ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

ПРЕДВАРИТЕЛЬНЫЙ НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПНСТ 877— 2023 (ИСО/МЭК 30147:2021)

Информационные технологии

ИНТЕРНЕТ ВЕЩЕЙ

Методология обеспечения доверенности

(ISO/IEC 30147:2021, Information technology — Internet of things — Methodology for trustworthiness of IoT system/service, MOD)

Издание официальное

Москва
Российский институт стандартизации
2023

Предисловие

1 ПОДГОТОВЛЕН Федеральным государственным бюджетным образовательным учреждением высшего образования «МИРЭА — Российский технологический университет» (РТУ МИРЭА) на основе собственного перевода на русский язык англоязычной версии стандарта, указанного в пункте 4

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 194 «Кибер-физические системы»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 27 ноября 2023 г. № 71-пнст

4 Настоящий стандарт является модифицированным по отношению к международному стандарту ИСО/МЭК 30147:2021 «Информационные технологии. Интернет вещей. Методология обеспечения доверенности системы/сервиса ИВ» (ISO/IEC 30147:2021 «Information technology — Internet of things — Methodology for trustworthiness of IoT system/service», MOD) путем изменения отдельных фраз (слов, значений показателей, ссылок), которые выделены в тексте курсивом. Внесение указанных технических отклонений направлено на учет потребностей национальной экономики Российской Федерации.

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

Сведения о соответствии ссылочных национальных стандартов международным стандартам, использованным в качестве ссылочных в примененном международном стандарте, приведены в дополнительном приложении ДА

5 Некоторые элементы настоящего стандарта могут быть объектами патентных прав. Федеральное агентство по техническому регулированию и метрологии не несет ответственности за установление подлинности каких-либо или всех таких патентных прав

Правила применения настоящего стандарта и проведения его мониторинга установлены в ГОСТ Р 1.16—2011 (разделы 5 и 6).

Федеральное агентство по техническому регулированию и метрологии собирает сведения о практическом применении настоящего стандарта. Данные сведения, а также замечания и предложения по содержанию стандарта можно направить не позднее чем за 4 мес до истечения срока его действия разработчику настоящего стандарта по адресу: 119454 Москва, проспект Вернадского, д. 78 и/или в Федеральное агентство по техническому регулированию и метрологии по адресу: 123112 Москва, Пресненская набережная, д. 10, стр. 2.

В случае отмены настоящего стандарта соответствующая информация будет опубликована в ежемесячном информационном указателе «Национальные стандарты» и также будет размещена на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (www.rst.gov.ru)

Содержание

Введение

В системах Интернета вещей (ИВ) все устройства ИВ взаимно соединены друг с другом, и ожидается, что это даст определенные преимущества в повседневной жизни. При этом традиционные устройства управления системами (термостаты, системы освещения, системы управления светофорами и т. д.), ранее не подключавшиеся к интернету, присоединяются без учета уровня доверенности, требуемого целевой системе. Многие устройства подключаются без использования мер и средств контроля и управления безопасностью и без процессов обеспечения безопасности для серверов, ПК и смартфонов. Ошибки или сбои в этих устройствах, обусловленные недостаточным уровнем доверенности, могут оказать значительное влияние на пользователей и работу систем. Это означает, что у систем и сервисов ИВ имеются отличительные свойства и характеристики по сравнению с иными ИТ-системами и сервисами, в том числе:

- крайне высокие масштаб и степень воздействия угроз;
- срок службы систем и сервисов ИВ может быть сверхдлинным, особенно при эксплуатации и обслуживании;
- мониторинг и управление некоторыми типами устройств ИВ могут быть очень сложны;
- сущности связи, включая устройства ИВ, могут не знать в достаточной мере окружение друг друга;
- функции и характеристики устройств ИВ могут быть ограничены технологически;
- в системах и сервисах ИВ могут быть установлены такие соединения между сущностями, которые не предполагали разработчики сущностей.

Целью настоящего стандарта является предоставление рекомендаций по обеспечению доверенности систем ИВ. Настоящий стандарт определяет процессы жизненного цикла системы для обеспечения доверенности систем ИВ посредством применения *ГОСТ Р 57193—2016*.

ПРЕДВАРИТЕЛЬНЫЙ НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационные технологии

ИНТЕРНЕТ ВЕЩЕЙ

Методология обеспечения доверенности

Information technology. Internet of things. Methodology for trustworthiness

**Срок действия — с 2024—01—01
до 2025—01—01**

1 Область применения

Настоящий стандарт определяет процессы жизненного цикла системы для внедрения и поддержания доверенности системы или сервиса ИВ посредством применения *ГОСТ Р 57193*. Процессы жизненного цикла системы применимы к системам и услугам ИВ для широкого спектра областей применения.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ Р 27.016 (МЭК 62853:2018) Надежность в технике. Надежность открытых систем

ГОСТ Р 57149/ISO/IEC Guide 51:2014 Аспекты безопасности. Руководящие указания по включению их в стандарты

ГОСТ Р 57193—2016 Системная и программная инженерия. Процессы жизненного цикла систем

ГОСТ Р ИСО 31000 Менеджмент риска. Принципы и руководство

ГОСТ Р ИСО/МЭК 27000 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология

ГОСТ Р ИСО/МЭК 27005 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности

ГОСТ Р ИСО/МЭК 27031 Информационная технология. Методы и средства обеспечения безопасности. Руководство по готовности информационно-коммуникационных технологий к обеспечению непрерывности бизнеса

Примечание — При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодному информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по выпускам ежемесячного информационного указателя «Национальные стандарты» за текущий год. Если заменен ссылочный стандарт, на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого стандарта с учетом всех внесенных в данную версию изменений. Если заменен ссылочный стандарт, на который дана датированная ссылка, то рекомендуется использовать версию этого стандарта с указанным выше годом утверждения (принятия). Если после утверждения настоящего стандарта в ссылочный стандарт, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, рекомендуется применять в части, не затрагивающей эту ссылку.

Издание официальное

3 Термины и определения

В настоящем стандарте применены термины по *ГОСТ Р 57193, ГОСТ Р ИСО/МЭК 27000*, а также следующие термины с соответствующими определениями:

3.1 **компонент** (component): Модульная, развертываемая и заменяемая часть системы, которая инкапсулирует реализацию и предоставляет набор интерфейсов.

3.2 **безотказность** (reliability): Способность элемента работать в соответствии с требованиями, без сбоев, в течение заданного интервала времени в заданных условиях.

3.3 **способность к восстановлению** (resilience): Устойчивость системы к сбоям или способность восстанавливать функциональность после перегрузки.

4 Сокращения

В настоящем стандарте применены следующие сокращения:

ИВ — интернет вещей;

ИКТ — информационно-коммуникационные технологии;

ОС — операционная система;

ПИВ — промышленный интернет вещей;

ПК — персональный компьютер;

SoS — система систем (System of systems).

5 Системы/сервисы ИВ и доверенность

5.1 Отличительные характеристики систем и сервисов ИВ

Сервис ИВ — это сервис, предоставляемый системой ИВ, которая может быть системой систем (SoS) с такими характеристиками, как операционная и административная независимость. Если система ИВ является SoS, то возможна ситуация, когда никто не несет ответственности за систему. Таким образом, отличительным свойством системы ИВ является то, что для достижения доверенности системы ИВ необходимо взаимодействие с организациями, отвечающими за составляющие системы. Доверенность системы ИВ достигнута, если удовлетворены все требования доверенности ИВ, поскольку доверенность системы ИВ зависит от каждой системы.

Настоящий стандарт предназначен для пользователей, отвечающих за реализацию и поддержание доверенности ИВ. При отсутствии сущности, ответственной за всю систему или сервис ИВ, настоящий стандарт применяется к каждой составляющей системе или сервису, у которых определена ответственная сущность. При этом не имеет значения, что составляющая система или сервис могут состоять из нескольких подсистем, часть которых эксплуатируется и управляется другими сущностями.

Действия и задачи в каждом процессе для реализации доверенности ИВ включены в действия и задачи для системы ИВ, с помощью которой предоставляется сервис ИВ. Если не указано иное, то описания действий и задач представлены для системы ИВ. Действия и задачи, применимые для сервиса ИВ, распространяются на сервис ИВ.

Рисунок 1 — Система ИВ, система систем

Сущность в системе ИВ может иметь следующие состояния:

1) скомпрометированная сущность. Злоумышленник получил контроль над сущностью и предоставляемыми данными, командами и элементами управления с намерением нарушить настройку всей системы ИВ, что приведет к потере доверия к сущности. Это приводит к взлому, например, самолетов или автомобилей;

2) неправильная конфигурация сущности. Из-за ошибки в команде и управлении конфигурация сущности демонстрирует состояние, не ожидаемое и ранее не обнаруживаемое, что приводит к потере доверенности системы ИВ.

Пример — Неправильная конфигурация датчиков CO_2 и SO в газовой турбине;

3) повреждение сущности. Из-за определенных условий эксплуатации сущность повреждается, что приводит к ситуации или заявлению о том, что сущность не заслуживает доверия.

Пример — Датчик высоты, скорости или положения закрылков в самолете, что может привести к катастрофе;

4) некорректное взаимодействие из-за интерфейсов неудовлетворительного качества. Интерфейсы между сущностями потеряли совместимость из-за различных факторов (обновлений, неправильных патчей, неправильной конфигурации и т. д.), что приводит к потере доверия к сущности.

Пример — Не установленное или неправильно установленное обновление в медицинских устройствах, что может вызвать серьезную проблему со здоровьем;

5) несовместимость из-за неправильной конфигурации. Сущность настроена неправильно (например, единицы измерения, размер обмена данными, характер данных и т. д.), в результате чего получаемая информация является бесполезной, что приводит к потере доверия к сущности.

Пример — Неправильная скорость передачи данных, используемая для настройки устройств ИВ;

6) отсутствие ответа. Сущность не отвечает другим сущностям в определенных ситуациях из-за ряда факторов (неизвестный запрос, ненастроенный ответ и т. д.), что приводит к потере доверия к сущности со стороны других сущностей.

Пример — Авиакатастрофа рейса Air France 447 в результате временной рассинхронизации показаний скорости;

7) невозможность распознать данные. Сущность генерирует ответ, который не распознается как содержательная информация из-за неправильной конфигурации других сущностей, в результате чего происходит потеря взаимного доверия.

Пример — Расхождение между отображаемыми высотами в результате сбоя высотомера.

Системы ИВ имеют отличительные свойства и характеристики по сравнению с иными ИТ-системами и сервисами, в том числе:

a) крайне высокие масштаб и степень воздействия угроз. Воздействия могут включать ущерб жизни и имуществу людей, утечку конфиденциальной информации людей;

b) срок службы систем и сервисов ИВ может быть сверхдлинным, особенно при эксплуатации и обслуживании. Например, срок службы системы ПИВ в среднем составляет более десяти лет;

c) трудоемкость и сложность мониторинга и управления некоторыми устройствами ИВ. К системам ИВ могут подключаться неуправляемые устройства ИВ. При этом пользователи могут не знать о возникновении проблем.

Пример — Проблемы с безопасностью системы ИВ из-за отсутствия обновления или проблем с прошивкой;

d) сущности связи, включая устройства ИВ, могут не знать в достаточной мере окружение друг друга;

e) технологическое ограничение функций и производительности устройств ИВ;

f) в системах ИВ могут быть установлены такие соединения между сущностями, которые не предполагали разработчики сущностей. После подключения устройства ИВ система, в которую устройство ИВ предоставляет данные, может измениться. Со временем могут изменяться владельцы данных и пользователи системы ИВ.

В приложении А представлены риски системы ИВ ввиду вышеуказанных свойств и характеристик. В приложении В приведен обзор способов решения указанных проблем с помощью процессов, определенных в разделе 6.

5.2 Доверенность ИВ

Доверенность системы ИВ реализуется, если реализуется доверенность всех сущностей в системе ИВ.

Доверенность системы ИВ, особенно в отношении безопасности, реализуется не только путем использования элементов ИКТ. В настоящем стандарте рассмотрены только элементы ИКТ.

Понятие доверенности ИВ схоже с понятием надежности, которое охватывает безотказность, доступность, обслуживаемость и возможность поддержки, а также другие связанные свойства, такие как долговечность, целостность, восстанавливаемость и робастность (см. *ГОСТ Р 27.016*). Настоящий стандарт определяет, что безопасность включает в себя целостность и доступность. Доверенность ИВ не включает в себя непосредственно обслуживаемость, возможность поддержки, долговечность, восстанавливаемость и робастность, но они являются аспектами достижения способности к восстановлению и безотказности в контексте доверенности ИВ.

Относительная значимость безопасности, защищенности, приватности, безотказности и способности к восстановлению зависит от характера и контекста системы ИВ.

Следующие факторы также могут иметь отношение к доверенности ИВ, и их рекомендуется учитывать в каждом процессе при необходимости:

a) согласованность. Взаимодействие между двумя или более сущностями должно быть упорядоченным и значимым в контексте ситуации;

b) последовательность. Взаимодействие между двумя или более сущностями должно быть последовательным и соответствовать ожиданиям, определенным ранее;

c) гибкость. Сущность должна быть в состоянии адаптироваться к различным условиям при изменении условий окружающей среды, взаимосвязей, контекста ситуации, ответов и т. д.;

d) робастность. Сущность должна быть надежной и не быть уязвимой к изменениям, внесенным в окружающую среду или интернет намеренно или непреднамеренно;

e) связанность. Сущности системы ИВ должны беспрепятственно функционировать как единое целое;

f) возможность восстановления. Сущность должна иметь возможность поддерживать и сохранять заданный уровень обслуживания даже в случае сбоя в конкретном контексте использования;

g) масштабируемость. Добавление сущности или новой функции сущности не должно требовать обновления существующей рабочей методологии, а учитывать, поддерживать и сохранять потенциал роста системы.

6 Процессы обеспечения доверенности ИВ

6.1 Общие сведения

Для каждого процесса следует использовать соответствующий подпункт и положения *ГОСТ Р 57193*, если не указано иное. В настоящем стандарте не приведены подпункты «Цель» и «Выход (выходные результаты)» для каждого процесса, так как отсутствуют изменения по сравнению с аналогичными подпунктами в *ГОСТ Р 57193*. В настоящем стандарте представлены только дополнения к подпунктам «Действия и задачи» *ГОСТ Р 57193* для каждого процесса.

6.2 Процессы соглашения

6.2.1 Процесс приобретения

В дополнение к *ГОСТ Р 57193—2016, подпункт* 6.1.1.3, следует выполнить следующие действия:

a) в a) 1) включить критерии выбора.

Примечание — Критерии выбора могут включать, например:

i) корректно установленные и эксплуатируемые системы управления, качественную справочную систему и систему поддержки, а также эффективное и квалифицированное сервисное управление;

ii) условия завершения контракта с поставщиком (например, истечение срока действия контракта, окончание поддержки);

b) в a) 2) включить в запрос требования к уровню доверенности ИВ процессов и целевой системы ИВ, в том числе постоянное совершенствование стандартных мер, соответствующих процедур и других факторов обеспечения доверенности ИВ. Если продукт или услуга обрабатывает персональные данные пользователей целевой системы ИВ, то в запрос следует включить принципы приватности по отношению к целевой системе ИВ, такие как согласие, выбор, прозрачность и индивидуальное участие;

c) в e) 1) подтвердить, что продукт или услуга удовлетворяет требованиям к доверенности ИВ в соглашении, если таковые имеются.

6.2.2 Процесс поставки

В дополнение к *ГОСТ Р 57193—2016, подпункт* 6.1.2.3, следует выполнить следующие действия:

a) в a) 2):

1) включить в критерии условия завершения контракта с приобретающей стороной (например, истечение срока действия контракта, окончание поддержки);

2) учитывать важность поставляемой системы или услуги в системе или услуги покупателя при определении стратегии поставок;

b) в c) 1) включить в критерии приемки, включаемые в соглашение, объем ответственности за доверенность ИВ на протяжении всего жизненного цикла;

c) в e) 2) включить постоянное совершенствование стандартных мер, соответствующих процедур и других факторов обеспечения доверенности ИВ.

6.3 Процессы организационного обеспечения проекта

6.3.1 Процесс управления моделью жизненного цикла

В дополнение к *ГОСТ Р 57193—2016, подпункт* 6.2.1.3, следует выполнить следующие действия:

a) в a) 5):

1) рассмотреть каждый из пяти факторов доверенности ИВ. Следует учесть, если фактор требует применения конкретной модели жизненного цикла, отличной от моделей жизненного цикла для других факторов. Следует устранить конфликты из-за различных моделей жизненного цикла в соответствии с приоритетами факторов, устанавливаемыми политикой доверенности ИВ.

6.3.2 Процесс управления инфраструктурой

Дополнения к данному процессу отсутствуют.

6.3.3 Процесс управления портфелем

Дополнения к данному процессу отсутствуют.

6.3.4 Процесс управления человеческими ресурсами

Для реализации доверенности целевой системы ИВ следует выполнить действия и задачи согласно *ГОСТ Р 57193—2016, подпункт* 6.2.4.3, ввиду быстрого обновления технологий ИВ.

6.3.5 Процесс управления качеством

Для реализации доверенности целевой системы ИВ следует выполнить действия и задачи согласно *ГОСТ Р 57193—2016, подпункт* 6.2.5.3, с заменой термина «качество» на термин «доверенность ИВ».

6.3.6 Процесс управления знаниями

Для реализации доверенности целевой системы ИВ следует выполнить действия и задачи согласно *ГОСТ Р 57193—2016, подпункт* 6.2.6.3, ввиду быстрого обновления технологий ИВ.

6.4 Процессы технического управления

6.4.1 Процесс планирования проекта

В дополнение к *ГОСТ Р 57193—2016, подпункт* 6.3.1.3, следует выполнить следующие действия:

a) в a) 1) определить политику доверенности ИВ. На первом этапе следует определить каждое взаимодействие (ввод/вывод) с другими взаимосвязанными системами ИВ и их политиками защиты данных. На втором этапе следует определить, какие факторы доверенности ИВ относятся к каждому взаимодействию, и приоритизировать факторы при каждом взаимодействии. С учетом полученной информации следует определить политику доверенности ИВ, включая бесперебойность действия целевой системы ИВ;

b) в b) 4):

1) после определения ролей ответственности, подотчетности и полномочия других связанных систем или сервисов определить роли ответственности, подотчетности и полномочия для каждого фактора доверенности ИВ (защищенности, приватности, безотказности, способности к восстановлению и безопасности) на протяжении всего жизненного цикла. Следует также определить роль, которая будет нести ответственность за доверенность всей системы ИВ. В этой роли может выступать группа обеспечения доверенности ИВ с несколькими участниками и руководителем. Следует определить руководителя группы по каждому из пяти факторов доверенности ИВ;

2) определить каналы связи между группой обеспечения доверенности ИВ и группами по каждому из пяти факторов доверенности ИВ, а также между соответствующими организациями, ответственными за другие соответствующие системы или сервисы;

c) в b) 6) запланировать приобретение материалов и услуг обеспечивающих систем, поставляемых извне проекта, особенно из других систем в системе ИВ, взаимосвязанных с целевой системой ИВ.

6.4.2 Процесс оценки и контроля проекта

В дополнение к *ГОСТ Р 57193—2016, подпункт* 6.3.2.3, следует выполнить следующие действия:

a) в a) 1) определить действия для приобретенных продуктов или систем, которые не соответствуют договорным требованиям относительно процессов технического управления и технических процессов;

b) в b) 7):

1) провести необходимый управленческий и технический анализ при возникновении внутренних и внешних инцидентов, связанных с доверенностью ИВ, и при подключении целевой системы ИВ к новым устройствам/системам ИВ;

2) проверить влияние, вызванное внутренними и внешними инцидентами, на доверенность ИВ в отношении производительности целевой системы ИВ, если это применимо.

c) в c) 1):

1) включить постоянную оптимизацию действий и задач для обеспечения доверенности ИВ в связанных процессах.

Примечание — Оптимизация включает обнаружение инцидентов безопасности, планы действий в чрезвычайных ситуациях и т. д.;

2) включить действия, которые сводят к минимуму ущерб и смягчают влияние возможных инцидентов на доверенность ИВ;

3) включить действия для функционирования целевой системы ИВ, позволяющие сохранить качество продуктов, если это применимо.

6.4.3 Процесс управления решениями

В дополнение к *ГОСТ Р 57193—2016, подпункт* 6.3.3.3, следует выполнить следующие действия:

a) в a) 3) вовлекать соответствующие заинтересованные стороны, которые связаны с целевой системой ИВ, в принятие решений, чтобы использовать их опыт и знания.

b) в b) 2) включить определенные факторы и риски в оцениваемые критерии выбора.

6.4.4 Процесс управления рисками

В дополнение к *ГОСТ Р 57193—2016, подпункт* 6.3.4.3, следует выполнить следующие действия:

a) проводить мероприятия по управлению рисками в соответствии с *ГОСТ Р ИСО 31000* или проводить их отдельно и параллельно для каждого фактора доверенности ИВ, например в соответствии со стандартами: *ГОСТ Р ИСО/МЭК 27005* в отношении защищенности, *ГОСТ Р ИСО/МЭК 27031* в отношении способности к восстановлению, *ГОСТ Р 57149* и другими стандартами в отношении безопасности. Следует учесть физические риски в отношении защищенности и изучить соответствующие несчастные случаи и инциденты, которые уже произошли в данной области деятельности;

b) в a) 1) определить, когда, при каких условиях и как часто следует проводить оценку риска. Это связано с тем, что риски и приемлемые риски целевой системы ИВ могут меняться с течением времени;

c) в a) 2):

1) определить активы и процессы целевой системы ИВ;

2) приоритизировать их по каждому из пяти факторов доверенности ИВ, где уровни приоритета определяются независимо от пяти факторов и утверждаются группой обеспечения доверенности ИВ;

d) в b) 1) определить критерии определения значимости риска. Критерии могут учитывать состояние риска (последствия и их вероятность) или другие факторы и быть различными для каждого фактора доверенности ИВ (например, решение о том, следует ли обрабатывать риск защищенности, может включать критерий максимально возможного и практически достижимого снижения рисков);

e) в c) записать результаты каждой задачи;

f) в c) 1) учесть:

1) риски, которые могут быть вызваны другими системами ИВ, подключаемыми к целевой системе ИВ в настоящее время или в будущем, в том числе при замене устройств ИВ/системы, а также риски возникновения инцидента в случае, когда целевая система ИВ получает противоречивые запросы от нескольких сущностей, между которыми нет связи;

2) риски целевой системы ИВ, которые могут повлиять на другие системы ИВ;

3) риски, вызванные внутренней фальсификацией, ошибками в работе и неосведомленностью пользователей о технических характеристиках устройств/систем ИВ;

g) по завершении действий d) 2) для каждого фактора оценить предлагаемые реакции на риски для проверки того, что реакции не создают новых рисков для целевой системы ИВ или других факторов доверенности ИВ. Данную задачу следует повторять до тех пор, пока все факторы не получат согласованные результаты. При наличии конфликтов между результатами процесса управления рисками факторов доверенности ИВ следует разрешить конфликты путем взаимодействия. Если конфликты не разрешены, группа обеспечения доверенности ИВ определяет приоритет среди рисков и разрешает конфликты;

h) в d) 4) рассмотреть и утвердить результаты всей деятельности процесса управления рисками, где группа обеспечения доверенности ИВ информируется о наличии разрешенных конфликтов, а также обновить существующий контроль новыми методами обработки рисков.

6.4.5 Процесс управления конфигурацией

В дополнение к *ГОСТ Р 57193—2016, подпункт* 6.3.5.3, следует выполнить следующие действия:

a) в a) 1):

1) управлять автоматическими обновлениями конфигурации;

2) включить защиту конфигурации в необходимые базовые линии;

3) координировать стратегию управления конфигурацией в организациях, управляющих системами ИВ, подключенными к целевой системе ИВ для охвата всего жизненного цикла целевой системы ИВ или объема контракта, в зависимости от ситуации;

b) в b) 4) рассмотреть риски защищенности, вызванные подключением к интернету, и учесть результаты в базовой линии, в частности для устройств/систем ИВ, ранее не подключенных к интернету;

c) в c) рассмотреть управление изменениями конфигурации с точки зрения доверенности ИВ.

6.4.6 Процесс управления информацией

В дополнение к *ГОСТ Р 57193—2016, подпункт* 6.3.6.3, следует выполнить следующие действия:

a) в a) 1):

1) определить стратегию для соблюдения принципов приватности, если целевая система ИВ обрабатывает персональные данные;

2) определить, кто и из каких ресурсов собирает релевантную информацию о доверенности ИВ и каким образом она анализируется.

Примечание — Информационные ресурсы могут включать поставщиков устройств ИВ, консультационные компании, национальную группу реагирования на инциденты компьютерной безопасности и т. д. Информация включает в себя контрмеры по доверенности ИВ, о которых должны быть осведомлены заинтересованные стороны;

3) классифицировать собранную и обработанную информацию в зависимости от важности и влияния, а также классифицировать заинтересованные стороны.

Примечание — Классификация собранной информации может быть основана на 5 факторах доверенности ИВ. Это упростит ее распространение среди соответствующих заинтересованных сторон для поддержания доверенности целевой системы ИВ;

4) определить уровень срочности информации;

5) определить в отношении каждого класса информации: кто, каким классам заинтересованных сторон, как, насколько срочно и на каком этапе жизненного цикла распространяет информацию;

Примечание — Данное действие включает в себя коммуникации с руководством и другими заинтересованными сторонами, включая внешние организации, по вопросам ответственности целевой системы ИВ, восстановления после крупного инцидента и т. д.;

6) определить правила раскрытия информации об инцидентах, произошедших в целевой системе ИВ;

b) в a) 4) определить форматы и структуру для каждого класса заинтересованных сторон во избежание непонимания передаваемой информации.

6.4.7 Процесс измерений

Для реализации доверенности целевой системы ИВ следует выполнить действия и задачи согласно *ГОСТ Р 57193 —2016, подпункт* 6.3.7.3.

6.4.8 Процесс гарантии качества

Для реализации доверенности целевой системы ИВ следует выполнить действия и задачи согласно *ГОСТ Р 57193—2016, подпункт* 6.3.8.3, путем замены термина «качество» на «доверенность ИВ».

В дополнение к *ГОСТ Р 57193—2016, подпункт* 6.3.8.3, следует выполнить следующие действия:

a) в a) 1) учесть следующие аспекты, связанные с характеристиками целевой системы ИВ:

1) тестирование защищенности и приватности в условиях, отражающих поведение и среду пользователей;

2) тестирование функций эксплуатации и обслуживания, которые предполагается использовать в течение длительного времени;

3) тестирование, при котором используется большой объем данных и множество устройств ИВ;

4) тестирование, при котором система ИВ используется непредусмотренным образом;

5) тестирование облачных/периферийных вычислений с внедрением целевой системы ИВ;

6) регуляторные требования, действующие в пределах области использования целевой системы ИВ.

6.5 Технические процессы

6.5.1 Процессы анализа бизнеса или назначения

В дополнение к *ГОСТ Р 57193—2016, подпункт* 6.4.1.3, следует выполнить следующие действия:

a) в a) 1) рассмотреть проблемы и возможности, связанные с доверенностью ИВ;

b) в b) 2) определить доверенность целевой системы ИВ.

Примечание — Определение доверенности ИВ при необходимости проверяется в последующих процессах;

c) в c) 1) определить базовые концепции функционирования (эксплуатации) и другие концепции с точки зрения доверенности ИВ.

6.5.2 Процесс определения потребностей и требований заинтересованной стороны

При проведении процесса определения потребностей и требований заинтересованной стороны следует включить организации, которые владеют/управляют системами ИВ, подключаемыми к целевой системе ИВ в перечень заинтересованных сторон.

В дополнение к *ГОСТ Р 57193—2016, подпункт* 6.4.2.3, следует выполнить следующие действия:

a) в a) 2) определить приоритеты потребностей и требований заинтересованных сторон с учетом важности целевой системы ИВ для продолжения деятельности;

b) в b) 1) включить точки зрения на доверенность ИВ и учесть срок эксплуатации целевой системы ИВ;

c) в b) 2) включить потребности заинтересованных сторон в доверенности ИВ;

d) в b) 3) учесть взаимосвязи между пятью факторами доверенности ИВ, включая конфликты;

e) в c) 2) включить взаимодействие между пользователями и системой и системами ИВ, которые должны быть подключены, при наличии;

f) в d) 3) включить требования заинтересованных сторон, соответствующие концепциям жизненного цикла, сценариям, взаимодействиям, ограничениям и критическим характеристикам качества в отношении доверенности ИВ;

g) в e) 1) учесть приоритет среди пяти факторов доверенности ИВ, если применимо;

h) в e) 2) включить показатели доверенности ИВ, если применимо.

6.5.3 Процесс определения системных требований

При проведении процесса определения системных требований следует определить требования к доверенности системы ИВ.

В дополнение к *ГОСТ Р 57193—2016, подпункт* 6.4.3.3, следует выполнить следующие действия:

a) в a) 1) принять во внимание доверенность ИВ;

b) в a) 2) уточнить существующие требования, относящиеся к устройствам и сетям ИВ, которые являются элементами целевой системы ИВ, например:

1) законодательные и нормативные требования;
2) существенные требования, не указанные в 1);
3) дополнительные отраслевые требования.

Примечание — Регуляторные требования могут исходить из нескольких источников и различаться в зависимости от юрисдикции. В качестве регуляторных требований к системе ИВ могут быть рассмотрены регуляторные требования в отношении кибербезопасности, защиты критической инфраструктуры, здоровья и безопасности, защиты окружающей среды и национальной безопасности.

c) в b) 1) классифицировать функции на административные и неадминистративные и при необходимости определить отношение к доверенности ИВ;

d) в b) 2) определить необходимые ограничения реализации в отношении доверенности ИВ, в частности с учетом ограниченных ресурсов устройств ИВ;

e) в b) 3) определить системные требования, которые относятся к рискам, критичности системы или критическим характеристикам качества в отношении доверенности ИВ;

Примечание — Системные требования в отношении доверенности ИВ включают:

- соответствующие начальные настройки и их проверку;
- авторизацию запросов к целевой системе ИВ;
- аутентификацию доступа и запросов к целевой системе ИВ, включая аутентификацию для физического доступа. В зависимости от важности приложения и риска доступа и запросов необходимо учитывать методы аутентификации, меры для множественных неудачных попыток аутентификации и т. д. Также необходимо учитывать многофакторную аутентификацию;
- защиту функций и активов. Защита включает шифрование и проверку целостности хранимых и передаваемых данных, проверку недействительности передаваемых данных и использование защищенного от несанкционированного доступа оборудования, если это применимо. При использовании криптографии необходимо учитывать управление жизненным циклом криптографических ключей;
- заблаговременное оповещение об аномалиях, например, исходя из прогностической информации;
- проактивные контрмеры против аномалий;
- мониторинг, запись и отчетность об аномалиях;
- получение зарегистрированных данных для выявления причин аномалий;
- мониторинг конфигураций компонентов в целевой системе ИВ;
- поддержание работы даже при возникновении аномалий. Выделение ресурсов в достаточном объеме необходимо для поддержания работы даже в случае отказа в обслуживании или стихийного бедствия в целевой системе ИВ;
- восстановление сразу после аномалий. Для восстановления необходимы резервное копирование соответствующих системных компонентов и проверка резервных данных;
- автономную остановку и приостановку работы;
- ограничение установки программного обеспечения после начала работы;
- удаление данных;
- поддержание доверенности ИВ даже по прошествии времени.

f) в b) 4) определить системные требования и обоснование доверенности ИВ;

g) в c) 1) анализировать полный набор системных требований с точки зрения доверенности ИВ, в частности согласуется ли данный набор с пятью факторами доверенности ИВ;

h) в c) 2) определить критические показатели функционирования, которые обеспечивают оценку степени технического достижения в отношении доверенности ИВ, если это необходимо;

i) в d) 1) получить подробное соглашение по системным требованиям от руководителя группы обеспечения доверенности ИВ.

6.5.4 Процесс определения архитектуры

В дополнение к *ГОСТ Р 57193—2016, подпункт* 6.4.4.3, следует выполнить следующие действия:

a) в a) 2) определить интересы заинтересованных сторон в отношении доверенности ИВ;

b) в a) 3) учесть поэтапный и непрерывный подход, поскольку в соответствующих регуляторных требованиях и технологиях, реализованных в системе ИВ, могут быть изменения, вызванные технологическими инновациями;

c) в a) 4) определить критерии оценки доверенности ИВ и принять во внимание:

1) такую архитектуру, при которой влияние аномалий в архитектурном объекте не распространяется на другие архитектурные сущности;

2) такую архитектуру, при которой архитектурные сущности могут поддерживать доверенность ИВ даже при подключении неопределенной сущности к целевой системе ИВ;

d) в b) 1) учесть уровни облачных, периферийных устройств и устройств ИВ;

e) в c) 1) рассмотреть доверенность ИВ в отношении интерфейсов и взаимодействия с внешними сущностями;

f) в c) 2) определить соответствующие архитектурные сущности, которые реализуют каждое требование доверенности ИВ с учетом аппаратных ресурсов и других ограничений. Требование может выполняться несколькими архитектурными сущностями в рамках всей системы ИВ;

g) в c) 3) выделить те, которые относятся к доверенности ИВ;

h) в d) 2) учесть сегментацию сети между элементами системы;

i) в e) оценить варианты архитектуры с точки зрения доверенности ИВ;

j) в f) 1) определить руководителя группы обеспечения доверенности ИВ для управления;

k) в f) 2) получить официальное согласование архитектуры руководителем группы обеспечения доверенности ИВ.

6.5.5 Процесс определения проекта

В дополнение к *ГОСТ Р 57193—2016, подпункт* 6.4.5.3, следует выполнить следующие действия:

a) в a) 2) определить необходимые факторы доверенности ИВ;

b) в a) 3) учесть пять факторов доверенности ИВ;

c) в a) 4) определить критерии оценки доверенности ИВ и принять во внимание:

1) проектирование таким образом, чтобы не только каждый элемент системы мог поддерживать доверенность ИВ, но и вся система могла поддерживать доверенность ИВ;

2) проектирование таким образом, чтобы влияние аномалий в элементе системы не распространялось на другие элементы системы;

3) проектирование таким образом, чтобы обеспечить согласованность между пятью факторами доверенности ИВ;

4) проектирование таким образом, чтобы системные элементы могли поддерживать доверенность ИВ даже при подключении неопределенных элементов к целевой системе ИВ;

5) проектирование таким образом, чтобы стабильные части и нестабильные части функций были разделены с учетом последовательных обновлений функций ИВ;

6) стратегия ведения журнала целевой системы ИВ, включая классификацию приоритета, период хранения для каждого классифицированного приоритета, время, передачу, разрешение на доступ и т. д.;

d) в b) 1) распределить системные требования по системным элементам в отношении доверенности ИВ (см. 6.5.3);

e) в c) 2) оценить каждый вариант для неразрабатываемых объектов и новую альтернативу проекта с точки зрения доверенности ИВ;

f) в d) 1) сопоставить пять факторов доверенности ИВ.

6.5.6 Процесс системного анализа

В дополнение к *ГОСТ Р 57193—2016, подпункт* 6.4.6.3, следует выполнить следующие действия:

a) в a) 1) определить проблему или вопрос, который требует системного анализа с точки зрения доверенности ИВ;

b) в a) 2) включить в перечень заинтересованных сторон группу обеспечения доверенности ИВ и группы по пяти факторам;

c) в a) 3):

1) включить анализ инцидентов, каждый из которых вызван нарушением одного или нескольких факторов доверенности ИВ;

2) включить анализ воздействия этих инцидентов на целевую систему ИВ и заинтересованные стороны;

3) получить официальное согласование руководителем группы обеспечения доверенности ИВ;

d) в a) 4):

1) включить корреляционный анализ событий и сравнительный анализ с информацией об инцидентах, полученной извне целевой системой ИВ, с определением уровня риска события по заданным критериям;

2) проанализировать намерения злоумышленников для инцидентов безопасности;

3) учесть возможное использование методов цифровой криминалистики для любого типа инцидента, включая не только инциденты защищенности;

e) в a) 5) определить период рассмотрения метода системного анализа;

f) в b) 3) рассмотреть результат анализа по вопросам, в которых факторы доверенности ИВ взаимосвязаны друг с другом;

g) в b) 5) классифицировать результаты системного анализа в соответствии с воздействием, соответствующим компонентом, вовлеченной заинтересованной стороной и т. д.

6.5.7 Процесс реализации

В дополнение к *ГОСТ Р 57193—2016, подпункт* 6.4.7.3, следует выполнить следующие действия:

a) в a) 1) рассмотреть применение технологий в зависимости от каждого уровня (облачное, периферийное устройство или устройство ИВ) целевой системы ИВ. Включить синхронизацию часов, используемых при ведении журнала;

b) в a) 2) учитывать ограниченные ресурсы устройств ИВ;

c) в b) 3) проверить, что целевая система ИВ соответствует системным требованиям, и зарегистрировать объективные доказательства в соответствии с важностью соответствующего системного требования.

6.5.8 Процесс комплексирования

В дополнение к *ГОСТ Р 57193—2016, подпункт* 6.4.8.3, следует выполнить следующие действия:

a) в a) 1) определить точки контроля корректности функционирования и целостности скомплексированных взаимодействий и отобранных функций системы для начальных настроек;

b) в a) 2) определить, когда и при каких условиях сегмент сети в целевой системе ИВ соединяется с другими сегментами сети.

6.5.9 Процесс верификации

В дополнение к *ГОСТ Р 57193—2016, подпункт* 6.4.9.3, следует выполнить следующие действия.

a) в a) 1) учесть:

1) максимальные значения величин, относящихся к целевой системе ИВ (максимальное количество подключенных устройств ИВ, максимальный объем данных, срок службы устройств ИВ, максимальное количество подключений устройств ИВ и т. д.);

2) варианты устройств и систем ИВ, подключаемых к целевой системе ИВ (интероперабельность функций и данных и т. д.);

3) варианты пользователей, поведения пользователей и пользовательских сред, связанных с целевой системой ИВ, с учетом демографических данных пользователей, защиты приватности пользователей и т. д.;

4) действия в отношении системных сбоев и исключительных событий в целевой системе ИВ (подключение неопределенных устройств ИВ, обработка непредусмотренных данных, сбои устройств или систем ИВ при подключении к целевой системе ИВ, коммуникационные сбои, использование целевой системы ИВ в течение длительного периода времени при исчерпании ресурсов, противоречивые запросы от нескольких внешних систем и т. д.);

5) меры защищенности без существенных побочных эффектов на другие факторы доверенности ИВ (обнаружение эксплуатации уязвимостей, подключение к системе с политикой защищенности, не согласованной с политикой защищенности целевой системы ИВ, влияние функций защищенности на

другие факторы, очистка/удаление данных и восстановление исходной конфигурации при необходимости при утилизации или передаче устройства/системы ИВ другому владельцу);

6) устойчивый режим работы в течение длительного периода времени (функции анализа отказов, функции обновления и т. д.);

b) в a) 2) учесть вышеприведенные пункты от 1) — 6) в a). Отразить результаты в требованиях, архитектуре или проектировании;

c) в a) 3) выбрать те методы верификации или методики, которые учитывают вышеприведенные пункты от 1) — 6) в a). Ввиду массовых событий верификации рассмотреть:

1) повышение эффективности;

2) реорганизацию и упорядочение верификации;

3) сокращение трудозатрат в человеко-часах;

4) облегчение рекурсивной и композиционной верификации;

d) в a) 4) рассмотреть проектирование среды верификации крупномасштабной системы и верификацию данных и эффективности;

Примечание — Принимаются во внимание следующие элементы:
- подключение различных типов устройств ИВ через доступные интерфейсы;
- обработка большого количества данных;
- обработка искаженных данных;
- обработка отказов и исключительных событий;
- обработка аномалий защищенности;
- сценарии верификации: 1) когда используется реальная система ИВ; 2) когда используется смоделированная система; 3) когда используется комбинация реальной системы ИВ и смоделированной системы;
- реорганизация и рационализация верификации;
- сокращение трудозатрат процессов верификации в человеко-часах;
- облегчение рекурсивной и композиционной верификации.

e) в a) 5) учесть:

1) функции верификации;

2) модульность архитектуры;

3) унификацию интерфейса, используемого для верификации, в частности для контроля и мониторинга;

f) в b) 1) включить процедуру верификации подключения к работающей реальной системе ИВ, если это необходимо;

g) в c) 2) зарегистрировать эксплуатационные инциденты и проблемы, включая доказательства и причину принятия такого решения.

Примечание — Если проблемы возникают после начала эксплуатации, может потребоваться объяснение заинтересованным сторонам. Следует регистрировать дополнительную информацию, в дополнение к успешному/неуспешному результату включая причину принятия такого решения в процессе верификации.

6.5.10 Процесс передачи

В дополнение к *ГОСТ Р 57193—2016, подпункт* 6.4.10.3, следует выполнить следующие действия:

a) в b) 2) проконтролировать начальные установки;

b) в b) 4) продемонстрировать корректные начальные настройки, в том числе:

1) физическую блокировку ненужных портов машин и устройств ИВ;

2) подключение к реальным системам ИВ, при необходимости;

c) в b) 5) информировать о:

1) необходимых действиях для подключения целевой системы ИВ к внешней сети;

2) изменении исходного идентификатора и пароля и необходимости надежности пароля;

3) необходимости обслуживания составных компонентов и состоянии обслуживания;

4) устаревании функций защищенности и необходимости новейшей версии программного обеспечения в качестве меры противодействия новым уязвимостям;

5) реакциях на сбои, проблемы и инциденты;

6) очистке/удалении данных и восстановлении исходной конфигурации, при необходимости, при утилизации или передаче устройства/системы ИВ другому владельцу;

d) в c) 3) поддержать прослеживаемость переданных системных элементов в зависимости от важности системных элементов в целевой системе ИВ.

6.5.11 Процесс валидации

В дополнение к *ГОСТ Р 57193—2016, подпункт* 6.4.11.3, следует выполнить следующие действия:

a) в пункте a) 1) определить область валидации и соответствующие действия валидации с точки зрения доверенности ИВ;

Примечание — Принимаются во внимание следующие элементы:

- функции, характерные для ИВ;
- приемлемые отличия производительности устройств ИВ от спецификации;
- вариации устройств и протоколов ИВ, используемых для связи с устройствами ИВ;
- число соединений;
- вариации типов данных и размеров данных;
- действия по последующему расширению;
- роли и поведение пользователей;
- пользовательские среды и местоположения;
- обратная связь о состоянии использования в соответствии с принципом приватности целевой системы ИВ и в соответствии с регуляторными положениями о приватности;
- сбои и проблемы устройств ИВ и их износ;
- меры противодействия угрозам и уязвимостям;
- реакции на снижение производительности и функциональные сбои при расширении системы;
- устранение проблем и обработка инцидентов с устройствами и сервисами ИВ, используемыми в целевой системе ИВ;
- функционирование системы мониторинга значимых событий, включая сбои и инциденты;
- замена и прекращение использования устройств и услуг ИВ, используемых в целевой системе ИВ.

b) в a) 2) определить ограничения с учетом пунктов в примечании к пункту a);

c) в a) 3) учесть:

1) использование сценария валидации;

2) использование инструмента стресс-тестирования, инструмента генерации квази-сбоев, инструмента фаззинга, симулятора устройства ИВ, симулятора сети и других инструментов для тестирования угроз и опасностей для проверки доверенности ИВ;

d) в a) 4) рассмотреть возможность валидации с использованием сценария валидации. Получить официальное согласование руководителем группы обеспечения доверенности ИВ после проверки группой;

e) в b) 1) при необходимости включить процедуру проверки подключения к работающей реальной системе ИВ;

f) в c) 2) записать эксплуатационные инциденты и проблемы, включая доказательства и причину принятия такого решения.

Примечание — Для подотчетности следует регистрировать дополнительную информацию, помимо к успешного/неуспешного результата включая отчет о действиях по валидации и журнал выполнения. Следует зарегистрировать доказательства однозначного соглашения заинтересованных сторон.

6.5.12 Процесс функционирования

В дополнение к *ГОСТ Р 57193—2016, подпункт* 6.4.12.3, следует выполнить следующие действия:

a) в a) 1) определить стратегию функционирования с учетом доверенности ИВ.

Примечание — Как правило, стратегия функционирования с учетом доверенности ИВ включает:

- сферу ответственности и сотрудничество с другими организациями, эксплуатирующими другие соответствующие системы;
- процедуры установки устройств и программного обеспечения ИВ с целью проверки их подлинности;
- процедуры обработки персональных данных в соответствии с принципом приватности целевой системы ИВ и в соответствии с регуляторными положениями о приватности;
- разделение функций для системных администраторов и для пользователей;
- соответствующие процедуры управления жизненным циклом для пользователей и других сущностей;
- контроль физического доступа, а также контроль логического доступа, включая удаленный доступ, с соответствующей политикой контроля доступа;
- подготовку и поддержку наиболее вероятного поведения целевой системы ИВ;
- запланированное резервное копирование и проверку соответствующих компонентов целевой системы ИВ;
- параметры ведения журнала и мониторинга, например указание источника/адресата специальных сущностей целевой системы ИВ, коммуникации с внешними сущностями и физический доступ к устройствам ИВ и другим, в соответствии с применимыми регуляторными правилами, директивами, промышленными стандартами и т. д.;

- процедуры обновления программного обеспечения;
- деятельность по мониторингу функций, включая приоритизацию аномалий и инцидентов;

b) в a) 5) включить обучение по:

1) подключению устройств ИВ;
2) регистрации пользователя и сопутствующих действий;
3) обращению с продуктами, поддержка которых прекращена;
4) удалению данных в соответствующие сроки;

c) в b) 3) обратить внимание на влияние обновления программного обеспечения. Пересмотреть процедуру обновления, если есть влияние на функционирование целевой системы ИВ или других соответствующих сущностей;

d) в b) 5) выполнять операции по реакции на непредвиденные обстоятельства в соответствии со стратегией функционирования;

e) в d) 1) предоставить информацию о системах ИВ, включая риски, в соответствии со стратегией управления информацией.

6.5.13 Процесс сопровождения

В дополнение к *ГОСТ Р 57193—2016, подпункт* 6.4.13.3, следует выполнить следующие действия:

a) в a) 1) определить стратегию сопровождения в соответствии с соглашением владельца целевой системы ИВ.

Примечание — Как правило, стратегия сопровождения с учетом доверенности ИВ включает:

- стратегию обслуживания с учетом важности каждого компонента целевой системы ИВ, воздействия таких событий, как аномалии и инциденты, и наиболее вероятного поведения системы при аномалиях и инцидентах с применимыми регуляторными правилами, директивами, промышленными стандартами и т. д.;
- объем ответственности и сотрудничества, особенно в отношении инцидентов, с организациями, поддерживающими другие системы;
- процедуры дистанционного обслуживания, включая разрешения от соответствующих организаций;
- процедуры обработки персональных данных в соответствии с принципом приватности целевой системы ИВ и в соответствии с регуляторными положениями о приватности;
- надлежащую проверку журналов, в частности журналов коммуникаций с внешними сущностями, и физического доступа к устройствам ИВ;
- реакции на сбои, проблемы и инциденты целевой системы ИВ (приостановка/деградация) и других систем (отключение сети);
- процедуры восстановления целевой системы ИВ в соответствии с политикой способности к восстановлению;
- плановые действия по профилактическому обслуживанию, такие как обновление криптографических ключей, проверка уязвимостей и обнаружение событий защищенности;
- компетенции по работе с инцидентами для поддержания доверенности целевой системы ИВ;

b) в a) 3) включить информацию о системах ИВ, включая риски, в соответствии со стратегией управления информацией;

c) в b) 5) включить меры противодействия новым уязвимостям и ухудшению функций защищенности. Учесть влияние обновления программного обеспечения. Пересмотреть процедуру обновления при наличии влияния на функционирование целевой системы ИВ или других соответствующих сущностей.

6.5.14 Процесс изъятия и списания

В дополнение к *ГОСТ Р 57193—2016, подпункт 6.4.14.3*, следует выполнить следующие действия:

a) в a) 1):

1) определить процедуры для удаления персональных данных в соответствии с принципами приватности целевой системы и соответствующими регуляторными правилами в отношении приватности;

2) сообщить пользователям целевой системы ИВ соответствующие элементы стратегии изъятия и списания.

Приложение А
(справочное)

Примеры рисков, характерных для систем ИВ

А.1 Общие положения

Согласно ГОСТ Р ИСО 31000 риск — это следствие влияния неопределенности на достижение поставленных целей. Риски доверенности ИВ состоят из рисков каждого фактора доверенности ИВ (защищенность, приватность, безотказность, способность к восстановлению и безопасность) и рисков, которые возникают из-за взаимной зависимости между пятью факторами.

А.2 Пример 1. Риск защищенности

Пример — Злоумышленники получили физический ключ от служебной дверцы банкомата и открыли корпус банкомата; сняли наличные деньги в банкомате путем использования мобильного телефона или заразив банкомат вирусом и т. д.

Спецификации банкоматов стали более стандартизированными, что упростило анализ модели одного производителя для атаки на банкомат другого производителя. Поскольку большинство банкоматов работают на ОС общего назначения, злоумышленники могут анализировать ОС, подготавливать специальные устройства для атаки на ОС и атаковать банкоматы, используя ОС. Подробнее см. [*1*].

А.3 Пример 2. Риск безотказности

Зафиксирован инцидент, когда дефект в файле шаблона антивирусного программного обеспечения привел к значительному снижению производительности ПК. Поскольку инцидент произошел в субботу, то промышленный ущерб был ограничен редакциями, транспортными компаниями и т. д., однако было сделано примерно 161 000 телефонных запросов от частных пользователей и 13 000 от корпоративных пользователей, из которых только около 4 000 звонков обработали в ближайшее время после инцидента. В системах ИВ к интернету подключаются не только ПК, но и автомобили, бытовые электроприборы и различные другие устройства и системы. Если они становятся недоступными все одновременно по какой-либо причине, как в приведенном выше случае, это оказывает значительное влияние на повседневную жизнь. При обновлении программного обеспечения следует не повлиять на доверенность, что позволит пользователям использовать системы в любое время. Подробнее см. *[3]*.

А.4 Пример 3. Риск безопасности

На масштабном мероприятии по информационной безопасности была проведена демонстрация бортового устройства движущегося автомобиля, к которому злоумышленники получили удаленный доступ и управляли двигателем и рулем. Уровень риска в данном случае является высоким, поскольку при управлении автомобилями дистанционно невидимыми злоумышленниками может быть причинен серьезный вред здоровью и жизни людей. После демонстрации было отозвано 1,4 млн автомобилей модели, используемой в демонстрации.

Основная причина вышеуказанной атаки заключается в том, что при разработке любого из составляющих элементов, включая мобильные сети, автомобильные устройства, автомобильные сети и службы отображения информации о транспортном средстве, недостаточно учтен риск. Это делает возможной серию атак, в ходе которых злоумышленники проникали из мобильных сетей, получали несанкционированный доступ к бортовым устройствам и изменяли прошивку чипов для отправки несанкционированных инструкций через автомобильные сети. Атаки должны быть остановлены внутри составных элементов системы транспортного средства.

Функции безопасности используемых компонентов могут быть неэффективными против преднамеренных атак, потому что при разработке компонентов не учитывалось подключение к интернету. В системах ИВ необходимо учитывать подключение к интернету и противостоять атакам через интернет на функции безопасности. Подробности см. в *[3]*.

А.5 Пример 4. Риск приватности

а) В умные автомобили интегрируют устройства ИВ с целью дополнительной функциональности для водителей и пассажиров. Такие устройства взаимодействуют друг с другом и с внешней частью автомобиля (другими автомобилями, внешними службами и т. д.). Задокументировано множество случаев атак на такие автомобильные системы. Злоумышленники могут отслеживать целевую автомобильную систему, изменять GPS-координаты, измерять ее скорость и ставить отметки на карте, чтобы проследить маршрут, в результате чего приватность человека, перемещающегося в машине, находится под угрозой. Другая проблема заключается в том, что датчики могут не проверять подписчика на информацию от датчиков, что приводит к обмену персональных данных с третьими лицами. Мобильная связь автомобильной системы может оказывать неблагоприятное воздействие на приватность, например, в случае удаленного отслеживания автомобиля неизвестными людьми. Также может осуществляться мошенничество путем клонирования ключа, при этом злоумышленник может неправомерно использовать личность пользователя или другую личность, используемую для связи с дорожной инфраструктурой, серверной частью производителя и т. д. Подробнее см. *[4]*.

b) Медицинские данные считаются приватными данными. Пациент может чувствовать себя уязвимым, если раскрываются персональные данные, такие как «у человека *p* есть определенное заболевание *d*». Разглашение персональных данных неблагоприятно влияет не только на пациента, но и на его семью и общество. С расширением удаленного мониторинга пациентов повышается риск утечки данных о состоянии здоровья от датчиков тела пациентов, попадающих в облачный сервер для доступа врачей. Должны быть приняты меры для защиты приватности пациента. Это может быть реализовано с помощью надлежащих методов управления доступом. Доступ к данным пациентов должен предоставляться по принципу «необходимости знать», и ни один пользователь не должен получать больше информации, чем ему нужно. Данные из беспроводной сети устройства мониторинга сначала передаются в локальное хранилище, которое, в свою очередь, подключается к облачному серверу. Необходимо принимать меры на каждом этапе, поскольку локальное хранилище, как правило, выступает в качестве точки сбора данных для более чем одного пациента. В облачном хранилище должны быть обеспечены аутентификация и авторизация пользователя. Подробности см. в [*5*] — [*7*].

А.6 Пример 5. Риск способности к восстановлению

Умные системы общественного транспорта используют множество интегрированных устройств ИВ. Эти устройства связываются друг с другом, а также с операторами и пользователями по целому ряду причин и предоставляют разнообразную информацию. Хотя система в целом устойчива к известным сбоям, вызванным конкретными причинами или их комбинациями, влияние каскадных причин или комбинаций причин на нескольких фронтах может быть фатальным. Например, масштабное отключение электричества, неблагоприятные погодные условия и отказ сети связи приведут к краху системы общественного транспорта, особенно при высокой зависимости от общественного транспорта. Подробнее см. *[8], [9]*.

А.7 Пример 6. Риск, возникающий из-за взаимосвязанных факторов доверенности ИВ

При атаке на украинскую сеть электроснабжения в 2015 году злоумышленниками была отключена телефонная линия, что способствовало увеличению времени компрометации сети. Поддержка только по телефону является ненадежной, и риск нарушения этой функции связан с увеличением риска инцидентов безопасности.

Риски также могут возникать из-за конфликтных ситуаций. Например, из соображений безопасности может потребоваться код аварийного доступа к оборудованию. Раскрытие этих кодов посторонним лицам может привести к нарушению безопасности. В то же время сохранение в секрете кодов по умолчанию или их изменение с помощью пароля может привести к ситуации, когда угроза безопасности не будет устранена вовремя.

Приложение В
(справочное)

Обзор процесса и его применение

В.1 Обзор процесса обеспечения доверенности ИВ

Перечисления a) — f) в 5.1 являются характеристиками систем ИВ, и в то же время они могут быть рассмотрены как проблемы, которые необходимо решить для обеспечения доверенности ИВ. В разделе В.1 представлен обзор процесса обеспечения доверенности ИВ путем решения a) — f) в 5.1 с точки зрения жизненного цикла системы и процессов.

На протяжении всего жизненного цикла необходимы организационные подходы для решения проблем доверенности ИВ. Следует разработать согласованные политики в отношении доверенности ИВ для решения вопросов a) — f) для обеспечения доверенности ИВ, в которой пять факторов взаимосвязаны друг с другом. Требуются сотрудники, занимающиеся вопросами доверенности ИВ, для реализации политик путем внедрения и поддержания доверенности ИВ. Требует рассмотрения также согласованность между пятью факторами доверенности ИВ. Поэтому в отношении всего жизненного цикла следует предпринимать следующие действия:

- базовый процесс 1): определить политику доверенности ИВ;
- базовый процесс 2): назначить персонал для обеспечения доверенности ИВ;
- базовый процесс 3): учесть согласованность между пятью факторами доверенности ИВ.

В системе ИВ много неопределенностей, для работы с которыми необходимо управление рисками. На первом этапе управления рисками необходимо определить активы и процессы, которые необходимо защитить в системе ИВ. Для реализации контроля элемента a) необходимо проанализировать, как риски в системе ИВ влияют на другие системы, подключенные к системе ИВ, и как риски в других системах, подключенных к системе ИВ, влияют на систему ИВ. Это снижает риски, связанные с перечислениями c), d) и f) в 5.1. Кроме того, во время работы могут изменяться среды и варианты использования системы ИВ, как указано в перечислениях b) и f) в 5.1. Изменения могут создать новые риски. Это означает, что для системы ИВ необходим новый анализ рисков. Следовательно, в управлении рисками необходимы следующие базовые процессы, характерные для систем ИВ:

- базовый процесс 4): определить активы и обработку системы ИВ;
- базовый процесс 5): учитывать риски, которые могут быть вызваны другими системами ИВ, подключенными к целевой системе ИВ;
- базовый процесс 6): учитывать риски системы ИВ, которые могут влиять на другие системы ИВ;
- базовый процесс 7): повторный анализ рисков в соответствующее время.

При проектировании требование доверенности ИВ должно быть закреплено за соответствующими системными элементами, поскольку любой системный элемент, такой как устройство ИВ с ограниченными ресурсами, как описано в e), не всегда может реализовать такое требование. Поскольку система ИВ может не знать в достаточной мере о подключенных системах/устройствах ИВ, как в перечислениях c), d) и f) в 5.1, влияние аномального состояния в системном элементе на соседние области должно быть минимизировано. Это также уменьшает явления, описанные в a) в 5.1. Система ИВ должна быть спроектирована таким образом, чтобы она могла поддерживать доверенность ИВ даже при подключении непредусмотренных элементов к системе ИВ аналогично f) в 5.1. Система также должна быть спроектирована так, чтобы поддерживать доверенность ИВ в течение очень долгого времени, поскольку срок службы систем ИВ очень велик по сравнению с другими типами систем согласно b) в 5.1. Это также может улучшить ситуацию, описанную в f) в 5.1;

- базовый процесс 8): определить соответствующие системные элементы, которые реализуют каждое требование доверенности ИВ с учетом аппаратных ресурсов и других ограничений;
- базовый процесс 9): проектировать систему ИВ таким образом, чтобы влияние аномалий в системном элементе не распространялось на другие системные элементы;
- базовый процесс 10): проектировать систему ИВ таким образом, чтобы системные элементы могли поддерживать доверенность ИВ даже при подключении к системе ИВ непредусмотренных элементов;
- базовый процесс 11): проектировать систему ИВ таким образом, чтобы поддерживать доверенность ИВ даже по прошествии времени;
- базовый процесс 12): проектировать систему ИВ таким образом, чтобы она создавала журналы для соответствующих событий.

При верификации и валидации доверенности ИВ следует учитывать широкий спектр устройств ИВ, подключенных систем ИВ и пользовательских сред. Это соответствует перечислениям a), c), e) и f) в 5.1. Поскольку для устранения последствий a) требуется стабильное функционирование системы ИВ, должны быть проверены немедленное обнаружение и восстановление после сбоев, проблем и инцидентов защищенности. b) также должен быть отражен в верификации и валидации;

- базовый процесс 13): учесть варианты устройств и систем ИВ, подключенных к системе ИВ, а также пользователей, поведения пользователей и пользовательской среды;

- базовый процесс 14): проверить обработку сбоев, проблем и инцидентов защищенности;
- базовый процесс 15): учесть стабильное функционирование в течение длительного периода времени.

Базовые процессы 13) — 15) применимы не только к верификации и валидации доверенности системы ИВ, но также к верификации и валидации системы ИВ в целом.

При эксплуатации и обслуживании могут случаться инциденты с доверенностью ИВ. В таких случаях необходимы быстрый анализ инцидента и быстрое восстановление, чтобы уменьшить влияние, как в a) в 5.1. Подготовка к ним проводится заранее, потому что непредвиденные события могут возникать часто, как в f) в 5.1. Перечисления a) и f) в 5.1 также требуют осведомленности заинтересованных сторон о доверенности ИВ, включая конечных пользователей, для контроля инцидентов. Это делается путем постоянного обмена информацией между заинтересованными сторонами. Поскольку владельцы систем/устройств ИВ могут меняться с течением времени, как в f), следует предпринять соответствующие действия, такие как удаление данных;

- базовый процесс 16): подготовиться к анализу и восстановлению после инцидентов, связанных с доверенностью ИВ;
- базовый процесс 17): обеспечить непрерывный обмен информацией между заинтересованными сторонами, включая конечных пользователей;
- базовый процесс 18): предпринимать соответствующие действия при смене владельцев систем/устройств ИВ.

В таблице B.1 показано соотношение между типичными характеристиками систем ИВ, перечисленными в разделе 5, и базовыми процессами для реализации и поддержания доверенности ИВ.

Таблица B.1 — Соотношение между характеристиками систем ИВ и базовыми процессами

Характеристика (перечисления в 5.1)	Весь жизненный цикл																	
				Управление рисками				Проектирование					Верификация и валидация			Эксплуатация и обслуживание		
	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12	B13	B14	B15	B16	B17	B18
a)	x	x		x	x	x			x				x	x		x	x	
b)	x	x		x			x				x	x			x			
c)	x	x		x	x	x			x				x					
d)	x	x			x	x			x									
e)	x	x						x					x					
f)	x	x		x	x	x	x		x	x	x	x	x			x	x	x
Сложность доверенности ИВ		x	x															
Примечание — B1, B2 и т. д. означают номер базового процесса.																		

B.2 Применение процесса для повышения доверенности ИВ

Процесс, определенный в настоящем стандарте, применяется к системе ИВ для повышения доверенности ИВ аналогично применению к системе *ГОСТ Р 57193*. В зависимости от модели разработки и других элементов всего жизненного цикла, применяемых к целевой системе ИВ, процессы выбираются путем применения процесса, описанного в настоящем стандарте, в дополнение к действиям и задачам для каждого выбранного процесса в жизненном цикле целевой системы ИВ.

Приложение ДА
(справочное)

Сведения о соответствии ссылочных национальных стандартов международным стандартам, использованным в качестве ссылочных в примененном международном стандарте

Таблица ДА.1

Обозначение ссылочного национального стандарта	Степень соответствия	Обозначение и наименование ссылочного международного стандарта
ГОСТ Р 57149—2016/ISO/IEC Guide 51:2014	IDT	ISO/IEC Guide 51:2014 «Аспекты безопасности. Руководящие указания по включению их в стандарты»
ГОСТ Р 57193—2016	NEQ	ISO/IEC/IEEE 15288:2015 «Системная и программная инженерия. Процессы жизненного цикла систем»
ГОСТ Р ИСО 31000—2019	IDT	ISO 31000:2018 «Менеджмент риска. Принципы и руководство»
ГОСТ Р ИСО/МЭК 27005—2010	IDT	ISO/IEC 27005:2008 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности»
ГОСТ Р ИСО/МЭК 27031—2012	IDT	ISO/IEC 27031:2011 «Информационная технология. Методы и средства обеспечения безопасности. Руководство по готовности информационно-коммуникационных технологий к обеспечению непрерывности бизнеса»

Примечание — В настоящей таблице использованы следующие условные обозначения степени соответствия стандартов:

- IDT — идентичные стандарты;
- NEQ — неэквивалентный стандарт.

Библиография

[1] Рекомендации по безопасности CCDS WG ATM SWG: Рекомендации по безопасности для категорий продуктов — Банкоматы — Практическое руководство по обзору мер безопасности — Анализ инцидентов с преступностью и разработка контрмер — Версия 1.00, 29 мая 2017 г. (CCDS Security Guidelines WG ATM SWG: Security Guidelines for Product Categories — Automated Teller Machines (ATMs) — Security Measures Review Practice Guide — Analyzing Crime Incidents and Formulating Countermeasures — Ver. 1.00, 2017/05/29)

[2] Ошибка в антивирусном программном обеспечении поражает локальные сети JR East, The Japan Times, 24 апреля 2005 г. (Bug in antivirus software hits LANs at JR East, The Japan Times, Apr 24, 2005)

[3] Кошмар взлома автомобилей, INFOSEC, 26 августа 2015 г. (The Nightmare of Car Hacking, INFOSEC, August 26, 2015)

[4] Хакеры удаленно уничтожили джип на шоссе — Со мной в нем, WIRED, 21 июля 2015 г. (Hackers Remotely Kill a Jeep on the Highway — With Me in It, WIRED, 21.07.2015)

[5] Майкл Брюммер: Диагностика рисков онлайн-здравоохранения (Michael Bruemmer: Diagnosing the Risks of Online Healthcare)

[6] Нандини Мукерджи, Сармишта Неоги, Самиран Чаттопадхьяй: Большие данные в электронном здравоохранении: проблемы и перспективы, Чепмен и Холл/CRC, 2 января 2019 г. (Nandini Mukherjee, Sarmistha Neogy, Samiran Chattopadhyay: Big Data in ehealthcare: Challenges and Perspectives, Chapman and Hall/CRC, 2 January 2019)

[7] Командный стазис: Дистанционное наблюдение за пациентами: все, что вам нужно знать, 4 декабря 2018 г. (Team Stasis: Remote Patient Monitoring: Everything You Need to Know, December 4, 2018)

[8] Агентство Европейского союза по сетевой и информационной безопасности: Кибербезопасность и устойчивость интеллектуального общественного транспорта, передовой опыт и рекомендации, декабрь 2015 г. (European Union Agency For Network And Information Security: Cyber Security and Resilience of Intelligent Public Transport, Good practices and recommendations, December 2015)

[9] Агентство Европейского союза по сетевой и информационной безопасности: Кибербезопасность и устойчивость интеллектуальных автомобилей, передовой опыт и рекомендации, декабрь 2016 г. (European Union Agency For Network And Information Security: Cyber Security and Resilience of smart cars, Good practices and recommendations, December 2016)

УДК 004.738:006.354

ОКС 35.020
35.110

Ключевые слова: информационные технологии, интернет вещей, доверенность

Редактор *Л.В. Коретникова*
Технический редактор *И.Е. Черепкова*
Корректор *Л.С. Лысенко*
Компьютерная верстка *Е.А. Кондрашовой*

Сдано в набор 29.11.2023. Подписано в печать 15.12.2023. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 2,79. Уч.-изд. л. 2,51.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

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