ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р МЭК 62988— 2023

БЕСПРОВОДНЫЕ УСТРОЙСТВА СИСТЕМ КОНТРОЛЯ И УПРАВЛЕНИЯ, ВАЖНЫЕ ДЛЯ БЕЗОПАСНОСТИ АТОМНЫХ СТАНЦИЙ

Порядок выбора и использования по назначению

(IEC 62988:2018, Nuclear power plants — Instrumentation and control systems important to safety — Selection and use of wireless devices, IDT)

Издание официальное

Москва
Российский институт стандартизации
2023

Предисловие

1 ПОДГОТОВЛЕН Акционерным обществом «Русатом Автоматизированные системы управления» (АО «РАСУ») на основе собственного перевода на русский язык англоязычной версии стандарта, указанного в пункте 4

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 322 «Атомная техника»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 19 июня 2023 г. № 408-ст

4 Настоящий стандарт идентичен международному стандарту МЭК 62988:2018 «Атомные электростанции. Системы контроля и управления, важные для безопасности. Выбор и использование беспроводных устройств» (IEC 62988:2018 «Nuclear power plants — Instrumentation and control systems important to safety — Selection and use of wireless devices», IDT).

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 тексте настоящего стандарта, выделенные курсивом, приведены для пояснения текста оригинала

5 ВВЕДЕН ВПЕРВЫЕ

6 Положения настоящего стандарта действуют в целом в отношении атомных станций, сооружаемых по российским проектам за пределами Российской Федерации.

Положения настоящего стандарта могут применяться в отношении атомных станций, сооружаемых или модернизируемых в Российской Федерации, в части, не противоречащей требованиям федеральных норм и правил, действующих в области использования атомной энергии

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.rst.gov.ru)

Содержание

Введение

a) Техническая справка, основные вопросы и организация настоящего стандарта

Настоящий стандарт устанавливает требования к беспроводным устройствам, применяемым на атомных станциях для реализации важных для безопасности функций.

Настоящий стандарт предназначен для использования операторами АС (эксплуатирующими организациями), экспертами по оценке систем (системотехниками) и лицензирующими органами.

b) Положение настоящего стандарта в структуре серии стандартов подкомитета МЭК ПК 45А

МЭК 62988 является стандартом третьего уровня серии стандартов ПК 45А МЭК, в котором рассмотрены выбор и использование беспроводных устройств в составе важных для безопасности систем контроля и управления (СКУ), используемых на АС.

Более подробное описание структуры серии стандартов ПК 45А МЭК приведено в пункте d) настоящего введения.

c) Рекомендации и ограничения, касающиеся применения настоящего стандарта

Важно отметить, что настоящий стандарт применим ко всем важным для безопасности системам, содержащим беспроводные устройства, включая системы, выполняющие функции категорий А и В (при этом настоящим стандартом использование беспроводных устройств в таких системах запрещено). Таким образом, выполнение требований настоящего стандарта распространяется только на системы, реализующие функции категории С.

Для гарантии того, что настоящий стандарт останется актуальным в будущем, особое внимание уделено принципиальным вопросам, а не конкретным технологиям.

d) Описание структуры серии стандартов подкомитета МЭК ПК 45А и их взаимосвязи с другими документами МЭК и документами других организаций (МАГАТЭ, ИСО)

Стандартами самого высокого уровня серии стандартов ПК 45А МЭК являются МЭК 61513 и МЭК 63046. МЭК 61513 содержит общие требования к СКУ и оборудованию, используемым для выполнения важных для безопасности АС функций. МЭК 63046 содержит общие требования к электроэнергетическим системам АС и распространяется на системы электроснабжения, включая системы питания СКУ. МЭК 61513 и МЭК 63046 следует рассматривать вместе и на одном уровне. МЭК 61513 и МЭК 63046 формируют структуру серии стандартов ПК 45А МЭК и определяют законченную, четкую и логичную концепцию, определяющую общие требования к системам контроля и управления и к электротехническим системам атомных станций.

МЭК 61513 и МЭК 63046 содержат прямые ссылки на другие стандарты ПК 45А МЭК по общим вопросам, связанным с категоризацией функций и классификацией систем, квалификацией, разделением, защитой от отказов по общим причинам, проектированием пунктов управления, электромагнитной совместимостью, кибербезопасностью, программными и аппаратными аспектами программируемых цифровых систем, согласованием требований безопасности и защиты информации и управлением старением. Стандарты, на которые напрямую ссылаются МЭК 61513 и МЭК 63046, являющиеся стандартами второго уровня, следует рассматривать вместе с МЭК 61513 и МЭК 63046 как единый комплект документов.

Третий уровень стандартов ПК 45А МЭК составляют стандарты, на которые отсутствуют прямые ссылки в МЭК 61513 или МЭК 63046, относящиеся к конкретному оборудованию, техническим методам или определенным видам деятельности. Как правило, эти стандарты, содержащие ссылки на стандарты второго уровня по общим темам, могут быть использованы самостоятельно.

Четвертый уровень документов ПК 45А МЭК представлен техническими отчетами, которые не являются нормативными документами.

Серия стандартов ПК 45А МЭК постоянно реализует и детализирует принципы безопасности и защиты информации, а также базовые аспекты, содержащиеся в соответствующих стандартах безопасности МАГАТЭ и соответствующей серии документов МАГАТЭ по ядерной безопасности (NSS). В частности, к этим документам относятся нормы безопасности МАГАТЭ SSR-2/1, устанавливающие требования безопасности, связанные с проектированием АС, руководство по безопасности МАГАТЭ SSG-30, в котором рассмотрена классификация безопасности конструкций, систем и компонентов АС, руководство по безопасности МАГАТЭ SSG-39, относящееся к проектированию систем контроля и управления АС, руководство по безопасности МАГАТЭ SSG-34, рассматривающее проектирование электроэнергетических систем для АС, а также внедряемое руководство NSS17 по компьютерной безопасности оборудования атомных станций. Термины и определения, используемые в стандартах ПК 45А по безопасности и защите информации, соответствуют терминам и определениям, используемым в документах МАГАТЭ.

МЭК 61513 и МЭК 63046 представлены в том же формате, что и основной стандарт по безопасности МЭК 61508, с той же схемой жизненного цикла в целом и схемой жизненного цикла системы. В отношении ядерной безопасности МЭК 61513 и МЭК 63046 содержат толкование основных требований, действующих в атомной энергетике и изложенных в МЭК 61508-1, МЭК 61508-2 и МЭК 61508-4. В этой структуре МЭК 60880, МЭК 62138 и МЭК 62566 соответствуют МЭК 61508-3 для атомной энергетики. МЭК 61513 и МЭК 63046 содержат ссылки на документы ИСО, а также на документы МАГАТЭ GS-R-3, МАГАТЭ GS-G-3.1 и МАГАТЭ GS-G-3.5 по вопросам, связанным с обеспечением качества (ОК). На втором уровне по вопросам ядерной безопасности вводным документом для серии стандартов по безопасности ПК 45А МЭК является МЭК 62645. Он основан на действующих принципах высокого уровня и главных концепциях стандартов по безопасности, в частности ИСО/МЭК 27001 и ИСО/МЭК 27002. МЭК 62645 адаптирует и дополняет их применительно к атомной отрасли и приводит в соответствие с серией стандартов МЭК 62443. По пунктам управления на втором уровне первичным документом для стандартов ПК 45А МЭК является МЭК 60964, а по вопросам управления старением — МЭК 62342.

Примечание — Предполагается, что при проектировании систем контроля и управления АС, реализующих стандартные функции безопасности (например, обеспечение безопасности работников, защита объекта, химическая безопасность, энергетическая безопасность технологических процессов), будут применяться международные или национальные стандарты.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

БЕСПРОВОДНЫЕ УСТРОЙСТВА СИСТЕМ КОНТРОЛЯ И УПРАВЛЕНИЯ, ВАЖНЫЕ ДЛЯ БЕЗОПАСНОСТИ АТОМНЫХ СТАНЦИЙ

Порядок выбора и использования по назначению

Wireless devices in instrumentation and control systems important to safety of nuclear power plants. Order of selection and intended use

Дата введения — 2023—09—01

1 Область применения

Настоящий стандарт устанавливает требования, относящиеся к выбору и использованию беспроводных устройств в составе систем контроля и управления (СКУ), важных для безопасности, применяемых на атомных станциях (АС). Такие СКУ могут целиком состоять из беспроводных устройств.

Примечание — Слово «использование» обозначает интеграцию устройства, его квалификацию, административный контроль, а также любые иные действия, которые могут потребоваться для применения устройства в целях обеспечения безопасности.

Настоящий стандарт применим в отношении СКУ новых АС, а также при незначительной модификации СКУ действующих АС. В область распространения настоящего стандарта входят любые беспроводные устройства или беспроводные системы, важные для безопасности. Область распространения включает в себя как стационарные, так и мобильные устройства, и устройства, обеспечивающие любые типы данных (голосовая связь, обработка данных и т. д.), при условии, что ими реализуется классифицируемая по безопасности функция.

Настоящий стандарт ограничивает использование беспроводных устройств системами, поддерживающими функции категории С согласно МЭК 61226, однозначно исключая их использование для выполнения функций категорий А и В.

Настоящий стандарт может быть использован в качестве руководства для работы с беспроводными устройствами и системами, напрямую не участвующими в обеспечении безопасности, например для доказательства отсутствия помех в работе устройств, важных для безопасности.

В разделе 5 приведено описание фундаментальных требований к безопасности и кибербезопасности.

В разделе 6 представлены требования конкретно к беспроводным устройствам, которые должны быть учтены при проектировании системы.

В разделе 7 приведены требования к выбору и интеграции беспроводных устройств.

Раздел 8 посвящен вопросам электромагнитной совместимости и управления спектром.

В разделе 9 приведены требования к беспроводным устройствам, имеющие отношение к кибербезопасности.

В разделе 10 описаны требования к квалификации беспроводных устройств и среде, в которой их используют.

2 Нормативные ссылки

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

Издание официальное

IEC/IEEE 60780-323, Nuclear facilities — Electrical equipment important to safety — Qualification (Объекты использования атомной энергии. Электрооборудование, важное для безопасности. Квалификация)

IEC 60987:2007, Nuclear power plants — Instrumentation and control important to safety — Hardware design requirements for computer-based systems (Электростанции атомные. Контрольно-измерительные приборы и системы управления, важные для обеспечения безопасности. Требования к проектированию аппаратуры для компьютерных систем)[1)]

IEC 61513:2011, Nuclear power plants — Instrumentation and control important to safety — General requirements for systems (Атомные станции. Системы контроля и управления, важные для безопасности. Общие требования)

IEC 62138, Nuclear power plants — Instrumentation and control important for safety — Software aspects for computer-based systems performing category B or C functions (Атомные электростанции. Системы контроля и управления, важные для безопасности. Программное обеспечение компьютерных систем, выполняющих функции категории В или С)

IEC 62645, Nuclear power plants — Instrumentation and control systems — Requirements for security programmes for computer-based systems (Атомные электростанции. Системы контроля и управления. Требования к программам обеспечения безопасности для компьютерных систем)

IEC 62671, Nuclear power plants — Instrumentation and control important to safety — Selection and use of industrial digital devices of limited functionality (Атомные электростанции. Системы контроля и управления, важные для безопасности. Выбор и использование промышленных цифровых устройств ограниченной функциональности)

3 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями:

3.1 **аутентификация** (authentication): Обеспечение гарантии того, что заявленные характеристики объекта являются подлинными.

[ИСО/МЭК 27000:2018, 3.5]

3.2 **категория функции контроля и управления** (category of an I&C function): Одно из трех возможных обозначений (А, В, С) функций СКУ, устанавливаемых в соответствии со значимостью выполнения функции для безопасности[2)].

Примечания

1 См. также термин «класс СКУ».

2 Категории функций СКУ устанавливают в соответствии с МЭК 61226. Каждой категории соответствует набор требований, применяемый как к каждой функции (требования к спецификации, проектированию, реализации, верификации и валидации), так и ко всей цепочке элементов, которые необходимы для реализации функции (требования к свойствам и соответствующей квалификации), независимо от того, как эти элементы распределены в ряду взаимосвязанных СКУ. Другими словами, настоящий стандарт определяет категории функций СКУ и классы СКУ и устанавливает связь между категорией функции и минимальным требуемым классом соответствующих систем и оборудования.

[МЭК 61513:2011, 3.4]

3.3 **класс СКУ** (class of an I&C system): Одно из трех возможных обозначений (1, 2, 3) СКУ, важных для безопасности, присваиваемых в соответствии с необходимостью их использования для выполнения функций СКУ различной степени важности для безопасности[3)].

[1)] *Действует IEC 60987:2021 «Nuclear power plants — Instrumentation and control important to safety — Hardware requirements». Однако для однозначного соблюдения требований стандарта, приведенного в датированной ссылке, рекомендуется использовать только указанное в этой ссылке издание.*

[2)] *Согласно НП-026-16 «Требования к управляющим системам, важным для безопасности атомных станций» в российских нормативных документах в области использования атомной энергии управляющим и информационным функциям назначают категории в соответствии с федеральными нормами и правилами в области использования атомной энергии.*

[3)] *Федеральные нормы и правила в области использования атомной энергии НП-001-15 «Общие положения обеспечения безопасности атомных станций» устанавливают классификацию элементов по классам безопасности 1, 2, 3, 4 в зависимости от влияния отказа конкретного элемента на безопасность АС.*

Примечание — См. также термины «категория функции контроля и управления», «система безопасности».

[МЭК 61513:2011, 3.6]

3.4 **управление спектром, обеспечение совместимости** (spectrum management, coexistence management): Процесс создания и поддержания совместимости, включающий в себя организационно-технические мероприятия.

[МЭК 62657-2:2017, 3.1.14, измененный — добавлен предпочтительный термин «управление спектром»]

3.5 **кибербезопасность** (cybersecurity): Комплекс действий и мер, направленных на предотвращение, выявление и реагирование на цифровые атаки, совершаемые с целью:

- раскрытия информации, которая может быть использована для совершения злоумышленных действий, результатом которых может стать авария, небезопасная ситуация или ухудшение эксплуатационных показателей АС (несоблюдение конфиденциальности);
- злоумышленной модификации функций, которая может поставить под угрозу доставку информации или целостность, обеспечиваемые системами на основе компьютерных или HDL-программируемых устройств[1)] (включая потерю управления), результатом чего может стать авария, небезопасная ситуация или ухудшение эксплуатационных показателей АС (нарушение целостности);
- злоумышленной приостановки или прекращения доступа к информации, данным или ресурсам, а также их передачи (включая утрату возможности просмотра), что может привести к отказу необходимого сервиса, реализуемого СКУ, результатом чего может стать авария, небезопасная ситуация или ухудшение эксплуатационных показателей АС (нарушение доступности).

Примечание — Данное определение адаптировано с учетом области применения настоящего стандарта, где первоочередное внимание уделяется предотвращению, выявлению и реагированию на злоумышленные действия, совершаемые с использованием цифровых средств в отношении СКУ на основе компьютерных или HDL-программируемых устройств. Следует отметить, что термин «кибербезопасность» в других стандартах и руководствах трактуется более широко, часто включая неумышленные действия, человеческие ошибки и защиту от природных катастроф, которые в данном стандарте не рассматриваются (см. раздел 1).

[МЭК 62645:2014, 3.6]

3.6 **электрический/электронный/программируемый элемент;** Э/Э/ПЭ-элемент (electrical/electronic/programmable electronic item, E/E/PE item): Элемент, основанный на электрической (Э), и/или электронной (Э), и/или программируемой электронной (ПЭ) технологии.

[МЭК 61508-4:2010, 3.3.2, измененный]

Примечание — В данном термине и его определении слово «элемент» может быть заменено следующими словами: система, оборудование или устройство.

3.7 **шифрование** (encryption): Зависящий от криптографического ключа процесс обратимого преобразования открытого текста в шифрованный текст[2)].

[ИСО/МЭК 18033-1:2015, 2.21]

3.8 **точка доступа; шлюз** (access point, gateway): Сетевое устройство, включающее по меньшей мере один хост-интерфейс, например интерфейс последовательной передачи данных или Ethernet, действующий в качестве входной или выходной точки, обеспечивающий передачу данных между хост-приложениями и беспроводными устройствами.

[МЭК 62591:2016, 3.2.47, измененный — добавлен предпочтительный термин «точка доступа»]

3.9 **система контроля и управления;** СКУ (I&C system): Система, основанная на Э/Э/ПЭ-элементах, выполняющая функции контроля и управления АС, а также функции эксплуатации и мониторинга, связанные с работой самой системы.

Примечания

1 Данный термин используют как общий, включающий в себя все элементы системы, такие как внутренние источники электроснабжения, датчики и другие устройства ввода данных, магистрали передачи данных и другие

[1)] *Устройство, программируемое на языке описания аппаратных средств (HDL-программируемое устройство) — это интегральная схема, конфигурируемая (для СКУ АС) с помощью языков описания аппаратных средств и соответствующих программных инструментов (МЭК 62645, 3.11).*

[2)] *Адаптировано из ИСО/МЭК 18033-1:2021, 3.11. См. также ИСО/МЭК 11770-1:2010, 2.10; ИСО/МЭК 9797-1:2011, 3.6; ИСО/МЭК 11770-3:2021, 3.9.*

коммуникационные тракты, интерфейсы исполнительных механизмов и прочие устройства вывода. Различные функции внутри системы могут использовать специальные или общие ресурсы.

2 Элементы, включенные в конкретную СКУ, определены в спецификации границ системы.

3 См. также определение термина «Э/Э/ПЭ-элемент» и примечание к нему.

4 В соответствии с их стандартным функционалом МАГАТЭ подразделяет СКУ на системы автоматизации/управления, системы ЧМИ, системы блокировки и системы защиты.

3.10 **элемент, важный для безопасности** (item important to safety): Элемент, который является частью группы безопасности[1)] и/или неисправность или отказ которого может привести к радиационному облучению персонала на площадке или населения и/или к превышению установленных нормативов по выбросам и сбросам[2)].

Примечание — Элементы, важные для безопасности, включают в себя:

a) конструкции, системы и компоненты системы, неисправность или отказ которых могут приводить к чрезмерному радиационному облучению персонала на площадке или населения;

b) конструкции, системы и компоненты систем, которые препятствуют перерастанию нарушений нормальной эксплуатации в аварийные условия;

c) средства, которые предусмотрены для смягчения последствий неисправности или отказа конструкций, систем и компонентов системы.

[Глоссарий МАГАТЭ по вопросам безопасности, 2016]

3.11 **задержка** (latency): Время, необходимое для передачи пакета(ов) от отправителя к получателю через сетевое подключение.

[МЭК 62591:2016, 3.2.57]

3.12 **сеть с ячеистой структурой** (mesh network): Сетевая топология, при которой между каждой парой сетевых узлов имеются резервированные физически разнообразные пути маршрутизации.

Примечание — Беспроводная сеть с ячеистой структурой используется для расширения покрытия за счет возможности использования нескольких протоколов и/или повышения надежности передачи данных за счет организации резервированных маршрутов между устройствами.

[МЭК 62734:2014, 3.1.2.95, измененный — термин «сеточная топология» заменен термином «сеть с ячеистой структурой»]

3.13 **сеть** (network): Последовательность устройств, соединенных между собой коммуникационной средой одного типа.

[МЭК 62591:2016, 3.2.70, измененный — в определении слово «узлы» заменено на «устройства»; удалено примечание 1]

3.14 **обеспечение качества** (quality assurance): Функция системы управления качеством, которая обеспечивает уверенность в том, что установленные требования будут выполнены.

Примечание — Данное определение сопоставимо с определением, приведенным в ИСО 9000:2015, 3.3.6.

[Глоссарий МАГАТЭ по вопросам безопасности, 2016 измененный — термин «управление качеством» заменен термином «обеспечение качества»]

3.15 **резервирование** (redundancy): Обеспечение альтернативных (однотипных или разнотипных) конструкций, систем и элементов, чтобы любая конструкция, система или элемент могли выполнять требующуюся функцию независимо от эксплуатационного состояния или отказа любой другой из них.

[Глоссарий МАГАТЭ по вопросам безопасности, 2016]

3.16 **система, связанная с безопасностью** (safety related system): Система, важная для безопасности и не входящая в систему безопасности.

[Глоссарий МАГАТЭ по вопросам безопасности, 2016]

---

1) *Согласно ГОСТ Р МЭК 61513—2020, пункт 3.46: «Группа безопасности — группа оборудования, предназначенная для выполнения всех действий, требующихся в случае конкретного постулируемого в проекте исходного события, с целью обеспечить невозможность превышения пределов, установленных в проекте для ожидаемых при эксплуатации событий и проектных аварий».*

2) *Согласно НП-001-15, приложение № 2, пункт 97: «Элементы АС (элементы) — строительные конструкции, оборудование, приборы, трубопроводы, средства измерения, контроля, управления и автоматики, кабели и другие изделия, обеспечивающие выполнение заданных функций самостоятельно или в составе систем и рассматриваемые в проекте АС в качестве структурных единиц при выполнении анализов надежности и безопасности».*

3.17 **система безопасности** (safety system): Система, важная для безопасности, обеспечивающая безопасный останов реактора или отвод остаточного тепла из активной зоны либо ограничивающая последствия ожидаемых при эксплуатации событий и проектных аварий[1)].

[Глоссарий МАГАТЭ по вопросам безопасности, 2016]

3.18 **беспроводное устройство** (wireless device): Устройство, которое может устанавливать беспроводное подключение к другому беспроводному устройству, которое может как входить, так и не входить в состав беспроводной сети.

4 Сокращения

В настоящем стандарте использованы следующие сокращения:

АС — атомная станция (nuclear power plant, NPP);

ДМЗ — демилитаризованная зона (demilitarized zone, DMZ);

РЧИ — радиочастотное излучение (radio frequency interference, RFI);

СКУ — система контроля и управления (instrumentation and control system, I&C system);

ССТ — спецификация системных требований (system requirement specification, SRS);

ЦПУ — центральное процессорное устройство (central processing unit, CPU);

ЭМИ — электромагнитное излучение (electromagnetic interference, EMI);

ЭМС — электромагнитная совместимость (electromagnetic compatibility, EMC).

5 Фундаментальные требования

5.1 Классификация по безопасности

Беспроводные устройства необходимо применять только в СКУ, выполняющих функции категории С, и не следует применять в СКУ, поддерживающих функции категорий А и В.

Класс безопасности беспроводных коммуникационных систем должен соответствовать категории С функций СКУ, поддерживаемых и реализуемых ими. Такие коммуникационные системы должны быть отнесены к классу безопасности 3.

5.2 Физическое разделение и изоляция

Беспроводные коммуникационные системы должны быть гальванически развязаны и физически отделены от проводных коммуникационных каналов СКУ, поддерживающих функции категорий А и В.

Беспроводные коммуникационные системы для функций категории С должны быть спроектированы таким образом, чтобы любые их отказы не влияли на проводные коммуникационные каналы СКУ, выполняющих функции категорий А и В.

5.3 Кибербезопасность

Не допускается использование беспроводной передачи данных в системах, отнесенных к степени защищенности S1 или S2 в соответствии с МЭК 62645.

Каждое сетевое подключение к системам с более высоким классом безопасности следует рассматривать в рамках общего плана кибербезопасности в целях реализации адекватных мер, касающихся кибербезопасности.

Дополнительная информация по кибербезопасности приведена в разделе 9.

6 Применение беспроводной связи: системные требования

6.1 Общие положения

Должны выполняться требования МЭК 61513. В частности, для обеспечения проектирования должна быть разработана ССТ.

[1)] *Согласно НП-001-15, приложение № 2, пункт 72: «Системы (элементы) безопасности — системы (элементы), предназначенные для выполнения функций безопасности при проектных авариях».*

6.2 Сетевая архитектура

С учетом предусмотренного назначения и функций беспроводной системы, в ССТ должно быть определено и обосновано следующее:

- сетевая топология;
- размещение точек доступа;
- конфигурация сети.

В сетях с ячеистой структурой должны быть реализованы алгоритмы распределения нагрузки при маршрутизации. Это означает, что если между узлами А и В имеется несколько маршрутов, то выбранный маршрут не должен включать перегруженные промежуточные узлы.

Алгоритмы сетевой маршрутизации должны обеспечивать возможность обработки пакетов/сообщений с разными приоритетами.

6.3 Производительность сети

В связи с предусмотренным назначением в ССТ должно быть определено и обосновано следующее:

- задержка при передаче данных между соответствующими точками сети (стандартная и максимальная);
- скорость передачи данных между соответствующими точками сети (стандартная и минимальная).

Примечание — В МЭК 62657-1 рассматриваются временные характеристики беспроводных коммуникационных систем, такие как время передачи данных, время обновления и готовность.

Сетевая нагрузка должна быть контекстно-независимой. Это означает, что при возникновении отслеживаемого события, сетевая нагрузка не должна повышаться.

Примечание — Истинно контекстно-независимый проект сложно реализуем, в связи с чем достаточным является обеспечение контекстно-независимого прикладного слоя.

6.4 Контроль функционирования и диагностика состояния сети

Должны быть предусмотрены средства для наблюдения и контроля беспроводной сети. Такие средства должны обеспечивать возможность выявления и корректировки аномалий в беспроводной сети.

Должен обеспечиваться контроль возникновения ошибок в передаваемых по сети данных. В ССТ должен быть определен допустимый коэффициент потери пакетов, а также указано, должна ли выполняться повторная пересылка потерянных сообщений.

Примечание — Для снижения частоты возникновения ошибок в коммуникационной системе до допустимого уровня, указанного в проекте системы, также может быть выполнен контроль времени задержки и/или изменений времени задержки.

Должна быть обеспечена возможность контроля:

- параметров состояния сети: нагрузки, частоты появления ошибок передачи, потери пакетов, задержки;
- полного перечня устройств, подключенных к сети;
- сетевых журналов, включая невыполненные подключения (попытки неавторизованного доступа и т. д.);
- для каждого устройства:
    - его самоконтролируемых переменных (см. 7.5);
    - его характеристик (версия программного обеспечения и т. д.);
    - его физического местонахождения (если применимо).

6.5 Требования к электропитанию

Должны быть использованы резервированные источники питания, если это необходимо в соответствии с назначением.

Беспроводные устройства должны обеспечиваться питанием от аккумулятора, если это необходимо в соответствии с назначением. В этом случае:

- в ССТ должно быть указано минимальное время автономной работы при максимальной нагрузке для предусмотренного режима;
- удаленные устройства должны быть физически доступны для обеспечения возможности замены неисправного или разрядившегося аккумулятора. Если это невозможно, емкость аккумулятора должна

быть рассчитана по последнему заранее заданному времени работы, достаточность которого была подтверждена.

Потеря электропитания длительностью до часа не должна изменять конфигурацию устройства. Такие потери электропитания могут происходить вследствие перебоев сетевого электропитания или при замене аккумулятора. В ССТ может быть указана различная длительность сохранения конфигурации.

6.6 Физическая безопасность

Должны быть предусмотрены меры по физической защите беспроводных устройств так, чтобы они не могли быть взломаны или непредумышленным образом повреждены.

6.7 Электромагнитная безопасность

Должна быть предусмотрена защита от намеренно созданных ЭМИ, адекватная важности беспроводной системы для безопасности АС.

7 Выбор устройств: подтверждение правильности и интеграция устройства

7.1 Общие положения

Широко распространена практика использования уже существующих устройств для создания новых беспроводных систем. В разделе 7 приведены требования к выбору таких устройств и их интеграции в систему.

7.2 Обеспечение качества

Выбранное устройство должно иметь достаточное свидетельство того, что при его разработке применена адекватная программа обеспечения качества.

Примечание — Беспроводное устройство, разработанное в соответствии с МЭК 61513 или удовлетворяющее требованиям МЭК 62671, является хорошим примером устройства с надлежащей программой обеспечения качества.

7.3 Функциональная и эксплуатационная пригодность

Для выбираемого устройства должна быть выполнена оценка эксплуатационных характеристик, функциональных особенностей и возможностей с тем, чтобы определить его соответствие установленным системным требованиям (раздел 6).

Примечание — Например, если в ССТ указано, что используется шифрование, то и выбранное устройство должно поддерживать соответствующую функцию шифрования.

Выбор устройства тесно связан с требованиями к системе, в связи с чем большинство требований с большой долей вероятности будут определять соответствующие критерии выбора. Например, требования к электропитанию, изложенные в разделе 6, очевидным образом определяют критерии выбора устройства (продолжительность работы от аккумулятора и т. д.).

7.4 Интеграция в конкретную систему

При интеграции уже существующего устройства применяют требования в соответствии:
- с МЭК 61513:2011, 6.2.3.2 (выбор уже существующих компонентов);
- МЭК 62671.

Примечание — МЭК 62671:2013, 5.3.2 содержит требования к разработке плана оценки и применения для выбора и оценки уже существующего устройства для АС.

7.5 Самоконтроль устройства

Беспроводное устройство должно обеспечивать контроль и передачу информации о следующих параметрах:
- статус электропитания;
- уровень заряда аккумулятора (если применимо);

- качество беспроводного сигнала (при приеме и передаче данных);
- скорость передачи данных;
- нагрузка на процессор;
- состояние оперативной памяти;
- температура процессора.

7.6 Предпочтительные решения

Протоколы передачи данных беспроводными устройствами должны быть основаны на задокументированных стандартах и задокументированных протоколах передачи данных.

8 Радиочастотное излучение

8.1 Электромагнитная совместимость

Аспекты электромагнитной совместимости (ЭМС) должны быть учтены до установки беспроводных устройств вблизи важного для безопасности оборудования. Это необходимо для обеспечения надлежащей работы беспроводного устройства и предотвращения помех для работы другого оборудования.

До установки системы на АС должен быть проведен анализ на предмет ЭМС.

Анализ воздействия электромагнитного излучения может включать анализ и оценку системы в сочетании с лабораторными испытаниями и/или испытаниями на площадке в соответствии с МЭК 62003, а именно:

- анализ отчетов об испытаниях на ЭМС оборудования АС, расположенного поблизости;
- определение охранных зон в соответствии с отраслевыми руководящими документами;
- описание электромагнитной обстановки;
- испытание беспроводных устройств на их восприимчивость к воздействию с целью проверки их устойчивости к среде АС;
- испытания помехоустойчивости расположенного поблизости оборудования АС во время реализации программ технического обслуживания.

Примечание — Данные требования направлены на защиту важных для безопасности систем и ключевых систем управления от электромагнитного излучения, исходящего от беспроводных устройств.

Стационарные беспроводные устройства, такие как точки доступа, должны устанавливаться на заданном расстоянии от иного важного для безопасности оборудования, если такое оборудование чувствительно к сигналам беспроводных устройств. Это расстояние (размер охранной зоны) следует рассчитывать на основании моделей распространения волн в свободном пространстве с учетом выходной мощности и коэффициента направленного действия антенны беспроводного устройства, а также подтвержденного уровня помехоустойчивости оборудования, выполняющего функции категорий А и В. Подтвержденный уровень помехоустойчивости должен быть на 8 дБ выше ожидаемой напряженности электромагнитного поля беспроводного устройства на границе охранной зоны. Если важное для безопасности оборудование не было испытано на устойчивость к электромагнитному излучению на передающей частоте беспроводного устройства в соответствии с МЭК 61000-4-3 (или аналогичным стандартом), то необходимо провести дополнительные испытания и/или оценку. Дополнительные испытания могут включать испытания на месте помехоустойчивости важного для безопасности оборудования (или испытания аналогичного оборудования в имитированной среде) в то время, когда его функция останова/управления может быть заблокирована, например во время останова для перегрузки топлива в соответствии с указаниями МЭК 62003. При проведении данных испытаний определяют помехоустойчивость оборудования АС и устанавливают размер охранной зоны для беспроводного устройства (при наличии).

Аналогичные процедуры осуществляют в отношении мобильных беспроводных устройств, но при этом необходимо также подключить административные меры, включающие, например, проведение обучения, использование информационных табличек и других способов предотвращения нарушения установленных охранных зон.

8.2 Требования к радиоохвату

Размещение точки доступа определяют на основании карты покрытия и/или распространения электромагнитного/радиочастотного излучения (ЭМИ/РЧИ) исследуемого объекта.

Должна быть определена необходимая зона охвата коммуникационной системы в соответствии с предусмотренным назначением.

8.3 Управление спектром

8.3.1 Основные положения

Должна быть определена и задокументирована официальная программа управления спектром для обеспечения официального контроля за всеми беспроводными устройствами, используемыми на АС. Данная программа должна включать положения, гарантирующие следующее:

- беспроводные устройства проходят оценку и одобрение до внедрения и использования;
- используемый спектр включает запас по диапазону во избежание возникновения помех между каналами;
- используемый спектр учитывает устройства, не участвующие в обеспечении безопасности, которые могут работать в тех же зонах;
- обеспечивается управление конфигурацией беспроводных устройств на протяжении срока их службы, в частности, в отношении их технического обслуживания, модификации и замены.

Положения программы должны также включать документирование частоты, уровня мощности и иных характеристик беспроводных передающих устройств, а также систематический контроль используемого спектра для проверки использования среды АС. При внедрении на АС новых беспроводных устройств следует рассмотреть возможность использования незадействованных частот, чтобы избежать перегрузки существующих каналов.

При использовании беспроводных устройств на АС требуются гибкость, мобильность и управление отказами.

8.3.2 Гибкость

При необходимости размещения нескольких доступных беспроводных устройств в разных местах должно быть обеспечено надлежащее покрытие сетью нужных зон АС.

8.3.3 Мобильность

При необходимости любое устройство должно иметь доступ ко всей необходимой информации в режиме реального времени во всех предусмотренных для этого точках. Устройство и система должны допускать возможность перемещения устройства из одной зоны в другую без потери сигнала связи, если такое требование предъявляют в соответствии с предусмотренным назначением.

9 Кибербезопасность

9.1 Общие требования

Должны выполняться требования МЭК 62645.

Для беспроводной передачи данных должно быть использовано шифрование. Методы шифрования (или его отсутствие) должны отвечать требованиям общего плана безопасности[1)].

Следует использовать аутентификацию всех сообщений. Процесс аутентификации (или его отсутствие) должен отвечать требованиям общего плана безопасности.

9.2 Требования, специфичные для беспроводных устройств

9.2.1 Протоколирование данных

Должно быть предусмотрено устройство записи данных с тем, чтобы обеспечить регистрацию беспроводными устройствами следующей информации:

- попытки аутентификации и подключения;
- данные по техническому обслуживанию (износ аккумулятора, нагрузка на ЦПУ, результаты автоматического испытания и т. д.);

---

1) *В Российской Федерации в соответствии с требованиями к защите информации (см. ГОСТ Р 58833—2020) для беспроводной передачи данных используют криптографические алгоритмы и протоколы, определяемые документами национальной системы стандартизации: ГОСТ 34.12—2018, ГОСТ 34.13—2018, Р 1323565.1.030—2020, Р 1323565.1.029—2019. Разработку средств криптографической защиты информации осуществляют в соответствии с принципами разработки и модернизации шифровальных (криптографических) средств защиты информации (Р 1323565.1.012—2017).*

- данные технологического процесса, специфичные для конкретной системы (температура, давление, уровень вибрации и т. д.).

Эти данные должны быть доступны для аудита кибербезопасности в случае подозрения на нарушающие ее события.

9.2.2 Топология площадки

При проведении оценки кибербезопасности и составлении общего плана безопасности должна быть учтена топология площадки.

Необходимо иметь в виду, что сетевое подключение может быть выполнено из удаленной точки при помощи специализированных и/или модифицированных устройств, таких как направленные антенны и/или устройства с мощностью на выходе, превышающей стандартную, и др.

9.2.3 Подключение к проводной сети

При подключении беспроводной сети к проводной сети между ними должен быть установлен фильтр.

Примечание — Функцию фильтрации может выполнять ДМЗ, аппаратный фильтр и т. д.

9.2.4 Наблюдение за сетью

Неудачные попытки подключения должны быть проанализированы соответствующим персоналом, отвечающим за кибербезопасность.

Для стационарных инструментальных сетей персонал, отвечающий за кибербезопасность, должен контролировать следующие события:

- подключение новых устройств к сети;
- излучение мощности беспроводных устройств;
- колебания времени задержки при передаче данных (особенно для сетей с ячеистой структурой);
- нестандартная скорость разрядки аккумулятора.

10 Квалификация

10.1 Квалификация технических средств

Должна быть выполнена экологическая квалификация устройств. В МЭК 60987:2007 (5.4) и IEC/IEEE 60780-323 приведены дополнительные требования к проектированию и квалификации технических средств.

10.2 Квалификация программного обеспечения

Программное обеспечение должно соответствовать требованиям МЭК 62138 (для функций категории С).

11 Документация

Документированию подлежат процедуры запуска и отключения беспроводной сети.

Должен быть задокументирован порядок подключения нового устройства к беспроводной сети.

Документированию подлежит процедура замены неисправного устройства в беспроводной сети. Сюда же относится порядок передачи всех соответствующих параметров конфигурации со старого на новое устройство, подключаемое к беспроводной сети.

Беспроводные устройства, как и любые системы, имеют проблемы, связанные с устареванием, которые должны быть учтены на этапах проектирования и внедрения.

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
IEC/IEEE 60780-323	—	*
IEC 60987:2007	—	*
IEC 61513:2011	IDT	ГОСТ Р МЭК 61513—2020 «Системы контроля и управления, важные для безопасности атомной станции. Общие требования»
IEC 62138	IDT	ГОСТ Р МЭК 62138—2021 «Программное обеспечение систем контроля и управления атомной станции, выполняющих функции безопасности категорий В и С. Общие требования»
IEC 62645	—	*
IEC 62671	—	**

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

** Соответствующий национальный стандарт отсутствует. Текст документа на русском языке доступен на http://www.iaea.org/.

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

- IDT — идентичные стандарты.

Библиография

IEC 61000-4-3	Electromagnetic compatibility (EMC) — Part 4-3: Testing and measurement techniques — Radiated, radio-frequency, electromagnetic field immunity test
IEC 61226	Nuclear power plants — Instrumentation and control important to safety — Classification of instrumentation and control functions
IEC 62003	Nuclear power plants — Instrumentation and control important to safety — Requirements for electromagnetic compatibility testing
IEC 62657-1:2017	Industrial communication networks — Wireless communication networks — Part 1: Wireless communication requirements and spectrum considerations
IEC 62657-2:2017	Industrial communication networks — Wireless communication networks — Part 2: Coexistence management
IEC TR 62918:2014	Nuclear power plants — Instrumentation and control important to safety — Use and selection of wireless devices to be integrated in systems important to safety

УДК 621.311.3.049.75:006.354 ОКС 27.120.20

Ключевые слова: атомные станции; системы контроля и управления, важные для безопасности; передача данных; оборудование передачи данных; беспроводные устройства

Редактор *Н.В. Таланова*
Технический редактор *И.Е. Черепкова*
Корректор *О.В. Лазарева*
Компьютерная верстка *И.Ю. Литовкиной*

Сдано в набор 20.06.2023. Подписано в печать 22.06.2023. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 2,32. Уч-изд. л. 2,10.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

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