

**Соглашение о внедрении системы
дистанционного контроля промышленной безопасности**

_____ 2021 г.

№ _____

Федеральная служба по экологическому, технологическому и атомному надзору в лице заместителя руководителя Геллера Анатолия Яковлевича, действующего на основании доверенности (*реквизиты*), с одной стороны, и [*организация, индивидуальный предприниматель*] (далее – Организация) в лице [*ФИО*], действующего на основании [*документ*], с другой стороны, совместно именуемые «Стороны», заключили настоящее Соглашение о нижеследующем.

I. Предмет Соглашения

1.1. Предметом настоящего Соглашения является экспериментальное внедрение на опасном производственном объекте Организации системы дистанционного контроля промышленной безопасности, обеспечивающей получение от автоматизированных систем контроля информации о состоянии промышленной безопасности и технологических процессах, расчет показателей состояния промышленной безопасности, оперативную оценку рисков возникновения аварий, а также передачу информации в создаваемую государственную информационную систему «Цифровая платформа «Автоматизированная информационная система Ростехнадзора» (далее – цифровая платформа АИС Ростехнадзора).

1.2. Эксперимент по внедрению системы дистанционного контроля промышленной безопасности проводится в соответствии с постановлением Правительства Российской Федерации от 31 декабря 2020 г. № 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.

1.4. Целями эксперимента по внедрению системы дистанционного контроля промышленной безопасности являются:

1.4.1. Апробация динамической модели риск-ориентированного подхода в области промышленной безопасности с использованием системы дистанционного контроля промышленной безопасности.

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 системы дистанционного контроля промышленной безопасности на опасных производственных объектах.

1.4.4. Формирование методических, организационных и технологических условий для обеспечения возможности функционирования и применения системы дистанционного контроля промышленной безопасности.

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 системы дистанционного контроля промышленной безопасности.

1.4.7. Оценка достоверности сведений, вносимых в систему дистанционного контроля, по итогам проведения эксперимента.

II. Обязательства Сторон

2.1. В рамках проведения эксперимента Организация:

2.1.1. Обеспечивает непрерывную передачу информации о показателях состояния промышленной безопасности опасного производственного объекта, указанного в пункте 1.3 Соглашения, в цифровую платформу АИС Ростехнадзора в электронном виде посредством системы дистанционного контроля промышленной безопасности согласно перечню, указанному в приложении № 2 к Соглашению.

2.1.2. Обеспечивает доработку и адаптацию системы дистанционного контроля промышленной безопасности опасного производственного объекта в случае необходимости для обеспечения передачи данных, указанных в пункте 2.1.1 Соглашения, в цифровую платформу АИС Ростехнадзора.

2.2. В рамках проведения эксперимента Ростехнадзор:

2.2.1. Использует информацию, получаемую посредством системы дистанционного контроля промышленной безопасности, при осуществлении федерального государственного надзора в области промышленной безопасности, в целях реализации постановления Правительства Российской Федерации от 31 декабря 2020 г. № 2415 «О проведении эксперимента по внедрению системы дистанционного контроля промышленной безопасности».

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

2.3. Стороны при проведении эксперимента:

2.3.1. Осуществляют соблюдение требований 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, и обеспечивают соблюдение правил и порядка идентификации, аутентификации и авторизации с использованием системы дистанционного контроля промышленной безопасности участников информационного взаимодействия, осуществляющих в ней формирование, размещение, изменение и удаление информации, в соответствии с приложением № 3 к Соглашению.

2.3.2. Обеспечивают соблюдение порядка приема и хранения информации, поступившей в цифровую платформу АИС Ростехнадзора 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.

2.3.3. Своевременно рассматривают обращения и предложения, направленные Сторонами Соглашения.

2.4. К системе дистанционного контроля промышленной безопасности опасного производственного объекта, подключаемой к цифровой платформе АИС Ростехнадзора, предъявляется требование о наличии положительного заключения (вывода) в акте приемки (или аттестате соответствия) о соответствии указанной системы требованиям, приведенным в приложении № 3 к Соглашению. Указанная приемка (аттестация) осуществляется

в соответствии с пунктом 12.7 Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденных приказом Федеральной службы по техническому и экспортному контролю (далее – ФСТЭК России) от 25 декабря 2017 г. № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

III. Порядок взаимодействия Сторон

3.1. Для реализации целей Соглашения и осуществления оперативного взаимодействия по вопросам, относящимся к предмету Соглашения, Стороны формируют рабочую группу, состав которой определяется в ходе осуществления работ.

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, посредством направления сообщений, организации встреч представителей Сторон и иными способами.

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

IV. Заключительные положения

4.1. Настоящее Соглашение вступает в силу с момента его подписания Сторонами и действует до 31 декабря 2022 года.

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 пролонгировано по взаимному согласию Сторон посредством заключения дополнительного соглашения.

4.4. 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.

4.5. Соглашение может быть расторгнуто досрочно по взаимному согласию Сторон либо по инициативе одной из Сторон при условии

письменного уведомления другой Стороны не позднее, чем за 30 (тридцать) календарных дней до дня расторжения.

4.6. Во всем, что не предусмотрено настоящим Соглашением, Стороны руководствуются действующим законодательством.

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

V. Подписи Сторон

**Федеральная служба
по экологическому, технологическому
и атомному надзору**

Место нахождения: 105066, Российская
Федерация, Москва,
ул. А. Лукьянова, д. 4, стр. 1
ИНН 7709561778
КПП 770901001
ОГРН 1047796607650
ОКПО 00083701
Тел.: +7 (495) 646 57 96
E-mail: it-upr@gosnadzor.ru

**Заместитель руководителя
Федеральной службы
по экологическому, технологическому
и атомному надзору**

_____ / **А.Я. Геллер**

**Организация/Индивидуальный
предприниматель**

_____ / _____

Приложение № 1
к Соглашению от _____ 2021 г.
№ _____

**Сведения об опасном производственном объекте,
на котором проводится эксперимент по внедрению системы
дистанционного контроля промышленной безопасности**

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 <i>(чрезвычайно высокой опасности – I класс, высокой опасности – II класс, средней опасности – III класс, низкой опасности – IV класс)</i>	
1.4	Место нахождения (адрес) ОПО <i>(указывается адрес фактического места нахождения объекта (адресный ориентир или другие, позволяющие идентифицировать объект данные), согласно данных Государственного кадастра недвижимости и Единого государственного реестра недвижимости или документах, подтверждающих иное законное основание эксплуатации опасного производственного объекта, независимо от того, к какой категории относится объект недвижимости (точечный, линейный или полигональный (площадной))</i>	
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) <i>С указанием административно-территориальной единицы, населенного пункта, улицы, номер дома (корпуса, строения), соответствующего ему почтового индекса согласно учредительным документам (для ИП - адрес на основании записи в паспорте)</i>	
2.5	Сведения о правах владения ОПО, в том числе земельных участков, зданий, строений, сооружений с указанием вида права на ОПО, реквизитов документов подтверждающие 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.

**Перечень информации, передаваемой посредством
системы дистанционного контроля промышленной безопасности**

Система дистанционного контроля промышленной безопасности (далее – СДК ПБ) передает в цифровую платформу АИС Ростехнадзора 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, возможность передачи в цифровую платформу АИС Ростехнадзора, схемы технологических процессов объекта;

перечень контролируемых СДК ПБ параметров состояния промышленной безопасности, возможных к передаче в цифровую платформу АИС Ростехнадзора;

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, диагностированиях, 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 _____ 2021 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

В целях обеспечения защиты информации в системе дистанционного контроля при подключении к цифровой платформе АИС Ростехнадзора 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

Код	Меры защиты и обеспечения безопасности
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)

Код	Меры защиты и обеспечения безопасности
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

Код	Меры защиты и обеспечения безопасности
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

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 декабря 2017 г. № 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 февраля 2013 г. № 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 1 ноября 2012 г. № 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 февраля 2013 г. № 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, утвержденных приказом ФСТЭК России от 25 декабря 2017 г. № 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 марта 2014 г. № 31.

**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. Цифровая платформа АИС Ростехнадзора классифицирована как ГИС 2-го класса защищенности.

Защита канала и передача данных. Для передачи данных в цифровой платформе АИС Ростехнадзора предусмотрено создание защищенного канала связи с помощью программно-аппаратных средств АПКШ Континент и 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 внешних пользователей. При осуществлении доступа внешнего пользователя в защищенную сеть передачи данных Ростехнадзора необходимо выполнение следующих условий:

наличие и техническая поддержка программно-аппаратных средств криптографической защиты данных, совместимым с программно-аппаратными средствами криптографической защиты данных Ростехнадзора; дальнейшее инициирование Ростехнадзором подключения криптошлюза внешнего пользователя к защищенной сети передачи данных Ростехнадзора с целью предоставления доступа к цифровой платформе АИС Ростехнадзора, находящейся в государственной единой облачной платформе.

Обработка данных. Данные передаются в виде XML-схемы, содержащей информацию о названиях элементов и атрибутов, отношения между элементами и атрибутами, их структуре и типах данных. Значения параметров передаются в виде XML-документа. Данные и значения, передаваемые в цифровую платформу АИС Ростехнадзора, должны быть подписаны электронной подписью для исключения возможности их модификации.

Данные, размещенные в цифровой платформе АИС Ростехнадзора системой дистанционного контроля промышленной безопасности,

не подлежат изменению и удалению (обеспечивается ролевой моделью доступа к данным на базе программы защиты информации серверов приложений «WebGard»).
