ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 71452— 2024/ IEC/PAS 63325:2020

ТРЕБОВАНИЯ К ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ И ЗАЩИТЕ СИСТЕМЫ КОНТРОЛЯ ПРОМЫШЛЕННОЙ АВТОМАТИЗАЦИИ (IACS) НА ПРОТЯЖЕНИИ ЖИЗНЕННОГО ЦИКЛА

(IEC/PAS 63325:2020, IDT)

Издание официальное

Москва
Российский институт стандартизации
2024

gost.e-ecolog.ru

Предисловие

1 ПОДГОТОВЛЕН Обществом с ограниченной ответственностью «ЭОС Тех» (ООО «ЭОС Тех») и Федеральным государственным бюджетным учреждением «Российский институт стандартизации» (ФГБУ «Институт стандартизации») на основе собственного перевода на русский язык англоязычной версии документа, указанного в пункте 4

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 58 «Функциональная безопасность»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 13 июня 2024 г. № 777-ст

4 Настоящий стандарт идентичен международному документу IEC/PAS 63325:2020 «Требования к функциональной безопасности и защите системы контроля промышленной автоматизации (IACS) на протяжении жизненного цикла» (IEC/PAS 63325:2020 «Lifecycle requirements for functional safety and security for IACS», IDT)

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 (*gost.e-ecolog.ru

© IEC, 2020
© Оформление. ФГБУ «Институт стандартизации», 2024

Настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

Содержание

1 Область применения 1
2 Нормативные ссылки 1
3 Термины, определения и сокращения 1
3.1 Термины и определения 1
3.2 Сокращения 2
4 Стадии жизненного цикла 2
5 Требование к координации менеджмента 3
5.1 Общие положения 3
5.2 Требования к организации 3
5.3 Управление изменениями 3
6 Требования к жизненному циклу 4
6.1 Концепция и область применения 4
6.2 Оценка рисков 4
6.3 Разработка и внедрение 6
6.4 Эксплуатация и обслуживание 7
6.5 Вывод из эксплуатации 7
Приложение А (справочное) Возможные меры по координации функциональной безопасности и защиты информации на различных этапах жизненного цикла 8
Библиография 11

Введение

Безопасность и защищенность становятся все более взаимозависимыми. Традиционные системы, связанные с безопасностью, больше не изолируются, как это требовалось при их подключении и обеспечении функциональной совместимости, а угрозы и уязвимости могут увеличить вероятность атак на системы, связанные с безопасностью. Настоящий стандарт содержит некоторые основные рекомендации по функциональной безопасности и защите информации.

В настоящем стандарте описаны аспекты функциональной безопасности и защиты информации на различных этапах жизненного цикла, оптимизация оценки рисков, повышение эффективности действий по защите информации и обеспечению функциональной безопасности, в том числе при проектировании, предупреждение конфликтов между функциями обеспечения функциональной безопасности и контрмерами защиты информации. Настоящий стандарт также содержит ряд рекомендаций по совместному проектированию эффективных и экономичных систем обеспечения функциональной безопасности и защиты информации.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ТРЕБОВАНИЯ К ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ И ЗАЩИТЕ СИСТЕМЫ КОНТРОЛЯ ПРОМЫШЛЕННОЙ АВТОМАТИЗАЦИИ (IACS) НА ПРОТЯЖЕНИИ ЖИЗНЕННОГО ЦИКЛА

Lifecycle requirements for functional safety and security for IACS

Дата введения — 2025—07—01

1 Область применения

В настоящем стандарте содержатся требования и рекомендации по обеспечению и подтверждению функциональной безопасности и защиты информации на различных этапах жизненного цикла. Настоящий стандарт помогает координировать процессы оценки рисков, проектирования, управления и эксплуатации, а также предотвращает конфликты между функциональной безопасностью и защитой информации.

Настоящий стандарт нацелен не на создание абсолютно нового жизненного цикла, а на выработку требований и предложений по координации функциональной безопасности и защиты информации на основе жизненных циклов функциональной безопасности, защиты информации и других современных процессов проектирования.

Настоящий стандарт применим к системам управления промышленной автоматизации (IACS), в том числе к управляемому оборудованию (УО) и системам, связанным с безопасностью.

2 Нормативные ссылки

В настоящем стандарте нормативные ссылки отсутствуют.

3 Термины, определения и сокращения

3.1 Термины и определения

В настоящем стандарте применены следующие термины и определения.

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

- Платформа онлайн-просмотра ИСО; доступна по адресу: gost.e-ecolog.ru
- Электропедия МЭК; доступна по адресу: gost.e-ecolog.ru

Дополнительные определения могут включать в себя ссылки на серии стандартов МЭК 62443 и МЭК 61508.

3.1.1 **конфликт** (conflict): Ситуация, в которой одна или несколько мер обеспечения безопасности противоречат одной или нескольким контрмерам защиты и не способны обеспечивать необходимые целевые показатели эффективности.

Примечание — Настоящее определение конфликта относится к контексту настоящего стандарта.

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

[МЭК 61508-4:2010, 3.1.11 и МЭК 62443-1-1:2009, 3.2.94]

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

[МЭК 61508-4:2010, 3.1.12]

Издание официальное

3.1.4 **защита информации** (security):

a) меры, предпринимаемые 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).

[МЭК 62443-1-1:2009, 3.2.99]

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

[МЭК 62443-1-1:2009, 3.2.125]

3.1.6 **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 безопасности.

[МЭК 62443-1-1:2009, 3.2.135]

3.1.7 **актив** (asset): Физический или логический объект, который имеет воспринимаемую или реальную ценность для совокупности функций обеспечения безопасности и эксплуатационных функций IACS.

Примечание — Данное определение актива применяется в контексте настоящего стандарта.

3.1.8 **координация** (coordination): Деятельность IACS, благодаря которой:

- все факторы рисков учитываются и контролируются;
- процесс управления рисками выполняется надлежащим образом;
- отсутствуют конфликты между мерами обеспечения безопасности и контрмерами защиты информации.

3.2 Сокращения

IACS — система контроля промышленной автоматизации;
SOI — целевая система;
SIL — уровень полноты безопасности;
УО — управляемое оборудование.

4 Стадии жизненного цикла

На протяжении всего жизненного цикла необходимо поддерживать связь и взаимодействие между функциональной безопасностью и защитой информации, чтобы:

- все обоснованно прогнозируемые атаки и нарушения условий эксплуатации были определены и находились под контролем;
- все требования по снижению рисков были достигнуты;
- выработать компромиссные проектные решения, которые обеспечат совместимость и приемлемые уровни рисков, поскольку конфликт между мерами обеспечения функциональной безопасности и контрмерами защиты информации может приводить к увеличению рисков.

Как правило, выделяют следующие этапы жизненного цикла:

- концепцию и область применения;
- оценку рисков;
- разработку и внедрение;
- эксплуатацию и обслуживание;
- вывод из эксплуатации и утилизацию.

Примечание — Требования к жизненному циклу различны и зависят от конкретного стандарта (МЭК 61508, МЭК 61511, МЭК 62443 и др.); в настоящем стандарте рассматриваются только типовые этапы, которые наиболее важны для обеспечения совместимости между безопасностью и защитой информации.

5 Требование к координации менеджмента

5.1 Общие положения

Процессы технического менеджмента следует рассматривать в начале жизненного цикла; для конкретной организации рекомендуется планировать общие процессы технического менеджмента, включая специалистов, отвечающих за функциональную безопасность и защиту информации.

Процессы технического менеджмента должны быть реализованы на протяжении всего жизненного цикла. Если определены пересекающиеся требования к действиям по обеспечению функциональной безопасности и действиям по защите информации, то для их успешного соблюдения необходимо распределять ответственность (исключение составляют специальные для предметной области требования к менеджменту функциональной безопасности и защиты информации).

Основными целями обеспечения функциональной безопасности и защиты информации должны являться минимизация рисков причинения вреда людям и окружающей среде, а также нанесения серьезного материального и репутационного ущерба.

Подходы к управлению рисками охватывают как функциональную безопасность, так и защиту информации. Меры обеспечения функциональной безопасности и контрмеры защиты информации нацелены на достижение приемлемого уровня риска. При возникновении конфликта между мерами обеспечения функциональной безопасности и контрмерами защиты информации необходимо вырабатывать компромиссное проектное решение, которое обеспечивает приемлемый уровень риска.

5.2 Требования к организации

Ответственность:

- все специалисты, которые принимают общие меры по обеспечению функциональной безопасности и защиты информации, должны понимать свои обязанности и задачи;
- должны быть предусмотрены механизмы взаимодействия, в особенности между специалистами по функциональной безопасности и защите информации;
- должны быть выработаны специальные процедуры и механизмы координации для выполнения пересекающихся задач по обеспечению функциональной безопасности и защиты информации.

5.3 Управление изменениями

Необходимо выработать скоординированный подход к управлению изменениями.

Должны быть разработаны процедуры оценки возможных отрицательных воздействий на функциональную безопасность и защиту информации при внесении изменений в IACS (ее конфигурацию, рабочее состояние и др.)

Изменения, связанные с функциональной безопасностью, должны подвергаться встречному аудиту со стороны специалистов по защите информации для проверки допустимости и эффективности контрмер защиты информации.

Внесение изменений в системы, связанные с функциональной безопасностью, часто приводит к возникновению новых уязвимостей. В таких случаях обычно принимают дополнительные меры защиты информации, а при необходимости подтверждения их эффективности выполняют специальный анализ рисков.

При внесении изменений в меры защиты информации (например, установку исправлений) выполняют соответствующий анализ (а при необходимости также проводят соответствующие испытания) для проверки отсутствия отрицательного воздействия этих изменений на функцию безопасности.

Поскольку указанные изменения могут повлиять на полноту безопасности, а для внесения этих изменений с соблюдением требований по защите информации требуется время, необходимо отслеживать и контролировать уязвимость. При необходимости выполняют специальную оценку рисков для определения компенсирующих мер, которые сохраняют полноту безопасности. Реализацию этих компенсирующих мер осуществляют с разрешения специалиста по управлению защитой информации.

6 Требования к жизненному циклу

6.1 Концепция и область применения

Необходимо определить системы, связанные с безопасностью, и системы, связанные с защитой информации, область их применения, их периметр безопасности, задавая список целевых систем.

Чтобы достигнуть целей функциональной безопасности и защиты информации, должны быть рассмотрены все средства, системы управления и сетевая среда, в том числе:

- типы и применение заводского/цехового оборудования и его систем управления;
- физическая среда передачи и протокол связи для обмена данными между всеми устройствами, системами управления и общедоступной сетью;
- сети связи, которые необходимо изолировать;
- обозначение границ различных виртуальных сетей и физических областей (в том числе функциональных границ типовых систем).

Должны быть строго определены реакция или способ реагирования системы на критическую атаку. Возможные способы реагирования:

- продолжать работу в прежнем режиме в краткосрочном периоде без изменения системы;
- изолировать систему до устранения дефекта или угрозы;
- остановить производственный процесс и перевести систему в безопасное состояние.

ПРИМЕР — При сбое диспетчерской станции или ее заражении вирусом такую станцию достаточно временно изолировать, а при отказе контроллера системы безопасности может потребоваться немедленное отключение.

Необходимо классифицировать все системы и устройства (пример для оборудования технологического комплекса см. в таблице 1; в этой таблице не показана общая классификация, поскольку классификация зависит от конкретных применений).

Таблица 1 — Пример классификации всех систем и устройств

Системы и устройства	Связаны с функциональной безопасностью	Связаны с защитой информации
Неэлектрические/цифровые средства для базового управления	Нет	Нет
Электрические/цифровые средства для базового управления	Нет	Да
Неэлектрические/цифровые инструменты для управления защитой	Да	Нет
Электрические/цифровые инструменты для управления защитой	Да	Да
Блок базового управления	Нет	Да
Блок управления безопасностью	Да	Да
Человеко-машинный интерфейс для базового управления	Нет	Да
Человеко-машинный интерфейс для управления защитой	Да	Да
Межсетевой экран, шлюз	Нет	Да

Описание архитектуры (в том числе систем и сети) должно быть документально оформлено. Оно должно учитывать:

- полную изолированность системы;
- сквозной канал связи;
- изолированный канал связи с сетью уровня мониторинга;
- совместно используемый канал связи с сетью уровня мониторинга;
- подключение к промышленной сети;
- сетевое подключение гибридной системы управления, связанной/не связанной с безопасностью.

6.2 Оценка рисков

6.2.1 Общие требования

Перед традиционной связанной с безопасностью оценкой рисков и оценкой угроз и уязвимостей необходимо выполнять общую оценку рисков.

После традиционной связанной с безопасностью оценки рисков и оценки угроз и уязвимостей должен быть запущен процесс разрешения конфликта.

Необходима одна группа специалистов для выполнения комплексной оценки рисков или две группы специалистов для выполнения оценки рисков, связанных с безопасностью и с защитой информации, при надлежащей взаимной поддержке или взаимодействии.

Общий процесс оценки рисков показан на рисунке 1.

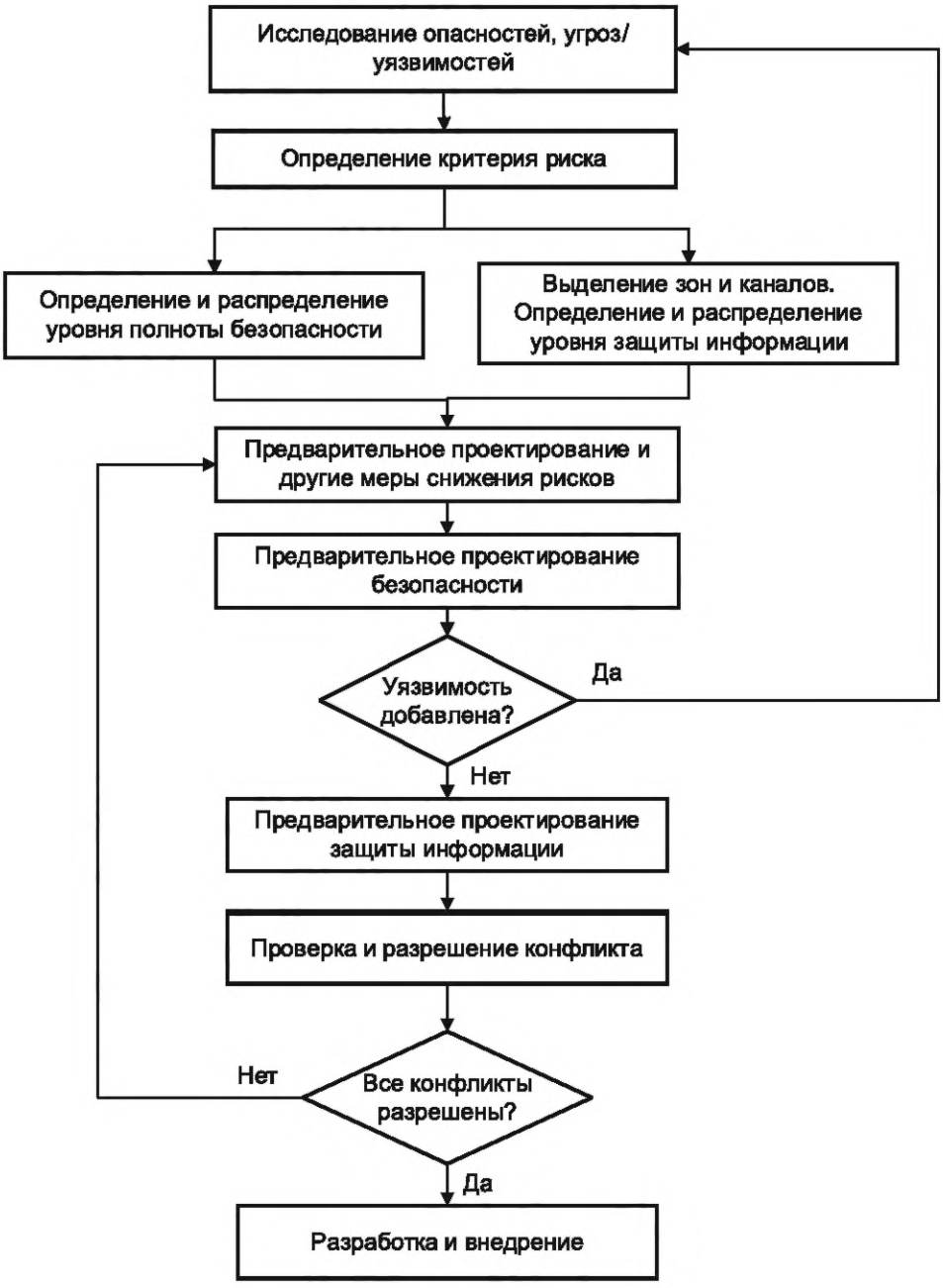

Рисунок 1 — Общий процесс оценки рисков

6.2.2 Анализ опасностей и рисков/оценка угроз и уязвимостей

В целях поддержания риска ниже допустимого уровня необходимо определить все возможные опасные события в определенных предметных областях, связанных с IACS, а также исчерпывающим образом применять и координировать меры, связанные с функциональной безопасностью, защитой информации, и другие технические меры безопасности.

Необходимо учитывать все действующие опасные факторы и возможные угрозы, в том числе людей, устройства, распорядительные документы, материалы, и определить следующее:

- режим эксплуатации систем;
- сложность систем;
- компетентность специалистов.

6.2.3 Критерий риска

Меры обеспечения функциональной безопасности уменьшают риск причинения вреда людям, окружающей среде и имуществу. Для достижения целей функциональной безопасности и защиты информации необходимо определять надлежащие критерии функциональной безопасности конкретной прикладной системы.

Выбор мер зависит от прикладной системы, а ее владелец обязан поддерживать уровни рисков на приемлемых уровнях в соответствии с критериями.

Источниками критериев риска могут являться:

- регламенты;
- стандарты;
- состояние общества;
- иные факторы.

6.2.4 Разрешение конфликтов

Конфликты разрешаются на каждой итерации оценки опасностей и рисков с выработкой компенсационных мер при необходимости.

При возникновении конфликтов следует вносить изменения в:

- проект системы функциональной безопасности для снижения общего риска, возможно внедряя иные защитные меры; при проектировании системы функциональной безопасности необходимо с самого начала учитывать, что это может приводить к новым уязвимостям, и искать альтернативные решения во избежание конфликтов;
- проект системы защиты информации, возможно, с использованием альтернативных мер защиты информации (при условии, что специалисты по защите информации знают или уведомлены о наличии конфликта; например, они могут внедрить альтернативную систему идентификации по отпечатку пальца, чтобы оператор, который забыл пароль, мог отправлять критически важные команды системам безопасности); или
- в компенсирующие меры, которые дают возможность ослаблять некоторые меры защиты информации благодаря тому, что они более эффективно снижают риски.

6.3 Разработка и внедрение

6.3.1 Общие положения

Если некоторые контрмеры защиты информации интегрированы в системы, связанные с безопасностью, но не изолированы должным образом, то все элементы этих контрмер защиты информации должны соответствовать требованиям МЭК 61508, части 1—3.

По окончании разработки и внедрения необходимо проводить испытания для проверки отсутствия неблагоприятных воздействий систем функциональной безопасности и защиты информации друг на друга.

Если испытания выполняют для производственных систем, то необходимо исключать воздействие испытательных процедур на требуемые эксплуатационные характеристики систем.

Испытания, которые проводят на уровне изделий или системы, должны демонстрировать, что:

a) функции безопасности работают, при этом сигналы безопасности отправляются и передаются беспрепятственно;

b) при нормальных условиях возможны надежная эксплуатация и обслуживание системы;

c) реагирование на сбои осуществляется штатным образом, система успешно переходит в безопасное состояние;

d) время реагирования приемлемо для прикладной системы.

6.3.2 Реакция на отказы системы или на события защиты информации

При обнаружении отказа в системе, связанной с безопасностью, необходимо выполнить процедуры в соответствии с планом обслуживания, в том числе учитывая диагностическую информацию, выполнить ремонт и повторную валидацию после ремонта.

Если нарушение защиты информации и принятие соответствующей защитной контрмеры происходят в процессе эксплуатации, то нарушение и контрмера подлежат регистрации и отслеживанию.

Если в процессе эксплуатации происходит какое-либо нарушение защиты информации и на него реагирует специальная контрмера нарушения защиты информации, то это событие и реакция контрмеры должны регистрироваться и контролироваться.

Кроме того, поскольку некоторая реакция системы защиты информации может приводить к аварийному отключению системы функциональной безопасности, то должен быть предусмотрен аварийный механизм, который предотвращает нежелательные отключения.

6.4 Эксплуатация и обслуживание

Как отмечено в разделе 5, для эксплуатации и обслуживания также должна быть предусмотрена система менеджмента.

В ходе контрольных проверок систем, связанных с безопасностью, проверяют отсутствие отрицательных воздействий систем функциональной безопасности и защиты информации друг на друга. Эти проверки в значительной степени зависят от конкретной прикладной системы, например, можно имитировать атаку в автономном режиме для проверки работоспособности мер обеспечения защиты информации, а затем можно проверить, может ли после этого функция безопасности оставаться работоспособной.

Примечание — В МЭК 62443-4-2:2019, пункт 7.5.3, указано, что верификация функциональности системы защиты информации в процессе нормальной эксплуатации должна выполняться с соблюдением мер предосторожности во избежание отрицательного воздействия, но она может быть неприемлема для систем функциональной безопасности. В данном случае ситуация иная: a) контрольная проверка функциональной безопасности обычно проводится в автономном режиме несмотря на то, что в пункте 7.5.3 указан рабочий режим. Это ключевая причина, по которой требования пункта 7.5.3 не подходят для системы функциональной безопасности, так как это может вызвать ложное срабатывание; и b) пункт 7.5.3 — это просто верификация функциональности, тогда как в данном случае речь идет о возможном конфликте.

Процессы внедрения средств обеспечения функциональной безопасности и защиты информации на этапе эксплуатации и обслуживания могут быть тесно связаны друг с другом. По этой причине деятельность по обеспечению защиты информации должна быть усовершенствованием зрелых процедур эксплуатации и технического обслуживания для обеспечения функциональной безопасности на предприятии, а риски защиты информации следует рассматривать как часть процессов управления рисками организации. Обычно к этим мерам относятся штатная эксплуатация и обслуживание, реагирование на нарушения функциональной безопасности/защиты информации и внесение необходимых изменений в системы, связанные с безопасностью. Следует уделять внимание мерам мониторинга, регистрации нарушений функциональной безопасности и защиты информации, а также реагирования на них (см. приложение А).

6.5 Вывод из эксплуатации

При выводе из эксплуатации любого компонента системы, связанной с безопасностью, анализируют возможные последствия этого вывода для функциональной безопасности. Обычно анализ выполняется в рамках отлаженной процедуры менеджмента функциональной безопасности. Когда рассматривают защиту информации, то должны быть включены дополнительные требования к управлению контрмерами защиты информации. Они включают мониторинг, тестирование и выпуск обновлений/исправлений программного обеспечения для контрмер защиты информации, а также повторную валидацию после внесения изменений.

Приложение А
(справочное)

Возможные меры по координации функциональной безопасности и защиты информации на различных этапах жизненного цикла

А.1 Оценка рисков

Для выявления возможных опасностей во внутренних системах предприятия необходимо выполнять взаимосвязанную оценку опасностей и рисков, в которой учитываются аспекты как функциональной безопасности, так и защиты информации. Как правило, учет угроз защиты информации приводит к увеличению риска функциональной безопасности. К возможным угрозам защиты информации, которые могут влиять на функциональную безопасность, относятся человеческие факторы, устройства/системы, подключенные к системе управления или системе, связанной с безопасностью, или ответная реакция/отказ самой контрмеры защиты информации.

Внешние или внутренние злоумышленники могут атаковать очень важную инфраструктуру или непосредственно системы, связанные с безопасностью. Добросовестные сотрудники, которые имеют право доступа к системе IACS, могут создать угрозы ее защите информации, совершая непреднамеренные ошибки.

Такие угрозы защите информации могут приводить к возникновению уязвимостей, в том числе отказов аппаратных средств и систематических отказов (например, ошибок в программном обеспечении системы управления и системы, связанной с безопасностью).

А.2 Разработка и внедрение

А.2.1 Меры физической защиты, необходимые для контроля доступа

Ключевые помещения (центральные операторские, щитовые, технические помещения) защищены физическими средствами контроля доступа (ограждения, контроль допуска, замки), системами видеонаблюдения и др. Посещение таких помещений разрешено только ограниченному кругу известных лиц в сопровождении уполномоченных сотрудников с обязательной регистрацией.

Следует использовать запирающиеся шкафы с оборудованием.

Рекомендуется удалять или блокировать ненужные интерфейсы ведущих вычислительных узлов предприятия, такие как USB, оптические дисководы и беспроводные устройства. Пользователь должен тщательно контролировать применение основных устройств обеспечения защиты информации, таких как электронные ключи инженерных/операторских станций, в системе менеджмента.

А.2.2 Разделение на зоны и защита периметра

Сети функциональной безопасности не изолированы, а подключаются к системе управления, корпоративным сетям для необходимого взаимодействия друг с другом. Эти сети подвержены более широкому кругу атак, чем традиционные физически разделенные сети; например, попытка несанкционированного доступа в корпоративную сеть может распространяться на системы, связанные с безопасностью, и наносить им ущерб. Для защиты сетевых интерфейсов систем, связанных с безопасностью, могут требоваться дополнительные средства пограничной защиты, такие как выделенный межсетевой экран для систем, связанных с безопасностью, системы аутентификации и авторизации сетевого доступа, доступ только для чтения к системам, связанным с безопасностью, проверка достоверности вводимых данных/проверка целостности данных/команд, передаваемых по сетям в систему, связанную с безопасностью.

А.2.3 Коммуникационный протокол для обеспечения функциональной безопасности и защиты информации

В традиционных системах, связанных с безопасностью, для экстренной связи обычно применяют закрытые протоколы; в то же время на предприятиях широко распространены общие протоколы связи (например, на основе Ethernet), что создает дополнительные риски (такие, как имитация экстренных сообщений и атаки типа «отказ в обслуживании») для протоколов экстренной связи. Необходимо уделять особое внимание усилению контрмер по защите информации для передаваемых данных.

А.2.4 Контроль удаленного доступа

Удаленный доступ редко применяется в традиционных средствах обеспечения функциональной безопасности, однако широко распространен в инфраструктурах предприятий. Это значительно увеличивает риск подслушивания и угрозы от получения доступа путем обмана, например при атаках с участием посредника. Необходимо внедрять контрмеры по защите информации для контроля удаленного доступа; также рекомендуется детализировать политики и процедуры защиты информации каждой внедренной системы.

А.2.5 Беспроводное управление доступом

Беспроводная связь широко применяется в интеллектуальном производстве (например, в промышленном Интернете вещей и вычислениях на периферийных устройствах). Существуют перспективы применения беспроводных технологий в системах обеспечения функциональной безопасности. При использовании беспроводной свя-

зи следует уделять особое внимание контролю доступа. В настоящем стандарте не рассматривается применение беспроводных технологий.

А.2.6 Уровень устройств

Производители устройств должны принимать меры по защите информации своих изделий и предотвращать распространение и выполнение вредоносного кода. Для повышения безопасности и защищенности устройств производители могут использовать ядра операционных систем, наборы протоколов и др.

Уязвимости операционной системы и приложений представляют непосредственную угрозу для устройства. Поставщики должны искать уязвимости, анализировать общее оборудование и устройства, обнаруживать и своевременно устранять уязвимости защиты информации в операционных системах и приложениях.

Владельцам предприятий следует уделять пристальное внимание уязвимостям защиты информации, выпуску исправлений для основных полевых устройств, принятию мер для своевременного обновления исправлений, строгой оценке защиты информации и испытанию исправлений перед установкой.

Для доступа к полевым устройствам применяются уникальные идентификаторы, которые зависят от функций оборудования и позволяют приложениям верхних уровней, в том числе промышленным Интернет-платформам, выполнять подтверждение личности на основе идентификаторов оборудования. Также следует обеспечивать возможность использования компонентов аппаратных средств (микросхем или встроенных программ) в качестве корня доверия для безопасной загрузки полевых устройств, конфиденциальной передачи и защиты целостности данных.

А.2.7 Уровень управления

Среда управления на предприятии интегрирует информационные и эксплуатационные технологии.

Традиционный процесс управления производством является закрытым, но заслуживающим доверия. Постепенное повышение связности значительно расширяет спектр последствий нарушений системы защиты информации. Информационная безопасность может ухудшать функциональную безопасность и вызывать ряд других последствий.

Следует обнаруживать возможные источники опасностей, опасные условия и инциденты и собирать информацию об обнаруженных опасностях (продолжительность, интенсивность, вредность, область действия, механические силы, взрывоопасные условия, скорость реакции, воспламеняемость, уязвимость, потеря информации и др.).

Необходимо определять опасные условия или инциденты, возникающие между управляющим программным обеспечением и устройствами, включая причину происшествия и типы событий (отказы компонентов, отказы программ, ошибки человека и другие связанные с отказами механизмы, которые могут приводить к опасным событиям).

Необходимо анализировать комплексное влияние на функциональную безопасность характеристик типовых производственных процессов, технологических процессов и управления качеством.

Следует рассматривать состояние отсутствия управления функциональной безопасностью, которое может возникать в результате автоматизации, интеграции и информатизации, а также определять механизмы мониторинга, раннего оповещения или аварийной сигнализации, диагностики неисправностей, восстановления, сбора и регистрации данных, которые необходимо внедрять.

Необходимо определять разумно предсказуемое неправильное использование, которое может возникать в ходе эксплуатации интеллектуальной системы оператором, а также способность этой интеллектуальной системы противодействовать атакам злоумышленников.

Интеллектуальные устройства и интеллектуальные системы должны быть способны противостоять или устранять влияние физических, электрических, магнитных, радиационных, пожарных и сейсмических условий, а также должны быть в состоянии обнаруживать и обрабатывать аварийные нарушения или прерывания.

А.2.8 Интеграция мер по защите информации

Необходимо интегрировать меры по защите информации в систему обеспечения функциональной безопасности:

- аутентифицировать пользователей с различными правами на выполнение операций различных типов;
- при разработке протоколов для функциональной безопасной связи должны использоваться соответствующие меры шифрования конфиденциальной информации, чтобы гарантировать, что информация двух сторон не будет получена третьей стороной;
- выполнять тестирование кода системы управления функциональной безопасностью перед эксплуатацией для обнаружения дефектов в программном обеспечении, использовать меры проверки целостности для верификации программного обеспечения управления функциональной безопасностью и своевременного обнаружения несанкционированного доступа к программному обеспечению. Создавать резервную копию программного обеспечения для управления функциональной безопасностью и программы конфигурации;
- для систем управления функциональной безопасностью принять меры контроля для обнаружения, предотвращения и восстановления при появлении вредоносного кода;
- тщательно тестировать изменения и обновления системы управления, разрабатывать подробный план восстановления предыдущего состояния, тестировать и внедрять важные исправления в максимально короткий срок, а при общих исправлениях — тестировать и развертывать только необходимые;

- поставщики систем управления функциональной безопасностью обязаны своевременно реагировать и предоставлять инструкции или решения по устранению уязвимостей в системе управления функциональной безопасностью либо возможные альтернативные решения, такие как закрытие портов, которые можно использовать;

- мониторинг и аудит защиты информации для системы управления функциональной безопасностью позволяет своевременно обнаруживать нарушения защиты информации в сети и избегать их, а также предоставлять подробную информацию для анализа нарушений защиты информации.

А.2.9 Интеграция мониторинга функциональной безопасности и защиты информации

Из-за большого количества новых технологий и устройств на предприятиях фактически отсутствуют ретроспективные данные об источниках опасностей, опасных событиях и их периодичности. По этой причине результаты оценки рисков при проектировании предприятия могут быть недостоверными, а функции безопасности, которые разработаны на их основе, — не соответствовать фактическим требованиям предприятия. В связи с этим на предприятии необходимо настроить реализованную платформу мониторинга рисков, используя которую определять источники опасностей, опасные события и их периодичность, угрозы информационной безопасности и их периодичность, а также рабочее состояние соответствующего устройства безопасности. Эту информацию используют для оценки функциональной безопасности и защиты информации интеллектуальных предприятий.

А.2.10 Мониторинг нормального режима работы

В целом эксплуатация систем, связанных с безопасностью, и связанных с защитой информации контрмер, должна соответствовать спецификации требований безопасности/защиты информации, чтобы гарантировать, что требуемые функции безопасности поддерживаются с требуемым значением УПБ.

В нормальном режиме работы систем, связанных с безопасностью, осуществляется их непрерывный онлайн-контроль с применением человеко-машинного интерфейса, а системой конфигурации доступ пользователей к системе, связанной с безопасностью, для программирования обычно запрещен. Во внутренних системах предприятия можно организовывать удаленный доступ к данным мониторинга, используя человеко-машинный интерфейс с мобильных устройств, однако эти данные должны быть доступны только для чтения. В этом случае самой серьезной проблемой с точки зрения защиты информации является конфиденциальность данных мониторинга. Необходимо обеспечивать конфиденциальность данных всех потоков, которые передаются по общедоступной сети (например, посредством шифрования), регистрировать попытки удаленного доступа и выполнять надлежащую аутентификацию и авторизацию при удаленном доступе.

А.2.11 Плановое техническое обслуживание и текущий осмотр

Учитывая аспекты безопасности, плановое техническое обслуживание систем, связанных с безопасностью, включает в себя контрольные проверки, текущий осмотр, обход и любые действия по профилактическому техническому обслуживанию. Как правило, эти действия выполняют квалифицированные специалисты, их также планируют и документально оформляют.

Контрольные проверки выполняют по плану в соответствии с письменно оформленной процедурой для проверки того, что функции безопасности работают согласно спецификации системы, а текущий осмотр выполняют периодически для обнаружения несанкционированных изменений. Следует регистрировать фактическую интенсивность и причину запросов для обнаружения несоответствий между фактическим и запланированным применением.

Байпас допускается только при наличии компенсирующих мер для обеспечения допустимого снижения риска. Выполнение байпаса должно быть санкционировано, зарегистрировано и ограничено по времени.

Для защиты информации следует периодически проверять системное программное обеспечение и контрмеры защиты информации (например, наличие изменений в конфигурации системы защиты информации). Кроме того, следует периодически выполнять верификацию механизмов обеспечения защиты информации, чтобы удостовериться, что все контрмеры защиты информации сконфигурированы и работают в соответствии с проектом.

Для обеспечения защиты информации следует строго контролировать удаленный доступ к системам, связанным с безопасностью, с правом записи, например при байпасе или даже для программирования. Разрешение на удаленный доступ должно предоставляться после аутентификации и авторизации. Необходимо контролировать целостность операций доступа и все подозрительные действия. Доступ должен быть ограничен во времени с обязательным последующим завершением сеанса.

А.2.12 Изменение

Необходимо проанализировать возможное воздействие изменений любой части системы, связанной с безопасностью, на функциональную безопасность. Как правило, такой анализ предусмотрен в отлаженной процедуре управления изменениями для функциональной безопасности. При проектировании защиты информации необходимо применять дополнительное управление изменениями для контрмер защиты информации, в том числе предусматривать мониторинг, тестирование и выпуск обновлений/исправлений программного обеспечения, выполняющего контрмеры защиты информации, а также повторную валидацию после модификации.

Библиография

[1] IEC 61508-1:2010, Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 1: General requirements

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

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

[4] IEC TR 62443-3-1:2009, Industrial communication networks — Network and system security — Part 3-1: Security technologies for industrial automation and control systems

[5] IEC 62443-3-2:2020, Security for industrial automation and control systems — Part 3-2: Security risk assessment for system design

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

[7] IEC TR 63069:2019, Industrial-process measurement, control and automation — Framework for functional safety and security

УДК 62-783:614.8:331.454.004.056.5:006.354

ОКС 13.110
25.040.99
29.020

Ключевые слова: безопасность функциональная, защита информации, жизненный цикл систем, системы управления, промышленная автоматизация, уровень полноты безопасности, уровень эффективности защиты, оценка рисков

Редактор *Н.А. Аргунова*
Технический редактор *В.Н. Прусакова*
Корректор *М.И. Першина*
Компьютерная верстка *И.А. Налейкиной*

Сдано в набор 14.06.2024. Подписано в печать 28.06.2024. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 1,86. Уч.-изд. л. 1,48.

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.

gost.e-ecolog.ru gost.e-ecolog.ru

gost.e-ecolog.ru