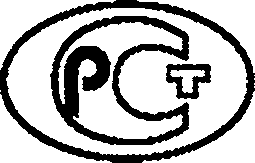
#### ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

**Н А Ц И О Н А Л Ь Н Ы Й С Т А Н Д А Р Т Р О С С И Й С К О Й**

Ф Е Д Е Р А Ц И И

**ГОСТР**

**МЭК 62280—**

**2017**

**ЖЕЛЕЗНЫЕ ДОРОГИ**

**Системы связи, сигнализации и обработки данных.**

**Требования к обеспечению безопасной передачи информации**

# (IEC 62280:2014, «Railway applications — Communication, signalling and processing systems —

**Safety related communication in transmission systems», IDT)**

#### Издание официальное

Стшдфттфцм

2M7

#### ГОСТ Р МЭК 62280—2017

**Предисловие**

1. ПОДГОТОВЛЕН Обществом с ограниченной ответственностью «Корпоративные электронные системы» на основе собственного перевода на русский язык англоязычной версии стандарта, указан\* ною в пункте 4
2. ВНЕСЕН Техническим комитетом по стандартизации ТК058 «Функциональная безопасность»
3. УТВЕРЖДЕН И 8ВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому ре\* гупироеанию и метрологии от 18 июля 2017 г. N9 716-ст
4. Настоящий стандарт идентичен международному стандарту МЭК 62280:2014 «Железные до\* роги. Системы связи, сигнализации и обработки данных. Коммуникации, связанные с безопасностью, в системах передачи» (IEC 62280:2014. «Railway applications — Communication, signalling and processing systems — Safety related communication in transmission systems». IDT).

Наименование настоящего стандарта изменено относительно наименования указанного между­ народного стандарта для приведения в соответствие с ГОСТ Р 1.5 (подраздел 6).

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

1. ВВЕДЕН 8ПЕРВЫЕ

*Правила применения настоящего стандарта установлены е статье 26 Федерального закона от 29 июня 2015 г.* № *162-ФЗ «О стандартизации в Российской Федерации». Информация* об из­ менениях *к настоящему стандарту публикуется в ежегодном (по состоянию на 1* января *текущего года) информационном указателе «Национальные стандартыр. а официальный текст изменений и поправок* — в *ежемесячном информационном указателе «Национальные стандартыр. В случае* пересмотра *(замены) или отмены настоящего стандарта соответствующее* уведомление *будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандартыр. Соответствующая информация,* уведомление *и тексты размещаются также в* ин­ формационной *системе общего пользования* — на *официальном сайте Федерального агентства по техническому регулированию и метрологии* в *сети Интернет (*[*www.gost.ru*](http://www.gost.ru/)*)*

© Стандартинформ. 2017

Настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и рас­ пространен в качестве официального издания без разрешения Федерального агентства по техническо­ му регулированию и метрологии

II

ГОСТ Р МЭК 62280—2017

**Содержание**

1. [Область применения. 1](#_bookmark0)
2. [Нормативные ссылки. 2](#_bookmark1)
3. [Термины, определения и сокращения. 2](#_bookmark2)
   1. [Термины и определения 2](#_TOC_250010)
   2. [Сокращения 5](#_TOC_250009)
4. [Эталонная архитектура. 6](#_bookmark3)
5. [Угрозы для системы передачи данных 7](#_bookmark4)
6. [Классификация систем передачи данных. 9](#_bookmark5)
   1. [Общие положения 9](#_TOC_250008)
   2. [Общие аспекты классификации 9](#_TOC_250007)
   3. [Критерии классификации систем передачи. 10](#_TOC_250006)
   4. [Системы передачи и угрозы 10](#_TOC_250005)
7. [Требования к защите. 11](#_bookmark6)
   1. [Общие положения 11](#_TOC_250004)
   2. [Общие требования. 11](#_TOC_250003)
   3. [Конкретные защиты 12](#_TOC_250002)
   4. [Применимость защит. 17](#_TOC_250001)

Приложение А (справочное) Угрозы в открытых системах передачи. 19

Приложение 8 (справочное) Категории систем передачи. 26

Приложение С (справочное) Руководство по применению средств защиты 28

Приложение О (справочное) Руководство по применению настоящего стандарта 40

Приложение Е (справочное) Связь с предыдущими стандартами. 44

Приложение ДА (справочное) Сведения о соответствии ссылочных международных стандартов

национальным стандартам Российской Федерации. 47

[Библиография. 48](#_TOC_250000)

ГОСТ Р МЭК 62280—2017

**Введение**

Если связанная с безопасностью электронная система включает передачу информации между различными компонентами оборудования системы, то система передачи является неотъемлемой частью системы, связанной с безопасностью, и это означает, что сквозная передача безопасна в соот­ ветствии с МЭК 62425.

Система передачи, рассматриваемая в настоящем стандарте, которая обеспечивает передачу ин­ формации между различными компонентами оборудования системы, в общем случае не должна удов­ летворять каким-либо особенным предварительным условиям. С точки зрения безопасности она может быть незащищенной или не полностью защищенной.

Настоящий стандарт рассматривает требования, которые должны быть учтены при передаче свя­ занной с безопасностью информации в таких системах передачи.

Несмотря на то. что вопросы безотказности, готовности и ремонтопригодности (RAM) в настоящем стандарте не рассматриваются, рекомендуется иметь в виду, что они — основной аспект глобальной безопасности.

Требования безопасности зависят от характеристик системы передачи. Чтобы уменьшить слож­ ность подхода при рассмотрении системы безопасности, системы передачи были разделены на следу­ ющие три категории.

Категория 1 состоит из систем, которые находятся под управлением разработчика и фиксированы в течение их срока службы.

Категория 2 состоит из систем, которые частично не известны или не фиксированы, однако не­ санкционированный доступ может быть исключен.

Категория 3 состоит из систем, которые не являются объектом управления разработчика и где не­

санкционированный доступ возможен.

Первая категория систем ранее была рассмотрена в МЭК 62280-1:2002, а остальные — в МЭК 62280-2:2002.

Если связанные с безопасностью коммуникационные системы, которые были реализованы в со­ ответствии с указанными выше стандартами, обслуживаются и/или расширяются, то может быть ис­ пользовано приложение Е для обеспечения согласованности (под)разделов настоящего стандарта с (под)разделами указанных выше стандартов.

IV

ГОСТ Р МЭК 62280—2017

Н А Ц И О Н А Л Ь Н Ы Й С Т А Н Д А Р Т Р О С С И Й С К О Й Ф Е Д Е Р А Ц И И

ЖЕЛЕЗНЫЕ ДОРОГИ

Системы связи, сигнализации и обработки данных.

Требования к обеспечению безопасной передачи информации

Rathvay applications. Communication, signalling and processing systems.

Safety communication requirements

Дата введения — 2019—07—01

# Область применения

#### Настоящий стандарт применим к связанным с безопасностью электронным системам, использую\* щим для цифровой связи системы передачи, которые не были специально разработаны для связанных с безопасностью.

Система передачи может быть подключена как к связанному, так и к не связанному с безопас­ ностью оборудованию.

Настоящий стандарт устанавливает основные требования, необходимые для обеспечения свя­

занной с безопасностью передачи данных между связанным с безопасностью оборудованием, соеди­ ненным системой передачи.

Настоящий стандарт применим при составлении спецификации требований безопасности свя­

занного с безопасностью оборудования, которое подключается посредством системы передачи, для достижения распределенных требований к полноте безопасности.

Требования безопасности, реализуемые в связанном с безопасностью оборудовании, обычно

разрабатываются в соответствии с МЭК 62425. В определенных случаях эти требования могут быть реализованы в другом оборудовании системы передачи, поскольку для реализации распределяемых требований к полноте безопасности выполняется управление мерами по обеспечению безопасности.

Спецификация требований безопасности является исходным документом для доказательства безопасности связанной с безопасностью электронной системы, для которой требуемое подтвержде­ ние безопасности определено в МЭК 62425. Подтверждение менеджмента безопасности и менеджмен­ та качества должно быть выполнено в соответствии с МЭК 62425. Настоящий стандарт рассматривает требования, связанные с передачей данных для подтверждения функциональной и технической без­ опасности.

Настоящий стандарт не определяет:

* + - систему передачи.
    - оборудование, подсоединенное к системе передачи.

- решения (например, для функциональной совместимости),

* + - а также какой вид данных связан с безопасностью, а какой не связан.

Оборудование, связанное с безопасностью, соединенное с помощью открытой системы передачи, может подвергаться многим различным угрозам, связанным с ИТ-безопасностью, для предотвращения которых должна быть определена общая программа, охватывающая вопросы менеджмента, а также технические и эксплуатационные вопросы.

Издание официальное

1

#### ГОСТ Р МЭК 62280—2017

Настоящий стандарт, однако, рассматривает некоторые вопросы безопасности ИТ-систем. но только преднамеренные атаки, реализуемые сообщениями к приложениям, связанным с безопасно\* стью.

Настоящий стандарт не охватывает общие проблемы безопасности ИТ-систем и. в частности, он не рассматривает проблемы безопасности ИТ-систем. связанные с:

\* обеспечением конфиденциальности информации, связанной с безопасностью,

* + - предотвращением перегрузки системы передачи.

# Нормативные ссылки

В настоящем стандарте используются нормативные ссылки на следующие целые документы или на их части, незаменимые для применения данного документа. 8 случае датированных ссылок дей­ ствует только цитируемое издание. Для недатированных ссылок действует самое позднее издание до­ кумента. на который производится ссылка (включая любые внесенные в него поправки).

IEC 62278 (all parts). Railway applications — Specification and demonstration of reliability, availability, maintainability and safety (RAMS) (Железные дороги. Технические условия и демонстрация надежности, эксплуатационной готовности, ремонтопригодности и безопасности (RAMS))

IEC 62425 Railway applications — Communication, signalling and processing systems — Safety related electronic systems for signaling (Железные дороги. Системы связи, сигнализации и обработки данных. Связанные с безопасностью электронные системы сигнализации)

# Термины, определения и сокращения

#### Термины и определения

В настоящем стандарте используются следующие термины и определения.

* + 1. абсолютная временная метка (absolute time stamp): Временная метка, связанная с гло­ бальным временем, которое является общим для группы объектов, использующих систему передачи.
    2. защита доступа (access protection): Процессы, разработанные для предотвращения несанк­

ционированного доступа при чтении или изменении информации либо в системах, связанных с без­ опасностью. либо в системе передачи.

* + 1. дополнительные данные (additional data): Данные, которые не используются в процессах

конечного пользователя, но используются для целей управления, готовности и безопасности.

* + 1. подлинное сообщение (authentic message): Сообщение, о котором известно, что содержа­ щаяся в нем информация сформирована в известном источнике.
    2. подлинность (authenticity): Свойство, характеризующее действительность информации и указывающее на то, что источник ее формирования известен.
    3. закрытая система передачи (closed transmission system): Связывающая фиксированное

количество или фиксированное максимальное количество участников система передачи с известными и фиксированными свойствами, в которой риск несанкционированного доступа считается незначитель­ ным.

* + 1. связь (communication): Передача информации между приложениями.
    2. конфиденциальность (confidentiality): Свойство, при котором информация недоступна или закрыта для неавторизованных лиц. субъектов или процессов.
    3. поврежденное сообщение (corrupted message): Сообщение, содержащее ошибки, из-за ко­ торого происходит повреждение данных.
    4. криптографические методы (cryptographic techniques): Метод вычисление выходных дан­

ных по некоторому алгоритму, используя входные данные и ключ в качестве параметра.

Примечание — Зная выходные данюе. невозможно в течение разумного времени вычислить входные данные без знания ключа. Также невозможно в течение разумного времени получить ключ из выходных данных, даже если входные данные известны.

#### циклическая избыточная проверка (cyclic redundancy check): Циклический процесс про­ верки. используемый для защиты сообщения от влияния повреждения данных.

* + 1. данные (data): Часть сообщения, которая представляет некоторую информацию.

2

#### ГОСТ Р МЭК 62280—2017

Прим еча нив — См. также определения 3.1.64 — пользовательские данные. 3.1.3 — дополнительные данные и 3.1.42 — избыточные данные.

#### повреждение данных (data corruption): Изменение данных.

* + 1. защита (defence): Мера, включенная в проект связанной с безопасностью системы связи, для противодействия определенным угрозам.
    2. задержанное сообщение (delayed message): Тип ошибки сообщения, при которой сообща

ние получено на один период позже, чем было предназначено.

* + 1. удаленное сообщение (deleted message): Тип ошибки сообщения, при которой сообщение удалено из потока сообщения.
    2. двойная временная метка (double time stamp): Случай, когда два объекта обмениваются и сравнивают свои временные метки. В этом случае временные метки в объектах независимы друг от Друга.
    3. ошибка (error): Отклонение от намеченного проекта, которое может привести к непредна- меренному поведению системы или отказу.
    4. отказ (failure): Отклонение от установленного функционирования системы.

Примечание —Отказ является следствием сбоя или ошибки в системе.

#### сбой (fault): Аварийное состояние, которое может привести к ошибке в системе.

Прим еча нив — Сбой мажет быть случайным или систематическим.

#### сообщение обратной связи (feedback message): Ответ от получателя к отправителю. че\* рез обратный канал.

* + 1. хакер (hacker): Лицо, пытающееся преднамеренно обойти защиту доступа.
    2. опасность (hazard): Условие, которое может привести к несчастному случаю.
    3. анализ опасности (hazard analysis): Процесс идентификации опасностей и анализа их при­ чин, а также формирование требований, ограничивающих вероятность и последствия опасностей до приемлемого уровня.
    4. неявные данные (implicit data): Дополнительные данные, которые не передаются, но из­ вестны отправителю и получателю.
    5. информация (information): Представление состояния или события процесса в форме «по\* мятной» процессу.
    6. вставленное сообщение (inserted message): Тип ошибки сообщения, при которой в поток сообщения вставляется дополнительное сообщение.
    7. целостность (integrity): Состояние, в котором информация полна и не изменяется.
    8. код обнаружения манипуляций (manipulation detection code): Функция от полного сообще­ ния без секретного ключа.

Прим еча ние — В отличие от кода аутентификации сообщений (MAC) в код обнаружения манипуляций (MDC) не включается никакой секретный ключ. Полное сообщение включает также любые неявные данные со­ общения. которые не отправляются в систему передачи. MDC часто основано на хеш-функции.

#### (подмененное) сообщение, выдающее себя за другое сообщение (masqueraded message): Тип вставленного сообщения, в котором создано недостоверное сообщение, которое кажет\* ся достоверным.

* + 1. сообщение (message): Информация, которая передана от отправителя (источника данных) к одному или более получателям (приемнику данных).
    2. код аутентификации сообщений (message authentication code): Криптографическая функ­ ция полного сообщения и секретного или открытого ключа.

Примечание — Полное сообщение включает также любые неявные данные сообщения, которые не от­ правляются в систему передачи.

#### шифрование сообщения (message enciphering): Преобразование битов в сообщении с помощью криптографического метода, в соответствии с алгоритмом, которым управляют ключи, чтобы существенно затруднить случайное чтение данных. Не обеспечивает защиту от повреждения данных.

* + 1. ошибки, связанные с сообщением (message errors): Набор всех возможных видов отка­ зов сообщения, которые могут привести к потенциально опасным ситуациям, или к сокращению готов­ ности системы. Каждый тип ошибки может иметь много причин.

3

#### ГОСТ Р МЭК 62280—2017

* + 1. целостность сообщения (message integrity): Сообщение, в котором информация полна и не изменяется.
    2. поток сообщений (message stream): Упорядоченное множество сообщений.
    3. не криптографический код защиты (non-cryptographic safety code): Избыточные данные на основе не криптографических функций, включенные в связанное с безопасностью сообщение и обе\* опочивающие обнаружение поврежденных данных с помощью связанной с безопасностью функции передачи.

3.1.3d открытая система передачи (open transmission system): Система передачи с неизвест­

ным числом участников, с неизвестными, переменными и не доверенными свойствами, используемая для неизвестных телекоммуникационных услуг и обладающая возможностью несанкционированного доступа.

* + 1. сеть общего пользования (public network): Сеть с неизвестными пользователями, в част­ ности. не находится под управлением железных дорог.
    2. случайный отказ (random failure): Отказ, который происходит в произвольный момент вре­

мени.

* + 1. проверка на избыточность (redundancy check): Тип проверки, которая выявляет наличие

предопределенной связи между избыточными данными и данными пользователя в сообщении, чтобы доказать целостность сообщения.

* + 1. избыточные данные (redundant data): Дополнительные данные, сформированные связан­

ной с безопасностью функцией передачи для данных пользователя.

* + 1. относительная метка времени (relative time stamp): Метка времени, на которую ссылают­ ся локальные часы объекта. В общем случае не существует никакой связи с часами других объектов.
    2. повторное сообщение (repeated message): Тил ошибки сообщения, при которой одно со­ общение получено несколько раз.
    3. переупорядоченное сообщение (re-sequenced message): Тип ошибки сообщения, при ко­ торой изменен порядок сообщений в потоке сообщений.
    4. безопасное состояние с пониженной скоростью передачи данных (safe faU back state): Безопасное состояние связанного с безопасностью оборудования или системы, близкое к безотказному состоянию, но им не являющееся, которое достигается в результате реакции системы безопасности, приводящей к снижению функциональности связанных с безопасностью функций, а также возможно не связанных с безопасностью функций.
    5. безопасность (safety): Отсутствие неприемлемых уровней риска.
    6. доказательство безопасности (safety case): Документированное подтверждение того, что изделие (например, систома'подсистсма/оборудование) соответствует заданным требованиям без­ опасности на этапах жизненного цикла.
    7. код защиты (safety code): Избыточные данные, включенные в связанное с безопасностью сообщение, обеспечивающие выявление поврежденных данных связанной с безопасностью функцией передачи.
    8. уровень полноты безопасности (safety integrity level): Число, которое указывает требу­ емую степень достоверности, что система будет выполнять свои заданные функции безопасности по отношению к систематическим отказам.
    9. реакция безопасности (safety reaction): Связанная с безопасностью защита, реализуемая процессом безопасности в ответ на событие (такое, как отказ системы передачи), которое может при­ вести к нарушению безопасного состояния оборудования.
    10. связанный с безопасностью (safety related): Отвечающий за безопасность.
    11. связанная с безопасностью функция передачи (safety related transmission function): Функция связанного с безопасностью оборудования, гарантирующая достоверность, целостность, акту­ альность и последовательность данных.
    12. порядковый номер (sequence number): Дополнительное поле данных, содержащее число, которое изменяется предопределенным способом от сообщения к сообщению.
    13. идентификатор источника и идентификатор адресата (source and destination identifier):

Идентификатор, который присваивается каждому объекту. Этот идентификатор может быть именем, числом или произвольной комбинацией двоичных символов. Этот идентификатор будет использовать­ ся для связанной с безопасностью передачи. Обычно идентификатор добавляется к данным пользова­ теля.

4

#### ГОСТ Р МЭК 62280—2017

* + 1. систематический отказ {systematic failure): Отказ, который неоднократно повторяется при некоторой определенной комбинации входов или для некоторых определенных состояний окружающей среды.
    2. угроза (threat): Потенциальное нарушение безопасности.
    3. временная метка (time stamp): Информация о времени передачи, присоединенная к со- общению отправителем.
    4. актуальность (timeliness): Состояние, в котором информация доступна в нужное время в

соответствии с требованиями.

* + 1. код передачи (transmission code): Дополнительная информация, которая добавляется к связанному и не связанному с безопасностью сообщению незащищенной системы передачи и гаранти­ рует целостность сообщения во время передачи.
    2. система передачи (transmission system): Служба, используемая приложением для пере- дачи потоков сообщений между несколькими участниками, которые могут быть источниками или при­ емниками информации.
    3. доверенный (trusted): Обладающий свойствами, которые используются в качестве доказа­ тельства при обеспечении демонстрации безопасности.
    4. несанкционированный доступ (unauthorised access): Ситуация, е которой к информации пользователя или к информации в системе передачи имеют доступ и/или ее изменяют лица, не наде­ ленные полномочиями, или хакеры.
    5. данные пользователя (user data): Данные, которые представляют состояния или события процесса пользователя без любых дополнительных данных. В случае передачи между связанным с безопасностью оборудованием данные пользователя содержат связанные с безопасностью данные.
    6. подтвержденное сообщение (valid message): Сообщения, форма которых во всех отноше­ ниях удовлетворяет заданным требованиям пользователя.
    7. достоверность (validity): Состояние, которое во всех отношениях удовлетворяет заданным

требованиям пользователя.

#### 3.2 Сокращения

**вен —** код Bose. Ray-Chaudhuri. Hocquenghem: ВМЕ — основные ошибки сообщений;

BSC — симметричный канал для передачи двоичных данных; CAN — локальная сеть контроллеров;

CRC — циклическая проверка чётности с избыточностью; ЕС — Европейское сообщество;

ЕСВ — метод прямого шифрования: EMI — электромагнитные помехи; РТА — анализ дерева отказов:

GPRS — система пакетной радиосвязи общего пользования;

GSM-R — глобальная система мобильной связи на железной дороге; НЕ — опасные события;

HW — аппаратные средства:

IT — информационные технологии; LAN — локальная вычислительная сеть; MAC — код аутентификации сообщений; MDC — код обнаружения манипуляций:

MD4. MD5 — алгоритмы представления сообщения в краткой форме; MH — основная опасность;

MTBF — средняя наработка на отказ (между отказами);

MVB — универсальная шина подвижного транспортного средства: PROFIBUS — высокоскоростная шина цифрового технологического оборудования;

5

ГОСТ Р МЭК 62280—2017

QSC — q-арный симметричный канал;

RAMS — безотказность, готовность, ремонтопригодность и безопасность; SIL — уровень полноты безопасности;

SR — связанный с безопасностью;

SRS — спецификации требований безопасности; SW — программное обеспечение;

ТХ — передача (данных);

UTC — всемирное координированное время. WAN — глобальная сеть передачи данных:

Wi-Fi — торговая марка для сетей на базе IEEE 802.11.

# Эталонная архитектура

Настоящий стандарт определяет требования безопасности для безопасной коммуникации между связанным с безопасностью оборудованием через систему передачи, которая может быть либо за» крытой, либо открытой. В обоих случаях к системе передачи может быть подсоединено как связанное с безопасностью, так и не связанное с безопасностью оборудование. Настоящий раздел описывает возможные конфигурации связанных с безопасностью коммуникаций е системах передачи, включая определение передаваемых функциональных блоков. Далее будут определены конкретные требова­ ния. которым должны удовлетворять эти блоки.

Общее представление (для открытой и закрытой системы передачи) основной архитектуры пока­ зано на рисунке 1. где все коммуникационные элементы соединены согласно информационному потоку обмена связанной с безопасностью информацией между связанным с безопасностью оборудованием. На рисунке 1 также показан не связанный с безопасностью интерфейс, который не всегда присутствует. Обычно он может быть использован для диагностических сообщений, направляемых в центр техобслу­ живания.

Помимо источника и пункта назначения связанной с безопасностью коммуникации эталонная ар­ хитектура представляет связанную с безопасностью систему коммуникации, которая может быть раз­ делена на;

* связанные с безопасностью функции передачи, выполняемые на связанном с безопасностью оборудовании. Эти функции гарантируют достоверность, целостность, актуальность и последователь­ ность данных,
* связанные с безопасностью криптографические методы, которые защищают связанное с без­ опасностью сообщение. Они могут быть реализованы или в связанном с безопасностью оборудовании, или вне этого оборудования, но должны быть проверены методами безопасности. Эти методы защища­ ют связанное с безопасностью сообщение в системе передачи Категории 3 и не используются в случае системы передачи Категорий 1 или 2.
  + - не связанные с безопасностью, открытые или закрытые системы передачи, которые могут сами включать в себя функции защиты передачи и/или функции защиты доступа.

Характеристики закрытых систем передачи (Категория 1) следующие:

* + - число элементов, подсоединенного оборудования (или связанных с безопасностью, или не свя­ занных) к системе передачи, известно и фиксировано;
    - риск несанкционированного доступа считается незначительным:
    - физические характеристики системы передачи (например, среды передачи, окружающая среда, предусмотренные в проекте, и т. д.) фиксированы и неизменны в течение жизненного цикла системы.

Открытая система передачи (Категория 2 и/или 3) может иметь некоторые или все следующие характеристики:

* элементы, которые читают, хранят, обрабатывают или ретранслируют данные, созданные и

представленные пользователями системы передачи в соответствии с программой, не известны пользо­ вателю. Число пользователей обычно также неизвестно, и с открытой системой передачи может быть соединено связанное и не связанное с безопасностью оборудование и оборудование, которое не свя­ зано с железнодорожными применениями;

6

#### ГОСТ Р МЭК 62280—2017

. среды передачи любого типа с характеристиками передачи и чувствительностью к внешним влияниям, которые неизвестны пользователю:

* + - системы управления сетью и системы менеджмента выполняют маршрутизацию (и динамиче­ ское изменение маршрута), обмениваются сообщениями по любому пути, сформированному в среде передачи одного типа или в средах передачи нескольких типов между концами открытой системы пере­ дачи в соответствии с программой, не известной пользователю;
    - другие пользователи системы передачи, не известные разработчику связанных с безопасностью приложений, отправляют неизвестный объем информации в неизвестных форматах.

Открытая система передачи Категории 3 может быть подвержена несанкционированному доступу со злонамеренными целями.

Эталонная архитектура не ограничивает реализации; возможны различные структуры, см. при­ меры в приложении Сив частности С.5 для не связанных с безопасностью сообщений.

# Угрозы для системы передачи данных

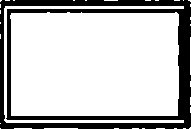
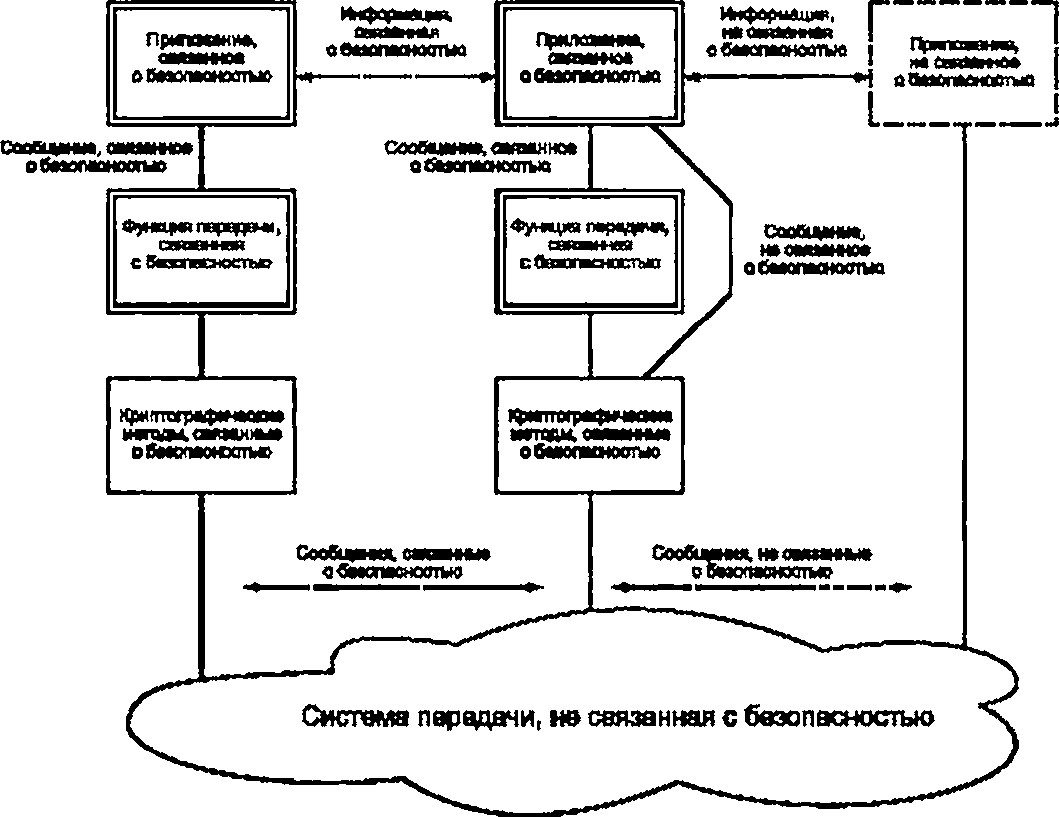
Основной опасностью для связанной с безопасностью коммуникации является отказ в получении подтвержденного сообщения, то есть иметь достоверное, целостное, последовательное и актуальное сообщение на стороне получателя. Настоящий стандарт рассматривает угрозы, возникающие в систе­ ме передачи, для этих свойств сообщения. Угрозы связанного с безопасностью оборудования необхо­ димо рассматривать в соответствии с МЭК 62425.

Однако соответствие требованиям настоящего стандарта не защищает от преднамеренного или непреднамеренного неправильного использования, возникающего из-за неавторизованных источников. При доказательстве безопасности необходимо рассматривать эти вопросы.

В приложение А включена дополнительная информация с руководящими указаниями по анализу угроз и доказательству безопасности. Однако необходимо подчеркнуть, что для каждого проекта дол­ жен быть выполнен анализ, так как. несмотря на то. что может быть использована методология анализа ошибок сообщения из приложения А. она сама по себе не обязательно является полной.

7

#### ГОСТ Р МЭК 62280—2017



~~ГЛ~~ОТНИ—1Р»0б^^ИММ. ~~«Ш~~1~~Щ~~С0вЮДДН0СТЦО,

РМйпкШМмкдля систем перво\*\* КатнгйрииЗ к

«сДпруда\*ео,~~б«М~~инсшаДюагоановгью.аооа~~'п~~0~~1'йт~~и~~1~~аМЭК8Я<М

иш

»рдП|1)7ГМ1т1»0>ПШ»ШОб«>СтбНОР1У10.ПрП>1рПШШ8ПС1«ОЦМО

#### МИад^<М~~Ш~~11»0С0С8>ВП1ОЮСВУ0»

**г** ^е^^вооевюк

I I -оДоруэто1и.м1ь»цшм\*сбиопидиостыо,ипи

I I -о~~В~~ои~~дя~~ин~~и~~.<жихноиебаюгаонэстыоСинтерфв~~йо«иод~~у♦»■мим».

#### I I ЩЦ~~1Ш~~И11—|.тжин»~~с1ст~~я1им\*сб»ктаснхп\*>,(рд»р»\*ь<1

I I • ежп\*егсшмеИЭК624ЭД.

Рисунок 1 — Эталонная архитектура для связанной с безопасностью передачи данных

8

#### ГОСТ Р МЭК 62280—2017

Опасные идентифицированные события могут включать:

* + - систематический отказ;
    - обрыв проводников:
    - ошибки кабельных соединений:
    - ошибка ориентирования антенны;
    - потеря производительности;
    - случайный отказ и старение аппаратных средств;
    - ошибка человека;
    - ошибка обслуживающего персонала:
* EMI;
  + - перекрестные помехи;
    - тепловой шум;
    - постепенное ухудшение свойств;
    - перегрузка системы передачи:
    - магнитная буря;
    - пожар;
    - землетрясение:
    - молния.

а также сознательно вызванные события такие как:

* + - перехватывание информации в проводных линиях:
    - повреждение или несанкционированное изменение аппаратных средств;
    - несанкционированное изменение программного обеспечения;
    - контроль каналов;
    - передача несанкционированных сообщений.

Однако, несмотря на то. что существует широкий спектр возможных опасных событий, основными ошибками сообщения, которые формируют угрозы для системы передачи, являются следующие:

* + - повторение;
    - стирание:
    - вставка:
    - переупорядочивание;
    - повреждение;

. задержка:

* + - подмена.

Таблица А.1 предлагает, какие угрозы для системы передачи могут быть вызваны каждым из этих типов опасных событий. Идентифицировав опасные события, не защищенные другими средствами и которые могут произойти для рассматриваемой системы, такая таблица может использоваться в ка­ честве руководства для идентификации угроз, которые должны быть рассмотрены для этой системы.

Таблица А.1 не содержит вероятности возникновения; это должно быть частью анализа угроз.

# Классификация систем передачи данных

#### Общие положения

Данный раздел определяет процесс, который будет использоваться для классификации всех си\* стем передачи, идентифицируя важные для таких систем угрозы, которые влияют на выбор защит для их использования в приложении, обеспечивающем безопасность.

#### Общие аспекты классификации

Существует много факторов, которые могут влиять на угрозы связанной с безопасностью комму\* никационной системе.

Например, возможно, что услуги передачи могут быть оказаны пользователю системы сигнализа­ ции от частных или общедоступных телекоммуникационных поставщиков услуг. В соответствии с таки­ ми контрактами по предоставлению услуг ответственность поставщика услуг за обеспечение гаранти­ рованной производительности системы передачи может быть ограничена.

9

ГОСТ Р МЭК 62280—2017

Поэтому значение угроз (и. следовательно, требования к защите от них) зависит от осуществляв\* мой пользователем степени управления системой передачи, включая следующие вопросы:

* технические свойства системы, включая гарантии надежности или доступности к системе, уро­ вень хранения данных, существующий в системе (который может влиять на задержку или переупоря- дочивание сообщений);
* стабильность производительности системы на всем времени ее эксплуатации (например, вслед­ ствие выполнения изменений в системе и изменений в базе данных пользователя), а также влияние за­ грузки трафика другими пользователями;
* доступ к системе в зависимости от того, частная ли сеть или общедоступная, предоставляемая оператору степень управления доступом для других пользователей, возможности для неправильного использования системы другими пользователями, а также возможный доступ специалистов по обслу­ живанию для реконфигурирования системы или получение доступа к самой среде передачи.

В соответствии с этими проблемами могут быть определены три категории систем передачи.

#### Критерии классификации систем передачи

* + 1. Критерии системы передачи Категории 1

Считается, что система передачи имеет Категорию 1. если выполнены следующие предваритель­ ные условия (ПУ).

ПУ1. Число единиц подсоединяемого оборудования (или связанного, или не связанного с безопас­ ностью) к системе передачи известно и фиксировано. Поскольку связанная с безопасностью коммуни­ кация зависит от этого параметра, то требование о максимальном количестве единиц оборудования, которое разрешено соединять вместе, будет включено в спецификацию требований безопасности в качестве предварительного условия. Конфигурация системы должна быть определена/включена в до­ казательство безопасности. Любому последующему изменению этой конфигурации должен предше­ ствовать анализ его влияния на доказательство безопасности.

ПУ2. Характеристики системы передачи (например, среды передачи, внешней среды с наихудши­ ми условиями и т. д.) известны и фиксированы. Они должны сохраняться во время жизненного цикла системы. Если должны быть изменены основные параметры, которые использовались в доказатель­ стве безопасности, то все связанные с безопасностью аспекты должны быть рассмотрены вновь.

ПУЗ. Риск несанкционированного доступа к системе передачи должен быть незначительным.

Если система передачи удовлетворяет всем вышеупомянутым предварительным условиям, то можно считать, что она имеет Категорию 1 и является закрытой системой, и поэтому она должна соот­ ветствовать обычно сокращенному набору процессов и требований, представленных в разделе 7.

* + 1. Критерии системы передачи Категории 2

Если система передачи не удовлетворяет ПУ1 или ПУ2 из 6.3.1, но удовлетворяет ПУЗ. то можно считать, что она имеет Категорию 2 и является открытой системой, поэтому ее необходимо оценивать более обширным набором процессов и требований, представленных в разделе 7.

* + 1. Критерии системы передачи Категории 3

Если система передачи не удовлетворяет ПУЗ из 6.3.1. то можно считать, что она имеет Катего­ рию 3 и является открытой системой, поэтому ее необходимо оценивать полным набором процессов и требований, представленных в разделе 7.

#### Системы передачи и угрозы

Значение угроз для связанной с безопасностью коммуникационной системы должно быть оценено в соответствии с возможностями управления системой передачи, которое осуществляет пользователь.

Угрозы, определенные в разделе 5. применимы ко всем категориям систем передачи, за исключе­

нием подмены, которая применима только к открытой системе передачи.

В таблице В.1. приложение В. представлен пример классификации систем передачи данных, а в таблице В.2 дан пример отношения угроэа/категория.

Применимость раздела 7 зависит от категории системы передачи.

10

#### ГОСТ Р МЭК 62280—2017

# Требования к защите

#### Общие положения

Ранее для систем передачи данных (связанных и не связанных с безопасностью) были пред\* ложены определенные методы защиты от угроз. Эти методы представляют «библиотеку» возможных методов, которые доступны для разработчика систем управления и защиты и используются для обе­ спечения защиты от каждой из перечисленных выше угроз.

Для снижения риска, связанного с перечисленными в предыдущем разделе угрозами, в открытых и закрытых системах передачи, необходимо рассмотреть и довести до уровня, требующегося для при­ менения. следующие фундаментальные службы безопасности, обеспечивающие:

* + - достоверность сообщения;
    - целостность сообщения;
    - своевременность сообщения;
    - последовательность сообщений.

Был выделен следующий набор известных методов защиты:

1. порядковый номер:
2. временная метка;
3. тайм-аут;
4. идентификаторы источника и пункта назначения;
5. сообщение обратной связи; 0 процедура идентификации; д) код защиты:

h) криптографические методы.

*Ряд* проблем архитектуры должен быть рассмотрен для конкретного применения и подтвержден в доказательстве безопасности, например:

* условия для утверждения о соответствии и поддержания соответствия системы передачи Кате­ гории 1 или 2 предварительным условиям;
  + - критерии разделения систем передачи различных категорий между собой;
* устойчивость систем передачи к отказу в обслуживании, возникающего в результате информа­ ционных атак. например, необходимость использования брандмауэров.

В отношении перечисления h) следует отметить, что область применения настоящего стандарта

не включает общие проблемы безопасности ИТ-систем:

* + - рассматриваются атаки только во время стадии эксплуатации;
    - в настоящем стандарте рассматриваются только атаки, выполняемые сообщениями, на связан­ ные с безопасностью приложения.

Однако политика обеспечения защиты полного доступа должна учесть:

* + - процедуры и вопросы обслуживания защиты доступа:
    - что уязвимость программного обеспечения не рассматривается для связанного с безопасностью приложения;
    - конфиденциальность информации.

#### Общие требования

* + 1. Должны быть обеспечены соответствующие средства защиты от всех определенных выше угроз безопасности для систем, использующих открытую или закрытую систему передачи. Любые пред­ положения угроз, которые игнорируются, должны быть обоснованы и зарегистрированы в доказатель­ стве безопасности. В приложении А представлен возможный список угроз, который можно использовать в качестве руководства.
    2. Если реализуется коммуникация между приложениями, связанными с безопасностью, и при­ ложениями. не связанными с безопасностью, через одну и ту же систему передачи данных, то приме­ няют следующие требования:
* для защит безопасности, реализуемых связанными с безопасностью функциями передачи, должно быть продемонстрировано, что они являются функционально независимыми от защит, реали­ зуемых не связанными с безопасностью функциями;
  + - связанные и не связанные с безопасностью сообщения должны иметь разные структуры, так как в связанных с безопасностью сообщениях применяется код защиты. Этот код защиты должен быть

11

#### ГОСТ Р МЭК 62280—2017

способен защитить систему до требуемой полноты безопасности (см. 7.3.8). так что не связанные с без\* опасностью сообщения не могут быть повреждены в связанных с безопасностью сообщениях.

* + 1. Подробные требования для защит, необходимых для приложения, должны учитывать:

. уровень риска (частота/последствие), определенный для каждой определенной угрозы, и

. уровень полноты безопасности соответствующих данных и процесса.

В приложении С представлены указания по выбору известных в настоящее время методов защи­ ты от угроз. При выборе защиты необходимо тщательно проанализировать вопросы эффективности, рассмотренные в этом приложении.

* + 1. Требования к необходимым защитам должны быть включены в спецификацию требований к системе и в спецификацию требований безопасности системы для определенного приложения и долж­ ны сформировать исходную информацию для раздела «Обеспечение правильной работы» доказатель­ ства безопасности для этого приложения.
    2. Все защиты должны быть реализованы согласно требованиям, определенным в МЭК 62425. Это подразумевает, что защиты:
    - будут реализованы полностью в связанном с безопасностью оборудовании передачи (с возмож­

ным исключением некоторой криптографической архитектуры, см. 7.3.9 и С.2);

* будут функционально независимы от уровней, используемых в незащищенной системе пере­ дачи данных.
  + 1. В последующих подразделах даны обязательные требования для конкретных защит. Они

применяются, если эта конкретная защита используется.

* + 1. Кроме описанных в настоящем стандарте, могут использоваться другие защиты, при усло­ вии. что анализ их эффективности противостоять угрозам включен в доказательство безопасности.
    2. Доказательство функциональной и технической безопасности должно выполняться в соот­ ветствии с процедурой, определенной в МЭК 62425. включая:
    - создание полной модели ошибки:
    - формирование функциональной спецификации на основе анализа полной модели ошибки:
* анализ каждой защиты, используемой в связанной с безопасностью коммуникации:
  + - формирование реакции системы безопасности в случае обнаруженной ошибки коммуникации:
* спецификация требований к полноте безопасности и распределение значений уровня полноты безопасности.
  + 1. Подраздел 7.3 определяет исчерпывающий набор защит. Однако, для систем передачи Кате­ гории 1 достаточен следующий сокращенный набор, по-прежнему поддерживающий фундаментальные службы безопасности:
* идентификаторы источника и/или адресата (в случае больше, чем одного отправителя, и/или больше, чем одного получателя);
* порядковый номер и/или временные метки в объеме, необходимом приложению; и
* код защиты.

#### Конкретные защиты

* + 1. Общие положения

Следующие пункты содержат краткое введение и требования для конкретных защит, которые яв­ ляются эффективными при их отдельном применении или в комбинации, от одиночных или объединен­ ных угроз. Должны быть применены все общие упомянутые выше требования.

Более подробные описания защит и отношения со всеми возможными угрозами даны в справоч­ ном приложении С.

* + 1. Порядковый номер
       1. Общие положения

Нумерация сообщений заключается в добавлении очередного номера (названного порядковым номером) к каждому сообщению, которыми обмениваются отправитель и получатель. Это позволяет получателю проверять последовательность сообщений, обеспеченных отправителем.

* + - 1. Требования

Доказательство безопасности должно демонстрировать соответствие процесса определенному уровню полноты безопасности и природу связанного с безопасностью процесса, учитывая:

* + - длину порядкового номера:

12

#### ГОСТ Р МЭК 62280—2017

* + - условие для инициализации и преобразования порядкового номера:
    - условие восстановления после прерывания последовательности сообщений.
    1. Временная метка
       1. Общие положения

Когда объект получает информацию, значение информации часто связано со временем. Степень зависимости между информацией и временем может различаться между приложениями. В некоторых случаях старая информация может быть бесполезной и безопасной, а е других случаях информация может быть потенциально опасной для пользователя. 8 зависимости от поведения процессов во ере- мени. в которых происходит обмен информацией (циклический, событийный и т. д.) может отличаться и решение.

Одно решение, которое охватывает отношения информация-время, состоит в том. чтобы добав­ лять временные метки к информации. Такой вид информации может использоваться вместо или вместе с порядковыми номерами в зависимости от требований приложения. Различное использование меток времени и их свойств показано в С. 1. приложение С.

* + - 1. Требования

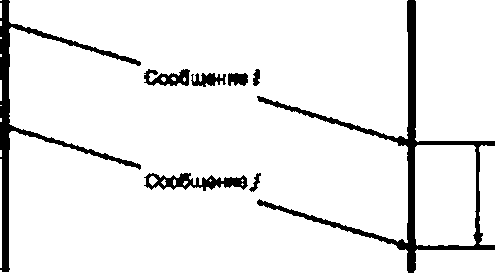
Доказательство безопасности должно демонстрировать соответствие процесса определенному уровню полноты безопасности и природу связанного с безопасностью процесса, учитывая:

* + - значение приращения времени:
    - точность приращения времени;
    - размер таймера;
    - абсолютное значение таймера (например. UTC или любые другие глобальные часы);
* синхронизацию таймеров в различных объектах;

. задержку между возникновением информации и добавлением метки времени к ней;

* + - задержку между проверкой метки времени и использованием информации.
    1. Тайм-аут
       1. Общие положения

При передаче (обычно циклической) получатель может проверить, превышает ли задержка между двумя сообщениями предопределенное разрешенное максимальное время (см. рисунок 2). Если это происходит, то предполагается ошибка.

Оттфиито ГфИИКННК

<■0

*t< Ttrmx*

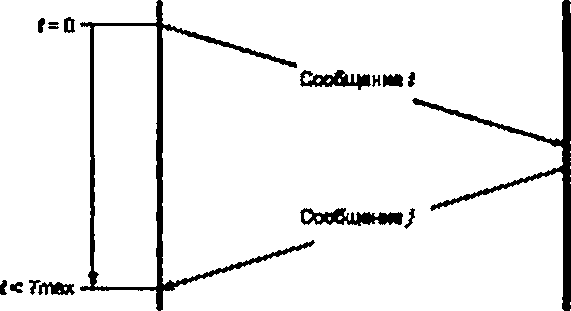
Рисунок 2 — Циклическая передача сообщений

#### Если обратный канал доступен, то отправителем может быть выполнен контроль. Отправитель запускает таймер, посылая сообщение /. Приемник сообщения / отвечает сообщением подтверждения

). связанным с полученным сообщением *i.* Если отправитель не получает сообщение подтверждения *j* в течение предопределенного времени, то предполагается ошибка (см. рисунок 3).

13

ГОСТ Р МЭК 62280—2017

ОПфЫИТШЪ Гфшмнж

#### Требования

Рисунок 3 — Двунаправленная передача сообщений

#### Доказательство безопасности должно демонстрировать соответствие процесса определенному уровню полноты безопасности и природу связанного с безопасностью процесса, учитывая:

* + - приемлемую задержку:
* точность тайм-аута.
  + 1. Идентификаторы источника и адресата
       1. Общие положения

Для многоабонентных коммуникационных процессов нужны соответствующие средства для про­ верки источника всей полученной информации, прежде чем она будет использоваться. Чтобы это обе­ спечить. сообщения должны включать дополнительные данные.

Сообщения могут содержать уникальный идентификатор источника, или уникальный идентифи­ катор адресата, или оба вместе. Выбор делается согласно связанному с безопасностью приложению. Эти идентификаторы добавляются в связанные с безопасностью функции передачи приложения.

* + - Включение в сообщения идентификатора источника может позволить пользователям сообще­ ний проверить, что сообщения из намеченного источника, без какого либо диалога между получателем и отправителем. Это может быть полезно, например, в однонаправленных или широковещательных передачах.
* Включение в сообщения идентификатора адресата может позволить пользователям сообще­ ний проверить, что сообщения предназначены для них без какого либо диалога между получателем и отправителем. Это может быть полезно, например, в однонаправленных или широковещательных передачах. Идентификаторы адресата могут быть выбраны, чтобы идентифицировать отдельные ме­ ста назначения или группы пользователей.
  + - 1. Требования

Доказательство безопасности должно демонстрировать соответствие процесса определенному уровню полноты безопасности и природу связанного с безопасностью процесса, учитывая:

* уникальность идентификаторов для объектов во всей системе передачи:
* размер поля данных идентификатора.
  + 1. Сообщение обратной связи
       1. Общие положения

Если доступен надлежащий обратный канал передачи, то сообщение обратной связи может быть отправлено от получателя критической для безопасности информации к отправителю. Содержание это­ го сообщения обратной связи может включать:

* данные, полученные из содержания исходного сообщения в идентичной или видоизмененной форме;
* данные, добавленные получателем, полученным из его собственной локальной информации.
  + - дополнительные данные для целей безопасности или защиты.

Использование такого сообщения обратной связи может способствовать безопасности процесса множеством различных способов:

14

#### ГОСТ Р МЭК 62280—2017

* + - обеспечивая успешное подтверждение приема достоверных и полученных вовремя сообщений;
    - обеспечивая успешное подтверждение приема поврежденных сообщений, чтобы позволить принять соответствующие меры;
    - подтверждая идентификационные данные оборудования получения;
    - упрощая синхронизацию часов в оборудовании отправки и получения;
    - упрощая динамические процедуры проверки между сторонами.
      1. Требования

Существование обратного какала само по себе не обеспечивает защиту от какой-либо опреде­ ленной угрозы. Он является механизмом поддержки для других защит на прикладном уровне. Поэтому кет никаких определенных требований безопасности для такого канала обратной связи.

* + 1. Процедура идентификации
       1. Общие положения

Предыдущий пункт касался требований для объектов, которые будут идентифицированы.

Открытые системы передачи могут дополнительно увеличивать риск сообщениями от других (не­ известных) пользователей, перепутанных с информацией, выходящей из предназначенного источника (форма подмены).

Специально разработанная процедура идентификации в связанном с безопасностью процессе может обеспечить защиту от этой угрозы.

Различают два типа процедур идентификации.

*Двунаправленная идентификация*

Если доступен обратный канал передачи, то обмен идентификаторами объекта между отправи­ телями и получателями информации может обеспечить дополнительную гарантию, что передача дей­ ствительно выполняется между предназначенными сторонами.

*Процедуры динамической идентификации*

Динамический обмен информацией между отправителями и получателями, включая преобразо­ вание и обратную связь полученной информации к отправителю, может обеспечить гарантию, что свя­ зывающиеся стороны не только «заявляют», что обладали корректными идентификационными данны­ ми. но также и «ведут себя» ожидаемым образом. Этот тип процедуры динамической идентификации может использоваться, чтобы обеспечить предисловием передачу информации между связанными с безопасностью процессами коммуникации и/или это может использоваться во время самой передачи информации.

* + - 1. Требования

Процедура идентификации является частью связанного с безопасностью прикладного процесса.

Подробные требования должны быть определены в спецификации требований безопасности.

* + 1. Код защиты
       1. Общие положения

в системах передачи, как правило, коды передачи используются для обнаружения случайных ошибок, и/или ошибок в линии передачи пакетных данных, и/или для улучшения качества передачи ме­ тодами коррекции ошибок. Даже при том. что эти коды передачи могут быть очень эффективными, они могут перестать работать из-за отказов аппаратных средств, внешних влияний или систематических ошибок.

Связанный с безопасностью процесс не должен доверять таким кодам передачи с точки зрения безопасности. Поэтому для обнаружения повреждения сообщения дополнительно требуются коды за­ щиты. которые находятся под управлением связанного с безопасностью процесса.

Доказательство безопасности должно демонстрировать соответствие процесса определенному уровню полноты безопасности и природу связанного с безопасностью процесса, учитывая;

* + - способность обнаружения повреждений сообщений, связанных с предполагаемыми системати­ ческими отказами;
* вероятность обнаружения случайных отказов в поврежденных сообщениях.

Прим еча нив — Код защиты может быть комбинацией различных кодов, например, линейного кода, объ­ единенного с постоянным значением.

#### Указания по выбору кодов защиты даны в С.З. приложение С.

* + - 1. Требования
         1. Код защиты должен отличаться от кода передачи, если целостность сообщения не будет обеспечена исключительно кодом защиты. Это различие может быть получено:

15

ГОСТ Р МЭК 62280—2017

* + - или с помощью различных алгоритмов, или
    - с помощью различных параметров конфигурации (например, полиномов) для тех же алгорит- мое. Если оба кода будут основываться на CRC. то полиномы должны различаться. Если у обоих по» линомов будут общие множители, то их вкладом в эффективность кода защиты нужно пренебречь при анализе безопасности.

В случае закрытой системы передачи разработчик может просто выбрать код защиты, который отличается от кода передачи, потому что у него есть полное представление о системе передачи. В случае открытой системы передачи это требование может быть выполнено применением кода защиты, который не используется коммерческими системами передачи.

* + - * 1. Код защиты должен обнаруживать.
    - ошибки передачи, например, вызванные EMI;
    - систематические ошибки, вызванные отказами аппаратных средств в незащищенной системе передачи.

Отказы, которые будут имитировать код защиты, не могут быть надлежащим образом обнару­ жены. Поэтому код защиты должны быть более сложными, чем ожидаемые отказы. Следовательно, можно предположить, что отказ аппаратных средств в незащищенной системе передачи не может гене­ рировать достоверный код защиты.

* + - * 1. Чтобы удовлетворить требуемому значению полноты безопасности, необходимо, чтобы код защиты был достаточно сложным, например, на основе CRC. чтобы обнаруживать и обрабатывать типичные отказы и ошибки. Анализ, по крайней мере, должен включать:
    - разрывы в линии передачи;
    - все биты логического 0;
    - все биты логической 1;
* инверсию сообщения;
  + - ошибка синхронизации (в случае последовательной передачи):
    - случайные ошибки;
* пакетные ошибки.
  + - систематические ошибки, например, повторяющиеся шаблоны ошибок;
* комбинации упомянутых выше отказов и ошибок.
  + - * 1. Вероятностный анализ эффективности кода защиты должен отвечать требованиям цели безопасности. Должна быть обеспечена модель видов отказа, а также все предположения, сделанные для вычислений, должны быть проверены и согласованы.

Вероятность необнаруженных ошибок линейных кодов часто вычисляется при помощи модели двоичного симметричного канала (BSC) (см. С.4. приложение С). В случае если используется недвоич­ ный код. то может более подойти q-несимметричный канал (QSC). Настоящий стандарт рекомендует ограничить эту вероятность значением наихудшего случая, вычисленным по этим моделям.

BSC хорошо подходит для случайных ошибок, вызванных EMI. Но простые случайные ошибки

обычно устраняются незащищенной системой передачи. Поэтому, если ошибка обнаружена кодом за­ щиты. то обычно в связанном с безопасностью сообщении нарушается много битов. Поскольку для таких случаев никакие простые модели не доступны, то настоящий стандарт не рекомендует работать с более низкими значениями вероятностей необнаруженных ошибок, чем поделенное пополам значение наихудшего случая, полученное применением BSC для интенсивности битовых ошибок (см. С.4, при­ ложение С).

Пример упрощенной модели для закрытой системы передачи представлен в С.4. приложение С.

* + 1. Криптографические методы
       1. Общие положения

Криптографические методы могут использоваться, если вредоносные атаки в открытой сети связи не могут быть исключены.

Обычно это происходит, если связанная с безопасностью коммуникация использует:

* + - общедоступную сеть.
    - систему радиопередачи.
* систему передачи, подсоединенную к общедоступным сетям.

Против преднамеренных атак, выполняемых сообщениями, на связанные с безопасностью при­ ложения сообщения, связанные с безопасностью, должны быть защищены криптографическими мето­ дами.

16

#### ГОСТ Р МЭК 62280—2017

Это требование, нацеленное на предотвращение подмены сообщений от неавторизованных зло­ умышленников. может быть удовлетворено одним из следующих решений:

1. использование кода защиты в состоянии обеспечить криптографическую защиту;
2. шифрование сообщений после формирования кода защиты;
3. добавление криптографического кода к коду защиты.

Эти методы могут быть объединены с механизмом кодирования безопасности или выполняться отдельно. В приложении С представлены некоторые возможные решения.

Криптографические методы подразумевают использование ключей и алгоритмов. Степень эф­ фективности этих методов зависит от эффективности алгоритмов и обеспечения секретности ключей. Секретность ключа зависит от его длины и управления им.

* + - 1. Требования

Доказательство безопасности должно демонстрировать соответствие процесса определенному уровню полноты безопасности и природу связанного с безопасностью процесса, учитывая:

* + - технический выбор криптографических методов, включающий:
      * исполнение криптографического алгоритма (например, симметричный или асимметричный).
* характеристики ключа (например, фиксированный или сеансовый).
* обоснование выбранной длины ключа.
* частоту обновления ключа.
  + - * физическое хранение ключей:
    - технический выбор архитектуры шифрования, включающий:

- проверку правильного функционирования (до и во время эксплуатации) шифровальных про­ цессов. когда они реализованы не в связанном с безопасностью оборудовании;

* + - управленческую деятельность, включающую:
      * формирование, хранение, распределение и аннулирование конфиденциальных ключей.
      * управление оборудованием.
      * процесс рассмотрения соответствия методов шифрования с рисками злонамеренных атак.

Криптографический алгоритм должен быть применен ко всем данным пользователя, а также к

дополнительным данным, которые не передаются, но известны отправителю и получателю (неявные данные).

Должны быть описаны обоснованные предположения о природе, мотивации, финансовых и тех­ нических средствах потенциального субъекта атаки, учитывая также обстоятельства (как технические: увеличение мощности компьютеров, уменьшение стоимости быстрых процессоров, распространение знаний об алгоритмах, так и «социальные»: экономические конфликты, распространение вандализма, и т. д.), которые можно ожидать в процессе жизненного цикла системы.

Для управления ключами настоятельно рекомендуется использовать стандартизированные мето­ ды (например, согласно серии ИСО/МЭК 11770).

#### Применимость защит

* + 1. Общие положения

Защиты, кратко рассмотренные в 7.3. могут быть связаны с набором возможных угроз, определен­ ных в разделе 5. Каждая защита может обеспечить защиту от одной или более угроз при передаче со­ общений. В доказательстве безопасности должно быть продемонстрировано, что существует, по край­ ней мере, одна соответствующая защита или комбинация защит для каждой определенной возможной угрозы.

* + 1. Матрица угроз/эащит

1. таблице 1 *X* указывают, что данное средство может обеспечить защиту против соответствующей угрозы. В соответствии с 7.2.7 средства защиты в таблице 1 могут быть расширены.

17

ГОСТ Р МЭК 62280—2017

Таблица 1 — Матрица угроз и средств защиты

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Угрозы | Средства зашит» | | | | | | | |
| Поряд­ ковый номер | времен-  н о й метка | Тайм-аут | Идеити\* фикаторы источника и адресата | Сообще­ ние обратной связи | Процеду­ ра иденти- фмхаиии | Код защиты | Крнптотра- фические методы |
| Повторение | X | X |  |  |  |  |  |  |
| Стирание | X |  |  |  |  |  |  |  |
| Вставка | X |  |  | х°> | X1» | X\*» |  |  |
| Переупорядо- чивание | X | X |  |  |  |  |  |  |
| Повреждение |  |  |  |  |  |  | Xе) | X |
| Задержка |  | X | X |  |  |  |  |  |
| Подмена |  |  |  |  | X1» | х») |  | Xе\* |

а> Применимо только для исходного идентификатора. Обнаруживает вставку только из недопустимого источника. Если уникальные идентификаторы не могут быть определены из-за неизвестных пользователей, то должен использоваться криптографический метод, см. 7.3.9.

ь> Зависит от приложения.

с) См. 7.4.3 и С.2. приложение С.

#### Выбор и использование кода защиты и криптографических методов

Выбор кода защиты и криптографических методов должен быть определен согласно следующему:

* + - может ли несанкционированный доступ быть исключен;
    - предлагаемый тип криптографического кода;
    - отделен ли связанный с безопасностью процесс защиты доступа от связанного с безопасностью процесса.

Указания по этим проблемам даны в С.2. приложение С.

18

#### ГОСТ Р МЭК 62280—2017

Приложение А (справочное)

#### Угрозы в открытых системах передачи

А.1 Представление системы

Угрозы сообщениям, отправленным по каналу системой управления и системой защиты, происходят в ре­ зультате возможных изменений в работе канала, которые могут возникнуть либо при нормальных условиях (напри­ мер в отсутствии отказов), либо в условиях аварии (например после отказов системы передачи).

Для выделения ряда угроз был принят подход, основанный на разделении анализа риска, представленного е форме дерева (см. рисунок А.1). на три отдельных уровня:

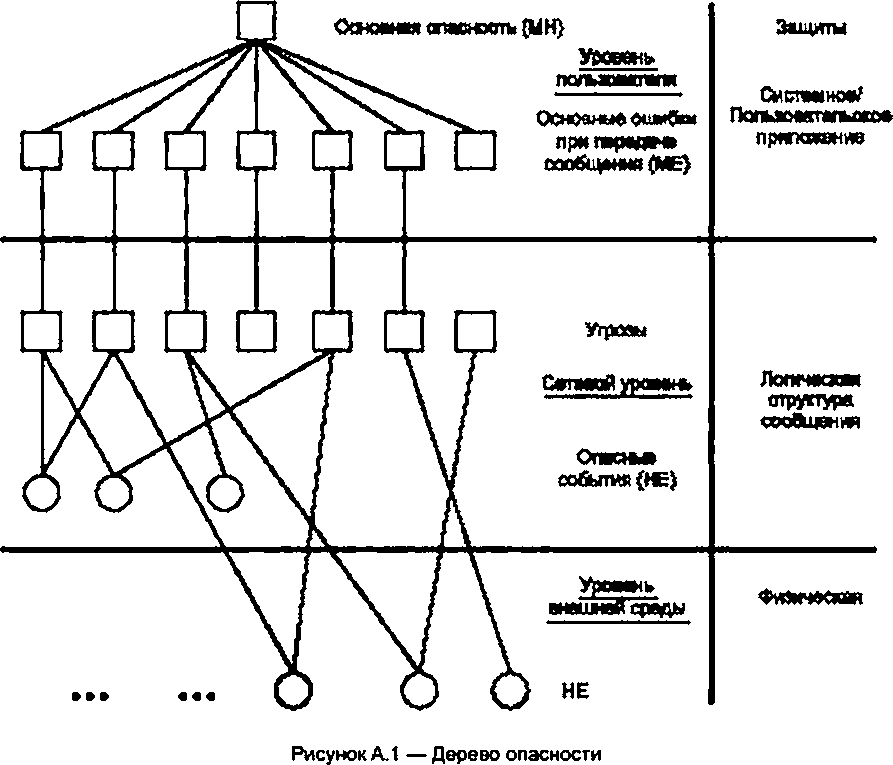
* + - уровень пользователя;
    - сетевой уровень;
    - уровень внешней среды.

Эти уровни следуют сверху вниз, начиная с основной опасности (МН). которая является отказом в получении лодтвереденного сообщения в терминах аутентификации, целостности, последовательности и своевременности на стороне получения.

С помощью анализа возможных поведений сообщения, наблюдаемых на стороне получения, были выде­ лены потенциально опасные ситуации (основные опасности) и был рассмотрен ряд основных ошибок сообщения (ВМЕ). предназначенных для классификации всех возможных видов отказа сообщения.

Установление соответствующих угроз, рассматриваемых как виды отказа сети (т. е. основных ошибок со­ общения с точки зрения сети), выполняется просто. Угроза — эта сущность, которая создает опасную ситуацию для безопасности (т. е. может привести к несчастному случаю), и поэтому является причиной (на сетевом уровне) возможной основной ошибки сообщения. Спвдовагегъно. отношение основная угроза — ошибка сообщения имеет вид 1:1.

В свою очередь, угроза может быть сгенерирована рядом причин, названных опасными событиями (НЕ), которые могут присутствовать и в сети, и на уровне внешней среды. Очевидно, что одно и то же опасное событие может быть связано с различными угрозами.



#### 19

ГОСТ Р МЭК 62280—2017

Разделение выполнения анализа на разных уровнях также обеспечивает возможность использования (по крайней мере) трех уровней защит.

a) одна защита на уровне прикладной системы/польэовзтеля. которая выполняется при реализации системы независимо от среды передачи, например удаление, которое может быть неопасно, если система была разработа­ на так. чтобы удаленные сообщения не представляли опасность:

b) одна защита, связанная с логической структурой сообщения, например все возможные ходы, которые мо­ гут быть применены к сообщению или конкретные контрмеры, такие как порядковые номера, метки времени и т. д.;

c) одна защита на физическом уровне, например экранирование, чтобы избежать повреждения из-за элек­ тромагнитных помех.

Настоящее приложение не будет рассматривать далее эту тему, которая была упомянута только с целью предоставления общей картины принятой методологии.

А.2 Установление основных ошибок при передаче сообщений

Сообщение — основной предмет всего анализа, поэтому процесс передачи данных был изучен с точки зре­ ния получателя. Сообщение может быть определено как «полезная информация, порожденная источником, кото­ рая доставляется за время д( от начала передачи».

Целостность потока сообщений — основной фактор, который необходимо учитывать при идентификации опасностей, которые могут произойти при передаче связанного с безопасностью сообщения в открытой системе передачи.

«Поток сообщений» определен как упорядоченное множество сообщений, являющееся уникальным для каж­ дого временного окне и получателя в сети при отсутствии каких либо отказов, атак или некорректных операций.

Реально полученный поток сообщений может отличаться от ожидаемого по ряду причин. Определены три их подкласса (основных опасностей}:

* получено больше сообщений, чем ожидалось:
* получено меньше сообщений, чем ожидалось:
  + - количество полученных и ожидаемых сообщений одинаково.

*Получено больше* сообщении, чем ожидалось

В этом случав одно или бопве сообщений были получены повторно, или внешнее сообщение было вставле­ но в канал передачи. Поэтому основные ошибки сообщения — повторные и вставленные сообщения.

*Получено меньше сообщений,* чем *ожидалось*

В этом случае одно или бопве сообщений было удалено. Поэтому основные ошибки сообщения — удален­ ные сообщения

Го же самое количество полученных *и ожидаемых сообщений*

В этом случае существует несколько возможностей:

* все сообщения в потоке правильны по содержанию и по времени передачи, но неверна последователь­ ность передачи — произошло первупорядочивание:
  + - сообщение в потоке достигло получателя за время больше, чем номинальное значение *£J* — произошла задержка:
    - сообщение было изменено — произошло повреждение сообщения:
    - получатель полагает, что отправитель сообщения отличается от истинного отправителя — произошла под­

мена.

В последних двух случаях должна быть рассмотрена целостность этого одиночного сообщения. Основными

ошибками при передаче сообщений являются: переупорядоченные, задержанные, поврежденные и подмененные сообщения.

Поэтому был определен следующий набор основных ошибок при передаче сообщений:

* + - повторное сообщение:
* удаленное сообщение:
  + - вставленное сообщение:
* переупорядоченное сообщение:
  + - поврежденное сообщение:
* задержанное сообщение;
  + - подмененное сообщение.

Определенные выше основные ошибки при передаче сообщения не являются взаимоисключающими. Воз­ можно. что большое количество сообщений в потоке и даже одиночное сообщение оказываются под воздействием более чем одного вида ошибки.

А.З Угрозы

А.3.1 Общие положения

Если основные ошибки при передаче сообщения определены, как е А.2, то происхождение соответствующих угроз становится понятным.

Пусть А В и С будут тремя уполномоченными сторонами, которые передают связанные с безопасностью со­ общения. в то время как X предпринимает атаку.

20

#### ГОСТ Р МЭК 62280—2017

Необходимо отметить, что случайные и систематические отказы аппаратных средств или программного обе­ спечения тахже учтены в списке угроз. Последующие объяснения являются только примерами и поэтому не будут исчерпывающими.

А.3.2 Повторение

* *X* копирует сообщение «Максимальная скорость: 250 км/ч\* и воспроизводит его в неподходящей ситуации (в то время, копа поезд движется с низкой скоростью] или
  + - вследствие отказа аппаратных средств небезопасная система передачи повторяет старое сообщение. А.3.3 Удаление
* *X* удаляет сообщение *[X* удаляет сообщение «Аварийная остановка» или «Максимальная скоростъ:250 км/ч»] или
* сообщение удалено из-за отказа аппаратных средств. А.3.4 Вставка
* *X* вставляет сообщение [Максимальная скорость: 250 км/ч] или
* уполномоченная третья сторона С непреднамеренно вставляет сообщение в информационный поток от А к В {или то же происходит из-за ошибки в сети).

А.3.5 Переулорядочивание

* X преднамеренно изменяет последовательность сообщений для В (например, задерживая сообщение или вынуждая сообщение реализовать другой путь по сети) или
* последовательность сообщений изменяется из-за отказа аппаратных средств. А.3.6 Повреждение
  + - Сообщение случайно изменяется (например, вследствие EMI) и превращается в другое формально кор­ ректное сообщение или
* *X* изменяет сообщение [«Максимальная скорость: 30 км/ч» на «Максимальная скорость: 250 км/ч»] правдо­ подобным способом так. чтобы А и/игы В не смогли обнаружить изменение.

А.3.7 Задержка

* Система передачи перегружена нормальным трафиком (например, из-за неправильного проекта или слу­ чайно большого трафика) или
* *X* создает перегрузку в системе передачи, генерируя поддельные сообщения так. чтобы этот сервис вы­ полнялся с задержкой или был остановлен.

А.3.8 Подмена

* + - А и В обмениваются связанными с безопасностью данными, а
* *X* при передаче сообщений от А к В или от В к А (или в обоих направлениях) позволяет себе получить до­ ступ к связанным с безопасностью данным или рассматривать себя легальным пользователем системы.

А.4 Возможный подход к построению доказательства безопасности А.4.1 Общие положения

Подход, который будет кратко представлен ниже, является примером, но не является единственным, которо­ му можно следовать. Для полного анализа опасности приложения необходимо глубокое знание этого приложения, чтобы выполнить для него надлежащую оценку риска.

А.4.2 Структурированные методы идентификации опасных событий А.4.2.1 Общие положения

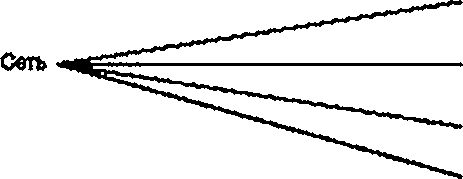
Анализ начинается с рассмотрения того, что исследуемый случай имеет дело с сетью (Network), взаимодей­ ствующей с внешней средой (External environment). Эти два объекта структурированы на подобъекты (на рисунке А.2 подчеркнуты), которые можно рассматривать как причины возможных опасных событий в анализируемой си­ стеме. Объект Network декомпозирован согласно нескольким шагам его жизненного цикла, е то время как объект External environment делится на две группы возможных характеристик, которые связаны с физическими процесса­ ми и с человеком.

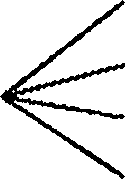
Листья дерева на рисунке А.2 представляют причины опасностей: для каждой причины определены соответ­ ствующие сгенерированные опасные события. Если вероятность отдельной причины определена, то такой способ также упрощает выделение вероятности для каждого опасного произошедшего события.

Ниже каждая причина разделяется на несколько возможных опасных событий. Это разделение не исчер­ пывающее: во время анализа опасности некоторые другие опасные события могут быть учтены в зависимости от конкретного приложения.

21

#### ГОСТ Р МЭК 62280—2017



Фишчюеа

Внмдняйорада

Работы парад мором в даАствма Работы аоарсаю ввода *в* яайсгете

Эыцуищ\* w ctoyo—ш ВЫэадизэишлуатацвгясписи»~~»~~

**1кжтрс)ижтхитот Нахи ~~и~~ мао«** *тср/мм*

*Кпшшг*

Бетесгвежыв событии

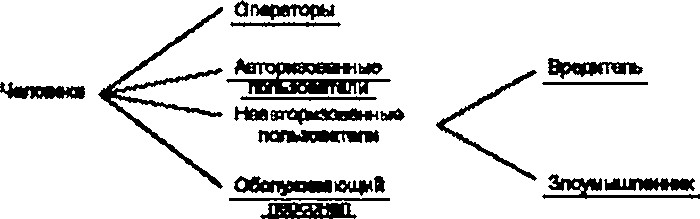


Рисунок А.2 — Причины угроз

А.4.2.2 Сеть

А.4.2.2.1 Общие положения

Стадии жизненного цикла сети могут быть определены согласно МЭК 62278. Для области применения на­ стоящего приложения (т. е. для идентификации опасных событий, являющихся результатом «ошибок» на каждой стадии), они могут группироваться следующим образом:

* + - разработка концепции, определение системы и условий применения, анализ рисков, системные требо­ вания. распределение системных требований, разработка и реализация, изготовление. Все эти стадии связаны с работами до ввода в эксплуатацию системы:
    - установка, подтверждение соответствия системы и принятие системы. Эти стадии связаны с вводом в действие системы:
* эксплуатация и обслуживание:
  + - вывод из эксплуатации и списание. А.4.2.2.2 Работы до ввода в действие

Ошибки во время данной стадии могут привести к:

* систематическим отказам аппаратных средств:
  + - систематическим отказам программного обеспечения. А 4.2.2.3 Работы во время ввода в действие

Ошибки во время данной стадии могут привести к:

* перекрестным помехам:
  + - повреждениям проводов:
* ошибке ориентирования антенны:
  + - ошибкам в кабельных соединениях. А.4.2.2.4 Эксплуатация и обслуживание

Во время данной стадии жизненного цикла опасные события могут возникнуть и из-за ухудшения эксплуата­ ционных характеристик компонентов системы и из-за ошибок во время ремонта и/или модификаций:

* + - ухудшение эксплуатационных характеристик:
* случайный отказ аппаратных средств:
  + - старение аппаратных средств.

22

#### ГОСТ Р МЭК 62280—2017

А.4.2.2.5 Обслуживание

* + - использование некалиброванных инструментов:
    - испогъзование неподходящих инструментов:
    - некорректная замена аппаратных средств;
    - некорректное обновление или замена программного обеспечения. А.4.2.2.6 Модификация

. эффекты замирания:

* + - ошибки человека\*\*.

А.4,2.2.7 Вывод из эксплуатации и списание

* + - Не предусматривается, что опасные события, связанные с ошибками связи, могут возникнуть во время данной стадии жизненного цикла сети.

А.4.2.3 Внешняя среда

А.4.2.3.1 Электромагнитные поля

* + - EMI.
    - перекрестные помехи (с внешними кабельными соединениями или линиями радиосвязи). А.4.2.3.2 Механические нагрузки
    - случайные отказы аппаратных средств:
    - старение аппаратных средств.

А.4.2.3.3 Климат

* + - термический шум;
    - старение аппаратных средств:
    - случайные отказы аппаратных средств:
    - эффекты замирания.

А.4.2.3.4 Природные явления

* + - магнитная буря;
    - пожар;
    - землетрясение:
    - молния.

А.4.2.3.5 Операторы

* + - ошибки человека\*).

А.4.2.3.6 Авторизованные пользователи

* + - ошибки человека\*);
    - перегрузка системы передачи.

А.4.2.3.7 Обслуживающий технический персонал

* + - испогъзование некалиброванных инструментальных средств:
    - использование неподходящих инструментагъных средств;
    - замена некорректно работающих аппаратных средств:
    - ошибки человека\*);
    - модификация или замена некорректно работающего программного обеспечения. А.4.2.3.8 Вредитель\* 2)
    - тайное прослушивание телефонных разговоров;
    - повреждение или останов, или изменение аппаратных средств:
    - несанкционированные изменения программного обеспечения. А.4.2.3.9 Злоумышленник2)
    - контроль каналов;
    - передача несанкционированных сообщений. А.4.2.4 Отношение опасные события — угрозы

В соответствии с разделом А.1 каждую угрозу может рассматривать как набор опасных событий, которые ее генерируют. Начиная с опасных событий, определенных в предыдущем разделе, следующим шагом явля­ ется построение отношений между ними и угрозами, кратко рассмотренными в А.З. используя восходящий ме­ тод3). Цель состоит в том. чтобы проверить, что никакая дополнительная угроза не обнаружена, чго доказывает правомерность используемого подхода. Отношение «угрозы — опасные события» может быть представлено таблицей А.1.

1>Они зависят от конкретного типа применения и поэтому не могут быть определены на этом уровне анализа (здесь и далее).

2) Вредитель и злоумышленник являются хакерами, но их действия различны. Вредителя не беспокоит то. что он подключен к линии связи, его целью является только нарушение работы сети. А злоумышленник не наруша­ ет работу сети, он использует ее. чтобы получить некоторое преимущество (здесь и далее).

3\* Вообще говоря, во время анализа доказательства безопасности такой восходящий метод должен использоваться для оценки угроз, вызванных всеми опасными событиями, связанными с конкретным применением.

#### 23

ГОСТ Р МЭК 62280—2017

Как видно, никакая дополнительная угроза не была обнаружена после анализа каждого опасного события.

Это доказывает, что список в разделе А.Э является исчерпывающим.

(Необходимо отметить, что данная таблица для каждого опасного события рассматривает только его основ­ ное влияние, поэтому могут быть определены и другие отношения.}

А.5 Резюме

Были определены два различных подхода для получения набора возможных угроз для связанных с безопас­ ностью коммуникаций в системах передачи. Первый — нисходящий метод, начинающийся с основной опасности и заканчивающийся классификацией всех возможных опасных событий, приводящих к опасности. Второй — начина­ ется с определения двух основных объекте» рассматриваемой системы (т. е. сеть и внешняя среда), чтобы класси­ фицировать все возможные причины опасных событий, связанных с этой системой; эти события затем связывают с угрозой (угрозами), которую они генерируют.

Эти два исследования приводят к одному и тому же набору утроз. поэтому оба подхода могут использоваться для анализа опасностей в открытых системах передачи.

Табл ица А.1 — Связь между опасными событиями и угрозами

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Опасные события | Угрозы | | | | | | |
| Повторе\* нис | Уде пе­ нно | вставка | Переупоря­ дочи ванне | Поврежде­ ние | Задержка | Подмена |
| Систематические отказы аппаратных средств | X | X | X | X | X | X |  |
| Систематические отказы программного обеспечения | X | X | X | X | X | X |  |
| Перекрестные помехи |  | X | X |  | X |  |  |
| Повреждения проводов |  | X |  |  | X | X |  |
| Ошибка ориентирования антенны |  | X |  |  | X |  |  |
| Ошибки в кабельных соединениях |  | X | X | X | X | X |  |
| Случайные отказы аппаратных средств | X | X | X | X | X | X |  |
| Старение аппаратных средств | X | X | X | X | X | X |  |
| Использование не калибро­ ванных инструментов | X | X | X | X | X | X |  |
| Использование неподходящих инструментов | X | X | X | X | X |  |  |
| Некорректная замена аппаратных средств | X | X | X | X | X | X |  |
| Эффекты замирания |  | X |  | X | X | X |  |
| EMI |  | X |  |  | X |  |  |
| Ошибки человека |  | X | X | X | X | X |  |
| Термический шум |  | X |  |  | X |  |  |
| Магнитная буря |  | X |  |  | X | X |  |
| Пожар |  | X |  |  | X | X |  |
| Землетрясение |  | X |  |  | X | X |  |
| Молния |  | X |  |  | X | X |  |
| Перегрузка системы передачи |  | X |  |  |  | X |  |

24

#### ГОСТ Р МЭК 62280—2017

*Окончание таблицы А. 1*

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Опасные события | Угрозы | | | | | | |
| Повторе\* нив | Удало\* кие | Вставка | Переупоря- дочиммие | Поврежде­ ние | Задержка | Подмена |
| Тайное прослушивание телефонных разговоре» | X | X | X |  | X | X |  |
| Повреждение или останов аппаратных средств |  | X |  |  |  | X |  |
| Несанкционированные изменения программного обеспечения | X | X | X |  | X | X | Ха| |
| Передача несанкционирован­ ных сообщений | X |  | X |  |  |  | X"» |
| Контроль каналов0’ |  |  |  |  |  |  |  |

В этом случав сообщение является злонамеренным с самого начала: поэтому необходима серьезная защита, например использование ключа.

Несанкционированный контроль связанных с безопасностью сообщений не считается непосредственно опасным событием: опасности для безопасности системы возникают из-за «передачи несанкционированных сообщений», появляющиеся в результате несанкционированного контроля. Конфиденциальность данных приложения — отдельное системное требование и не входит в область применения настоящего стандарта.

#### 25

ГОСТ Р МЭК 62280—2017

Приложение В (справочное)

#### Категории систем передачи

В.1 Категории систем передачи

В б.З определено три категории систем передачи.

Категория 1. Закрытые системы передачи, е которых все основные свойства системы находятся под управле­ нием разработчика связанной с безопасностью системы и может быть определен упрощенный набор требований безопасности.

Категория 2. Открытые системы передачи, в которых, несмотря на то. что передача не полностью находится под управлением разработчика связанной с безопасностью системы, риск злонамеренной атаки, можно считать незначительным.

Категория 3. Открытые системы передачи, в которых существует возможность вредоносной атаки и для кото­ рых требуются криптографические меры защиты.

В таблице В.1 представлены некоторые дополнительные указания о том. как реальные системы передачи, которые могут использоваться в связанных с безопасностью применениях, могут быть отнесены к указанным выше трем категориям, на основе характеристик используемых ими технологий и основных характеристик их конфигу­ раций.

Невозможно быть точным при рассмотрении в качестве примера чисто гипотетических систем, но основные характеристики, перечисленные в таблице, могут помочь пользователю настоящего стандарта определить: должна ли конкретная система при анализе рассматриваться как система категории 1, 2 или 3.

Таблица В.1—Категории систем передачи

|  |  |  |
| --- | --- | --- |
| Категория | Основные характеристики | Пример систем передачи |
| Категория 1 | Разработана для известного и фик­ сированного максимального числа участников.  Все свойства системы передачи из­ вестны и постоянны на протяжении времени жизни системы.  Наличие незначительной возможно­ сти для несанкционированного до­ ступа | Закрытая передача (например, связь точечного путевого датчика с антенной локомотива).  Собственная последовательная шина, внутри связанной с безопасностью системы [например. PROFIBUS. CAN. MVB (многофункциональная поездная шина, определен­ ная в МЭК)].  Стандартная LAN. соединяющая различное оборудова­ ние (связанное и несвязанное с безопасностью) в единую систему с учетом выполнения и поддержки предваритель­ ных условий |
| Категория 2 | Свойства неизвестны, частично не­ известны или изменяются на протя­ жении времени жизни системы.  Возможности для расширения груп­ пы пользователей ограничены.  Группа или группы пользователей известны.  Существуют незначительные возмо­ жности для несанкционированного доступа (сети надежны).  Случайное использование ненадеж­ ных сетей | Собственная последовательная шина внутри связанной с безопасностью системы (например. PROFIBUS. CAN. MVB), но систему передачи можно переконфигурировать или заменить другой системой передачи на протяжении времени жизни системы.  Стандартная LAN. соединяющая различные системы (связанные и не связанные с безопасностью) в управля­ емой и ограниченной зоне.  WAN. принадлежащая железной дороге, соединяющая различные системы (связанные и не связанные с безопас­ ностью) на различных участках.  Коммутируемая линия в общедоступной телефонной сети, используемая случайно и в непредсказуемые мо­ менты времени (например, коммутируемая удаленная диагностика системы централизации).  Постоянно арендованный канал прямой связи в общедо­ ступной телефонной сети. |

26

#### ГОСТ Р МЭК 62280—2017

*Окончание таблицы В. 1*

|  |  |  |
| --- | --- | --- |
| Категория | Основные характеристики | Пример систем передачи |
|  |  | Система радиопередачи с ограниченным доступом (на­ пример. использование волноводов или излучающих кабелей с энергетическим бюджетом канала, ограничи­ вающим возможность приема только ближайшей радио­ станцией или использование собственной схемы моду­ ляции. не позволяющей воспроизведение сообщений с помощью серийно выпускаемого или доступного по цене лабораторного оборудования} |
| Категория 3 | Свойства неизвестны, частично не­ известны или изменяются на протя­ жении времени жизни системы.  Неизвестны группы многочисленных пользователей.  Наличие благоприятных возможно­ стей для несанкционированного до­ ступа | Система передачи данных с пакетной коммутацией в об­ щедоступной телефонной сети.  Интернет.  Радиоканал передачи данных с коммутацией каналов (на­ пример, GSM-R).  Радиоканал передачи данных с коммутацией пакетов (на­ пример, GPRS).  Радиопередачи малой дальности (например. Wi-Fi).  Системы радиопередачи без ограничений |

В.2 Связь категории системы передачи с угрозами

Таблица В.2 показывает приближенное распределение угроз для каждой из категорий систем передачи, определенных выше.

Таблица В.2 — Связь «категория—угрозы\*

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Категория | Повторение | Уделение | Вставка | Пврвупоря\* дочиоанне | Повреждение | Задержка | Подмене |
| Категория 1 | + | ♦ | + | + |  | + | - |
| Категория 2 | ++ | ♦♦ | ++ | + |  | - | - |
| Категория 3 | ++ | ++ | ++ | ++ |  | ++ | ++ |

Обозначения:

-------угрозой можно пренебречь:

+ — угроза существует, но редко: нужны достаточно слабые контрмеры;

++ — угроза существует; требуются серьезные контрмеры.

Примечание — Данная матрица угроз является только руководством, поэтому всегда необходим анализ, чтобы определить, требуются ли контрмеры и в какой степени. Каждая угроза будет зависеть от типа сети, приложения и конфигурации.

На таком общем уровне невозможно определить значение УПБ на основании категории системы передачи, а также средств защиты, необходимых для каждой угрозы. Необходимо проанализировать конкретное приложение, чтобы определить значение УПБ.

27

#### ГОСТ Р МЭК 62280—2017

Приложение С (справочное)

#### Руководство по применению средств защиты

С.1 Применения меток времени

Метка времени может быть использована в различных целях.

а} Для установления времени события 8 объекте, которое является важным для процесса получения инфор­ мации. События могут быть связаны друг с другом по времени. Если известны моменты времени и значения для последовательности событий, го можно интерполировать значения и увеличить точность расчетных значений (на­ пример. для скорости, ускорения). Могут быть обработаны задержки передачи.

Ограничения:

* если используется абсолютная метка времени, то время в объектах должно синхронизироваться. У каждо­ го объекта должно быть безопасное время проверки и обновления глобального времени. Задержки в сети влияют на глобальное распределение тактовых сигналов, корректность информации и характеристики процесса;
  + - отсутствие сообщений не будет обнаружено, если не будет обеспечена диалоговая коммуникационная процедура.

b) Для упорядочивания последовательностей событий, которые могут быть проверены получателем. Ограничения:

* если величина кванта времени слишком велика, то упорядочивающие свойства событий могут быть не­ определимыми. В таких случаях информация должна быть дополнена порядковыми номерами:
  + - на порядок сообщений влияют сетевая маршрутизация сообщений и задержки в сети:
* отсутствие сообщений не будет обнаружено, если не будет обеспечена диалоговая коммуникационная процедура.

1. Для измерения времени между событиями, полученными от объекта, отправляющего последовательность сообщений, тем самым для проверки того, что события не были задержаны.

Если объектом А неоднократно запрашивается информация из другого объекта В. то последний получает информацию локальных часов партнера от меток времени с учетом задержек. Эта информация может быть связа­ на с его собственным синхросигналом, учитывающим задержки передачи. Синхросигнал для логики создается из локального синхросигнала объекта В.

Ограничение:

* + - на синхросигнал для логики влияет изменение задержек в сети и обработка в объекте А.

1. Для проверки корректности информации объекта А требуется возврат метки времени, переданной объ­ ектом В е предыдущем сообщении объекту А. Это гарантирует конкретный ответ (идентификационные данные), а также проверяет его по предварительно определенному времени цикла. Создаваемый порядковый номер (или метка) и время, контролируемое е объекте В. сделают ту же работу. В каком-либо глобальном времени нет необ­ ходимости (если это не требуется другими приложениями).

Получатель обнаруживает потерю информации, используя тайм-аут. Ограничения:

* + - процедура должна обрабатывать прерывание в связи с неисправностями или инициализацией;
* процедура не гарантирует аутентификацию сообщений.

1. Для создания процедуры, названной двойное назначение временных меток (15). Эта процедура наследует свойства комбинации случаев Ь). с) и d). Процедура двойного назначения временных меток допускает асинхронную синхронизацию в объектах, таким образом, избегая проблем, связанных с поддержкой объектов, обновляемых глобальным временем. Эго метод может использоваться для:
   * + формирования синхросигнала для логики из локального синхросигнала партнеров и относительных меток времени от собственного локального синхросигнала (и организация тактовой синхронизации между этими двумя объектами):

* установления связи событий с относительными метками времени, учитывая задержку в сети;
  + - проверки правильного порядка сообщений:
* проверки синхросигнала партнеров, чтобы проверить правильность синхросигнала (зависящего от при­ ложения) на Вашей стороне.

Передача допустима для диалога между двумя партнерами или для связи «ведущий-ведомый». Последняя более применима для циклической передачи данных, чем при формировании временных меток для отдельных со­ бытий. где для конкретной функции важно время.

Ограничения:

* если величина кванта времени слишком велика, то упорядочивающие свойства событий могут быть не­ определимыми. В таких случаях информация должна быть дополнена порядковыми номерами:

28

#### ГОСТ Р МЭК 62280—2017

* + - двойное назначение временных меток может потребовать знаний о задержках двойного (туда и обратно) прохождения сигнала, если применение рассматривает случай, представленный в перечислении а).

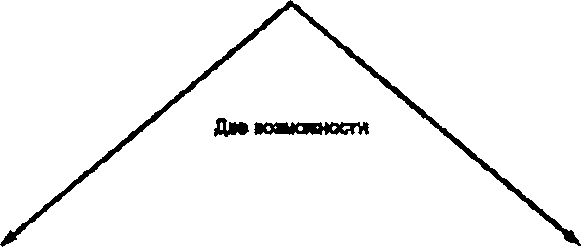
Были предложены более сложные схемы, чем двойное назначение временных меток, которые позволяют упорядочивать события, происходящие более чем в двух системах.

С.2 Выбор и использование кодов защиты и криптографических методов

Несмотря на то, что система передачи мота быть неизвестной или изменяться во время ее жизни, в боль­ шинстве случаев можно определить, могут ли быть исключены вредоносные атаки на связанные с безопасностью сообщения или они возможны. Это очень полезно знать, потому что в случае возможности этих вредоносных атак потребуются криптографические механизмы с секретными ключами. Рекомендуется это выяснить на ранней ста­ дии. чтобы ограничить связанную с безопасностью функциональность. Если существует возможность несанкцио­ нированного доступа. то может быть применен отдельный слой защиты доступа {типа ВО или В1). см. рисунок С.1. или защита обеспечивается связанной с передачей данных функцией безопасности, использующей криптографи­ ческие механизмы {тип А1), и 8 этом смысле в последующем тексте использован термин «криптографический код защиты».

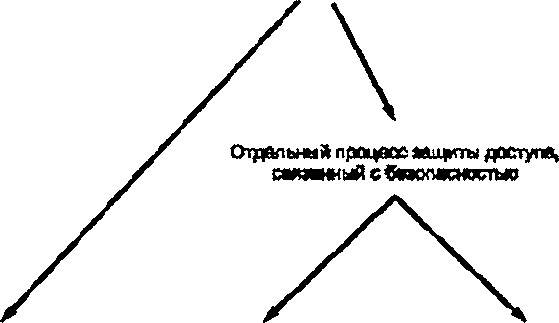
29

#### ГОСТ Р МЭК 62280—2017

Кэииумшационнмвиетша,шиютяобмаяшноотш

Т»ырв~~ето~~|ж~~эцвв~~нныйдоступ Наиторюошлныйдо(п^нш1»иашк7Ч1гг>

Кртпзгрвфмчесшеметоды,исгигыута1\*\*аиретньЛкода



|  |  |  |  |
| --- | --- | --- | --- |
| НиригтгряфиишиМ ом  «мол\*\*\*™ | Критпмрафмчммй им  ««опасное™ | Hi цшгтгрйфичвошЯ моя боктоенос™  ♦uautvoww | К» (фмгммрофмаммй им ОМОгИвнОСп.  ♦ЖрИТТОфЯфНКЯМЙ км |
| *ЪпАй* | ТипА1 | Тип ВО | Тип В1 |

Структуресообщения, ОмирисуиокС.2

Структуре

СООбЩвНИЯ,

см. рисунок СЛ

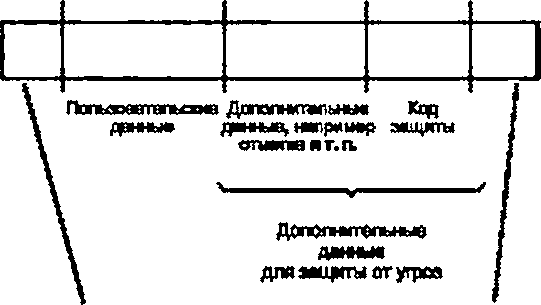
Структуре сообщения, ем. рисунок (Х5

Рисунок С. 1 — Классификация связанных с безопасностью систем связи

30

#### ГОСТ Р МЭК 62280—2017

Принцигы структур сообщения для сообщений типов АО и А1 представлены на рисунке С.2.



|  |  |  |
| --- | --- | --- |
|  | | |
|  |  |  |
| Пшъаоаитольааи»данью |
| Дополнительны»данные огфушцжпарадач\*амаажы! едяолкноегыв |
| Кадидоы | | |

Дртепннтльныеяшншсистемы парадны,на~~сада~~м»\*\* сбоаопвсиоспао

Ншртеюр,заголовок Hanprewp,ионпередачи



Допэпнитальные данные системыпарад\*\* насапамнойобаавпаоноотьв

Рисунок С.2 — Модель представления сообщения в системе передачи {тип АО. А1)

Отдельные слои защиты доступа полезны в тех случаях, где группы связанных с безопасностью компью­ теров. соединенных локальной сетью {LAN), должны передавать данные по открытым системам передачи (см. рисунок С.Э). Неявное предположение для модели, изображенной на рисунхе С.З. состоит в том. что локальные сети могут быть отнесены к категории 2. Аппаратные средства и программное обеспечение криптографии могут быть сконцентрированы в однозначно определенной точке входа открытой системы передачи. Другие интерфей­ сы открытой системы передачи должны быть исключены. Криптографические функции могут быть объединены с функциями шгъоза. которые обычно требуются, когда локальная сеть соединена, например, с глобальной сетью.

31

ГОСТ Р МЭК 62280—2017

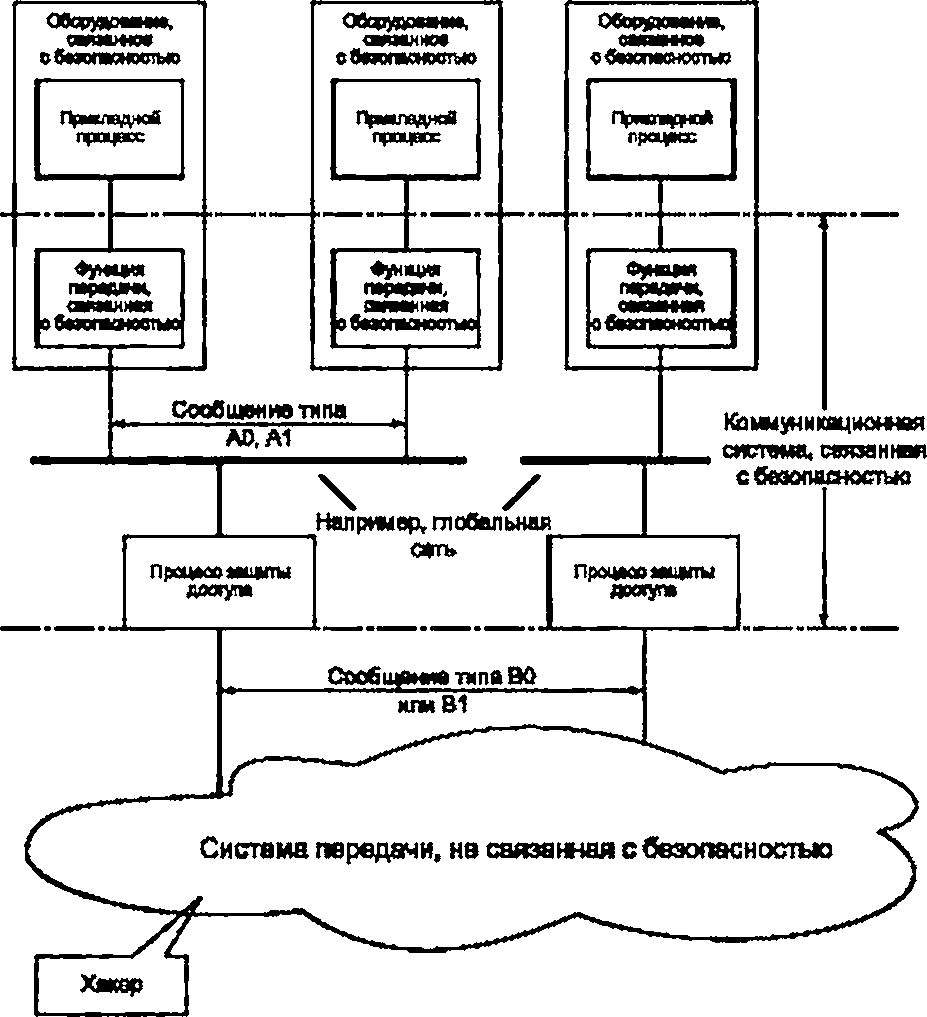


Рисунок С.З — Использование отдельного слоя защиты доступа

Процесс защиты доступа может быть реализован различными способами:

a) шифрование сообщений:

b) добавление криптографического кода.

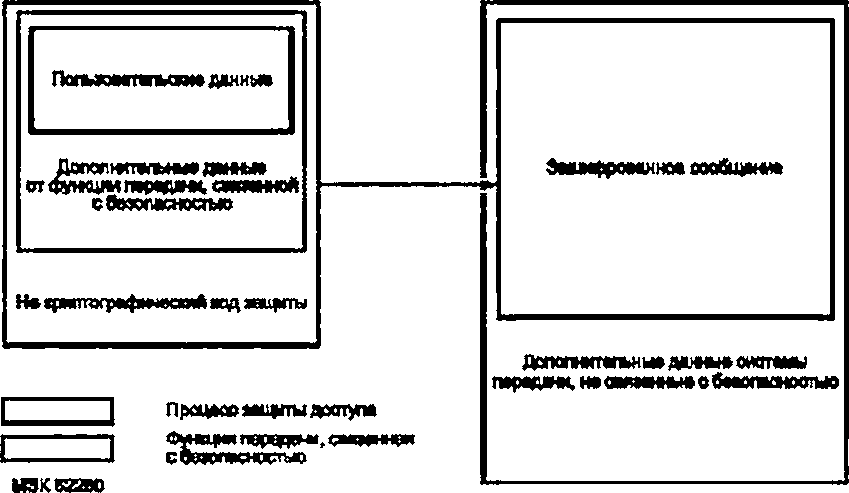
В обоих случаях применяются коды защиты перед тем. как связанное с безопасностью сообщение посылает­ ся к слою защиты доступа. Оборудование, содержащее слой защиты доступа, не должно быть безопасным само по себе. см. общие требования в 7.2. Необходимо отметить, что должны быть рассмотрены отказы процеоса защиты доступа.

Принципы структур сообщения для типов сообщений ВО и В1 изображены на рисунках С.4 и С.5.

В этих примерах показана криптографическая защита, применяемая сразу после кода защиты. В других при­ мерах она может быть применена на более низких уровнях (например, транспортном или сетевом).

32

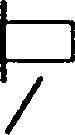
#### ГОСТ Р МЭК 62280—2017



Пммгнш<1хин> Плплпшгтчма tt> вмтспмйжчаашА MHN *~~т~~шш,* ирримц) ММММ1Ш

ОПШПИТ.П.

дсгалншттимдо»и»длимщлыerугров

\3шнфкжтм ооо рщрвр 

#### Нмргмор, евгалэес\* Ншрммккн

пвирнн



Дриад и~~шцщ~~ данные о етшы пфврум!, нв «панной с бшччж ность»

Рисунок С.4 — Модель представления сообщения е системе передачи (тип ВО)

33

#### ГОСТ Р МЭК 62280—2017

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
| ГЪлиоягплмяладмны» |  |  |
| Дапопнитапьмывдым» отфункциимрадм\*амажай  «бвхтоиооть» | |  |
| Накр»гггпгрьфн1ягГ|Л«одзащиты | | | |

D^MttarptcfwwKMli мм бввомоновн

Дх«лншшыыеданнw<\*кгтыперед»\*, невешннобобвютонооть»

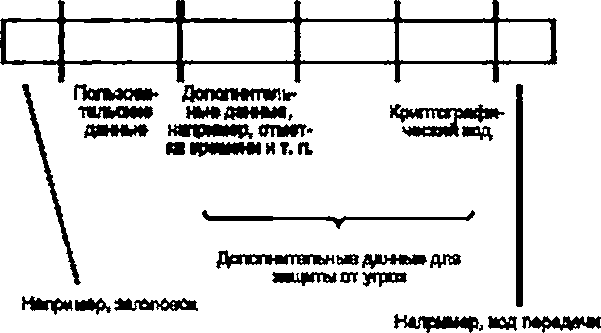
I 1 Продесс\*\*.цтыдпстун1

I1 I <hjnw педедии. ~~ш~~ни~~шнм~~

Iаовигамнооть»

**мэквггво** Нвфи~~иц~~рв» фичвмвип

вампы



Дспопнитапьнывдням»~~шпи~~кIперемни. неои~~и~~е~~и~~юОобмашноашо

Рисунок С.5 — Модель представления сообщения в системе передачи (тип В1)

С.З Код защиты

С.3.1 Общие положения

Требуемые свойства кода защиты зависят от характеристик системы передаем и архитектуры связанной с безопасностью системы передачи данных (см. рисунок С. 1).

Если несанкционированный доступ к системе передачи данных может быть исключен, то коды защиты долж­ ны обнаруживать все виды случайных и систематических битовых ошибок. Необходимо отметить, что обычно си­ стема передачи защищает свои сообщения своим собственным кодом передачи, который уже разработан так. чтобы соответствовать определенному уровню качества и заданной интенсивности битовых ошибок. Следователь­ но. если система передачи данных передает недопустимое сообщение, то либо сбой е канале передачи был на­ столько большим, что код передачи был поврежден, либо произошел отказ. В любом случае необходимо считать, что остаточные битовые ошибки не случайны, и могут иметь произвольный вес Хэминга (17].

Если несанкционированный доступ не может быть исключен, то вредоносная атака не может быть предот­ вращена. но может быть обнаружена и обезврежена. Обычным способом предотвращения вредоносной атаки является применение криптографических алгоритмов, по крайней мере, с одним секретным ключом. Сам код за­ щиты может быть основан на таком алгоритме или может быть реализован отдельный слой защиты доступа с криптографическими функциями. В последнем случав код защиты также может обнаружить отказы оборудования защиты доступа.

С.3.2 Основные блочные коды С.3.2.1 Общие положения

Следующие подпункты кратко описывают некоторые блочные ходы и их основные характеристики. Более подробно см. в [17].

С.3.2.2 Линейные блочные коды

Блочный код линеен, если, и тогько если, сумма любых кодовых слое также является кодовым словом.

Большинство кодов, использующихся для коррекции ошибок, являются линейными двоимыми кодами. Также используются недвоичные коды, например, кеды Рида-Соломона. Эти коды превосходны для борьбы со случайными ошибками и с ошибками в пинии передачи пакетных данных. Эти коды могут быть разработаны с конкретным минимальным расстоянием Хемминга *d.* Это означает, что ошибки до <М неверных символов полно­ стью обнаруживаются. Вследствие их линейности коды могут быть протестированы на возможность обнаружения систематических ошибок передачи.

Полезными моделями являются двоичный симметричный канал (BSC) и q-арный симметричный канал (QSC).

Эти коды могут быть также протестированы на обнаружение систематических ошибок передачи. 34

#### ГОСТ Р МЭК 62280—2017

С.3.2.Э Циклические блочные коды

Линейный блочный код является циклическим, если каждый циклический сдвиг кодовой комбинации также является кодовой комбинацией. Циклический код может быть описан полиномами. Математическое описание ко­ дов можно найти, например. 8 [17].

Эти коды превосходны для борьбы со случайными ошибками и с ошибками в линии передачи пакетных данных. Эти коды могут быть разработаны с конкретным минимальным расстоянием Хемминга *d.* Эти коды могут также быть протестированы на обнаружение систематических ошибок передачи. Циклический код с с избыточными символами обнаруживает все пакетные ошибки размером до с символов.

В некоторых приложениях может быть использована циклическая природа кода, чтобы избежать опасности синхронизации запрещенного кодового слова. Для этого, необходимо расширить код. но конечный результат будет превосходить системы, полагающиеся на отдельные символы синхронизации.

С.3.2.4 Блочные хеш-коды

Хэш-коды могут быть линейными или нелинейными. Наиболее важными являются нелинейные односторон­ ние функции, которые сжимают входные данные до «цифрового отпечатка пальца». Из-за их нелинейности ми­ нимальное расстояние Хемминга не может быть получено, за исключением небольшого количества тривиальных случаев. Однако возможность обнаружения ошибок высока для удачных хэш-кодов. Изменение одного разряда во входных денных изменяет в среднем половину битое е значении хэш-функции. Зная значение хэш-функции, невоз­ можно вычислить входные данные, которые хешируются этим значением хэш-функции (свойство однонаправлен­ ности). и зная входные данные, невозможно вычислить другие входные данные, которые хешируются таким же значением хэш-функции коллизия для слабых хеш-функций), и невозможно с помощью вычислительных методов найти какие либо два набора входных данных, которые хешируются одним и тем же значением хэш-функции (кол­ лизия для сильных хеш-функций).

В [7] определяются хэш-коды для целей безопасности 8 общем случае. В (6) описываются хэш-коды, исполь­ зуя п-разрядный алгоритм блочного шифрования без применения ключа. Кроме того, в качестве хэш-кода может использоваться код аутентификации сообщений (MAC), но в этом случае требуется ключ.

Хорошая эффективность программного обеспечения может быть получена с алгоритмами представления сообщения в краткой форме, относящихся к сфере общего пользования. MD4 и MD5. которые являются классами кодов обнаружения манипуляций (MDC). Никаких повышенных требований к критериям коллизий не требуется, т. к. вредоносные атаки защищены другими средствами. Это означает, что используется или криптографический блочный код (MAC) или применена криптографическая защита для всего связанного с безопасностью сообщения, включая значение хэш-функции.

С.3.2.5 Цифровые подписи

Цифровая подпись — это некоторое число разрядов, которое зависит от общего числа битое входных дан­ ных (данные пользователя и дополнительные данные), а также от секретного ключа. Ее правильность может быть проверена при помощи открытого ключа.

С.3.2.6 Криптографические блочные ходы

Криптографические блочные коды являются нелинейными блочными хеш-кодами на основе криптографи­ ческих алгоритмов. Их преимущество состоит в том. что они могут защитить от вредоносной атаки, если они ос­ нованы на ключах. Самый известный код — это код аутентификации сообщений (MAC), который описан в [4] и [5].

С.3.3 Рекомендации по применению кодов защиты

Примеры для оценки разнообразных основных методов даны в таблице С.1.

Таблица С.1 — Оценка механизмов кодирования, обеспечивающих безопасность (см. примечание)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Тил\*' | Ссылка, см. раздел 2 и библиографию | Тип связанной с безопасностью системы коммуникации, см рисунок С.1 | | | |
| АО | А1 | во6> | Bib) |
| CRC«> | [Peterson] | R | USd> | \_•) | R |
| MAC61 | ИСО/МЭК 9797-1 и 2 | R | HR | R | R |
| Хэш-кодс) | ИСО/МЭК 10118-2 | R | USd> | HR | HR |
| Цифровая подпись61 | ИСО/МЭК 9796-2 и 3 | R | R | R | R |

Примечание — Если рекомендуется более одного механизма кодирования безопасности, го должна быть отобрана подходящая комбинация одного или нескольких механизмов.

HR — метод настоятельно рекомендуется для этой архитектуры. Если этот метод не используется, то это должно быть подробно обосновано в техническом отчете по безопасности;

R — метод рекомендуется для этой архитектуры. Этот уровень расположен ниже уровня рекомендации

«HR»;

- — метод или мера не имеет рекомендации по использованию ни за. ни против;

#### 35

ГОСТ Р МЭК 62280—2017

*Окончание таблицы С. 1*

US — метод не подходит для защиты системы этой категории.

а> Возможны другие меры по обеспечению безопасности, но здесь не рассмотрены.

ь\* Только не криптографические коды защиты. Криптографические методы должны быть рассмотрены отдельно.

с> Способность обнаружения ошибки одинакова для одного и того же числа битов избыточности.

d> Запрашиваемый секретный ключ этим механизмом не может быть выполнен.

е> Если используются методы шифрования потока, то применение CRC в качестве кода защиты не приемлемо. В противном случае субъект атаки может создавать связанные с безопасностью сообщения с действительным CRC, добавляя произвольное сообщение с действительным CRC к зашифрованному сообщению потока, не ломая ключ.

Хотя знание характеристик ошибок конкретного канала может позволить некоторые типы ошибок игнориро­ вать и обеспечить его лучшую работу, но в «открытом» канале (черном канале) никаких таких знаний нельзя пред­ положить. В этом сценарии идеальным решением был бы случайный код. Поэтому не должны устанавливаться никакие требования к вероятности необнаруженных ошибок *рие* кода защиты, которая ниже, чем вероятность случайного кода, которая равна = *2~с,* где с обозначает число битое избыточности.

С.3.4 Криптографические методы

При использовании методов криптографической защиты рекомендуются стандартизированные режимы ра­ боты. например, в соответствии с [6]. Этот стандарт не рекомендует метод прямого шифрования (ЕСВ) для длины входной последовательности, превышающей размер блока алгоритма шифрования. Рекомендуются хорошо из­ вестные и проверенные алгоритмы, такие как в (16].

С.4 Длина кода защиты

Настоящее приложение применимо только к Категории 1. т.е. к закрытым системам передачи, так как данные формулы основаны на конкретных предположениях в системе передачи.

На самом деле описанная ниже модель частично опирается на механизмы обнаружения и управления ошиб­ ками систем передачи. Обычно в исправном состоянии механизм обнаружения ошибок системы передачи обна­ руживает и противодействует всем ошибкам передачи. В этом случае код защиты не обнаруживает ошибок. Тем не менее, сама система передачи или ее механизм обнаружения ошибок может прекратить работу из-за отказов аппаратных средств либо некоторые ошибки передачи являются ошибками такого высокого уровня, что они не обнаруживаются. Во всех подобных случаях код защиты должен обнаружить эти отказы.

Использование этой модели ведет к более низким требованиям полноты безопасности для кода защиты по сравнению с моделями, пренебрегающими возможностями обнаружения ошибок системы передачи. С другой сто­ роны. систему передачи в этом случае фиксируют и ее нельзя поменять на другую без адаптации доказательства безопасности. Эта модель может быть (и должна быть, если необходимо) изменена для систем, игнорирующих их механизмы обнаружения ошибок или влияние интенсивностей отказов, источником которых являются аппаратные средства.

Настоящее приложение дает простые формулы для вычисления длины кода защиты. Выполнение данных требований гарантирует, что цель безопасности будет достигнута.

Базовая модель для вычисления длины кода защиты показана на рисунке С.б. Существует три возможности появления опасности:

a) сбои аппаратных средств системы передачи, приводящие к повреждению сообщений:

b) битовые ошибки, возникающие из-за ЕМ) и не обнаруженные кодированием передачи:

c) сбои происходят в средстве проверки кода передачи, поэтому каждое поврежденное сообщение может быть передано из недоверигельной системы передачи в связанное с безопасностью оборудование.

36

#### ГОСТ Р МЭК 62280—2017

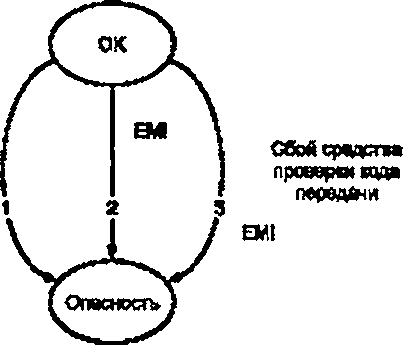
СвоАамглшы тредами(Вв\*(боя орепота проверки код\*передни)

Рисунок С.6 — Базовая модель ошибки

Введем следующие определения:

*RH* — целевая интенсивность опасных отказов всей системы передачи.

*RH,* — иювнсивностъ опасных отказов от сбоев аппаратных средств без средства проверки хода передами:

*Rh 2* — интенсивность опасных отказов от EMI;

*R»3* — интенсивность опасных отказов средства проверки кода передачи: *RH*уу— интенсивность опасных отказов недоверигельной системы передачи: *Pus* — вероятность необнаруженных отказов при выполнении кода защиты;

— вероятность необнаруженных отказов при выполнении кода передачи:

Прим еча н и е — Если недоверигельные системы передачи не содержат механизмов кодирования пере­ дачи. то должно быть принято *Рщ -* 1.

*1ц* — максимальная частота сообщений для одного получателя;

*f*w— частота неправильных (поврежденных) сообщений:

Г — отрезок времени: если за этот отрезок времени было получено поврежденных сообщений больше определенного количества, то будет осуществлен возврат в безопасное состояние: {безопасное со­ стояние с пониженной скоростью передачи данных);

*к*, — коэффициент для сбоев аппаратных средств, включающий запас безопасности;

*к2* — коэффициент, который описывает процент сбоев аппаратных средств, которые приводят к необнару­ женному отключению декодирования передачи:

*т* — запас безопасности, включен в А,:

*п* — количество последовательных поврежденных сообщений, после которого выполняется переход в без­ опасное состояние с пониженной скоростью передачи данных.

С этими определениями необходимо оценить следующие формулы:

|  |  |
| --- | --- |
| *RHW' PUS*' \*1 = *RH1* • | (C.1) |
| *PUT* ' *PUS* ' *iw~* R«21)' | (C.2) |
| 1 |  |
| \*2 ’ *PUS'~^ = RH3-* | (C.3) |

Сумма всех трех значений интенсивностей не должна превышать *RH:*

*R Hi\*R H2\*R H3SRH-*

1> Это предполагает, что код защиты и код передачи независимы. Это может быть очень трудно доказать.

Более консервативный подход должен основываться только на коде защиты.

37

#### ГОСТ Р МЭК 62280—2017

Поскольку нельзя предположить, что отказ случаен, не обходимо принять во вниманью запас безопасности *т*

а коэффициенте к,. Коэффициент к1 должен быть вычислен согласно следующей формуле:

*кл* г *п ■ т.*

Коэффициент ш представляет запас безопасности с ш г 5.

Максимальная частота неправильных сообщений /^должна быть оценена:

* + - либо с помощью оценки наихудшего случая *fw* = *}^*
* гыбо с помощью ограничения на максимальную интенсивность или количество неправильных сообщений, где реализованы безопасные счетчики и/или безопасные таймеры. Если в определенном временном интервале получено богъше одного неправильного сообщения, то безопасная передача должна быть прервана, и должен быть выполнен переход в безопасное состояние с пониженной скоростью передачи данных. Математический вы­ вод доказывает, что определенный предел не может быть превышен.

В циклической передаче частоты *fu* определена точно. В случав нециклической передачи необходимо ис­ пользовать максимально возможное значение частоты.

При помощи «подходящего» или «хорошего» CRC1\* максимальное значение *РиТ* можег быть оценено как:

*Рит" 2-\*.*

где *b* означает число битое избыточности.

Если используются другие коды, например, комбинация двух кодов, то должно быть использовано значение вероятности ошибки блока в наихудшем случае, применяя модель «двоичного симметричного канала»2).

Коэффициент *к2* трудно оценить. Если возможна периодическая проверка корректной работы механизма кодирования передачи, то коэффициентом *к2* можно было пренебрег».

Без каких либо обоснований можно считать, что *к2* » 1. Примечание — Следующий вывод дан только для информации.

Если в аппаратных средствах происходит сбой, то только в одном из 10000 случаев в средстве проверки кода передачи происходит необнаруженный отказ.

В этом случае средняя продолжительность этого состояния (без учета EMI) составляет:

#### 1

т=мтв *\*HW*

RMW

Следует отметить, что небольшое ухудшение качества передачи обычно приводит к выполнению перехода в безопасное состояние с пониженной скоростью передачи данных, поэтому такая оценка очень пессимистична.

При этих предположениях может быть принято значение для *к2* = 10 .

Формула (С.З) приводит к минимальному временному интервалу, на котором позволена только одна ошибка, выявляемая кодом защиты. Если такой механизм не используется, то после первой обнаруженной ошибки будет немедленно выполнен переход в безопасное состояние с пониженной скоростью передачи данных, иначе должны быть выполнены другие меры по предотвращению условий возможных ошибок.

Максимальная вероятность для необнаруженных ошибок кода защиты с числом разрядов с должна быть оценена как:

*Pus ж 2~е-*

Эта формула может использоваться е качестве грубой оценки вероятности необнаруженных ошибок. Это справедливо для большого класса кодов (например, кодов Хэмминга, некоторых ВСН-кодов, криптографических кодов и т. д.) при реальных предположениях. Тем не менее необходимо продемонстрировать, что требования «под­ ходящий» или «хороший»1\* для выбранного линейного кода были выполнены.

Повторяя каждое сообщение и проверяя согласованность двух взаимно независимых сообщений, значение с можег быть уменьшено наполовину, по крайней мере, для достижения той же самой цели. На самом деле можно получить некоторое дальнейшее улучшение, но чтобы избежать сложных математических вычислений, данную пвссимгстическую оценку следует считать пределом.

’) «Подходящий» означает, что отношение между вероятностью битовой ошибки (меньше, чем 0,5) и вероят­ ностью необнаруженной ошибки является монотонным. «Хороший» означает, что у вероятности необнаруженной ошибки есть свой абсолютный максимум при вероятности битовой ошибки, равной 0.5.

2) Двойной симметричный канал: с вероятностью *р* полученный бит сфальсифицирован (0—1 и 1—0). Каж­ дый бит независим друг от друга.

#### 38

ГОСТ Р МЭК 62280—2017

Прим еча нив — Этот механизм основан на том. что отказы по общей причине, влияющие на два сообще­ ния. незначительны.

C.S Коммуникация между связанными и не связанными с безопасностью приложениями

На рисунке С.7 представлен пример передачи сообщений между связанными и не связанными с безопасно­ стью приложениями.

В доверительных сетях (Категории 1 и 2) не связанные с безопасностью приложения могут передавать со­ общения по той же среде передачи, которую используют, связанные с безопасностью приложения. Требования см. в7.2.

В этом примере сообщения, не связанные с безопасностью, также защищены криптографическими метода­ ми при прохождении через системы передачи Категории 3.

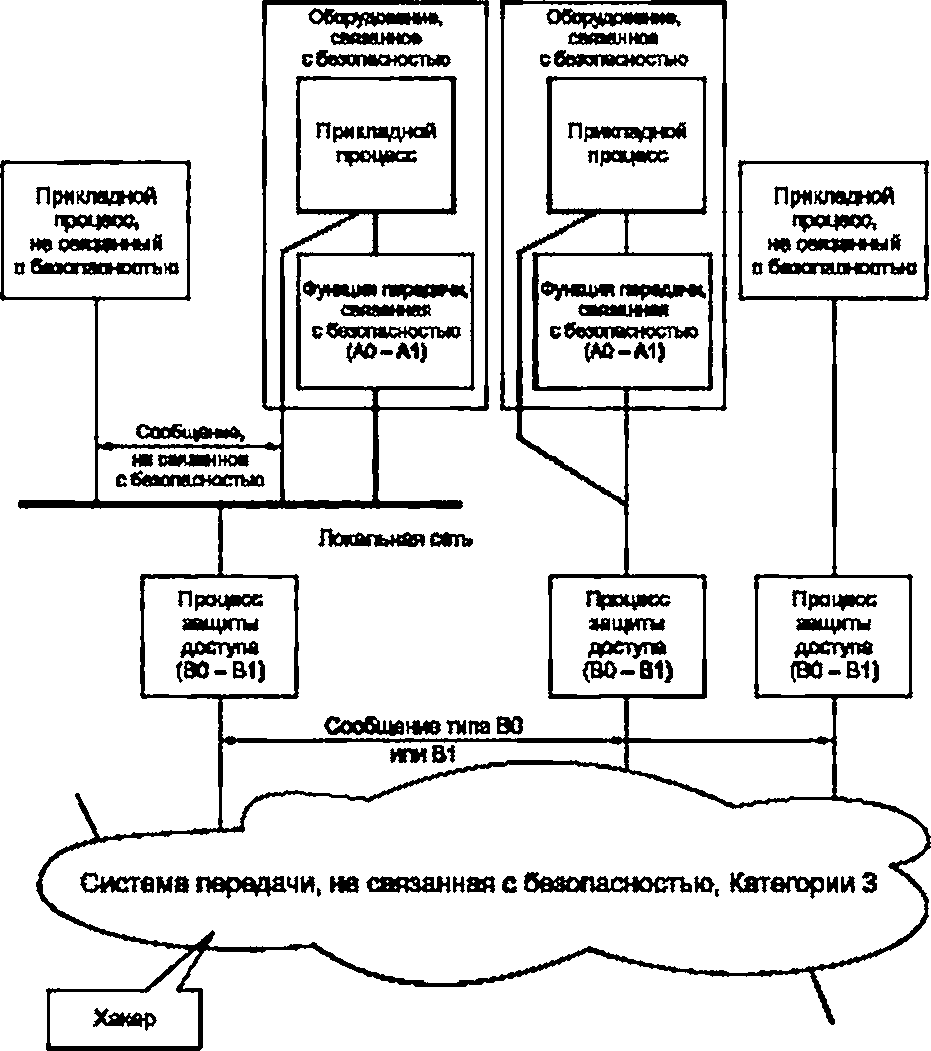


Рисунок С.7 — Коммуникация между связанными и не связанными с безопасностью приложениями

#### 39

ГОСТ Р МЭК 62280—2017

Приложение D (справочное)

#### Руководство по применению настоящего стандарта

* 1. Процедура
     1. Общие положения

Чтобы выполнить действия по проектированию системы в соответствии с МЭК 62425, можно выделить не­ сколько различных этапов, которые определены ниже:

# 4

#### Аюлюрмок

**4**

Сплавим\*риска

4

Определениеанвчвни\*УПБишзпичветэенньвцелей

**4**

СпедифмацмтрабмиммАбваодаснрст(SRS)

Каждый из этих шагов описан более подробно в следующих подпунктах.

* + 1. Приложение

Разработчик системы должен понимать приложение системы передачи, а именно: потоки данных, типы дан­ ных. частоту и природу обновлений (например, периодические обновления или управляемые событиями), влияние всех решений, которые будут сделаны при разработке системы передачи. Также для системы должна быть опреде­ лена (пользователем или полномочным органом по безопасности) глобальная цель безопасности (интенсивность или качественные параметры и нефункциональные параметры).

* + 1. Анализ риска

Качественный анализ угроз системы (8 соответствии с МЭК 62278) должен идентифицировать опасностей) верхнего уровня, которая может возникнуть в результате отказов оборудования отправки и получения или самой линии передачи. Этот анализ должен рассмотреть эксплуатационные или другие внешние условия, которые могут подвергать систему опасности. Для каждой угрозы системы может быть включена возможность применения за­ щиты в проекте системы.

* + 1. Снижение риска

Зная глобальную количественную цель безопасности для системы и результаты качественного анализа ри­ ска. разработчик системы может распределить цели безопасности для каждой идентифицированной угрозы. Опре­ деление таких целен может быть итеративным, начиная с упрощенного определения, и улучшаясь в соответствии с более детальным анализом и нахождением компромиссов. Используя количественные данные о возникновении внешних условий, вызывающих опасность в системе, может быть определена степень снижения риска, задавае­ мого для каждого средства защиты.

* + 1. Определение значений УПБ и количественных целей

В зависимости от степени снижения риска, необходимого для каждого средства защиты, используя проце­ дуры. определенные в МЭК 62425. можно определить УПБ. Зная значение УПБ для средства защиты, могут быть выбраны надлежащие методы их проектирования, изготовления и эксплуатации.

Из количественно определенной интенсивности опасных отказов, определенной для средства защиты, ис­ пользуя таблицы е МЭК 62425. метут быть выбраны методы проектирования аппаратных средств, а также может быть вычислена интенсивность возникновения опасных отказов из-за случайных отказов.

* + 1. Спецификации требований безопасности (SRS)

Описание средств защиты, определенных как необходимые для безопасной работы системы, значение УПБ для реализации этих средств защиты и определенные количественные значения целей безопасности для системы должны быть представлены в SRS на систему.

* 1. Пример
     1. Общие положения

Следующий пример показывает только некоторые основные принципы процедуры. Он не был предназначен для описания полного примера, корректного во всех деталях.

* + 1. Приложение

Команды разрешения на проследование отправляются поездам по второстепенной пинии посредством со­ общений по радиосети.

Для системы определена глобальная цель безопасности 10~х в час.

40

#### ГОСТ Р МЭК 62280—2017

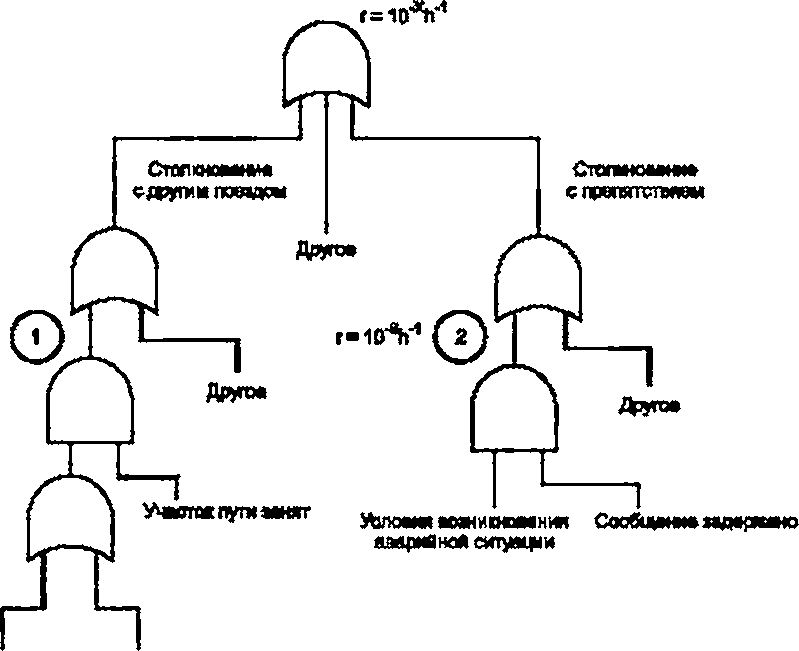
0.2.3 Анализ риска

Можно определить две конкретных опасности (в числе прочих, здесь не рассматриваемых):

a) прием некорректного (опасного) сообщения на борту поезда может привести к переходу поезда на занятый участок пути и к столкновению с другим поездом:

b) задержка получения сообщения об экстренной остановке может привести к столкновению поезда с пре­ пятствием на пути.

Они показаны на дереве отказов (рисунок 0.1) в примере одного из методов выполнения анализа риска.

НвснвстньЛ случай

#### .«V

гиуЕиннпасообщение Гфоиааопьивяоиибт

ООоа~~мно~~нмя:

О -елямИ;

О -~~д~~а~~р~~ен~~и~~ о т ни мали случая 1(см. рисую\* D.2J;

### ^2^ -дврваооткмеи для случая я (сы. рисунок 0.3); г -допуетм1ИВ1аггансмносгьагисндсп1.

Рисунок 0.1 — Дерево отказов для опасности «авария»

41

#### ГОСТ Р МЭК 62280—2017

Глобальная цель безопасности системы 10~х в час распределена и целевое значение, полученное для слу­ чаю 1 и 2 (например) равно 10-® в час для каждого случая.

Рассмотрим случаи 1 и 2 более подробно.

* + 1. Случай 1
       1. Снижение риска

Если сообщение для поезда повреждается из-за случайных ошибок, то оно может позволить поезду перейти на занятый участок пути и сталкиваться с другим поездом.

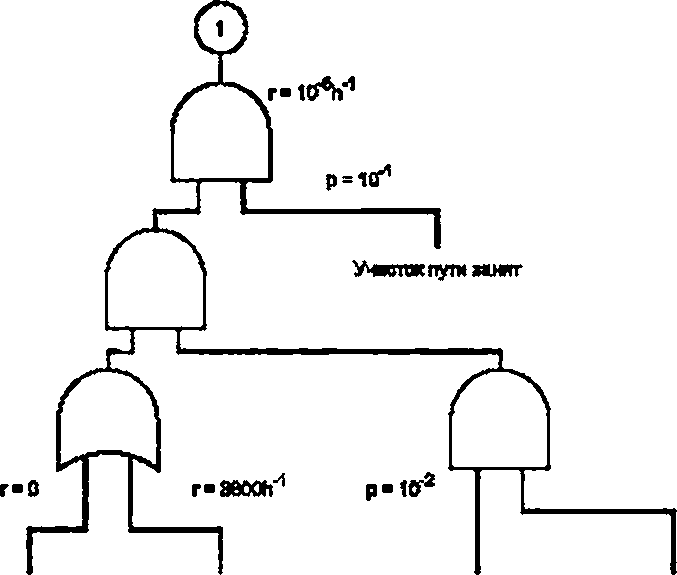
Кроме того, могли быть предприняты преднамеренные попытки, чтобы вставить нелравигъное сообщение в систему (например, хакером).

Предположим, что вероятность того, что участок пути занят, оценивается как 10'1.

Настоящий стандарт предлагает, чтобы возможным средством защиты от повреждения сообщения является использование кода защиты, присоединенного к информации пользователя в сообщении.

Введем такую защиту в часть дерева отказов для этого случая и получим следующий результат на рисунке

0.2:



ПоддельноеПлеменноесообщение ОшбвтведутОлршдоюоии№к,саяэшное

оообщам\*npaKmirhMOttourfNH кнебеспшену оребото\*кодаэшжты

состоял\*\*»

Рисунок D.2 —Дерево отказов для случая 1

Рассматривая количественные цели безопасности, предположим, что в открытой системе каждое сообще­ ние может быть повреждено (т. е. вероятность повреждения = 1). Однако не каждое поврежденное сообщение санкционирует движение поезда по определенному участку пути. Предполагая эту вероятность равной 10-2 и пред­ полагая. что сообщение длиной 100 битов отправлено поезду по каналу со скоростью передачи 100 бит/с (т. е.

3 600 сообщения в час), становится понятно, что кед защиты для сообщения должен гарантировать вероятность необнаруженной ошибки меньше, чем 3 \* 10-9 для сообщения, или частота этого вида событий не должна превы­ шать 10-5 в час.

* + - 1. Определение значений УПБ и количественных целей

Согласно МЭК 62425 может быть получено значение УПБ для реализации функции «вычисление кода за­ щиты». Это значение УПБ может быть ниже, чем для элемента всей системы «связанная с безопасностью система связи».

Разработчик системы должен выбрать код защиты достаточной длины, чтобы достигнуть требуемого каче­ ства функционирования.

Настоящий стандарт предполагает, что необходимо рассмотреть возможность преднамеренных попыток соз­ дания неправильных сообщений в открытой системе передачи. Например, для редкой передачи коротких сообще­

42

#### ГОСТ Р МЭК 62280—2017

ний вероятность преднамеренных попыток создать аварию может быть относительно низкой. Эти факторы могут влиять на решение о том. принять ли криптографические коды защиты, и если так. то на выбор параметров (длина ключа и т. д.) для этого кода.

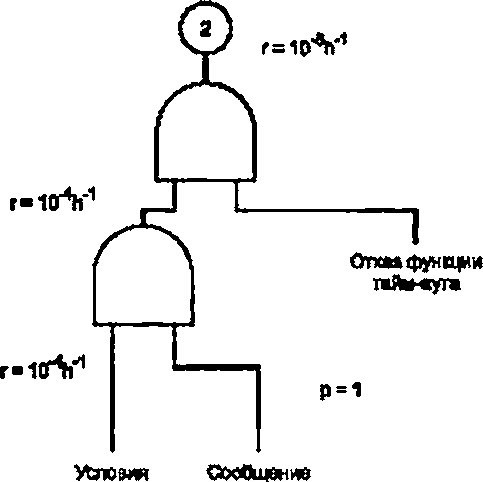
* + 1. Случай 2
       1. Снижение риска

Если в случае возникновения аварийной ситуации (например, из-за препятствия на участке пути) сообще­ ние об экстренной остановке поезда задерживается, то может произойти столкновение. Предположим, что такие аварийные ситуации могут происходить с частотой 10-4 в час.

Предположим, что. используя радиосеть совместно с неконтролируемым числом других пользователей, за­ держка не максимального сообщения гарантируется, и поэтому задержка должна быть (т. е. предполагается, что вероятность задержки равна 1).

Настоящий стандарт предлагает, чтобы возможным средством защиты от задержки сообщения является ис­ пользование тайм-аута в оборудовании получения, вместе с циклической передачей сообщения.

Введя информацию об этом средстве защиты в дерево отказов для рассматриваемого случая, получим ре­ зультаты. представленные на рисунке D.3:



■owMHoeweeiеедврвшнр амфмвно\*

ситуации

Рисунок D.3 — Дерево отказов для случая 2

Рассматривая количественные цели безопасности, понятно, что у функции тайм-аута должна быть вероят­ ность появления опасной ошибки по запросу не больше, чем 1(И.

* + - 1. Определение значений УПБ и количественных целей

В МЭК 62425 показано, как достигнуть требуемого значения УПБ.

Поэтому эта фунхция должна быть разработана, используя методы, предложенные в МЭК 62425, которые являются подходящим для полученного значения УПБ. если при реапиэации она не будет интегрирована с другими функциями с более высоким значением УПБ (например, е системе процессора).

#### 43

ГОСТ Р МЭК 62280—2017

Приложение Е (справочное)

#### Связь с предыдущими стандартами

Настоящий стандарт является результатом пересмотра и объединения предыдущих стандартов МЭК 62280- 1*.2002* и МЭК 62280-2:2002. Главным образом были выполнены тогъко исправления и улучшения. Для обеспече­ ния согласованности появилась необходимость в некоторой новой информации.

В таблицах Е.1 и Е.2 показано отображение (под)разделов и приложений предыдущих стандартов МЭК 62280-1:2002 и МЭК 62280-2:2002 на (под)раэделы и приложениям настоящего стандарта.

Они должны облегчить прослеживаемость в случае обслуживания и^или расширений систем, созданных в соответствии с предыдущими стандартами МЭК 62280-1:2002 и МЭК 62280-2:2002. а также понимание настоящего стандарта.

Отображение е таблицах Е. 1 и Е.2 делается только для (под)разделов предыдущих стандартов на (подраз­ делы настоящего стандарта, но не наоборот.

Таблица Е.1 — Отображение МЭК 62280-1:2002 на настоящий стандарт

|  |  |  |  |
| --- | --- | --- | --- |
| (Под|рашелы МЭК $2260-1:2002 | Справочный/ Обязательный | (Под|радаепы настоящего стандарта | Не изменен\* изменен |
| Введение | Справочный | Введение | р |
| 1 Область применения | Обязательный | 1 Область применения | р |
| 2 Нормативные ссылки | Обязательный | 2 Нормативные ссылки | р |
| 3 Определения | Обязательный | 3 Термины, определения и сокращения | р |
| 4 Эталонная архитектура | Обязательный | 4 Эталонная архитектура | **т** |
| ПУ1 | Обязательный | 6.3.1 ПУЗ | р |
| ПУ2 | Обязательный | 6.3.1 ПУ1 | р |
| ПУЗ | Обязательный | 6.3.1 ПУ2 | р |
| 5 Связь между характеристиками системы передачи и процедурами безопасности | Обязательный | 7.2.8 | р |
| 5.1 Требование функциональной полноты (текст до Р1) | Обязательный | Не используется |  |
| Р1—Р5 | Обязательный | 7.1 Общие положения | **т** |
| Р6 | Обязательный | 7.2.5 | р |
| 5.2 Требования полноты безопасности R1—R6 | Обязательный | 7.2 Общие требования | **т** |
| 6.1 Общие положения | Обязательный | Не используется |  |
| 6.2 Безопасность оборудования | Обязательный | 7.1 и 7 *2* | **т** |
| 6.3 Передача данных между связанным  и не связанным с безопасностью оборудованием | Обязательный | 7.2.2 | р |
| Обязательный | 7.3.8.2.1 | р |
| 6.4 Передача данных между не связанным с безопасностью оборудованием | Обязательный | Не используется |  |
| 7.1 Общие требования | Обязательный | 7.3.8.2.3 | р |
| 7.2 Цель безопасности | Обязательный | 7.2.5 |  |
| 7.3 Длина кода защиты | Обязательный | 7.3.8.2.4 | р |
| Приложение А Длина кода защиты | Справочный | С.4 Длина кода защиты | **н** |

44

#### ГОСТ Р МЭК 62280—2017

*Окончание таблицы Е. 1*

Н — {не изменен) включают изменения ссылок и изменения терминологии, чтобы достигнуть согласован­ ности всего стандарта:

Р — (редакционные изменения) включают только перестановки и улучшения, но не изменяют содержание; Т — (технические изменения) включают изменения содержания или перемещение его в другие (подпун­

кты.

Таблица Е.2 —Отображение МЭК 62280-2:2002 на настоящий стандарт

|  |  |  |  |
| --- | --- | --- | --- |
| «Поднаймы МЭК 62280-2:2002 | Справочный/ Обязательный | (Под)разд\*лы настоящего стандарт\* | Но «онемей; изменен |
| Введение | Справочный | Введение | р |
| 1 Область применения | Обязательный | 1 Область применения | р |
| 2 Нормативные ссылки | Обязательный | 2 Нормативные ссыгки | р |
| 3 Определения | Обязательна | 3 Термины, определения и сокращения | р |
| 4 Эталонная архитектура | Обязательный | 4 Эталонная архитектура | **т** |
| 5 Угрозы для системы передачи данных | Обязательный | 5 Угрозы для системы передачи данных | **н** |
| 6.1 Введение | Обязательный | 7.1 Общие положения | **н** |
| 6.2 Общие требования | Обязательный | 7.2 Общие требования | **т** |
| 6.3 Конкретные защиты | Обязательный | 7.3 Конкретные защиты | **н** |
| 6.3.1 Поредковый номер | Обязательный | 7.3.2 Порядковый номер | **н** |
| 6.3.2 Временная метка | Обязательный | 7.3.3 Временная метка | **н** |
| 6.3.3 Тайм-аут | Обязательный | 7.3.4 Тайм-аут | **н** |
| 6.3.4 Идентификаторы источника и адресата | Обязательный | 7.3.5 Идентификаторы источника и адресата | **н** |
| 6.3.5 Сообщение обратной связи | Обязательный | 7.3.6 Сообщение обратной связи | **н** |
| 6.3.6 Процедура идентификации | Обязательный | 7.3.7 Процедура иденти­ фикации | **н** |
| 6.3.7 Код защиты | Обязательный | 7.3.8 Код защиты | **т** |
| 6.3.8 Криптографические методы | Обязательный | 7.3.9 Криптографические методы | **т** |
| 7.1 Введение | Обязательный | 7.4.1 Общие положения | **н** |
| 7.2 Матрица угроэ/эащит | Обязательный | 7.4.2 Матрица угроэ/эащит | **н** |
| 7.3 Выбор и использование кода защиты и криптографических методов | Обязательный | 7.4.3 Выбор и использова­ ние кода защиты и крипто­ графических методов | **н** |
| А. 1 Применение меток времени | Справочный | С.1 Применение меток времени | **н** |
| А.2 Выбор и использование ходов защиты и криптографических методов | Справочный | С.2 Выбор и использова­ ние кодов защиты и крип­ тографических методов | **т** |
| Библиография | Справочный | Библиография | **т** |

#### 45

ГОСТ Р МЭК 62280—2017

*Окончание таблицы Е.2*

|  |  |  |  |
| --- | --- | --- | --- |
| (Подразделы МЭК 62280-2.2002 | Слраоечиым/ Обязательный | (Под)ргэдепы настоящего стандарта | Не изменен/ мзыемеи |
| С.1 Область применения/цель | Справочный | 6.1 Общие положения | т |
| С.2 Классификация систем передачи | Справочный | 6.2 Общие аспекты клас­ сификации | т |
| Приложение В. Категории систем передачи | т |
| С.Э Процедура | Справочный | D.1 Процедура | н |
| С.4 Пример | Справочный | D.2 Пример | н |
| Приложение 0. Угрозы в открытых системах передачи | Справочный | Приложение А. Угрозы 8 открытых системах пере­ дачи | р |

Н — (не изменен) включают изменения ссылок и изменения терминологии, чтобы достигнуть согласован­ ности всего стандарта:

Р — (редакционные изменения) включают только перестановки и улучшения, но не изменяют содержание;

Т — (технические изменения) включают изменения содержания или перемещение его в другие (под)гтун-

кты.

46

#### ГОСТ Р МЭК 62280—2017

Приложение ДА (справочное)

#### Сведения о соответствии ссылочных международных стандартов национальным стандартам Российской Федерации

Таблица ДА.1

|  |  |  |
| --- | --- | --- |
| Обозначение ссылочного международного стандарта | Степень соответствия | Обозначение и наименование соответствующею национальною стандарта |
| IEC 62278 (all parts) | — | • |
| IEC 62425:2007 | — | • |
| \* Соответствующий национальный стандарт отсутствует. До его утверждения рекомендуется использовать перевод на русский язык данного международного стандарта. | | |

47

#### ГОСТ Р МЭК 62280—2017

#### Библиография

1. IEC 61025. Fault Tree Analysis (FTA)
2. ISO/IEC 9796-2:2010, Information technology — Security techniques — Digital signature schemes giving message recovery — Part 2: Integer factorization based mechanisms
3. ISO/IEC 9796-3:2006, Information technology — Security techniques — Digital signature schemes giving message recovery — Part 3: Discrete logarithm based mechanisms
4. ISO/IEC 9797-1:2011, Information technology — Security techniques — Message Authentication Codes (MACs)—

Part 1: Mechanisms using a block cipher

1. ISO/IEC 9797-2:2011, Information technology — Security techniques — Message Authentication Codes (MACs) —

Part 2: Mechanisms using a dedicated hash-function

1. ISO/IEC 10116:2006. Information technology — Security techniques — Modes of operation for an n-bit block cipher
2. ISO/IEC 10116-1:2000. Information technology — Security techniques — Hash-functions — Part 1: General
3. ISO/IEC 10118-2:2010, information technology — Security techniques — Hash-functions — Part 2: Hash-functions using an n-bit block cipher
4. ISO/IEC 10118-3:2004, Information technology — Security techniques — Hash-functions — Part3: Dedicated hash- functions
5. ISO/IEC 10118-4:1998, Information technology — Security techniques — Hash-functions — Part 4: Hash-functions using modular arithmetic
6. ISO/IEC 11770-1:2010. Information technology — Security techniques — Key management — Part 1: Framework
7. ISO/IEC 11770-2:2008, Information technology — Security techniques — Key management — Part 2: Mechanisms using symmetric techniques
8. ISO/IEC 11770-3:2008. Information technology — Security techniques — Key management — Pari 3: Mechanisms using asymmetric techniques
9. UIC 738, Processing and transmission of safety information
10. UIC/ORE A155.1 Report RP 4. September 1984: Survey of available measures for protection of safety information during transmission (also available in German and French)
11. FIPS PUB 197, 26.11.2001: Advanced Encryption Standard
12. W.Wesley Peterson, Error correction Codes. M.l.T. Press. 1967

#### 48

ГОСТ Р МЭК 62280—2017

УДК 62-783:614:006.354 ОКС 45.060 Группа TS1

Ключевые слова: железнодорожная электросвязь, методы контроля, уровень полноты безопасности, системы передачи, безопасная передача данных

49

БЗ 8-2017/27

Редактор *А.Ф. Катин*

Технически редактор *И.Е.* Черепкова Корректор *ЕЮ.* Митрофанова Компьютерная верстка *ЕЛ. Кондрашовой*

**Сдано в набор 20.07.2017. Подписано в печать 03.08 2017. Формат 60\*04%. Гарнитура Ариал.**

**Уел. печ. л. 6.05. Уч.-иэд. л. 5.47. Тирах 27 экэ. Зак. >266**

**Подготовлено на основе электронной версии, предоставленной разработчиком стандарта**

**Издано и отпечатано во ФГУП «СТАНДАРТИНФОРМ». 12300! Москва. Гранатный пер.. 4.** [**www.goslinfo.ru**](http://www.goslinfo.ru/) [**info@gos**1**info.ru**](mailto:info@gos1info.ru)