ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 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

Москва
Стандартинформ
2017

gost.e-ecolog.ru

Предисловие

1 ПОДГОТОВЛЕН Обществом с ограниченной ответственностью «Корпоративные электронные системы» на основе собственного перевода на русский язык англоязычной версии стандарта, указанного в пункте 4

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 058 «Функциональная безопасность»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 18 июля 2017 г. № 716-ст

4 Настоящий стандарт идентичен международному стандарту МЭК 62280:2014 «Железные дороги. 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 международного стандарта для приведения в соответствие с ГОСТ Р 1.5 (подраздел 6).

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

5 ВВЕДЕН ВПЕРВЫЕ

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

© Стандартинформ, 2017

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

Содержание

1 Область применения 1
2 Нормативные ссылки 2
3 Термины, определения и сокращения 2
3.1 Термины и определения 2
3.2 Сокращения 5
4 Эталонная архитектура 6
5 Угрозы для системы передачи данных 7
6 Классификация систем передачи данных 9
6.1 Общие положения 9
6.2 Общие аспекты классификации 9
6.3 Критерии классификации систем передачи 10
6.4 Системы передачи и угрозы 10
7 Требования к защите 11
7.1 Общие положения 11
7.2 Общие требования 11
7.3 Конкретные защиты 12
7.4 Применимость защит 17
Приложение А (справочное) Угрозы в открытых системах передачи 19
Приложение В (справочное) Категории систем передачи 26
Приложение С (справочное) Руководство по применению средств защиты 28
Приложение D (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

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 соответствии с МЭК 62425.

Система передачи, рассматриваемая в настоящем стандарте, которая обеспечивает передачу информации между различными компонентами оборудования системы, в общем случае не должна удовлетворять 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 связанной 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 сложность подхода при рассмотрении системы безопасности, системы передачи были разделены на следующие 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 несанкционированный доступ может быть исключен.

Категория 3 состоит из систем, которые не являются объектом управления разработчика и где несанкционированный 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 соответствии с указанными выше стандартами, обслуживаются и/или расширяются, то может быть использовано приложение Е для обеспечения согласованности (под)разделов настоящего стандарта с (под)разделами указанных выше стандартов.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ЖЕЛЕЗНЫЕ ДОРОГИ

Системы связи, сигнализации и обработки данных. Требования к обеспечению безопасной передачи информации

Railway applications. Communication, signalling and processing systems. Safety communication requirements

Дата введения — 2019—07—01

1 Область применения

Настоящий стандарт применим к связанным с безопасностью электронным системам, использующим 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 безопасностью оборудованию.

Настоящий стандарт устанавливает основные требования, необходимые для обеспечения связанной с безопасностью передачи данных между связанным с безопасностью оборудованием, соединенным системой передачи.

Настоящий стандарт применим при составлении спецификации требований безопасности связанного 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 подтверждение безопасности определено в МЭК 62425. Подтверждение менеджмента безопасности и менеджмента качества должно быть выполнено в соответствии с МЭК 62425. Настоящий стандарт рассматривает требования, связанные с передачей данных для подтверждения функциональной и технической безопасности.

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

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

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.

2 Нормативные ссылки

В настоящем стандарте используются нормативные ссылки на следующие целые документы или на их части, незаменимые для применения данного документа. В случае датированных ссылок действует только цитируемое издание. Для недатированных ссылок действует самое позднее издание документа, 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)

3 Термины, определения и сокращения

3.1 Термины и определения

В настоящем стандарте используются следующие термины и определения.

3.1.1 **абсолютная временная метка** (absolute time stamp): Временная метка, связанная с глобальным временем, которое является общим для группы объектов, использующих систему передачи.

3.1.2 **защита доступа** (access protection): Процессы, разработанные для предотвращения несанкционированного доступа при чтении или изменении информации либо в системах, связанных с безопасностью, либо в системе передачи.

3.1.3 **дополнительные данные** (additional data): Данные, которые не используются в процессах конечного пользователя, но используются для целей управления, готовности и безопасности.

3.1.4 **подлинное сообщение** (authentic message): Сообщение, о котором известно, что содержащаяся в нем информация сформирована в известном источнике.

3.1.5 **подлинность** (authenticity): Свойство, характеризующее действительность информации и указывающее на то, что источник ее формирования известен.

3.1.6 **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 незначительным.

3.1.7 **связь** (communication): Передача информации между приложениями.

3.1.8 **конфиденциальность** (confidentiality): Свойство, при котором информация недоступна или закрыта для неавторизованных лиц, субъектов или процессов.

3.1.9 **поврежденное сообщение** (corrupted message): Сообщение, содержащее ошибки, из-за которого происходит повреждение данных.

3.1.10 **криптографические методы** (cryptographic techniques): Метод вычисление выходных данных по некоторому алгоритму, используя входные данные и ключ в качестве параметра.

Примечание — Зная выходные данные, 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.

3.1.11 **циклическая избыточная проверка** (cyclic redundancy check): Циклический процесс проверки, используемый для защиты сообщения от влияния повреждения данных.

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

Примечание — См. также определения 3.1.64 — пользовательские данные, 3.1.3 — дополнительные данные и 3.1.42 — избыточные данные.

3.1.13 **повреждение данных** (data corruption): Изменение данных.

3.1.14 **защита** (defence): Мера, включенная в проект связанной с безопасностью системы связи, для противодействия определенным угрозам.

3.1.15 **задержанное сообщение** (delayed message): Тип ошибки сообщения, при которой сообщение получено на один период позже, чем было предназначено.

3.1.16 **удаленное сообщение** (deleted message): Тип ошибки сообщения, при которой сообщение удалено из потока сообщения.

3.1.17 **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.

3.1.18 **ошибка** (error): Отклонение от намеченного проекта, которое может привести к непреднамеренному поведению системы или отказу.

3.1.19 **отказ** (failure): Отклонение от установленного функционирования системы.

Примечание — Отказ является следствием сбоя или ошибки в системе.

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

Примечание — Сбой может быть случайным или систематическим.

3.1.21 **сообщение обратной связи** (feedback message): Ответ от получателя к отправителю, через обратный канал.

3.1.22 **хакер** (hacker): Лицо, пытающееся преднамеренно обойти защиту доступа.

3.1.23 **опасность** (hazard): Условие, которое может привести к несчастному случаю.

3.1.24 **анализ опасности** (hazard analysis): Процесс идентификации опасностей и анализа их причин, а также формирование требований, ограничивающих вероятность и последствия опасностей до приемлемого уровня.

3.1.25 **неявные данные** (implicit data): Дополнительные данные, которые не передаются, но известны отправителю и получателю.

3.1.26 **информация** (information): Представление состояния или события процесса в форме «понятной» процессу.

3.1.27 **вставленное сообщение** (inserted message): Тип ошибки сообщения, при которой в поток сообщения вставляется дополнительное сообщение.

3.1.28 **целостность** (integrity): Состояние, в котором информация полна и не изменяется.

3.1.29 **код обнаружения манипуляций** (manipulation detection code): Функция от полного сообщения без секретного ключа.

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

3.1.30 **(подмененное) сообщение, выдающее себя за другое сообщение** (masqueraded message): Тип вставленного сообщения, в котором создано недостоверное сообщение, которое кажется достоверным.

3.1.31 **сообщение** (message): Информация, которая передана от отправителя (источника данных) к одному или более получателям (приемнику данных).

3.1.32 **код аутентификации сообщений** (message authentication code): Криптографическая функция полного сообщения и секретного или открытого ключа.

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

3.1.33 **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.

3.1.34 **ошибки, связанные с сообщением** (message errors): Набор всех возможных видов отказов сообщения, которые могут привести к потенциально опасным ситуациям, или к сокращению готовности системы. Каждый тип ошибки может иметь много причин.

3.1.35 **целостность сообщения** (message integrity): Сообщение, в котором информация полна и не изменяется.

3.1.36 **поток сообщений** (message stream): Упорядоченное множество сообщений.

3.1.37 **не криптографический код защиты** (non-cryptographic safety code): Избыточные данные на основе не криптографических функций, включенные в связанное с безопасностью сообщение и обеспечивающие обнаружение поврежденных данных с помощью связанной с безопасностью функции передачи.

3.1.38 **открытая система передачи** (open transmission system): Система передачи с неизвестным числом участников, с неизвестными, переменными и не доверенными свойствами, используемая для неизвестных телекоммуникационных услуг и обладающая возможностью несанкционированного доступа.

3.1.39 **сеть общего пользования** (public network): Сеть с неизвестными пользователями, в частности, не находится под управлением железных дорог.

3.1.40 **случайный отказ** (random failure): Отказ, который происходит в произвольный момент времени.

3.1.41 **проверка на избыточность** (redundancy check): Тип проверки, которая выявляет наличие предопределенной связи между избыточными данными и данными пользователя в сообщении, чтобы доказать целостность сообщения.

3.1.42 **избыточные данные** (redundant data): Дополнительные данные, сформированные связанной с безопасностью функцией передачи для данных пользователя.

3.1.43 **относительная метка времени** (relative time stamp): Метка времени, на которую ссылаются локальные часы объекта. В общем случае не существует никакой связи с часами других объектов.

3.1.44 **повторное сообщение** (repeated message): Тип ошибки сообщения, при которой одно сообщение получено несколько раз.

3.1.45 **переупорядоченное сообщение** (re-sequenced message): Тип ошибки сообщения, при которой изменен порядок сообщений в потоке сообщений.

3.1.46 **безопасное состояние с пониженной скоростью передачи данных** (safe fall 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.

3.1.47 **безопасность** (safety): Отсутствие неприемлемых уровней риска.

3.1.48 **доказательство безопасности** (safety case): Документированное подтверждение того, что изделие (например, система/подсистема/оборудование) соответствует заданным требованиям безопасности на этапах жизненного цикла.

3.1.49 **код защиты** (safety code): Избыточные данные, включенные в связанное с безопасностью сообщение, обеспечивающие выявление поврежденных данных связанной с безопасностью функцией передачи.

3.1.50 **уровень полноты безопасности** (safety integrity level): Число, которое указывает требуемую степень достоверности, что система будет выполнять свои заданные функции безопасности по отношению к систематическим отказам.

3.1.51 **реакция безопасности** (safety reaction): Связанная с безопасностью защита, реализуемая процессом безопасности в ответ на событие (такое, как отказ системы передачи), которое может привести к нарушению безопасного состояния оборудования.

3.1.52 **связанный с безопасностью** (safety related): Отвечающий за безопасность.

3.1.53 **связанная с безопасностью функция передачи** (safety related transmission function): Функция связанного с безопасностью оборудования, гарантирующая достоверность, целостность, актуальность и последовательность данных.

3.1.54 **порядковый номер** (sequence number): Дополнительное поле данных, содержащее число, которое изменяется предопределенным способом от сообщения к сообщению.

3.1.55 **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 использоваться для связанной с безопасностью передачи. Обычно идентификатор добавляется к данным пользователя.

3.1.56 **систематический отказ** (systematic failure): Отказ, который неоднократно повторяется при некоторой определенной комбинации входов или для некоторых определенных состояний окружающей среды.

3.1.57 **угроза** (threat): Потенциальное нарушение безопасности.

3.1.58 **временная метка** (time stamp): Информация о времени передачи, присоединенная к сообщению отправителем.

3.1.59 **актуальность** (timeliness): Состояние, в котором информация доступна в нужное время в соответствии с требованиями.

3.1.60 **код передачи** (transmission code): Дополнительная информация, которая добавляется к связанному и не связанному с безопасностью сообщению незащищенной системы передачи и гарантирует целостность сообщения во время передачи.

3.1.61 **система передачи** (transmission system): Служба, используемая приложением для передачи потоков сообщений между несколькими участниками, которые могут быть источниками или приемниками информации.

3.1.62 **доверенный** (trusted): Обладающий свойствами, которые используются в качестве доказательства при обеспечении демонстрации безопасности.

3.1.63 **несанкционированный доступ** (unauthorised access): Ситуация, в которой к информации пользователя или к информации в системе передачи имеют доступ и/или ее изменяют лица, не наделенные полномочиями, или хакеры.

3.1.64 **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.

3.1.65 **подтвержденное сообщение** (valid message): Сообщения, форма которых во всех отношениях удовлетворяет заданным требованиям пользователя.

3.1.66 **достоверность** (validity): Состояние, которое во всех отношениях удовлетворяет заданным требованиям пользователя.

3.2 Сокращения

BCH — код Bose, Ray-Chaudhuri, Hocquenghem;

BME — основные ошибки сообщений;

BSC — симметричный канал для передачи двоичных данных;

CAN — локальная сеть контроллеров;

CRC — циклическая проверка чётности с избыточностью;

EC — Европейское сообщество;

ECB — метод прямого шифрования;

EMI — электромагнитные помехи;

FTA — анализ дерева отказов;

GPRS — система пакетной радиосвязи общего пользования;

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

HE — 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;

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;
TX — передача (данных);
UTC — всемирное координированное время;
WAN — глобальная сеть передачи данных;
Wi-Fi — торговая марка для сетей на базе IEEE 802.11.

4 Эталонная архитектура

Настоящий стандарт определяет требования безопасности для безопасной коммуникации между связанным с безопасностью оборудованием через систему передачи, которая может быть либо закрытой, 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 в системах передачи, включая определение передаваемых функциональных блоков. Далее будут определены конкретные требования, которым должны удовлетворять эти блоки.

Общее представление (для открытой и закрытой системы передачи) основной архитектуры показано 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 техобслуживания.

Помимо источника и пункта назначения связанной с безопасностью коммуникации эталонная архитектура представляет связанную с безопасностью систему коммуникации, которая может быть разделена на:

- связанные с безопасностью функции передачи, выполняемые на связанном с безопасностью оборудовании. Эти функции гарантируют достоверность, целостность, актуальность и последовательность данных,
- связанные с безопасностью криптографические методы, которые защищают связанное с безопасностью сообщение. Они могут быть реализованы или в связанном с безопасностью оборудовании, или вне этого оборудования, но должны быть проверены методами безопасности. Эти методы защищают 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 связанных) 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 пользователю. Число пользователей обычно также неизвестно, и с открытой системой передачи может быть соединено связанное и не связанное с безопасностью оборудование и оборудование, которое не связано с железнодорожными применениями;

- среды передачи любого типа с характеристиками передачи и чувствительностью к внешним влияниям, которые неизвестны пользователю;

- системы управления сетью и системы менеджмента выполняют маршрутизацию (и динамическое изменение маршрута), обмениваются сообщениями по любому пути, сформированному в среде передачи одного типа или в средах передачи нескольких типов между концами открытой системы передачи 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. примеры в приложении С и в частности С.5 для не связанных с безопасностью сообщений.

5 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 системе передачи, для этих свойств сообщения. Угрозы связанного с безопасностью оборудования необходимо 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 должен 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.

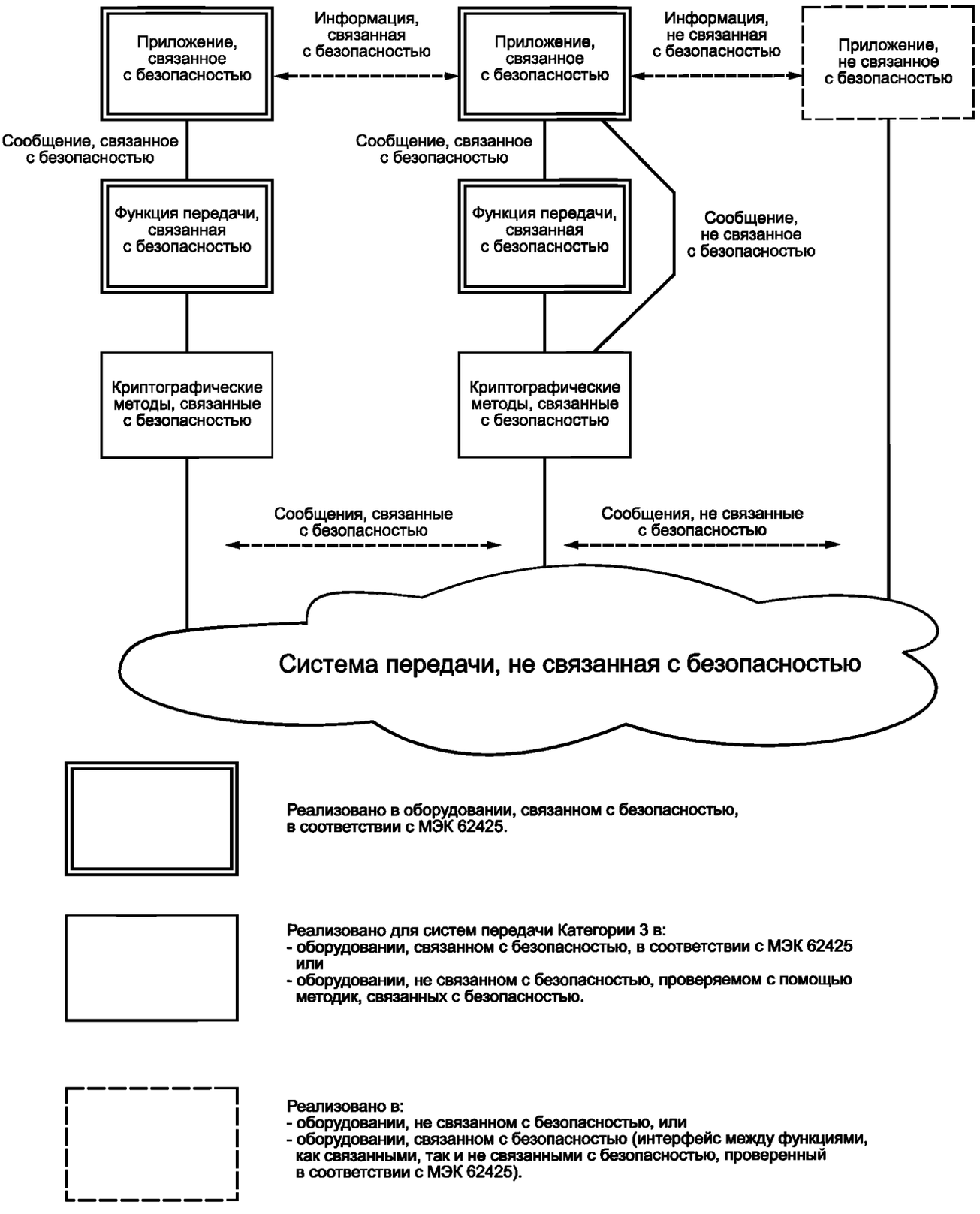


Рисунок 1 — Эталонная архитектура для связанной с безопасностью передачи данных

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 качестве руководства для идентификации угроз, которые должны быть рассмотрены для этой системы.

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

6 Классификация систем передачи данных

6.1 Общие положения

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

6.2 Общие аспекты классификации

Существует много факторов, которые могут влиять на угрозы связанной с безопасностью коммуникационной системе.

Например, возможно, что услуги передачи могут быть оказаны пользователю системы сигнализации от частных или общедоступных телекоммуникационных поставщиков услуг. В соответствии с такими контрактами по предоставлению услуг ответственность поставщика услуг за обеспечение гарантированной производительности системы передачи может быть ограничена.

Поэтому значение угроз (и, следовательно, требования к защите от них) зависит от осуществляемой пользователем степени управления системой передачи, включая следующие вопросы:

- технические свойства системы, включая гарантии надежности или доступности к системе, уровень хранения данных, существующий в системе (который может влиять на задержку или переупорядочивание сообщений);
- стабильность производительности системы на всем времени ее эксплуатации (например, вследствие выполнения изменений в системе и изменений в базе данных пользователя), а также влияние загрузки 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 обслуживанию для реконфигурирования системы или получение доступа к самой среде передачи.

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

6.3 Критерии классификации систем передачи

6.3.1 Критерии системы передачи Категории 1

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

ПУ1. Число единиц подсоединяемого оборудования (или связанного, или не связанного с безопасностью) к системе передачи известно и фиксировано. Поскольку связанная с безопасностью коммуникация 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 доказательство безопасности. Любому последующему изменению этой конфигурации должен предшествовать анализ его влияния на доказательство безопасности.

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

ПУ3. 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 соответствовать обычно сокращенному набору процессов и требований, представленных в разделе 7.

6.3.2 Критерии системы передачи Категории 2

Если система передачи не удовлетворяет ПУ1 или ПУ2 из 6.3.1, но удовлетворяет ПУ3, 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.

6.3.3 Критерии системы передачи Категории 3

Если система передачи не удовлетворяет ПУ3 из 6.3.1, то можно считать, что она имеет Категорию 3 и является открытой системой, поэтому ее необходимо оценивать полным набором процессов и требований, представленных в разделе 7.

6.4 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 исключением 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 угроза/категория.

Применимость раздела 7 зависит от категории системы передачи.

7 Требования к защите

7.1 Общие положения

Ранее для систем передачи данных (связанных и не связанных с безопасностью) были предложены определенные методы защиты от угроз. Эти методы представляют «библиотеку» возможных методов, которые доступны для разработчика систем управления и защиты и используются для обеспечения 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 применения, следующие фундаментальные службы безопасности, обеспечивающие:

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

Был выделен следующий набор известных методов защиты:

a) порядковый номер;
b) временная метка;
c) тайм-аут;
d) идентификаторы источника и пункта назначения;
e) сообщение обратной связи;
f) процедура идентификации;
g) 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 Категории 1 или 2 предварительным условиям;
- критерии разделения систем передачи различных категорий между собой;
- устойчивость систем передачи к отказу в обслуживании, возникающего в результате информационных 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 связанные 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.

7.2 Общие требования

7.2.1 Должны быть обеспечены соответствующие средства защиты от всех определенных выше угроз безопасности для систем, использующих открытую или закрытую систему передачи. Любые предположения угроз, которые игнорируются, должны быть обоснованы и зарегистрированы в доказательстве безопасности. В приложении А представлен возможный список угроз, который можно использовать в качестве руководства.

7.2.2 Если реализуется коммуникация между приложениями, связанными с безопасностью, и приложениями, не связанными с безопасностью, через одну и ту же систему передачи данных, то применяют следующие требования:

- для защит безопасности, реализуемых связанными с безопасностью функциями передачи, должно быть продемонстрировано, что они являются функционально независимыми от защит, реализуемых 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

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

7.2.3 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 защиты от угроз. При выборе защиты необходимо тщательно проанализировать вопросы эффективности, рассмотренные в этом приложении.

7.2.4 Требования к необходимым защитам должны быть включены в спецификацию требований к системе и в спецификацию требований безопасности системы для определенного приложения и должны сформировать исходную информацию для раздела «Обеспечение правильной работы» доказательства безопасности для этого приложения.

7.2.5 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 возможным исключением некоторой криптографической архитектуры, см. 7.3.9 и С.2);
- будут функционально независимы от уровней, используемых в незащищенной системе передачи данных.

7.2.6 В последующих подразделах даны обязательные требования для конкретных защит. Они применяются, если эта конкретная защита используется.

7.2.7 Кроме описанных в настоящем стандарте, могут использоваться другие защиты, при условии, что анализ их эффективности противостоять угрозам включен в доказательство безопасности.

7.2.8 Доказательство функциональной и технической безопасности должно выполняться в соответствии 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.

7.2.9 Подраздел 7.3 определяет исчерпывающий набор защит. Однако, для систем передачи Категории 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.

7.3 Конкретные защиты

7.3.1 Общие положения

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

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

7.3.2 Порядковый номер

7.3.2.1 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.

7.3.2.2 Требования

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

- длину порядкового номера;

- условие для инициализации и преобразования порядкового номера;
- условие восстановления после прерывания последовательности сообщений.

7.3.3 Временная метка

7.3.3.1 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 в других случаях информация может быть потенциально опасной для пользователя. В зависимости от поведения процессов во времени, 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 добавлять 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.

7.3.3.2 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.

7.3.4 Тайм-аут

7.3.4.1 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.

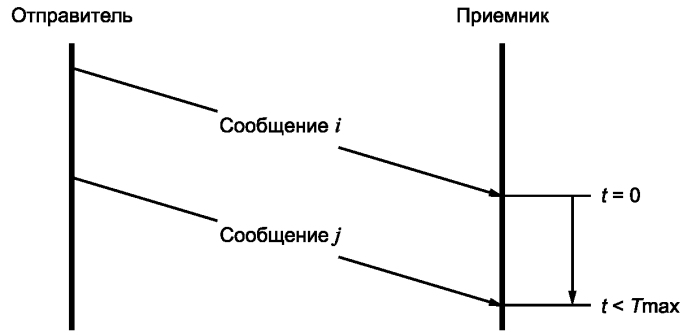


Рисунок 2 — Циклическая передача сообщений

Если обратный канал доступен, то отправителем может быть выполнен контроль. Отправитель запускает таймер, посылая сообщение *i*. Приемник сообщения *i* отвечает сообщением подтверждения *j*, связанным с полученным сообщением *i*. Если отправитель не получает сообщение подтверждения *j* в течение предопределенного времени, то предполагается ошибка (см. рисунок 3).

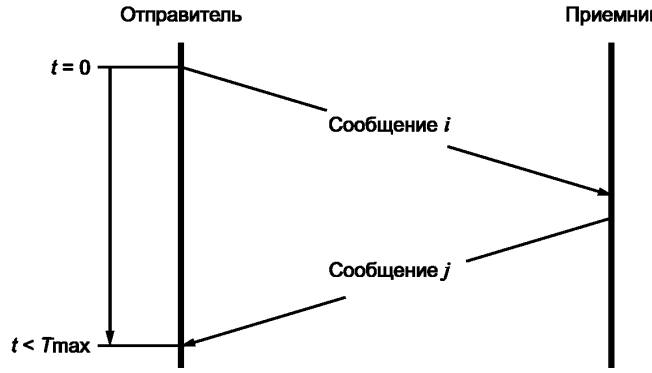


Рисунок 3 — Двунаправленная передача сообщений

7.3.4.2 Требования

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

- приемлемую задержку;
- точность тайм-аута.

7.3.5 Идентификаторы источника и адресата

7.3.5.1 Общие положения

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

Сообщения могут содержать уникальный идентификатор источника, или уникальный идентификатор 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 сообщений 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 сообщений 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 места назначения или группы пользователей.

7.3.5.2 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.

7.3.6 Сообщение обратной связи

7.3.6.1 Общие положения

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

- 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.

7.3.6.2 Требования

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

7.3.7 Процедура идентификации

7.3.7.1 Общие положения

Предыдущий пункт касался требований для объектов, которые будут идентифицированы.

Открытые системы передачи могут дополнительно увеличивать риск сообщениями от других (неизвестных) 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 отправителями и получателями информации может обеспечить дополнительную гарантию, что передача действительно выполняется между предназначенными сторонами.

Процедуры динамической идентификации

Динамический обмен информацией между отправителями и получателями, включая преобразование и обратную связь полученной информации к отправителю, может обеспечить гарантию, что связывающиеся стороны не только «заявляют», что обладали корректными идентификационными данными, 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.

7.3.7.2 Требования

Процедура идентификации является частью связанного с безопасностью прикладного процесса. Подробные требования должны быть определены в спецификации требований безопасности.

7.3.8 Код защиты

7.3.8.1 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 методами 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 защиты, 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 систематическими отказами;
- вероятность обнаружения случайных отказов в поврежденных сообщениях.

Примечание — Код защиты может быть комбинацией различных кодов, например, линейного кода, объединенного с постоянным значением.

Указания по выбору кодов защиты даны в С.3, приложение С.

7.3.8.2 Требования

7.3.8.2.1 Код защиты должен отличаться от кода передачи, если целостность сообщения не будет обеспечена исключительно кодом защиты. Это различие может быть получено:

- или с помощью различных алгоритмов, или
- с помощью различных параметров конфигурации (например, полиномов) для тех же алгоритмов. Если оба кода будут основываться на CRC, то полиномы должны различаться. Если у обоих полиномов 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.

7.3.8.2.2 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 обнаружены. Поэтому код защиты должны быть более сложными, чем ожидаемые отказы. Следовательно, можно предположить, что отказ аппаратных средств в незащищенной системе передачи не может генерировать достоверный код защиты.

7.3.8.2.3 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.

7.3.8.2.4 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 недвоичный 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 защиты, 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, приложение С).

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

7.3.9 Криптографические методы

7.3.9.1 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 приложения сообщения, связанные с безопасностью, должны быть защищены криптографическими методами.

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

a) использование кода защиты в состоянии обеспечить криптографическую защиту;

b) шифрование сообщений после формирования кода защиты;

c) 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 эффективности этих методов зависит от эффективности алгоритмов и обеспечения секретности ключей. Секретность ключа зависит от его длины и управления им.

7.3.9.2 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 процессов, 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 технических 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 методы (например, согласно серии ИСО/МЭК 11770).

7.4 Применимость защит

7.4.1 Общие положения

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

7.4.2 Матрица угроз/защит

В 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.

Таблица 1 — Матрица угроз и средств защиты

Угрозы	Средства защиты							
	Порядковый номер	Временная метка	Тайм-аут	Идентификаторы источника и адресата	Сообщение обратной связи	Процедура идентификации	Код защиты	Криптографические методы
Повторение	X	X						
Стирание	X							
Вставка	X			X[a)]	X[b)]	X[b)]		
Переупорядочивание	X	X						
Повреждение							X[c)]	X
Задержка		X	X					
Подмена					X[b)]	X[b)]		X[c)]

[a)] 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.

[b)] Зависит от приложения.

[c)] См. 7.4.3 и С.2, приложение С.

7.4.3 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.

Приложение А
(справочное)

Угрозы в открытых системах передачи

А.1 Представление системы

Угрозы сообщениям, отправленным по каналу системой управления и системой защиты, происходят в результате возможных изменений в работе канала, которые могут возникнуть либо при нормальных условиях (например 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 в 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 (MH), которая является отказом в получении подтвержденного сообщения в терминах аутентификации, целостности, последовательности и своевременности на стороне получения.

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

Установление соответствующих угроз, рассматриваемых как виды отказа сети (т. е. основных ошибок сообщения с точки зрения сети), выполняется просто. Угроза — это 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. Следовательно, отношение основная угроза — ошибка сообщения имеет вид 1:1.

В свою очередь, угроза может быть сгенерирована рядом причин, названных опасными событиями (HE), 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.

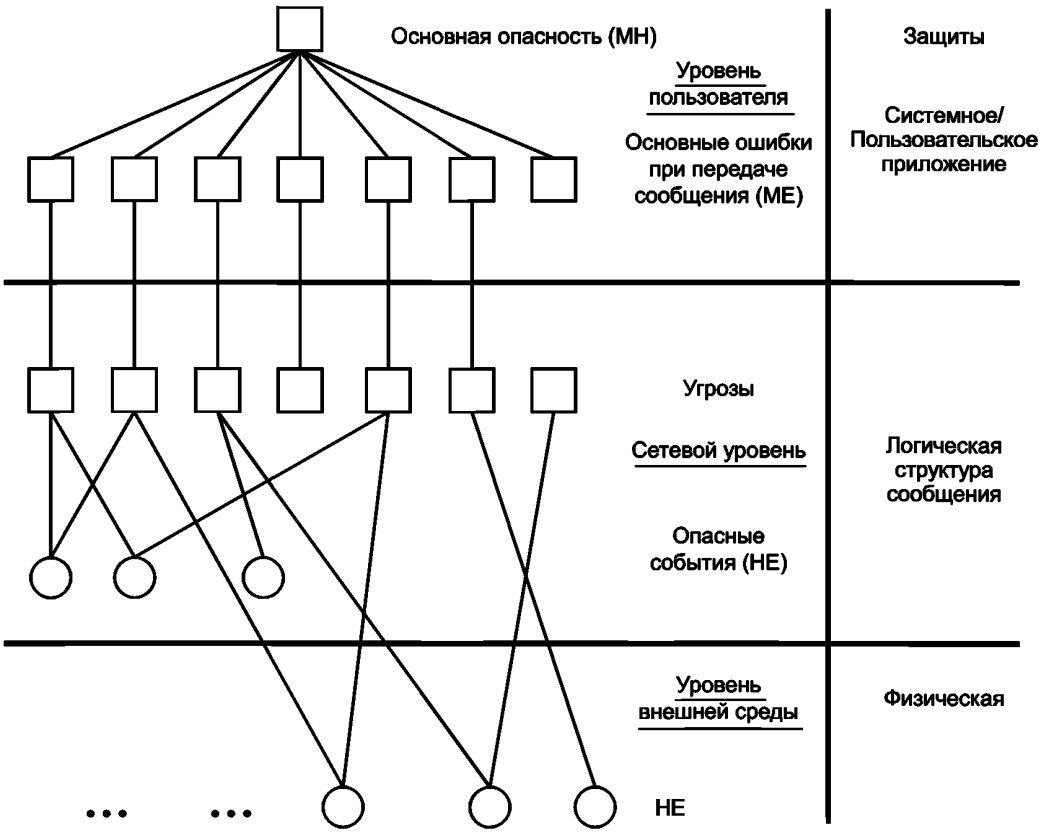


Рисунок А.1 — Дерево опасности

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

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

b) одна защита, связанная с логической структурой сообщения, например все возможные коды, которые могут 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 электромагнитных помех.

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

A.2 Установление основных ошибок при передаче сообщений

Сообщение — основной предмет всего анализа, поэтому процесс передачи данных был изучен с точки зрения получателя. Сообщение может быть определено как «полезная информация, порожденная источником, которая доставляется за время Δt 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 каждого временного окна 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 сообщений, чем ожидалось

В этом случае одно или более сообщений были получены повторно, или внешнее сообщение было вставлено в канал передачи. Поэтому основные ошибки сообщения — повторные и вставленные сообщения.

Получено меньше сообщений, чем ожидалось

В этом случае одно или более сообщений было удалено. Поэтому основные ошибки сообщения — удаленные сообщения.

То 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 последовательность передачи — произошло переупорядочивание;
- сообщение в потоке достигло получателя за время больше, чем номинальное значение Δt — произошла задержка;
- сообщение было изменено — произошло повреждение сообщения;
- получатель полагает, что отправитель сообщения отличается от истинного отправителя — произошла подмена.

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. Возможно, что большое количество сообщений в потоке и даже одиночное сообщение оказываются под воздействием более чем одного вида ошибки.

A.3 Угрозы

A.3.1 Общие положения

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

Пусть A, B и C будут тремя уполномоченными сторонами, которые передают связанные с безопасностью сообщения, в то время как *X* предпринимает атаку.

Необходимо отметить, что случайные и систематические отказы аппаратных средств или программного обеспечения также 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, когда 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 скорость: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 Переупорядочивание

- *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 корректное сообщение или
- *X* изменяет сообщение [«Максимальная скорость: 30 км/ч» на «Максимальная скорость: 250 км/ч»] правдоподобным способом так, чтобы А и/или В не смогли обнаружить изменение.

А.3.7 Задержка

- Система передачи перегружена нормальным трафиком (например, из-за неправильного проекта или случайно большого трафика) или
- *X* создает перегрузку в системе передачи, генерируя поддельные сообщения так, чтобы этот сервис выполнялся 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 доступ 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, которому 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), взаимодействующей 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 системе. Объект Network декомпозирован согласно нескольким шагам его жизненного цикла, в то время как объект External environment делится на две группы возможных характеристик, которые связаны с физическими процессами и с человеком.

Листья дерева на рисунке А.2 представляют причины опасностей: для каждой причины определены соответствующие 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 исчерпывающее: во время анализа опасности некоторые другие опасные события могут быть учтены в зависимости от конкретного приложения.

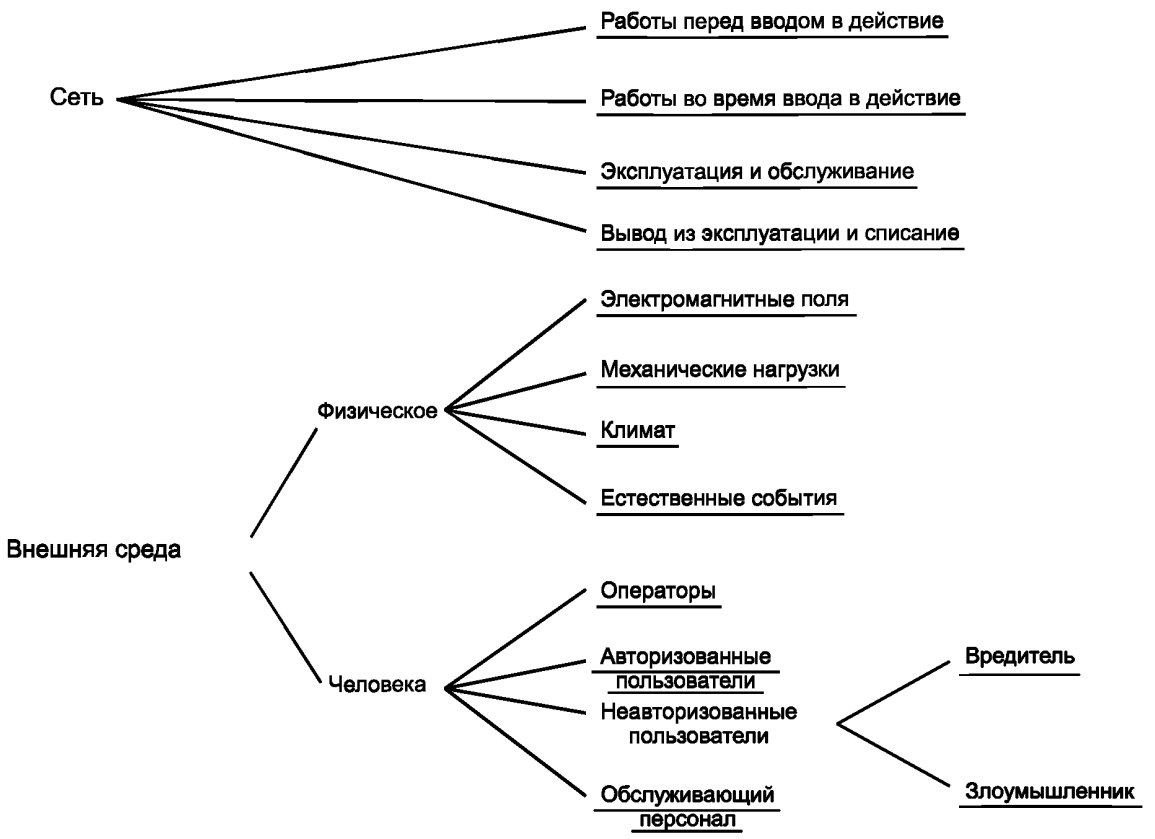


Рисунок А.2 — Причины угроз

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 настоящего 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 требования, 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 эксплуатационных характеристик компонентов системы и из-за ошибок во время ремонта и/или модификаций:

- ухудшение эксплуатационных характеристик;
- случайный отказ аппаратных средств;
- старение аппаратных средств.

А.4.2.2.5 Обслуживание
- использование некалиброванных инструментов;
- использование неподходящих инструментов;
- некорректная замена аппаратных средств;
- некорректное обновление или замена программного обеспечения.

А.4.2.2.6 Модификация
- эффекты замирания;
- ошибки человека[1)].

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[1)].

А.4.2.3.6 Авторизованные пользователи
- ошибки человека[1)];
- перегрузка системы передачи.

А.4.2.3.7 Обслуживающий технический персонал
- использование некалиброванных инструментальных средств;
- использование неподходящих инструментальных средств;
- замена некорректно работающих аппаратных средств;
- ошибки человека[1)];
- 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 Злоумышленник[2)]
- 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 является построение отношений между ними и угрозами, кратко рассмотренными в А.3, используя восходящий метод[3)]. Цель состоит в том, чтобы проверить, что никакая дополнительная угроза не обнаружена, что 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 нарушает 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.

Как видно, никакая дополнительная угроза не была обнаружена после анализа каждого опасного события. Это доказывает, что список в разделе А.3 является исчерпывающим.

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

А.5 Резюме

Были определены два различных подхода для получения набора возможных угроз для связанных с безопасностью коммуникаций в системах передачи. Первый — нисходящий метод, начинающийся с основной опасности и заканчивающийся классификацией всех возможных опасных событий, приводящих к опасности. Второй — начинается с определения двух основных объектов рассматриваемой системы (т. е. сеть и внешняя среда), чтобы классифицировать 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 угроз, поэтому оба подхода могут использоваться для анализа опасностей в открытых системах передачи.

Таблица А.1 — Связь между опасными событиями и угрозами

Опасные события	Угрозы						
	Повторение	Удаление	Вставка	Переупорядочивание	Повреждение	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 некалиброванных 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	

Окончание таблицы А.1

Опасные события	Угрозы						
	Повторение	Удаление	Вставка	Переупорядочивание	Повреждение	Задержка	Подмена
Тайное прослушивание телефонных разговоров	X	X	X		X	X	
Повреждение или останов аппаратных средств		X				X	
Несанкционированные изменения программного обеспечения	X	X	X		X	X	X[a)]
Передача несанкционированных сообщений	X		X				X[a)]
Контроль каналов[b)]							

[a)] В этом случае сообщение является злонамеренным с самого начала; поэтому необходима серьезная защита, например использование ключа.

[b)] 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.

Приложение В
(справочное)

Категории систем передачи

В.1 Категории систем передачи

В 6.3 определено три категории систем передачи.

Категория 1. Закрытые системы передачи, в которых все основные свойства системы находятся под управлением 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 которых 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 конфигураций.

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 фиксированного максимального числа участников. Все свойства системы передачи известны и постоянны на протяжении времени жизни системы. Наличие незначительной возможности для несанкционированного доступа	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, определенная в МЭК)]. Стандартная LAN, соединяющая различное оборудование (связанное и несвязанное с безопасностью) в единую систему с учетом выполнения и поддержки предварительных условий
Категория 2	Свойства неизвестны, частично неизвестны или изменяются на протяжении времени жизни системы. Возможности для расширения группы пользователей ограничены. Группа или группы пользователей известны. Существуют незначительные возможности для несанкционированного доступа (сети надежны). Случайное использование ненадежных 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 управляемой и ограниченной зоне. WAN, принадлежащая железной дороге, соединяющая различные системы (связанные и не связанные с безопасностью) на различных участках. Коммутируемая линия в общедоступной телефонной сети, используемая случайно и в непредсказуемые моменты времени (например, коммутируемая удаленная диагностика системы централизации). Постоянно арендованный канал прямой связи в общедоступной телефонной сети.

Окончание таблицы В.1

Категория	Основные характеристики	Пример систем передачи
		Система радиопередачи с ограниченным доступом (например, использование волноводов или излучающих кабелей с энергетическим бюджетом канала, ограничивающим возможность приема только ближайшей радиостанцией или использование собственной схемы модуляции, не позволяющей воспроизведение сообщений с помощью серийно выпускаемого или доступного по цене лабораторного оборудования)
Категория 3	Свойства неизвестны, частично неизвестны или изменяются на протяжении времени жизни системы. Неизвестны группы многочисленных пользователей. Наличие благоприятных возможностей для несанкционированного доступа	Система передачи данных с пакетной коммутацией в общедоступной телефонной сети. Интернет. Радиоканал передачи данных с коммутацией каналов (например, GSM-R). Радиоканал передачи данных с коммутацией пакетов (например, 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	Удаление	Вставка	Переупорядочивание	Повреждение	Задержка	Подмена
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.

Приложение С
(справочное)

Руководство по применению средств защиты

С.1 Применения меток времени

Метка времени может быть использована в различных целях.

a) Для установления времени события в объекте, которое является важным для процесса получения информации. События могут быть связаны друг с другом по времени. Если известны моменты времени и значения для последовательности событий, то можно интерполировать значения и увеличить точность расчетных значений (например, для скорости, ускорения). Могут быть обработаны задержки передачи.

Ограничения:

- если используется абсолютная метка времени, то время в объектах должно синхронизироваться. У каждого 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 неопределимыми. 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.

c) 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 связана 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.

d) Для проверки корректности информации объекта А требуется возврат метки времени, переданной объектом В в 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 в объекте В, сделают ту же работу. В каком-либо глобальном времени нет необходимости (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.

e) Для создания процедуры, названной двойное назначение временных меток [15]. Эта процедура наследует свойства комбинации случаев b), c) и d). Процедура двойного назначения временных меток допускает асинхронную синхронизацию в объектах, таким образом, избегая проблем, связанных с поддержкой объектов, обновляемых глобальным временем. Это 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 приложения) 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 событий, где для конкретной функции важно время.

Ограничения:

- если величина кванта времени слишком велика, то упорядочивающие свойства событий могут быть неопределимыми. В таких случаях информация должна быть дополнена порядковыми номерами;

- 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 могла быть неизвестной или изменяться во время ее жизни, в большинстве 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 стадии, чтобы ограничить связанную с безопасностью функциональность. Если существует возможность несанкционированного доступа, то может быть применен отдельный слой защиты доступа (типа В0 или В1), см. рисунок С.1, или защита обеспечивается связанной с передачей данных функцией безопасности, использующей криптографические механизмы (тип А1), и в этом смысле в последующем тексте использован термин «криптографический код защиты».

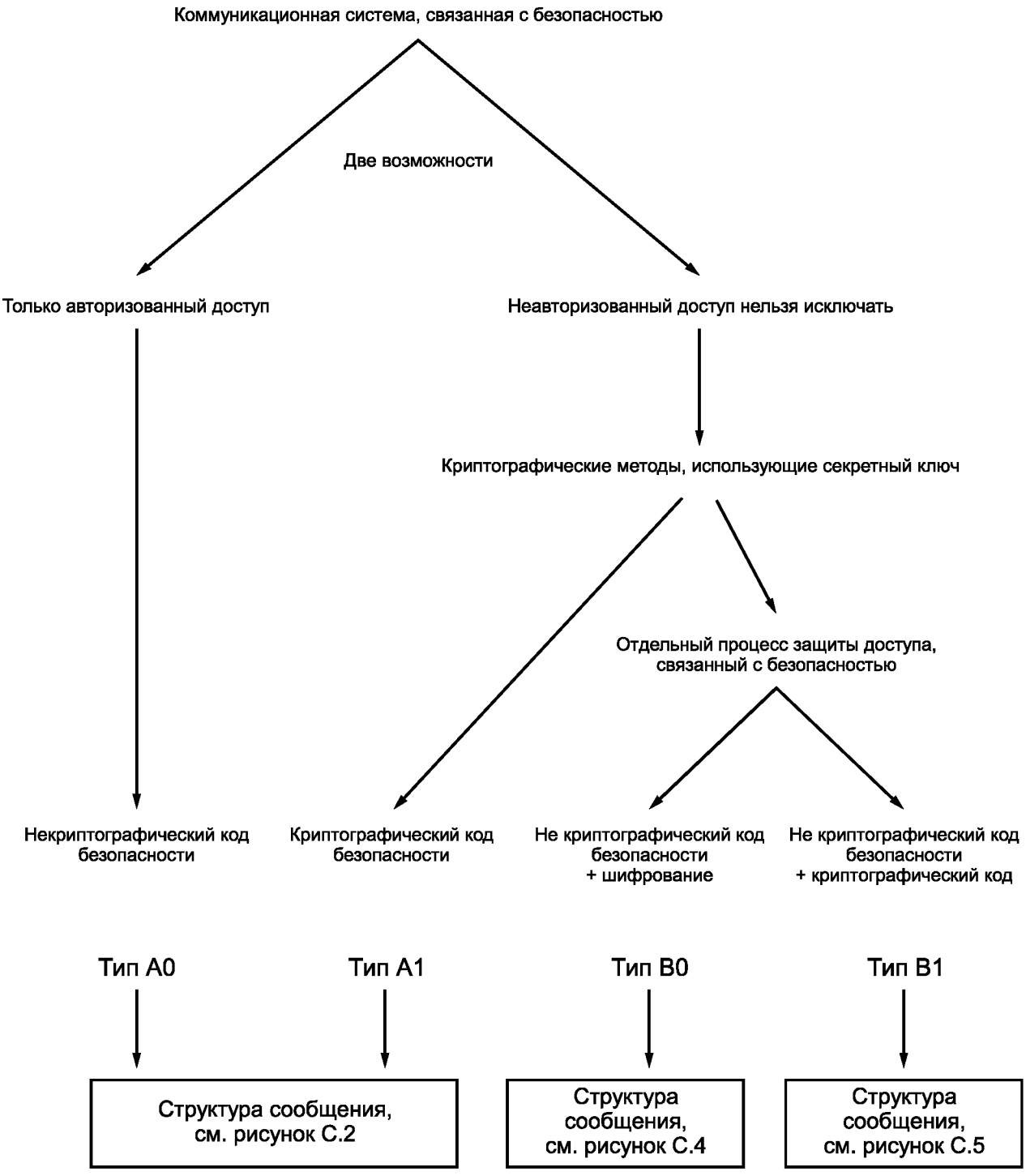


Рисунок С.1 — Классификация связанных с безопасностью систем связи

Принципы структур сообщения для сообщений типов А0 и А1 представлены на рисунке С.2.

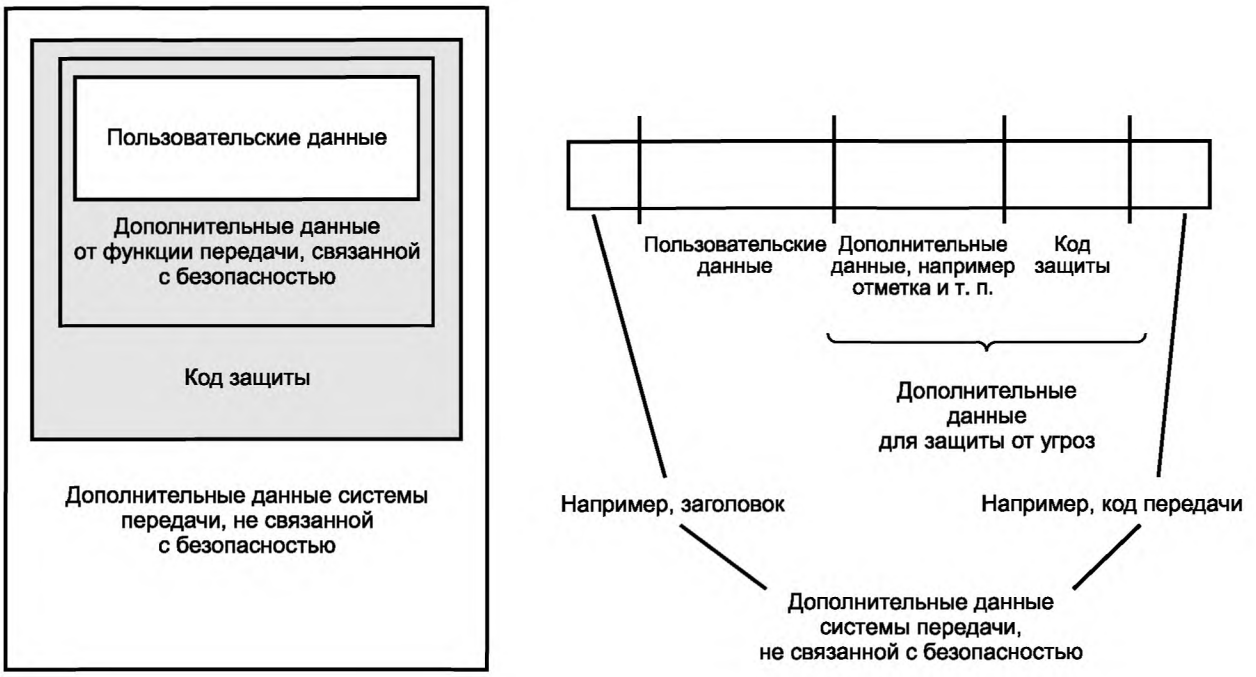


Рисунок С.2 — Модель представления сообщения в системе передачи (тип А0, А1)

Отдельные слои защиты доступа полезны в тех случаях, где группы связанных с безопасностью компьютеров, соединенных локальной сетью (LAN), должны передавать данные по открытым системам передачи (см. рисунок С.3). Неявное предположение для модели, изображенной на рисунке С.3, 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 интерфейсы открытой системы передачи должны быть исключены. Криптографические функции могут быть объединены с функциями шлюза, которые обычно требуются, когда локальная сеть соединена, например, с глобальной сетью.

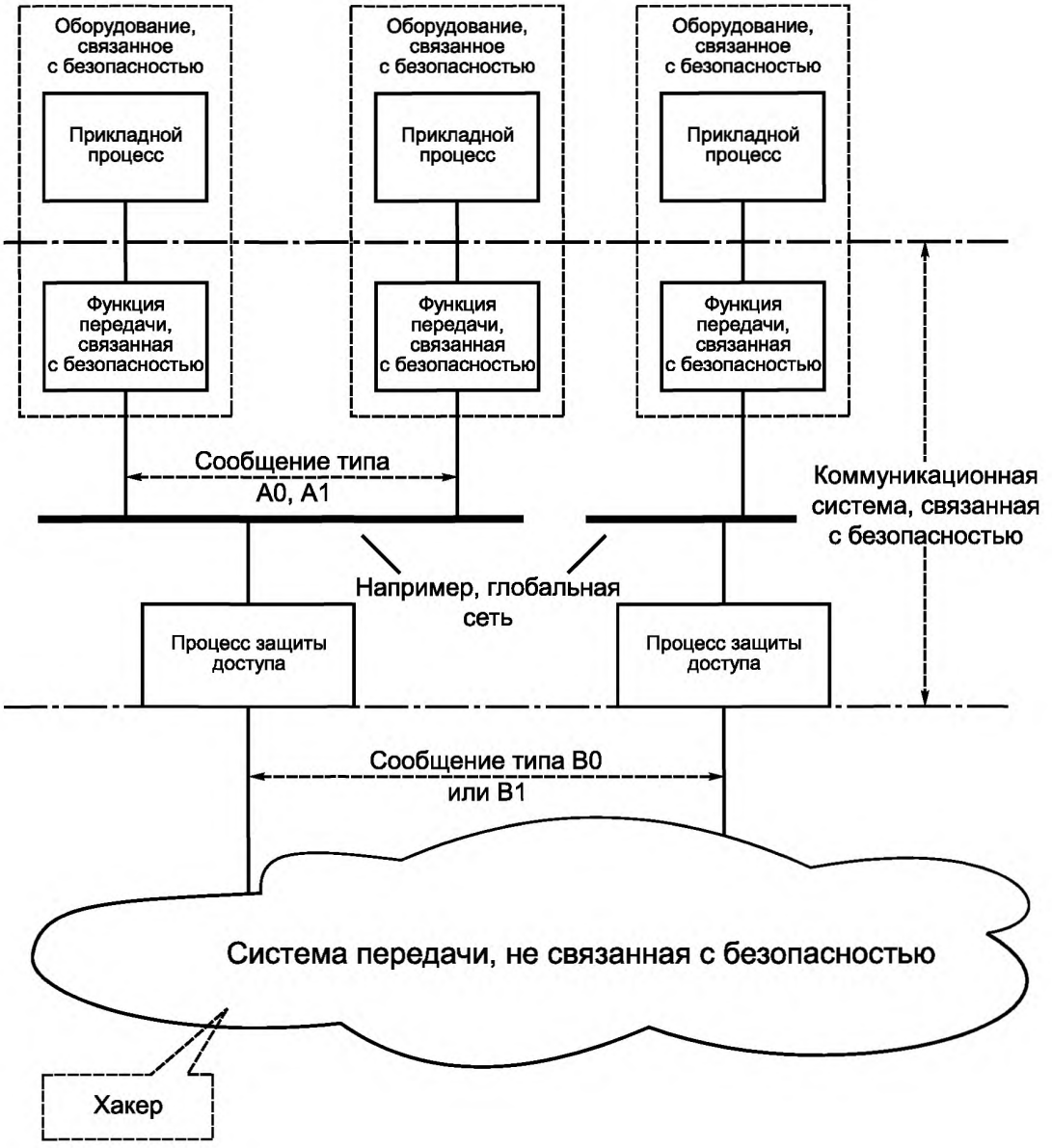


Рисунок С.3 — Использование отдельного слоя защиты доступа

Процесс защиты доступа может быть реализован различными способами:

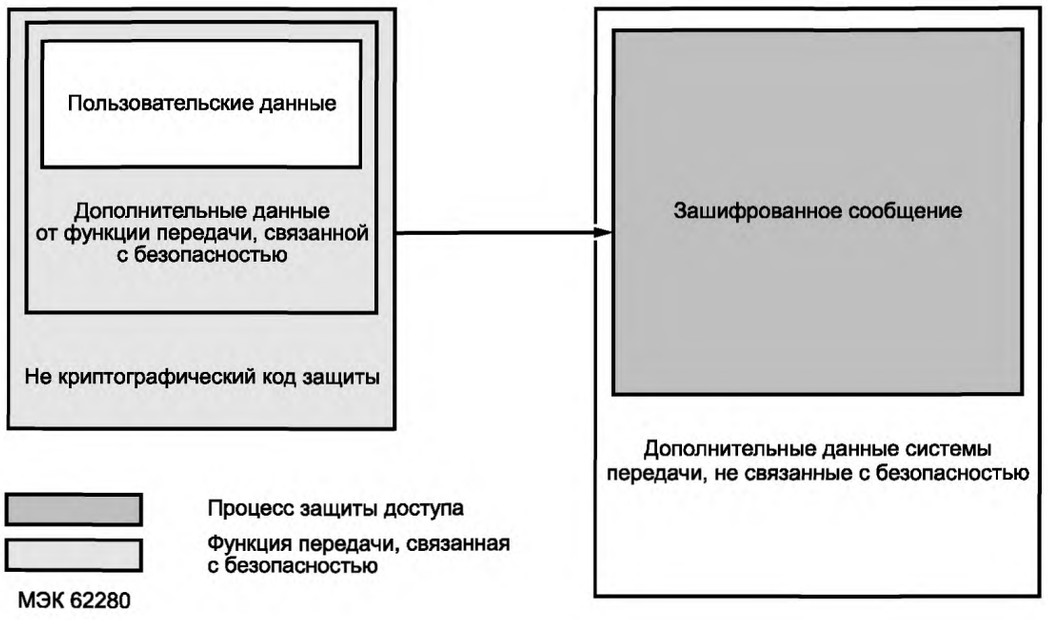
a) шифрование сообщений;

b) добавление криптографического кода.

В обоих случаях применяются коды защиты перед тем, как связанное с безопасностью сообщение посылается 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 процесса защиты доступа.

Принципы структур сообщения для типов сообщений B0 и B1 изображены на рисунках С.4 и С.5.

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



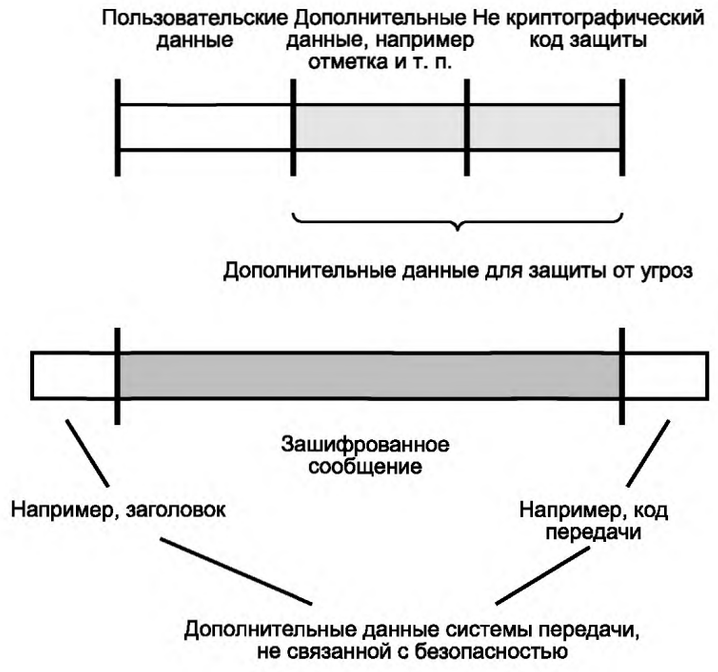


Рисунок С.4 — Модель представления сообщения в системе передачи (тип В0)

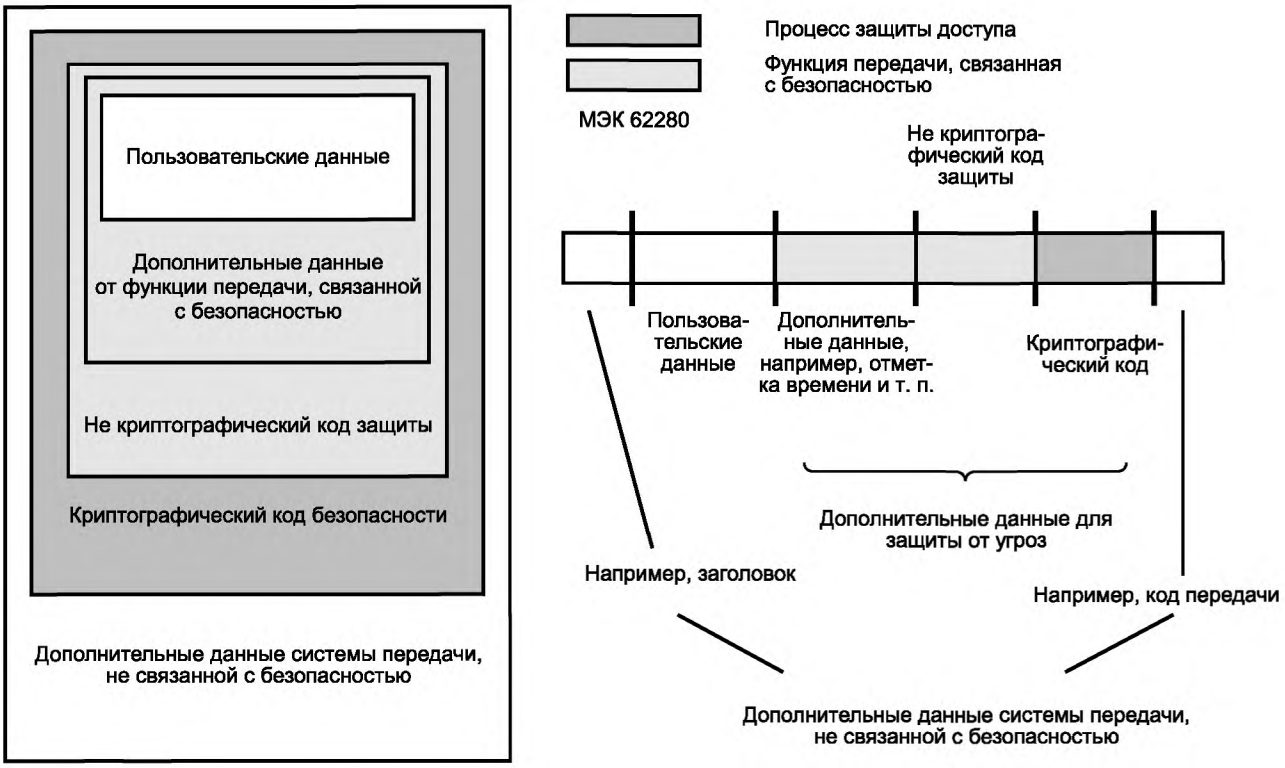


Рисунок С.5 — Модель представления сообщения в системе передачи (тип В1)

С.3 Код защиты

С.3.1 Общие положения

Требуемые свойства кода защиты зависят от характеристик системы передачи 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 должны обнаруживать все виды случайных и систематических битовых ошибок. Необходимо отметить, что обычно система передачи защищает свои сообщения своим собственным кодом передачи, который уже разработан так, чтобы соответствовать определенному уровню качества и заданной интенсивности битовых ошибок. Следовательно, если система передачи данных передает недопустимое сообщение, то либо сбой в канале передачи был настолько 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 предотвращена, но может быть обнаружена и обезврежена. Обычным способом предотвращения вредоносной атаки является применение криптографических алгоритмов, по крайней мере, с одним секретным ключом. Сам код защиты может быть основан на таком алгоритме или может быть реализован отдельный слой защиты доступа с криптографическими функциями. В последнем случае 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 коды и их основные характеристики. Более подробно см. в [17].

С.3.2.2 Линейные блочные коды

Блочный код линеен, если, и только если, сумма любых кодовых слов также является кодовым словом.

Большинство кодов, использующихся для коррекции ошибок, являются линейными двоичными кодами. Также используются недвоичные коды, например, коды Рида-Соломона. 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*. Это означает, что ошибки до *d*-1 неверных символов полностью 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.

С.3.2.3 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 кодов можно найти, например, в [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 *c* избыточными символами обнаруживает все пакетные ошибки размером до *c* 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 односторонние функции, которые сжимают входные данные до «цифрового отпечатка пальца». Из-за их нелинейности минимальное 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 данных изменяет в среднем половину битов в значении хэш-функции. Зная значение хэш-функции, невозможно вычислить входные данные, которые хешируются этим значением хэш-функции (свойство однонаправленности), 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 (коллизия для сильных хеш-функций).

В [7] определяются хэш-коды для целей безопасности в общем случае. В [8] описываются хэш-коды, используя *n*-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 битов входных данных (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 коды

Криптографические блочные коды являются нелинейными блочными хеш-кодами на основе криптографических алгоритмов. Их преимущество состоит в том, что они могут защитить от вредоносной атаки, если они основаны 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)

Тип[a)]	Ссылка, см. раздел 2 и библиографию	Тип связанной с безопасностью системы коммуникации, см. рисунок С.1			
		A0	A1	B0[b)]	B1[b)]
CRC[c)]	[Peterson]	R	US[d)]	–[e)]	R
MAC[c)]	ИСО/МЭК 9797-1 и 2	R	HR	R	R
Хэш-код[c)]	ИСО/МЭК 10118-2	R	US[d)]	HR	HR
Цифровая подпись[c)]	ИСО/МЭК 9796-2 и 3	R	R	R	R

Примечание — Если рекомендуется более одного механизма кодирования безопасности, то 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;

Окончание таблицы С.1

US — метод не подходит для защиты системы этой категории.

[a] Возможны другие меры по обеспечению безопасности, но здесь не рассмотрены.

[b] Только не криптографические коды защиты. Криптографические методы должны быть рассмотрены отдельно.

[c] Способность обнаружения ошибки одинакова для одного и того же числа битов избыточности.

[d] Запрашиваемый секретный ключ этим механизмом не может быть выполнен.

[e] 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 игнорировать и обеспечить его лучшую работу, но в «открытом» канале (черном канале) никаких таких знаний нельзя предположить. В этом сценарии идеальным решением был бы случайный код. Поэтому не должны устанавливаться никакие требования к вероятности необнаруженных ошибок P_{UE} кода защиты, которая ниже, чем вероятность случайного кода, которая равна $P_{UE} = 2^{-c}$, где c обозначает число битов избыточности.

С.3.4 Криптографические методы

При использовании методов криптографической защиты рекомендуются стандартизированные режимы работы, например, в соответствии с [6]. Этот стандарт не рекомендует метод прямого шифрования (ECB) для длины входной последовательности, превышающей размер блока алгоритма шифрования. Рекомендуются хорошо известные 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 ошибками систем передачи. Обычно в исправном состоянии механизм обнаружения ошибок системы передачи обнаруживает 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 стороны, 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.6.

Существует три возможности появления опасности:

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

b) битовые ошибки, возникающие из-за EMI и не обнаруженные кодированием передачи;

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

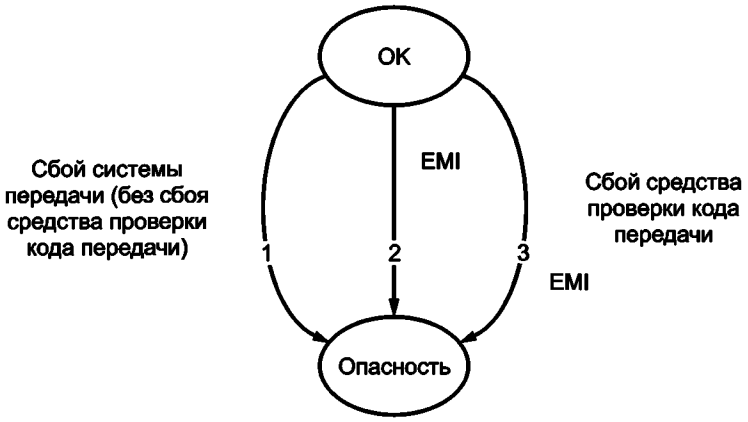


Рисунок С.6 — Базовая модель ошибки

Введем следующие определения:

R_H — целевая интенсивность опасных отказов всей системы передачи;

R_{H1} — интенсивность опасных отказов от сбоев аппаратных средств без средства проверки кода передачи;

R_{H2} — интенсивность опасных отказов от EMI;

R_{H3} — интенсивность опасных отказов средства проверки кода передачи;

R_{HW} — интенсивность опасных отказов недоверительной системы передачи;

P_{US} — вероятность необнаруженных отказов при выполнении кода защиты;

P_{UT} — вероятность необнаруженных отказов при выполнении кода передачи;

Примечание — Если недоверительные системы передачи не содержат механизмов кодирования передачи, то должно быть принято $P_{UT} = 1$.

f_M — максимальная частота сообщений для одного получателя;

f_W — частота неправильных (поврежденных) сообщений;

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

k_1 — коэффициент для сбоев аппаратных средств, включающий запас безопасности;

k_2 — коэффициент, который описывает процент сбоев аппаратных средств, которые приводят к необнаруженному отключению декодирования передачи;

m — запас безопасности, включен в k_1;

n — количество последовательных поврежденных сообщений, после которого выполняется переход в безопасное состояние с пониженной скоростью передачи данных.

С этими определениями необходимо оценить следующие формулы:

$$R_{HW} \cdot P_{US} \cdot k_1 = R_{H1}, \quad (C.1)$$

$$P_{UT} \cdot P_{US} \cdot f_W = R_{H2}^{1)}, \quad (C.2)$$

$$k_2 \cdot P_{US} \cdot \frac{1}{T} = R_{H3}. \quad (C.3)$$

Сумма всех трех значений интенсивностей не должна превышать R_H:

$$R_{H1} + R_{H2} + R_{H3} \le R_H.$$

[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.

Поскольку нельзя предположить, что отказ случаен, необходимо принять во внимание запас безопасности m в коэффициенте k_1. Коэффициент k_1 должен быть вычислен согласно следующей формуле:

$$k_1 \geq n \cdot m.$$

Коэффициент m представляет запас безопасности с $m \geq 5$.

Максимальная частота неправильных сообщений f_W должна быть оценена:

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

В циклической передаче частоты f_M определена точно. В случае нециклической передачи необходимо использовать максимально возможное значение частоты.

При помощи «подходящего» или «хорошего» CRC[1)] максимальное значение P_{UT} может быть оценено как:

$$P_{UT} = 2^{-b},$$

где b означает число битов 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 k_2 трудно оценить. Если возможна периодическая проверка корректной работы механизма кодирования передачи, то коэффициентом k_2 можно было пренебречь.

Без каких либо обоснований можно считать, что $k_2 = 1$.

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:

$$T = \mathrm{MTBF}_{HW} = \frac{1}{R_{\mathrm{HW}}}.$$

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 $k_2 = 10^{-4}$.

Формула (С.3) 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 c должна быть оценена как:

$$P_{US} = 2^{-c}.$$

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

Повторяя каждое сообщение и проверяя согласованность двух взаимно независимых сообщений, значение c может 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 пессимистическую оценку следует считать пределом.

---

1) «Подходящий» означает, что отношение между вероятностью битовой ошибки (меньше, чем 0,5) и вероятностью 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 p полученный бит сфальсифицирован (0→1 и 1→0). Каждый бит независим друг от друга.

Примечание — Этот механизм основан на том, что отказы по общей причине, влияющие на два сообщения, незначительны.

С.5 Коммуникация между связанными и не связанными с безопасностью приложениями

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

В доверительных сетях (Категории 1 и 2) не связанные с безопасностью приложения могут передавать сообщения по той же среде передачи, которую используют, связанные с безопасностью приложения. Требования см. в 7.2.

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

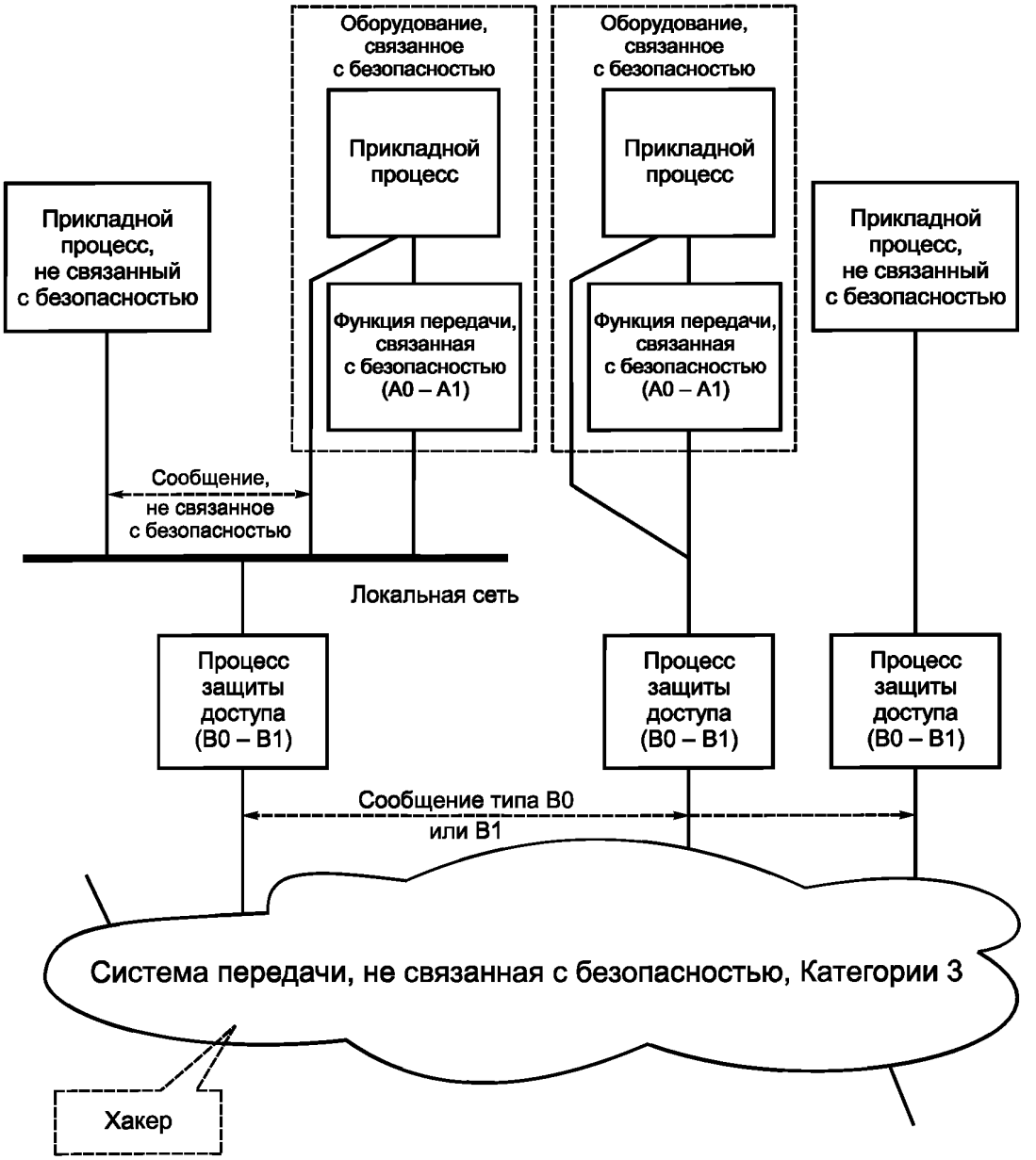


Рисунок С.7 — Коммуникация между связанными и не связанными с безопасностью приложениями

Приложение D
(справочное)

Руководство по применению настоящего стандарта

D.1 Процедура

D.1.1 Общие положения

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

Приложение
↓
Анализ риска
↓
Снижение риска
↓
Определение значений УПБ и количественных целей
↓
Спецификации требований безопасности (SRS)

Каждый из этих шагов описан более подробно в следующих подпунктах.

D.1.2 Приложение

Разработчик системы должен понимать приложение системы передачи, а именно: потоки данных, типы данных, 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 определена (пользователем или полномочным органом по безопасности) глобальная цель безопасности (интенсивность или качественные параметры и нефункциональные параметры).

D.1.3 Анализ риска

Качественный анализ угроз системы (в соответствии с МЭК 62278) должен идентифицировать опасность(и) 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 защиты в проекте системы.

D.1.4 Снижение риска

Зная глобальную количественную цель безопасности для системы и результаты качественного анализа риска, разработчик системы может распределить цели безопасности для каждой идентифицированной угрозы. Определение таких целей 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, задаваемого для каждого средства защиты.

D.1.5 Определение значений УПБ и количественных целей

В зависимости от степени снижения риска, необходимого для каждого средства защиты, используя процедуры, 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, используя таблицы в МЭК 62425, могут быть выбраны методы проектирования аппаратных средств, а также может быть вычислена интенсивность возникновения опасных отказов из-за случайных отказов.

D.1.6 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.

D.2 Пример

D.2.1 Общие положения

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

D.2.2 Приложение

Команды разрешения на проследование отправляются поездам по второстепенной линии посредством сообщений по радиосети.

Для системы определена глобальная цель безопасности 10^{-x} в час.

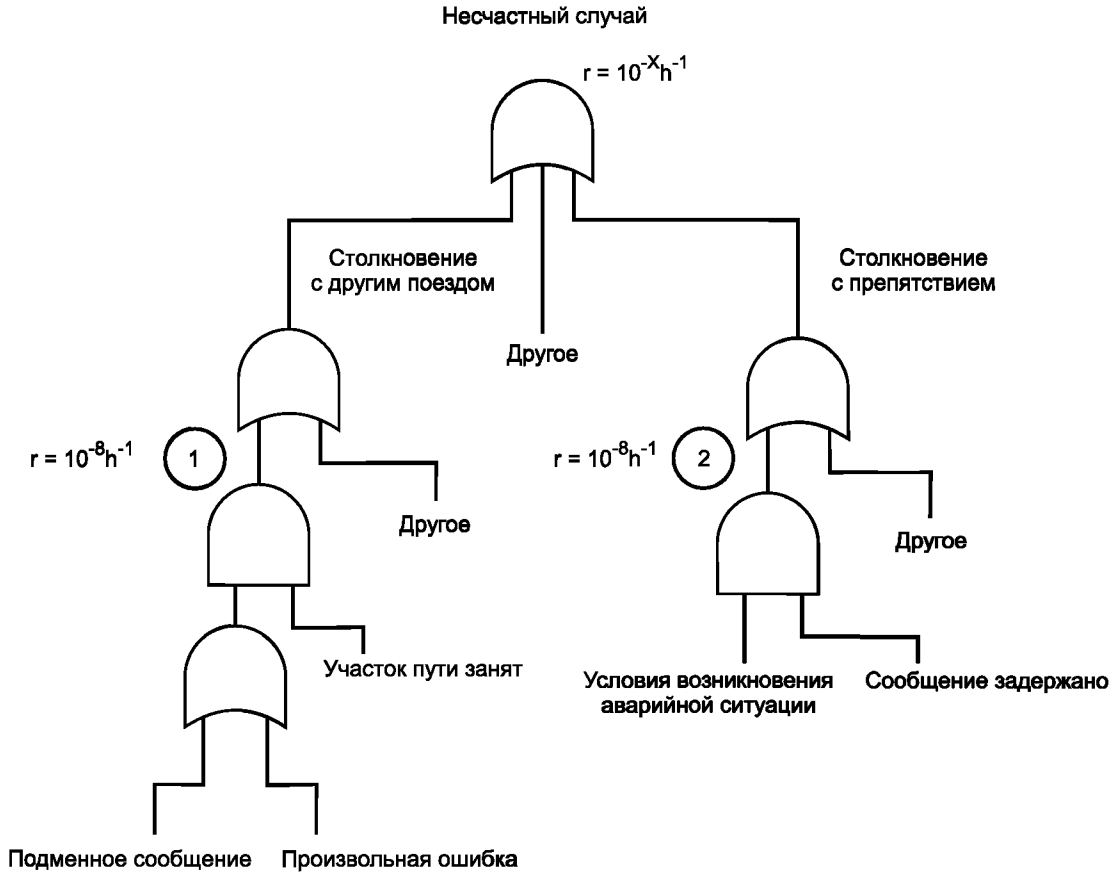
D.2.3 Анализ риска

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 препятствием на пути.

Они показаны на дереве отказов (рисунок D.1) в примере одного из методов выполнения анализа риска.



Обозначения:

– схема ИЛИ;

– схема И;

1 – дерево отказов для случая 1 (см. рисунок D.2);

2 – дерево отказов для случая 2 (см. рисунок D.3);

r – допустимая интенсивность опасности.

Рисунок D.1 — Дерево отказов для опасности «авария»

Глобальная цель безопасности системы 10^{-x} в час распределена и целевое значение, полученное для случаев 1 и 2 (например) равно 10^{-8} в час для каждого случая.

Рассмотрим случаи 1 и 2 более подробно.

D.2.4 Случай 1

D.2.4.1 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 неправильное 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 D.2:

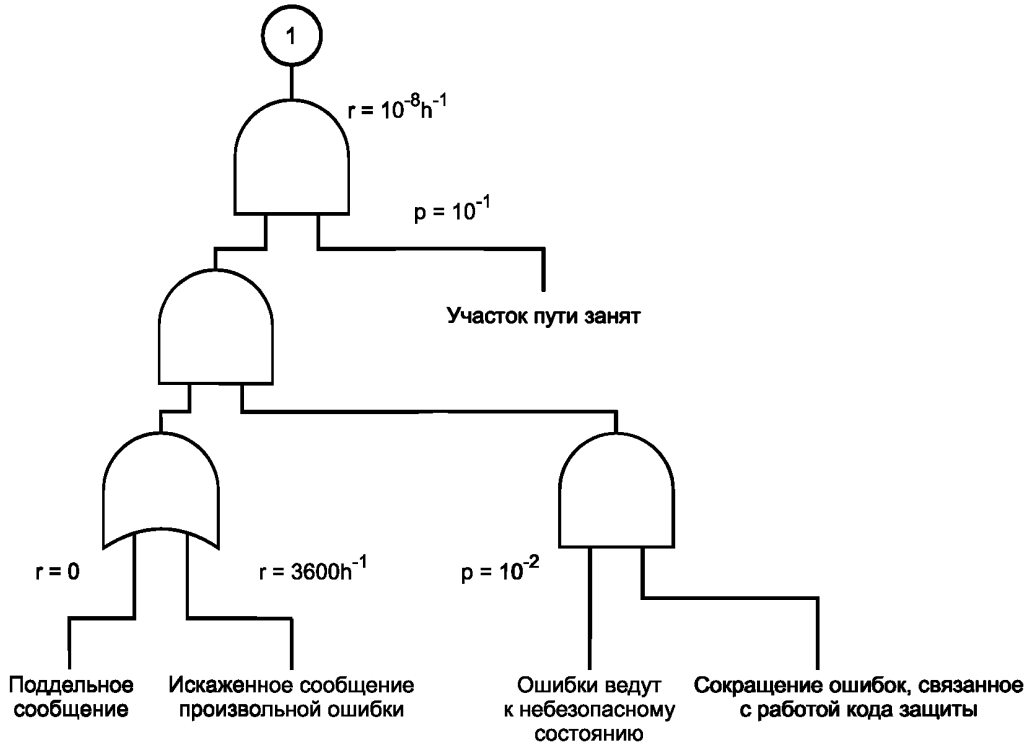


Рисунок D.2 — Дерево отказов для случая 1

Рассматривая количественные цели безопасности, предположим, что в открытой системе каждое сообщение 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 предполагая, 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 код защиты для сообщения должен гарантировать вероятность необнаруженной ошибки меньше, чем 3×10^{-9} для сообщения, или частота этого вида событий не должна превышать 10^{-5} в час.

D.2.4.2 Определение значений УПБ и количественных целей

Согласно МЭК 62425 может быть получено значение УПБ для реализации функции «вычисление кода защиты». 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 качества функционирования.

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

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.

D.2.5 Случай 2

D.2.5.1 Снижение риска

Если в случае возникновения аварийной ситуации (например, из-за препятствия на участке пути) сообщение 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, задержка 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 использование тайм-аута в оборудовании получения, вместе с циклической передачей сообщения.

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

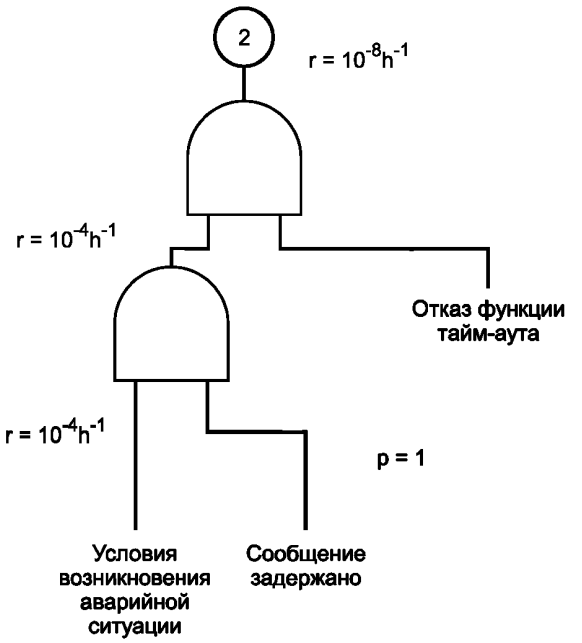


Рисунок D.3 — Дерево отказов для случая 2

Рассматривая количественные цели безопасности, понятно, что у функции тайм-аута должна быть вероятность появления опасной ошибки по запросу не больше, чем 10^{-4}.

D.2.5.2 Определение значений УПБ и количественных целей

В МЭК 62425 показано, как достигнуть требуемого значения УПБ.

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

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 только исправления и улучшения. Для обеспечения 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)разделы 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 в таблицах Е.1 и Е.2 делается только для (под)разделов предыдущих стандартов на (под)разделы настоящего стандарта, но не наоборот.

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

(Под)разделы МЭК 62280-1:2002	Справочный/ Обязательный	(Под)разделы 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 ПУ3	Р
ПУ2	Обязательный	6.3.1 ПУ1	Р
ПУ3	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

Окончание таблицы Е.1

Н — (не изменен) включают изменения ссылок и изменения терминологии, чтобы достигнуть согласованности 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)пункты.

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

(Под)разделы МЭК 62280-2:2002	Справочный/ Обязательный	(Под)разделы 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
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 Порядковый 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 идентификации	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 угроз/защит	Обязательный	7.4.2 Матрица угроз/защит	Н
7.3 Выбор и использование кода защиты и криптографических методов	Обязательный	7.4.3 Выбор и использование кода защиты и криптографических методов	Н
А.1 Применение меток времени	Справочный	С.1 Применение меток времени	Н
А.2 Выбор и использование кодов защиты и криптографических методов	Справочный	С.2 Выбор и использование кодов защиты и криптографических методов	Т
Библиография	Справочный	Библиография	Т

Окончание таблицы Е.2

(Под)разделы МЭК 62280-2:2002	Справочный/ Обязательный	(Под)разделы настоящего стандарта	Не изменен/ изменен
С.1 Область применения/цель	Справочный	6.1 Общие положения	Т
С.2 Классификация систем передачи	Справочный	6.2 Общие аспекты классификации	Т
		Приложение В. Категории систем передачи	Т
С.3 Процедура	Справочный	D.1 Процедура	Н
С.4 Пример	Справочный	D.2 Пример	Н
Приложение D. Угрозы в открытых системах передачи	Справочный	Приложение А. Угрозы в открытых системах передачи	Р

Н — (не изменен) включают изменения ссылок и изменения терминологии, чтобы достигнуть согласованности 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)пункты.

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 соответствующего национального стандарта
IEC 62278 (all parts)	—	*
IEC 62425:2007	—	*
* Соответствующий национальный стандарт отсутствует. До его утверждения рекомендуется использовать перевод на русский язык данного международного стандарта.		

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

[5] ISO/IEC 9797-2:2011, Information technology — Security techniques — Message Authentication Codes (MACs) — Part 2: Mechanisms using a dedicated hash-function

[6] ISO/IEC 10116:2006, Information technology — Security techniques — Modes of operation for an n-bit block cipher

[7] ISO/IEC 10118-1:2000, Information technology — Security techniques — Hash-functions — Part 1: General

[8] ISO/IEC 10118-2:2010, Information technology — Security techniques — Hash-functions — Part 2: Hash-functions using an n-bit block cipher

[9] ISO/IEC 10118-3:2004, Information technology — Security techniques — Hash-functions — Part 3: Dedicated hash-functions

[10] ISO/IEC 10118-4:1998, Information technology — Security techniques — Hash-functions — Part 4: Hash-functions using modular arithmetic

[11] ISO/IEC 11770-1:2010, Information technology — Security techniques — Key management — Part 1: Framework

[12] ISO/IEC 11770-2:2008, Information technology — Security techniques — Key management — Part 2: Mechanisms using symmetric techniques

[13] ISO/IEC 11770-3:2008, Information technology — Security techniques — Key management — Part 3: Mechanisms using asymmetric techniques

[14] UIC 738, Processing and transmission of safety information

[15] 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)

[16] FIPS PUB 197, 26.11.2001: Advanced Encryption Standard

[17] W.Wesley Peterson, Error correction Codes, M.I.T. Press, 1967

УДК 62-783:614:006.354 ОКС 45.060 Группа Т51

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

БЗ 8–2017/27

Редактор *А.Ф. Колчин*
Технический редактор *И.Е. Черепкова*
Корректор *Е.Ю. Митрофанова*
Компьютерная верстка *Е.А. Кондрашовой*

Сдано в набор 20.07.2017. Подписано в печать 03.08.2017. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 6,05. Уч.-изд. л. 5,47. Тираж 27 экз. Зак. 1266.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Издано и отпечатано во ФГУП «СТАНДАРТИНФОРМ», 123001 Москва, Гранатный пер., 4.
gost.e-ecolog.ru gost.e-ecolog.ru

gost.e-ecolog.ru