ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 59505— 2021/ IEC TR 63069:2019

ИЗМЕРЕНИЕ, УПРАВЛЕНИЕ И АВТОМАТИЗАЦИЯ ПРОМЫШЛЕННОГО ПРОЦЕССА

Основные принципы обеспечения функциональной безопасности и защиты информации

(IEC TR 63069:2019, IDT)

Издание официальное

Москва
Стандартинформ
2021

Предисловие

1 ПОДГОТОВЛЕН Федеральным государственным учреждением «Федеральный исследовательский центр «Информатика и управление» Российской академии наук» совместно с Обществом с ограниченной ответственностью «Информационно-аналитический вычислительный центр» (ООО ИАВЦ) и Обществом с ограниченной ответственностью «Корпоративные электронные системы» на основе собственного перевода на русский язык англоязычной версии документа, 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 19 мая 2021 г. № 396-ст

4 Настоящий стандарт идентичен международному документу IEC TR 63069:2019 «Измерение, управление и автоматизация промышленного процесса. Основные принципы обеспечения функциональной безопасности и защиты информации» (IEC TR 63069:2019 «Industrial-process measurement, control and automation — Framework for functional safety and security», IDT).

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

5 ВВЕДЕН ВПЕРВЫЕ

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 Цель настоящего стандарта

В областях функциональной безопасности и защиты информации было разработано большое число отраслевых руководств, стандартов и технических рекомендаций. Вместе с тем промышленные хозяйствующие субъекты в большей степени ожидают разработки общего документа по основным принципам функциональной безопасности и защиты информации. Даже термины «safety» и «security» в этих документах иногда описывают разные понятия. В результате бывает довольно трудно одновременно применять их к производственной системе.

0.2 Предпосылки

Информационная безопасность стала новым фактором, который следует учитывать при разработке систем. В комплексе стандартов МЭК 61508, опубликованном в 2010 г., было указано, что информационная безопасность может влиять на функциональную безопасность.

В ТК 65 МЭК (Измерение, управление и автоматизация в производственных процессах) возникли серьезные опасения в отношении влияния инцидентов, связанных с информационной безопасностью, на функции безопасности в системах промышленной автоматики и контроля (IACS). Многие сложные системы такого типа становятся связанными между собой системами (в частности, благодаря взаимодействию, основанному на беспроводной связи, датчиков/исполнительных механизмов со сложным оборудованием предприятий, сетевыми средствами и т. д.) в процессе технического обслуживания и эксплуатации. Возникает общий вопрос: «Как в таком случае проектировать и управлять функциональной безопасностью и информационной безопасностью — рассматривать системы как взаимодействующие, или полностью интегрированные, или как отдельные системы?»

0.3 Вопросы терминологии

Определения некоторых терминов, таких как «функциональная безопасность», «информационная безопасность» и «риск», иногда отличаются в различных документах. Хотя эти термины согласуются в комплексе документов в каждой из областей функциональной безопасности и информационной безопасности, но они могут оказаться несогласованными, когда оба стандарта применяются одновременно. Поэтому в настоящем стандарте терминология используется с большой осторожностью.

0.4 Целевая аудитория

Целевой аудиторией настоящего стандарта являются (но этим аудитория не ограничивается):
- собственники активов организаций (включая ответственных за методологию и управление);
- системные интеграторы (включая ответственных за проектирование и реализацию);
- поставщики продукции (включая ответственных за проектирование и реализацию);
- поставщики услуг (включая эксплуатирующие и сопровождающие организации);
- государственные органы (в том числе ответственные за оценку и аудит).

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ИЗМЕРЕНИЕ, УПРАВЛЕНИЕ И АВТОМАТИЗАЦИЯ ПРОМЫШЛЕННОГО ПРОЦЕССА

Основные принципы обеспечения функциональной безопасности и защиты информации

Industrial-process measurement, control and automation.
Framework for functional safety and security

Дата введения — 2021—11—30

1 Область применения

В настоящем стандарте разъясняются и даются рекомендации по общему применению стандартов МЭК 61508 (все части) и МЭК 62443 (все части) в области измерения, управления и автоматизации промышленных процессов.

Настоящий стандарт может применяться в других промышленных секторах, где применяются МЭК 61508 (все части) и МЭК 62443 (все части).

Примечание — Для отраслевых стандартов рекомендуется использовать или делать ссылку на настоящий стандарт.

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).

IEC 61508 (all parts), Functional safety of electrical/electronic/programmable electronic safety-related systems (Системы электрические/электронные/программируемые электронные, связанные с функциональной безопасностью)

IEC 62443 (all parts), Security for industrial automation and control systems (Безопасность систем промышленной автоматизации и контроля)

3 Термины, определения и сокращения

3.1 Термины и определения, используемые в настоящем стандарте

В настоящем стандарте применены следующие термины и определения.

ИСО и МЭК для применения в стандартизации поддерживают терминологические базы данных:

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

Примечание — В настоящем стандарте новые термины и определения создаются только в том случае, если они отсутствуют в стандартах МЭК 61508 или МЭК 62443.

3.1.1 **обработка инцидентов** (incident handling): Действия по выявлению, отчетности, оценке, реагированию, борьбе (решению) и извлечению опыта из инцидентов защиты информации.

[ИСО/МЭК 27035-1:2016, пункт 3.6, модифицировано — слова «инциденты информационной безопасности» заменены словами «инциденты защиты информации»]

Издание официальное

3.1.2 **реагирование на инцидент** (incident response): Действия, предпринятые для смягчения или устранения инцидента защиты информации, включая меры, принятые для защиты и восстановления нормальных рабочих режимов эксплуатации IACS и хранящейся в ней информации.

[ИСО/МЭК 27035-1:2016, пункт 3.7, модифицировано — слова «инциденты информационной безопасности» заменены словами «инциденты защиты информации», а «информационная система» — на «IACS»]

3.1.3 **предметная область функциональной безопасности** (safety domain): Мероприятия по обеспечению функциональной безопасности, выполняемые назначенными лицами или организациями, и их результаты в соответствии с МЭК 61508 (все части).

3.1.4 **предметная область информационной безопасности** (security domain): Мероприятия по обеспечению информационной безопасности, выполняемые назначенными лицами или организациями, и их результаты в соответствии с МЭК 62443 (все части).

3.1.5 **защищенная среда** (security environment): Рассматриваемая область, где реализованы и эффективны все соответствующие меры защиты информации.

3.1.6 **доступ** (access): Возможность и средства для обмена сообщениями или иного взаимодействия с системой в целях использования ресурсов системы.

Примечание — Доступ может предполагать физический доступ (физическая авторизация, предоставляемая для доступа в участок, наличие механического замка, ПИН-код, или карта доступа, или биометрические признаки, обеспечивающие доступ) или логический доступ (авторизация для входа в систему и программу, осуществляемая путем комбинации логических и физических средств).

[IEC/TS 62443-1-1:2009, пункт 3.2.1]

3.1.7 **архитектура** (architecture): Конкретная конфигурация элементов аппаратных средств и программного обеспечения системы.

[МЭК 61508-4:2010, пункт 3.3.4]

3.1.8 **актив** (asset): Физический или логический объект, который принадлежит организации или относится к ней иным способом, представляя для нее ощущаемую или реальную ценность.

Примечание — В случае систем промышленной автоматики и контроля физические объекты, имеющие наибольшую ценность, измеримую непосредственно, представляют, например, оборудование, которым управляют.

[IEC/TS 62443-1-1:2009, пункт 3.2.6]

3.1.9 **атака** (attack): Посягательство на систему, которое является следствием продуманного планирования, т. е. умышленного действия, представляющее собой продуманную попытку (особенно в плане метода или стратегии) обойти сервисы информационной безопасности и нарушить политику информационной безопасности системы.

Примечание — Существуют различные общепризнанные типы атак:

- «активная атака» имеет целью преобразовать ресурсы системы или воздействовать на ее работу;

- «пассивная атака» имеет целью заполучить или использовать информацию системы без воздействия на ресурсы системы;

- «внутренняя атака» — атака, инициированная субъектом в пределах периметра информационной безопасности («инсайдером»), т. е. субъектом, который наделен правами на получение доступа к ресурсам системы, но использует их в целях, не одобренных теми, кто предоставил эти права;

- «внешняя атака» — атака, инициированная за пределами периметра информационной безопасности неавторизованным или неуполномоченным пользователем системы (им может быть и инсайдер, атакующий за пределами периметра информационной безопасности). Потенциальными злоумышленниками, осуществляющими внешнюю атаку, могут быть как простые любители пошутить, так и организованные преступные группы, международные террористы и враждебные правительства.

[IEC/TS 62443-1-1:2009, пункт 3.2.9]

3.1.10 **доступность** (availability): Способность компонента выполнить требуемую функцию при заданных условиях в заданный момент времени или в течение заданного интервала времени, если предоставлены необходимые внешние ресурсы.

Примечание 1 — Эта способность зависит от следующих аспектов, рассматриваемых в совокупности: надежности, удобства сопровождения и качества технической поддержки.

Примечание 2 — Необходимые внешние ресурсы, отличные от ресурсов технического обслуживания, не влияют на показатель доступности компонента.

[IEC/TS 62443-1-1:2009, пункт 3.2.16]

3.1.11 **конфиденциальность** (confidentiality): Гарантии того, что информация не будет раскрыта несанкционированным лицам, процессам или устройствам.

[IEC/TS 62443-1-1:2009, пункт 3.2.28]

3.1.12 **контрмера** (countermeasure): Действие, устройство, процедура или стратегия, которые ослабляют угрозу, уязвимость или противодействуют атаке путем ее отражения или предотвращения, или минимизации ущерба, который она способна нанести, или путем ее обнаружения и сообщения о ней, чтобы могло быть предпринято корректирующее действие.

Примечание 1 — В некоторых контекстах для описания этого понятия используется также термин «мера защиты» (control). В IEC/TS 62443-1-1:2009 выбран термин «контрмера» во избежание путаницы с термином «управление» (control), относящимся к управлению процессами.

Примечание 2 — Слова «минимизация ущерба» в этом определении не относятся к функциональной безопасности.

[IEC/TS 62443-1-1:2009, пункт 3.2.33, модифицировано — добавлено примечание 2]

3.1.13 **опасный отказ** (dangerous failure): Отказ элемента и/или подсистемы, и/или системы, влияющий на выполнение функции безопасности:

a) препятствует выполнению функции безопасности, если необходимо ее выполнение (в режиме запроса), или вызывает прекращение выполнения функции безопасности (в непрерывном режиме), переводя управляемое оборудование (EUC) в опасное или потенциально опасное состояние; или

b) снижает вероятность корректного выполнения функции безопасности, если необходимо ее выполнение.

[МЭК 61508-4:2010, пункт 3.6.7]

3.1.14 **эшелонированная защита** (defence in depth): Наличие множественной защиты, в частности — в виде уровней, с целью предотвращения или хотя бы сдерживания атаки.

Примечание — Эшелонированная защита предполагает наличие уровней защиты и обнаружения угроз даже на обособленных системах и обладает следующими признаками:

- злоумышленники сталкиваются с проблемой незаметного прохождения или обхождения каждого уровня;

- дефект на одном уровне может быть ослаблен возможностями других уровней;

- информационная безопасность системы сводится к набору уровней, которые определяют также общую информационную безопасность сети.

[IEC/TS 62443-1-1:2009, пункт 3.2.40]

3.1.15 **жизненно важная функция** (essential function): Функция или характеристика, которая требуется для поддержания охраны труда, техники безопасности, охраны окружающей среды, а также работоспособности и доступности управляемого оборудования.

Примечание — Жизненно важные функции включают в себя, но не ограничиваются этим, функцию безопасности приборной системы безопасности (ФБ ПСБ), функцию управления и способность оператора отслеживать и манипулировать управляемым оборудованием. Утратой жизненно важных функций обычно называют утрату защиты, утрату управления и утрату отслеживаемости соответственно. В некоторых отраслях промышленности дополнительные функции, такие как архивирование, могут считаться жизненно важными.

[МЭК 62443-3-3:2013, пункт 3.1.22]

3.1.16 **функциональная безопасность** (functional safety): Часть общей безопасности, обусловленная применением EUC и системы управления EUC и зависящая от правильности функционирования электрических/электронных/программируемых электронных (Э/Э/ПЭ) систем, связанных с безопасностью, и других средств по снижению риска.

[МЭК 61508-4:2010, пункт 3.1.12]

3.1.17 **вред** (harm): Физическое повреждение или ущерб, причиняемый здоровью людей, имуществу или окружающей среде.

[МЭК 61508-4:2010, пункт 3.1.1]

3.1.18 **опасность** (hazard): Потенциальный источник причинения вреда.

Примечание — Термин включает в себя возможную опасность для людей в короткий промежуток времени (например, при пожаре и взрыве), а также опасность, имеющую долгосрочное воздействие на здоровье людей (например, при утечке токсического вещества).

[МЭК 61508-4:2010, пункт 3.1.2]

3.1.19 **инцидент** (incident): Событие, которое не является частью запланированной работы системы или услуги и приводит или может привести к сбою, приостановке или снижению качества услуг, предоставляемых системой.

[МЭК 62443-2-1:2010, пункт 3.1.18]

3.1.20 **системы промышленной автоматики и контроля**; IACS (industrial automation and control systems): Группа персонала, а также совокупность аппаратных средств и программного обеспечения, которые могут регулировать или воздействовать иным образом на безопасное, защищенное и безотказное функционирование производственного процесса.

Примечание — Такие системы могут включать в себя, но не ограничиваются этим:

- промышленные системы управления, включающие в себя распределенные системы управления (DCS), программируемые логические контроллеры (PLC), пульты дистанционного управления (RTU), интеллектуальные электронные устройства, системы диспетчерского контроля и сбора данных (SCADA), объединенные системы электронного детектирования и контроля, а также системы мониторинга и диагностики. (В данном контексте системы управления процессами наделены базовыми функциями системы управления процессами и приборной системы безопасности (SIS), которые могут быть или физически отделены друг от друга, или объединены друг с другом);

- ассоциированные информационные системы, например системы упреждающего или многосвязного регулирования, а также сетевые оптимизаторы, специальные мониторы к оборудованию, графические интерфейсы, архиваторы, автоматизированные системы управления производственными процессами и информационно-управляющие системы предприятия;

- ассоциированные внутренние, пользовательские, сетевые или машинные интерфейсы, используемые для обеспечения управления, безопасности и функциональности производственных операций в ходе непрерывных, периодических, дискретных и других процессов.

[IEC/TS 62443-1-1:2009, пункт 3.2.57]

3.1.21 **целостность** (integrity): Свойство системы, отражающее логическую корректность и безотказность операционной системы, логическую полноту аппаратных средств и программного обеспечения, которые реализуют защитные механизмы, а также согласованность структуры и содержания хранимых данных.

Примечание — В формальном укладе информационной безопасности целостность часто понимают в более узком смысле — в значении защищенности от несанкционированного преобразования или уничтожения информации.

[IEC/TS 62443-1-1:2009, пункт 3.2.60]

3.1.22 **риск** (risk) (функциональная безопасность): Сочетание вероятности события причинения вреда и тяжести этого вреда.

[ISO/IEC Guide 51:1999, пункт 3.2]

Примечание — Дальнейшее обсуждение этого определения содержится в МЭК 61508-5:2010, приложение А.

[МЭК 61508-4:2010, пункт 3.1.6, модифицировано — к термину в скобках добавлена предметная область]

3.1.23 **риск** (risk) (информационная безопасность): Ожидание ущерба, выраженное как вероятность того, что определенный источник угрозы воспользуется определенной уязвимостью системы, и это приведет к определенным последствиям.

[IEC/TS 62443-1-1:2009, пункт 3.2.87, модифицировано — к термину в скобках добавлена предметная область]

3.1.24 **безопасное состояние** (safe state): Состояние EUC, в котором достигается безопасность.

[МЭК 61508-4:2010, пункт 3.1.13, модифицировано — исключено примечание]

3.1.25 **безопасность** (safety): Отсутствие неприемлемого риска.

[МЭК 61508-4:2010, пункт 3.1.11]

3.1.26 **функция безопасности** (safety function): Функция, реализуемая Э/Э/ПЭ системой, связанной с безопасностью, или другими мерами по снижению риска, предназначенная для достижения или поддержания безопасного состояния EUC по отношению к конкретному опасному событию.

Пример — Примерами функций безопасности являются:

- функции, которые должны быть выполнены как позитивные меры, чтобы снизить влияние опасной ситуации (например, выполняют выключение двигателя); и

- функции, которые осуществляют превентивные действия, не допускающие возникновения опасных ситуаций (например, предотвращают запуск двигателя).

[МЭК 61508-4:2010, пункт 3.5.1]

3.1.27 **полнота безопасности** (safety integrity): Вероятность того, что Э/Э/ПЭ система, связанная с безопасностью, будет удовлетворительно выполнять требуемые функции безопасности при всех оговоренных условиях в течение заданного интервала времени.

Примечание 1 — Чем выше уровень полноты безопасности, тем ниже вероятность того, что система, связанная с безопасностью, не сможет выполнить указанные функции безопасности или не будет в состоянии, когда потребуется, принять указанное состояние.

Примечание 2 — Существует четыре уровня полноты безопасности для систем (см. 3.5.8 МЭК 61508-4:2010).

Примечание 3 — При определении полноты безопасности должны учитываться все причины отказов (случайных отказов аппаратных средств и систематических отказов), которые приводят к небезопасному состоянию, например отказы аппаратных средств, отказы, вызванные программным обеспечением, и отказы, вызванные электрическими помехами. Некоторые из этих типов отказов, например случайные отказы аппаратных средств, могут быть описаны количественно, с использованием таких параметров, как интенсивность отказов в опасном режиме или вероятность того, что система защиты, связанная с безопасностью, не сможет выполнить запрос. Однако полнота безопасности системы также зависит и от многих факторов, которым нельзя дать точную количественную оценку и которые могут быть оценены только качественно.

Примечание 4 — Полнота безопасности включает в себя полноту безопасности аппаратных средств (см. 3.5.7 МЭК 61508-4:2010) и полноту безопасности по отношению к систематическим отказам (см. 3.5.6 МЭК 61508-4:2010).

Примечание 5 — Данное определение основывается на определении безотказности систем, связанных с безопасностью, при выполнении ими функций безопасности.

[МЭК 61508-4:2010, пункт 3.5.4, модифицировано — текст примечания 5, приведенный в скобках, удален]

3.1.28 **уровень полноты безопасности**; УПБ [safety integrity level (SIL)]: Дискретный уровень (принимающий одно из четырех возможных значений), соответствующий диапазону значений полноты безопасности, при котором уровень полноты безопасности, равный 4, является наивысшим уровнем полноты безопасности, а уровень полноты безопасности, равный 1, соответствует наименьшей полноте безопасности.

Примечание 1 — Меры целевых отказов (см. 3.5.17 МЭК 61508-4:2010) для четырех уровней полноты безопасности указаны в таблицах 2 и 3 МЭК 61508-1.

Примечание 2 — Уровни полноты безопасности используют при определении требований полноты безопасности для функций безопасности, которые должны быть распределены по Э/Э/ПЭ системам, связанным с безопасностью.

Примечание 3 — Уровень полноты безопасности (УПБ) не является свойством системы, подсистемы, элемента или компонента. Правильная интерпретация фразы «УПБ системы, связанной с безопасностью, равен *n*» (где *n* = 1, 2, 3 или 4) означает: система потенциально способна к реализации функций безопасности с уровнем полноты безопасности до значения, равного *n*.

[МЭК 61508-4:2010, пункт 3.5.8]

3.1.29 **система, связанная с безопасностью** (safety-related system): Специальная система, которая:

- реализует необходимые функции безопасности, требующиеся для достижения и поддержки безопасного состояния управляемого оборудования (EUC), и

- предназначена для достижения своими средствами или в сочетании с другими Э/Э/ПЭ системами, связанными с безопасностью, и другими средствами снижения риска необходимой полноты безопасности для требуемых функций безопасности.

Примечание 1 — Данный термин относится к системам, обозначенным как системы, связанные с безопасностью, и предназначенным для достижения совместно с внешними средствами снижения риска (см. 3.4.2 МЭК 61508-4:2010) необходимого снижения риска для соответствия требованиям приемлемого риска (см. 3.1.7 МЭК 61508-4:2010). См. также приложение А МЭК 61508-5:2010.

Примечание 2 — Системы, связанные с безопасностью, предназначены для того, чтобы предотвратить переход EUC в опасное состояние путем выполнения необходимых действий при обнаружении условий, которые могут привести к опасному событию. Отказ системы, связанной с безопасностью, может быть отнесен к событиям, ведущим к возникновению определенной опасности или опасностей. Хотя могут существовать и другие системы, имеющие функции безопасности, именно системы, связанные с безопасностью, предназначены для достижения требуемого приемлемого риска. В широком смысле системы, связанные с безопасностью, могут быть разделены на две категории: системы управления, связанные с безопасностью, и системы защиты, связанные с безопасностью.

Примечание 3 — Системы, связанные с безопасностью, могут быть составной частью системы управления EUC либо могут быть связаны с EUC с помощью датчиков и/или исполнительных устройств. Это означает, что необходимый уровень полноты безопасности может быть достигнут реализацией функций безопасности в системе управления EUC (и, возможно, также дополнительными отдельными и независимыми системами), либо функции безопасности могут быть реализованы отдельными, независимыми системами безопасности.

Примечание 4 — Система, связанная с безопасностью, может быть предназначена:

a) для предотвращения опасного события (т. е. если система, связанная с безопасностью, выполняет свои функции безопасности, то опасного события не происходит);

b) для ослабления последствий вредного события, снижая риск путем уменьшения последствий;

c) для достижения целей перечислений a) и b).

Примечание 5 — Человек может быть частью системы, связанной с безопасностью. Например, человек может получать информацию от программируемого электронного устройства и выполнять действие, связанное с безопасностью, основываясь на этой информации, либо выполнять действие, используя программируемое электронное устройство.

Примечание 6 — Система, связанная с безопасностью, включает в себя все аппаратные средства, программное обеспечение и дополнительные средства (например, источники питания), необходимые для выполнения указанных функций безопасности (датчики, другие устройства ввода, исполнительные элементы (устройства привода) и другие устройства вывода включаются в систему, связанную с безопасностью).

Примечание 7 — Система, связанная с безопасностью, может основываться на широком диапазоне технологий, включая электрическую, электронную, программируемую электронную, гидравлическую и пневматическую технологии.

[МЭК 61508-4:2010, пункт 3.4.1]

3.1.30 **защита** (security):

a) меры, принимаемые для защиты системы;

b) состояние системы, которое является результатом разработки и проведения мер защиты системы;

c) состояние ресурсов системы, которые защищены от несанкционированного доступа к ним и несанкционированного или случайного их изменения, уничтожения, а также от утери;

d) возможность компьютерной системы гарантировать в достаточной степени, что неавторизованные лица и системы не смогут ни видоизменять программное обеспечение и данные о нем, ни получать доступ к функциям системы, но в то же время гарантировать, что это возможно для авторизованных лиц и систем;

e) предотвращение несанкционированного или нежелательного проникновения, а также вмешательства в исправную и запланированную работу системы промышленной автоматики и контроля.

Примечание — Указанные меры могут представлять собой меры защиты, относящиеся к физической безопасности (управление физическим доступом к вычислительным объектам) или логической безопасности (возможность входа в конкретную систему и приложение).

[IEC/TS 62443-1-1:2009, пункт 3.2.99]

3.1.31 **инцидент информационной безопасности** (security incident): Неблагоприятное событие в системе или сети, а также угроза такого события.

Примечание — Иногда используется термин «несостоявшийся инцидент» для описания события, которое могло обернуться инцидентом при нескольких других обстоятельствах.

[IEC/TS 62443-1-1:2009, пункт 3.2.106]

3.1.32 **уровень информационной безопасности** (security level; SL): Степень необходимой эффективности контрмер и внутренне присущих свойств информационной безопасности устройств и систем для зоны или тракта, основанная на оценке риска для данных зоны или тракта.

[IEC/TS 62443-1-1:2009, пункт 3.2.108, модифицировано — добавлено сокращение SL]

3.1.33 **патч информационной безопасности** (security patch): Программная корректировка, которая связана с информационной безопасностью компонента программного обеспечения.

Примечание 1 — Для целей настоящего определения микропрограммное обеспечение считается программным обеспечением.

Примечание 2 — Программные корректировки могут устранить известные или потенциальные уязвимости или просто повысить информационную безопасность программного компонента, включая его безотказное функционирование.

[МЭК 62443-2-4:2015, пункт 3.1.17]

3.1.34 **периметр информационной безопасности** (security perimeter): Граница (логическая или физическая) домена, в пределах которой применимы политика безопасности или архитектура безопасности, т. е. граница области, в которой сервисы информационной безопасности защищают ресурсы системы.

[IEC/TS 62443-1-1:2009, пункт 3.2.110]

3.1.35 **зона информационной безопасности** (security zone): Совокупность логических или физических объектов, к которым предъявляются общие требования информационной безопасности.

Примечание 1 — Термин «зона», употребляемый в настоящем стандарте, следует всегда относить к зоне информационной безопасности.

Примечание 2 — Зона имеет четкую границу с другими зонами. Политика информационной безопасности зоны обычно определяется комбинацией механизмов как на периферии зоны, так и внутри нее. Зоны могут иметь иерархическую структуру в том смысле, что могут быть образованы совокупностью подзон.

[IEC/TS 62443-1-1:2009, пункт 3.2.117]

3.1.36 **стойкость к систематическим отказам** (systematic capability): Мера уверенности (выраженная в диапазоне ССО 1 — ССО 4) в том, что систематическая полнота безопасности элемента соответствует требованиям заданного значения УПБ для определенной функции безопасности элемента, если этот элемент применен в соответствии с указаниями, определенными для этого элемента в соответствующем руководстве по безопасности.

Примечание 1 — Стойкость к систематическим отказам определяется с учетом требований по предотвращению систематических отказов и управлению ими (см. МЭК 61508-2 и МЭК 61508-3).

Примечание 2 — Механизм систематического отказа зависит от природы элемента. Например, для элемента, представляющего программное обеспечение, должны быть рассмотрены только механизмы ошибок в программах. Для элемента, включающего в себя аппаратное средство и программное обеспечение, должны быть рассмотрены механизмы систематических отказов как для аппаратных средств, так и для программного обеспечения.

Примечание 3 — Стойкость к систематическим отказам элемента ССО N при выполнении определенной функции безопасности означает, что элемент соответствует УПБ N для систематических отказов, если этот элемент применен в соответствии с указаниями, определенными для этого элемента в соответствующем руководстве по безопасности.

[МЭК 61508-4:2010, пункт 3.5.9]

3.1.37 **угроза** (threat): Потенциальная возможность нарушения информационной безопасности при наличии обстоятельства, средства, процесса или события, способных нарушить информационную безопасность и нанести ущерб.

[IEC/TS 62443-1-1:2009, пункт 3.2.125]

3.1.38 **фактор угрозы** (threat agent): Причинный фактор угрожающего действия.

[IEC/TS 62443-1-1:2009, пункт 3.2.127]

3.1.39 **уязвимость** (vulnerability): Дефект или несовершенство структуры или способа реализации системы, а также ее функционирования и управления, как благоприятная возможность для нарушения целостности системы или политики ее информационной безопасности.

[IEC/TS 62443-1-1:2009, пункт 3.2.135]

3.2 Сокращения

BPCS — базовая система управления процессами (Basic Process Control System);

DCS — распределенная система управления (Distributed Control System);

DoS — отказ в обслуживании (Denial of Service);

E/E/PE — электрический/электронный/программируемый электронный (Electrical/Electronic/Programmable Electronic);

EUC — управляемое оборудование (Equipment Under Control);

HFT — отказоустойчивость аппаратных средств (Hardware Fault Tolerance);

IACS — система промышленной автоматики и контроля (Industrial Automation and Control Systems);

PLC — программируемый логический контроллер (Programmable Logic Controller);

RTU — пульт дистанционного управления (Remote Terminal Unit);

SC — стойкость к систематическим отказам (Systematic Capability);

SCADA — система диспетчерского контроля и сбора данных (Supervisory Control And Data Acquisition);

SIF — функция безопасности приборной системы безопасности (Safety Instrumented Function);

SIL — уровень полноты безопасности (Safety Integrity Level),

SIS — приборная система безопасности (Safety Instrumented System);

SL — уровень информационной безопасности (Security Level).

3.3 Объяснение общих терминов с различными определениями

Некоторые термины имеют различные определения в комплексе стандартов МЭК 61508 и комплексе стандартов МЭК 62443. Пояснения приведены в таблице 1.

В настоящем стандарте уточняется смысл каждого из этих терминов с указанием их предполагаемого контекста.

Идентификатор предметной области «(функциональная безопасность)», следующий за термином, указывает на то, что значение этого термина определяется в соответствии с МЭК 61508 (все части). Аналогично идентификатор предметной области «(информационная безопасность)» указывает, что его значение определяется в соответствии с МЭК 62443 (все части).

Примечание — Если термин, который может иметь идентификатор предметной области, используется без идентификатора предметной области, то термин рассматривается как общий термин.

В таблице 1 приводится дополнительная информация о существующих терминах и определениях в МЭК 61508 (все части) и МЭК 62443 (все части).

Примечание — Таблица 1 не содержит примечаний к определениям.

Таблица 1 — Термины с несколькими определениями

Термин	Определение из МЭК 61508	Определение из МЭК 62443	Пояснения
Безопасность	Отсутствие неприемлемого риска [МЭК 61508-4:2010, 3.1.11]	Отсутствие недопустимого риска [IEC/TS 62443-1-1:2009, 3.2.94]	Оба определения ссылаются на риск (безопасность — safety). Примечание — Под безопасностью (safety) понимают функциональную безопасность только в комплексе стандартов МЭК 61508, но она может быть воспринята иначе в рамках других стандартов (например, электробезопасность или механическая безопасность)
Защита	Не определено	a) Меры, принимаемые для защиты системы; b) Состояние системы, которое является результатом разработки и проведения мер защиты системы; c) Состояние ресурсов системы, которые защищены от несанкционированного доступа к ним и несанкционированного или случайного их изменения, уничтожения, а также от утери; d) Возможность компьютерной системы гарантировать в достаточной степени, что неавторизованные лица и системы не смогут ни видоизменять программное обеспечение и данные о нем, ни получать доступ к функциям системы, но в то же время гарантировать, что это возможно для авторизованных лиц и систем; e) Предотвращение несанкционированного или нежелательного проникновения, а также вмешательства в исправную и запланированную работу системы промышленной автоматики и контроля. [IEC/TS 62443-1-1:2009, 3.2.99]	В IEC Guide 120 дается компактное и полезное определение: условие, которое возникает в результате установления и поддержания защитных мер, обеспечивающих состояние неприкосновенности от враждебных действий или влияний. [IEC Guide 120:2008, 3.13]
Риск	Сочетание вероятности события причинения вреда и тяжести этого вреда. [МЭК 61508-4:2010, 3.1.6]	Ожидание ущерба, выраженное как вероятность того, что определенный источник угрозы воспользуется определенной уязвимостью системы и это приведет к определенным последствиям. [IEC/TS 62443-1-1:2009, 3.2.8]	Существующее различие в определениях обусловлено различиями между функциональной безопасностью и информационной безопасностью с точки зрения последствий. Если последствия в случае функциональной безопасности связаны с ущербом, то последствия, связанные с информационной безопасностью, могут быть неизвестны. Риск (функциональная безопасность): - причины — опасности;

Продолжение таблицы 1

Термин	Определение из МЭК 61508	Определение из МЭК 62443	Пояснения
Риск	Сочетание вероятности события причинения вреда и тяжести этого вреда. [МЭК 61508-4:2010, 3.1.6]	Ожидание ущерба, выраженное как вероятность того, что определенный источник угрозы воспользуется определенной уязвимостью системы и это приведет к определенным последствиям. [IEC/TS 62443-1-1:2009, 3.2.8]	- больше внимания уделяется снижению вреда. Риск (информационная безопасность): - причины — угрозы/несанкционированный доступ; - больше внимания уделяется влиянию на бизнес, финансы и окружающую среду
Функция безопасности	Функция, реализуемая Э/Э/ПЭ системой, связанной с безопасностью, или другими мерами по снижению риска, предназначенная для достижения или поддержания безопасного состояния EUC по отношению к конкретному опасному событию (см. 3.4.1 и 3.4.2). [МЭК 61508-4:2010, 3.5.1]	Не определено	Термин необходим только в предметной области функциональной безопасности
Система, связанная с безопасностью	Специальная система, которая: - реализует необходимые функции безопасности, требующиеся для достижения и поддержки безопасного состояния EUC, и - предназначена для достижения своими средствами или в сочетании с другими Э/Э/ПЭ системами, связанными с безопасностью, и другими средствами снижения риска необходимой полноты безопасности для требуемых функций безопасности. [МЭК 61508-4:2010, 3.4.1]	Не определено	См. приборная система безопасности (ПСБ) для МЭК 62443 (все части)

Продолжение таблицы 1

Термин	Определение из МЭК 61508	Определение из МЭК 62443	Пояснения
Жизненно важная функция	Не определено	Функция или способность, которая требуется для поддержания охраны труда, безопасности, охраны окружающей среды, а также доступности управляемого оборудования. [МЭК 62443-3-3:2013, 3.1.22]	Дополнительные сведения см. в 4.2
Базовая система управления процессами (BPCS)	Не определено	Система, которая реагирует на входные сигналы от процесса, связанного с ним оборудования, других программируемых систем и/или оператора и генерирует выходные сигналы, приводящие к тому, что процесс и связанное с ним оборудование функционируют требуемым образом, но не выполняют каких-либо функций безопасности приборной системы безопасности (SIF). [МЭК 62443-2-4:2015, 3.1.14]	Дополнительные сведения см. в 4.2
Приборная система безопасности	Не определено	Система, используемая для выполнения функции безопасности. [МЭК 62443-2-4:2015, 3.1.14] Система, используемая для выполнения одной или нескольких функций, связанных с безопасностью. [МЭК 62443-3-3:2015, 3.1.37]	Дополнительные сведения см. в 4.2
Уязвимость	Не определено	Дефект или несовершенство структуры или способа реализации системы, а также ее функционирования и управления, как благоприятная возможность для нарушения целостности системы или политики ее информационной безопасности. [IEC/TS 62443-1-1:2009, 3.2.135] Примечание — Политики информационной безопасности обычно включают политики защиты конфиденциальности, целостности и доступности системных ресурсов	Уязвимость нельзя сравнивать с ошибкой, сбоем или отказом, поскольку они различаются способом влияния. Дополнительную информацию см. в разделе 5
Системы промышленной автоматики и контроля (IACS)	Не определено	Группа персонала, а также совокупность аппаратных средств и программного обеспечения, которые могут регулировать или воздействовать иным образом на безопасное, защищенное и безотказное функционирование производственного процесса. Примечание — Такие системы могут включать в себя, но не ограничиваются этим:	Не определено в комплексе МЭК 61508, в котором дано общее представление для всех связанных с безопасностью функций, реализованных с использованием Э/Э/ПЭ систем

Окончание таблицы 1

Термин	Определение из МЭК 61508	Определение из МЭК 62443	Пояснения
Системы промышленной автоматики и контроля (IACS)	Не определено	- промышленные системы управления, включающие в себя распределенные системы управления (DCS), программируемые логические контроллеры (PLC), пульты дистанционного управления (RTU), интеллектуальные электронные устройства, системы диспетчерского контроля и сбора данных (SCADA), объединенные системы электронного детектирования и контроля, а также системы мониторинга и диагностики. (В данном контексте системы управления процессами наделены базовыми функциями системы управления процессами и приборной системы безопасности (SIS), которые могут быть или физически отделены друг от друга, или объединены друг с другом); - ассоциированные информационные системы, например системы упреждающего или многосвязного регулирования, а также сетевые оптимизаторы, специальные мониторы к оборудованию, графические интерфейсы, архиваторы, автоматизированные системы управления производственными процессами и информационно-управляющие системы предприятия; - ассоциированные внутренние, пользовательские, сетевые или машинные интерфейсы, используемые для обеспечения управления, безопасности и функциональности производственных операций в ходе непрерывных, периодических, дискретных и других процессов. [IEC/TS 62443-1-1:2009, 3.2.57]	Не определено в комплексе МЭК 61508, в котором дано общее представление для всех связанных с безопасностью функций, реализованных с использованием Э/Э/ПЭ систем
Инцидент	Не определено	Событие, которое не является частью запланированной работы системы или услуги и приводит или может привести к сбою, приостановке или снижению качества услуг, предоставляемых системой. [МЭК 62443-2-1:2010, 3.1.18]	
Вред	Физическое повреждение или ущерб, причиняемый здоровью людей, имуществу или окружающей среде. [МЭК 61508-4:2010, 3.1.1]	Не определено	Определение вреда также вписывается в предметную область информационной безопасности и может быть определено аналогично

4 Контекст информационной безопасности, связанный с функциональной безопасностью

4.1 Описание функций

В МЭК 61508 (все части) основное внимание уделяется реализации функций безопасности, а описания архитектуры в большей степени связаны с такими характеристиками, как отказоустойчивость аппаратных средств (HFT) и стойкость к систематическим отказам. Однако предварительно определенной архитектуры, общей для всех предполагаемых систем, не существует. Вместо этого в МЭК 61508 (все части) определяются критерии полноты безопасности, такие как уровень полноты безопасности (SIL) и стойкость к систематическим отказам (SC), что позволяет определить показатель уровня функциональной безопасности, специально разработанный для IACS, и соответствующие характеристики, достигающие достаточно низкой интенсивности случайных отказов, а также сформировать адекватный набор мер для снижения систематических отказов. В некоторых частях комплекса МЭК 62443 рассматривается структура системы IACS, состоящая из базовой системы управления технологическим процессом и приборной системы безопасности, а также описываются характеристики их установки для перерабатывающего производства. Однако окончательное описание архитектуры и его содержание предполагают некоторую реализацию, которая не обязательно удовлетворяет требованиям информационной безопасности или функциональной безопасности. На рисунке 1 представлен обзор функций IACS, включающий функции безопасности, жизненно важные функции, базовые функции управления и дополнительные функции IACS.

Рисунок 1 — Обзор функций IACS

Жизненно важные функции включают также функции безопасности IACS. Жизненно важные функции, характеристики которых определяются в результате оценки угроз-рисков (информационная безопасность), могут быть реализованы в специально разработанной системе, связанной с безопасностью, а также в системе, которая не является системой, связанной с безопасностью.

4.2 Защищенная среда

В настоящем стандарте предложена идея защищенной среды, чтобы правильно понять представленную на рисунке 2 общую область для предметных областей функциональной безопасности и информационной безопасности.

Защищенная среда, показанная на рисунке 3, включает в себя набор мер защиты информации, необходимых для обеспечения эффективной защиты среды при выполнении функций безопасности системой, связанной с безопасностью. Однако эти меры защиты не ограничиваются лишь защитой функций безопасности.

Защищенная среда включает (но этим не ограничивается) следующие меры защиты информации:

- все меры защиты информации, защищающие периметры защищенной среды;
- все меры защиты информации, касающиеся взаимодействия между различными функциональными элементами в защищенной среде;
- все меры защиты информации, применяемые в функциональных элементах в защищенной среде.

Примечание 1 — На практике меры защиты информации могут охватывать не только функции безопасности.

Примечание 2 — Защищенная среда отличается от «зоны», описанной в комплексе МЭК 62443.

Примечание 3 — Защищенная среда может включать стратегию «эшелонированной защиты» (см. 5.4 IEC/TS 62443-1-1:2009) для достижения достаточной устойчивости приложения от внешних воздействий.

Меры защиты информации в защищенной среде могут быть интегрированы в любой функциональный элемент технической системы, включая функциональный элемент системы, связанной с безопасностью.

Рисунок 2 — Предметная область функциональной безопасности и предметная область информационной безопасности

Структуры, описанные в МЭК 62443 (все части), включают в себя концепцию зоны, предполагающую наличие строго определенных периметров защиты для каждой зоны, а также наличие выделенных соединений между зонами, называемых трактами. В качестве мер защиты информации для защищенной среды могут быть определены одна или несколько зон или трактов.

Для предотвращения влияющих на функции безопасности и использующих уязвимости угроз от несанкционированного доступа или ошибок человека защищенную среду необходимо сформировать и поддерживать.

На рисунке 3 показаны взаимосвязи между защищенной средой, средой эксплуатации системой, связанной с безопасностью.

Уязвимости не следует понимать как ошибки или сбои технической системы в предметной области функциональной безопасности, поскольку в техническую систему уязвимость может быть внесена нарушителем и может привести к отказам.

Пример — Нарушитель может использовать методы социальной инженерии, используя уязвимости процессов или людей.

Примечание — Управление уязвимостями с участием поставщика может быть мерой защиты информации, определяемой в результате оценки угроз-рисков (информационная безопасность).

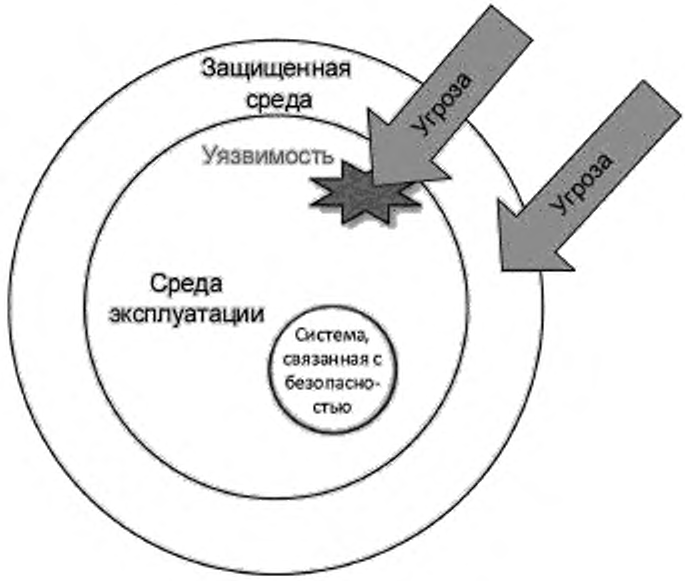

Рисунок 3 — Защищенная среда

5 Основополагающие принципы

В настоящем разделе представлены наиболее общие рекомендации, которые в настоящем стандарте называются основополагающими принципами, касающиеся мер обеспечения защиты информации для функций безопасности, выполняемых IACS.

Основополагающий принцип 1. Защита информации в реализациях систем, связанных с безопасностью.

Меры защиты информации должны эффективно предотвращать или защищать от негативного влияния угроз системы, связанные с безопасностью, и реализуемые ими функции безопасности. Оценки функций безопасности должны учитывать допущение о наличии эффективных мер (защиты информации).

Примеры

1 Предполагается, что меры защиты информации предотвращают несанкционированную модификацию программного обеспечения, связанного с безопасностью, выполняемую, например, посредством удаленного доступа.

2 Расследование инцидентов информационной безопасности в отношении программного обеспечения/кода, связанного с функциональной безопасностью, или действий, связанных с управлением технологическими процессами, позволяет предотвращать непреднамеренное внедрение вредоносного программного обеспечения в критический код системы, связанной с безопасностью.

Основополагающий принцип 2. Защита реализаций информационной безопасности.

Меры обеспечения функциональной безопасности не должны оказывать негативное влияние на эффективность реализации информационной безоласности.

Примечание — Человеческий фактор учитывается как в предметной области функциональной безопасности, так и в предметной области информационной безопасности.

Примеры

1 Средствам обеспечения функциональной безопасности запрещено добавлять функционал, например удаленный доступ к системам, если для этого функционала не была выполнена оценка информационной безопасности.

2 Функции безопасности могут быть более чувствительными к DoS атакам (отказ в обслуживании) и, следовательно, являются возможной целью негативного влияния на доступность системы.

Основополагающий принцип 3. Совместимость реализаций.

Средства реализации защиты информации и средства реализации системы, связанной с безопасностью, не должны оказывать негативного влияния на функционирование друг друга.

Примеры

1 На скорость передачи данных в системе влияют меры защиты информации, что оказывает негативное влияние на временные характеристики функции безопасности.

2 Криптографические методы, используемые для обеспечения информационной безопасности, не должны оказывать негативного влияния на меры защиты канала связи, используемого системой, связанной с безопасностью.

Если рассматривать ослабление рисков, реализуемое системами функциональной безопасности и информационной безопасности, то заранее определенного предпочтения между ними не существует.

6 Рекомендации к жизненному циклу IACS при совместном проектировании

6.1 Общие положения

Обмен информацией и взаимодействие между специалистами из предметных областей функциональной и информационной безопасности должны осуществляться на протяжении всего жизненного цикла IACS, с тем чтобы обеспечить соответствующую защищенную среду для выполнения жизненно важных функций, включая функции безопасности.

В кратком изложении в настоящем разделе рекомендуются следующие действия:

1) разработка в областях применения функциональной и информационной безопасности должна осуществляться параллельно, и при необходимости информация должна использоваться заинтересованными сторонами совместно;

2) разрешение конфликтов должно основываться на консенсусе, сформированном заинтересованными сторонами в обеих областях;

3) перед установкой и вводом в эксплуатацию заинтересованные стороны из обеих областей должны обеспечить совместимость мер защиты информации с процедурами эксплуатации и обслуживания реализованной системы, связанной с безопасностью.

Реализация методологии функциональной безопасности обеспечивает корректное функционирование систем, связанных с безопасностью. Для систем, в которых безопасность зависит от систем, связанных с безопасностью, меры защиты информации вносят свой вклад в выполнение функций безопасности в системах, связанных с безопасностью. Для реализации этого вклада с помощью набора мер защиты информации должна быть создана защищенная среда. Поэтому рекомендуется взаимодействие между экспертами области функциональной безопасности и области информационной безопасности. Конкретная реализация взаимодействия зависит от типа приложения и/или политики организации. Обзор возможных взаимодействий представлен на рисунке 4.

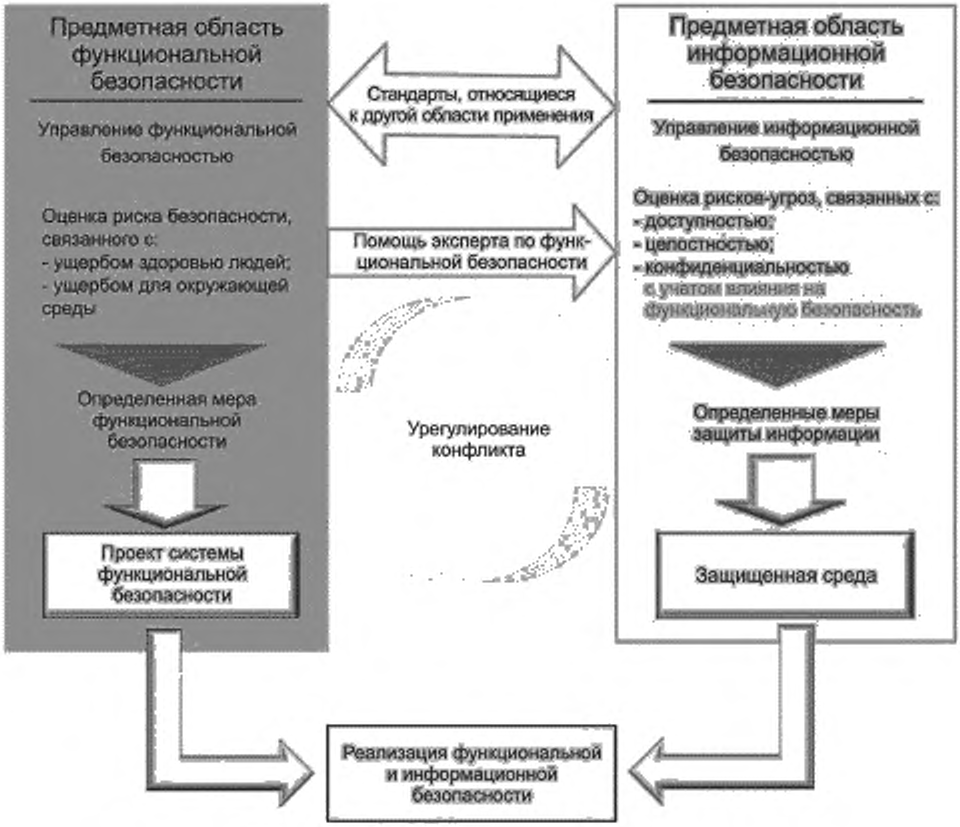

Рисунок 4 — Взаимодействие функциональной и информационной безопасности

Согласно МЭК 61508 (все части) предметная область функциональной безопасности должна быть охвачена менеджментом функциональной безопасности. Согласно МЭК 62443 (все части) предметная область информационной безопасности должна быть охвачена менеджментом и информационной безопасности.

Оценка рисков (функциональная безопасность) и оценка рисков-угроз (информационная безопасность) должны проводиться на основе результатов оценки рисков более высокого уровня.

Хотя оценка рисков в предметной области функциональной безопасности и в предметной области информационной безопасности выполняется аналогично, но существует отличие, поскольку для функциональной безопасности случайные и неслучайные причины нарушений работоспособности оцениваются как статические сбои. В предметной области информационной безопасности неслучайные причины оцениваются с помощью динамических сценариев уязвимости. Поэтому целесообразно установить различные процессы анализа функциональной безопасности и информационной безопасности. Корреляции между уровнем полноты функциональной безопасности (SIL) и уровнем информационной безопасности (SL) не существует. Их следует считать независимыми понятиями.

Для элементов защиты информации не выполняется оценка риска (функциональная безопасность). Для них осуществляется оценка рисков-угроз (информационная безопасность). Однако для оценки рисков-угроз (информационная безопасность) необходимо сотрудничество между экспертами из обеих областей.

В ходе оценки рисков-угроз (информационная безопасность) эксперты в области защиты информации и эксперты в области функциональной безопасности изучают их возможное влияние на функции безопасности. Эксперты в области функциональной безопасности должны предоставлять более подробное описание системы безопасности, касающееся реализованных функций безопасности, включая

перечень средств, относящихся к системе, связанной с безопасностью, и соответствующие данные (например, спецификации и конфигурации). Эксперт в области защиты информации должен понимать сценарии применения системы, связанной с безопасностью, чтобы выявлять риски (информационная безопасность), которые могут повлиять на функциональную безопасность.

В случае выявления конфликтной ситуации процесс ее урегулирования должен быть выполнен до реализации системы. В зависимости от организации урегулирование конфликтных ситуаций может быть под надзором ответственных лиц различных сторон и должно быть согласовано со всеми экспертами.

Основополагающие принципы, представленные в разделе 5, должны применяться на протяжении всего жизненного цикла IACS. В таблице 2 перечислены рекомендуемые мероприятия, которые должны осуществляться на каждой стадии жизненного цикла IACS для обеспечения этих основополагающих принципов.

Поскольку в соответствии с требованиями МЭК 61508 (все части) или МЭК 62443 (все части) существует большое количество возможных работоспособных реализаций IACS, то в таблице 2 для каждой стадии жизненного цикла представлены только наиболее общие рекомендации.

Таблица 2 — Рекомендуемые действия на стадиях жизненного цикла IACS

Стадия жизненного цикла	Рекомендуемые действия	Руководящие указания по документированию
Разработка концепции	Определить угрозы для защищаемой среды. Провести оценки рисков-угроз (информационная безопасность) с учетом запланированных функций безопасности, представленных в подробном описании системы, связанной с безопасностью. Найти решения возможных конфликтных ситуаций между функциями безопасности системы, связанной с безопасностью и мерами защиты информации. Рекомендуется поддержка эксперта в области функциональной безопасности	Документировать информацию, связанную с жизненно важными функциями (включая функции безопасности системы, связанной с безопасностью), во время оценки рисков-угроз (информационная безопасность). Сформировать концепцию информационной безопасности. Следует учесть человеческий фактор
Разработка/Реализация	Предоставить соответствующую информацию для мер защиты информации (например, временные ограничения) для обеспечения выполнения функций безопасности системы, связанной с безопасностью. Рассмотреть возможные конфликтные ситуации при реализации функций безопасности системы, связанной с безопасностью, и мер защиты информации. В процессе разработки обеспечить взаимодействие с экспертами по информационной безопасности при внесении изменений в проект в целях обеспечения функциональной безопасности (возможно, влияющих на результаты оценки рисков-угроз (информационная безопасность)). Обеспечить реализацию всех систем, связанных с безопасностью, в защищенной среде. Убедиться в том, что используемые инструментальные средства охвачены мерами защиты информации в защищенной среде	Документировать информацию, связанную, в частности, с мерами защиты информации, которые относятся к защищенной среде. Разработать руководство по информационной безопасности для сопроводительной документации. Проконсультироваться с экспертами по информационной безопасности, чтобы определить, как осуществить защищенный доступ к системам, связанным с безопасностью
Модификация/обслуживание	При внесении изменений в систему, связанную с безопасностью, обеспечить взаимодействие с экспертами по информационной безопасности (возможно, это повлияет на результаты оценки рисков-угроз (информационная безопасность). К системе, связанной с безопасностью, не должны применяться патчи информационной безопасности без анализа их влияния на параметры функциональной безопасности и без выполнения необходимой верификации	Разработать руководство/процедуры выполнения изменений. Документировать внесенные изменения, связанные, в частности, с мерами защиты информации, которые поддерживают защищенную среду

Окончание таблицы 2

Стадия жизненного цикла	Рекомендуемые действия	Руководящие указания по документированию
Производство	Система должна быть подготовлена к работе в соответствии с определенными мерами защиты информации. Готовую систему следует верифицировать на отсутствие известных уязвимостей (например, вредоносное ПО, вирус). Реализованные меры защиты информации должны быть активны или установлены в определенное начальное состояние	Предоставлять документацию по информационной безопасности вместе с системой
Эксплуатация	Реагировать на инциденты и опасные события. Устранять возможные конфликтные ситуации при обновлении мер защиты информации. Убедиться, что эти действия не влияют на другую предметную область	Документировать последние сведения об уязвимостях в других проектах и системах
Поддержка	Предоставлять операторам необходимую информацию, в том числе об исправлениях/обновлениях	Документировать изменения в управлении конфигурацией при выполнении патчей информационной безопасности и обновлений программного обеспечения. Сообщать о новых инцидентах в подразделение управления производством
Вывод из эксплуатации	Обеспечить, чтобы отмененные меры защиты информации не оказывали влияния на оставшиеся функции безопасности системы, связанной с безопасностью	Документировать концепцию вывода из эксплуатации

6.2 Вопросы управления защитой информации, связанные с обеспечением функциональной безопасности

При взаимодействии предметных областей функциональной и информационной безопасности, как показано на рисунке 4, рекомендуется следующее.

a) вопросы защиты информации, связанные с обеспечением функциональной безопасности, должны контролироваться в предметной области информационной безопасности и анализироваться в процессе оценки рисков-угроз (информационная безопасность).

Примечание — Выполнять контроль в предметной области информационной безопасности должны не только эксперты в области защиты информации;

b) возможное влияние действий по обеспечению защиты информации при их негативном влиянии на функции безопасности должно устраняться с помощью контрмер, определенных для защищаемой среды;

c) меры при проектировании системы, связанной с безопасностью, и меры защиты информации должны осуществляться в соответствии с основополагающими принципами, с тем чтобы обеспечить требуемое снижение рисков в обеих областях.

7 Рекомендации по оценке рисков

7.1 Оценка рисков на более высоком уровне

Для выявления и классификации рисков их оценку на более высоком уровне можно рассматривать как деятельность на уровне системы, охватывающую как вопросы информационной безопасности, так и вопросы функциональной безопасности.

Начальный этап заключается в выполнении оценки риска на более высоком уровне для определения общего риска, который должен быть снижен.

Процессы оценки рисков (функциональная безопасность) и оценки рисков-угроз (информационная безопасность) являются схожими, поскольку в обоих случаях предполагается учитывать последствия угроз и/или отказов. Однако по ряду аспектов они различаются. Например, вероятность того, что источники возможных угроз воспользуются уязвимостью, не детерминирована и может быть оценена только качественно на основе накопленного опыта. Характеристики защиты информации невозможно определить количественно.

Оценка риска-угроз (информационная безопасность) должна соответствовать требованиям МЭК 62443-2-4, МЭК 62443-4-1 и МЭК 62443-3-3.

Корреляция между обеспечением функциональной безопасности и информационной безопасности IACS аналогична корреляции между обеспечением функциональной безопасности и электромагнитной совместимости, когда возможное влияние требует оценки, но нельзя найти общего компромиссного решения.

Информация, полученная в результате оценки рисков на более высоком уровне, должна быть доступна одновременно для областей информационной и функциональной безопасности. В обеих областях на основе этой информации проводятся соответствующие оценки рисков. Эксперты из обеих областей сотрудничают в разрешении возможных конфликтных ситуаций и проблем совместимости. Выявленные конфликтные ситуации должны быть устранены, что может повлиять на проект системы, связанной с безопасностью, а также на проект системы защиты информации. См. рисунок 5.

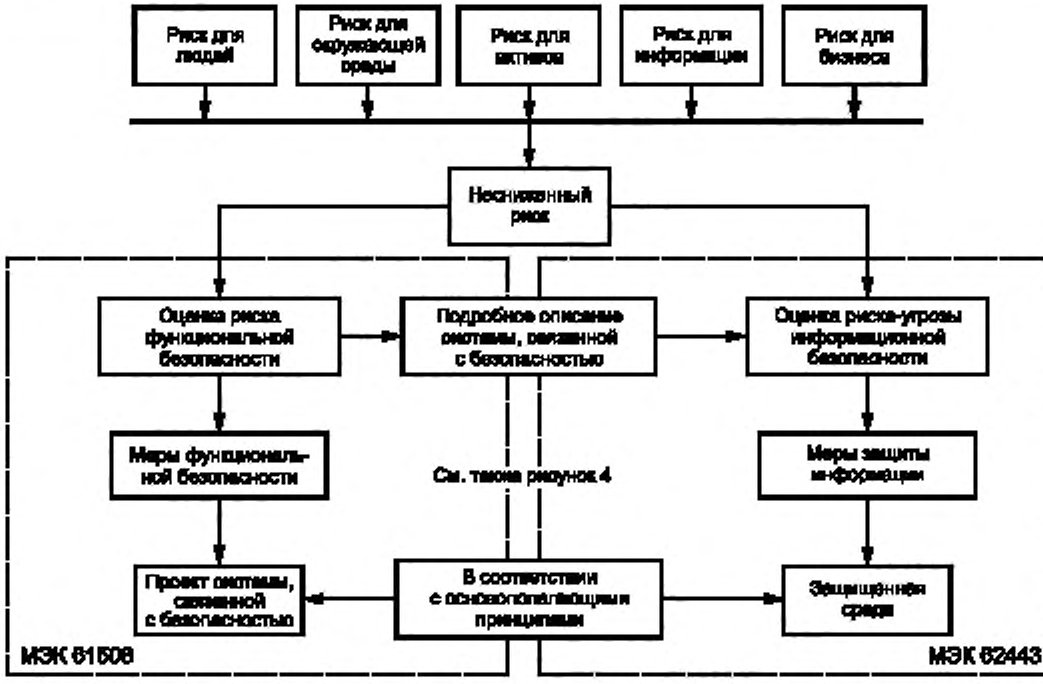

Рисунок 5 — Оценка рисков функциональной безопасности и информационной безопасности как часть оценки рисков на более высоком уровне

Результаты оценки рисков на более высоком уровне следует использовать в качестве основы для оценки рисков-угроз (информационная безопасность), а также оценки рисков (функциональная безопасность). В силу различной природы этих рисков оба анализа выполняются отдельно. В обеих областях необходимо определить меры по снижению первоначального риска.

Все действия в области функциональной безопасности и области информационной безопасности могут выполняться независимо отдельными группами специалистов или одной общей группой.

Эксперты по функциональной безопасности и эксперты по информационной безопасности должны попытаться достичь согласия. Если согласие не будет достигнуто, то следует выполнить анализ для достижения компромисса, как описано в 7.2.

7.2 Анализ для достижения компромисса

Управление компромиссами между различными видами рисков является важной частью оценки рисков на более высоком уровне, а также менеджмента. В целом число конфликтных ситуаций может быть сокращено за счет использования рациональных методов проектирования, а также рассмотрения и сокращения возможных побочных эффектов, однако могут возникнуть проблемы между обеспечением функциональной безопасности и информационной безопасности, которые требуют разрешения. Для этого используется процесс, который называется «анализ компромиссов». Хотя подготовить достаточно строгое руководство для всех областей невозможно, тем не менее сформированный процесс достижения компромисса должен содержать некоторые указания на то, что следует учитывать при анализе компромиссов, например: имеются ли приоритеты, какова ответственность за принятие компромиссных решений, а также требование о документальном оформлении результата и причины принятия решения.

7.3 Вопросы оценки рисков-угроз (информационная безопасность)

7.3.1 Общие положения

Для оценки рисков-угроз (информационная безопасность) должны быть составлены и документально оформлены следующие рекомендации по обеспечению защиты информации, которые могут повлиять на достижение функциональной безопасности.

7.3.2 Рекомендации по оценке рисков-угроз (информационная безопасность)

В процессе оценки рисков-угроз должно быть выполнено следующее:

1) подготовлено подробное описание системы, связанной с безопасностью;

2) определены угрозы и их возможное влияние на защищенную среду;

3) определены опасности, которые могут возникнуть в результате попыток несанкционированного доступа;

4) определено функционирование системы, связанной с безопасностью, и/или ее архитектура, а также способы появления в ней уязвимостей;

5) на основе собранной информации определены и установлены необходимые меры защиты информации, реализующие эффективную защищенную среду.

7.3.3 О мерах защиты информации

Должно быть применено следующее:

1) меры защиты информации должны создавать защищенную среду, которая эффективно защищает функции безопасности;

2) защищенная среда не должна подвергаться негативному влиянию или блокироваться функциями безопасности.

7.3.4 Уязвимости и примеры их исходных причин

Уязвимости могут эффективно использоваться нарушителями для реализации угрозы безопасности информации в защищенной среде и, следовательно, для негативного воздействия на функции безопасности.

Примерами исходных причин уязвимостей, которыми могут воспользоваться угрозы безопасности информации, являются.

a) недостаточная информированность об информационной безопасности лиц/организаций (например, неконтролируемое использование USB-накопителей);

b) недостатки в управлении активами (например, у существующих активов организации статус их версий не ясен, не полон или устарел);

c) добавление новых уязвимостей в системы/решения или возвращение к старым уязвимостям в результате обновлений или исправлений (например, исправление решает одну проблему и создает две новые);

d) недостатки систем/решений (например, отсутствие надлежащих процедур и мер по обеспечению защиты информации);

e) внутренне присущие проекту ограничения, связанные с производительностью (например, простой случай отказа в обслуживании (DoS) приводит к проблемам обеспечения функциональной безопасности);

f) преднамеренно неправильное использование функций/характеристик (например, ввод вредоносного программного обеспечения по каналу обслуживания удаленного доступа);

g) реальное использование отличается от предполагаемого использования (например, в процессе эксплуатации был добавлен удаленный доступ);

h) изменения в среде угроз, делающие существующие решения более уязвимыми (например, нарушение методов шифрования).

Уязвимости не должны рассматриваться как сбои, отказы или ошибки, как определено в МЭК 61508 (все части), поскольку их происхождение и характер отличаются от сбоев в системах, связанных с безопасностью.

Уязвимости следует рассматривать как недостатки или слабые места технологий, процессов и процедур или персонала, как это определено в МЭК 62443 (все части).

7.4 Неправомерные и несанкционированные действия

7.4.1 Общие положения

В настоящем подразделе поясняется существующая лексика, относящаяся к областям применения функциональной безопасности и информационной безопасности, с тем чтобы обеспечить взаимопонимание между экспертами этих областей.

7.4.2 Разумно предсказуемое неправильное использование (функциональная безопасность)

Анализ разумно предсказуемых обстоятельств или неправильного использования, описанный в МЭК 61508-1 и определенный в МЭК 61508-4, не включает рассмотрение действий, выполняемых человеком, с единственным намерением причинить ущерб или нанести травмы. Рассмотрение предсказуемых обстоятельств или неправильного использования не следует путать с рассмотрением обеспечения защиты информации. Разумно предсказуемое неправильное использование скорее относится к поведению, при котором игнорируется надлежащее использование систем и реализуются намерения нарушить меры обеспечения безопасности, которые воспринимаются как неудобные в повседневной работе.

7.4.3 Предотвращение неправомерных и несанкционированных действий (информационная безопасность)

Исходя из предполагаемого уровня защиты информации меры по обеспечению информационной безопасности для предотвращения неправомерных и несанкционированных действий нарушителя должны учитывать более широкий спектр его манипуляций. Для исследования системы и определения подходящих механизмов предотвращения несанкционированного доступа должен использоваться комплекс МЭК 62443.

Примечание — Такие механизмы могут включать в себя предотвращение несанкционированного физического доступа к системам и осведомленность об опасностях социальной инженерии.

7.4.4 Сочетание мер для защиты паролем

Требования к паролю в системах, связанных с безопасностью, например в случае предсказуемого неправильного использования, могут не соответствовать более строгим рекомендациям по обеспечению защиты информации. Обычно меры по обеспечению информационной безопасности отвечают требованиям функциональной безопасности, связанным с защитой паролем.

Примечание — Возможные решения с механическими элементами и электрическими линиями могут рассматриваться отдельно.

8 Готовность к реагированию на инциденты и их обработка

8.1 Общие положения

Обработка инцидентов для IACS должна включать в себя действия по предотвращению опасных отказов функции(й) безопасности. В случае обнаружения критического инцидента информационной безопасности его следует оценить и обработать в соответствии с процедурами обработки инцидентов, а также принять ответные меры для того, чтобы защищаемая среда непрерывно находилась в защищенном состоянии.

8.2 Готовность к реагированию на инциденты

Должны быть готовые к использованию процедуры и технические возможности для обнаружения и регистрации инцидентов информационной безопасности, с тем чтобы в дальнейшем обеспечить их анализ.

Примечание — Кроме того, могут применяться местные законы и нормативные акты.

Однако из-за характера атак на систему защиты информации вполне возможно, что успешные атаки вообще могут быть не обнаружены как инциденты информационной безопасности.

8.3 Обработка инцидентов

К обработке инцидентов IACS должны привлекаться эксперты по функциональной безопасности, которые в процессе анализа определяют возможное влияние инцидентов на функцию(и) безопасности.

Для расследования инцидентов информационной безопасности, связанных с защищенной средой, должен использоваться метод оценки рисков-угроз (информационная безопасность). Как правило, целью должно быть поддержание или восстановление эффективности защиты информации защищенной среды при реализации решения или системы.

При расследовании инцидентов информационной безопасности следует учитывать следующее, но этим не ограничиваясь:

a) Анализ инцидента информационной безопасности должен учитывать потенциальную глубину проникновения по отношению к модели глубокоэшелонированной защиты.

b) Временные характеристики попыток несанкционированного доступа должны рассматриваться независимо от оценки рисков (функциональная безопасность), основанной на конкретных сценариях негативного воздействия. Следовательно, допущение, сделанное при анализе одиночного сбоя, связанное с режимом выполнения функции безопасности (непрерывным или с низкой частотой запросов), может быть некорректным, так как задержка выполнения функции безопасности в системе, функционирующей в режиме с низкой частотой запросов, является допустимой в течение определенного периода времени. В случае наличия инцидентов информационной безопасности эта временная оценка не справедлива, поскольку ее невозможно предсказать, если инцидент информационной безопасности нанесет ущерб хотя бы одной части системы, связанной с безопасностью.

c) Следует обратить внимание на инциденты информационной безопасности, влияющие на несколько частей системы одновременно, вследствие использования для их создания аналогичной технологии (для аппаратных средств или программного обеспечения).

d) Следует учитывать тот факт, что, как правило, для создания потенциально опасной ситуации необходим несанкционированный доступ к нескольким частям системы, связанной с безопасностью;

e) При правильной настройке для успеха несанкционированного доступа, указанного в перечислении d), необходимо наличие источника угроз.

Такими источниками угроз могут быть (но этим не ограничивается):

- внешние нарушители (от одиночных нарушителей до госучреждения недружественной страны);
- инсайдеры, неправомерно использующие свои знания.

f) Следует рассмотреть вопрос о том, в какой степени могут быть учтены определенные предварительные условия и какая информация позволяет успешно способствовать попыткам несанкционированного доступа, например:

- информация ограниченного доступа, связанная с используемыми технологиями или процессами;
- недостатки проекта, возникающие в результате развития технического прогресса (со временем).

Могут применяться различные решения.

Реагирование на инцидент включает следующие действия:

g) управляемый останов системы или выпуска продукции;

h) отключение конкретных функций или частей системы;

i) изменения программного обеспечения/микропрограммного обеспечения (использование патча информационной безопасности);

j) изменения принципов построения или архитектуры системы (например, при замене активов организации или технологий);

k) добавление организационных мер или процедур для снижения вероятности успешных попыток несанкционированного доступа;

l) продолжение эксплуатации при незначительном воздействии обнаруженного инцидента/уязвимости защиты информации.

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов и документов национальным стандартам

Таблица ДА.1

Обозначение ссылочного международного стандарта, документа	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
IEC 61508-1	IDT	ГОСТ Р МЭК 61508-1—2012 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 1. Общие требования»
IEC 61508-2	IDT	ГОСТ Р МЭК 61508-2—2012 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 2. Требования к системам»
IEC 61508-3	IDT	ГОСТ IEC 61508-3—2018 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 3. Требования к программному обеспечению»
IEC 61508-4	IDT	ГОСТ Р МЭК 61508-4—2012 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 4. Термины и определения»
IEC 61508-5	IDT	ГОСТ Р МЭК 61508-5—2012 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 5. Рекомендации по применению методов определения уровней полноты безопасности»
IEC 61508-6	IDT	ГОСТ Р МЭК 61508-6—2012 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 6. Руководство по применению ГОСТ Р МЭК 61508-2 и ГОСТ Р МЭК 61508-3»
IEC 61508-7	IDT	ГОСТ Р МЭК 61508-7—2012 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 7. Методы и средства»
IEC/TS 62443-1-1	IDT	ГОСТ Р 56205—2014/IEC/TS 62443-1-1:2009 «Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 1-1. Терминология, концептуальные положения и модели»
IEC 62443-2-1	IDT	ГОСТ Р МЭК 62443-2-1—2015 «Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 2-1. Составление программы обеспечения защищенности (кибербезопасности) системы управления и промышленной автоматики»
IEC TR 62443-2-3	—	*
IEC 62443-2-4	—	*
IEC/TR 62443-3-1	—	*

Окончание таблицы ДА.1

Обозначение ссылочного международного стандарта, документа	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
IEC 62443-3-3	IDT	ГОСТ Р МЭК 62443-3-3—2016 «Сети промышленной коммуникации. Безопасность сетей и систем. Часть 3-3. Требования к системной безопасности и уровни безопасности»
IEC 62443-4-1	—	*
IEC 62443-4-2	—	*

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

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

- IDT — идентичные стандарты.

Библиография

IEC 60050-351, International Electrotechnical Vocabulary — Part 351: Control technology (available at www.electropedia.org)

IEC 61508-1, Functional safety of electrical/electronic/programmable electronic safety related systems — Part 1: General requirements

IEC 61508-2, Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 2: Requirements for electrical/electronic/program-mable electronic safety-related systems

IEC 61508-3, Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 3: Software requirements

IEC 61508-4:2010, Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 4: Definitions and abbreviations

IEC 61508-5:2010, Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 5: Examples of methods for the determination of safety integrity levels

IEC 61511 (all parts), Functional safety — Safety instrumented systems for the process industry sector

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

IEC 62443-2-1:2010, Industrial communication networks — Network and system security — Part 2-1: Establishing an industrial automation and control system security program

IEC 62443-2-4:2015, Security for industrial automation and control systems — Part 2-4: Security program requirements for IACS service providers

IEC 62443-3-3:2013, Industrial communication networks — Network and system security — Part 3-3: System security requirements and security levels

IEC 62443-4-1, Security for industrial automation and control systems — Part 4-1: Secure product development lifecycle requirements

IEC 62859, Nuclear power plants — Instrumentation and control systems — Requirements for coordinating safety and cybersecurity

ISO/IEC Guide 51, Safety aspects — Guidelines for their inclusion in standards

IEC Guide 120:2018, Security aspects — Guidelines for their inclusion in publications

ISO/IEC 27035-1:2016, Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management

ISO/IEC 27035-2, Information technology — Security techniques — Information security incident management — Part 2: Guidelines to plan and prepare for incident response

УДК 62-783:614.8:331.454.004.056.5:006.354

ОКС 13.110
25.040
29.020

Ключевые слова: безопасность функциональная, безопасность информационная, жизненный цикл систем, уязвимости, риски, угрозы, контрмеры, защищенная среда, эшелонированная защита

Технический редактор *И.Е. Черепкова*
Корректор *Л.С. Лысенко*
Компьютерная верстка *М.В. Лебедевой*

Сдано в набор 20.05.2021. Подписано в печать 31.05.2021. Формат 60×84¼. Гарнитура Ариал.
Усл. печ. л. 3,72. Уч.-изд. л. 3,34.

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