ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 59506— 2021/ IEC TR 63074:2019

БЕЗОПАСНОСТЬ МАШИН

Вопросы защиты информации в системах управления, связанных с обеспечением функциональной безопасности

(IEC TR 63074:2019, 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. № 397-ст

4 Настоящий стандарт идентичен международному документу IEC TR 63074:2019 «Безопасность машин. Вопросы защиты информации в системах управления, связанных с обеспечением функциональной безопасности» (IEC TR 63074:2019 «Safety of machinery — Security aspects related to functional safety of safety-related control systems», IDT).

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

Дополнительные сноски в тексте стандарта, выделенные курсивом, приведены для пояснения текста оригинала

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

Умышленное нарушение информационной безопасности систем промышленной автоматики может происходить вследствие того, что:

- к системе управления возможен доступ, например перепрограммирование функций машины (включая связанные с безопасностью);
- происходит «сближение» между стандартными ИТ системами и промышленными системами;
- во встроенных системах стали появляться операционные системы, собственные сетевые протоколы заменяются IP протоколами и данные передаются в офисную сеть непосредственно из сети SCADA;
- программное обеспечение разрабатывается путем повторного использования существующих компонентов программного обеспечения сторонних производителей;
- удаленный доступ от поставщиков стал стандартным способом эксплуатации/технического обслуживания с повышенным риском нарушения кибербезопасности, учитывая, например, несанкционированный доступ, нарушение доступности и целостности защищаемых ресурсов.

Связанные с безопасностью системы управления машин являются частью систем промышленной автоматики и могут подвергаться атакам, которые могут привести к потере способности поддерживать безопасное функционирование машины.

Примечание 1 — Возникающий риск, связанный с возможностями атак, является значительным с учетом тенденций и изменений угроз, а также количества известных уязвимостей. Цели защиты информации описываются главным образом с точки зрения конфиденциальности, целостности и доступности, которые необходимо определять в целом и с учетом приоритетов, используя риск-ориентированный подход.

Цели функциональной безопасности учитывают риск, оценивая тяжесть причиненного вреда и вероятность возникновения этого вреда. Последствия любого риска (опасное событие) определяют требования к полноте безопасности (уровень полноты безопасности (SIL) согласно МЭК 62061 или МЭК 61508 или уровень эффективности защиты (PL) согласно ИСО 13849-1).

Что касается функции безопасности, то угрозы нарушения защиты информации (внутренние или внешние) могут влиять на полноту безопасности и общую готовность системы.

Примечание 2 — Чтобы обеспечить достижение целей защиты информации, необходимо использовать содержащиеся в МЭК 62443-3-3 определения и рекомендуемые требования к защите информации («фундаментальные требования»), которые должны быть выполнены соответствующей системой.

Примечание 3 — В настоящем стандарте не рассматривается общая стратегия защиты информации, так как она представлена, например, в МЭК 62443 (все части) или ИСО/МЭК 27001.

В некоторых стандартах по функциональной безопасности машин [например, МЭК 61496 (все части) и ИСО 14119] рассматривается нецелевое физическое использование.

Примечание 4 — «Нецелевое физическое использование» не связано с физической защитой информации, которая определена в МЭК 62443 (все части), например в 4.3.3.3 МЭК 62443-2-1:2010. С физической защитой информации связано, например, управление (ограничение) доступом посредством физического препятствия.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

БЕЗОПАСНОСТЬ МАШИН

Вопросы защиты информации в системах управления, связанных с обеспечением функциональной безопасности

Safety of machinery.
Security aspects related to functional safety of safety-related control systems

Дата введения — 2021—11—30

1 Область применения

В настоящем стандарте представлено руководство по применению стандарта МЭК 62443 (все части), связанное с теми вопросами угроз и уязвимостей информационной безопасности, которые могут повлиять на функциональную безопасность, выполняемую и реализуемую системами управления, связанными с безопасностью (SCS), а также могут привести к потере способности поддерживать безопасную эксплуатацию машины.

Примечание 1 — Например, попытка несанкционированного доступа к машине (ее функции безопасности), которая влияет на готовность машины и может привести к блокировке функции безопасности.

В настоящем стандарте рассматриваются следующие вопросы, связанные с защитой информации в машине, с возможным их применением к SCS:

- уязвимости SCS, которые могут быть использованы прямо или косвенно (через другие части машины), что может привести к нарушению информационной безопасности;
- влияние на характеристики функциональной безопасности и способность SCS должным образом выполнять свою функцию (функции);
- определение типового варианта использования и применение соответствующей модели угрозы.

Примечание 2 — Для других вопросов, связанных с угрозами и уязвимостями информационной безопасности, могут применяться положения МЭК 62443 (все части).

2 Нормативные ссылки

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

IEC 62061, Safety of machinery — Functional safety of safety-related electrical, electronic and programmable electronic control systems (Безопасность машин. Функциональная безопасность электрических, электронных и программируемых электронных систем управления, связанных с безопасностью)

ISO 12100:2010, Safety of machinery — General principles for design — Risk assessment and risk reduction (Безопасность машин. Общие принципы конструирования. Оценка риска и снижение риска)

ISO 13849-1:2015, Safety of machinery — Safety-related parts of control systems — Part 1: General principles for design (Безопасность машин. Элементы систем управления, связанные с безопасностью. Часть 1. Общие принципы конструирования)

Издание официальное

3 Термины и определения

3.1 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/
- онлайн-платформа ИСО: доступна по адресу https://www.iso.org/obp.

3.1.1 **актив** (asset): Физический или логический объект, который представляет для системы управления ощущаемую или реальную ценность.

[МЭК 62443-3-3:2013, пункт 3.1.1; изменено — «IACS», заменена «система управления», удалено примечание]

3.1.2 **атака** (attack): Посягательство на систему, являющееся следствием рациональной угрозы.

[МЭК 62443-3-3:2013, пункт 3.1.3; изменено — удалены примечания]

3.1.3 **доступность (работоспособность)** (availability): Способность компонента выполнить требуемое действие при заданных условиях в заданный момент времени или в продолжение 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.

Примечание 3 — Во французском языке используется также термин «disponibilit» в значении «текущая доступность», а в немецком языке в этом значении используется также термин «Verfügbarkeit».

[IEC/TS 62443-1-1:2009, пункт 3.2.16, изменено — в примечании 3 добавлена информация о термине на немецком языке]

3.1.4 **конфиденциальность** (confidentiality): Сохранение разрешенных ограничений на доступ к информации лицам, процессам или устройствам.

[IEC/TS 62443-1-1:2009, пункт 3.2.28]

3.1.5 **система управления** (control system): Система, которая реагирует на входные данные, например, от технологического процесса, других элементов машины, оператора, внешнего оборудования контроля и генерирует выходной сигнал (выходные данные), вызывая предписанное функционирование машины.

3.1.6 **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 машину в опасное или потенциально опасное состояние, или

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

[МЭК 61508-4:2010, пункт 3.6.7; изменено — «УО» заменено на «машину»]

3.1.7 **функциональная безопасность** (functional safety): Часть общей безопасности, обусловленная применением оборудования и системы управления оборудованием, которая зависит от правильности функционирования связанной с безопасностью системы управления, связанных с безопасностью систем управления, основанных на других технологиях, и внешних средств по снижению риска.

[МЭК 61508-4:2010, пункт 3.1.12; изменено — «УО» заменено на «оборудование», «Э/Э/ПЭ» удалено]

3.1.8 **машины, механизмы** (machine, machinery): Оборудованная или предназначенная для оборудования системой привода совокупность связанных между собой частей и устройств, одно из которых движется и которые соединены вместе для определенного применения.

Примечание — Термин «машина»/«механизм» также распространяется на совокупность машин, которые конструируются и управляются таким образом, чтобы функционировать как единое целое.

[ИСО 12100:2010, пункт 3.1; изменено — удалено примечание 1]

3.1.9 **защитные меры** (protective measure): Меры, предпринимаемые для адекватного снижения степени риска:

- конструктором (разработка безопасной конструкции машины, средств защиты и дополнительных защитных мер, информации для пользователя);

- пользователем (осуществление безопасной эксплуатации, технический контроль, система допуска к работе; применение дополнительных защитных мер; использование средств индивидуальной защиты; обучение персонала).

[ИСО 12100:2010, пункт 3.19; изменено — удалено примечание]

3.1.10 **риск** (risk): Сочетание вероятности нанесения и степени тяжести возможного ущерба или вреда здоровью.

[ИСО 12100:2010, пункт 3.12]

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

[Руководство ИСО/МЭК 51:2014, пункт 3.14]

3.1.12 **функция безопасности** (safety function): Функция машины, отказ которой может привести к немедленному возрастанию риска(ов).

[ИСО 12100:2010, пункт 3.30]

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

[МЭК 61508-4:2010, пункт 3.5.4; изменено — «Э/Э/ПЭ система, связанная с безопасностью» заменено на «система управления, связанная с безопасностью», удалены приложения]

3.1.14 **система управления, связанная с безопасностью** (SCS, Safety-related Control System): Часть системы управления машиной, выполняющая функцию безопасности.

Примечание — SCS эквивалентна SRECS, определенной в МЭК 62061:2015, или одной или нескольким SRP/CS, определенным в ИСО 13849-1.

[МЭК 62061, пункт 3.2.4; изменено — удалено примечание]

3.1.15 **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).

[IEC/TS 62443-1-1:2009, пункт 3.2.99]

3.1.16 **контрмера, мера защиты информации** (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.

[IEC/TS 62443-1-1:2009, пункт 3.2.33; изменено — добавлен второй предпочтительный термин «мера защиты информации», удалено примечание]

3.1.17 **уровень защиты информации**; УЗИ (security level): Мера достоверности того, что IACS (система промышленной автоматики и контроля) лишена уязвимостей и функционирует надлежащим образом.

[МЭК 62443-3-3:2013, пункт 3.1.38, изменено — удалено примечание]

3.1.18 **риск нарушения информационной безопасности** (security risk): 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 — «риск» заменено на «риск нарушения информационной безопасности»]

3.1.19 **оценка риска нарушения информационной безопасности** (security risk assessment): Процесс систематического выявления потенциальных уязвимостей значимых ресурсов системы и угроз для этих ресурсов, количественной оценки потенциального ущерба и последствий на основе вероятностей их возникновения, и (в случае необходимости) разработки рекомендаций по выделению ресурсов для организации контрмер с целью минимизации уязвимости.

[IEC/TS 62443-1-1:2009, пункт 3.2.88, изменено — «оценка риска» заменено на «оценка риска нарушения информационной безопасности», «общей уязвимости» заменено на «уязвимости», удалены примечания]

3.1.20 **подсистема** (subsystem): Объект высокоуровневого проектирования архитектуры системы, связанной с безопасностью, где опасный отказ подсистемы приводит к опасному отказу функции безопасности.

[МЭК 61508-4:2010, 3.4.4: изменено — в определении удалена ссылка на 3.6.7, перечисление а)]

3.1.21 **угроза** (threat): Обстоятельство или событие, способное негативно отразиться на процессах хозяйствования (включая задачи, функции, имидж или репутацию), объектах, системах управления или людях посредством получения несанкционированного доступа, уничтожения, раскрытия, видоизменения данных и/или отказа в обслуживании.

[МЭК 62443-3-3:2013, пункт 3.1.44]

3.1.22 **пользователь машины** (user of the machine): Субъект, несущий полную ответственность за машину.

3.1.23 **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 защищенности.

Примечание — Уязвимости могут появиться в результате преднамеренного выбора конструкции или могут быть непреднамеренными в результате непонимания условий эксплуатации. Они также могут возникать по мере износа оборудования и в результате его окончательного старения, что происходит за более короткий период времени, чем это обычно происходит для основного процесса или управляемого оборудования. Уязвимости не ограничиваются электронными или сетевыми системами.

Машина, которая изначально имеет ограниченную уязвимость, может стать более уязвимой в таких ситуациях, как изменение внешней среды, изменение технологии, отказ системных компонентов, несоответствие требованиям по замене компонентов, текучесть кадров и появление разведывательной информации о новых угрозах.

[IEC/TS 62443-1-1:2009, пункт 3.2.135, изменено — добавлено примечание]

3.1.24 **оценка уязвимости** (vulnerability assessment): Формальное описание и анализ уязвимости системы.

[МЭК 62443-2-1:2010, пункт 3.1.44]

4 Функциональная безопасность и информационная безопасность

4.1 Общие положения

Взаимосвязь между вопросами обеспечения функциональной безопасности и информационной безопасности можно охарактеризовать следующим образом:

- машина имеет соответствующие меры защиты;
- меры защиты информации, применяемые для машины, должны обеспечить предотвращение ухудшения эффективности мер защиты, которые реализуют функцию(и) безопасности.

Примечание — Лица, обладающие квалификацией для реализации мер защиты информации, не обязательно имеют квалификацию, необходимую для реализации SCS. Поэтому специалистам целесообразно взаимно обмениваться информацией и помощью.

4.2 Цели обеспечения функциональной безопасности

Безопасность машин основывается на оценке риска (безопасности) в соответствии с ИСО 12100 или на соответствии стандарту типа С[1)] для конкретных типов машин в сочетании с производными мерами по снижению риска, которые реализуются функцией(ями) безопасности.

Примечание — Для обеспечения возможности проектирования машин, безопасных для их предполагаемого использования, конструкторы при разработке машин выполняют оценку риска, включая также реализацию мер по снижению риска.

Функции безопасности, выполняемые SCS, должны обеспечивать уровень полноты безопасности, соответствующий значению SIL согласно МЭК 62061 или значению PL согласно ИСО 13849-1.

4.3 Цели обеспечения информационной безопасности

Вообще говоря, целью информационной безопасности главным образом является обеспечение конфиденциальности, целостности и доступности информации.

Примечание 1 — Например, цели обеспечения защиты информации:
- предотвращение несанкционированного изменения или уничтожения данных;
- обеспечение конфиденциальности методами, общими как для специалистов по информационной безопасности, так и для специалистов по промышленной автоматике;
- обеспечение доступности (в обычном и более широком смысле) машины(машин) (включая функции безопасности).

Оценка рисков информационной безопасности осуществляется путем оценки достижения всех идентифицированных целей информационной безопасности.

Оценка достижения целей информационной безопасности должна быть основана на рассмотрении изделия/системы в его/ее среде эксплуатации, к которой применимы угрозы и известные уязвимости. Цель этой деятельности состоит в том, чтобы выработать соответствующие меры защиты информации, применяемые к машине для достижения всех целей информационной безопасности.

Примечание 2 — См. также 5.5 IEC/TS 62443-1-1:2009.

В контексте функциональной безопасности машины меры по защите информации предназначены для защиты способности обеспечивать безопасную эксплуатацию машины, а их применение не должно негативно влиять на какую-либо функцию безопасности (см. рисунок 1).

Примечание 3 — Жизненно важные функции согласно МЭК 62443-3-3 включают функции безопасности.

В силу характера угроз и известных факторов уязвимостей выполнение оценки рисков нарушения информационной безопасности должно управляться событиями или выполняться периодически (периодический анализ защиты информации), см. также приложение В.

Примечание 4 — См. также IEC/TS 62443-1-1, жизненный цикл уровня информационной безопасности.

Примечание 5 — Оценка и управление рисками нарушения информационной безопасности имеют жизненно важное значение для определения того, что именно необходимо защитить и каким образом это может быть достигнуто.

В рамках данного контекста на рисунке 2 представлены возможные последствия нарушения информационной безопасности для SCS.

[1)] *Стандарты типа С — стандарты по безопасности машин, рассматривающие детализированные требования к безопасности отдельной машины или группы машин.*

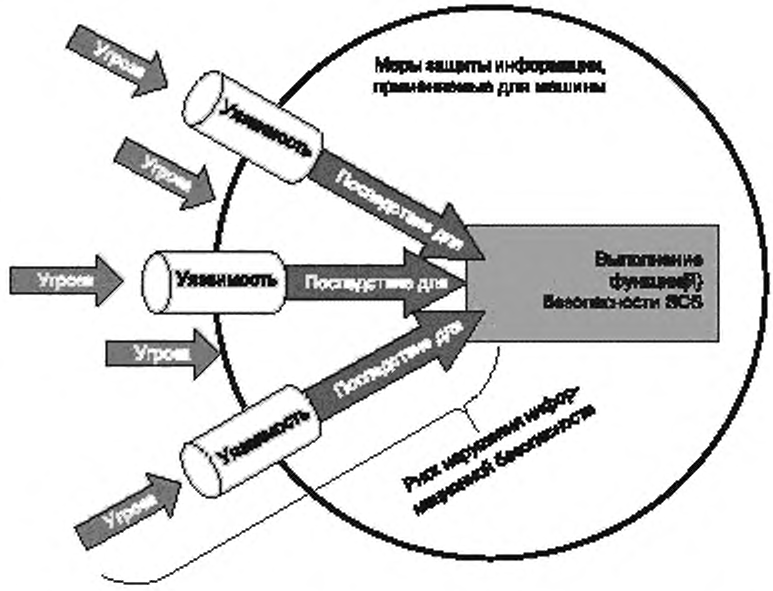


Рисунок 1 — Взаимосвязь между угрозами, уязвимостями и последствиями нарушения информационной безопасности для SCS, выполняющей функцию(и) безопасности

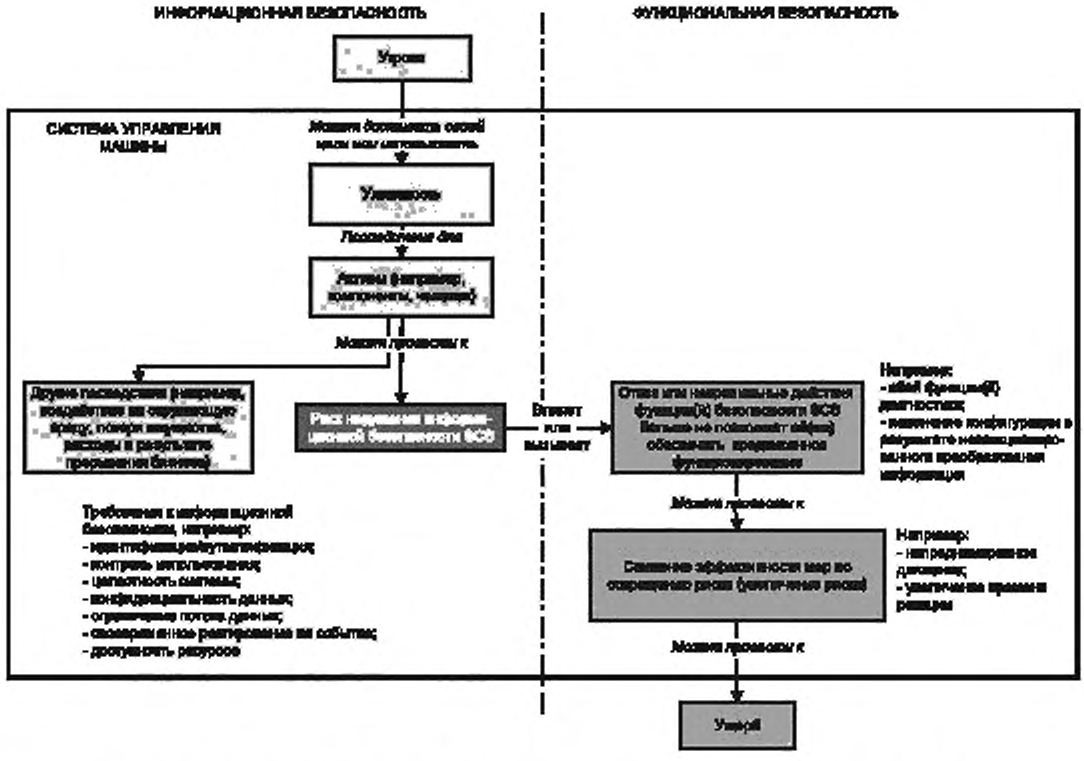


Рисунок 2 — Возможные последствия нарушения информационной безопасности в SCS

5 Вопросы защиты информации, связанные с функциональной безопасностью

5.1 Общие положения

5.1.1 Оценка рисков нарушения информационной безопасности

Примечание 1 — Дополнительная информация приведена в МЭК 62443-2-1 и МЭК 62443-3-2.

Оценка рисков нарушения информационной безопасности для SCS является частью общей оценки рисков нарушения информационной безопасности машины в ее внешней среде и включает в себя выполнение этой оценки на различных стадиях, таких как проектирование, реализация, ввод в эксплуатацию, эксплуатация и техническое обслуживание.

Примечание 2 — Производитель машины обычно не имеет достаточной информации о функционировании машины в ее внешней среде для того, чтобы выполнить общую оценку риска нарушения информационной безопасности, поэтому такая оценка обычно выполняется пользователем машины и ее производителем совместно.

Примечание 3 — Реализация или возникновение «скрытых» угроз или уязвимостей возможны на всех стадиях жизненного цикла.

Примечание 4 — МЭК 62443-4-1 содержит рекомендации по использованию для всех изделий актуализированной модели угроз, в которой учитываются следующие характеристики:

- регламентированный поток классифицированной информации по всей системе;
- границы доверия;
- процессы;
- хранилища данных;
- взаимодействующие внешние объекты;
- внутренние и внешние протоколы связи, реализуемые в изделии;
- внешние физические порты доступа, включая порты отладки;
- соединительные элементы монтажных плат, такие как разъемы JTAG, или заголовки файлов отладки, которые могут использоваться для несанкционированного доступа на компоненты аппаратных средств;
- возможные направления атак, включая атаки на аппаратные средства, если применимо;
- возможные угрозы и их серьезность, определяемые балльной системой оценки уязвимости, например CVSS (Общая система оценки уязвимости);
- ослабление последствий и/или устранение для каждой угрозы;
- выявленные проблемы, связанные с защитой информации;
- внешние зависимости от драйверов или сторонних приложений (их код не разрабатывается поставщиком), с которыми скомпоновано приложение.

Оценка уязвимости является частью оценки риска нарушения информационной безопасности.

Поэтому для выявления уязвимостей машины (которыми можно воспользоваться для реализации угроз) и возможного их влияния на обеспечение функциональной безопасности необходимо выполнить оценку ее уязвимости.

Для этого должна быть доступна следующая информация:

a) описание устройств, для которых выполняется оценка уязвимостей (например, мобильный пульт управления или любое другое устройство, подключенное к системе управления, связанной с безопасностью);

b) описание выявленных уязвимостей, которые могут быть использованы для реализации угроз и могут привести к повышению риска нарушения информационной безопасности.

Примечание 5 — Уязвимости могут появиться в результате преднамеренного выбора конструкции или могут быть случайными, например вследствие непонимания некоторых условий эксплуатации машины;

c) описание частей SCS (например, аппаратных средств или программного обеспечения), которые должны быть защищены мерами защиты информации.

Производитель машины может сделать некоторое допущение об угрозах и реализовать меры защиты информации на основе результатов описанной выше оценки уязвимости.

Примечание 6 — В некоторых случаях связь между производителем машины и пользователем машины невозможна.

Для того, чтобы меры защиты информации соответствовали контексту общей оценки риска нарушения информационной безопасности, должна проводиться верификация мер защиты информации.

Примечание 7 — Верификация соответствия мер(ы) защиты информации обычно выполняется в пользовательской среде машины, для этого может потребоваться информация о допустимых угрозах.

Ниже приводятся примеры задач, решаемых в процессе оценки риска нарушения информационной безопасности:

- выявление угроз и их источников (включая преднамеренные атаки на аппаратные средства, прикладные программы и связанное с ними программное обеспечение);
- описание возможных последствий (рисков нарушения информационной безопасности), обусловленных сочетанием выявленных угроз и уязвимостей (см. рисунок 1);
- определение требований к дополнительным мерам.

Примечание 8 — Дополнительными мерами для снижения последствий угрозы могли быть соответствующие связанные с безопасностью функции(я) управления, например связанный с безопасностью контроль предельных значений, дополнительные меры защиты информации, организационные меры или комбинации из этих мер;

- описание или ссылки на информацию о мерах защиты информации, принятых для сокращения или устранения угроз.

Примечание 9 — Связанная с безопасностью система управления, которая изначально имеет ограниченную уязвимость, может стать более уязвимой в таких ситуациях, как изменение внешней среды, изменение технологии, отказ системы, невозможность замены устройств, текучесть кадров и дополнительные разведданные о новых угрозах.

5.1.2 Стратегия снижения рисков нарушения информационной безопасности

Примечание 1 — Дополнительная информация приведена в 5.6.4 IEC/TS 62443-1-1:2009.

Примечание 2 — Сопоставимым с термином «ослабление риска» является термин «снижение риска», используемый для реализации функциональной безопасности механизмов.

Стратегия снижения рисков нарушения информационной безопасности должна быть определена в процессе оценки риска нарушения информационной безопасности SCS и учтена в общей оценке рисков нарушения информационной безопасности машины.

Меры по снижению рисков нарушения информационной безопасности для обеспечения функциональной безопасности механизмов включают:

- уменьшение недопустимых рисков нарушения информационной безопасности, используя:

a) исключение из проекта рисков нарушения информационной безопасности (избегая их); либо

b) ограничение рисков нарушения информационной безопасности (например, непосредственно производителем машины, или мерами защиты информации, применяемыми пользователем машины, или мерами, совместно используемыми производителем и пользователем машины).

Примечание 3 — Стратегия снижения рисков нарушения информационной безопасности может представлять собой стратегию эшелонированной защиты в соответствии с рисунком 3 МЭК 62443-4-1:2018;

- принятие риска нарушения информационной безопасности, если он является допустимым.

Примечание 4 — Если риск нарушения информационной безопасности является допустимым, то дальнейшие действия не требуются.

5.2 Меры защиты информации

5.2.1 Общие положения

Любая мера защиты информации, применяемая в машине, не должна негативно влиять на функцию безопасности, выполняемую SCS. Необходимо провести дальнейшее исследование, например, более глубокое изучение влияния мер защиты информации на функциональную безопасность (например, на время реакции функции безопасности).

Примечание 1 — Меры защиты информации, применяемые к функциям в штатном режиме работы (функциям машины), могут оказывать влияние на функции безопасности, выполняемые SCS.

Особенно следует рассмотреть следующие вопросы:

- сетевая архитектура.

Примечание 2 — Могут возникнуть проблемы архитектуры, относящиеся к SCS, например:

a) проектирование сети (например, см. зональную и трактовую модель в 6.5 IEC/TS 62443-1-1:2009);

b) конфигурация брандмауэра;
c) авторизация и аутентификация пользователя;
d) взаимодействие различных сетей управления производственным процессом;
e) беспроводные коммуникации;
f) доступ к внешним сетям (т. е. к Интернету);

- портативные устройства;
- беспроводные устройства и датчики (это часть предыдущей сетевой архитектуры);
- удаленный доступ;
- интерфейсы с другими системами или интерфейсы человек—машина.

В приложении А содержится некоторая информация об угрозах, которая может помочь лучше понять взаимосвязь между угрозой и уязвимостью.

Примечание 3 — Меры защиты информации могут быть вне машины (например, процедуры политик и осведомленность о них, физическая безопасность, защита информации в сети, компьютерная безопасность и безопасность приложений).

Примечание 4 — SCS как часть общей системы управления может использоваться для дополнения и поддержки мер защиты информации.

Меры защиты информации должны учитывать фундаментальные требования, описанные в МЭК 62443 (все части), и возможное их влияние на SCS. В таблице 1 представлен обзор фундаментальных требований.

Кроме того, меры защиты информации должны разрабатываться с учетом мотивации нарушителя и последствий несанкционированных воздействий на защищаемую информацию.

Таблица 1 — Фундаментальные требования и возможное их влияние на SCS

Фундаментальные требования защиты информации	Краткое описание	Безопасность механизмов Возможное влияние на SCS
Управление идентификацией и аутентификацией	Идентифицировать и аутентифицировать всех пользователей (людей, программно-реализуемые процессы и устройства) перед предоставлением им доступа к системе управления	Модификация или несанкционированное использование
Контроль использования	Контролировать соблюдение привилегий, закрепленных за аутентифицированным пользователем (физическим лицом, программно-реализуемым процессом или устройством), на выполнение запрашиваемого действия применительно к системе управления и отслеживать использование этих привилегий	Модификация или несанкционированное использование
Целостность системы	Обеспечивать целостность системы управления для предотвращения несанкционированного использования	Влияние на полноту безопасности
Конфиденциальность данных	Обеспечивать конфиденциальность информации в коммуникационных каналах и в хранилищах данных для предотвращения ее несанкционированного извлечения	Может иметь значение для безопасности
Ограничение потока данных	Сегментировать систему управления на зоны и тракты для ограничения неоправданного потока данных	Влияние на полноту безопасности
Своевременный отклик на события	Реагировать на нарушения защищенности путем уведомления соответствующего ответственного лица или инстанции, предоставлять необходимые свидетельства нарушения и принимать своевременные корректирующие действия при выявлении инцидентов	Может иметь значение для полноты безопасности
Доступность ресурсов	Обеспечивать доступность к ресурсам системы управления без ущерба ее функциональности и отказов жизненно важных сервисов	Влияние на готовность

Примечание 1 — На основе фундаментальных требований, представленных в 5.3 IEC/TS 62443-1-1:2009 и приложении В МЭК 62443-3-3:2013.

Примечание 2 — Нет никакой прямой корреляции между SIL/PL, определенными в МЭК 61508, МЭК 62061 и ИСО 13849-1, и SL (уровень защиты информации), определенным в МЭК 62443-3-3.

5.2.2 Идентификация и аутентификация

Может потребоваться возможность идентификации и аутентификации доступа к SCS.

Примечание 1 — Дополнительная информация приведена в разделе 5 МЭК 62443-3-3:2013.

Примеры предотвращения несанкционированного доступа и модификации:
- идентификация и аутентификация пользователей;
- аутентификация сетей;
- управление учетными записями для программного обеспечения;
- управление беспроводным доступом;
- аутентификация с помощью паролей;
- создание паролей и ограничение их длительности действия для пользователей;
- процедуры идентификации и аутентификации между машинами.

Примечание 2 — Информация об управлении аутентификаторами, включая использование паролей, устанавливаемых по умолчанию, приведена в 5.7.2 МЭК 62443-3-3:2013.

5.2.3 Контроль использования

Как только пользователь идентифицирован и аутентифицирован, SCS должна разграничить допустимые действия по авторизованному использованию SCS (назначенными привилегиями для аутентифицированного пользователя).

Примечание — Дополнительная информация приведена в разделе 6 МЭК 62443-3-3:2013.

5.2.4 Целостность системы

Обычно после ввода машины(ин) в эксплуатацию ее собственник отвечает за поддержание целостности системы управления (включая SCS) для предотвращения неавторизованных манипуляций.

Примечание 1 — Обеспечение целостности системы основано на оценке рисков нарушения информационной безопасности. Информацию о событиях, инициирующих оценку рисков нарушения информационной безопасности, см. в приложении В.

Примечание 2 — Дополнительная информация приведена в разделе 7 МЭК 62443-3-3:2013.

Поэтому могут быть важны следующие аспекты:

- целостность/устранение нарушений в коммуникациях (LAN, WLAN и т. д.) может достигаться, например, при использовании криптографической защиты целостности в недоверенных сетях;
- защита от вредоносного кода (от неавторизованных манипуляций, например вирусов, червей, троянских коней и шпионского программного обеспечения) может быть обеспечена, например, при использовании соответствующих механизмов для интерфейсов (например, USB, интерфейсов программирования PLC или SCS);
- целостность программного обеспечения и информации (обеспечивается защитой от неавторизованных изменений);
- валидация входных данных (выполняется с использованием правил проверки входных данных, а также значений вне допустимого диапазона).

5.2.5 Конфиденциальность данных

Некоторая информация, генерируемая системами управления, либо хранящаяся, либо передаваемая, носит конфиденциальный или важный характер. Это предполагает, что некоторые коммуникационные каналы и хранилища данных нуждаются в защите от перехвата данных и неавторизованного доступа к ним.

Примечание — Дополнительная информация приведена в разделе 8 МЭК 62443-3-3:2013.

Для системы(систем) управления этот аспект может быть важен для функциональной безопасности, например неавторизованный доступ к базе данных, предоставляющей идентификационные данные и привилегии авторизованных лиц.

5.2.6 Ограничение потока данных

Любые требования к ограничениям потока информации будут определяться в результате общей оценки рисков нарушения информационной безопасности машины.

Примечание — Дополнительная информация приведена в разделе 9 МЭК 62443-3-3:2013.

Задержка передачи данных или увеличенное время отклика на запрос могут влиять на полноту безопасности SCS (например, конфигурацию сети).

5.2.7 Своевременное реагирование на событие

Собственник машины (машин) должен устанавливать политики и регламенты защиты информации, а также надлежащие пути взаимодействия и управления, необходимые для реагирования на нарушения информационной безопасности машины.

Примечание — Дополнительная информация приведена в разделе 10 МЭК 62443-3-3:2013.

Этот аспект будет рассматриваться в процессе общей оценки рисков нарушения информационной безопасности машины и может влиять на полноту безопасности SCS.

5.2.8 Доступность ресурсов

Цель состоит в обеспечении устойчивости системы управления к разного рода событиям отказа в обслуживании.

Примечание — Дополнительная информация приведена в разделе 11 МЭК 62443-3-3:2013.

Этот аспект будет учитываться в процессе общей оценки рисков нарушения информационной безопасности машины.

Задержка передачи данных или увеличение времени отклика на запрос могут повлиять на готовность SCS.

6 Верификация и техническое обслуживание мер защиты информации

Реализация мер по обеспечению защиты информации должна верифицироваться и технически обслуживаться пользователем машины(машин), производителем машины и производителем подсистемы в зависимости от обстоятельств (см. также 5.1.1 об оценке рисков нарушения информационной безопасности).

Примечание — Верификация может быть выполнена путем тестирования или анализа.

7 Информация для пользователя машины (машин)

В целях поддержки общей оценки рисков нарушения информационной безопасности производитель машины должен предоставить пользователю машины(машин) определенную информацию.

Такая информация обычно может включать в себя:

- краткое описание функций безопасности (архитектура, топология сети и т. д.).

Примечание 1 — Это описание может включать предварительные требования к мерам защиты информации для предотвращения снижения эффективности функции безопасности, выполняемой SCS (см. 5.2):

- информацию, основанную на оценке уязвимости (см. 5.1.1), или в соответствующих случаях, основанную на выявленных или подтвержденных уязвимостях;
- информацию о мерах защиты информации, уже реализованных в машине (см. 5.2), где это было необходимо.

Примечание 2 — Информация о начальном обмене и обновлении информации содержится в приложениях В и С.

Приложение А
(справочное)

Основные сведения об угрозах и подходе к моделированию угроз

А.1 Оценка угроз

Угрозы характеризуют возможные действия, которые могут быть предприняты в отношении системы. По форме угрозы могут быть случайными либо в форме несанкционированных изменений.

Угрозы для активов могут возникнуть как от непреднамеренных событий, так и от преднамеренных злонамеренных вмешательств.

Фактор угрозы — это термин, используемый для описания субъекта, представляющего собой угрозу. Факторы угрозы известны и как нарушители или злоумышленники.

В конечном счете никакая защита от несанкционированных проникновений, отказов, ошибок или стихийных бедствий никогда не может быть стопроцентной.

Факторами угроз являются:

- злоумышленник, который целенаправленно несанкционированно проникает в системы ради финансов, власти, из мести или иной выгоды, а именно:
- инсайдер — «доверенное» лицо, сотрудник, подрядчик или поставщик, владеющий информацией, которая, как правило, не известна общественности. Инсайдер может представлять собой угрозу даже при отсутствии неблаговидных намерений. Например, угроза может возникнуть в результате обхождения инсайдером элементов управления безопасностью для «выполнения своей работы»;
- аутсайдер — лицо или группа, не наделенные правом внутреннего доступа, известные или не известные целевой организации. Аутсайдеры могли когда-то быть инсайдерами;
- неумышленная ошибка (ошибка), вызванная лицом, которое либо по ошибке не обратило внимание, либо не осознало последствий своих действий. Компьютерные приложения также могут иметь «ошибки» или другие дефекты, которые вызывают неверное выполнение операций. К этой категории относятся также не достаточно глубоко проработанные системы и несоответствующие процедуры эксплуатации;
- отказ оборудования (отказ), в котором нет вины какого-либо лица, но который отражает тот факт, что электронные и механические устройства могут выйти из строя. Оборудование, которое реагирует непредвиденным образом в нормальных условиях, также может быть отнесено к этой категории;
- стихийные бедствия (катастрофы), вызванные событиями абсолютно независимыми от людей.

Угрозы могут быть пассивными или активными.

Пассивная угроза. Факторы таких угроз обычно собирают пассивную информацию при случайных вербальных коммуникациях с сотрудниками и подрядчиками.

Активная угроза. Примерами активных угроз являются:

- коммуникационная атака — ее целью является нарушение коммуникации в системах управления;
- вторжение в базу данных — атаки с вторжением в базу данных применяют для похищения информации из базы данных или нарушения целостности данных базы данных;
- воспроизведение — из коммуникационных путей систем управления могут быть скопированы сигналы, которые впоследствии могут быть воспроизведены для обеспечения доступа к защищенным системам или фальсификации данных в системе управления;
- фиктивная авторизация и маскировка под законного пользователя — в контексте вычислительных сетей данное понятие используют для описания разнообразных способов, которыми можно «обмануть» аппаратные средства или программное обеспечение;
- социальная инженерия — факторы данной угрозы также получают или пытаются получить иным образом конфиденциальные данные, обманом заставляя человека раскрыть конфиденциальную информацию;
- фишинг — основан на социальной инженерии, т. к. человек склонен верить в надежность брендов, связывая их с авторитетностью;
- вредоносный код — вредоносные коды, используемые в ходе атак, могут принимать форму вирусов, червей, автоматических эксплоитов или троянских коней;
- отказ в обслуживании (DoS) — отказ (или ухудшение) в обслуживании, происходящий в ходе атак, влияет на работоспособность сети, операционной системы или прикладных ресурсов;
- расширение привилегий — благодаря расширенным привилегиям злоумышленник может совершать действия, которые в противном случае будут запрещены;
- физическое повреждение — атаки с физическим повреждением имеют целью разрушение или выведение из строя физических компонентов (например, аппаратных средств, устройств хранения программного обеспечения, соединительных элементов, датчиков и контроллеров), которые являются частью системы управления.

Примечание — Дополнительная информация об угрозах приведена в 5.6.5 IEC/TS 62443-1-1:2009.

А.2 Примеры угроз для устройств, связанных с безопасностью

Следует рассмотреть возможный сценарий атаки, который может повлиять на функцию(ии) безопасности, которую(ые) выполняет SCS, используя одно или несколько устройств, связанных с безопасностью.

Следует рассмотреть вопрос о возможном доступе к устройствам, входящим в состав SCS, любого лица с намерением нанести вред. Злонамеренные действия (человека) представляют угрозу, заключающуюся во взятии контроля над устройством, связанным с безопасностью. Такое злонамеренное действие может произойти непосредственно с устройством, связанным с безопасностью, например:

- с интерактивным экраном или панелью управления;
- переключателями или кнопками для конфигурирования устройства;
- конфигурацией или программой, хранящимися в памяти, например на съемной SD-карте.

Примечание — Перечень вышеперечисленных действия является далеко не полным. Существует много других возможных уязвимостей для выполнения злонамеренного действия, включая инструментальные средства, предоставленные производителем для конфигурирования системы управления, связанной с безопасностью.

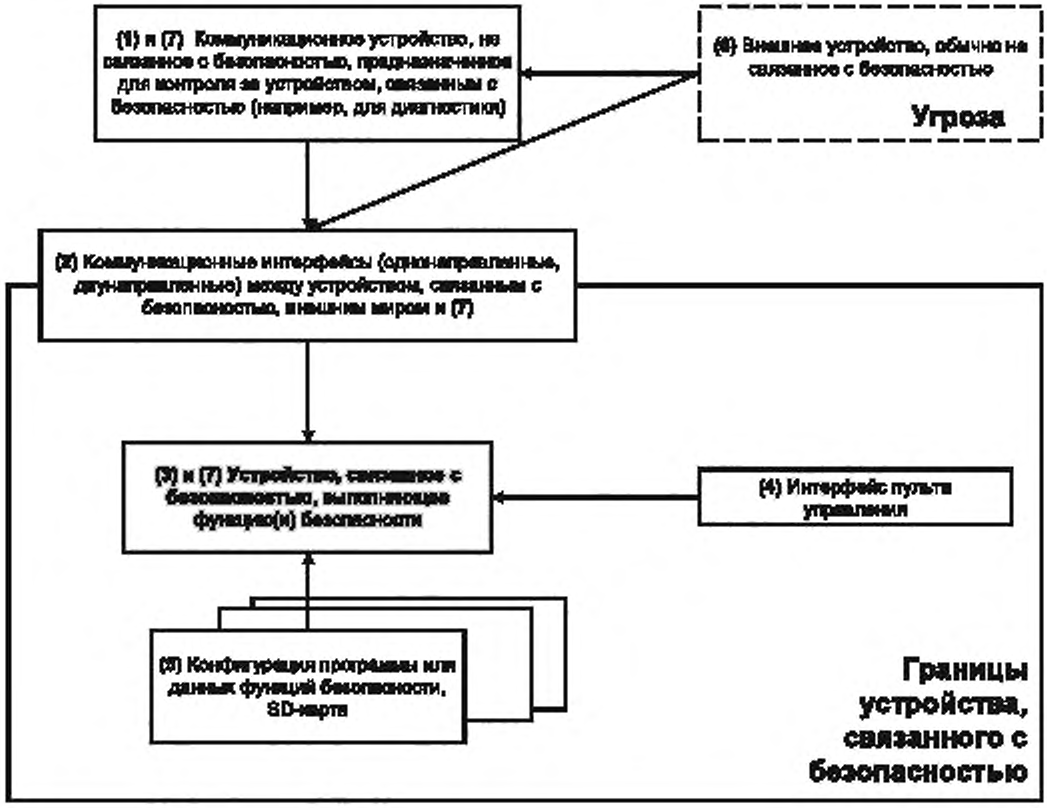
Несанкционированное проникновение в устройство, связанное с безопасностью, может произойти неявно, например в результате применения:

- компьютерной технологии;
- технологии коммуникационных сетей;
- технологии беспроводной связи.

В этих трех случаях доступ к связанному с безопасностью устройству можно получить неявно с помощью других технологий. Несанкционированные проникновения хорошо известны в компьютерных технологиях.

Уязвимость защиты информации устройства, связанного с безопасностью, связана с технологиями, используемыми для доступа к нему. Меры защиты информации должны уделять особое внимание «слабым местам» каждой такой технологии.

На рисунке А.1 показан пример уязвимости, когда функция безопасности может быть изменена в результате угрозы.



На каждом уровне, где возможен доступ к функции безопасности, необходимы различные меры, например:

Уровень	Пояснение
1	Связь между устройством контроля и устройством, связанным с безопасностью, может быть источником уязвимости. В результате несанкционированного проникновения в связанное с безопасностью устройство или отказа устройства контроля может произойти неправомерный доступ к функции безопасности.
2	Связь между связанным с безопасностью устройством и системой контроля в большинстве случаев осуществляется через соединительный разъем. Выбор однонаправленного ответвителя (от связанного с безопасностью устройства к системе контроля) может ограничить доступ злонамеренного действия к функции безопасности. Эта технология аналогична используемой для серверов и сетей. Сбои хорошо известны, и в таких местах применяются хорошо опробованные меры защиты от хакерских атак.
3	Устройство, связанное с безопасностью, выполняющее функцию(и) безопасности.
4	Пульт управления может иметь доступ к устройствам, выполняющим функцию безопасности. Различные уровни защиты паролей для различных привилегий доступа могут уменьшить уязвимость.
5	На некоторых устройствах, связанных с безопасностью, конфигурирование выполняется с помощью сетевых коммутаторов или защищенной цифровой карты памяти (SD-карты). Несанкционированное проникновение может представлять из себя замену сетевых коммутаторов или SD-карты, содержащей программу конфигурирования. Поэтому необходима реализация мер защиты информации.
6	Портативное внешнее устройство, которое обычно не подключено, может получить доступ к устройству, связанному с безопасностью, через коммуникационный интерфейс или коммуникационное устройство. В данном случае это угроза, аналогичная той, которая описана для уровня 2.
7	В ситуации, описанной в уровне 6, источником несанкционированного проникновения может быть программа, загруженная в коммуникационный интерфейс, которая может управлять устройством безопасности по запросу. — примеры такого типа атаки на DNS-серверы известны

Рисунок А.1 — Связанное с безопасностью устройство и возможности доступа к нему

Приложение В
(справочное)

События, инициирующие оценку рисков нарушения информационной безопасности

В.1 Общие положения

Оценка рисков нарушения информационной безопасности главным образом зависит от установленных условий использования, в результате чего уменьшается необходимость в дальнейшей итерации оценки рисков. Возможно, это не так для оценки рисков нарушения информационной безопасности, когда характер угроз точно не определен, и в таком случае оценка рисков нарушения информационной безопасности инициируется событием или выполняется периодически.

В.2 Инициирующие события

Для инициирования оценки рисков нарушения информационной безопасности конечным пользователем машины такими событиями могут быть, например:

- проектирование, разработка или модификация машины (исходные данные предоставляются производителем машины);
- интеграция и использование машины (исходные данные предоставляются изготовителем машины).

Примечание 1 — Например, подключение ранее автономно функционирующей машины к Интернету;

- изменение использования машины.

Примечание 2 — Например, одна и та же машина производит различные изделия (активы), которые ценятся выше, чем производились до этого, или когда ценность одной и той же продукции (активов) выше, по общему мнению. Более высокая ценность изделия может вызвать серьезный мотив для несанкционированного проникновения;

- обновление подсистемы или элементов подсистемы (например, устройств), включая коммерчески доступное (COTS) программное обеспечение или программное обеспечение с открытым исходным кодом (исходные данные предоставляются поставщиком подсистемы или устройства или производителем машины);
- информация о том, что интерфейс/услуга становятся уязвимыми в другом месте, даже если они используются в системе с закрытым исходным кодом (исходные данные предоставляются поставщиком подсистемы или устройства или производителем машины на основе исходных данных от поставщика технологии);
- организационные и кадровые изменения в компании, которые могут иметь последствия для защиты информации;
- слияние с более крупной компанией/известным брендом.

Примечание 3 — Более крупные компании, возможно, более популярны для атак, даже если их продукция не менялась (за исключением торговой марки).

Приложение С
(справочное)

Пример информационного потока между поставщиком устройства, производителем машины (интегратором) и конечным пользователем машины

С.1 Общие положения

В настоящем приложении представлен пример, описывающий поток информации между поставщиком устройства, производителем машины (интегратором) и конечным пользователем машины.

С.2 Пример

На рисунке С.1 представлен пример, демонстрирующий информационные потоки между поставщиком устройства, производителем машины (интегратором) и пользователем машины на стадии проектирования. Производитель машины играет ключевую роль на стадии проектирования для достижения требований, полученных от пользователя машины, с учетом информации от поставщиков устройства и дополнительных мер защиты информации.

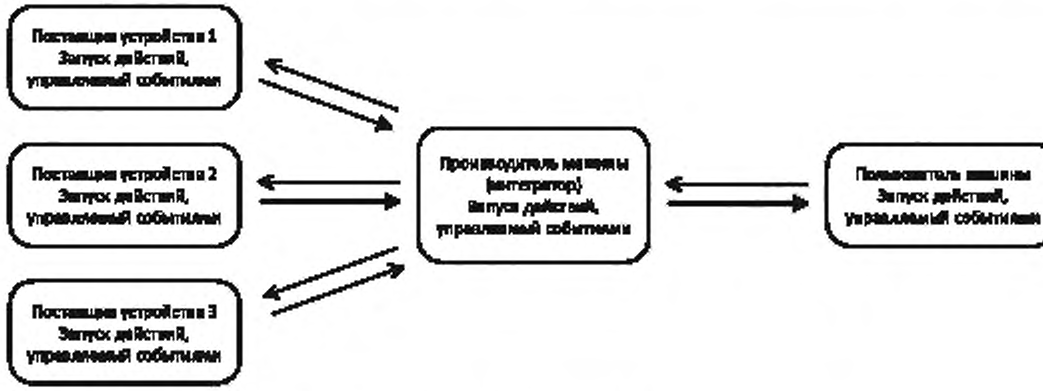


Рисунок С.1 — Пример потока информации на этапе проектирования

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов национальным и межгосударственным стандартам

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального, межгосударственного стандарта
IEC 62061	IDT	ГОСТ Р МЭК 62061—2015 «Безопасность оборудования. Функциональная безопасность систем управления электрических, электронных и программируемых электронных, связанных с безопасностью»
ISO 12100:2010	IDT	ГОСТ ISO 12100—2013 «Безопасность машин. Основные принципы конструирования. Оценки риска и снижения риска»
ISO 13849-1:2015	—	*

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

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

- IDT — идентичные стандарты.

Библиография

IEC 60204-1, Safety of machinery — Electrical equipment of machines — Part 1: General requirements

IEC 61496 (all parts), Safety of machinery — Electro-sensitive protective equipment

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

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

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

IEC 62443 (all parts), Security for industrial automation and control systems

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

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

IEC 62443-4-1:2018, Security for industrial automation and control systems — Part 4-1: Secure product development lifecycle requirements

IEC TR 62351-12, Power systems management and associated information exchange — Data and communications security — Part 12: Resilience and security recommendations for power systems with distributed energy resources (DER) cyber-physical systems

ISO/IEC Guide 51:2014, Safety aspects — Guidelines for their inclusion in standards

ISO/IEC 27001, Information technology — Security techniques — Information security management systems — Requirements

ISO 13849-2:2012, Safety of machinery — Safety-related parts of control systems — Part 2: Validation

ISO 14119, Safety of machinery — Interlocking devices associated with guards — Principles for design and selection

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, защита информации, машины и механизмы, уязвимости, риски, угрозы, меры защиты информации

Технический редактор *В.Н. Прусакова*
Корректор *Л.С. Лысенко*
Компьютерная верстка *М.В. Лебедевой*

Сдано в набор 20.05.2021. Подписано в печать 28.05.2021. Формат 60×84¼. Гарнитура Ариал.
Усл. печ. л. 2,79. Уч.-изд. л. 2,52.

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