперимента по внедрению СДК ПБ являются:

1.4.1. Апробация динамической модели риск-ориентированного подхода
в области промышленной безопасности с использованием СДК ПБ.

1.4.2. Определение эффективности и удобства применения для организаций и индивидуальных предпринимателей технологий сбора, аналитической обработки информации о состоянии промышленной безопасности и технологических процессах на эксплуатируемых ими опасных производственных объектах, расчета показателей состояния промышленной безопасности, оперативной оценки рисков возникновения аварий и передачи информации в Ростехнадзор.

1.4.3. Оценка параметров применения СДК ПБ на опасных производственных объектах.

1.4.4. Формирование методических, организационных и технологических условий для обеспечения возможности функционирования и применения
СДК ПБ.

1.4.5. Апробация новых подходов к обеспечению федеральных органов исполнительной власти автоматизированным инструментарием оценки рисков возникновения аварий на опасных производственных объектах
с использованием систем оперативного мониторинга технологических процессов и расчета показателей состояния промышленной безопасности.

1.4.6. Формирование модели бесперебойного функционирования СДК ПБ.

1.4.7. Оценка достоверности сведений, вносимых в СДК ПБ, по итогам проведения эксперимента.

**2. Права и обязанности сторон**

**2.1. В рамках проведения эксперимента Организация:**

2.1.1. Обеспечивает передачу информации о показателях состояния промышленной безопасности опасного производственного объекта, указанного в пункте 1.3 Соглашения, в информационный ресурс Ростехнадзора
в электронном виде посредством СДК ПБ согласно перечню, указанному
в приложении № 2 к Соглашению.

2.1.2. Обеспечивает передачу информации о показателях состояния промышленной безопасности с соблюдением требований к обеспечению информационной безопасности и защиты информации, используемой в рамках функционирования СДК ПБ, в том числе от несанкционированного
ее копирования, распространения, уничтожения и модификации, блокирования доступа к ней, а также иных неправомерных действий предусмотренные приложением № 3 к настоящему Соглашению.

2.1.3. Обеспечивает при необходимости доработку СДК ПБ опасного производственного объекта для обеспечения передачи данных, указанных
в пункте 2.1.1 Соглашения, в информационный ресурс Ростехнадзора.

2.1.4. Устанавливает и соблюдает правила и порядок идентификации, аутентификации и авторизации с использованием СДК ПБ для формирования, размещения, изменения и удаления информации, предусмотренные приложением № 3 к настоящему Соглашению.

2.1.5. Обеспечивает соблюдение Порядка приема и хранения информации, поступившей с использованием системы дистанционного контроля промышленной безопасности, а также учета действий пользователей
по ее изменению и удалению, в соответствии с приложением № 4 к настоящему Соглашению.

**2.2. В рамках проведения эксперимента Ростехнадзор:**

2.2.1. Использует информацию, получаемую посредством СДК ПБ, при осуществлении федерального государственного надзора в области промышленной безопасности в целях реализации постановления Правительства Российской Федерации от 31.12.2020 № 2415 «О проведении эксперимента
по внедрению системы дистанционного контроля промышленной безопасности».

2.2.2. При необходимости привлекает к реализации Соглашения подведомственные организации Ростехнадзора.

2.2.3. Обеспечивает прием, контроль и хранение поступающей
от организации информации в соответствии с приложением № 4 к настоящему Соглашению.

2.2.4. В соответствии с требованиями о защите информации, утвержденными приказом ФСТЭК России от 11.02.2013 № 17 обеспечивает защиту поступающей в соответствии с настоящим Соглашением от Организации информации в информационный ресурс Ростехнадзора.

2.2.5. Обеспечивает контроль соблюдения Организацией порядка приема
и хранения информации, поступившей в информационный ресурс Ростехнадзора с использованием СДК ПБ, а также учета действий пользователей по ее изменению и удалению в соответствии с приложением № 4 к настоящему Соглашению.

2.2.6. В случае выявления Ростехнадзором недостаточности проводимого Организацией комплекса технических и организационных мер для определения состояния промышленной безопасности эксплуатируемого опасного производственного объекта (ОПО), а также выявления неэффективности функционирования СДК ПБ, Ростехнадзор вправе указать на необходимость доработки СДК ПБ, в том числе в части изменения (дополнения) контролируемых показателей состояния промышленной безопасности ОПО,
 а также осуществления Организацией иных действий (бездействий), необходимых для оценки и контроля промышленной безопасности объекта.

**2.3. Стороны при проведении эксперимента:**

2.3.1. При проведении эксперимента обеспечивают беспрерывную передачу информации посредством СДК ПБ. Передача данных из СДК ПБ
в информационный ресурс Ростехнадзора осуществляется после выполнения требований к обеспечению информационной безопасности и защиты информации, обеспечению защиты канала передачи данных, предусмотренных приложениями № 3 и № 4 к настоящему Соглашению.

2.3.2 Гарантируют отсутствие, в рамках тестирования передачи данных
из СДК ПБ Организации в информационный ресурс Ростехнадзора
в передаваемых данных информации содержащей конфиденциальные сведения и персональные данные, а также сведения, составляющие коммерческую и иную охраняемую законом тайну.

**3. Порядок взаимодействия Сторон**

3.1. Взаимодействие осуществляется в соответствии
с законодательством Российской Федерации и настоящим Соглашением.

3.2 Взаимодействие Сторон в рамках реализации эксперимента также осуществляется в форме обмена информацией и оказания экспертно-консультационной помощи по вопросам, относящимся к области взаимодействия Сторон в рамках Соглашения, для чего могут создавать рабочие группы, организовывать встречи, посредством создания рабочей группы при Ростехнадзоре, направления сообщений, организации встреч представителей рабочей группы и иными способами.

3.3. Взаимодействие Сторон и выполнение организационных мероприятий в рамках реализации Соглашения осуществляются
на безвозмездной основе.

**4. Заключительные положения**

4.1. Настоящее Соглашение вступает в силу с момента его подписания Сторонами и действует по 31.12.2025.

4.2. Спорные вопросы, касающиеся толкования и применения разделов или отдельных положений настоящего Соглашения, разрешаются Сторонами путем консультаций и переговоров.

4.3. Соглашение может быть изменено или дополнено по взаимному согласию Сторон. Все изменения и дополнения к настоящему Соглашению составляются в письменном виде и являются неотъемлемой частью Соглашения и вступают в силу только после подписания их Сторонами.

4.4. В случае несоблюдения Организацией требований пунктов 2.1.1, 2.1.2 настоящего Соглашения Ростехнадзор вправе в одностороннем порядке завершить проведение эксперимента по внедрению СДК ПБ и расторгнуть Соглашение путем уведомления Организации.

4.5. Во всем, что не предусмотрено настоящим Соглашением, Стороны руководствуются действующим законодательством Российской Федерации.

4.6. Настоящее Соглашение составлено в 2 (двух) экземплярах, имеющих равную юридическую силу, по 1 (одному) экземпляру для каждой из Сторон.

**Подписи сторон:**

|  |  |
| --- | --- |
| **Федеральная служба по экологическому, технологическому****и атомному надзору** | **Организация/Индивидуальный предприниматель** |
| 105066, Российская Федерация, Москва, ул. Таганская, д. 34,строение 1ИНН 7709561778КПП 770901001 ОГРН 1047796607650 ОКПО 00083701 Тел.: +7 (495) 646 57 96 Е-mail: it-upr@gosnadzor.ru**Заместитель руководителя Ростехнадзора** |  |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_/м.п. | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /\_\_\_\_\_\_\_\_\_\_\_\_\_\_/м.п. |

Приложение № 1 к Соглашению

от \_\_\_\_\_\_\_\_2025 г. №\_\_\_\_\_\_\_\_\_

**Сведения**

**об опасном производственном объекте,**

**на котором проводится эксперимент по внедрению СДК ПБ**

|  |  |
| --- | --- |
| **1** | **Сведения об опасном производственном объекте (ОПО)** |
| 1.1 | Полное наименование ОПО |  |
| 1.2 | Регистрационный номер ОПО в Государственном реестре опасных производственных объектов |  |
| 1.3 | Класс опасности ОПО и его числовое обозначение*(чрезвычайно высокой опасности – I класс, высокой опасности – II класс, средней опасности – III класс, низкой опасности – IV класс)* |  |
| 1.4 | Место нахождения (адрес) ОПО *(указывается адрес фактического места нахождения объекта (адресный ориентир или другие, позволяющие идентифицировать объект данные), согласно данным Государственного кадастра недвижимости и Единого государственного реестра недвижимости или документов, подтверждающих иное законное основание эксплуатации опасного производственного объекта, независимо от того, к какой категории относится объект недвижимости (точечный, линейный или полигональный (площадный)* |  |
| 1.5 | Дата ввода объекта в эксплуатацию (при наличии) |  |
| 1.6 | Наименование территориального органа Ростехнадзора |  |
| **2** | **Сведения об организации или индивидуальном предпринимателе, эксплуатирующей(ем) ОПО** |
| 2.1 | Полное наименование юридического лица, организационно-правовая форма или фамилия, имя и отчество (при наличии) индивидуального предпринимателя, эксплуатирующего ОПО |  |
| 2.2 | Идентификационный номер налогоплательщика (ИНН), эксплуатирующего ОПО |  |
| 2.3 | Основной государственный регистрационный номер (ОГРН), основной государственный регистрационный номер индивидуального предпринимателя (ОГРНИП) или сведения о внесении записи в государственный реестр аккредитованных филиалов, представительств иностранных юридических лиц (в случае, если имеется) |  |
| 2.4 | Адрес места нахождения (места жительства) юридического лица (индивидуального предпринимателя) *С указанием административно-территориальной единицы, населенного пункта, улицы, номера дома (корпуса, строения), соответствующего ему почтового индекса согласно учредительным документам (для ИП - адрес на основании записи в паспорте)* |  |
| 2.5 | Сведения о правах владения ОПО, в том числе земельными участками, зданиями, строениями, сооружениями, с указанием вида права на ОПО, реквизитов документов, подтверждающих право владения, кадастровые номера (при наличии) |  |
| **3** | **Сведения о собственнике ОПО (указываются в случае, если организация или индивидуальный предприниматель, эксплуатирующая(ий) ОПО, не является собственником ОПО)** |
| 3.1 | Полное наименование юридического лица, организационно-правовая форма или фамилия, имя, отчество (при наличии) индивидуального предпринимателя – собственника ОПО |  |
| 3.2 | Идентификационный номер налогоплательщика (ИНН) – собственника ОПО |  |

 **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

*Сведения заполняются Организацией в соответствии с данными в Свидетельстве о регистрации опасного производственного объекта в Государственном реестре опасных производственных объектов.*

Приложение № 2 к Соглашению

от \_\_\_\_\_\_\_\_2025 г. №\_\_\_\_\_\_\_\_\_

**Перечень информации, передаваемой посредством**

**системы дистанционного контроля промышленной безопасности**

Организация посредством Системы дистанционного контроля промышленной безопасности (далее – СДК ПБ) передает в Ростехнадзор информацию в виде XML-схемы, содержащей информацию о названиях элементов и атрибутов, отношениях между элементами и атрибутами, их структуре и типах данных. Значения параметров передаются в виде XML‑документа:

сведения о технических устройствах, зданиях и сооружениях, эксплуатируемых на опасном производственном объекте (включая идентификатор, тип, наименование, информацию о приборах и системах контроля безопасности, системах наблюдения, оповещения, связи и поддержки действий в случае аварии), перечень контролируемых параметров, их номинальные и пороговые значения, возможность сбора в автоматическом режиме;

 перечень контролируемых СДК ПБ параметров состояния промышленной безопасности;

 значения контролируемых СДК ПБ параметров;

 информация о зафиксированных событиях промышленной безопасности, аварийных ситуациях и их устранении, отчеты о принятых для устранения мерах;

 информация о проведении работ повышенной опасности (огневых, газоопасных, ремонтных и т.д.) от момента их планирования до завершения работ (с представлением распоряжений о проведении работ, наряд-допусков, журналов регистрации наряд-допусков, копий удостоверений персонала на допуск к проводимым работам);

 информация о проведенных ранее и планируемых технических обслуживаниях, ревизиях, диагностирования, испытаниях, освидетельствованиях, ремонтах, экспертизах промышленной безопасности и т.п. технических устройств, зданий и сооружений опасного производственного объекта (с представлением информации о подтверждении проведения работ и их результатов).

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

*Перечень заполняется Организацией исходя из уровня автоматизации опасного производственного объекта системами управления технологическими процессами/производством, технологической оснащенности программно-аппаратными комплексами дистанционного контроля состояния промышленной безопасности и рисков возникновения аварий, а также наличия технической возможности передачи указанной информации в Ростехнадзор в электронном виде.*

Приложение № 3 к Соглашению

от \_\_\_\_\_\_\_\_2025 г. №\_\_\_\_\_\_\_\_\_

**Требования к обеспечению информационной безопасности**

**и защиты информации, используемой в рамках функционирования системы дистанционного контроля промышленной безопасности,**

**в том числе от несанкционированного ее копирования, распространения, уничтожения и модификации, блокирования доступа к ней,**

**а также иных неправомерных действий, включая правила и порядок идентификации, аутентификации и авторизации с использованием системы дистанционного контроля промышленной безопасности участников информационного взаимодействия, осуществляющих в ней формирование, размещение, изменение и удаление информации**

1. В целях обеспечения защиты информации в СДК ПБ при организации информационного взаимодействия реализуются следующие меры защиты информации:

| **Код** | **Меры защиты и обеспечения безопасности** |
| --- | --- |
| **Идентификация и аутентификация (ИАФ)** |
| ИАФ.0 | Регламентация правил и процедур идентификации и аутентификации |
| ИАФ.1 | Идентификация и аутентификация пользователей и инициируемых ими процессов |
| ИАФ.2 | Идентификация и аутентификация устройств |
| ИАФ.3 | Управление идентификаторами |
| ИАФ.4 | Управление средствами аутентификации |
| ИАФ.5 | Идентификация и аутентификация внешних пользователей |
| ИАФ.7 | Защита аутентификационной информации при передаче |
| **Управление доступом (УПД)** |
| УПД.0 | Регламентация правил и процедур управления доступом |
| УПД.1 | Управление учетными записями пользователей |
| УПД.2 | Реализация модели управления доступом |
| УПД.4 | Разделение полномочий (ролей) пользователей |
| УПД.5 | Назначение минимально необходимых прав и привилегий |
| УПД.6 | Ограничение неуспешных попыток доступа в информационную (автоматизированную) систему |
| УПД.10 | Блокирование сеанса доступа пользователя при неактивности |
| УПД.11 | Управление действиями пользователей до идентификации и аутентификации |
| УПД.13 | Реализация защищенного удаленного доступа |
| УПД.14 | Контроль доступа из внешних информационных (автоматизированных) систем |
| **Ограничение программной среды (ОПС)** |
| ОПС.0 | Регламентация правил и процедур ограничения программной среды |
| ОПС.2 | Управление установкой (инсталляцией) компонентов программного обеспечения |
| **Защита машинных носителей информации (ЗНИ)** |
| ЗНИ.0 | Регламентация правил и процедур защиты машинных носителей информации |
| ЗНИ.5 | Контроль использования интерфейсов ввода (вывода) информации на съемные машинные носители информации |
| ЗНИ.7 | Контроль подключения съемных машинных носителей информации |
| **Аудит безопасности (АУД)** |
| АУД.0 | Регламентация правил и процедур аудита безопасности |
| АУД.1 | Инвентаризация информационных ресурсов |
| АУД.2 | Анализ уязвимостей и их устранение |
| АУД.3 | Генерирование временных меток и (или) синхронизация системного времени |
| АУД.4 | Регистрация событий безопасности |
| АУД.6 | Защита информации о событиях безопасности |
| АУД.7 | Мониторинг безопасности |
| АУД.8 | Реагирование на сбои при регистрации событий безопасности |
| АУД.10 | Проведение внутренних аудитов |
| **Антивирусная защита (АВЗ)** |
| АВЗ.0 | Регламентация правил и процедур антивирусной защиты |
| АВЗ.1 | Реализация антивирусной защиты |
| АВЗ.2 | Антивирусная защита электронной почты и иных сервисов |
| АВЗ.4 | Обновление базы данных признаков вредоносных компьютерных программ (вирусов) |
| **Обеспечение целостности (ОЦЛ)** |
| ОЦЛ.0 | Регламентация правил и процедур обеспечения целостности |
| ОЦЛ.1 | Контроль целостности программного обеспечения |
| **Защита технических средств и систем (ЗТС)** |
| ЗТС.0 | Регламентация правил и процедур защиты технических средств и систем |
| ЗТС.2 | Организация контролируемой зоны |
| ЗТС.3 | Управление физическим доступом |
| ЗТС.4 | Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр |
| **Защита информационной (автоматизированной) системы и ее компонентов (ЗИС)** |
| ЗИС.0 | Регламентация правил и процедур защиты информационной (автоматизированной) системы и ее компонентов |
| ЗИС.1 | Разделение функций по управлению (администрированию) информационной (автоматизированной) системой с иными функциями |
| ЗИС.2 | Защита периметра информационной (автоматизированной) системы |
| ЗИС.6 | Управление сетевыми потоками |
| ЗИС.19 | Защита информации при ее передаче по каналам связи |
| ЗИС.20 | Обеспечение доверенных канала, маршрута |
| ЗИС.27 | Обеспечение подлинности сетевых соединений |
| ЗИС.28 | Исключение возможности отрицания отправки информации |
| ЗИС.29 | Исключение возможности отрицания получения информации |
| ЗИС.32 | Защита беспроводных соединений |
| ЗИС.35 | Управление сетевыми соединениями |
| **Реагирование на компьютерные инциденты (ИНЦ)** |
| ИНЦ.0 | Регламентация правил и процедур реагирования на компьютерные инциденты |
| ИНЦ.1 | Выявление компьютерных инцидентов |
| ИНЦ.2 | Информирование о компьютерных инцидентах |
| ИНЦ.3 | Анализ компьютерных инцидентов |
| ИНЦ.4 | Устранение последствий компьютерных инцидентов |
| ИНЦ.5 | Принятие мер по предотвращению повторного возникновения компьютерных инцидентов |
| ИНЦ.6 | Хранение и защита информации о компьютерных инцидентах |
| **Управление конфигурацией (УКФ)** |
| УКФ.0 | Регламентация правил и процедур управления конфигурацией информационной (автоматизированной) системы |
| УКФ.2 | Управление изменениями |
| УКФ.3 | Установка (инсталляция) только разрешенного к использованию программного обеспечения |
| **Управление обновлениями программного обеспечения (ОПО)** |
| ОПО.0 | Регламентация правил и процедур управления обновлениями программного обеспечения |
| ОПО.1 | Поиск, получение обновлений программного обеспечения от доверенного источника |
| ОПО.2 | Контроль целостности обновлений программного обеспечения |
| ОПО.4 | Установка обновлений программного обеспечения |
| **Обеспечение действий в нештатных ситуациях (ДНС)** |
| ДНС.0 | Регламентация правил и процедур обеспечения действий в нештатных ситуациях |
| ДНС.1 | Разработка плана действий в нештатных ситуациях |
| ДНС.2 | Обучение и отработка действий персонала в нештатных ситуациях |
| ДНС.5 | Обеспечение возможности восстановления информационной (автоматизированной) системы в случае возникновения нештатных ситуаций |
| ДНС.6 | Анализ возникших нештатных ситуаций и принятие мер по недопущению их повторного возникновения |
| **Информирование и обучение персонала (ИПО)** |
| ИПО.0 | Регламентация правил и процедур информирования и обучения персонала |
| ИПО.1 | Информирование персонала об угрозах безопасности информации и о правилах безопасной работы |

Данный набор мер подлежит адаптации в соответствии с угрозами безопасности информации, применяемыми информационными технологиями
и особенностями функционирования СДК ПБ. При этом из набора могут быть исключены меры, непосредственно связанные с информационными технологиями, не используемыми в СДК ПБ, или характеристиками, не свойственными СДК ПБ.

2. Требования к обеспечению информационной безопасности и защиты информации должны быть определены в документации по эксплуатации СДК ПБ (техническом задании на ее создание (модернизацию) и обеспечивать информационное взаимодействия с информационным ресурсом Ростехнадзора
с учетом требований федерального законодательства.

В ходе информационного взаимодействия должно быть исключено прямое взаимодействие информационного ресурса Ростехнадзора
с компонентами автоматизированной системы управления технологическими процессами опасного производственного объекта.

К серверу коммуникаций СДК ПБ (интеграционной шине), непосредственно подключаемому к информационному ресурсу Ростехнадзора
и обеспечивающему информационное взаимодействие между СДК ПБ
и информационным ресурсом Ростехнадзора, предъявляется требование
о наличии положительного заключения (вывода) в акте приемки (или аттестате соответствия) о его соответствии требованиям, приведенным в пункте 1 настоящих требований.

Требования к обеспечению информационной безопасности и защиты информации должны быть реализованы в соответствии с проектной документацией на СДК ПБ и обеспечение информационного взаимодействия
с информационным ресурсом Ростехнадзора. До начала передачи данных
в информационный ресурс Ростехнадзора должна быть выполнена оценка соответствия системы указанным требованиям.

3. Оценка соответствия проводится в форме приемочных испытаний СДК ПБ, в ходе которых должен быть проведен комплекс организационных
и технических мероприятий (испытаний), в результате которых подтверждается в том числе соответствие сервера коммуникаций и решений по обеспечению его безопасности требованиям, приведенным в пункте 1 настоящих требований, Соглашению, а также требованиям технического задания на создание СДК ПБ.

В качестве исходных данных при приемочных испытаниях используются акт определения уровня защищенности персональных данных, техническое задание на создание (модернизацию) СДК ПБ, проектная и рабочая (эксплуатационная) документация на СДК ПБ, организационно-распорядительные документы по безопасности Организации, материалы предварительных испытаний и опытной эксплуатации, а также иные документы, разрабатываемые в соответствии с требованиями стандартов Организации.

4. Приемочные испытания СДК ПБ проводятся в соответствии
с программой и методикой приемочных испытаний. Результаты приемочных испытаний СДК ПБ, в том числе сервера коммуникаций и решений
по обеспечению его безопасности, с выводом о соответствии установленным требованиям включаются в акт приемки СДК ПБ в эксплуатацию.

Ввод в эксплуатацию СДК ПБ, в том числе сервера коммуникаций
и решений по обеспечению его безопасности, осуществляется при положительном заключении (выводе) в акте приемки о соответствии СДК ПБ установленным требованиям по обеспечению безопасности.

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

*Для реализации указанных мер применяются средства защиты информации, прошедшие сертификацию, испытания или приемку в соответствии с пунктами 28, 29 и 29.2 Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденных приказом ФСТЭК России от 25.12.2017 № 239, с учетом сроков вступления в силу соответствующих пунктов.*

*Для обеспечения безопасности в системах дистанционного контроля, являющихся государственными информационными системами, настоящие меры применяются с учетом Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 № 17.*

*Защита информации, обрабатываемой в системах дистанционного контроля, являющихся информационными системами персональных данных, осуществляется в соответствии с Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 01.11.2012 № 1119, Составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденными приказом ФСТЭК России от 18.02.2013 № 21, с учетом настоящих мер.*

*Для обеспечения безопасности в системах дистанционного контроля, являющихся значимыми объектами критической информационной инфраструктуры, настоящие меры применяются с учетом Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утверждённых приказом ФСТЭК России от 25.12.2017 № 239.*

*Для обеспечения безопасности в системах дистанционного контроля, являющихся автоматизированными системами управления, настоящие меры применяются с учетом 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, утвержденных приказом ФСТЭК России от 14.03.2014 № 31.*

Приложение № 4 к Соглашению

от \_\_\_\_\_\_\_\_2025 г. №\_\_\_\_

**Рекомендуемый порядок приема и хранения информации,**

**поступившей с использованием системы дистанционного контроля промышленной безопасности, а также учета действий пользователей**

**по ее изменению и удалению**

**Класс защищенности.** Информационный ресурс Ростехнадзора классифицирован как ГИС 2-го класса защищенности.

 **Защита канала и передача данных.** Для передачи данных
в информационный ресурс Ростехнадзора предусмотрено создание защищенного канала связи с помощью ViPNet Coordinator. Решение обеспечивает двустороннюю криптографическую аутентификацию абонентов
при установлении соединения, криптографическую защиту данных
(в соответствии с ГОСТ 28147–89), передаваемых по открытым каналам связи, защиту от несанкционированного доступа.

**Подключение СДК ПБ к информационному ресурсу Ростехнадзора.** При осуществлении доступа СДК ПБ в защищенную сеть передачи данных Ростехнадзора необходимо выполнение следующих условий:

наличие и техническая поддержка программно-аппаратных средств криптографической защиты данных, совместимых с программно-аппаратными средствами криптографической защиты данных Ростехнадзора;

дальнейшее инициирование Ростехнадзором подключения криптошлюза СДК ПБ к защищенной сети передачи данных Ростехнадзора с целью предоставления доступа к информационному ресурсу Ростехнадзора, находящейся в государственной единой облачной платформе.

**Обработка данных.** Значения параметров формируются в СДК ПБ в виде XML-документа, содержащего информацию о названиях элементов
и атрибутов, отношения между элементами и атрибутами, их структуре и типах данных, и передаются в информационный ресурс Ростехнадзора. СДК ПБ должны формироваться электронные подписи XML-документов, передаваемых
в информационный ресурс Ростехнадзора, для исключения возможности их модификации и обеспечения юридической значимости XML-документа.

Данные, передаваемые СДК ПБ в информационный ресурс Ростехнадзора, не подлежат изменению (обеспечивается ролевой моделью
и правами доступа к данным в рамках СДК ПБ) и хранятся в Организации
в течение 3 (трех) лет. По истечении данного срока поступившие данные удаляются средствами СДК ПБ.

В случае нарушения целостности сообщения, переданного СДК ПБ
в информационный ресурс Ростехнадзора, для определения источника нарушения используются журналы событий функционирования СДК ПБ.

Данные, размещенные в информационном ресурсе Ростехнадзора и СДК ПБ, не подлежат изменению и удалению (обеспечивается ролевой моделью доступа к данным на базе программы защиты информации серверов приложений WebGard).

\_\_\_\_\_\_\_\_\_\_\_\_