ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО/МЭК 27019— 2021

Информационные технологии

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Меры обеспечения информационной безопасности в энергетике (неатомной)

(ISO/IEC 27019:2017, Information technology — Security techniques — Information security controls for the energy utility industry, IDT)

Издание официальное

Москва
Стандартинформ
2021

Предисловие

1 ПОДГОТОВЛЕН Федеральным государственным учреждением «Федеральный исследовательский центр «Информатика и управление» Российской академии наук» (ФИЦ ИУ РАН), Обществом с ограниченной ответственностью «Информационно-аналитический вычислительный центр» (ООО ИАВЦ) и Федеральным бюджетным учреждением «Научно-технический центр Энергобезопасность» (ФБУ «НТЦ Энергобезопасность») на основе собственного перевода на русский язык англоязычной версии стандарта, указанного в пункте 4

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 022 «Информационные технологии»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 20 мая 2021 г. № 411-ст

4 Настоящий стандарт идентичен международному стандарту ИСО/МЭК 27019:2017 «Информационные технологии. Методы и средства обеспечения безопасности. Меры обеспечения информационной безопасности в энергетике» (ISO/IEC 27019:2017 «Information technology — Security techniques — Information security controls for the energy utility industry», IDT).

ИСО/МЭК 27019 разработан подкомитетом ПК 27 «Методы и средства обеспечения безопасности ИТ» Совместного технического комитета СТК 1 «Информационные технологии» Международной организации по стандартизации (ИСО) и Международной электротехнической комиссии (МЭК).

Наименование настоящего стандарта изменено относительно наименования указанного международного стандарта для приведения в соответствие с ГОСТ Р 1.5—2012 (пункт 3.5).

При применении настоящего стандарта рекомендуется использовать вместо ссылочных международных стандартов соответствующие им национальные стандарты, сведения о которых приведены в дополнительном приложении ДА.

Дополнительные сноски в тесте стандарта, выделенные курсивом, приведены для разъяснения текста оригинала

5 ВВЕДЕН ВПЕРВЫЕ

6 Некоторые положения международного стандарта, указанного в пункте 4, могут являться объектом патентных прав. Международная организация по стандартизации (ИСО) и Международная электротехническая комиссия (МЭК) не несут ответственности за идентификацию подобных патентных прав

Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (www.gost.ru)

Содержание

Введение

0.1 Предыстория и контекст

Настоящий стандарт содержит руководящие принципы, основанные на ИСО/МЭК 27002:2013, для управления информационной безопасностью применительно к системам управления технологическими процессами, используемым в энергетической отрасли. Целью настоящего стандарта является распространение содержания ИСО/МЭК 27002:2013 на область систем управления технологическими процессами и технологий автоматизации, что позволит предприятиям энергетики внедрить типовую и учитывающую отраслевую специфику систему менеджмента информационной безопасности (СМИБ), которая соответствует ИСО/МЭК 27001:2013 и распространяется от бизнеса до уровня управления технологическими процессами.

В дополнение к целям и мерам обеспечения безопасности, изложенным в ИСО/МЭК 27002:2013, к системам управления технологическими процессами, которые используются энергетическими компаниями и поставщиками энергии, предъявляются дополнительные особые требования. По сравнению с традиционными средами — информационно-телекоммуникационными активами (ICT)[1)] [например, офисными информационными технологиями (ИТ), системами торговли электрической энергией] — существуют фундаментальные и существенные различия в отношении разработки, эксплуатации, ремонта, технического обслуживания и условий эксплуатации систем управления технологическими процессами. Кроме того, технологические процессы, упомянутые в настоящем стандарте, могут представлять собой неотъемлемые компоненты критически важных инфраструктур[2)]. Следовательно, это означает, что они необходимы для безопасного и надежного функционирования данных инфраструктур. Эти различия и особенности должны быть должным образом учтены в процессах управления системами управления технологическими процессами, что является обоснованием их отдельного рассмотрения в рамках комплекса стандартов серии ИСО/МЭК 27000.

С точки зрения проектирования и функционирования системы управления технологическими процессами, используемые в энергетике, фактически являются системами обработки информации. Они собирают технологические данные и контролируют состояние физических процессов с помощью датчиков. Затем эти данные обрабатываются, и выполняемые действия регулируются с помощью исполнительных механизмов. Управление и регулирование осуществляется автоматически, но при этом возможно ручное вмешательство обслуживающего персонала. Таким образом, информация и системы обработки информации являются необходимой частью оперативных процессов в энергетике. Из этого следует важность того, чтобы соответствующие меры защиты информации применялись таким же образом, как и в отношении других организационных подразделений.

Программные и аппаратные компоненты (например, программируемая логика), основанные на стандартной технологии ICT, все чаще используются в средах управления технологическими процессами и также рассматриваются в настоящем стандарте. Кроме того, системы управления технологическими процессами в энергетическом секторе все больше взаимосвязаны и образуют сложные системы. Риски, связанные с этим направлением, должны учитываться при оценке рисков.

Информация и системы обработки информации в средах управления технологическими процессами также подвергаются все большему числу угроз и уязвимостей. Поэтому крайне важно, чтобы в области управления технологическими процессами в энергетике была обеспечена адекватная информационная безопасность за счет внедрения и постоянного совершенствования СМИБ в соответствии с ИСО/МЭК 27001:2013.

Эффективное обеспечение ИБ в области управления технологическими процессами в энергетическом секторе может быть достигнута путем установления, внедрения, мониторинга, пересмотра и, при необходимости, совершенствования применимых мер, изложенных в настоящем стандарте, для достижения конкретных целей безопасности и бизнеса организации. Здесь важно уделить отдельное

---

1) Далее по тексту введено сокращение ICT.

2) См. также Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», предусматривающий необходимость разработки модели угроз безопасности информации и соответствующих методов защиты для объектов критической информационной инфраструктуры.

внимание особой роли энергосбытовых компаний в обществе и экономическую необходимость гарантированного и надежного энергоснабжения. В конечном итоге общий успех кибербезопасности энергетических отраслей основывается на совместных усилиях всех заинтересованных сторон (производителей, поставщиков, потребителей и т. д.).

0.2 Положения по безопасности для систем управления технологическими процессами, используемых энергетическими компаниями

Положения по общей и всесторонней структуре ИБ для области управления технологическими процессами в энергетике опирается на несколько основных требований:

a) потребители ожидают гарантированного и надежного энергоснабжения;

b) нормативно-правовые требования обуславливают необходимость безопасной, надежной и гарантированной работы систем энергоснабжения;

c) поставщики энергии требуют ИБ для защиты своих деловых интересов, удовлетворения потребностей потребителей и соблюдения правовых норм.

0.3 Требования по информационной безопасности

Важно, чтобы энергетические компании определили свои требования по безопасности. Существует три основных источника требований по безопасности:

a) результаты оценки рисков организации с учетом общих бизнес-стратегий и целей организации. С помощью оценки рисков выявляются источники рисков и события, оцениваются потенциальные последствия и вероятность возникновения рисков;

b) требования, вытекающие из федеральных законов и подзаконных актов, распоряжений и договоров, которые должны быть выполнены организацией, а также социально-культурных потребностей. Конкретные примеры включают обеспечение надежного, эффективного и безопасного энергоснабжения, также как и надежное выполнение требований нерегулируемого энергетического рынка, в частности надежную и безопасную передачу данных третьим лицам;

c) конкретные принципы, цели и бизнес-требования, предъявляемые к обработке информации, которые были разработаны компанией для поддержки ее бизнес-операций.

Примечание — Важно, чтобы энергетическая компания обеспечила анализ требований безопасности системы управления технологическими процессами и адекватное отражение их в политике ИБ. Анализ требований и целей ИБ включает рассмотрение всех соответствующих критериев для безопасного энергоснабжения и поставки, например:

- нарушение безопасности энергоснабжения;
- ограничение энергетического потока;
- доля пострадавшего населения;
- опасность физического увечья;
- воздействие на другие критически важные инфраструктуры;
- влияние на конфиденциальность информации;
- финансовые последствия.

Необходимые меры безопасности или контроля определяются методической оценкой рисков безопасности. Необходимо, чтобы расходы на меры обеспечения безопасности были сбалансированы с экономическими потерями, которые могут быть понесены из-за проблем безопасности. Результаты оценки рисков облегчают:

- определение адекватных управленческих действий и приоритетов для управления рисками информационной безопасности;
- осуществление мер обеспечения безопасности, выбранных для противодействия этим рискам.

Оценка риска должна повторяться периодически, чтобы учесть все изменения, которые могут повлиять на оцениваемые результаты.

Требования к оценке рисков и выбору средств и мер обеспечения безопасности приведены в ИСО/МЭК 27001:2013.

0.4 Выбор мер обеспечения безопасности

После того как требования безопасности и риски были определены и приняты решения о том, как противостоять этим рискам, выбираются и внедряются соответствующие меры обеспечения безопасности для снижения рисков до допустимого уровня.

В дополнение к мерам по безопасности, обеспечиваемым комплексной СМИБ, настоящий стандарт предусматривает дополнительную помощь и секторальные меры для систем управления технологическими процессами, используемых в энергетическом секторе, с учетом особых требований, предъявляемых в данных условиях. При необходимости могут быть разработаны дополнительные меры для выполнения конкретных требований. Выбор мер безопасности зависит от решений, принимаемых организацией на основе ее собственных критериев принятия риска, вариантов решения проблемы риска и общего подхода организации к управлению рисками. При выборе мер следует также учитывать соответствующие нормы национального и международного права, правовые постановления и нормативные акты.

0.5 Целевая аудитория

Настоящий стандарт адресован лицам, ответственным за функционирование систем управления технологическими процессами, используемых энергетическими компаниями, менеджерам по ИБ, поставщикам, системным интеграторам и аудиторам. Для этой целевой группы он детализирует основные меры в соответствии с целями ИСО/МЭК 27002:2013 и определяет конкретные меры для систем управления технологическими процессами в энергетике, вспомогательных систем и соответствующей инфраструктуры[1)].

[1)] *Положения настоящего стандарта должны рассматриваться с учетом требований национальных нормативных правовых актов и стандартов Российской Федерации в области защиты информации.*

Федеральное агентство
по техническому регулированию
и метрологии
Федеральное агентство
по техническому регулированию
и метрологии

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационные технологии

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Меры обеспечения информационной безопасности в энергетике (неатомной)

Information technology. Security techniques. Information security controls for the energy utility industry (non-nuclear)

Дата введения — 2021—11—30

1 Область применения

Настоящий стандарт содержит руководящие указания, основанные на положениях ИСО/МЭК 27002:2013, применяемых к системам управления технологическими процессами, используемым в энергетике для контроля и мониторинга выработки или производства, передачи, хранения и распределения электроэнергии, тепла, газа, нефти и нефтепродуктов, а также для контроля связанных с ними вспомогательных процессов. Это включает в себя в частности следующее:

- централизованные и распределенные технологии управления технологическими процессами, контроля и автоматизации, а также информационные системы, используемые для их функционирования, такие как устройства программирования и параметризации;
- цифровые контроллеры и компоненты автоматизации, такие как управляющие и полевые устройства или программируемые логические контроллеры (ПЛК), включая цифровые сенсорные и приводные элементы;
- все дополнительные вспомогательные информационные системы, используемые в области управления технологическими процессами, например, для выполнения дополнительных задач визуализации данных и для целей контроля, мониторинга, архивирования данных, ведения журнала событий, отчетности и документации;
- коммуникационные технологии, используемые в области управления технологическими процессами, например, сети, телеметрия, приложения телеконтроля и технологии дистанционного управления;
- компоненты развитой инфраструктуры измерений, например, интеллектуальные счетчики;
- измерительные приборы, например, для определения значений выбросов, связанных с экологией;
- цифровые системы защиты и безопасности, например, релейная защита, предохранительные механизмы;
- системы энергоменеджмента, например, системы распределенных энергетических ресурсов, электрозарядной инфраструктуры, в частных домохозяйствах, жилых зданиях или промышленных объектах потребителя;
- распределенные компоненты среды интеллектуальной энергетической сети, например, в энергетических сетях, в частных домохозяйствах, жилых зданиях или промышленных объектах потребителя;
- все программное обеспечение, микропрограммное обеспечение и приложения, установленные на вышеуказанных системах, например, система рационального использования и распределения или система управления отключением подачи электроэнергии;
- любые помещения, в которых находятся вышеуказанное оборудование и системы;
- удаленные системы технического обслуживания для вышеперечисленных систем.

Настоящий стандарт не распространяется на область управления технологическими процессами ядерных установок. Эта область охватывается МЭК 62645.

Издание официальное

В настоящем стандарте также включается требование адаптировать процессы оценки и обработки рисков, описанные в ИСО/МЭК 27001:2013, к конкретным руководящим указаниям по энергетике, содержащимся в настоящем стандарте.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты. Для датированных ссылок применяют только указанное издание, для недатированных — последнее издание (включая все изменения ссылочного стандарта).

ISO/IEC 27000, Information technology — Security techniques — Information security management systems — Overview and vocabulary (Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология)

ISO/IEC 27001:2013, Information technology — Security techniques — Information security management systems — Requirements (Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования)

ISO/IEC 27002:2013, Information technology — Security techniques — Information security management systems — Requirements (Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил применения мер обеспечения информационной безопасности)

3 Термины и определения

В настоящем стандарте применены термины по ИСО/МЭК 27000, а также следующие термины с соответствующими определениями:

ИСО и МЭК ведут терминологические базы данных для их использования в стандартизации по следующим адресам:

- Электропедия МЭК: доступна по адресу http://www.electropedia.org/;
- платформа онлайн-просмотра ИСО: доступна по адресу http://www.iso.org/obp.

3.1 **блэкаут** (blackout): Массовое отключение электричества.

3.2 **команда реагирования на инциденты компьютерной безопасности;** CSIRT (computer security incident response team, CSIRT): Команда реагирования на инциденты в компьютерной безопасности.

3.3 **критически важный актив** (critical asset): Актив, который может оказывать непосредственное влияние на производство или выработку, передачу, хранение и распределение электроэнергии, тепла, газа, нефти и нефтепродуктов.

3.4 **критическая инфраструктура** (critical infrastructure): Совокупность организаций и объектов, имеющих существенное значение для функционирования общества и экономики в целом.

Примечание — Отказ или неисправность таких организаций и объектов может привести к постоянному дефициту поставок, оказать значительное воздействие на общественную безопасность и иметь другие широкомасштабные последствия.

3.5 **отладка** (debugging): Действие анализа неисправностей в компьютерных системах.

3.6 **система распределения** (distribution system): Распределительная сеть для транспортировки электрической энергии с использованием сети высокого, среднего или низкого напряжения, а также локальная или региональная распределительная сеть для транспортировки тепла, газа, нефти или нефтепродуктов.

3.7 **система управления энергопотреблением;** EMS (energy management system, EMS): Оборудование/инфраструктура, используемые для мониторинга, измерения и контроля потребления энергии в частных домохозяйствах, жилых зданиях или промышленных объектах потребителя.

Примечание — Термин EMS также обычно используется для обозначения набора приложений, используемых операторами передающей энергосистемы для мониторинга, контроля и оптимизации производительности системы генерации и/или передачи.

3.8 **предложение электроэнергии** (energy supply): Процесс выработки, производства или хранения энергии для доставки потребителям и эксплуатации сети энергоснабжения.

3.9 **энергетическая компания** (energy utility): Юридическое лицо, обеспечивающее поставку энергии (электрической, тепловой, газовой или энергии, базирующейся на переработке нефти) другим лицам, в энергораспределительную или накопительную сеть.

3.10 **человеко-машинный интерфейс;** ЧМИ (human-machine interface, HMI): Пользовательский интерфейс для работы и мониторинга системы управления технологическим процессом или установки.

3.11 **профилактическое обслуживание** (maintenance): Меры, применяемые в области предложения электроэнергии (3.8), которые обычно связаны с инспекцией, устранением неисправностей и улучшением.

3.12 **система управления технологическими процессами** (process control system): Система, предназначенная для контроля и мониторинга выработки, производства, передачи, хранения и распределения электроэнергии, тепла, газа, нефти и нефтепродуктов, включая контроль сопутствующих вспомогательных процессов.

Примечание — Систему управления технологическими процессами часто называют в более общем смысле промышленной системой управления. В настоящем стандарте термин «система управления технологическими процессами» ограничивается технологиями и компонентами, используемыми в энергетике.

3.13 **безопасность** (safety): Отсутствие недопустимого риска.

[Руководство ИСО/МЭК 51:2014, 3.14]

3.14 **система безопасности** (safety system): Система и компоненты, необходимые для обеспечения безопасности (3.13).

3.15 **диспетчерское управление и сбор данных;** SCADA-система (supervisory control and data acquisition SCADA): Система управления технологическими процессами (3.12), обычно используемая для контроля за распределенными активами с применением централизованного сбора данных и диспетчерского контроля.

3.16 **интеллектуальная энергетическая сеть** (smart grid): Электроэнергетическая сеть, использующая технологии обмена информацией и управления, распределенные вычисления и связанные с ними датчики и исполнительные механизмы.

Примечание — Технологии интеллектуальной энергетической сети используются для таких целей, как:
- учет поведения и действий пользователей сети и других заинтересованных сторон;
- эффективное обеспечение устойчивых, экономичных и безопасных поставок электроэнергии.

3.17 **система передачи** (transmission system): Система, обеспечивающая передачу электрической энергии с использованием средств высоковольтной или сверхвысоковольтной передачи энергии, или газотранспортная система для транспортировки природного газа с использованием сети трубопроводов высокого давления.

4 Структура документа

4.1 Общие положения

Настоящий стандарт представляет собой стандарт, относящийся к ИСО/МЭК 27002:2013 применительно к отрасли энергетики. Типовые задачи управления и меры обеспечения безопасности в энергетическом секторе перечислены в приложении А.

4.2 Уточнение требований ИСО/МЭК 27001:2013

ИСО/МЭК 27001:2013, 6.1.3, перечисление c), уточнен следующим образом:

Сравнивают элементы управления, определенные в 6.1.3, перечисление b) выше, с элементами управления, указанными в приложении А ИСО/МЭК 27001:2013 и в приложении А настоящего стандарта, чтобы убедиться в том, что никакие необходимые меры обеспечения безопасности не были упущены.

ИСО/МЭК 27001:2013, 6.1.3, перечисление d), уточняется следующим образом:

Подготавливают заявку о применимости, которая содержит:

- необходимые меры обеспечения безопасности [см. ИСО/МЭК 27001:2013, 6.1.3, перечисления b) и c)];
- обоснование их включения;
- осуществляются ли необходимые меры обеспечения безопасности или нет;
- обоснование для исключения любых мер обеспечения безопасности, предусмотренных в приложении А ИСО/МЭК 27001:2013 или в приложении А настоящего стандарта.

Примечание — Эти уточнения необходимы в связи с введением в настоящем стандарте новых мер обеспечения безопасности в отношении конкретного энергетического сектора.

Все другие требования, содержащиеся в разделах 4—10 ИСО/МЭК 27001:2013, применяются без изменений. Каких-либо дополнительных требований, предъявляемых конкретно к энергетическим компаниям, не существует.

4.3 Специальное руководство по энергетике, относящееся к ИСО/МЭК 27002

Все положения, цели контроля, меры обеспечения безопасности, руководящие указания по внедрению и другая информация, относящаяся к энергетическому сектору, а также положения ИСО/МЭК 27002:2013, которые применяются без изменений, перечислены в разделах 5—18.

Примечание — Наименования разделов, подразделов и элементов управления, которые не содержатся в ИСО/МЭК 27002:2013, имеют префикс ИБЭ (означающий «информационную безопасность в энергетике»).

5 Политика информационной безопасности

Дополнительная информация, относящаяся к энергетическому сектору, в соответствии с разделом 5 ИСО/МЭК 27002:2013 отсутствует.

6 Организация деятельности по информационной безопасности

6.1 Внутренняя организация деятельности по обеспечению информационной безопасности

6.1.1 Роли и обязанности по обеспечению информационной безопасности

Дополнительное руководство по внедрению, приведенное в ИСО/МЭК 27002:2013, 6.1.1, является следующим:

Инженеры систем управления, инженеры систем телекоммуникаций и другие сотрудники должны быть уведомлены о возложенных на них ролях и обязанностях в части, касающейся аспектов ИБ систем управления технологическими процессами.

6.1.2 Разделение обязанностей

Дополнительная информация, относящаяся к энергетическому сектору, для ИСО/МЭК 27002:2013, 6.1.2, отсутствует.

6.1.3 Контакт с органами управления и ведомствами

Дополнительное руководство по внедрению, приведенное в ИСО/МЭК 27002:2013, 6.1.3, является следующим:

Прикладные системы и инфраструктура систем управления технологическими процессами энергообеспечения могут быть частью критически важных инфраструктур и иметь важное значение для функционирования сообщества, общества и экономики в целом. Поэтому операторы таких систем должны поддерживать контакт со всеми соответствующими органами управления и ведомствами. В дополнение к соответствующим государственным ведомствам (пожарная служба, инспекции и т. д.) это могут быть, например:

- национальные и международные учреждения и инициативы по сотрудничеству в области защиты важнейших инфраструктур;
- национальные и международные команды реагирования на инциденты в компьютерной безопасности;
- организации гражданской обороны и группы по оказанию помощи в случае стихийных бедствий;
- аварийно-спасательные организации и персонал организации.

Для операторов критически важных компонентов инфраструктуры могут применяться дополнительные законы, локальные подзаконные акты и нормативные акты, касающиеся организации взаимодействия с органами управления и ведомствами. Энергетическим компаниям следует удостовериться в том, чтобы информация, полученная в результате контактов с органами управления и ведомствами, анализировалась и оценивалась в контексте организации экспертами по тематическим вопросам и своевременно распространялась среди ответственных сторон внутри организации.

Дополнительная информация для ИСО/МЭК 27002:2013, 6.1.3, является следующей:

Во время работы системы, оперативного планирования и подготовительных работ для исключительных ситуаций может потребоваться информация о метеоусловиях. Поэтому следует установить

прямой контакт с соответствующими местными, региональными и национальными метеорологическими службами и соответствующими информационными службами (например, предупреждение о грозе, обнаружение молний).

6.1.4 Контакты с заинтересованными профессиональными группами

Дополнительное руководство по внедрению, приведенное в ИСО/МЭК 27002:2013, 6.1.4, является следующим:

В целях обмена информацией по вопросам безопасности, связанным с мерами обеспечения безопасности за конкретными процессами, и содействия межорганизационному сотрудничеству, следует поддерживать контакты с национальными и международными ассоциациями поставщиков и операторов и их соответствующими рабочими группами, занимающимися вопросами безопасности. Процесс информирования учитывает применимый правовой контекст.

Энергетические компании должны обеспечить в контексте организации анализ и оценку экспертами по тематическим вопросам информации, полученной в результате контактов с заинтересованными профессиональными группами, и своевременное ее распространение среди ответственных сторон внутри организации.

6.1.5 Информационная безопасность при управлении проектами

Дополнительная информация, относящаяся к энергетическому сектору, для ИСО/МЭК 27002:2013, 6.1.5, отсутствует.

6.1.6 ИБЭ-идентификация рисков, связанных с внешними сторонами

Дополнительная мера обеспечения безопасности для ИСО/МЭК 27002:2013, 6.1, является следующей:

Мера обеспечения безопасности

Перед предоставлением доступа к информации и средствам обработки информации организации следует выявить риски, связанные с бизнес-процессами, в которых участвуют внешние стороны, и внедрить соответствующие меры обеспечения безопасности.

Рекомендация по реализации

Системы управления технологическими процессами могут состоять из сложных индивидуально настроенных систем и компонентов. Поставщики систем, интеграторы и другие внешние стороны зачастую принимают активное участие в обслуживании и эксплуатации этих систем. Что касается процессов технического обслуживания и устранения неисправностей, то, возможно, этим внешним сторонам необходимо использовать системы дистанционного доступа, которые позволяют осуществлять техническое обслуживание из отдаленных районов. Возможно также, что сотрудники внешних сторон также нуждаются в доступе к контролируемым с точки зрения безопасности районам для проведения технического обслуживания на местах.

Тесное сотрудничество между различными системными операторами на уровнях производства, генерации, передачи и распределения может потребовать тесной взаимосвязи систем управления и сетей связи различных организаций. Кроме того, внешние стороны, такие как поставщики, системные интеграторы или деловые партнеры, также могут требовать доступ к информации, относящейся к критически важным активам.

Риски, связанные с доступом такой внешней стороны к критически важным активам и соответствующей информации, должны оцениваться и приниматься во внимание, особенно с точки зрения подверженности риску физического процесса, который подлежит контролю или мониторингу. Если внешние стороны имеют доступ к критически важным активам или конфиденциальной информации, то должно быть гарантировано, например, на основе договорных соглашений, чтобы они обеспечили сопоставимый уровень безопасности, определенный для внутренней организации энергетической компании.

6.1.7 ИБЭ-решение вопросов безопасности при работе с потребителями

Дополнительная мера обеспечения безопасности для ИСО/МЭК 27002:2013, 6.1, является следующей:

Мера обеспечения безопасности

Все выявленные требования безопасности должны быть учтены до предоставления потребителям доступа к информации или активам предприятия.

Рекомендация по реализации

Сложные и разнообразные отношения между владельцами активов, системными операторами, поставщиками услуг и внутренними и внешними потребителями в секторе энергоснабжения могут привести к разграничению ответственности в отношении технического обслуживания, эксплуатации и владения активами.

В качестве примера можно привести следующее:

- внутренний поставщик услуг, который отвечает за эксплуатацию и техническое обслуживание инфраструктуры сети передачи или распределения, выделенной для отдельного внутреннего организационного подразделения;

- поставщик услуг, отвечающий за эксплуатацию и техническое обслуживание электростанций или объектов распределенной генерации;

- внутренний или внешний поставщик услуг, который отвечает за функционирование инфраструктуры управления технологическими процессами;

- внутренний или внешний потребитель, подключенный к инфраструктуре энергоснабжения и связанным с ней системам управления технологическими процессами и коммуникационной инфраструктуре.

Такие разнообразные и/или сложные деловые отношения должны приниматься во внимание при определении и удовлетворении требований безопасности, необходимых для предоставления потребителю доступа к информации или активам. При размещении оборудования в помещениях других энергокомпаний или потребителей или при наличии взаимосвязанных систем управления технологическими процессами следует учитывать меры, описанные в 11.3.1, 11.3.2, 11.3.3 и 13.1.5.

6.2 Мобильные устройства и дистанционная работа

6.2.1 Политика использования мобильных устройств

Дополнительная рекомендация по реализации, приведенная в ИСО/МЭК 27002:2013, 6.2.1, является следующей:

Если мобильные устройства используются в сети управления технологическими процессами, энергетические компании должны включить в свои политики безопасности мобильных устройств следующее:

a) определение и назначение ролей, разрешенных для выполнения задач, требующих доступа к системам управления технологическими процессами через мобильное устройство;

b) определить действия, которые эти устройства могут выполнять время, в течение которого эти действия разрешены, и явно установить чрезвычайные исключения;

c) указать, какие изменения могут быть внесены в устройство, кому разрешено вносить эти изменения и как они могут быть внесены;

d) указать места и коммуникационные сети, которые эти устройства могут использовать для доступа, например: дом, офис, удаленный офис или служебные транспортные средства;

e) определить любые процессы, необходимые для управления механизмами безопасности, такими как управление ключами, контроль доступа, управление конфигурацией и управление идентификацией;

f) указать, как каждое устройство может быть подключено к сети управления технологическим процессом, например, через шлюз, ДМЗ, VPN-туннелирование;

g) разделение использования в системах управления технологическими процессами и других сетях (например, бизнес-сетях);

h) указать типы данных, которые могут передаваться, и явно запретить все другие типы передачи данных.

6.2.2 Дистанционная работа

Дополнительная рекомендация по реализации, приведенная в ИСО/МЭК 27002:2013, 6.2.2, является следующей:

Удаленный доступ к системам управления технологическими процессами, осуществляемый персоналом энергосервисной организации, поставщиками или другими внешними сторонами, должен быть обеспечен несколькими мерами обеспечения безопасности, включая следующее:

a) многофакторную аутентификацию;

b) принятие методов, запрещающих что-либо иное, кроме косвенного подключения к целевой системе или сети;

c) минимизацию функций, которые может выполнять удаленная сторона, например удаленное управление, удаленная настройка и программирование систем управления технологическими процессами;

d) проверку состояния безопасности системы удаленного доступа (например, наличие своевременных исправлений и состояние защиты от вредоносных программ, отсутствие известных программ,

занесенных в черный список) и защита от передачи вредоносных программ из системы удаленного доступа (см. 12.2.1):

e) обеспечение соблюдения перечня разрешенных мест доступа и/или систем;

f) обеспечение мониторинга и контроля за удаленным доступом и отслеживание изменений и модификаций важнейших активов;

g) обеспечение того, чтобы для удаленного доступа и удаленного обслуживания использовались только известные и одобренные программно-инструментальные средства.

7 Безопасность, связанная с персоналом

7.1 При приеме на работу

7.1.1 Проверка

Дополнительная рекомендация по реализации, приведенная в ИСО/МЭК 27002:2013, 7.1.1, является следующей:

При необходимости следует тщательно продумать и внедрить процесс строгого отбора сотрудников, имеющих доступ к критическим активам или ответственных за процессы эксплуатации и технического обслуживания критических активов. Это особенно важно в том случае, если активы являются частью критической инфраструктуры или если они необходимы для функционирования критической инфраструктуры.

Прежде чем будущему персоналу будет разрешено работать с компонентами, входящими в состав критической инфраструктуры, может потребоваться специальное разрешение на право работы (в области обеспечения безопасности), предоставляемое государственными органами, в зависимости от соответствующего (местного) законодательства.

7.1.2 Правила и условия работы

Дополнительная рекомендация по реализации, приведенная в ИСО/МЭК 27002:2013, 7.1.2, является следующей:

Энергетическая компания должна обеспечить с помощью соответствующих условий работы, чтобы ключевые навыки и персонал всегда были доступны для эксплуатации критически важных инфраструктур. Для ключевого персонала, ответственного за эксплуатацию критических инфраструктур и систем, следует рассматривать получение разрешения на превышение длительности максимального рабочего времени в чрезвычайных ситуациях, с учетом применимых правовых требований. Соглашения о наблюдении и регистрации конкретных действий, таких как контроль операций или доступом к программированию и оцениванию параметров, также должны приниматься во внимание при составлении трудового договора.

7.2 Во время работы

7.2.1 Обязанности руководства организации

Дополнительная информация, относящаяся к энергетическому сектору, для ИСО/МЭК 27002:2013, 7.2.1, отсутствует.

7.2.2 Осведомленность, обучение и практическая подготовка (тренинги) в области информационной безопасности

Дополнительная рекомендация по реализации, приведенная в ИСО/МЭК 27002:2013, 7.2.2, является следующей:

Персонал, работающий в энергетическом секторе, отвечающий за технологию систем управления технологическими процессами, должен обладать соответствующими знаниями и навыками для управления и надзора за установкой, техническим обслуживанием и безопасной эксплуатацией систем управления технологическими процессами. Это также должно включать в себя достаточный опыт.

7.2.3 Дисциплинарный процесс

Дополнительная информация, относящаяся к энергетическому сектору, для ИСО/МЭК 27002:2013, 7.2.3, отсутствует.

7.3 Увольнение и смена места работы

Дополнительная информация, относящаяся к энергетическому сектору, для ИСО/МЭК 27002:2013, 7.3, отсутствует.

8 Менеджмент активов

8.1 Ответственность за активы

8.1.1 Инвентаризация активов

Дополнительная рекомендация по реализации, приведенная в ИСО/МЭК 27002:2013, 8.1.1, является следующей:

Инвентаризация активов должна включать все бизнес-процессы и системы управления технологическими процессами, имеющие отношение к энергоснабжению, такие как информация, прикладные программы и другие вспомогательные активы.

Дополнительная информация для ИСО/МЭК 27002:2013, 8.1.1, является следующей:

Активы в области энергоснабжения включают широкий спектр отраслевых категорий активов, таких как:

a) **информация:** планы электросетей и других сетей, календарное планирование и данные оперативного управления, географические и гео-привязанная информация, кризисные и чрезвычайные планы, планы аварийного восстановления энергосистемы, данные коммутационных процессов, измеряемые величины и результаты измерений, счетчики и их данные, эксплуатационная учетная документация, данные прикладного программирования и параметризации данных, архив измерений и сигналов, исторические данные и данные трендов и т. д.;

Примечание — Сюда также входят данные прикладного программирования и параметризации цифровых контроллеров и компонентов автоматизации.

b) **программное обеспечение:** программное обеспечение для управления технологическими процессами, системы визуализации, программное обеспечение для управления энергопотреблением и его оптимизацией, программное обеспечение для моделирования, программное обеспечение для параметризации, системы управления и мониторинга, системы оперативного планирования ресурсов, программные среды, микропрограммное обеспечение, архивирование, отчетность и предыдущие версии программного обеспечения и т. д.;

c) **физические активы:** элементы управления и автоматизации, компоненты телеметрического и телеуправления, удаленные терминальные блоки, компоненты системы передачи данных, компоненты цифровой защиты и безопасности, цифровые счетчики и измерительные приборы, интеллектуальные счетчики, цифровые датчики и исполнительные элементы, параметрические и программируемые устройства, визуализация и оперативные компоненты, цифровые системы мониторинга и регистрации и т. д.;

d) **услуги:** телекоммуникационные услуги, услуги экстренной связи, информационные услуги, метеорологические услуги, услуги средств массовой информации и новостей, тайм-сервисы и т. д.

8.1.2 Владение активами

Дополнительная рекомендация по реализации, приведенная в ИСО/МЭК 27002:2013, 8.1.2, является следующей:

Потенциально сложная структура организаций, использующих системы управления технологическими процессами, означает, что могут существовать весьма разнообразные обязанности в отношении коммерческой и операционной собственности. В результате должны быть определены и задокументированы права собственности и обязанности в отношении активов, а также роли владельца активов и оператора активов в отношении информационной безопасности.

8.1.3 Допустимое использование активов

Дополнительная информация, относящаяся к энергетическому сектору, для ИСО/МЭК 27002:2013, 8.1.2, отсутствует.

8.1.4 Возврат активов

Дополнительная информация, относящаяся к энергетическому сектору, для ИСО/МЭК 27002:2013, 8.1.4, отсутствует.

8.2 Категорирование информации

8.2.1 Категорирование информации

Дополнительная рекомендация по реализации, приведенная в ИСО/МЭК 27002:2013, 8.2.1, является следующей:

При необходимости следует расширить критерии категорирования для конкретных энергетических компаний, включив в них следующие элементы:

- активы, системы и информация, обеспечивающие функционирование важнейших инфраструктур и важнейших активов;

- активы, системы и информация, необходимые для восстановления системы энергоснабжения после серьезного нарушения в энергоснабжении (восстановление энергосистемы), т. е. системы и компоненты, способные к запуску генерации без питания от внешнего источника;

- активы, системы и информация, необходимые для обеспечения охраны труда и техники безопасности, а также безопасности основных средств;

- активы, системы и информация, необходимые для выполнения нормативных требований, таких как правила подключения потребителей к электросетям, или другие специальные требования;

- информация, считающаяся конфиденциальной или частной внешними сторонами, т. е. потребителями или регулирующими органами.

8.2.2 Маркировка информации

Дополнительная информация, относящаяся к энергетическому сектору, для ИСО/МЭК 27002:2013, 8.2.2, отсутствует.

8.2.3 Обращение с активами

Дополнительная информация, относящаяся к энергетическому сектору, для ИСО/МЭК 27002:2013, 8.2.3, отсутствует.

8.3 Обращение с носителями информации

Дополнительная информация, относящаяся к энергетическому сектору, для ИСО/МЭК 27002:2013, 8.3, отсутствует.

9 Управление доступом

9.1 Требования бизнеса к управлению доступом

9.1.1 Политика управления доступом

Дополнительная рекомендация по реализации, приведенная в ИСО/МЭК 27002:2013, 9.1.1, является следующей:

Кроме того, политика должна учитывать следующее:

a) применение условий и правил, касающихся использования групповых учетных записей, когда использование персональных учетных записей пользователей невозможно. Для обеспечения достаточного уровня безопасности и отслеживаемости следует определить четкие правила, касающиеся исключений, наряду с дополнительными мерами;

b) условия и правила, применимые к системам, которые не поддерживают строгую политику паролей или где такая политика паролей невозможна по эксплуатационным причинам. Для обеспечения достаточного уровня безопасности необходимо, в частности, определить дополнительные меры;

c) необходимость того, чтобы персонал и внешний персонал аварийно-спасательных служб мог обойти меры безопасности в условиях объявленной чрезвычайной ситуации;

d) доступ к услугам или приложениям со стороны систем, не имеющих надлежащей аутентификации (т. е. в контексте межмашинной связи). Для обеспечения достаточного уровня безопасности следует рассмотреть вопрос о контроле доступа к сети или других средствах.

Дополнительная информация для ИСО/МЭК 27002:2013, 9.1.1, является следующей:

IEC/TS 62351-8 дает дополнительные рекомендации по внедрению контроля доступа пользователей и автоматизированных агентов к объектам данных в энергосистемах с помощью ролевого контроля доступа.

9.1.2 Доступ к сетям и сетевым сервисам

Дополнительная рекомендация по реализации, приведенная в ИСО/МЭК 27002:2013, 9.1.2, является следующей:

Для защиты сетевого оборудования, обеспечивающего доступ к критическим сетям, необходимо учитывать следующее:

a) обеспечение физической защиты доступа к сетевому оборудованию, особенно в удаленных местах;

b) удаление или отключение с помощью программного обеспечения или физического отключения всех служб и портов сетевого оборудования, не требующихся для нормальной эксплуатации (например, неиспользуемые порты коммутатора), аварийная эксплуатация или техническое обслуживание, включая как коммуникационные порты, так и физические порты ввода — вывода.

9.2 Процесс управления доступом пользователей

9.2.1 Регистрация и отмена регистрации пользователей

Дополнительная рекомендация по реализации, приведенная в ИСО/МЭК 27002:2013, 9.2.1, является следующей:

Использование уникальных идентификаторов пользователей не всегда возможно в системах управления технологическими процессами энергетических компаний, например, для доступа к операционной системе или микропрограммам встроенных систем, таких как контроллеры/ПЛК, или для процессов технического обслуживания в распределенных системах. Возникающий в результате этого риск следует учитывать и принимать соответствующие контрмеры по снижению риска.

Использование индивидуальных и групповых учетных записей пользователей должно соответствовать применимым требованиям ведения журнала (см. 12.4.1).

9.2.2 Предоставление пользователю прав доступа

Дополнительная информация, относящаяся к энергетическому сектору, для ИСО/МЭК 27002:2013, 9.2.2, отсутствует.

9.2.3 Управление привилегированными правами доступа

Дополнительная информация, относящаяся к энергетическому сектору, для ИСО/МЭК 27002:2013, 9.2.3, отсутствует.

9.2.4 Процесс управления закрытой аутентификационной информацией пользователей

Дополнительная информация, относящаяся к энергетическому сектору, для ИСО/МЭК 27002:2013, 9.2.4, отсутствует.

9.2.5 Пересмотр прав доступа пользователей

Дополнительная информация, относящаяся к энергетическому сектору, для ИСО/МЭК 27002:2013, 9.2.5, отсутствует.

9.2.6 Аннулирование или корректировка прав доступа

Дополнительная информация, относящаяся к энергетическому сектору, для ИСО/МЭК 27002:2013, 9.2.6, отсутствует.

9.3 Ответственность пользователей

9.3.1 Использование закрытой аутентификационной информации

Дополнительная рекомендация по реализации, приведенная в ИСО/МЭК 27002:2013, 9.3.1, является следующей:

В области управления технологическими процессами не всегда возможно обеспечить использование защищенной закрытой аутентификационной информации, например:

- устаревшие системы часто не позволяют использовать индивидуальные пароли и/или пароли с необходимой стойкостью;
- зачастую невозможно подключить системы, работающие на децентрализованных предприятиях, таких как подстанции или распределенные источники генерирования электрической энергии, производственное оборудование, к центральной службе каталогов, что означает необходимость использования локальных учетных записей. Это делает практически невозможным регулярное изменение закрытой аутентификационной информации для этих учетных записей.

Поэтому следует четко указывать пользователю, когда применяется общая политика закрытой аутентификации и когда допускаются исключения, например, когда должны использоваться различные пароли или когда вообще невозможно использовать какие-либо пароли (для устаревших систем).

Особенно в ситуациях, когда для доступа к системе используется общая информация о закрытой аутентификации, следует учитывать следующее:

- общая информация о закрытой аутентификации должна быть максимально защищена;
- ее следует менять чаще, чем отдельные закрытые аутентификационные данные;
- она должна быть изменена в случае кадровых перестановок.

В частности, стандартные пароли, используемые поставщиками систем, должны рассматриваться как небезопасные и поэтому должны быть изменены. Закрытая аутентификационная информация должна быть доступна только лицам, участвующим в работе системы.

9.4 Управление доступом к системам и приложениям

9.4.1 Ограничение доступа к информации

Дополнительная информация, относящаяся к энергетическому сектору, для ИСО/МЭК 27002:2013, 9.4.1, отсутствует.

9.4.2 Безопасные процедуры входа в систему

Дополнительная рекомендация по реализации, приведенная в ИСО/МЭК 27002:2013, 9.4.2, является следующей:

Активация сеансов блокировки из-за простоя и заставок нецелесообразна в некоторых приложениях управления технологическими процессами, например в ЧМИ и приложениях визуализации, используемых для непрерывного мониторинга технологических процессов эксплуатирующим персоналом, например, в центрах управления. Для таких приложений следует принимать во внимание возникающие риски, связанные с работающими без оператора сеансами, и применять соответствующие дополнительные контрмеры.

9.4.3 Система управления паролями

Дополнительная информация, относящаяся к энергетическому сектору, для ИСО/МЭК 27002:2013, 9.4.3, отсутствует.

9.4.4 Использование привилегированных служебных программ

Дополнительная информация, относящаяся к энергетическому сектору, для ИСО/МЭК 27002:2013, 9.4.4, отсутствует.

9.4.5 Управление доступом к исходному коду программы

Дополнительная рекомендация по реализации, приведенная в ИСО/МЭК 27002:2013, 9.4.5, является следующей:

Исходный код, используемый энергетическими предприятиями, также включает данные прикладного программирования и параметризации цифровых контроллеров и компонентов автоматизации.

10 Криптография

10.1 Криптографическая защита информации

10.1.1 Политика использования криптографической защиты информации

Дополнительная информация, относящаяся к энергетическому сектору, для ИСО/МЭК 27002:2013, 10.1.1, отсутствует.

10.1.2 Управление ключами

Дополнительная информация для ИСО/МЭК 27002:2013, 10.1.2, является следующей:

МЭК 62351-9 определяет, как генерировать, распространять, отзывать и обрабатывать цифровые сертификаты и криптографические ключи для связи энергосистем. Его можно использовать и для других энергетических областей[1)].

11 Физическая безопасность и защита от воздействия окружающей среды

11.1 Зоны безопасности

11.1.1 Периметр физической безопасности

Дополнительная рекомендация по реализации, приведенная в ИСО/МЭК 27002:2013, 11.1.1, является следующей:

Компоненты, особенно в системах передачи и распределения энергии и в области распределенной выработки и производства, распределяются по децентрализованным участкам. Оборудование размещается в диспетчерских и технических помещениях в здании компании и в периферийных, потенциально незанятых местах. Иногда оборудование размещается в помещениях внешних сторон или в общественных местах. Как правило, невозможно достичь всеобъемлющего уровня физической защиты периферийных объектов; поэтому следует оценивать и, при необходимости, уменьшать степень риска с помощью дополнительных и компенсационных мер обеспечения безопасности.

11.1.2 Меры управления физическим доступом

Дополнительная рекомендация по реализации, приведенная в ИСО/МЭК 27002:2013, 11.1.2, является следующей:

---

1) Вопросы создания, выдачи, аннулирования, обработки сертификатов ключа проверки электронной подписи, а также использования криптографических ключей для энергосистем определяются действующими в Российской Федерации нормативными документами, включая документы национальной системы стандартизации, в области криптографической защиты информации.

Следует также рассмотреть вопрос об использовании физических систем управления доступом для периферийных объектов, где расположены критически важные активы (см. 11.1.9).

11.1.3 Безопасность зданий, помещений и оборудования

Дополнительная информация, относящаяся к энергетическому сектору, для ИСО/МЭК 27002:2013, 11.1.3, отсутствует.

11.1.4 Защита от внешних угроз и угроз со стороны окружающей среды

Дополнительная информация, относящаяся к энергетическому сектору, для ИСО/МЭК 27002:2013, 11.1.4, отсутствует.

11.1.5 Работа в зонах безопасности

Дополнительная информация, относящаяся к энергетическому сектору, для ИСО/МЭК 27002:2013, 11.1.5, отсутствует.

11.1.6 Зоны погрузки и разгрузки

Дополнительная информация, относящаяся к энергетическому сектору, для ИСО/МЭК 27002:2013, 11.1.6, отсутствует.

11.1.7 ИБЭ-обеспечение безопасности центров управления

Дополнительная мера обеспечения безопасности, приведенная в ИСО/МЭК 27002:2013, 11.1, является следующей:

Мера обеспечения безопасности

Следует спроектировать, разработать и применять меры по обеспечению физической безопасности центров управления, например, там, где размещены серверы систем управления, ЧМИ и вспомогательные системы.

Рекомендация по реализации

Для защиты объектов центральной системы управления, таких как центральное диспетчерское управление или диспетчерские пункты централизованных или распределенных электростанций, генерирующих или производственных блоков (далее — центры управления), необходимо учитывать следующие моменты:

a) для строительства центров управления следует выбрать участок, расположенный на твердом грунте; в тех случаях, когда такой твердый грунт отсутствует, следует принять соответствующие меры для обеспечения достаточной несущей способности грунта фундамента;

b) для центров управления следует выбрать участок, на котором меньше всего ожидается ущерб, наносимый окружающей средой — ветром, водой и т. д.; если какой-либо существующий участок подвержен таким угрозам окружающей среды, то следует принять соответствующие меры для предотвращения такого ущерба;

c) для центров управления следует выбирать площадку, где потенциальный ущерб от сильных электромагнитных полей незначителен; если существующая площадка подвергается воздействию сильных электромагнитных полей, то следует принять соответствующие меры для защиты оборудования в помещениях центров управления с использованием электромагнитного экранирования;

d) центры управления не должны располагаться на объектах, непосредственно примыкающих к объектам, используемым для хранения опасных материалов, представляющих угрозу взрыва или горения;

e) если центр управления расположен в районе, подверженном стихийным бедствиям, таким как землетрясение, цунами, извержение вулкана и торнадо, то здания центра управления должны иметь противоаварийную конструкцию;

f) здания центра управления должны быть огнеупорными или огнестойкими;

g) здания центра управления должны быть спроектированы с достаточной структурной устойчивостью для удовлетворения всех необходимых требований к нагрузке на пол; для существующих объектов должны быть приняты соответствующие меры по обеспечению адекватной структурной устойчивости для удовлетворения всех необходимых требований к нагрузке на пол;

h) в центрах управления должны быть установлены автоматические системы пожарной сигнализации, включая соответствующие системы раннего обнаружения и пожаротушения.

Информация для энергетических компаний

Активы системы управления технологическими процессами иногда размещаются во внешнем центре обработки данных вместе с другими информационно-телекоммуникационными активами (ICT). Физическое разделение между системами управления и другими системами ICT и строгое «разделение обязанностей» имеют важное значение, когда внешние операторы управляют либо ICT, либо системами управления. Во многих случаях это происходит на объекте, удаленном от центра обработки данных и находящемся под управлением энергокомпании.

11.1.8 ИБЭ-обеспечение безопасности для помещений с оборудованием

Дополнительная мера обеспечения безопасности, приведенная в ИСО/МЭК 27002:2013, 11.1, является следующей:

Мера обеспечения безопасности

Следует спроектировать, разработать и внедрить меры по обеспечению физической безопасности помещений, в которых расположены системы управления, используемые энергетическими предприятиями.

Рекомендация по реализации

Для защиты помещения, в котором расположено оборудование системы управления, используемого энергетическими предприятиями (здесь и далее — помещения системы управления), следует рассмотреть следующие меры по управлению:

a) помещение системы управления должно быть расположено там, где оно в наименьшей степени подвержено воздействию внешних факторов, таких, как экстремальные условия окружающей среды или стихийные бедствия; для существующих помещений системы управления, следует принять надлежащие меры для его защиты от опасного внешнего воздействия;

b) помещение системы управления должно располагаться там, где доступ постороннего персонала ограничен; для существующих помещений систем управления должны быть приняты адекватные меры по предотвращению или обнаружению возможного несанкционированного доступа;

c) по возможности помещение системы управления должно быть свободным. Должно быть дано минимум указаний на его использование в качестве помещения для оборудования системы управления технологическими процессами;

d) помещение системы управления должно располагаться там, где оно наименее подвержено затоплению или другому попаданию воды. Если помещение не соответствует этому требованию, то для предотвращения этого должны быть приняты необходимые меры, такие как повышение уровня пола, водонепроницаемость конструкции здания или установка специальных водоотводных сооружений и т. д.;

e) помещение системы управления должно быть расположено там, где оно лучше всего защищено от сильных электромагнитных полей. Если помещение не соответствует этому требованию, то оно должно быть защищено электромагнитными щитами или другими подходящими мерами. Это особенно важно в непосредственной близости от высоковольтного/сильноточного оборудования или трансформаторов и т. д. Меры защиты от электромагнитного излучения следует применять также в том случае, если помещение оборудования системы управления используется в качестве хранилища данных и/или для резервного копирования данных;

f) компоненты с повышенными требованиями к безопасности должны размещаться в специально отведенном аппаратном помещении системы управления с повышенной физической защитой;

g) в районах с риском землетрясения следует принимать меры для предотвращения обрушения и падения предметов и материалов, используемых для защиты пола, стен, крыш от обвалов и обрушения;

h) противопожарные мероприятия должны осуществляться для оборудования систем управления и помещений хранения данных;

i) следует принять меры для устранения неисправностей, вызванных статическими зарядами;

j) воздуховоды, соединяющие помещения оборудования системы управления, должны быть спроектированы таким образом, чтобы замедлить или предотвратить распространение огня;

k) автоматическая пожарная сигнализация должна быть установлена в помещениях систем управления и кондиционирования воздуха;

l) огнетушители должны устанавливаться в помещениях систем управления и кондиционирования воздуха;

m) помещения системы управления должны быть проветриваемые по мере необходимости. Наличие кондиционера должно быть обеспечено, например, путем защиты его от отключения электроэнергии.

Примечание — Если помещение системы управления расположено на периферийных объектах, то не все рекомендации руководства полностью применимы (см. 11.1.9).

11.1.9 ИБЭ-защита периферийных объектов

Дополнительная мера обеспечения безопасности, приведенная в ИСО/МЭК 27002:2013, 11.1, является следующей:

Мера обеспечения безопасности

Для периферийных объектов, где расположено оборудование системы управления, используемое энергетическими компаниями, должны быть спроектированы, разработаны и внедрены средства управ-

ления физической безопасностью или применены соответствующие контрмеры для снижения риска, если достаточный уровень физической защиты периферийных объектов недостижим.

Рекомендация по реализации

Особенно в сетях передачи и распределения электроэнергии, а также в распределенных системах генерации и производства, компоненты инфраструктуры системы управления могут быть распределены по периферийным участкам, которые часто остаются незанятыми. Для защиты таких децентрализованных объектов, на которых расположены объекты системы управления, следует рассмотреть следующие меры обеспечения безопасности:

a) если периферийный объект расположен в зоне риска стихийных бедствий, он должен быть устойчив к стихийным бедствиям и удовлетворять требованиям соответствующих национальных и региональных стандартов;

b) в тех случаях, когда критические активы эксплуатируются на периферийных объектах, следует устанавливать оборудование автоматического противопожарного контроля;

c) периферийные объекты должны контролироваться с целью обнаружения неисправностей компонентов, сбоев в электроснабжении, пожара и т. д. При необходимости следует также контролировать влажность и температуру воздуха;

d) в тех случаях, когда критические активы эксплуатируются на периферийных объектах, следует устанавливать адекватные, физически безопасные периметры с использованием, например, надежного ограждения. Кроме того, следует установить автоматическую сигнализацию и осуществлять контроль за ней из центрального помещения.

В тех случаях, когда достаточный уровень физической защиты периферийных объектов недостижим, этот риск следует принимать во внимание и смягчать путем применения соответствующих контрмер. При выборе таких контрмер в первую очередь следует учитывать критичность активов, эксплуатируемых на этих периферийных объектах, а также концепции избыточности и резервирования, реализуемые для их соответствующей системной функциональности.

11.2 Оборудование

11.2.1 Размещение и защита оборудования

Дополнительная рекомендация по реализации, приведенная в ИСО/МЭК 27002:2013, 11.2.1, является следующей:

При определенных обстоятельствах возможно, что системные компоненты систем управления технологическими процессами и вспомогательной инфраструктуры необходимо устанавливать в помещениях с интенсивным выделением пыли, тепла, холода, электромагнитного излучения, влажности и т. д. Оборудование должно быть соответствующим образом спроектировано и сконструировано для работы в таких условиях окружающей среды. В противном случае для обеспечения надежной работы следует применять дополнительные защитные контрмеры, например подходящие внешние корпусные шкафы.

11.2.2 Вспомогательные средства

Дополнительная рекомендация по реализации, приведенная в ИСО/МЭК 27002:2013, 11.2.2, является следующей:

Все критические активы, службы связи и другое оборудование, необходимое для восстановления системы после крупного отключения электроэнергии, должны быть спроектированы и эксплуатироваться таким образом, чтобы они были независимы от внешних служб в течение соответствующего периода времени. Это касается, в частности, внешнего энергоснабжения.

В зависимости от планов восстановления системы критические активы, необходимые для восстановления системы, должны быть способны к эксплуатации независимо от внешнего источника питания в течение соответствующего промежутка времени, определенного планами восстановления системы. В отдаленных районах может возникнуть необходимость обеспечить автономное электроснабжение, которое может работать в течение нескольких дней. Это включает в себя, например, аварийный электрогенератор с автоматическим запуском, а также соответствующий запас топлива.

Организации следует определить необходимое резервное время для обеспечения бесперебойного энергоснабжения важнейших объектов.

11.2.3 Безопасность кабельной сети

Дополнительная рекомендация по реализации, приведенная в ИСО/МЭК 27002:2013, 11.2.3, является следующей:

В частности, в области передачи и распределения энергии коммуникационные сети устанавливаются на обширных площадях, чтобы обеспечить связь с периферийными объектами и обеспечить

удаленный доступ к техническому обслуживанию. Зачастую невозможно обеспечить такой же уровень защиты внешней кабельной сети, как внутренней. Связанные с этим риски должны быть оценены соответствующим образом и смягчены, насколько это возможно, путем осуществления дополнительных физических мер. В зависимости от требований безопасности передаваемых данных следует также рассмотреть дополнительные нефизические меры, такие как криптографическая защита.

11.2.4 Техническое обслуживание оборудования

Дополнительная информация, относящаяся к энергетическому сектору, для ИСО/МЭК 27002:2013, 11.2.4, отсутствует.

11.2.5 Перемещение активов

Дополнительная информация, относящаяся к энергетическому сектору, для ИСО/МЭК 27002:2013, 11.2.5, отсутствует.

11.2.6 Безопасность оборудования и имущества вне помещений организации

Дополнительная информация, относящаяся к энергетическому сектору, для ИСО/МЭК 27002:2013, 11.2.6, отсутствует.

11.2.7 Безопасная утилизация или повторное использование оборудования

Дополнительная информация, относящаяся к энергетическому сектору, для ИСО/МЭК 27002:2013, 11.2.7, отсутствует.

11.2.8 Оборудование, оставленное пользователем без присмотра

Дополнительная информация, относящаяся к энергетическому сектору, для ИСО/МЭК 27002:2013, 11.2.8, отсутствует.

11.2.9 Политика «чистого стола» и «чистого экрана»

Дополнительная рекомендация по реализации, приведенная в ИСО/МЭК 27002:2013, 11.2.9, является следующей:

В области процесса управления энергетическими предприятиями ЧМИ часто не могут быть отключены или защищены экранными заставками, например ЧМИ SCADA-системы или устройства регистрации данных. Следует обеспечить, чтобы такие ЧМИ были установлены либо в физическом защищенном месте с постоянным наблюдением человека (например, в центре управления), либо в режиме отображения, где могут выполняться только некритические действия (например, режим только просмотра).

11.3 ИБЭ-безопасность в служебных помещениях третьих лиц

Дополнительная цель контроля, приведенная в разделе 11 ИСО/МЭК 27002:2013, является следующей:

Цель: защита оборудования, находящегося вне помещений, энергетических компаний от физических угроз и угроз окружающей среды.

11.3.1 ИБЭ-оборудование, расположенное на территории других энергетических компаний

Мера обеспечения безопасности

В тех случаях, когда энергетические компании устанавливают оборудование за пределами своих собственных объектов или помещений на территории, находящейся под ответственностью других энергетических компаний, как например при межсистемной связи станций, оборудование должно быть размещено на охраняемой территории, с тем чтобы снизить любые риски, связанные с угрозами окружающей среды, и уменьшить вероятность несанкционированного доступа.

Рекомендация по реализации

Для защиты оборудования энергетической компании, находящегося на территории других энергетических компаний, следует учитывать следующие меры обеспечения безопасности:

a) должен быть определен круг ответственности и взаимодействия с другими энергетическими компаниями, и при необходимости должна быть обеспечена возможность легко изолировать оборудование от оборудования другой организации (см. 11.3.3);

b) соглашения должны заключаться на договорной основе с другой энергетической компанией на поставку вспомогательных инфраструктурных услуг, таких как энергоснабжение, охлаждение, отопление и т. д.;

c) необходимо обеспечить, чтобы эксплуатационная площадка, на которой будет установлено оборудование, отвечала всем необходимым требованиям безопасности.

Другая информация

Для обеспечения того, чтобы уровень безопасности помещений другой компании соответствовал уровню безопасности собственных помещений энергокомпании, соответствующие условия должны быть согласованы заранее.

11.3.2 ИБЭ-оборудование, размещенное на территории потребителя

Мера обеспечения безопасности

В тех случаях, когда энергетические компании устанавливают оборудование в помещениях потребителя, например, для контроля или измерения поставок энергии и/или предоставления дополнительных услуг, оборудование компаний должно быть защищено таким образом, чтобы снизить любые риски, связанные с угрозами окружающей среды, и уменьшена вероятность несанкционированного доступа.

Рекомендация по реализации

Для защиты оборудования, расположенного на территории потребителя энергетической компании, необходимо учитывать следующие меры обеспечения безопасности:

a) шкафы оборудования, установленные на территории потребителя, не должны легко открывать посторонние лица. Любая форма манипуляции должна быть легко обнаружима;

b) следует определить круг ответственности и интерфейсы связи с потребителем, а также обеспечить возможность изолировать коммуникационные интерфейсы от интерфейсов связи с потребителем;

c) должна быть обеспечена возможность для того, чтобы энергетические компании осуществляли строгий контроль за состоянием или дистанционно эксплуатировали оборудование.

11.3.3 ИБЭ-взаимосвязанные системы управления и связи

Мера обеспечения безопасности

В тех случаях, когда системы управления, имеющие линии связи, взаимодействуют с системами внешних сторон, круг ответственности и интерфейсы с внешней стороной должны быть четко определены таким образом, чтобы можно было отключать и изолировать каждую организацию от других в течение соответствующего периода времени во избежание выявленных рисков.

Рекомендация по реализации

Энергетические компании должны следить за состоянием своих межсоединений.

Для того чтобы диагностировать проблемные зоны и принимать корректирующие меры, организации должны иметь средства для изоляции связей между собой и внешними сторонами и для повторного подключения изолированных связей, когда это необходимо.

Энергетические организации должны указывать в договорах или соглашениях, что межсистемные соединения могут быть приостановлены в тех случаях, когда возникают серьезные помехи в работе собственных служб организации.

Должны быть четко определены критерии и условия, необходимые для приостановления системных взаимосвязей. Кроме того, следует оценить возможные последствия приостановления системных взаимосвязей и при необходимости определить и подготовить резервные меры, если это необходимо.

Примечание — Этот элемент управления применяется не только к маршрутизированной сетевой связи, но и к последовательной связи.

12 Безопасность при эксплуатации

12.1 Эксплуатационные процедуры и обязанности

12.1.1 Документально оформленные эксплуатационные процедуры

Дополнительная рекомендация по реализации, приведенная в ИСО/МЭК 27002:2013, 12.1.1, является следующей:

В документации по эксплуатационным процессам должно быть точно указано, при каких условиях следует применять процедуры аварийного или кризисного управления.

12.1.2 Процесс управления изменениями

Дополнительная рекомендация по реализации, приведенная в ИСО/МЭК 27002:2013, 12.1.2, является следующей:

Изменение аппаратных систем часто приводит к изменению информационных систем и систем или приложений управления технологическими процессами из-за программного обеспечения, встроенного в эти системы. Все связанные с этим изменения должны контролироваться.

12.1.3 Управление производительностью

Дополнительная информация, относящаяся к энергетическому сектору, для ИСО/МЭК 27002:2013, 12.1.3, отсутствует.

12.1.4 Разделение сред разработки, тестирования и эксплуатации

Дополнительная рекомендация по реализации, приведенная в ИСО/МЭК 27002:2013, 12.1.4, является следующей:

Необходимо обеспечить надлежащую безопасность систем разработки и тестирования. В соответствии с их критичностью следует обеспечить, чтобы системы тестирования и разработки были достаточно изолированы от других систем и сетей (например, работа в изолированной сетевой среде, отсутствие прямого доступа в Интернет, отсутствие прямого доступа к другим операционным системам и т. д.) и чтобы они использовались исключительно для разработки и тестирования.

В области управления технологическими процессами энергетических предприятий разделение систем разработки, тестирования и эксплуатации не всегда возможно в полной мере. Это особенно верно в тех случаях, когда для разработки, тестирования, устранения неполадок и отладки требуются данные процесса в реальном времени. В этих особых случаях, когда требуются взаимосвязи между разработкой, тестированием и эксплуатационными системами или когда необходимо тестирование и отладка на уровне операционной системы, эти накладки должны быть сведены к абсолютному минимуму. Следует выявить возникающие в результате этого риски и рассмотреть возможные альтернативы, такие как эмуляторы данных технологического процесса или удаленная отладка (отладка операционной системы с использованием защищенных интерфейсов системы связи).

Если разделение систем разработки, тестирования и эксплуатации не может быть осуществлено, то следует разработать индивидуальные процедуры управления изменениями, инцидентами, чрезвычайными ситуациями и кризисными ситуациями, позволяющие быстро и адекватно реагировать на сбои и проблемы в операционной системе, совместимые с критичностью рассматриваемой системы.

12.2 Защита от вредоносных программ

12.2.1 Меры и средства информационной безопасности в отношении вредоносных программ

Дополнительная рекомендация по реализации, приведенная в ИСО/МЭК 27002:2013, 12.2.1, является следующей:

Если программное обеспечение, защищающее от вредоносных программ, не может быть развернуто по техническим причинам (например, из-за несовместимости систем управления технологическими процессами с антивирусным программным обеспечением, или в результате отсутствия поддержки поставщика или одобрения поставщика, или невозможности установки своевременных обновлений), то следует выявить возникающие риски и внедрить другие виды управления, обеспечивающие по меньшей мере равную степень защиты.

Другие средства борьбы с вредоносными программами включают в себя, среди прочего:

- защиту всех физических и логических интерфейсов передачи данных;
- сетевую изоляцию и реализацию сегментированных зон сетевой безопасности, ограничивающих воздействие инцидента с вредоносным ПО;
- комплексные меры по укреплению системы для минимизации риска инцидентов с вредоносными программами.

В частности, следует принимать во внимание возможные последствия инцидентов с вредоносными программами для оборудования, используемого для управления технологическими процессами в реальном времени и связанной с ними связи (например, в результате перегрузки и сбоев), и смягчать их путем внедрения соответствующих средств контроля.

12.3 Резервное копирование

Дополнительная информация, относящаяся к энергетическому сектору, для ИСО/МЭК 27002:2013, 12.3, отсутствует.

12.4 Регистрация и мониторинг

12.4.1 Регистрация событий

Дополнительная рекомендация по реализации, приведенная в ИСО/МЭК 27002:2013, 12.4.1, является следующей:

В энергетическом секторе соответствующие регистрационные журналы могут также включать определенные действия, выполняемые техническим персоналом, например, операции управления, коммутации, изменения параметров или установок, изменения в программах управления. Регистрационные журналы и обязательства по сохранению таких записей могут быть предусмотрены отраслевым законодательством и регулирующими органами для широкого спектра электронных документов.

Сбор, обработка и управление протоколами событий и данными должны осуществляться в соответствии со всеми применимыми деловыми, законодательными, нормативными и внутренними требованиями.

12.4.2 Защита информации регистрационных журналов

Дополнительная информация, относящаяся к энергетическому сектору, для ИСО/МЭК 27002:2013, 12.4.2, отсутствует.

12.4.3 Регистрационные журналы действий администратора и оператора

Дополнительная информация, относящаяся к энергетическому сектору, для ИСО/МЭК 27002:2013, 12.4.3, отсутствует.

12.4.4 Синхронизация часов

Дополнительная рекомендация по реализации, приведенная в ИСО/МЭК 27002:2013, 12.4.4, является следующей:

Для всех систем, которые прямо или косвенно связаны с внешними партнерами, следует использовать общий и согласованный стандарт времени, такой как всемирное координированное время (UTC).

Дополнительная информация, приведенная в ИСО/МЭК 27002:2013, 12.4.4, является следующей:

В зависимости от критичности рассматриваемой системы управления технологическими процессами следует рассмотреть вопрос об использовании выделенных, не синхронизированных через интернет серверов точного времени (NTP) или криптографически защищенных временных сообщений NTP для защиты целостности и подлинности данных временной синхронизации.

Для высокоточной синхронизации времени, согласно IEEE 1588, следует использовать коды аутентификации сообщений, которые описаны в приложении K IEEE 1588:2008. Информация о синхронизации времени в области измерений синхрофазора содержится в IEEE C37.118.

12.5 Контроль программного обеспечения, находящегося в эксплуатации

12.5.1 Установка программного обеспечения в эксплуатируемых системах

Дополнительная рекомендация по реализации, приведенная в ИСО/МЭК 27002:2013, 12.5.1, является следующей:

Энергетические компании должны минимизировать любой риск нарушения функционирования операционных систем, соблюдая следующие руководящие принципы по контролю изменений (управлению изменениями):

a) если изменения в приложениях и основных системах (например, программное обеспечение операционной системы, микропрограммное обеспечение) должны быть реализованы на критических активах, то комплексные тесты должны быть проведены заранее в специальной тестовой среде, максимально приближенной к среде операционной системы и ее взаимодействию с физическим процессом (см. 12.1.4);

b) в случае критических активов следует сохранять достаточное количество поколений программного обеспечения, наборов параметров и конфигурационных данных.

12.6 Менеджмент технических уязвимостей

12.6.1 Процесс управления техническими уязвимостями

Дополнительная рекомендация по реализации, приведенная в ИСО/МЭК 27002:2013, 12.6.1, является следующей:

Чтобы обеспечить адекватное управление техническими уязвимостями, энергетическая компания должна обеспечить получение полного и актуального перечня программного обеспечения (включая программное обеспечение внешних сторон) от системных интеграторов и поставщиков систем после каждой соответствующей установки, обновления или изменения программного обеспечения.

12.6.2 Ограничения на установку программного обеспечения

Дополнительная информация, относящаяся к энергетическому сектору, для ИСО/МЭК 27002:2013, 12.6.2, отсутствует.

12.7 Особенности аудита информационных систем

Дополнительная информация, относящаяся к энергетическому сектору, для ИСО/МЭК 27002:2013, 12.7, отсутствует.

12.8 ИБЭ-устаревшие системы

Дополнительная цель контроля, приведенная в разделе 12 ИСО/МЭК 27002:2013, является следующей:

Цель: защита от рисков, возникающих в результате использования устаревших систем, в которых не могут быть реализованы адекватные меры безопасности.

12.8.1 ИБЭ-учет устаревших систем

Мера обеспечения безопасности

Энергетическая компания должна обеспечить, чтобы все стандартные унаследованные технологии, системы и компоненты систем управления технологическими процессами (далее — унаследованные системы) были идентифицированы вместе с их потенциальными уязвимостями в области ИБ и чтобы соответствующие меры обеспечения безопасности осуществлялись в соответствии с определенным процессом обработки рисков информационной безопасности.

Рекомендация по реализации

Большое количество систем управления технологическими процессами, используемых в энергетике, основаны на устаревших технологиях, которые не имеют базовых функций безопасности. Для обеспечения надлежащего уровня безопасности необходимо определить риски, связанные с продолжающимся использованием устаревших систем и технологий. В ситуациях, когда стандартные меры обеспечения безопасности не могут быть реализованы, следует применять другие виды контрмер, например:

a) осуществление строгого и целесообразного изолирования в сетях;

b) следует избегать удаленного доступа для целей настройки и технического обслуживания. Если необходим удаленный доступ, то должна быть обеспечена надлежащая развязка сети, например, с помощью защищенных прокси-сервисов. Эти защищенные прокси-сервисы должны регулярно защищаться и исправляться. Доступ для целей технического обслуживания должен обеспечиваться только через определенные точки соединения, которые надежно эксплуатируются и контролируются;

c) строгие правила контроля доступа должны соблюдаться на сетевом, системном и прикладном уровнях.

Следует обеспечить, чтобы оборудование и компоненты, используемые для технического обслуживания и настройки устаревших систем, были надлежащим образом защищены.

12.9 ИБЭ-функции безопасности

Дополнительная цель контроля, приведенная в разделе 12 ИСО/МЭК 27002:2013, является следующей:

Цель: обеспечить целостность и доступность функций безопасности.

12.9.1 ИБЭ-целостность и доступность функций безопасности

Мера обеспечения безопасности

Целостность и доступность информации, активов, систем, компонентов и функций, необходимых для обеспечения функций безопасности, должны защищаться в соответствии с отраслевыми стандартами и требованиями нормативных правовых актов.

Рекомендация по реализации

Для обеспечения функций безопасности эксплуатации следует рассмотреть следующие меры:

a) использование специальных изолированных систем связи для передачи данных, связанных с безопасностью;

b) обеспечение, когда это возможно, независимости функций безопасности от систем управления технологическими процессами и автоматизации;

c) недопущение внесения изменений в критические системы безопасности и связанные с безопасностью конфигурационные данные с помощью средств удаленного доступа;

d) протоколирование изменений в конфигурации систем безопасности.

13 Безопасность системы связи

13.1 Менеджмент безопасности сетей

13.1.1 Меры и средства информационной безопасности для сетей

Дополнительная рекомендация по реализации, приведенная в ИСО/МЭК 27002:2013, 13.1.1, является следующей:

В области систем управления технологическими процессами в энергетическом секторе часто используются радио- и другие технологии беспроводной связи, например, для связи в широком диапазоне. При разработке сетевых средств управления особое внимание следует уделять безопасности этих технологий.

13.1.2 Безопасность сетевых сервисов

Дополнительная информация, относящаяся к энергетическому сектору, для ИСО/МЭК 27002:2013, 13.1.2, отсутствует.

13.1.3 Разделение в сетях

Дополнительная рекомендация по реализации, приведенная в ИСО/МЭК 27002:2013, 13.1.3, является следующей:

Там, где это применимо и технически осуществимо, сетевая инфраструктура систем управления технологическими процессами должна быть разделена на несколько зон с различными функциями и требованиями к защите. В частности, различные технические и эксплуатационные области должны быть отделены друг от друга.

Там, где это технически возможно, сетевые зоны должны быть разделены, например, брандмауэрами, однонаправленными шлюзами, фильтрующими маршрутизаторами или шлюзами. Сетевые соединения с внешними сетями, такими как корпоративная офисная сеть, внешние партнеры или удаленные соединения доступа к техническому обслуживанию, должны направляться исключительно через специально укрепленные прокси-серверы приложений, которые расположены в отдельной сетевой зоне (т. е. демилитаризованной зоне), специально предназначенной для этой цели.

Если это применимо и технически осуществимо, то сети и распределенные системы должны быть разделены на независимые горизонтальные сегменты (например, в зависимости от различных местоположений или производственных единиц). Эти сегменты должны быть разделены, например, брандмауэрами, однонаправленными шлюзами, фильтрующими маршрутизаторами или шлюзами.

13.1.4 ИБЭ-обеспечение безопасности передачи данных управления технологическим процессом

Дополнительная мера обеспечения безопасности, приведенная в ИСО/МЭК 27002:2013, 13.1, является следующей:

Мера обеспечения безопасности

Должны быть спроектированы, разработаны и внедрены меры по обеспечению требований безопасности, выявленных в ходе оценки рисков (например, конфиденциальность, целостность и доступность) передачи данных внутреннего и внешнего управления технологическими процессами.

Рекомендация по реализации

В области передачи данных управления технологическими процессами существует несколько отраслевых или общих технических стандартов и протоколов, таких как:

- МЭК 60870-5;
- МЭК 60870-6 (TASE.2);
- IEEE 1815 (DNP3);
- МЭК 61850;
- МЭК 61400-25;
- протокол Modbus.

Некоторые коммуникационные протоколы управления технологическими процессами не включают в себя специальные механизмы безопасности. Другие протоколы определяют дополнительные улучшения безопасности, которые не обязательно включаются во все реализации. Следует принимать во внимание риски, возникающие в результате этого, а также осуществление модифицированных контрмер. Контрмеры могут включать активацию уже поддерживаемых функций безопасности (например, в соответствии с МЭК 62351) или дополнительные меры криптографической защиты (например, шифрование, проверка целостности и аутентификация партнеров связи) на нижних уровнях связи.

Примечание — Элемент управления в 13.1.4 применяется не только к маршрутизированной сетевой связи, но и к последовательной связи.

13.1.5 ИБЭ-логическое соединение внешних систем управления технологическими процессами

Дополнительная мера обеспечения безопасности, приведенная в ИСО/МЭК 27002:2013, 13.1, является следующей:

Мера обеспечения безопасности

Прежде чем системы управления технологическими процессами и связанные с ними каналы связи с внешними сторонами будут логически соединены, энергетическая компания должна обеспечить оценку риска, возникающего в результате такого соединения систем, и возможность обмена по этому

каналу только разрешенными коммуникационными и информационными потоками, включая команды и сообщения системы управления.

Рекомендация по реализации

Системы управления технологическими процессами должны быть подсоединены к внешним системам только в том случае, если это необходимо по оперативным соображениям. Соединение должно осуществляться только в определенных точках соединения, которые надежно эксплуатируются и контролируются.

Следует определить и утвердить тип и объем разрешенных сообщений, включая необходимые команды обмена данными и управления. Следует рассмотреть возможность использования фильтрующих устройств (таких, как шлюзы, прокси-серверы или брандмауэры прикладного уровня) для разрешения только доверительных коммуникационных и информационных потоков.

13.2 Передача информации

Дополнительная информация, относящаяся к энергетическому сектору, для ИСО/МЭК 27002:2013, 13.2, отсутствует.

14 Приобретение, разработка и поддержка систем

14.1 Требования к безопасности информационных систем

14.1.1 Анализ и спецификация требований информационной безопасности

Дополнительная рекомендация по реализации, приведенная в ИСО/МЭК 27002:2013, 14.1.1, является следующей:

Для поддержки приобретения систем управления технологическими процессами в библиографии приводятся документы, относящиеся к энергетическому сектору, в качестве примеров, которые могут быть использованы при закупке систем.

14.1.2 Обеспечение безопасности прикладных сервисов, предоставляемых с использованием сетей общего пользования

Дополнительная информация, относящаяся к энергетическому сектору, для ИСО/МЭК 27002:2013, 14.1.2, отсутствует.

14.1.3 Защита транзакций прикладных сервисов

Дополнительная информация, относящаяся к энергетическому сектору, для ИСО/МЭК 27002:2013, 14.1.3, отсутствует.

14.2 Безопасность в процессах разработки и поддержки

14.2.1 Политика безопасной разработки

Дополнительная информация, относящаяся к энергетическому сектору, для ИСО/МЭК 27002:2013, 14.2.1, отсутствует.

14.2.2 Процедуры управления изменениями системы

Дополнительная информация, относящаяся к энергетическому сектору, для ИСО/МЭК 27002:2013, 14.2.2, отсутствует.

14.2.3 Техническая экспертиза приложений (прикладных программ) после изменений операционной платформы

Дополнительная информация, относящаяся к энергетическому сектору, для ИСО/МЭК 27002:2013, 14.2.3, отсутствует.

14.2.4 Ограничения на изменения пакетов программ

Дополнительная информация, относящаяся к энергетическому сектору, для ИСО/МЭК 27002:2013, 14.2.4, отсутствует.

14.2.5 Принципы безопасного проектирования систем

Дополнительная информация, относящаяся к энергетическому сектору, для ИСО/МЭК 27002:2013, 14.2.5, отсутствует.

14.2.6 Безопасная среда разработки

Дополнительная информация, относящаяся к энергетическому сектору, для ИСО/МЭК 27002:2013, 14.2.6, отсутствует.

14.2.7 Разработка с использованием аутсорсинга

Дополнительная информация, относящаяся к энергетическому сектору, для ИСО/МЭК 27002:2013, 14.2.7, отсутствует.

14.2.8 Тестирование безопасности систем

Дополнительная информация, относящаяся к энергетическому сектору, для ИСО/МЭК 27002:2013, 14.2.8, отсутствует.

14.2.9 Приемо-сдаточные испытания системы

Дополнительная информация, относящаяся к энергетическому сектору, для ИСО/МЭК 27002:2013, 14.2.9, отсутствует.

14.2.10 ИБЭ-минимизация функциональности

Дополнительная мера обеспечения безопасности, приведенная в ИСО/МЭК 27002:2013, 14.2, является следующей:

Мера обеспечения безопасности

Системы управления технологическими процессами должны быть спроектированы, сконфигурированы, эксплуатироваться и обслуживаться таким образом, чтобы обеспечивать только необходимые функции.

Рекомендация по реализации

Функциональные возможности системы управления технологическими процессами должны быть ограничены только теми, которые определены как необходимые для выполнения операций. Ненужные функции, программное обеспечение, порты, протоколы и службы должны быть задокументированы, а затем отключены и явно запрещены. Необходимые функции, программное обеспечение, порты, протоколы и службы также должны быть задокументированы и явно разрешены.

14.3 Тестовые данные

Дополнительная информация, относящаяся к энергетическому сектору, для ИСО/МЭК 27002:2013, 14.3, отсутствует.

15 Взаимоотношения с поставщиками

15.1 Информационная безопасность во взаимоотношениях с поставщиками

15.1.1 Политика информационной безопасности во взаимоотношениях с поставщиками

Дополнительная информация, относящаяся к энергетическому сектору, для ИСО/МЭК 27002:2013, 15.1.1, отсутствует.

15.1.2 Рассмотрение вопросов безопасности в соглашениях с поставщиками

Дополнительная рекомендация по реализации, приведенная в ИСО/МЭК 27002:2013, 15.1.2, является следующей:

В соответствии с условиями договорных соглашений следует обеспечить, чтобы требованиям защиты информации, относящейся к критически важным активам, уделялось достаточное внимание.

Владельцы активов должны пересмотреть все контракты, предусматривающие доступ внешних сторон к их системам управления технологическими процессами. Владельцы активов должны также оценить необходимость доступа внешних сторон к их системам управления технологическими процессами.

В тех случаях, когда телекоммуникационные услуги для систем управления технологическими процессами, используемых энергетическими компаниями, предоставляются внешними сторонами, должны быть определены, оговорены в контракте и контролироваться особые требования, касающиеся кризисной и аварийной связи, в частности в случае крупных отключений электроэнергии, стихийных бедствий, инцидентов или других возможных чрезвычайных ситуаций. Это относится в частности к любым необходимым превентивным мерам, которые могут потребоваться для предотвращения перегрузки услуг связи и обеспечения приемлемой степени независимости телекоммуникационных услуг от внешнего энергоснабжения (сопротивление отключению).

15.1.3 Цепочка поставок информационно-коммуникационной технологии

Дополнительная информация, относящаяся к энергетическому сектору, для ИСО/МЭК 27002:2013, 15.1.3, отсутствует.

15.2 Управление предоставлением услуги поставщиком

Дополнительная информация, относящаяся к энергетическому сектору, для ИСО/МЭК 27002:2013, 15.2, отсутствует.

16 Менеджмент инцидентов информационной безопасности

16.1 Менеджмент инцидентов информационной безопасности и улучшения

16.1.1 Обязанности и процедуры

Дополнительная информация, относящаяся к энергетическому сектору, для ИСО/МЭК 27002:2013, 16.1.1, отсутствует.

16.1.2 Сообщения о событиях информационной безопасности

Дополнительная информация, относящаяся к энергетическому сектору, для ИСО/МЭК 27002:2013, 16.1.2, отсутствует.

16.1.3 Сообщения о недостатках информационной безопасности

Дополнительная информация, относящаяся к энергетическому сектору, для ИСО/МЭК 27002:2013, 16.1.3, отсутствует.

16.1.4 Оценка и принятие решений в отношении событий информационной безопасности

Дополнительная информация, относящаяся к энергетическому сектору, для ИСО/МЭК 27002:2013, 16.1.4, отсутствует.

16.1.5 Реагирование на инциденты информационной безопасности

Дополнительная рекомендация по реализации, приведенная в ИСО/МЭК 27002:2013, 16.1.5, является следующей:

Мероприятия по реагированию должны включать сообщения в адрес других субъектов, которые могут быть затронуты той же предполагаемой причиной или которые могут иметь последствия от самого инцидента или от принятых мер реагирования. В тех случаях, когда для этой цели создается национальная или отраслевая команда реагирования на инциденты в компьютерной безопасности, она должна быть проинформирована по мере необходимости.

Сбор доказательств может вступать в противоречие с необходимостью своевременного восстановления системы для удовлетворения высоких требований к доступности и обеспечению безопасного энергоснабжения. Энергетическая компания должна определить, в каких случаях и для каких систем возможен сбор доказательств (см. 16.1.7).

16.1.6 Анализ инцидентов информационной безопасности

Дополнительная информация, относящаяся к энергетическому сектору, для ИСО/МЭК 27002:2013, 16.1.6, отсутствует.

16.1.7 Сбор свидетельств

Дополнительная информация, относящаяся к энергетическому сектору, для ИСО/МЭК 27002:2013, 16.1.7, отсутствует.

17 Аспекты информационной безопасности в рамках менеджмента непрерывности деятельности организации

17.1 Непрерывность информационной безопасности

Дополнительная информация, относящаяся к энергетическому сектору, для ИСО/МЭК 27002:2013, 17.1, отсутствует.

17.2 Резервирование оборудования

17.2.1 Доступность средств обработки информации

Дополнительная рекомендация по реализации, приведенная в ИСО/МЭК 27002:2013, 17.2.1, является следующей:

Энергетические компании должны рассматривать непрерывность общего энергоснабжения как одну из ключевых мер безопасности бизнеса при обеспечении безопасности населения в целом и сохранности активов. По этой причине следует рассмотреть концепции и процедуры аварийного восстановления для соответствующих аварийных и кризисных сценариев, влияющих на критические системы

управления технологическими процессами, например, запланированное отключение электричества, сбои и неисправности, для обеспечения доступности этих систем управления технологическими процессами.

При необходимости энергетические компании должны обеспечить резервирование средств связи с удаленными объектами с учетом таких факторов, как погодные условия.

Дополнительная информация для ИСО/МЭК 27002:2013, 17.2.1, является следующей:

ИСО/МЭК 27031 обеспечивает руководство по готовности информационно-коммуникационных технологий к непрерывности бизнеса.

17.2.2 ИБЭ-аварийная связь

Дополнительная мера обеспечения безопасности, приведенная в ИСО/МЭК 27002:2013, 17.2, является следующей:

Мера обеспечения безопасности

При возникновении крупных нарушений, стихийных бедствий, аварий или любых других чрезвычайных ситуаций или при наличии риска их возникновения энергетические компании должны обеспечивать поддержание основных линий связи со своим собственным аварийным персоналом и/или аварийным персоналом других коммунальных служб, с основными системами управления и с внешними аварийными организациями, необходимыми для защиты и устранения таких инцидентов.

Рекомендация по реализации

Основные линии связи могут быть использованы при передаче голосовой информации и данных, например:

- оперативным и аварийным персоналом в центральных или периферийных помещениях;
- внутренними и внешними антикризисными управляющими;
- электростанциями;
- предприятиями по добыче нефти и газа, а также выработки тепла;
- местами хранения энергии;
- распределенными производителями энергии;
- операторами систем передачи и распределения информации;
- метеорологическими организациями;
- организациями по предотвращению наводнений;
- пожарными службами;
- организациями по оказанию чрезвычайной помощи в случае стихийных бедствий;
- органами безопасности;
- провайдерами телекоммуникационных услуг;
- медицинскими организациями;
- другими национальными или местными организациями, занимающимися услугами первой необходимости.

Кроме того, аварийная связь может включать в себя каналы передачи данных со следующими системами:

- системами аварийного управления и связанными с ними подсистемами;
- системами аварийной сигнализации и мониторинга и связанными с ними подсистемами.

Особенно в области электроснабжения следует признать, что линии связи, необходимые для восстановления системы, в свою очередь могут опираться на электроснабжение.

18 Соответствие

18.1 Соответствие правовым и договорным требованиям

18.1.1 Идентификация применимых законодательных и договорных требований

Дополнительная рекомендация по реализации, приведенная в ИСО/МЭК 27002:2013, 18.1.1, является следующей:

Требования, характерные для энергетического сектора, могут включать в себя:

- требования, касающиеся защищенной, безопасной и надежной эксплуатации компонентов, систем и сетей энергетических объектов;
- требования, касающиеся недискриминации и разукрупнения регулируемых энергетических рынков;
- требования, касающиеся защиты критически важных инфраструктур;

- конкретные требования к защите данных, предъявляемые соответствующими регулирующими органами;

- другие нормативные требования.

В ходе планирования систем, которые будут иметь длительный срок службы, следует принимать во внимание, насколько это возможно, прогнозируемые изменения в требованиях, с тем, чтобы они могли быть реализованы с помощью управляемых усилий по модификации.

18.1.2 Права на интеллектуальную собственность

Дополнительная информация, относящаяся к энергетическому сектору, для ИСО/МЭК 27002:2013, 18.1.2, отсутствует.

18.1.3 Защита записей

Дополнительная информация, относящаяся к энергетическому сектору, для ИСО/МЭК 27002:2013, 18.1.3, отсутствует.

18.1.4 Конфиденциальность и защита персональных данных

Дополнительная информация, относящаяся к энергетическому сектору, для ИСО/МЭК 27002:2013, 18.1.4, отсутствует.

18.1.5 Регулирование криптографических мер и средств защиты информации

Дополнительная информация, относящаяся к энергетическому сектору, для ИСО/МЭК 27002:2013, 18.1.5, отсутствует.

18.2 Проверка информационной безопасности

18.2.1 Независимая проверка информационной безопасности

Дополнительная информация, относящаяся к энергетическому сектору, для ИСО/МЭК 27002:2013, 18.2.1, отсутствует.

18.2.2 Соответствие политикам и стандартам безопасности

Дополнительная информация, относящаяся к энергетическому сектору, для ИСО/МЭК 27002:2013, 18.2.2, отсутствует.

18.2.3 Анализ технического соответствия

Дополнительная рекомендация по реализации, приведенная в ИСО/МЭК 27002:2013, 18.2.3, является следующей:

Инструменты, используемые при оценке уязвимости или тестировании на проникновение в действующие системы управления технологическими процессами, должны быть надежно сконфигурированы во избежание сбоев. Для этой цели всегда следует отдавать предпочтение анализу пассивных режимов, даже если их эффективность хуже, чем у активных. Использование обнаруженных уязвимостей всегда должно осуществляться только в случае необходимости и с персоналом по реагированию на инциденты, готовым противостоять любому нарушению, которое может быть вызвано, включая отказ или неисправность целевой системы управления технологическими процессами.

Приложение А
(обязательное)

Типовые задачи управления и меры обеспечения безопасности в энергетическом секторе

Настоящее приложение расширяет действие приложения А ИСО/МЭК 27001:2013.

Типовые задачи управления и меры обеспечения безопасности, перечисленные в таблице А.1, непосредственно вытекают из задач управления и мер обеспечения безопасности, перечисленных в основном тексте настоящего стандарта, и согласуются с ними, а также должны использоваться в связи с положениями, изложенными в 4.2 и в приложении А ИСО/МЭК 27001:2013.

Таблица А.1 — Конкретные цели и меры обеспечения безопасности в энергетическом секторе

А.6 Организация деятельности по информационной безопасности		
А.6.1 Внутренняя организация деятельности по обеспечению информационной безопасности		
Цель: создание системы управления для инициирования и контроля внедрения и обеспечения информационной безопасности в рамках организации		
6.1.6	ИБЭ-идентификация рисков, связанных с внешними сторонами	Мера обеспечения безопасности. Перед предоставлением доступа к информации и средствам обработки информации организации следует выявить риски, связанные с бизнес-процессами, в которых участвуют внешние стороны, и внедрить соответствующие меры обеспечения безопасности
6.1.7	ИБЭ-решение вопросов безопасности при работе с потребителями	Мера обеспечения безопасности. Все выявленные требования безопасности должны быть учтены до предоставления потребителям доступа к информации или активам предприятия
А.11 Физическая безопасность и защита от воздействия окружающей среды		
А.11.1 Зоны безопасности		
Цель: предотвращение несанкционированного физического доступа, повреждения и вмешательства в работу информационных систем и средств обработки информации организации		
11.1.7	ИБЭ-обеспечение безопасности центров управления	Мера обеспечения безопасности. Следует спроектировать, разработать и применять меры по обеспечению физической безопасности центров управления, например, там, где размещены серверы систем управления, ЧМИ и вспомогательные системы
11.1.8	ИБЭ-обеспечение безопасности для помещений с оборудованием	Мера обеспечения безопасности. Следует спроектировать, разработать и внедрить меры по обеспечению физической безопасности помещений, в которых расположены системы управления, используемые энергетическими предприятиями
11.1.9	ИБЭ-защита периферийных объектов	Мера обеспечения безопасности. Для периферийных объектов, где расположено оборудование системы управления, используемое энергетическими компаниями, должны быть спроектированы, разработаны и внедрены средства управления физической безопасности или применены соответствующие контрмеры для снижения риска, если достаточный уровень физической защиты периферийных объектов недостижим

Продолжение таблицы А.1

11.3 ИБЭ-безопасность в служебных помещениях третьих лиц		
Цель: защита оборудования, находящегося вне помещений энергетических компаний, от физических угроз и угроз окружающей среды		
11.3.1	ИБЭ-оборудование, расположенное на территории других энергетических компаний	Мера обеспечения безопасности. В тех случаях, когда энергетические компании устанавливают оборудование за пределами своих собственных объектов или помещений в районах, находящихся под ответственностью других энергетических компаний, как например при межсистемной связи станций, оборудование должно быть размещено на охраняемой территории, с тем чтобы снизить любые риски, связанные с угрозами окружающей среды, и уменьшить вероятность несанкционированного доступа
11.3.2	ИБЭ-оборудование, размещенное на территории потребителя	Мера обеспечения безопасности. В тех случаях, когда энергетические компании устанавливают оборудование в помещениях потребителя, например для контроля или измерения поставок энергии и/или предоставления дополнительных услуг, оборудование компаний должно быть защищено таким образом, чтобы снизить любые риски, связанные с угрозами окружающей среды, и уменьшить вероятность несанкционированного доступа
11.3.3	ИБЭ-взаимосвязанные системы управления и связи	Мера обеспечения безопасности. В тех случаях, когда системы управления и связанные с ними линии связи взаимосвязаны с системами внешних сторон, круг ответственности и интерфейсы с внешней стороной должны быть четко определены таким образом, чтобы можно было отключать и изолировать каждую организацию от других в течение соответствующего периода времени во избежание выявленных рисков
А.12 Безопасность при эксплуатации		
12.8 ИБЭ-устаревшие системы		
Цель: защита от рисков, возникающих в результате использования устаревших систем, когда адекватные меры безопасности не могут быть реализованы		
12.8.1	ИБЭ-учет устаревших систем	Мера обеспечения безопасности. Энергетическая компания должна обеспечить, чтобы все стандартные унаследованные технологии, системы и компоненты систем управления технологическими процессами (далее — унаследованные системы) были идентифицированы вместе с их потенциальными уязвимостями в области ИБ и чтобы соответствующие меры обеспечения безопасности осуществлялись в соответствии с определенным процессом обработки рисков информационной безопасности
12.9 ИБЭ-функции безопасности		
Цель: обеспечить целостность и доступность функций безопасности		
12.9.1	ИБЭ-целостность и доступность функций безопасности	Мера обеспечения безопасности. Целостность и доступность информации, активов, систем, компонентов и функций, необходимых для обеспечения функций безопасности, должны защищаться в соответствии с отраслевыми стандартами и требованиями нормативных правовых актов
А.13 Безопасность системы связи		
А.13.1 Менеджмент безопасности сетей		
Цель: обеспечение защиты информации в сетях и ее вспомогательной обработке		

Окончание таблицы А.1

13.1.4	ИБЭ-обеспечение безопасности передачи данных управления технологическим процессом	Мера обеспечения безопасности. Должны быть спроектированы, разработаны и внедрены меры по обеспечению требований безопасности, выявленных в ходе оценки рисков (например, конфиденциальность, целостность и доступность), передачи данных внутреннего и внешнего управления технологическими процессами
13.1.5	ИБЭ-логическое соединение внешних систем управления технологическими процессами	Мера обеспечения безопасности. Прежде чем системы управления технологическими процессами и связанные с ними каналы связи с внешними сторонами будут логически соединены, энергетическая компания должна обеспечить оценку риска, возникающего в результате такого соединения систем, и возможность обмена по этому каналу только разрешенными коммуникационными и информационными потоками, включая команды и сообщения системы управления
А.14 Приобретение, разработка и поддержка систем		
А.14.2 Безопасность в процессах разработки и поддержки		
Цель: обеспечить, чтобы информационная безопасность проектировалась и реализовывалась в рамках жизненного цикла разработки информационных систем		
14.2.10	ИБЭ-минимизация функциональности	Мера обеспечения безопасности. Системы управления технологическими процессами должны быть спроектированы, сконфигурированы, эксплуатироваться и обслуживаться таким образом, чтобы обеспечивать только необходимые функции
А.17 Аспекты информационной безопасности в рамках менеджмента непрерывности деятельности организации		
А.17.2 Резервирование оборудования		
Цель: обеспечение доступности средств обработки информации		
17.2.2	ИБЭ-аварийная связь	Мера обеспечения безопасности. При возникновении крупных нарушений, стихийных бедствий, аварий или любых других чрезвычайных ситуаций или при наличии риска их возникновения энергетические компании должны обеспечивать поддержание основных линий связи со своим собственным аварийным персоналом и/или аварийным персоналом других коммунальных служб, с основными системами управления и с внешними аварийными организациями, необходимыми для защиты и устранения таких инцидентов

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов национальным стандартам

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
ISO/IEC 27000	IDT	ГОСТ Р ИСО/МЭК 27000—2012 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология»
ISO/IEC 27001:2013	—	*
ISO/IEC 27002:2013	—	*

* Соответствующий национальный стандарт отсутствует. До его принятия рекомендуется использовать перевод на русский язык данного международного стандарта. Перевод данного международного стандарта находится в Федеральном информационном фонде стандартов.

Примечание — В настоящей таблице использовано следующее условное обозначение степени соответствия стандарта:

- IDT — идентичный стандарт.

Библиография

[1] IEC 62645:2014, Nuclear power plants — Instrumentation and control systems — Requirements for security programmes for computer-based systems

[2] IEC 62351 (all parts), Power systems management and associated information exchange — Data and communications security

[3] IEC/TS 62351-8:2011, Power systems management and associated information exchange — Data and communications security — Part 8: Role-based access control

[4] IEC/TS 62443-1-1:2009, Industrial communication networks — Network and system security — Part 1-1: Terminology, concepts and models

[5] CEN-CENELEC-ETSI. SGIS (Smart Grid Information Security). 2014

[6] NIST. NISTIR 7628Revision 1 Guidelines for Smart Grid Cybersecurity. September 2014

[7] NERC CIP. North American Electric Reliability Corporation Critical Infrastructure Protection Version 6. 2015

[8] BDEW Bundesverband der Energie- und Wasserwirtschaft e. V.and Osterreichs E-Wirtschaft: Whitepaper. Requirements for Secure Control and Telecommunication Systems Version 1.1. March 2015

[9] US Department of Energy (DoE), Cybersecurity Procurement Language for Energy Delivery Systems. April 2014

[10] NIST. Special Publication (SP) 800-82 Revision 2. Guide to Industrial Control Systems (ICS) Security. May 2015

УДК 006.34:004.056:004.056.5:004.056.53:006.354 ОКС 35.030

Ключевые слова: информационная безопасность, информационная безопасность в энергетике, системы управления технологическими процессами в энергетике

Технический редактор *В.Н. Прусакова*
Корректор *М.И. Першина*
Компьютерная верстка *Л.А. Круговой*

Сдано в набор 21.05.2021. Подписано в печать 28.05.2021. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 4,65. Уч.-изд. л. 4,20.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении во ФГУП «СТАНДАРТИНФОРМ»
для комплектования Федерального информационного фонда стандартов,
117418 Москва, Нахимовский пр-т, д. 31, к. 2.
www.gostinfo.ru info@gostinfo.ru