АРСИБ

АССОЦИАЦИЯ РУКОВОДИТЕЛЕЙ СЛУЖБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

«Вопросы стандартизации в ИБ АСУ ТП»

Чучаев Сергей Викторович
Руководитель комитета по экспертизе АРСИБ

Ассоциация руководителей служб ИБ

Наши основные цели:

- Содействие развитию информационного общества за счет эффективного использования технологий и средств информационной безопасности во всех сферах деловой и социальной активности;
- Повышение престижа служб информационной безопасности (далее – «ИБ») и деятельности их руководителей в бизнесе и обществе;
- Обеспечение взаимодействия руководителей служб ИБ коммерческих и государственных организаций на общенациональном уровне и формирование российского сообщества руководителей служб ИБ.

Задачи, которые мы ставим перед собой сегодня:

- Развитие клубного движения руководителей ИБ;
- Формирование и выражение консолидированного мнения и позиций профессионалов в области ИБ;
- Взаимодействие с регуляторами по вопросам ИБ и воздействие на вопросы законодательного обеспечения ИБ;
- Популяризация идей и профессий в области информационной безопасности;
- Повышение уровня квалификации и компетенций специалистов и руководителей информационной безопасности;
- Создание в интересах членов собственного центра информационной и сетевой безопасности (типа CSIRT\CERT) и установление контактов с международными организациями;
- Взаимодействие с профильными ассоциациями.

Комитет по экпертизе

Основная цель:
— повышение качества нормативного регулирования членов АРСИБ и сторонних организаций в области ИБ

Функции:
— участие в разработке национальных, отраслевых и корпоративных стандартов в области ИБ;
— экспертиза проектов стандартов различного уровня в области ИБ;

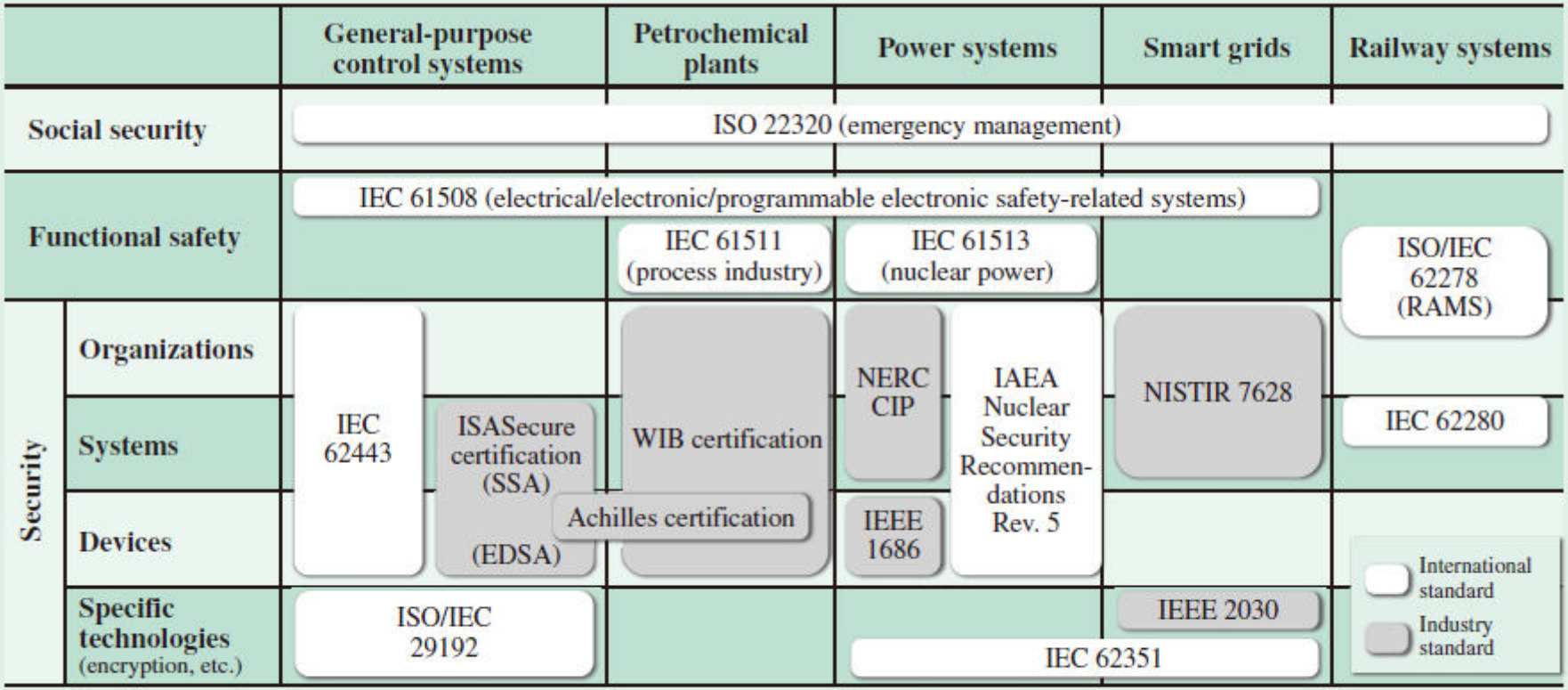
Закон или стандарт

- **Закон –** основной юридический акт, который формирует неотъемлемые нормы права, являющиеся обязательными к исполнению.

- **Стандарт –** документ, в котором для добровольного (если иное не установлено законодательно) и многократного применения устанавливаются общие характеристики объекта стандартизации, а также правила и общие принципы в отношении объекта стандартизации

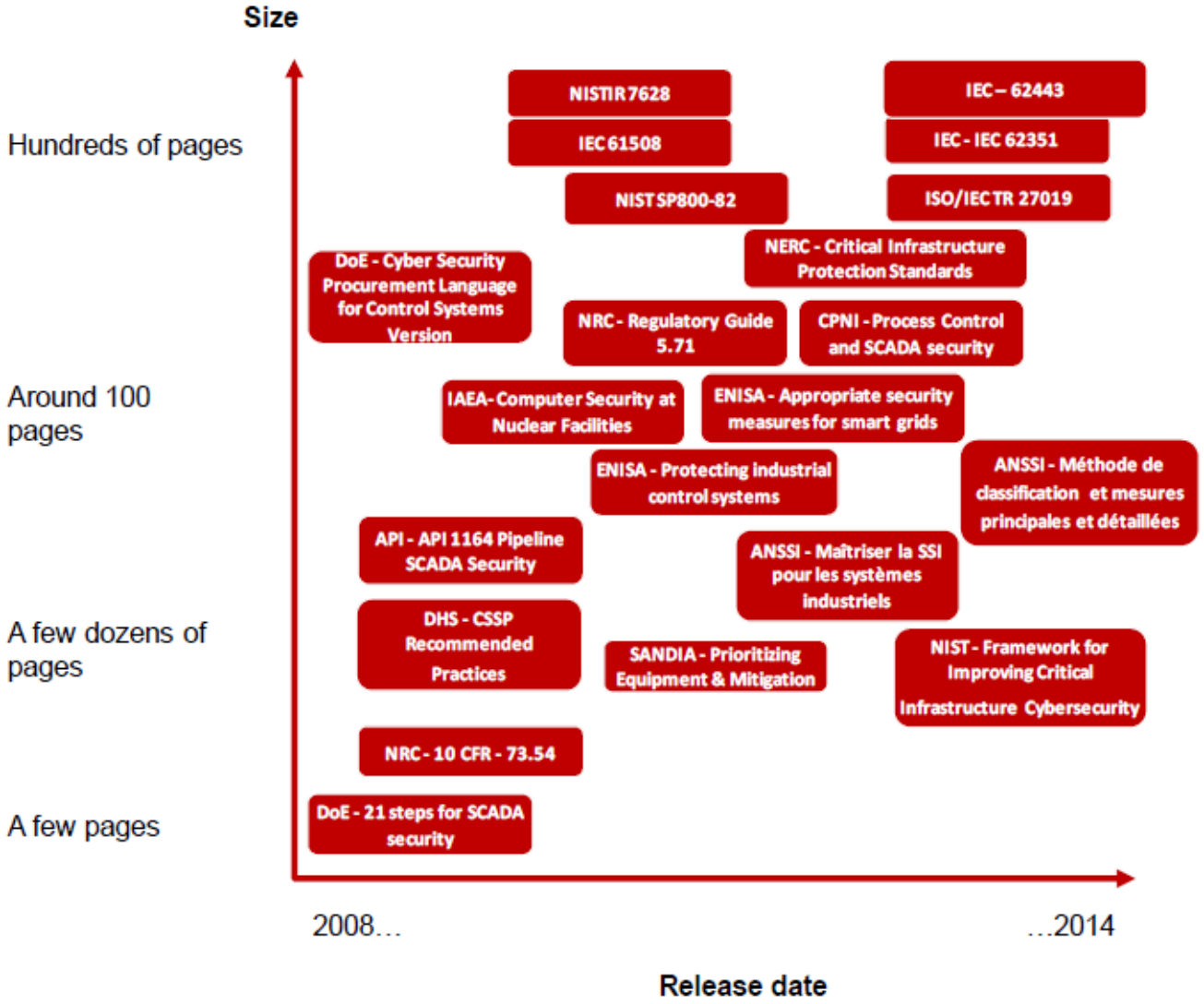
Объекты стандартизации

Зарубежные документы по безопасности АСУ ТП

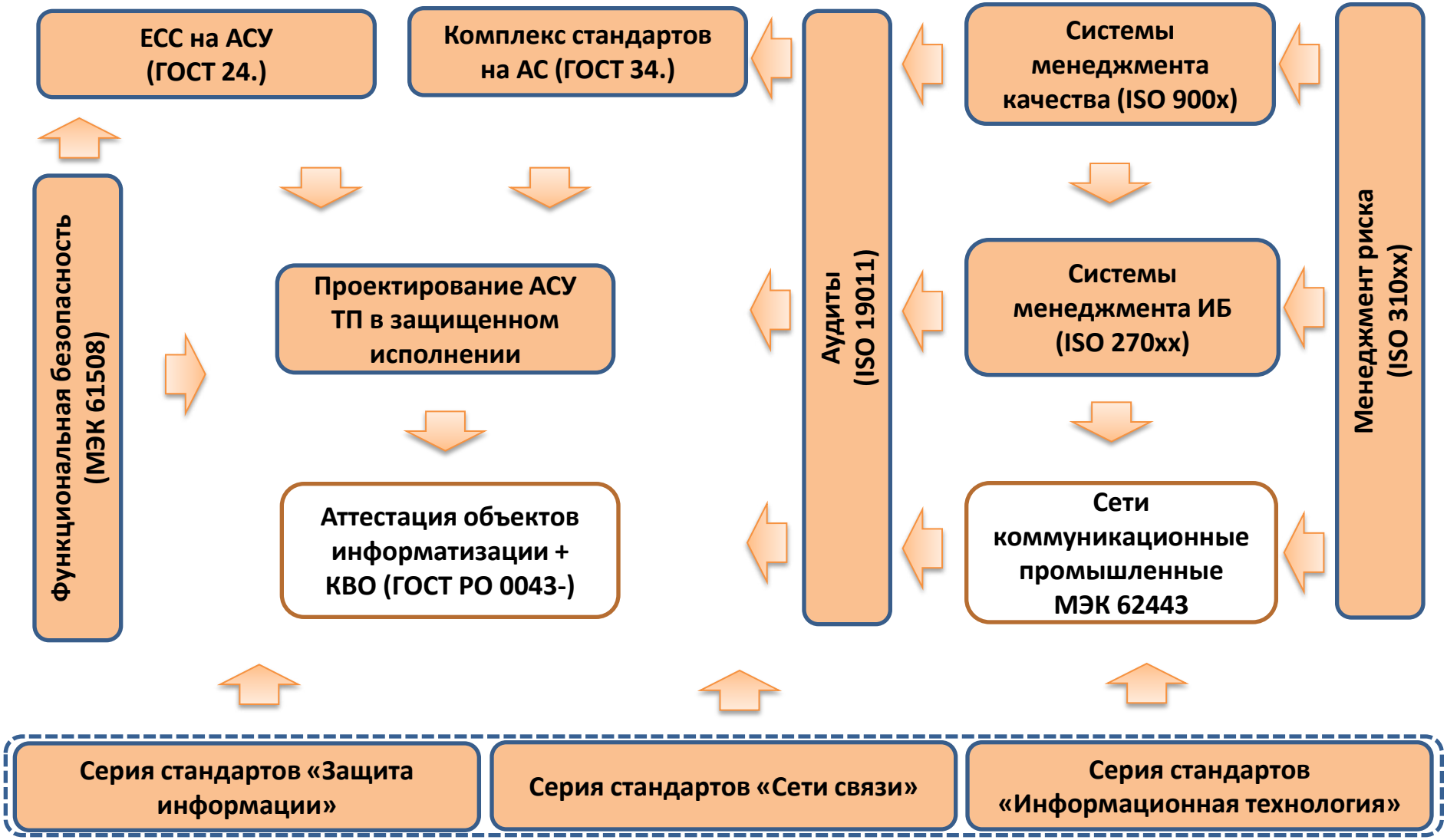


SSA: System Security Assurance EDSA: Embedded Device Security Assurance NERC: North American Electric Reliability Corporation
CIP: Critical Infrastructure Protection IAEA: International Atomic Energy Agency NISTIR: National Institute of Standards and Technology Interagency Report
RAMS: reliability, availability, maintainability and safety

Зарубежные документы по безопасности АСУ ТП



Стандарты обеспечения ИБ АСУ ТП



Законодательная и нормативная база национальной системы стандартизации

- **Конституция Российской Федерации (статья 71 пункт «р»)**
- **Международные соглашения, регулирующие вопросы стандартизации**
- ~~**Федеральный закон "О техническом регулировании" от 22 декабря 2002 года №184-ФЗ**~~
- **Федеральный закон «О стандартизации» от 29.06.2015 №162-ФЗ, определивший правовые основы стандартизации в Российской Федерации, участников работ по стандартизации, правила разработки и добровольность применения стандартов**
- **Нормативные правовые акты Правительства Российской Федерации по вопросам стандартизации, в том числе Концепция развития национальной системы стандартизации РФ в период до 2020 года, одобренная распоряжением Правительства РФ от 24.09.2012 г., № 1762-р, установившая стратегические цели, принципы, задачи и направления развития национальной системы стандартизации в период до 2020 года**
- **Документы в области стандартизации, используемые на территории РФ**

Национальная система стандартизации. Структура НСС

Федеральный информационный фонд технических регламентов и стандартов

- Документы национальной системы стандартизации
- Документы национальной системы стандартизации
- Документы национальной системы стандартизации

Федеральный орган исполнительной власти, осуществляющий функции по выработке государственной политики и нормативно-правовому регулированию области стандартизации

Национальный орган Российской Федерации по стандартизации

Научные организации по стандартизации

Общественный совет

Межотраслевые (отраслевые) советы

Федеральные органы исполнительной власти, ГК «Росатом», в пределах их полномочий в области стандартизации

СП

ТК (по стандартизации, по ОК)

Проектные технические комитеты

Организации и другие субъекты, деятельность которых связана с работами области стандартизации

Службы по стандартизации организаций и предприятий

СТО, ТУ

Структуры, определённые в проекте ФЗ «О стандартизации»

Структуры, определённые в 184-ФЗ, ГОСТ Р 1.0-2012

Структуры, поименованные в ПП 1762-р от 24.09.2012 «Концепция развития НСС до 2020 г»

Организация работ по стандартизации*

1. Организация разработки национальных стандартов

* В рамках презентации приведены основные шаги по планированию разработки и разработке национальных стандартов. Более подробную информацию можно получить в соответствующих НПА ФОИВ и национальных стандартах

Организация работ по стандартизации

2. Разработка национального стандарта

ГОСТ Р 1.2-2014

Экспертиза проектов национальных стандартов

ГОСТ Р 1.6-2013

Организация работ по стандартизации

2. Разработка национального стандарта (продолжение)

Разработчик национального стандарта

Формирует сводку отзывов, дорабатывает стандарт и организует публичные обсуждения

Направляет окончательную редакцию

Направляет уведомление об окончании публичных обсуждений

Национальный орган Российской Федерации по стандартизации

Размещает информацию

Сеть Интернет, ИУС печатный орган ФОИВ по ТР

Технический комитет

Направляет на утверждение*

Национальный орган Российской Федерации по стандартизации

Утверждает

национальный стандарт

ГОСТ Р 1.2-2014

Кто в России «делает» стандарты в области ИБ и связанных областях

Серия стандарта	Технический комитет по стандартизации
Серия «Защита информации»	ТК 362 – Защита информации (ГНИИИ ПТЗИ ФСТЭК России)
Серия 62443	ТК 306 – Измерения и управление в промышленных процессах (Институт проблем управления им.В.А.Трапезникова РАН)
Серия 61508	ТК 58 – функциональная безопасность (ФБУ «КВФ «Интерстандарт»)
27000 – 27005 (искл. 27002)	ТК 362
27002, 27011, 27013	ТК 22 – информационные технологии (Институт проблем информатики (ИПИ РАН)
Серия «ИТ»	ТК 22, ТК 362

Программа стандартизации на 2017 год

ТК 362 – Защита информации		
Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования	ГНИИ ПТЗИ ФСТЭК, ООО «ЦБИ»	10.2017
Защита информации. Разработка защищенного программного обеспечения. Общие положения	НПО Эшелон»	10.2017
Защита информации. Требования к органам по аттестации объектов информатизации	ГНИИ ПТЗИ ФСТЭК	10.2017
Защита информации. Документация по технической защите информации на объекте информатизации. Общие положения	ГНИИ ПТЗИ ФСТЭК	10.2017
Защита информации. Информационные системы. Угрозы безопасности информации. Общие положения	ГНИИ ПТЗИ ФСТЭК, ООО «ЦБИ», ООО НПФ «Кристалл»	10.2017
Защита информации. Основные термины и определения. Взамен ГОСТ Р 50922-2006	ГНИИ ПТЗИ ФСТЭК, ООО НПФ «Кристалл»	10.2017
Защита информации. Техника защиты информации. Номенклатура показателей качества. Взамен ГОСТ Р 52447-2005	ГНИИ ПТЗИ ФСТЭК	10.2017
Защита информации. Требования по защите информации, обрабатываемой с использованием технологий «облачных вычислений». Общие положения	ГНИИ ПТЗИ ФСТЭК	10.2017
Защита информации. Уязвимости информационных систем. Содержание и порядок выполнения работ по выявлению и оценке уязвимостей информационных систем	ООО «ЦБИ»	10.2017
Информационная технология. Методы и средства обеспечения безопасности. Детализация анализа уязвимостей программного обеспечения в соответствии с ГОСТ Р ИСО/МЭК 15408 и ГОСТ Р ИСО/МЭК 18045. Часть 1. Часть 2	ООО «ЦБИ»	10.2017
Информационная технология. Методы и средства обеспечения безопасности. Руководство по безопасности	ООО «ЦБИ»	10.2017

Программа стандартизации на 2017 год

ТК 362 – Защита информации		
Защита информации. Идентификация и аутентификация. Общие положения Разработка ГОСТ Р	ЗАО «Алладин Р.Д.», ГНИИ ПТЗИ ФСТЭК	09.2018
Защита информации. Разработка безопасного программного обеспечения. Угрозы безопасности информации при разработке программного обеспечения	ЗАО «НПО Эшелон», ГНИИ ПТЗИ ФСТЭК	09.2018
Защита информации. Управление потоками информации в информационной системе. Форматы обмена метками конфиденциальности Разработка ГОСТ Р	ОАО «НПО «РусБИТех», ГНИИ ПТЗИ ФСТЭК	09.2018
Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента Пересмотр ГОСТ Р ИСО/МЭК 27001-2006 Частичное применение ISO/IEC 27001:2013	ГНИИ ПТЗИ ФСТЭК, ООО «ЦБИ» (?)	09.2018
ТК 306 - Измерения и управление в промышленных процессах		
Защищенность (кибербезопасность) систем контроля и промышленной автоматики. Часть 2-3. Управление исправлениями в среде систем контроля и промышленной автоматики Прямое применение IEC/TR 62443-2-3(2015). (гармонизация)	Не определен	11.2018
Защищенность (кибербезопасность) систем контроля и промышленной автоматики. Часть 2-4. Требования к программе защищенности (кибербезопасности) для поставщиков услуг для систем контроля и промышленной автоматики Прямое применение IEC 62443-2-4(2015). (гармонизация)	Не определен	11.2018

СПАСИБО ЗА ВНИМАНИЕ

Чучаев Сергей Викторович
e-mail: S.Chuchaev@gmail.com
телефон: +7 (926) 222-42-18