**МИНИСТЕРСТВО СВЯЗИ
И МАССОВЫХ КОММУНИКАЦИЙ
РОССИЙСКОЙ ФЕДЕРАЦИИ**

Тверская ул., 7, Москва, 125375
Справочная: +7 (495) 771-8000

По списку

21.08.2017 № П9-1-070-19857

на №_____ от_____

Министерство связи и массовых коммуникаций Российской Федерации в целях реализации приоритетной программы по основному направлению стратегического развития Российской Федерации «Реформа контрольной и надзорной деятельности», утвержденной протоколом заседания президиума Совета при Президенте Российской Федерации по стратегическому развитию и приоритетным проектам от 21 декабря 2016 года № 12 направляет проект методических рекомендаций по использованию промышленного интернета вещей для оптимизации контрольной (надзорной) деятельности.

Просьба рассмотреть и согласовать/представить замечания по представленным материалам и направить позицию в адрес Минкомсвязи России в срок до 25 августа 2017 года.

Приложение: на 13 л. в 1 экз.

Директор Департамента
проектов по информатизации О.Ю. Качанов

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП

Сертификат: 00C6750D5B11E4D580E7117C61E1683664
Владелец: Качанов Олег Юрьевич
Действителен с 05.07.2017 до 05.07.2018

Тел.: 8-495-771-80-00 доб. 8412

Проект

Методические рекомендации по использованию промышленного интернета вещей для оптимизации контрольной (надзорной) деятельности

Содержание

1 ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Понятие промышленного интернета вещей

Термин «промышленный интернет вещей» используется для обозначения совокупности следующих автоматических или автоматизированных инструментов и технологий:

- средств измерения, обеспечивающих преобразование сведений о внешней среде в машиночитаемые данные (далее — средства измерения);
- средств передачи таких данных от средств измерений в информационные системы, где осуществляется их обработка, а также от информационных систем обработки к системам реагирования (далее — средства передачи данных);
- средств обработки данных, осуществляющих накопление и анализ данных, поступающих от средств измерения (далее — средства обработки данных);
- систем реагирования, обеспечивающих по результатам обработки данных наступление определенных последствий (далее — системы реагирования);
- системы дистанционного мониторинга работоспособности перечисленных выше инструментов и технологий (далее — системы мониторинга).

Промышленный интернет вещей может добровольно применяться гражданами и организациями при осуществлении ими своей деятельности для систематического внутреннего контроля и мониторинга, анализа и прогнозирования состояния исполнения ими обязательных требований, предотвращения вреда охраняемым законом ценностям.

Применение для тех же целей промышленного интернета вещей контрольно-надзорными органами (далее – КНО) описано в дальнейших разделах.

1.2 Промышленный интернет вещей в контрольно-надзорной деятельности

Промышленный интернет вещей, применяемый в контрольно-надзорной деятельности (далее – КНД)[1], представляет собой:

- совокупность автоматических или автоматизированных средств измерения, передачи и обработки данных, систем реагирования и дистанционного мониторинга, обеспечивающих контрольно-надзорные органы достоверными сведениями относительно объектов контроля (надзора), представляющих опасность причинения вреда жизни, здоровью людей и иным охраняемым ценностям (далее – средства и системы интернета вещей в КНД, или просто средства и системы),
- используемых для целей контроля (надзора) в соответствие с утвержденными в установленном порядке правовыми актами, стандартами, регламентами (далее — правовая база).

Средства и системы могут устанавливаться как на объектах контроля (надзора) (далее также – проверяемые объекты, или объекты), так и вне их и могут принадлежать или эксплуатироваться гражданами и организациями (проверяемыми лицами), контрольно-надзорными органами или иными лицами.

Использование средств и систем промышленного интернета вещей в КНД в автоматическом режиме предполагает проведение измерений, передачу, обработку, выбор мер реагирования относительно объектов контроля (надзора) без ручного ввода, преобразования или

[1] Далее в документе, где это не допускает двусмысленной интерпретации, используется для краткости понятие «промышленный интернет вещей» или «интернет вещей».

интерпретации данных со стороны инспекторов и иных должностных лиц контрольно-надзорных органов.

Использование автоматизированных средств и систем промышленного интернета вещей в КНД в отличие от использования полностью автоматических средств и систем допускает элементы участия человека (проверяемых лиц, общественности, инспекторов и иных должностных лиц). Допускается активация (применение) средств измерения в ручном режиме в установленных регламентом случаях при условии, что измерение носит объективный характер, не производится ручного ввода, преобразования или интерпретации измеренных данных со стороны должностных лиц КНО.

К промышленному интернету вещей КНД в общем случае не относятся открытые источники сведений и системы общественного контроля, содержащие данные относительно ущерба или угрозы ущерба охраняемым ценностям (например, форумы, чаты, группы в социальных сетях, мобильные приложения класса «Активный гражданин» и др.) за исключением случаев, когда их фиксация и передача осуществляются автоматически (например, с помощью доверенного мобильного приложения, не допускающего ручную обработку и иное изменение измеренных и переданных в КНО данных).

Примерами средств измерения промышленного интернета вещей, применяемого в КНД, являются датчики температуры, давления, освещенности, приборы учета потребления, иные объективные измерительные системы, несущие информацию относительно ущерба или угрозы ущерба охраняемым ценностям. В качестве средств передачи могут использоваться открытые или закрытые каналы Интернет (интранет), иные общие или выделенные, частные или общего пользования средства и системы связи, работающие как по TCP\IP, так и по иным протоколам. Характерными системами реагирования являются системы оповещения об опасности, блокировки механических частей промышленных устройств, управления подачей электроэнергии, формирования начислений. В качестве средств обработки данных, как правило, используются информационные системы КНО (если это предусмотрено правовой базой – также и информационные системы проверяемых лиц), алгоритмы обработки данных в которых реализованы в соответствии с правовой базой.

На данный момент за рубежом органами государственного контроля активно реализуются проекты с использованием промышленного интернета вещей, направленные на раннее предупреждение стихийных бедствий, оптимизацию транспортных потоков, оптимизацию расхода электроэнергии при использовании кондиционеров и для уличного освещения и т.п. В России использование элементов промышленного интернета вещей[2] характерно для отдельных видов государственного постоянного надзора.

1.3 Принципы использования промышленного интернета вещей в КНД

Целевым состоянием использования промышленного интернета вещей в КНД является переход к полностью дистанционному контролю (надзору), который позволит:

- отказаться от массовых и дорогих для бюджета проверок и сократить штатную численность инспекторского состава, высвободившийся финансовый ресурс направить на увеличение заработной платы инспекторов и повышение их профессионального уровня и мотивации;
- снизить коррупционные риски в КНД за счёт перехода к использованию данных,

[2] Предусмотрено передача данных в государственные органы, однако не предусмотрена их автоматическая обработка.

полученных с применением измерительных приборов и обработанных в автоматическом режиме;

- снизить ущерб охраняемым законом ценностям за счёт использования автоматических систем реагирования на возникновение опасности;
- сократить административную нагрузку на проверяемых лиц.

Таким образом, внедрение промышленного интернета вещей в КНД производится согласно следующим принципам:

1. **Нет человека посередине**: измерение, передача, обработка, выбор мер реагирования относительно объектов контроля (надзора) производятся без участия людей. Не используется ручной ввод, преобразование или произвольная интерпретация данных со контрольно-надзорных органов.
2. **Не используемые данные не собираются и не хранятся**: не осуществляется сбор данных, которые не влияют на КНД, а собранные данные не хранятся за пределами сроков их использования.
3. **Включение данных интернета вещей в текущие регламенты КНО**: данные интернета вещей влияют на КНД исключительно посредством изменения оценок значений индикаторов и присвоенных категорий риска (классов опасности), влекущим за собой изменение состава применимых к проверяемому лицу обязательных требований, изменение порядка назначения и проведения проверок, осуществления постоянного надзора, мероприятий без взаимодействия с проверяемым лицом.
4. **Нет регламента – нет сбора данных**: конкретный состав собираемых данных, порядок их использования, их влияние на осуществление КНД должны быть определены в правовых актах.
5. **Добровольность применения проверяемыми лицами**: КНО не могут принуждать граждан и организации к переходу на использование интернета вещей, в том числе к покупке и (или) установке датчиков, устройств, программного обеспечения и иных средств измерения, передачи и обработки данных интернета вещей.
6. **Деперсонификация (анонимизация) данных:** все хранимые КНО данные интернета вещей должны пройти процедуру деперсонификации – информационные ресурсы КНО не должны содержать данные интернета вещей, позволяющих отнести эти данные к тем или иным объектам контроля, проверяемым и иным лицам. Принадлежность данных тем или иным объектам контроля, проверяемым и иным лицам устанавливается с помощью локальных (внутрисистемных) идентификаторов.

При реализации мероприятий по проектированию и внедрению промышленного интернета вещей в КНД контрольно-надзорные органы обеспечивают строгое соответствие указанным принципам. Для внедрения промышленного интернета вещей в КНД должны быть реализованы технические, нормативные правовые и организационные меры.

2 УРОВНИ ВНЕДРЕНИЯ ПРОМЫШЛЕННОГО ИНТЕРНЕТА ВЕЩЕЙ В КНД

Внедрение промышленного интернета вещей не является самодостаточной целью для КНО. Возможность и целесообразность внедрения различных элементов интернета вещей должна оцениваться для каждого вида контроля (надзора).

2.1 Высокий уровень

Высокий уровень внедрения промышленного интернета вещей в КНД предполагает использование всех перечисленных в п. 1.2. средств и систем промышленного интернета вещей в полностью автоматическом режиме, в том числе:

- средства измерения обеспечивают КНО возможность достоверно оценивать состояние объекта полностью удалённо и не допускают искажения или подмены результатов измерений (или внесенные изменения легко выявляются);
- измерение носит объективный характер, не допускается ручной ввод или преобразование измеренных данных, средства передачи не допускают изменения или подмены результатов измерений (или внесенные изменения легко выявляются);
- средства передачи обеспечивают синхронный режим работы (передачу в режиме реального времени);
- доступные КНО данные относительно объектов контроля (надзора), поступающие от средств измерений, однозначно связаны с опасностью причинения вреда жизни, здоровью людей и иным охраняемым ценностям, увязаны с моделью рисков и мерами реагирования;
- системы реагирования исключают необходимость личного участия должностных лиц КНО;
- протоколы передачи и форматы представления данных, используемые всеми средствами и системами промышленного интернета вещей, реализованы в соответствии с открытыми стандартами, поддержанными рынком;
- все используемые средства и системы промышленного интернета вещей доступны на конкурентном рынке и соответствуют открытым стандартам, поддержанным рынком.

2.2 Средний уровень

Средний уровень внедрения промышленного интернета вещей в контрольно-надзорную деятельность предполагает соответствие высокому уровню за исключением:

- допускается ручная активация (применение) средств измерения проверяемыми лицами и (или) общественностью (но не должностными лицами КНО), включая применение носимых (возимых) средств измерения, при условии, что измерение носит объективный характер, исключается ручной ввод или преобразование измеренных данных (или внесенные изменения легко выявляются);
- допускается отсутствие автоматических средств реагирования и необходимость личного участия должностных лиц КНО;
- допускается реализация протоколов передачи и форматов представления данных, используемых средствами и системами, в соответствии с полностью документированными спецификациями, не имеющими статуса открытого стандарта;
- допускается применение средств измерения промышленного интернета вещей, реализующих полностью документированные спецификации, не имеющие, возможно, статуса открытого стандарта.

2.3 Базовый уровень

Базовый уровень внедрения промышленного интернета вещей в КНД предполагает использование отдельных элементов интернета вещей:

- средства измерения обеспечивают КНО возможность достоверно оценивать состояние объекта полностью удалённо и не допускают искажения или подмены результатов измерений (или внесенные изменения легко выявляются);
- допускается ручная активация (применение) средств измерения проверяемыми лицами, общественностью, должностными лицами КНО, включая применение носимых (возимых)

средств измерения, при условии, что измерение носит объективный характер, исключается ручной ввод или преобразование измеренных данных и правовая база устанавливает меры ответственности применяющих средства измерения лиц за их применение не в соответствии с установленным регламентом;

- доступные КНО сведения относительно объектов контроля (надзора) однозначно связаны с опасностью причинения вреда жизни, здоровью людей и иным охраняемым ценностям, увязаны с моделью рисков и мерами реагирования;
- допускается отсутствие автоматических средств реагирования и необходимость личного участия должностных лиц КНО;
- средства обработки данных могут обеспечивать оценку состояния проверяемого объекта в режиме визуализации результатов измерений (обработки) для должностного лица КНО при условии, что критерии оценки и меры реагирования однозначно установлены.

3 ПЛАНИРОВАНИЕ ВНЕДРЕНИЯ ПРОМЫШЛЕНОГО ИНТЕРНЕТА ВЕЩЕЙ В КНД

Планирование внедрения промышленного интернета вещей в КНД осуществляется в следующем порядке.

3.1 Анализ обязательных требований и критериев риска

3.1.1 Анализ обязательных требований

Анализ обязательных требований должен быть направлен на выявление требований, относящихся к объективно измеримым характеристикам состояния объекта (например, уровень задымления в помещении, уровень шума в помещении, движение транспорта, изменение уровня воды в водоёме).

Для требований, соответствующих описанному критерию, следует оценить:

- характер ущерба охраняемым законом ценностям в случае нарушения обязательного требования;
- вероятность нанесения ущерба охраняемым законом ценностям в случае нарушения обязательного требования;
- допустимые сроки осуществления действий, обеспечивающих предотвращение либо снижение ущерба охраняемым законом ценностям (с момента выявления факта нарушения обязательного требования);
- содержание действий, обеспечивающих предотвращение либо снижение ущерба охраняемым законом ценностям, и возможность автоматизации таких действий (к числу автоматизируемых действий относятся, например, объявление о необходимости покинуть помещение, аварийная остановка неисправного механизма);
- наличие лиц, заинтересованных в предотвращении или снижении ущерба охраняемым законом ценностям достаточно, чтобы участвовать в финансировании соответствующих мер (например, собственник завода может быть достаточно заинтересован в предотвращении аварийных ситуаций, влекущих за собой необходимость приостанавливать производство до момента устранения последствий аварии).

3.1.2 Анализ критериев риска

В ходе анализа должны быть выявлены такие критерии риска, которые относятся к объективно измеримым характеристикам состояния объекта, при этом не регулируются обязательными требованиями (например, интенсивность вибрации механизма, уровень влажности в складских помещениях).

Для критериев, соответствующих описанному критерию, следует оценить:

- вероятность и ожидаемых срок нарушения обязательного требования в случае выявления соответствующих фактов;
- вероятность и ожидаемый срок нанесения ущерба охраняемым законом ценностям в случае выявления соответствующих фактов (оценивается с учётом вероятности нанесения ущерба охраняемым законом ценностям в случае нарушения обязательного требования, связанного с критерием риска, а также вероятности ожидаемого срока нарушения обязательного требования в случае выявления соответствующих фактов), характер ущерба;
- наличие лиц, заинтересованных в предотвращении или снижении ущерба охраняемым законом ценностям достаточно, чтобы участвовать в финансировании соответствующих мер.

3.2 Оценка издержек, связанных с внедрением промышленного интернета вещей

При оценке издержек, связанных с внедрением промышленного интернета вещей, следует оценить:

- наличие на рынке (на проверяемых объектах) средств измерения, позволяющих оценивать их состояние;
- затраты на установку средств измерения, позволяющих оценивать состояние проверяемых объектов;
- затраты на внедрение средств передачи данных: в потоковом режиме, в пакетном режиме;
- затраты на внедрение средств обработки данных, обеспечивающих функционирование систем реагирования, агрегацию и передачу данных для анализа, визуализацию состояния проверяемого объекта;
- затраты на внедрение систем реагирования, обеспечивающих предотвращение или сокращение ущерба охраняемым законом ценностям;
- затраты на внедрение систем обеспечения информационной безопасности: исключающих риск фальсификации данных, утечки данных, выведения из строя средств измерения и систем реагирования (для проведения указанной оценки должна быть сформирована модель угроз), деперсонификации данных;
- затраты на внедрение систем мониторинга работоспособности средств измерения, передачи, обработки, обеспечения информационной безопасности, систем реагирования: в различных конфигурациях;
- источники сокращения издержек для проверяемых лиц, для иных заинтересованных лиц, для государственного бюджета в случае внедрения элементов промышленного интернета вещей: в различных конфигурациях.

Оценка издержек внедрения промышленного интернета вещей в КНД должна учитывать, что обеспечение абсолютно доверенного характера результатов измерения относительно объектов контроля (надзора), как правило, носит дорогостоящий характер, что может заблокировать его применение. Должен быть обеспечен уровень доверия к средствам измерения и передачи, которые обеспечат КНО возможностью достоверно оценивать состояние объекта. Возможность искажения или подмены результатов измерений должна компенсироваться мерами организационного и правового характера, в частности, мерами ответственности за искажения результатов измерений, проверками со стороны КНО, страхованием ответственности проверяемых лиц за искажение результатов измерений, механизмы саморегулирования и добровольного аудита и др.

Следует свести к разумному минимуму выдвижение требований по применению исключительно сертифицированных (например, по определенным классам защищенности) средств и систем, опираясь преимущественно но средства и системы промышленного интернета вещей, имеющие широкое распространение и низкую цену приобретения и эксплуатации, и отказываясь

от сбора, передачи и хранения избыточного объема данных, в том числе содержащих персональные данные или различные тайны (коммерческая, налоговая и др.).

3.3 Моделирование целевого состояния внедрения промышленного интернета вещей

Моделирование целевого состояния внедрения промышленного интернета вещей предполагает:

- определение целевой конфигурации элементов промышленного интернета вещей (см. раздел 4);
- определение порядка использования промышленного интернета вещей (см. раздел 5);
- выбор организационного решения при внедрении промышленного интернета вещей (см. раздел 6).

3.4 Внесение изменений в НПА

В нормативных правовых актах в соответствующей сфере должны быть отражены:

- целевое состояние внедрения промышленного интернета вещей – требования к используемым средствам измерения, передачи и обработки данных, средствам информационной безопасности, системам реагирования и мониторинга работоспособности указанных элементов;
- обязательности либо необязательность каждого из элементов промышленного интернета вещей, последствия отказа от внедрения необязательных элементов для проверяемых лиц (например, помещение в более высокую группу риска, сохранение практики выездных проверок);
- порядок обработки сведений, полученных с использованием промышленного интернета вещей: требование раскрывать сведения для всеобщего доступа в машиночитаемом виде (например, сведения о состоянии окружающей среды) либо, напротив, требования по защите сведений от несанкционированного доступа (например, данные, составляющие коммерческую тайну);
- требования к структуре и содержанию сведений, передаваемых в КНО, а также к порядку их передачи.
- ответственность за фальсификацию данных, а также выведение из строя элементов промышленного интернета вещей.

4 ЦЕЛЕВАЯ КОНФИГУРАЦИЯ ЭЛЕМЕНТОВ ПРОМЫШЛЕННОГО ИНТЕРНЕТА ВЕЩЕЙ

Критерии для определения целевой конфигурации элементов промышленного интернета вещей приведены в таблице 1.

Табл. 1. Определения целевой конфигурации элементов промышленного интернета вещей.

№	Характеристики элемента	Определяющие факторы
1.	Средства измерения: точность, защищённость.	Характер и вероятность ущерба охраняемым законом ценностям в случае изменения измеряемых характеристик объекта.
2.	Средства передачи данных: потоковая, пакетная передача данных,	Характер и вероятность ущерба охраняемым законом ценностям в случае изменения

	защищённость.	измеряемых характеристик объекта, допустимые сроки осуществления действий, обеспечивающих предотвращение либо снижение ущерба охраняемым законом ценностям.
3.	Системы реагирования: автоматические, полуавтоматические, отсутствует необходимость внедрения.	Характер и вероятность ущерба охраняемым законом ценностям в случае изменения измеряемых характеристик объекта, допустимые сроки осуществления действий, обеспечивающих предотвращение либо снижение ущерба охраняемым законом ценностям.
4.	Средства обработки данных: управление системами реагирования, агрегация и анализ данных, визуализация состояния проверяемого объекта.	Характер, вероятность, ожидаемые сроки нанесения ущерба охраняемым законом ценностям в случае изменения измеряемых характеристик объекта. Целесообразность внедрения систем реагирования.
5.	Системы реагирования: автоматические, полуавтоматические, отсутствует необходимость внедрения.	Характер и вероятность ущерба охраняемым законом ценностям в случае изменения измеряемых характеристик объекта, допустимые сроки осуществления действий, обеспечивающих предотвращение либо снижение ущерба охраняемым законом ценностям.
6.	Системы обеспечения информационной безопасности	Характер и вероятность ущерба охраняемым законом ценностям в случае изменения измеряемых характеристик объекта, допустимые сроки осуществления действий, обеспечивающих предотвращение либо снижение ущерба охраняемым законом ценностям. Специфика модели угроз.
7.	Системы мониторинга работоспособности элементов	Конфигурация перечисленных выше элементов. Характер и вероятность ущерба охраняемым законом ценностям в случае изменения измеряемых характеристик объекта, допустимые сроки осуществления действий, обеспечивающих предотвращение либо снижение ущерба охраняемым законом ценностям. Специфика модели угроз.

5 ИСПОЛЬЗОВАНИЕ ПРОМЫШЛЕННОГО ИНТЕРНЕТА ВЕЩЕЙ В РАМКАХ РАЗЛИЧНЫХ ВИДОВ КОНТРОЛЬНО-НАДЗОРНЫХ МЕРОПРИЯТИЙ

В зависимости от характера сведений, полученных с применением промышленного интернета вещей, предусматриваются различные подходы к их использованию.

5.1 Плановые и внеплановые проверки

В случаях, когда решение о выполнении либо невыполнении какого-либо обязательного требования к объекту проверки может быть принято на основании сведений, полученных с использованием промышленного интернета вещей, процедуру проверки соответствия такому требованию следует осуществлять в дистанционном режиме.

Соответствующий порядок проверки соответствия требованию (дистанционно, на основании показаний средств измерения) должен быть установлен в нормативном правовом акте и включать в себя требования к технологическому и организационному обеспечению сбора, хранения и передачи необходимых сведений, а также мониторинга работоспособности средств измерения и передачи данных.

5.2 Постоянный надзор

Использование сведений, полученных с применением средств в рамках постоянного надзора на настоящий момент является наиболее распространённым примером использования таких сведений.

К ключевым направлениям оптимизации мероприятий постоянного надзора с использованием промышленного интернета вещей следует отнести внедрение автоматизированных систем мониторинга работоспособности используемых технологических решений, а также расширение использования автоматических и полуавтоматических систем реагирования — для сокращения административной нагрузки на проверяемых лиц, оптимизации расходов КНО, исключения зависимости риска нанесения ущерба охраняемым законом ценности от человеческого фактора, снижения вероятности нанесения такого ущерба в конечном итоге;

Порядок использования промышленного интернета вещей при осуществлении постоянного надзора должен быть установлен в нормативном правовом акте и включать в себя требования к технологическому и организационному обеспечению сбора, хранения и передачи необходимых сведений, работы автоматических и полуавтоматических систем реагирования, а также мониторинга работоспособности используемых технологических решений.

5.3 Мероприятия без взаимодействия с проверяемым лицом и профилактические мероприятия

В случаях, когда реализация мер по обеспечению достоверности данных промышленного интернета вещей является дорогостоящей или сложно осуществимой в силу каких-либо иных причин, полученные таким образом сведения не могут быть использованы непосредственно в ходе проверок или мероприятий постоянного надзора, однако могут применяться в рамках мероприятий без взаимодействия с проверяемым лицом (в этом случае полученные сведения могут служить основанием для назначения внеплановой проверки), а также в рамках профилактических мероприятий (в этом случае полученные сведения могут служить основанием для направления проверяемому лицу предостережения).

В этом случае также порядок использования промышленного интернета вещей должен быть установлен в нормативном правовом акте и включать в себя основания для назначения внеплановой проверки, основания для направления предостережения, требования к технологическому и организационному обеспечению сбора, хранения и передачи необходимых сведений, а также мониторинга работоспособности средств измерения.

5.4 Оценка значений индикаторов риска

В случаях, когда решение о выполнении либо невыполнении какого-либо обязательного требования к объекту проверки не может быть принято на основании сведений, полученных с применением промышленного интернета вещей, однако указанным образом могут быть получены (накоплены) сведения, характеризующие вероятность нарушения обязательного требования, такие сведения следует использовать для оценки значений индикаторов риска и динамического управления моделью рисков.

В этом случае также порядок использования промышленного интернета вещей должен быть установлен в нормативном правовом акте и включать в себя порядок оценки значений индикаторов риска и присвоений категорий риска, требования к технологическому и организационному обеспечению сбора, хранения и передачи необходимых сведений, а также мониторинга работоспособности средств измерения.

6 ОРГАНИЗАЦИОННЫЕ РЕШЕНИЯ ПРИ ВНЕДРЕНИИ ПРОМЫШЛЕННОГО ИНТЕРНЕТА ВЕЩЕЙ

6.1 Сценарии финансирования

Существует три сценария финансирования внедрения промышленного интернета вещей:

- средства и системы промышленного и интернета вещей финансируются за счёт бюджетных средств и принадлежат КНО. Приобретение, установка и обслуживание осуществляются самостоятельно КНО или в рамках государственного заказа;
- средства и системы промышленного интернета вещей финансируются в рамках концессионных соглашений. Приобретение, установка и обслуживание осуществляются коммерческими структурами в рамках концессионных соглашений;
- средства и системы промышленного и интернета вещей финансируются за счёт проверяемых лиц. Приобретение, установка и обслуживание осуществляется проверяемыми лицами за собственные средства или на условиях аренды или аутсорсинга.

6.2 Выбор сценария финансирования

Выбор сценария оснащения проверяемых объектов средствами и системами промышленного и интернета вещей для каждого конкретного вида контроля (надзора) должен осуществляться с учётом результатов оценки издержек, а также следующих соображений:

- Финансирование внедрения промышленного интернета вещей за счёт бюджетных средств не в полной мере способствует снижению издержек КНО и в ограниченной степени влияет на развитие рынка решений промышленного интернета вещей. Описанный сценарий целесообразно использовать в случаях, когда внедрение промышленного интернета вещей позволяет существенно снизить вероятность и масштабы нанесения ущерба охраняемым законом ценностям, при этом лица, заинтересованные в финансировании таких внедрений и обладающие соответствующим ресурсом, отсутствуют.
- Финансирование внедрения промышленного интернета вещей в рамках концессионных соглашений уместно при наличии заинтересованности коммерческих структур в развитии

промышленного интернета вещей в конкретной отрасли, а также принципиальной допустимости использования полученных сведений на усмотрение собственника средств промышленного интернета вещей.

- Финансирование внедрения промышленного интернета вещей за счёт проверяемых лиц (на добровольной основе или с установлением обязательности внедрения соответствующих технологий) допустимо исключительно в тех случаях, когда такое решение не приводит к повышению административной нагрузки на проверяемых лиц.

6.3 Повторное использование данных промышленного интернета вещей

Данные, полученные с использованием промышленного интернета вещей, могут представлять ценность для коммерческого сектора и общества в целом, особенно в том случае, если предусмотрена их агрегация (по проверяемым объектам, по отраслям). В то же время, разрозненные сведения, по отдельности не подлежащие защите (персональные данные, различные виды тайн), в совокупности могут приобретать свойства, обуславливающие необходимость их защиты. В каждом случае внедрения средств и систем интернета вещей в КНД следует рассматривать и устанавливать нормативно порядок раскрытия (защиты) получаемых данных в машиночитаемой форме, допустимые сценарии агрегации получаемых данных, процедуры их деперсонификации и исключения возможности их неавторизованного сопоставления и анализа.

6.4 Информационное взаимодействие при внедрении промышленного интернета вещей в КНД

Архитектурные решения, используемые при внедрении промышленного интернета вещей в КНД, предусматривают взаимодействие следующих систем:

- информационные системы проверяемого лица;
- информационные системы собственника средств измерения и передачи данных;
- государственные и негосударственные ЦОД и платформы промышленного интернета вещей, в том числе облачные;
- ВИС КНО.

К общим принципам взаимодействия относятся:

- взаимодействие между государственными информационными системами, включая платформенные решения и облачные ЦОД, осуществляется посредством СМЭВ;
- порядок взаимодействия, включая требования по безопасности взаимодействия, должен быть установлен в нормативных правовых актах;
- доступ к государственным ЦОД и платформенным решениям должен осуществляться на недискриминационной основе.

7 ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

Планы внедрения промышленного интернета вещей в КНД, соответствующие положениям раздела 3 настоящего документа, а также отчётность о результатах выполнения мероприятий плана, представляются КНО в Минкомсвязи России.

Список

на рассылку письма от _____ №_____

№	Наименование ведомства	Адрес
1.	Аналитический центр при Правительстве Российской Федерации	107078, Москва проспект Академика Сахарова, 12
2.	Министерство внутренних дел Российской Федерации	119049, г. Москва, ул. Житная, д.16
3.	Министерство по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий	109012, г. Москва, Театральный проезд, д.3
4.	Министерство труда и социальной защиты Российской Федерации	127994, ГСП-4, г. Москва, ул. Ильинка, д. 21
5.	Министерство экономического развития Российской Федерации	125993, г. Москва, ул. 1-я Тверская-Ямская, д.1, 3
6.	Министерство юстиции Российской Федерации	119991, г. Москва, ул. Житная, д. 14
7.	Федеральная служба по ветеринарному и фитосанитарному надзору	107139, г. Москва, Орликов переулок, д. 1/11
8.	Федеральная служба по надзору в сфере защиты прав потребителей и благополучия человека	127994, г. Москва, Вадковский пер., дом 18, строение 5 и 7
9.	Федеральная служба по надзору в сфере здравоохранения	109074, г. Москва, Славянская площадь, д. 4, строение 1
10.	Федеральная служба по надзору в сфере природопользования	123995, г. Москва, ул. Большая Грузинская, д. 4/6
11.	Федеральная служба по надзору в сфере транспорта	125993, г. Москва, Ленинградский проспект, дом 37, корп.1
12.	Федеральная служба по труду и занятости	109012, г. Москва, Биржевая площадь, д. 1
13.	Федеральная служба по экологическому, технологическому и атомному надзору	105066, г. Москва, ул. Александра Лукьянова, д. 4, к. 8
14.	Федеральная антимонопольная служба	123995, г. Москва, ул. Садовая-Кудринская, д.11
15.	Федеральная налоговая служба	127381, г. Москва, Неглинная ул., д. 23
16.	Федеральная таможенная служба	121087, г. Москва, ул. Новозаводская, д. 11/5
17.	Генеральная прокуратура Российской Федерации	125993, г. Москва, ГСП-у, ул. Большая Дмитровка, 15а