МЕЖДУНАРОДНЫЙ СОЮЗ ЭЛЕКТРОСВЯЗИ

МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

Т.807

(05/2006)

СЕРИЯ Т: ОКОНЕЧНОЕ ОБОРУДОВАНИЕ ДЛЯ ТЕЛЕМАТИЧЕСКИХ СЛУЖБ

Информационная технология – Система кодирования изображений JPEG 2000: Стандарт Secure JPEG 2000

Рекомендация МСЭ-Т Т.807

МЕЖДУНАРОДНЫЙ СТАНДАРТ ИСО/МЭК 15444-8
РЕКОМЕНДАЦИЯ МСЭ-Т Т.807

Информационная технология – Система кодирования изображений JPEG 2000: Стандарт Secure JPEG 2000

Резюме

Целью данной Рекомендации | Международного стандарта является предоставление синтаксиса, делающего возможным услуги безопасности для применения к закодированным данным изображения JPEG 2000. Услуги безопасности включают конфиденциальность, подтверждение подлинности, аутентификацию источника, условный доступ, а также защищенную масштабируемую потоковую передачу данных и защищенную перекодировку. Данный синтаксис позволяет применять услуги безопасности к закодированным или незакодированным данным изображения или их части. Это соответствует требованиям неотъемлемых свойств JPEG 2000, таких как масштабируемость и доступ к различным пространственным областям, уровни разрешения, компоненты цвета, уровни качества, в то же время предоставляя услуги безопасности по данным элементам.

Источник

Рекомендация МСЭ-Т Т.807 утверждена 29 мая 2006 года 16-й Исследовательской комиссией МСЭ-Т (2005–2008 гг.) в соответствии с процедурой, изложенной в Рекомендации МСЭ-Т А.8. Идентичный текст также опубликован в виде ИСО/МЭК 15444-8.

ПРЕДИСЛОВИЕ

Международный союз электросвязи (МСЭ) является специализированным учреждением Организации Объединенных Наций в области электросвязи. Сектор стандартизации электросвязи МСЭ (МСЭ-Т) – постоянный орган МСЭ. МСЭ-Т отвечает за изучение технических, эксплуатационных и тарифных вопросов и за выпуск Рекомендаций по ним с целью стандартизации электросвязи на всемирной основе.

На Всемирной ассамблее по стандартизации электросвязи (ВАСЭ), которая проводится каждые четыре года, определяются темы для изучения Исследовательскими комиссиями МСЭ-Т, которые, в свою очередь, вырабатывают Рекомендации по этим темам.

Утверждение Рекомендаций МСЭ-Т осуществляется в соответствии с процедурой, изложенной в Резолюции 1 ВАСЭ.

В некоторых областях информационных технологий, которые входят в компетенцию МСЭ-Т, необходимые стандарты разрабатываются на основе сотрудничества с ИСО и МЭК.

ПРИМЕЧАНИЕ

В настоящей Рекомендации термин "администрация" используется для краткости и обозначает как администрацию электросвязи, так и признанную эксплуатационную организацию.

Соблюдение положений данной Рекомендации носит добровольный характер. Однако в Рекомендации могут содержаться определенные обязательные положения (например, для обеспечения возможности взаимодействия или применимости), и соблюдение положений данной Рекомендации достигается в случае выполнения всех этих обязательных положений. Для выражения необходимости выполнения требований используется синтаксис долженствования и соответствующие слова (такие, как "должен" и т. п.), а также их отрицательные эквиваленты. Использование этих слов не предполагает, что соблюдение положений данной Рекомендации является обязательным для какой-либо из сторон.

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

МСЭ обращает внимание на вероятность того, что практическое применение или реализация этой Рекомендации может включать использование заявленного права интеллектуальной собственности. МСЭ не занимает какую бы то ни было позицию относительно подтверждения, обоснованности или применимости заявленных прав интеллектуальной собственности, независимо от того, отстаиваются ли они членами МСЭ или другими сторонами вне процесса подготовки Рекомендации.

На момент утверждения настоящей Рекомендации МСЭ не получил извещение об интеллектуальной собственности, защищенной патентами, которые могут потребоваться для выполнения этой Рекомендации. Однако те, кто будет применять Рекомендацию, должны иметь в виду, что это может не отражать самую последнюю информацию, и поэтому им настоятельно рекомендуется обращаться к патентной базе данных БСЭ по адресу: http://www.itu.int/ITU-T/ipr/.

СОДЕРЖАНИЕ

Введение

В "цифровом веке" интернет дает правообладателям много новых возможностей, касающихся электронного распространения их работ (книги, видео, музыка, изображения и т. д.).

В то же время, новые информационные технологии чрезвычайно упрощают доступ пользователя к содержанию. Это идет рука об руку с все более распространяющейся проблемой пиратских цифровых копий – такого же качества, как и оригинал – и "обмена файлами" в одноранговых сетях, что уже долгое время вызывает жалобы на большие потери индустрии содержания.

Всемирной организации по охране интеллектуальной собственности (ВОИС) и Государствам-Членам (170) отведена большая роль в гарантировании, что в 21 веке авторское право, а также культурное и интеллектуальное выражение, которое оно поощряет, остается хорошо защищенным. Новая Цифровая экономика и творческие люди в каждой стране зависят от этого. Кроме того, в декабре 1996 года был опубликован Договор ВОИС по авторскому праву, где было две важных статьи (11 и 12) о технических мерах и обязательствах, касающихся Права на управленческую информацию:

Статья 11
Обязательства, касающиеся технических мер

Договаривающиеся стороны должны обеспечить соответствующую юридическую защиту и эффективные юридические меры против обхода эффективных технических мер, используемых авторами в связи с применением их прав в рамках данного Договора или Бернской конвенции, и ограничивающих действия в отношении их работ, которые не разрешены указанными авторами или запрещены законом.

Статья 12
Обязательства, касающиеся прав на управленческую информацию

(1) Договаривающиеся стороны должны обеспечить соответствующие и эффективные юридические меры по отношению к любому лицу, намеренно осуществляющему любое из следующих действий, зная, или что касается гражданских мер, которые имеют все основания быть известными, что эти действия вызовут, дадут возможность, облегчат или замаскируют нарушение любого права, на которое распространяется действие данного Договора или Бернской конвенции.

(i) Удаление или изменение любой информации по управлению электронными правами без соответствующих полномочий;

(ii) Распространение, импорт для распространения, вещание или передача публике, без соответствующих полномочий, работ или копий работ, зная, что информация по управлению электронными правами была удалена или изменена без соответствующих полномочий.

(2) Используемый в данной Статье термин "информация по управлению правами" обозначает информацию, которая идентифицирует работу, автора работы, владельца любых прав на работу, или информацию о постановлениях и условиях договора об использовании работы, а также любые числа или коды, представляющие такую информацию, когда любая часть этой информации присоединяется к копии работы или оказывается связанной с передачей работы публике.

Данный договор создает твердую основу для защиты интеллектуальной собственности. Что касается 2004 года, около 50 стран ратифицировали этот важный договор. Поэтому ожидается, что инструменты и методы защиты, рекомендуемые в JPEG 2000, должны обеспечивать безопасность транзакций, защиту содержания (Права Интеллектуальной собственности), и защиту технологий.

Вопросы безопасности такие, как аутентификация, целостность данных, защита авторского права и интеллектуальной собственности, неприкосновенность частной жизни, условный доступ, конфиденциальность, отслеживание транзакций – лишь некоторые из важных функций многих приложений обработки изображений, на которые направлен JPEG 2000.

Технологические средства защиты цифрового содержания описаны и могут быть достигнуты различными путями такими, как цифровые "водяные знаки", цифровая подпись, шифрование, метаданные, аутентификация и проверка целостности.

В Части 8 стандарта JPEG 2000 предоставляются инструменты и решения в виде спецификаций, позволяющих приложениям генерировать, потреблять и обмениваться потоками кода Secure JPEG 2000. Это называется **JPSEC**.

МЕЖДУНАРОДНЫЙ СТАНДАРТ
РЕКОМЕНДАЦИЯ МСЭ-Т

Информационная технология – Система кодирования изображений JPEG 2000: Стандарт Secure JPEG 2000

1 Сфера применения

В данной Рекомендации | Международном стандарте определяется структура, понятия и методология для защиты кодовых потоков JPEG 2000. В области применения данной Рекомендации | Международного стандарта дается определение:

1) нормативного синтаксиса кодового потока, содержащего информацию для интерпретирования защищенных данных изображения;
2) нормативного процесса регистрации инструментов JPSEC в органе регистрации, предоставляющем уникальный идентификатор;
3) информативных примеров инструментов JPSEC в типичных случаях использования;
4) информативных примеров того, как реализовывать услуги безопасности и смежные метаданные.

В области применения данной Рекомендации | Международного стандарта не описываются определенные приложения по защищенной обработке изображений или защищенная обработка изображений не ограничивается определенными методами, но описывается структура, которая позволит будущим расширениям развиться в методы защищенной обработки изображений.

2 Нормативные справочные документы

В перечисленных ниже Рекомендациях МСЭ-Т и другой справочной литературе содержатся положения, которые посредством ссылок на них в этом тексте составляют основные положения данной Рекомендации | Международного стандарта. На момент опубликования, действовали указанные редакции документов. Все Рекомендации и другая справочная литература, являются предметом корректировки, и стороны пришли к договоренности основываться на этой Рекомендации | Международном стандарте и стараться изыскивать возможность для использования самых последних изданий Рекомендации и справочной литературы, перечисленной ниже. Регулярно публикуется перечень действующих Рекомендаций МСЭ-Т. Ссылка на документ в рамках этой Рекомендации не дает ему, как отдельному документу, статуса рекомендации.

- Рекомендация МСЭ-Т Т.800 (2002 г.) | ИСО/МЭК 15444-1:2004, *Информационная технология – Система кодирования изображений JPEG 2000: Основы системы кодирования*.
- Рекомендация МСЭ-Т Т.801 (2002 г.) | ИСО/МЭК 15444-2:2004, *Информационная технология – Система кодирования изображений JPEG 2000: Добавления*.

3 Термины и определения

Для целей данной Рекомендации | Международного стандарта применяются следующие определения. К данной Рекомендации | Международному стандарту применяются определения, определенные в разделе 3 Рек. МСЭ-Т Т.800 | ИСО/МЭК 15444-1.

3.1 access control – управление доступом: Предотвращение несанкционированного использования ресурса, включая предотвращение использования ресурса несанкционированным образом.

3.2 authentication – аутентификация: Процесс подтверждения подлинности идентификационной информации, которая требуется объектом системы или для объекта системы.

3.2.1 source authentication – аутентификация источника: Подтверждение подлинности того, что объект источника (скажем, пользователь/участник) на самом деле является заявленным объектом источника.

3.2.2 fragile/semi-fragile – хрупкая/полухрупкая аутентификация изображения: Процесс, применяемый как для аутентификации источника изображения, так и для подтверждения целостности содержания данных/ изображения. Данный процесс должен обнаруживать любое изменение сигнала и определять, где оно произошло, и, по возможности, каким был сигнал до модификации.

ПРИМЕЧАНИЕ. – Используется для подтверждения аутентичности документа. Разница между хрупкой и полухрупкой аутентификацией изображения состоит в том, что первая проверяет целостность данных изображения, а вторая проверяет целостность содержания изображения.

3.3 confidentiality – конфиденциальность: Свойство, характеризующееся тем, что информация не предоставляется или не сообщается частным лицам, объектам или процессам, не имеющим разрешения.

3.4 data splitting – разделение данных: Метод защиты чувствительных данных от несанкционированного доступа при помощи шифрования данных и хранения различных частей файла на разных серверах.

ПРИМЕЧАНИЕ. – Когда осуществляется доступ к разделенным данным, все части отыскиваются, комбинируются и расшифровываются. Лицу, не имеющему полномочий, придется узнать месторасположение серверов, содержащих все части, смочь получить доступ к каждому серверу, узнать, какие данные нужно комбинировать, и как расшифровать их.

3.5 decryption, deciphering – расшифровка, дешифрование: Преобразование, обратное шифрованию.

3.6 digital signature – цифровая подпись: Данные, прикрепленные к или являющиеся криптографическим преобразованием единицы данных, которые позволяют получателю единицы данных подтвердить происхождение и целостность единицы данных и защитить данные от подделки, например получателем.

3.7 encryption – шифрование: Обратимое преобразование данных при помощи алгоритма шифрования, в результате которого получается зашифрованный текст, т. е. информационное содержание данных скрывается.

ПРИМЕЧАНИЕ. – Другое название алгоритма шифрования – шифр.

3.8 fingerprints – контрольная сумма файла: Характерная особенность объекта, которая позволяет отличить его от других похожих объектов, что позволит владельцу выследить зарегистрированных пользователей, нелегально распространяющих их (другие похожие объекты).

ПРИМЕЧАНИЕ. – В этом отношении, контрольная сумма файла обычно обсуждается в контексте проблемы выслеживания предателя.

3.9 hash function – хэш-функция: Функция, которая устанавливает соответствие между строками битов и строками битов фиксированной длины, соблюдая следующие два условия:

ПРИМЕЧАНИЕ. – Для данных выходных данных невозможно вычислить входные данные, соответствующие этим выходным данным. Для данных входных данных невозможно вычислить вторые входные данные, соответствующие этим же входным данным. Возможность вычисления зависит от определенных требований безопасности и окружения пользователя.

3.10 integrity – целостность: Свойство, характеризующееся способностью защищать точность и полноту средств.

3.10.1 image data integrity – целостность данных изображения: Свойство, характеризующееся тем, что данные не были изменены или уничтожены несанкционированным образом.

ПРИМЕЧАНИЕ. – Целостность данных изображения позволяет выполнять операции, сохраняющие содержание, в отношении изображений, не запуская сигнализацию о нарушении целостности.

3.11 JPSEC application – Приложение JPSEC: Любой процесс программного или аппаратного обеспечения, обладающий способностью потреблять потоки кода JPSEC путем интерпретации синтаксиса JPSEC для предоставления указанных услуг безопасности.

ПРИМЕЧАНИЕ. – Приложение JPSEC использует один или несколько инструментов JPSEC.

ПРИМЕР. – Приложение JPSEC сможет прочитать зашифрованные потоки кода JPSEC, расшифровать их, при наличии соответствующего ключа, и визуализировать первоначальные базовые данные изображения JPEG 2000.

3.12 JPSEC codestream – Кодовый поток JPSEC: Последовательность битов, получающаяся в результате кодирования и обеспечения безопасности изображения, использующего кодирование JPEG 2000 и инструменты безопасности JPSEC.

3.12.1 JPSEC creator – создатель JPSEC: Объект, создающий кодовый поток JPSEC из изображения, кодового потока JPEG 2000 или другого кодового потока JPSEC для обеспечения защиты некоторых услуг JPSEC.

3.12.2 JPSEC consumer – потребитель JPSEC: Объект, получающий кодовый поток JPSEC и оказывающий услугу JPSEC на основе данного кодового потока.

3.13 JPSEC service – служба JPSEC: Служба, обеспечивающая безопасность потребления изображений JPEG 2000. Данная служба отражает атаки безопасности и использует один или несколько инструментов JPSEC.

3.14 JPSEC registration authority – орган регистрации JPSEC: Объект, отвечающий за выдачу уникального ID для ссылки на инструмент JPSEC и хранящий список параметров описания инструмента JPSEC.

3.15 JPSEC tool – инструмент JPSEC: Процесс аппаратного или программного характера, использующий методы обеспечения безопасности для реализации службы безопасности.

3.15.1 JPSEC normative tool – нормативный инструмент JPSEC: Инструмент JPSEC, использующий заранее определенные шаблоны инструмента для расшифровки, аутентификации или хеширования, которые определены в нормативной части данной Рекомендации │ Международного стандарта.

3.15.2 JPSEC non-normative tool – ненормативный инструмент JPSEC: Инструмент JPSEC, определяемый при помощи идентификационного номера, выдаваемого органом регистрации JPSEC или приложения, определенного пользователем.

3.15.3 JPSEC user-defined tool – инструмент JPSEC, определенный пользователем: ненормативный инструмент JPSEC, который определяется при помощи приложения, определяемого пользователем.

3.15.4 JPSEC registration authority tool – инструмент органа регистрации JPSEC: ненормативный инструмент JPSEC, определяемый органом регистрации JPSEC.

3.16 JPSEC tool description – описание инструмента JPSEC: Описание параметров, используемых инструментом JPSEC.

ПРИМЕЧАНИЕ. – Однако описание инструмента JPSEC не описывает используемый метод или алгоритм. Описание инструмента JPSEC состоит их двух частей: списка параметров и их значений. В случае нормативных инструментов JPSEC, список параметров задается стандартом. В случае ненормативных инструментов JPSEC, список параметров может быть задан органом регистрации. В обоих случаях, значения параметров указываются в сегментах маркеров SEC и INSEC.

3.17 key – ключ: Последовательность символов, управляющая операциями шифрования и расшифровки.

3.17.1 symmetric keys – симметричные ключи: Пара ключей, в которой как отправитель, так и получатель используют один и тот же секретный ключ, или два ключа, которые можно легко вычислить один из другого в системе шифрования.

3.17.2 asymmetric key pair – асимметричная пара ключей: Пара ключей, в которой частный ключ определяет частное преобразование, а открытый ключ определяет открытое преобразование.

3.17.2.1 private key – частный ключ: Ключ асимметричной пары ключей, который не следует разглашать.

3.17.2.2 public key – открытый ключ: Ключ асимметричной пары ключей, который может быть общедоступным.

3.18 key generation, key generating function – генерирование ключа, функция генерирования ключа: Функция, которая берет в качестве входных данных несколько параметров, по крайней мере, один из которых должен быть секретным, и в качестве выходных данных выдает ключи в соответствии с намеченным алгоритмом и приложением.

ПРИМЕЧАНИЕ. – Для данной функции должно быть невозможно вычислить выходные данные без знания секретных входных данных.

3.19 key management – управление ключами: Генерирования, хранение, распространение, удаление, архивация и приложение ключей в соответствии с политикой безопасности.

3.20 marker emulation – эмуляция маркера: Зашифрованный текст, получающийся в результате процесса шифрования, который содержит начальную последовательность битов/начальный код JPEG.

3.21 message authentication code algorithm, cryptographic check function, cryptographic checksum function – алгоритм кода аутентификации сообщения, функция проверки шифрования, функция контрольной суммы: Алгоритм для вычисления функции, которая устанавливает соответствие между строками битов и секретным ключом и строками битов фиксированной длины, соблюдая следующие два условия:

- для любого ключа и любой строки входных данных данная функция может быть рационально вычислена;
- для любого фиксированного ключа, если ключ заранее не известен, невозможно вычислить значение функции по любой новой строке входных данных, даже если заданы набор строк входных данных и соответствующие значения функции, где значение i-й строки входных данных может быть выбрано после просмотра значения первых значений функции i-1.

ПРИМЕЧАНИЕ. – Возможность вычисления зависит от определенных требований безопасности и окружения пользователя.

3.21.1 message authentication code (MAC) – код аутентификации сообщения: Строка битов, являющая выходными данными алгоритма MAC.

3.22 non-repudiation – неотказуемость: Привязка объекта к операции, в которой он участвует так, чтобы в последствии от данной операции невозможно было отказаться (отрицать).

ПРИМЕЧАНИЕ. – То есть получатель операции может продемонстрировать нейтральной третьей стороне, что предполагаемый отправитель не выполнял операцию.

3.23 packet – пакет: Часть потока битов Части 1 JPEG 2000, в которую входят заголовок пакета и сжатые данные изображения с одного уровня одного участка одного разрешения одного компонента элемента изображения.

ПРИМЕЧАНИЕ. – Этот термин отличается от термина "пакет", используемого в передаче данных по сети.

3.24 protection – защита: Процесс обеспечения безопасности содержания.

3.24.1 protection template – шаблон защиты: Шаблон или список полей параметров, необходимых для работы метода защиты.

3.24.2 protection method – метод защиты: Метод, используемый для создания или потребления защищенного содержания, такой, как шифрование, расшифровка, аутентификация, проверка целостности.

3.25 security – безопасность: Все аспекты, относящиеся к определению, архивации и техническому обслуживанию конфиденциальности, целостности, доступности, проверяемости, подлинности и надежности.

ПРИМЕЧАНИЕ. – Продукт, система или услуга считаются безопасными настолько, насколько пользователи могут положиться на то, что они функционируют (или будут функционировать) надлежащим образом. Обычно этот аспект рассматривается в контексте определения реальных или воспринимаемых угроз.

3.26 signalling syntax – синтаксис сигнализации: Спецификация формата кодового потока JPSEC, содержащего всю требующуюся информацию для потребления защищенных изображений JPEG 2000.

3.27 transcoding – перекодировка: Операция, в ходе которой берется входящий сжатый кодовый поток, затем этот поток адаптируется или конвертируется, и получается выходной сжатый кодовый поток, обладающий требуемыми свойствами.

ПРИМЕР. – Выходной сжатый кодовый поток может представлять изображение с пространственным разрешением или битовой скоростью ниже, чем у входящего сжатого кодового потока.

3.27.1 secure transcoding – защищенная перекодировка: Операция, в ходе которой происходит перекодировка или адаптация защищенного входного сжатого содержания, без незащищенного содержания.

ПРИМЕЧАНИЕ. – Термин "защищенная перекодировка" используется, в противоположность перекодировке, чтобы подчеркнуть, что операция перекодировки выполняется без ущерба безопасности. Защищенную перекодировку можно также назвать осуществлением перекодировки в зашифрованной области.

3.28 watermark – водяной знак: Сигнал, незаметно добавляемый к основному сигналу для того, чтобы передать скрытые данные.

3.28.1 watermarking: Процесс, в ходе которого в мультимедийные данные незаметно вставляются данные, представляющие некоторую информацию, одним из следующих способов:

- Способ с частичной потерей информации, при котором после того, как вставлен водяной знак, восстановить основной сигнал в точности будет нельзя.
- Способ без потерь, при котором восстановить основной сигнал в точности можно после извлечения водяного знака.

4 Символы и сокращения

Для целей данной Рекомендации | Международного стандарта используются следующие сокращения.

BAS	Byte Aligned Segmen	Сегмент, выровненный по байтам
FBAS	Field Byte Aligned Segment	Поле-сегмент, выровненный по байтам
G	Granularity	Степень структурирования
GL	Granularity Level	Уровень степени структурирования
INSEC	In codestream security marker	Маркер безопасности внутри кодового потока
IP	Intellectual Property related to technology	Интеллектуальная собственность, относящаяся к технологии
IPR	Intellectual Property Rights related to content	Права интеллектуальной собственности, связанные с содержанием
JPSEC	Secure JPEG 2000	Защищенный JPEG 2000
KT	Key Template	Шаблон ключей
LSB	Least Significant Bit	Наименее значимый бит
MAC	Message Authentication Code	Код аутентификации сообщения
MSB	Most Significant Bit	Наиболее важный бит
PD	Processing Domain	Область обработки
PKI	Public Key Infrastructure	Инфраструктура открытых ключей
PO	Processing Order	Порядок обработки

RA	Registration Authority	Орган регистрации
RBAS	Range Byte Aligned Segment	Диапазон-сегмент, выровненный по байтам
SEC	Security marker	Маркер безопасности
T	Template	Шаблон
V	Values	Значения
VL	Value List	Список значений
ZOI	Zone of Influence	Зона влияния

5 Синтаксис JPSEC (нормативный)

5.1 Обзор структуры JPSEC

JPSEC определяет структуру для обеспечения безопасности данных, закодированных JPEG 2000. Основной частью данной Рекомендации | Международного стандарта является спецификация синтаксиса защищенного изображения JPEG 2000, *кодового потока JPSEC*. Данный синтаксис направлен на закодированные данные JPEG 2000 и делает возможной защиту всего кодового потока или частей кодового потока. Во всех случаях защищенные данные (т. е. кодовый поток JPSEC) должны соответствовать нормативному синтаксису, определенному в данной Рекомендации | Международном стандарте.

С кодовым потоком JPSEC связано несколько *услуг безопасности JPSEC,* включая конфиденциальность и аутентификацию происхождения и содержания.

Синтаксис сигнализации устанавливает:

- какие услуги безопасности связаны с данными изображения;
- какие *инструменты JPSEC* требуются для оказания соответствующих услуг;
- как применяются инструменты JPSEC;
- какие части данных изображения защищаются.

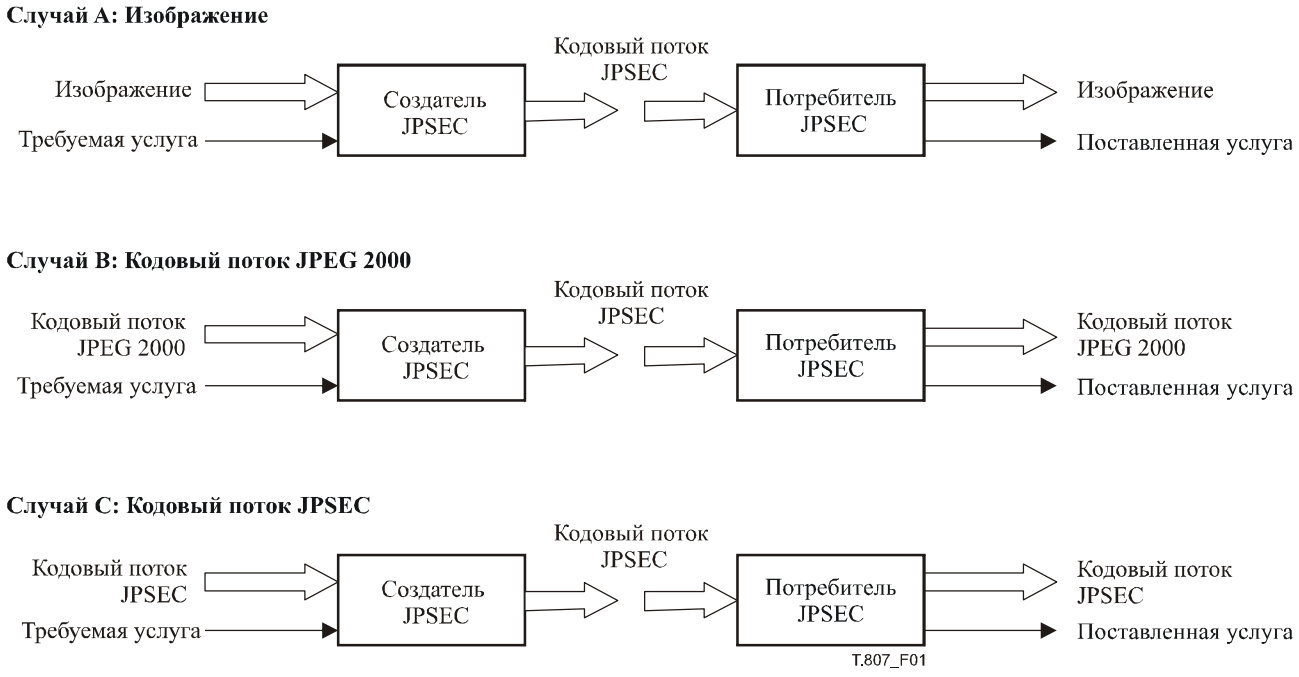


Рисунок 1 – Обзор концептуальных этапов в структуре JPSEC

Синтаксис кодового потока JPSEC является нормативным. Целью его является предоставление приложениям JPSEC возможности потреблять кодовые потоки JPSEC с возможностью взаимодействия сетей (см. рисунок 1). Приложение потребителя JPSEC интерпретирует кодовый поток JPSEC, идентифицирует и применяет сигнализированные инструменты JPSEC, предоставляет соответствующие услуги безопасности, а затем передает выходной кодовый поток или изображение JPEG 2000 для последующей обработки, например, программой просмотра изображений.

Как показано в случае С рисунка 1, кодовый поток JPSEC может быть создан из другого кодового потока JPSEC. Это может произойти, когда к одному и тому же содержимому применяются многочисленные инструменты JPSEC, но в разное время и разными объектами. Когда это происходит, важным может быть порядок, в котором применяются инструменты JPSEC во время операций создания и потребления.

Синтаксис сигнализации идентифицирует инструменты, используемые потребителем JPSEC. Инструменты определяются либо нормативной частью стандарта, либо регистрационным органом, либо частными инструментами. Нормативно определяемые инструменты поддерживают конфиденциальность (посредством инструментов шифрования), и аутентификацию источника и содержания. Они делают возможным высочайший уровень способности к взаимодействию, поскольку независимые реализации потребляющего процесса могут обрабатывать один и тот же кодовый поток JPSEC и оказывать соответствующие услуги с одним и тем же режимом работы.

То, каким образом создается кодовый поток JPSEC, находится вне области применения данной Рекомендации | Международного стандарта. Чтобы быть совместимыми, создатели JPSEC должны генерировать кодовые потоки JPSEC, включающие соответствующую сигнализацию JPSEC. Создать кодовые потоки JPSEC можно несколькими способами. Например, можно применить инструмент JPSEC к пикселам изображения или к коэффициентам волны малой амплитуды, или к квантованным коэффициентам, или к пакетам.

Потребитель может реализовывать один или более инструментов JPSEC. Например, можно выполнить расшифровку, используя блочный шифр AES в режиме ECB, и подтверждение подлинности подписи, используя хэш-функцию SHA-128 и открытый ключ RSA. С этими возможностями, можно будет выполнять такие услуги безопасности, как конфиденциальность и аутентификация.

В структуре JPSEC, инструменты JPSEC определяются шаблонами, определяемыми в частном порядке, или регистрируемыми *Органом регистрации JPSEC*. Инструменты JPSEC, определяемые шаблонами, имеют уникальный режим обработки и поэтому не требуют уникальной идентификации. Инструменты, определяемые органом регистрации, связаны с уникальным идентификационным номером, предоставляемым общим блоком регистрации.

5.2 Услуги безопасности JPSEC

Целью данного подпункта является перечисление и объяснение функциональных возможностей, включенных в область применения данной Рекомендации | Международного стандарта.

Инструменты JPSEC используются для выполнения функций безопасности. JPSEC является открытой структурой, что означает, что в будущем ее можно будет расширить. В настоящее время она концентрируется на следующих аспектах:

– *Конфиденциальность через шифрование и выборочное шифрование*

  Файл JPSEC может поддерживать трансформацию (изображения и/или метаданных) данных (открытый текст) в форму (зашифрованный текст), скрывающую первоначальное значение данных. Под выборочным шифрованием мы подразумеваем, что могут быть зашифрованы не все изображение и/или метаданные, а только части изображения и/или метаданных.

– *Проверка целостности*

  Файл JPSEC может поддерживать средства обнаружения манипуляций с изображением и/или метаданными и, таким образом, подтверждать их подлинность. Существует два класса проверки подлинности:

  1) Проверка целостности данных, при которой даже если только один бит данных изображения оказывается ошибочным, это приводит к ошибке проверки (т. е. в результате проверки получается "нет целостности"). Данный тип проверки также часто называется хрупкая проверка (целостности) изображения.

  2) Проверка целостности содержания изображения, при которой даже некоторое случайное изменение данных изображения приводит к успеху проверки, пока данное изменение не меняет содержание изображения с точки зрения зрительной системы человека; другими словами, значение восприятия изображения не изменяется. Такую проверку часть называют полухрупкой проверкой (целостности) изображения.

  Хрупкая или полухрупкая проверки целостности изображения могут идентифицировать месторасположения в данных изображения/содержании изображения, где целостность находится под вопросом. Решения могут включать в себя:

  1) Криптографические методы такие, как Коды аутентификации сообщения (MAC), цифровые подписи, криптографические контрольные суммы файла или закодированная хэш-функция.

2) Методы на основе "водяных знаков". В данной Рекомендации | Международном стандарте не определяется нормативный шаблон для технологии "водяных знаков", хотя она поддерживает ненормативные инструменты, использующие технологию "водяных знаков".

3) Комбинацию двух вышеупомянутых типов методов.

– *Аутентификация источника*

Файл JPSEC может поддерживать проверку целостности пользователя/стороны, которая сгенерировала данный файл JPSEC. Это может включать в себя методы, например, цифровой подписи или кода аутентификации сообщения (MAC).

– *Условный доступ*

Файл JPSEC может поддерживать механизм и политику для выдачи или ограничения доступа к данным изображения или части данных изображения. Это может позволить, например, просматривать изображение в низком разрешении (предварительный просмотр) без возможности визуализировать его при высоком разрешении.

– *Идентификация зарегистрированного содержания*

Файл JPSEC может быть зарегистрирован в Органе регистрации содержания. Он может поддерживать метод сопоставления (заявленных) данных изображения/содержания изображения с зарегистрированными данными изображения/содержанием изображения. Например, таким методом может быть: Чтение идентификатора файла (Лицензии), который был помещен внутрь метаданных, проверка согласованности между Лицензией и информацией, которая была загружена, когда процесс регистрации был выполнен. Лицензия может содержать достаточно информации, чтобы запрашивать информацию у органа регистрации, где данный файл был зарегистрирован, и проверять, соответствует ли файл идентификатору.

– *Защищенная масштабируемая потоковая передача данных и защищенная перекодировка*

Файл JPSEC или последовательность пакетов может поддерживать такие методы, что одинаковые или различные узлы могут выполнять потоковую передачу данных и перекодировку, не требуя регистрации или снятия защиты с содержания. Примером является случай, при котором защищенное содержание JPEG 2000 передается потоком на узел в середине сети или прокси, который, в свою очередь, перекодирует защищенное содержание JPEG 2000 таким образом, что оно сохраняет сквозную безопасность.

5.3 Комментарии по разработке и реализации защищенных систем JPSEC

Данная Рекомендация | Международный стандарт поддерживает широкий и гибкий набор услуг безопасности. Например, примитивы шифрования могут применяться различными способами для достижения различных целей, от шифрования всего кодового потока JPEG 2000 до выборочного шифрования только небольшой части кодового потока. Однако важно подчеркнуть, что при реализации любой системы безопасности, включая систему на основе JPSEC, следует быть очень осторожным.

Настоятельно рекомендуется, чтобы разработчики любой системы безопасности тщательно обдумывали рекомендуемые рекомендации для используемых примитивов безопасности. Для большинства примитивов безопасности, сигнализированных при помощи JPSEC, соответствующие стандарты ИСО/МЭК предоставляют важные рекомендации по их правильному использованию. Например, для шифрования, использующего блочный шифр и соответствующий режим блочного шифра (таблица 29), рекомендации по выбору режима блочного шифра и его работе даются в ИСО/МЭК 10116.

Кроме того, во многих приложениях безопасности аутентификация является наиболее важной услугой безопасности. Даже когда конфиденциальность является основной услугой безопасности, ее следует расширить за счет аутентификации для предотвращения различных форм атак. В особенности, даже во многих приложениях создания изображений, где конфиденциальность является основной целью, рекомендуется также использовать аутентификацию.

Управление ключами находится вне области применения JPSEC, однако следует подчеркнуть его важность. В любой криптографической системе управление ключами шифрования, контролирующими все операции, представляет чрезвычайную важность. Если эти ключи были подвергнуты риску, риску была подвержена безопасность всей системы, и, таким образом, что опасность не может быть обнаружена. Поэтому необходимо, чтобы генерирование, распределение, хранение и уничтожение ключей происходило на уровне безопасности, по крайней мере равном уровню безопасности данных, которые они защищают. Кроме того, поскольку вероятность подвергания ключа риску возрастает со временем, также необходимо, чтобы ключи использовались только в течение определенного срока. Более подробную информацию по использованию и управлению ключами шифрования см. в ИСО/МЭК 11770.

Как и со всеми системами безопасности, использование операций шифрования должно быть полностью скрыто от пользователя. То есть пользователь не должен узнать никакой информации об операциях шифрования, кроме выходных данных. Например, пользователь не должен иметь доступ к информации о том, почему в результате операции шифрования не получилось выходных данных. Также пользователь не должен обнаружить никакой дополнительной информации, даже если он/она прибегнет к измерению "побочных каналов" таких, как синхронизация по времени и/или анализ мощности. Короче говоря, пользователь не должен заметить никакой разницы в каких бы то ни было выходных данных приложения, вне зависимости оттого, что в настоящий момент делает это приложение, поскольку если это не случай, ведущий к утечке информации, который может потенциально подвергнуть риску безопасность системы.

Подводя итоги, следует сказать, что настоятельно рекомендуется, чтобы разработчики любой системы безопасности, включая систему на основе JPSEC, уделяли особое внимание деталям разработки системы для гарантирования ее безопасности.

5.4 Сегмент, выровненный по байтам (BAS)

5.4.1 Сегмент, выровненный по байтам

Для того чтобы обеспечить расширяемую сигнализацию для классов и режимов, в данной Рекомендации | Международном стандарте используется структура данных переменной длины, называемая "сегмент, выровненный по байтам" (BAS). Поля параметров с расширяемым числом полей, представлены в структуре Поля BAS (FBAS). Значения параметров с большими диапазонами широко представлены со структурой Диапазон BAS (RBAS).

Как показано на рисунке 2, BAS состоит из последовательности одного или более байтов BAS. Наиболее важный бит (MSB) каждого байта BAS обозначает существование следующего байта BAS. В частности, если MSB = 1, тогда далее следует байт BAS, в то время как, если MSB = 0, тогда последующий байт BAS не существует, и структура BAS заканчивается. Оставшиеся наименее значимые биты каждого байта BAS объединяются в виде списка битов, которые используются различными способами для различных параметров BAS. Часто они используются вместе со списком параметров, имеющим несколько элементов, и каждый бит BAS установлен на 1 или 0 для того, чтобы обозначить информацию о соответствующем элементе. Эта гибкая структура была выбрана из-за возможности ее расширения для соответствия будущим стандартам, поскольку она позволяет сигнализировать о новых параметрах расширяемым способом.

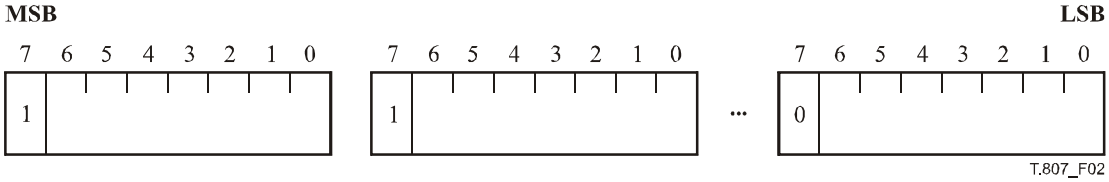


Рисунок 2 – Структура сегмента, выровненного по байтам (BAS)

5.4.2 Поле BAS (FBAS)

Поле BAS (FBAS) – это тип BAS, в котором оставшиеся биты байтов BAS используются для установки значений полей на 1 или 0. Примером использования FBAS является класс описания зоны влияния (DCzoi), где мы можем определить многочисленные определения изображения такие, как индекс элемента изображения, уровень разрешения и цветовой компонент. Если мы сделаем это, мы бы установили значение битов BAS, соответствующих элементу изображения, разрешению и цвету на 1.

Например, если бы мы хотели отобразить Поле BAS с 9 полями, от f1 до f9, тогда нам бы потребовалось использовать по крайней мере два байта BAS. Если бы эти два байта были байтами "a" и "b", наиболее важными битами каждого байта были бы a0 и b0, а FBAS выглядело бы следующим образом:

a0 a1 a2 a3 a4 a5 a6 a7 | b0 b1 b2 b3 b4 b5 b6 b7

a0 и b0 являются битами индикаторами. Поля от f1 до f7 представлены в битах от a1 до a7, поле f8 находится в бите b1, а поле f9 – в бите b2. Значение оставшихся битов от b3 до b7 зарезервировано и установлено на 0.

a0 f1 f2 f3 f4 f5 f6 f7 | b0 f8 f9 0 0 0 0 0

При использовании в потоке JPSEC, FBAS в данном примере может быть представлено одним или двумя байтами, в зависимости от действительных значений данного поля. Это происходит из факта, что заданное по умолчанию значение данных полей – 0. Таким образом, если значения полей f8 и f9 не установлены (т. е. их

значение равно 0), тогда второй байт BAS не нужен, и значение a0 устанавливается на 0. С другой стороны, если значения полей 8 или 9 установлены, тогда необходимы два байта. В таком случае значение a0 устанавливается на 1, а значение b0 устанавливается на 0.

Отметим, что биты полей "выровнены по левой стороне". Это позволяет нам совместимым образом добавлять больше полей с течением времени.

5.4.3 Диапазон BAS (RBAS)

Диапазон BAS (RBAS) используется для расширения диапазона или числа битов, используемых для представления значения. Существует два типа RBAS – RBAS-8 и RBAS-16.

RBAS-8 содержит один или более байтов RBAS, содержащих биты со значением. Как и в FBAS, первый бит каждого байта обозначает, следует ли далее другой байт RBAS.

В отличие от FBAS, RBAS "выровнено по правой стороне". Таким образом, если значение имеет 9 важных битов от v1 до v9, где v1 является наиболее важным битом, тогда оно будет представлено двумя байтами BAS:

a0 a1 a2 a3 a4 a5 a6 a7 | b0 b1 b2 b3 b4 b5 b6 b7

следующее:

1 0 0 0 0 0 v1 v2 | 0 v3 v4 v5 v6 v7 v8 v9

Если значение было маленьким так, что значение битов v1 и v2 было равно нулю, с v1 и v2, установленными на 0, можно использовать двухбайтовое представление, описанное выше, или можно использовать однобайтовое RBAS следующим образом, показанным ниже:

0 v3 v4 v5 v6 v7 v8 v9

RBAS-16 можно использовать для представления значений, которые обычно больше 7 битов, но меньше 15 битов. В таком случае первой частью RBAS являются два байта, причем первый бит является индикатором, а следующие 15 битов являются битами значения, а оставшиеся байты, расширяют один байт за один раз, используя типичную структуру BAS, причем первый бит каждого байта является индикатором следующих байтов BAS.

a0 a1 a2 a3 a4 a5 a6 a7 | b0 b1 b2 b3 b4 b5 b6 b7 | c0 c1 c2 c3 c4 c5 c6 c7

Если бы значение параметра имело 22 бита, его можно было бы представить одной из трехбайтовых структур RBAS-16, показанных ниже, причем a0 и c0 являются битам индикации, для указания следует ли далее байта BAS. Все оставшиеся байты BAS являются традиционными – байтовыми сегментами BAS.

a0 v1 v2 v3 v4 v5 v6 v7 | v8 v9 v10 v11 v12 v13 v14 v15 | c0 v16 v17 v18 v19 v20 v21 v22

Таким образом, биты индикатора показывают, что следует установить на следующие значения:

1 v1 v2 v3 v4 v5 v6 v7 | v8 v9 v10 v11 v12 v13 v14 v15 | 0 v16 v17 v18 v19 v20 v21 v22

Как для RBAS-8 и RBAS-16, биты значения также "выравниваются по правой стороне".

Отметим, что при написании создателей и потребителей JPSEC, важно обратить внимание на большие конечные/небольшие конечные представления.

5.5 Основной маркер безопасности (SEC)

5.5.1 Сегменты маркера безопасности

В данном подпункте мы представляем простой и гибкий, однако мощный синтаксис для сигнализации JPSEC. Для этой цели определяются сегменты маркера SEC, и они располагаются в основном заголовке. Синтаксис сегмента маркера SEC позволяет описать всю требующуюся информацию для обеспечения безопасности изображений JPEG 2000. Для того чтобы сделать это, синтаксис делает ссылки на нормативные инструменты JPSEC, определяемые шаблонами, описанными в п. 5.8, или при помощи ненормативных инструментов JPSEC,

которые могли быть зарегистрированы заранее в органе регистрации JPSEC или были определены в частном порядке. Затем синтаксис обеспечивает обработку параметров, относящихся к данным инструментам.

Кодовый поток JPSEC может быть защищен при помощи одного или более инструментов JPSEC. Каждый инструмент является нормативным или ненормативным инструментом JPSEC. Параметры данных инструментов сигнализируются в одном или более сегментах маркера SEC, расположенных в основном заголовке кодового потока после сегмента маркера SIZ. Когда используется несколько сегментов маркера SEC, они объединяются и должны последовательно появляться в основном заголовке. В большинстве случаев, все параметры JPSEC могут быть сигнализированы в одном сегменте маркера SEC. Однако в некоторых случаях длина сигнализации может превышать максимальный размер сегмента маркера. Когда это происходит, для сигнализации можно использовать дополнительные сегменты маркера SEC.

На рисунке 3 показан синтаксис сегмента маркера SEC. О данном сегменте сигнализирует маркер SEC 0xFF65. L_{SEC} – это длина сегмента маркера SEC, включая 2 байта для L_{SEC}, но не 2 байта для самого маркера SEC. Z_{SEC} – это индекс сегмента маркера SEC. Значение Z_{SEC} должно быть установлено на 0 для первого сегмента маркера, который появляется в кодовом потоке. P_{SEC} – это поле параметра, описывающее параметры безопасности, существенные для всего кодового потока, оно существует только в первом сегменте маркера SEC, т. е. если $Z_{SEC} = 0$. Данный синтаксис поддерживает использование нескольких инструментов JPSEC, о которых сигнализируется в одном или более сегментах маркера. Если используется более одного инструмента JPSEC, потребитель JPSEC должен обрабатывать инструменты в том порядке, в котором они появляются в кодовом потоке.

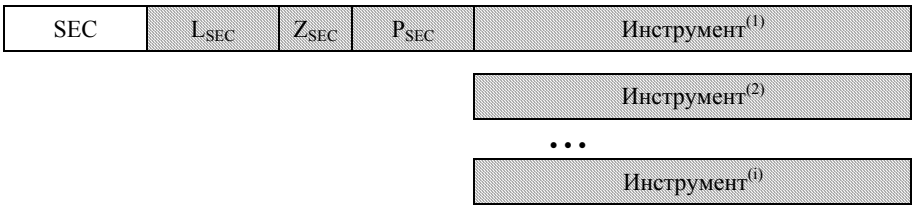


Рисунок 3 – Синтаксис основного сегмента маркера безопасности

SEC: Код маркера. В таблице 1 показаны размеры и значения символов и параметров для основного сегмента маркера безопасности.

L_{SEC}: Длина сегмента маркера в байтах (включая сам L_{SEC}, но исключая маркер).

Z_{SEC}: Индекс данного сегмента маркера, относящегося ко всем остальным сегментам маркера SEC, присутствующим в текущем заголовке. Это поле использует структуру RBAS.

P_{SEC}: Поле параметра для параметра безопасности кодового потока. Данное поле присутствует только в первом сегменте маркера SEC, т. е. когда Z_{SEC} равен 0.

Инструмент(i): Параметры для инструмента *i* JPSEC. Если сигнализируется о нескольких инструментах JPSEC, потребитель JPSEC должен обрабатывать все инструменты в порядке их появления в кодовом потоке JPSEC.

Таблица 1 – Значения основного параметра безопасности

Параметр	Размер (биты)	Значения
SEC	16	0xFF65
L_{SEC}	16	$2 \ldots (2^{16} - 1)$
Z_{SEC}	8 + 8 * n (RBAS)	$0 \ldots 2^{7+7*n}$
P_{SEC}	0, если $Z_{SEC} > 0$ В противном случае переменный	Если $Z_{SEC} = 0$, см. таблицу 2
Инструмент(i)	Переменный	См. пп. 5.6.2 и 5.6.3

На рисунке 4 показан синтаксис параметров безопасности в основном заголовке, когда используется несколько сегментов маркера SEC. В таком случае параметры инструмента JPSEC находятся в различных сегментах маркера SEC. Каждый сегмент маркера начинается с маркера SEC 0xFF65, а за ним следует длина и индекс сегмента маркера. Значение индекса первого сегмента маркера должно быть установлено на 0 и должно увеличиваться на один для каждого сегмента маркера в том порядке, как они появляются. Параметры безопасности для кодового потока содержатся только в первом сегменте маркера P_{SEC}. Все сегменты маркера содержат параметры для одного или более инструментов JPSEC.

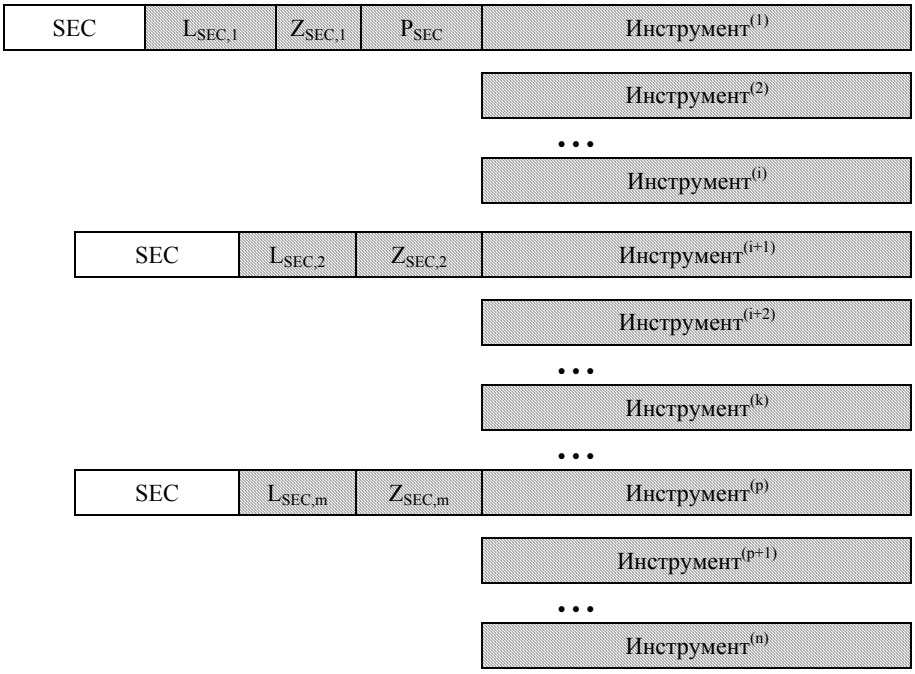


Рисунок 4 – Синтаксис основного маркера безопасности в случае использования нескольких сегментов маркера

Если потребуется, описание инструмента JPSEC может охватить несколько сегментов маркера SEC, например, это может произойти, если описание требует длины, превышающей максимальный размер маркера SEC. Поскольку длина описания инструмента полностью определена, создатель JPSEC просто разделяет инструмент по сегментам маркера SEC. Затем декодер должен объединить все сегменты, минус значения маркера SEC и L_{SEC} и Z_{SEC}, а затем интерпретировать данные инструменты соответствующим образом.

P_{SEC} – это поле параметра, описывающее параметры безопасности для всего кодового потока в противоположность определенному инструменту. Это поле используется для обозначения событий таких, как соответствие Части 1 JPEG 2000 или использование маркеров INSEC. Параметры P_{SEC} показаны на рисунке 5.

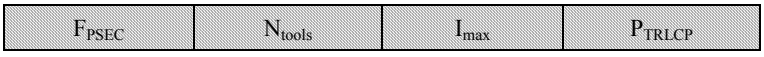


Рисунок 5 – Синтаксис параметров безопасности кодового потока (P_{SEC})

F_{PSEC}: Флаг для обозначения того, что используется сегмент маркера INSEC, если используются несколько сегментов маркера SEC, если первоначальные данные кодового потока Части 1 JPEG 2000 и если использование маркера TRLCP определено. Этим полем используется структура FBAS.

N_{tools}: Несколько инструментов JPSEC используются в кодовом потоке. Данное поле использует структуру RBAS.

I_{max}: Максимальное используемое значение указателя экземпляра для инструмента используется в кодовом потоке. Данное поле использует структуру RBAS.

P_{TRLCP}: Поле параметра для определения формата маркера TRLCP. Данное поле существует, если $F_{TRLCP} = 1$.

Таблица 2 – Параметры безопасности кодового потока (P_{SEC}) в первом сегменте маркера SEC

Параметр	Размер (биты)	Значения
F_{PSEC}	Переменный (FBAS)	См. таблицу 3
N_{tools}	8 + n * 8 (RBAS)	1 ... 2^{7+7*n}
I_{max}	8 + n * 8 (RBAS)	0 ... 2^{7+7*n}
P_{TRLCP}	0, если $F_{TRLCP} = 0$ 32, если $F_{TRLCP} = 1$	См. таблицу 4

F_{PSEC} – это структура FBAS, используемая для обозначения нескольких флагов параметров кодового потока JPSEC. Поля, представленные F_{PSEC}, показаны в таблице 3. Значение F_{INSEC} должно быть установлено на 1, если в кодовом потоке JPSEC используются маркеры INSEC. Значение $F_{multiSEC}$ должно быть установлено на 1, если в кодовом потоке JPSEC используется множество маркеров SEC. Значение F_{mod} должно быть установлено на 1, если первоначальные данные JPEG 2000 в кодовом потоке JPSEC были изменены. Отметим, что если используются маркеры INSEC, происходит изменение первоначальных данных JPEG 2000, и таким образом значения F_{INSEC} и F_{mod} должны быть установлены на 1. Значение F_{TRLCP} должно быть установлено на 1, если в P_{SEC} определено использование маркера TRLCP. Если маркер определен, в поле параметра P_{SEC} указывается дескриптор маркера TRLCP – P_{TRLCP}. Использование маркера TRLCP должно быть указано, если какой-либо инструмент в кодовом потоке JPSEC использует маркеры TRLCP.

Таблица 3 – Семантика значений F_{PSEC} (FBAS)

Поле BAS	Номер бита BAS	Значение (биты)	Семантика
F_{INSEC}	1	0	INSEC не используется
		1	INSEC используется
$F_{multiSEC}$	2	0	Используется один сегмент маркера SEC
		1	Используется множество сегментов маркера SEC
F_{mod}	3	1	Первоначальные данные JPEG 2000 были изменены
		0	В других случаях
F_{TRLCP}	4	0	Использование маркера TRLCP не определено в P_{SEC}
		1	Использование маркера TRLCP определено в P_{SEC}

JPSEC определяет структуру, называемую маркером TRLCP, которую можно использовать для уникальной идентификации пакета JPEG 2000. Пакет JPEG 2000 может быть уникально задан индексом элемента изображения, индексом уровня разрешения, индексом слоя, индексом компонента и индексом границы. Маркер TRLCP определяется как единица данных с фиксированным числом битов, используемых для точного определения каждого из данных значений индекса. Число битов для каждого индекса задается в P_{SEC}. P_{TRLCP} – это поле параметра, описывающее формат маркера TRLCP как он должен использоваться в инструментах JPSEC. Данное поле существует, только если $F_{TRLCP} = 1$. P_{TRLCP} состоит из следующих переменных на рисунке 6.

b_T	b_R	b_L	b_C	b_P	

дополнение

Рисунок 6 – Синтаксис дескриптора маркера TRLCP (P_{TRLCP})

b_T: Число битов для представления индекса элемента изображения – $b_T + 1$ в маркере TRLCP.

b_R: Число битов для представления индекса уровня разрешения – $b_R + 1$ в маркере TRLCP.

b_L: Число битов для представления индекса слоя – $b_L + 1$ в маркере TRLCP.

b_C: Число битов для представления индекса компонента – $b_C + 1$ в маркере TRLCP.

b_P: Число битов для представления индекса границы – $b_P + 1$ в маркере TRLCP.

Таблица 4 – Поле параметра для дескриптора маркера TRLCP (P_{TRLCP})

Параметр	Размер (биты)	Значения
b_T	8	0 ... (2^8 – 1)
b_R	4	0 ... 15
b_L	5	0 ... 31
b_C	5	0 ... 31
b_P	8	0 ... (2^8 – 1)
Дополнение	2	0

Размер каждого получающегося в результате маркера TRLCP представляет собой наименьший размер целого байта, содержащего все эти биты. Формат маркера TRLCP содержит биты для индекса элемента изображения, индекс уровня разрешения, индекс слоя, индекс компонента и индекс границы в таком порядке. Если для удовлетворения требованию размера целых байтов необходимы дополнительные биты, маркер TRLCP будет помещен в как можно менее важные биты, а значение дополнительных битов будет установлено на 0. Отметим, что эти дополнительные биты будут MSB маркера TRLCP, если они существуют.

5.5.2 Приложение множества инструментов JPSEC

Во многих приложениях необходимо применять множество инструментов JPSEC к одному потоку JPEG 2000. Например, для защиты изображения JPEG 2000 могут применяться шифрование и аутентификация. Общая ситуация применения многочисленных инструментов JPSEC изображена на рисунках 3, 4 и 7, где применяется N инструментов. Потребитель JPSEC прочитает N инструментов в порядке расположения в сегменте маркера SEC, показанного на рисунке 3 или рисунке 4, и применит их в том же порядке для выполнения потребления JPSEC в кодовом потоке JPSEC. Отметим, что, в то время как потребитель JPSEC применяет инструменты JPSEC в порядке 1, 2, ... , N, по мере прочтения из сегмента маркера SEC, во время создания кодового потока JPSEC эти инструменты JPSEC применялись в обратном порядке, т. е. N, N – 1, ... , 2, 1, как показано на рисунке 7. Отметим, что нумерация инструментов на рисунке была выбрана для того, чтобы подчеркнуть, что потребитель JPSEC применяет инструменты JPSEC в порядке, обратном порядку создателя JPSEC. Однако допустима любая нумерация инструментов JPSEC, поскольку любому инструменту JPSEC в кодовом потоке JPSEC дается уникальный номер для целей идентификации.

В сущности, инструменты JPSEC создаются и потребляются в обратном друг для друга порядке. Например, если создатель JPSEC применяет N инструментов JPSEC, тогда потребитель JPSEC обычно применяет те же N инструментов JPSEC, но в обратном порядке. Правильное потребление JPSEC многочисленных инструментов JPSEC можно гарантировать при помощи последовательного потребления N инструментов в правильном порядке, а также при помощи требования, чтобы любая промежуточная стадия у потребителя совпадала с соответствующим состоянием у создателя. Например, на рисунке 7, состояние у потребителя JPSEC после потребления инструмента 1 должно быть равно состоянию после применения инструмента 2 во время процесса создания. В качестве особого примера данного состояния, байтовые диапазоны должны быть совместимыми, поэтому все байты, добавленные при применении инструмента 1, должны быть удалены при удалении инструмента 1 у потребителя JPSEC.

В определенных приложениях может быть желательным, чтобы потребитель JPSEC потреблял многочисленные инструменты JPSEC способом, отличным от описанного выше. Например, потребитель JPSEC может предпочесть потреблять многочисленные инструменты в другом порядке или пропустить определенные инструменты при потреблении. Кроме того, потребитель JPSEC может предпочесть применение определенных инструментов JPSEC без удаления их, например, проверить электронную подпись, но не удалять ее. В таких случаях следует обратить особое внимание, чтобы гарантировать, что обработка не по порядку или с пропусками не приведет к неверным или непредвиденным последствиям. Такой режим работы не рекомендуется, если приложения JPSEC полностью не осознают потенциальных расхождений.

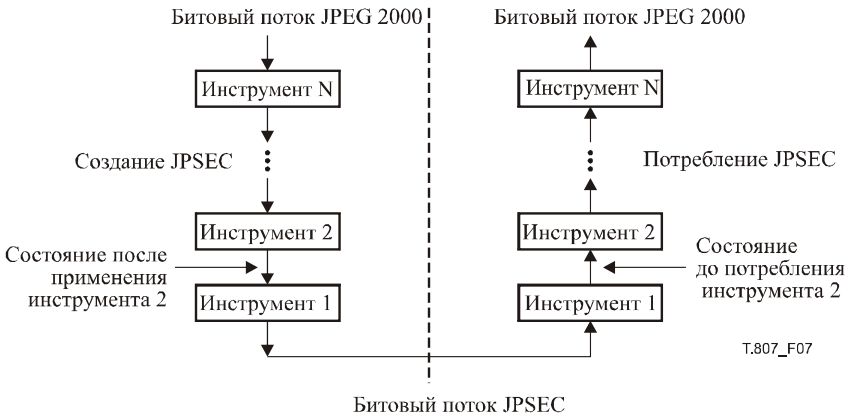


Рисунок 7 – Использование многочисленных инструментов JPSEC

5.6 Инструменты JPSEC

5.6.1 Синтаксис инструмента JPSEC

Как упоминалось ранее, существуют два типа инструментов JPSEC. Нормативные инструменты JPSEC задаются шаблонами метода защиты, описанными в п. 5.8, и также называются нормативными инструментами JPSEC. Ненормативные инструменты JPSEC определяются органом регистрации JPSEC или определенным приложением JPSEC на основе их идентификационного номера и, соответственно называются инструменты органов регистрации JPSEC или инструментами, определяемыми пользователями JPSEC. Синтаксис нормативных инструментов JPSEC описан в п. 5.6.2. Синтаксис ненормативных инструментов JPSEC описан в п. 5.6.3.

Синтаксис инструментов JPSEC показан на рисунке 8. Синтаксис инструмента JPSEC имеет три основные части:

1) какой инструмент применяется с его идентификацией;
2) где данный инструмент применяется с зоной структуры влияния; и
3) как данный инструмент применяется с более детализированным полем параметра.

Например, используя данный синтаксис, синтаксис инструмента JPSEC может указывать, что к компоненту наименьшего разрешения, расположенному в определенном байтовом диапазоне (где), следует применить инструмент расшифровки (что), используя расшифровку AES в режиме CBC при точно определенном наборе векторов и ключей инициализации (как).

Рисунок 8 – Синтаксис инструмента JPSEC (Инструмент$^{(i)}$)

t: Тип инструмента. Значение 0 для первого бита BAS указывает на нормативный инструмент JPSEC. Значение 1 для первого бита BAS указывает на ненормативный инструмент JPSEC. В данном поле используется структура FBAS.

i: указатель экземпляра инструмента (может использоваться в качестве уникального идентификатора). В данном поле используется структура RBAS.

ID: Значение идентификации для инструмента *i* JPSEC. Для нормативных инструментов JPSEC ID = ID_T составляет 8 битов и определяет тип шаблона. Для ненормативных инструментов JPSEC ID = ID_{RA} определяется по рисунку 10 и таблице 8.

L_{ZOI}: Длина ZOI в байтах (без учета L_{ZOI}). В данном поле используется структура RBAS.

ZOI: Зона влияния для инструмента *i* JPSEC.

L_{PID}: Длина P_{ID} в байтах (без учета L_{PID}). В данном поле используется структура RBAS.

P_{ID}: Параметры для инструмента *i* JPSEC.

Таблица 5 – Значения параметра инструмента JPSEC

Параметр	Размер (биты)	Значения
t	8 + 8 * n (FBAS)	x0xx xxxx $_b$, x1xx xxxx $_b$
i	8 + 8 * n (RBAS)	0 ... (2^{7+7*n} – 2) (2^{7+7*n} – 1), зарезервировано
ID	8, если t = 0 Переменный, если t = 1	См. таблицу 6 См. рисунок 10 и таблицу 8
L_{ZOI}	16 + 8 * n (RBAS)	0 ... 2^{15+7*n}
ZOI	Переменный	См. п. 5.7
L_{PID}	16 + 8 * n (RBAS)	0 ... 2^{15+7*n}
P_{ID}	Переменный	Таблица 7, если t = 0 Управляется Органом регистрации JPSEC, если t = 1

Каждый инструмент JPSEC имеет следующий синтаксис. Один первоначальный байт указывает, является ли инструмент нормативным или ненормативным инструментом JPSEC, и присваивает идентификатор экземпляра данному инструменту. Затем следует идентификатор инструмента **ID**. За ним следует L_{ZOI}, который указывает

длину последующего поля зоны влияния ZOI, и сама зона влияния, в которой описывается, в каком месте потока данных применяется инструмент JPSEC. Затем следует L_{PID}, который указывает длину следующего поля параметра P_{ID}, которое предназначено для передачи одного или более параметров инструмента JPSEC.

В первом байте данного инструмента используется однобайтовая структура FBAS, первый бит BAS которой представляет тип инструмента t, причем 0 определяет нормативный инструмент JPSEC, а 1 определяет ненормативный инструмент JPSEC. Затем следует указатель экземпляра i, который представлен при помощи использования структуры RBAS. Указатель экземпляра должен представлять собой уникальный идентификатор инструмента в рамках кодового потока, и, таким образом, не должен повторяться никаким другим инструментом в данном кодовом потоке, даже если он находится в другом сегменте маркера SEC. Указатель экземпляра особенно важен (и необходим), когда используются маркеры INSEC, поскольку каждый сегмент маркера INSEC содержит указатель экземпляра того инструмента, к которому он применяется. Рекомендуется, чтобы первый инструмент, применяемый в создателе JPSEC, имел указатель экземпляра равный 1, и чтобы присвоение индексов (указателей) происходило последовательно в том порядке, в котором инструменты применяются на устройстве защиты.

Кроме того, каждый инструмент JPSEC имеет идентификационный номер, который состоит из 8 битов для нормативных инструментов JPSEC и из 32 битов для ненормативных инструментов JPSEC. Для нормативных инструментов JPSEC идентификационный номер описывает, какой шаблон метода защиты используется, т. е. он определяет шаблон расшифровки, шаблон аутентификации или шаблон хэш-функции. Для ненормативных инструментов JPSEC первый бит указывает, является ли данный инструмент инструментом JPSEC органа регистрации или инструментом JPSEC, определяемым пользователем. В любом случае идентификационный номер указывает на определенный инструмент. Орган регистрации JPSEC может гарантировать уникальность действительных идентификационных номеров. Однако приложение JPSEC, использующее идентификационные номера, определяемые пользователем, подвергаются риску выбора идентификационного номера, уже используемого другим приложением JPSEC, поэтому их следует использовать с осторожностью.

Когда на создателе JPSEC применяется каждый инструмент JPSEC, поле параметра P_{SEC}, показанное в таблице 2, должно обновляться. Например, поле параметра P_{SEC} содержит параметр I_{max}, определяющий максимальный указатель экземпляра, используемый для всех инструментов в данном кодовом потоке JPSEC. Когда применяется новый инструмент, ему нужно присвоить уникальный указатель экземпляра. Чтобы определить, какой указатель экземпляра следует присвоить инструменту JPSEC, устройство защиты JPSEC может обратиться к параметру I_{max}, заданному в поле параметра P_{SEC}, например, оно может выбрать значение, которое больше текущего значения I_{max} на один, затем устройство защиты должно увеличить значение I_{max} на 1, соответственно.

5.6.2 Нормативный инструмент JPSEC

Нормативный инструмент JPSEC использует синтаксис инструмента JPSEC, описанный в п. 5.6.1 и показанный на рисунке 8, причем тип инструмента t = 0, а размер ID равен 8 битам. Нормативные инструменты JPSEC основаны на шаблонах метода защиты, описанных в п. 5.8. Существует три типа шаблонов методов защиты; тип, используемый данным инструментом, определяется идентификатором инструмента $ID = ID_T$ при помощи использования значений, приведенных в таблице 6.

Таблица 6 – Значения Шаблона ID нормативного инструмента JPSEC (ID_T)

Значения	Шаблон метода защиты
0	Зарезервировано
1	Шаблон расшифровки
2	Шаблон аутентификации
3	Шаблон хэш-функции
4	Инструмент NULL
	Все остальные значения, зарезервированные для использования ИСО

В случае использования нормативных инструментов JPSEC поле параметра P_{ID} имеет структуру, показанную на рисунке 9. P_{ID} состоит из четырех основных полей: шаблон метода защиты T, обрабатывающая область PD, степень его структурирования G и список его значений V. Синтаксис для каждого из этих полей дан в пп. 5.8, 5.9, 5.10 и 5.11, соответственно. Вместе эти поля описывают, как применяется данный инструмент. Шаблон метода защиты T описывает определенный метод защиты для шаблона расшифровки, шаблона аутентификации или шаблона хэш-функции, определенных ID нормативного инструмента. Здесь также может задаваться инструмент NULL, в таком случае не используется никакого шаблона, но могут использоваться другие функциональные возможности. Например, может быть определено, что зона влияния представляет участки изображения и соответствующие им байтовые диапазоны. Обрабатывающая область PD описывает область, в которой применяется метод защиты. Степень структурирования G описывает степень структурирования, с

которой применяется метод защиты. Список значений V содержит значения, которые могут потребоваться каждому методу защиты с более высокой степенью структурирования. Для шаблона расшифровки список значений может использоваться для определения более высокой степени структурирования набора значений инициализации, которые необходимо использовать. Для шаблона аутентификации список значений содержит набор значений MAC или цифровые подписи. Для шаблона хэш-функции список значений содержит набор значений хэш-функции. Во всех случаях список значений содержит степень структурирования значений, определяемых полем Степень структурирования G.

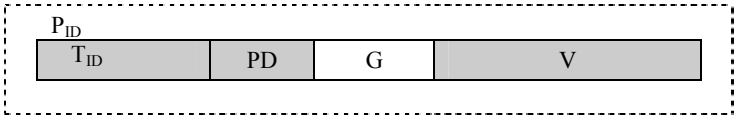


Рисунок 9 – Синтаксис параметров (P_{ID}) для нормативных инструментов JPSEC (t = 0)

T_{ID}: Параметры шаблона для нормативного инструмента JPSEC с идентификатором шаблона ID_T.

PD: Обрабатывающая область для нормативного инструмента JPSEC.

G: Степень структурирования для нормативного инструмента JPSEC.

V: Список значений для нормативного инструмента JPSEC, например, векторы инициализации, значения MAC, цифровые подписи или значения хэш-функции, зависящие от ID шаблона.

Отметим, что параметры шаблона зависят от ID шаблона. Однако Область обработки, Степень структурирования и Список значений не зависят от ID шаблона.

Таблица 7 – Значения параметра нормативного инструмента JPSEC

Параметр	Размер (биты)	Значения
T_{ID}	0, если $ID_T = 4$ В остальных случаях переменный	Не используется См. п. 5.8
PD	Переменный	См. п. 5.9
G	24	См. п. 5.10
V	Переменный	См. п. 5.11

5.6.3 Ненормативный инструмент JPSEC

В определенных случаях может оказаться полезным, если приложение JPSEC сможет применить инструмент, выходящий за рамки нормативных инструментов JPSEC. Эта возможность обеспечивается при помощи использования ненормативного инструмента JPSEC. Это позволяет использовать многие элементы нормативных инструментов JPSEC, включая шаблоны ZOI и JPSEC, но добавляет гибкости при использовании данных параметров другим способом, связанным со значением ID инструмента.

Ненормативный инструмент использует синтаксис инструмента JPSEC, описанный в п. 5.6.1 и показанный на рисунке 8, где тип инструмента t = 1, а идентификатор ID_{RA} состоит из пространства имен и номера ID, как определено на рисунке 10 и таблице 8.

Существует два класса ненормативных инструментов JPSEC:

1) Инструменты JPSEC органа регистрации: ненормативные инструменты JPSEC, сигнализация которых определяется органом регистрации.
2) Инструменты JPSEC, определяемые пользователем: ненормативные инструменты JPSEC, сигнализация которых определяется приложением JPSEC.

Сигнализация данных двух классов ненормативных инструментов JPSEC осуществляется при помощи 32-битного идентификатора $ID_{RA,id}$, показанного в таблице 9. Идентификаторы, значение первого бита которых равно 0, определяются органом регистрации, а те идентификаторы, значение первого бита которых равно 1, определяются отдельным приложением JPSEC.

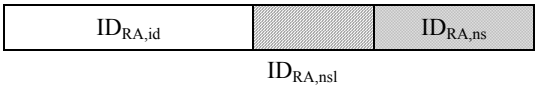


Рисунок 10 – Синтаксис ID_{RA}

$ID_{RA,id}$: Идентификатор инструмента для инструмента RA и инструмента, определяемого пользователем

$ID_{RA,nsl}$: Длина поля $ID_{RA,ns}$ в байтах. В данном поле используется RBAS.

$ID_{RA,ns}$: Строка, содержащая пространство имен указанного инструмента RA или инструмента, определяемого пользователем.

Таблица 8 – Значения параметров в синтаксисе ID_{RA}

Параметр	Размер (бит)	Значения
$ID_{RA,id}$	32	См. таблицу 9
$ID_{RA,nsl}$	8 + 8 * n (RBAS)	0 ... $(2^{7+7*n} - 1)$
$ID_{RA,ns}$	Переменный	Строка, содержащая пространство имен

Таблица 9 – Значения ID для ненормативных инструментов JPSEC ($ID_{RA,id}$)

$ID_{RA,id}$	Значение
0x00 00 00 00 ... 0x7F FF FF FF	Инструмент JPSEC органа регистрации. Значениями должен управлять орган регистрации JPSEC
0x80 00 00 00 ... 0xEF FF FF FF	Инструмент JPSEC, определяемый пользователем. Значения могут определяться отдельным приложением JPSEC
0xF0 00 00 00 ... 0xFF FF FF FF	Зарезервировано для использования ИСО

Для инструментов RA поле $ID_{RA,ns}$ содержит пространство имен Органа регистрации (RA), в котором зарегистрирован данный инструмент. Поскольку каждый RA имеет уникальное пространство имен, для идентификации инструмента RA $ID_{RA,id}$ и $ID_{RA,ns}$ используются вместе. Для инструментов, определяемых пользователем, разработчиками было выбрано поле $ID_{RA,ns}$. Для того чтобы ограничить риск конфликтов ID, рекомендуется, чтобы разработчики стремились к уникальности при выборе пространства имен, например, путем выбора доменного имени их организации или компании. Отметим, однако, что для инструментов, определяемых пользователем, невозможно гарантировать уникальность пространства имен, поэтому могут происходить конфликты ID, и следует тщательно продумывать этот аспект при использовании инструментов, определяемых пользователем.

Поле P_{ID} используется для передачи одного или более параметров для ненормативного инструмента *i* JPSEC. Формат поля P_{ID} не задан в области применения JPSEC полностью. Если используется орган регистрации, формат регистрируется в данном органе регистрации наряду с ID. Если орган регистрации не используется и инструмент определяется пользователем, тогда указывается только длина этого поля, и соответствующее использование данного поля остается на усмотрение пользователей.

Однако в JPSEC действительно разрешается использовать синтаксические структуры, определенные для нормативных инструментов JPSEC в поле P_{ID} для ненормативных инструментов JPSEC. Например, ненормативный инструмент JPSEC может использовать поля шаблонов метода защиты, обрабатывающей Области, Степени структурирования, и Списка значений, описанные в пп. 5.8, 5.9, 5.10 и 5.11, соответственно.

Данный синтаксис является очень гибким и может приспосабливаться к широкому кругу методик безопасности таких, как целостность данных изображения, управление доступом и методы защиты прав. Следовательно, он предлагает большой набор функциональных возможностей, будучи при этом простым и кратким.

5.7 Синтаксис зоны влияния (ZOI)

5.7.1 Введение

Зону влияния (ZOI) можно использоваться для описания зоны обслуживания инструмента JPSEC. Данные в зоне обслуживания (определяемые ZOI) называются данные под влиянием. Нормативные инструменты JPSEC должны использовать ZOI для описания своей зоны обслуживания. Ненормативные инструменты JPSEC могут использовать ZOI для описания своей зоны обслуживания или могут использовать альтернативный метод. Если используется какой-либо альтернативный метод, длина ZOI составляет 0, т. е. этого показателя не существует.

Зона влияния (ZOI) описывает зону обслуживания каждого инструмента JPSEC. Данная зона обслуживания может быть описана при помощи параметров, связанных с изображением, например, при помощи разрешения или участка изображения; или параметров, не связанных с изображением, например, при помощи сегментов кодового потока и указателей (индексов) пакетов. В случаях, когда параметры, связанные с изображением и не связанные с изображением, используются вместе, ZOI описывает соответствие между данными зонами (обслуживания). Например, ZOI можно использовать для указания на то, что разрешения и участки изображения, заданные при помощи параметров, связанных с изображением, соответствуют сегментам кодового потока, заданным при помощи параметров, не связанных с изображением. Это позволяет использовать ZOI в качестве метаданных, сигнализирующих о том, в какой части кодового потока JPSEC расположены определенные части изображения.

На рисунке 11 показана концептуальная структура ZOI. ZOI содержит одну или более зон. Когда в одной ZOI используется много зон, ZOI определяется их объединением. Это указывает на то, что инструмент JPSEC следует применять ко всем зонам. Каждая зона в ZOI описывается при помощи трех основных единиц измерения: класса описания, режима параметров и элементов параметра (значений). В данной Рекомендации | Международном стандарте определяется два класса описания: класс описания, связанный с изображением, и класс описания, не связанный с изображением. Данные параметры можно задать, используя несколько режимов, например, одно значение, много значений в списке или диапазон. Затем значения параметров или элементов перечисляются в соответствии с режимом.

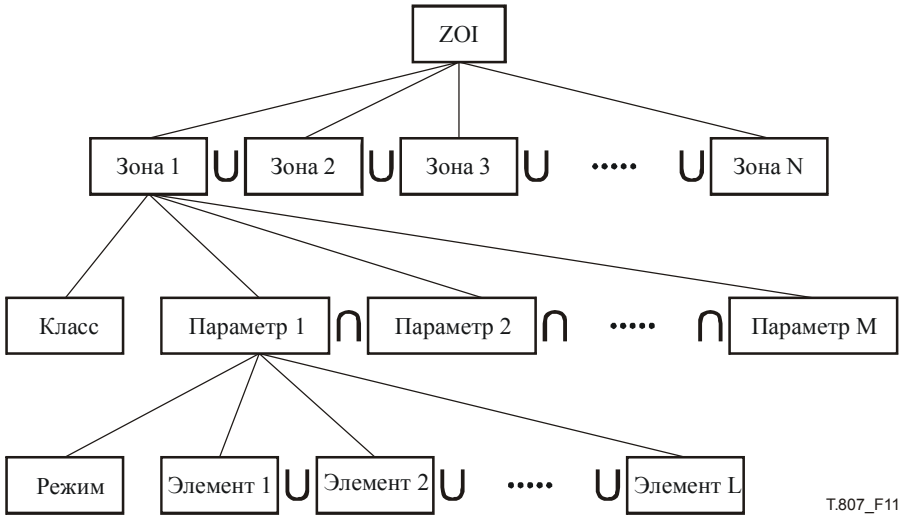


Рисунок 11 – Схематическая структура Зоны влияния

5.7.2 Синтаксис ZOI

На рисунке 12 показан синтаксис ZOI. ZOI может содержать одну или более зон. Она также может быть пустой, в таком случае значение NZzoi должно быть равно 0. Когда это происходит, влияние инструмента задается при помощи других средств таких, как маркер INSEC или параметры, определенные ненормативным инструментом защиты JPSEC.

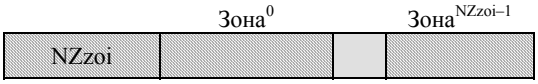


Рисунок 12 – Синтаксис ZOI

NZzoi: Число зон. В данном поле используется структура RBAS.

Зона^{k}: Зона. Ее структура определена в п. 5.7.3.

Таблица 10 – Значения параметра поля зоны влияния (ZOI)

Параметр	Размер (биты)	Значения
NZzoi	8 + 8 * n (RBAS)	0 ... (2^{7+7*n} – 2) (2^{7+7*n} – 2), зарезервировано
Зона^{k}	Переменный	См. п. 5.7.3

5.7.3 Синтаксис Зоны

Данная Зона содержит индикатор поля для класса описания зоны, за которым следуют параметры данного класса. В классе описания зоны используется структура FBAS. Как показано на рисунке 13, второй наиболее важный бит каждого байта, помеченный "x", сигнализирует об использовании определенного класса описания. В данной Рекомендации | Международном стандарте определяются два типа классов: класс описания, связанный с изображением, и класс описания, не связанный с изображением (см. таблицу 12). В таблице 13 и 14 приводятся номера указателя поля для класса описания, связанного с изображением, класса описания, несвязанного с изображением, соответственно. Соединение шести битов, помеченных "y", в каждом байте, который следует за флагом класса описания, указывает на использование определенного описания в рамках данного класса описания. Значение бита "1" в номере бита в каждом классе указывает на то, что существует соответствующее поле параметра. Число параметров должно быть таким же, как и число указателей поля класса для описания зоны, установленных на '1', и они должны появляться в том порядке, в котором сигнализируется об указателе поля класса. Класс описания зоны имеет переменное число байтов; когда MSB равняется 1, тогда следует класс описания другой зоны. MSB последнего байта класса описания равняется 0. Если используются классы описания как связанные с изображением, так и не связанные с ним, байты класса описания, связанного с изображением, должны предшествовать байту класса описания, не связанного с изображением. Когда при помощи данной структуры представлено несколько элементов, первый элемент в списке должен соответствовать наиболее важному доступному биту первого байта.

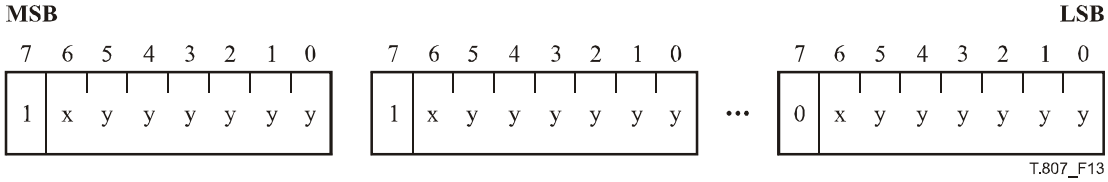


Рисунок 13 – Структура класса описания Зоны (DCzoi)

На рисунке 14 показан синтаксис Зоны.

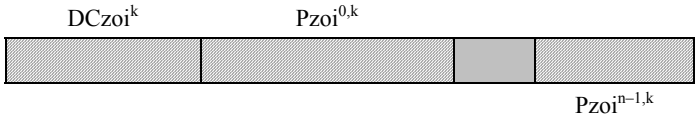


Рисунок 14 – Синтаксис зоны состоит из класса описания и одного или более наборов параметров

DCzoi^{k}: k-ый класс описания Зоны. В данном поле используется структура FBAS.

Pzoi^{i,k}: Параметры зоны в соответствии с указанным классом описания Зоны (DCzoi^{k}). См. п. 5.7.6.

DCzoi^{k} определяется число *n* существующих полей класса описания зоны, на основе числа битов, значение которых установлено на 1. Для каждого поля класса описания зоны существует одно поле параметра зоны Pzoi^{i,k}. Данные поля появляются последовательно в том же порядке, что и флаги, появляющиеся в DCzoi^{k}.

Таблица 11 – Значения параметры зоны

Параметр	Размер (биты)	Значения
DCzoi^{k}	Переменный (FBAS)	Варьируется в соответствии с набором значений в таблице 12
Pzoi^{i,k}	Переменный	Синтаксис данного поля см. в п. 5.7.6

Таблица 12 – Значение указателя класса описания

Значение	Класс описания
0	Класс описания, связанный с изображением. Следующие номера битов определены в таблице 13
1	Класс описания, не связанный с изображением. Следующие номера битов определены в таблице 14

Таблица 13 – Класс описания, связанный с изображением

Номер бита	Семантика
1	Участок изображения
2	Элемент(ы) изображения, как определено в Части 1 JPEG 2000
3	Уровень(и) разрешения, как определено в Части 1 JPEG 2000
4	Слой(и), как определено в Части 1 JPEG 2000
5	Компонент(ы), как определено в Части 1 JPEG 2000
6	Граница(ы), как определено в Части 1 JPEG 2000
7	Маркер(ы) TRLCP (элемент изображения – разрешение – слой – компонент – граница)
8	Пакет(ы), как определено в Части 1 JPEG 2000
9	Поддиапазоны (субдиапазоны), как определено в Части 1 JPEG 2000
10	Блок(и) кода, как определено в Части 1 JPEG 2000
11	ROI
12	Битовая скорость
13	Определяется пользователем. Подробности должны быть определены другими средствами. (Например, ID JPSEC.)
	Все остальные значение зарезервированы

Таблица 14 – Класс описания, не связанный с изображением

Номер бита	Семантика
1	Пакет(ы), как определено в Части 1 JPEG 2000
2	(Дополненный(е)) Байтовый(е) диапазон(ы) (начинающиеся с первого байта после первого маркера SOD)
3	(Дополненный (е)) Байтовый(е) диапазон(ы) (начинающиеся с первого байта после первого маркера SEC)
4	Не дополненный(ые) байтовый(е) диапазон(ы), когда используется дополнение
5	Маркер(ы) TRLCP (элемент изображения – разрешение – слой – компонент – граница)
6	Значение(я) искажений
7	Относительная(ые) важность(и)
8	Определяется пользователем. Подробности должны быть определены другими средствами. (Например, ID JPSEC.)
	Все остальные значение зарезервированы

В элементе изображения указатели пакетов нумеруются последовательно, и поэтому не могут быть уникальными среди элементов изображения. Кроме того, номера указателей пакетов в элементе изображения могут сбрасываться, когда превышается их максимальное значение – 65 535. По этой причине присвоение указателей пакетам описано более подробно. Когда число указателей пакетов в элементе изображения не превышают 65 535 пакетов, указатель пакетов, описанный в таблице 13, определяется указателем пакета, заданным параметром Nsop SOP, как определено в таблице A.40 Части 1 стандарта JPEG 2000. Отметим, что если максимальное значение не превышает 65 536, один пакет JPEG 2000 может быть уникально определен при помощи указателя элемента изображения и указателя пакета. Когда число указателей пакетов превышает 65 535 пакетов, указатель пакета Части 1 JPEG 2000 сбрасывается на 0. В таком случае указатель пакета не может уникальным образом идентифицировать пакет, и его нельзя использовать. В таком случае рекомендуется использовать вместо этого маркер TRLCP. Напомним, что если указатель пакета сбрасывается и повторяется, услуги безопасности, требующие уникальности указателей пакета, становятся уязвимыми.

Когда используется маркер TRLCP, его формат должен быть определен в поле параметра P_{SEC}, показанного в таблице 2. В частности, формат маркера TRLCP определяется полем параметра P_{TRLCP} в таблице 4. Это определяет размер маркеров TRLCP в ZOI.

Класс описания, не связанный с изображением, может также иметь много наборов полей одновременно. Когда это происходит, режимы для различных полей параметров должны иметь одинаковое число элементов (одно исключение из данного правила описывается ниже). Эти элементы должны однозначно соответствовать друг другу в одном и том же порядке. Например, если данная зона использует байтовые диапазоны и диапазоны пакетов, каждый из них должен иметь одно и то же число элементов диапазона, где первый байтовый диапазон соответствует первому диапазону пакетов и т. д.

Существует одно исключение из вышеописанного правила, касающееся требования одного и того же числа элементов для каждого поля. Это происходит, когда одно из полей f1 содержит 1 элемент, определяющий диапазон элементов (как описано при помощи режима диапазона в п. 5.7.6), где данный диапазон содержит N элементов, когда другое поле f2 определяется списком N элементов. В таком случае поле f1, содержащее только один элемент (диапазон), рассматривается как список из N элементов. Данные N элементов, определенные диапазоном f1 должны однозначно соответствовать N элементам, перечисленным в f2. Поэтому диапазон элементов может быть связан либо с отдельным элементом, либо со многими элементами (одним для каждого элемента диапазона).

Указатели присваиваются данным байтам, начиная либо с первого байта после первого маркера SOD, либо после первого байта после первого маркера SEC. В любом случае этот первый байта помечается как байт 0.

Поля искажений (как поля искажения, так и поля относительной важности) предоставляют возможность сигнализировать о важности участков, определяемых ZOI. Параметр искажения определяет снижающий искажения вклад указанного сегмента данных, будь то для набора пакетов или байтового диапазона или для указанного участка, связанного с изображением. Искажение выражается в единицах суммарной квадратичной ошибки, используя либо однобайтовое, либо двухбайтовое описание, сигнализируемое в Mzoi. Дополнительные подробности и форматы данных полей описаны в п. 5.7.3.2.

Маркер TRLCP определяет элемент изображения, разрешение, слой, компонент и границу защищенного пакета в кодовом потоке. Маркер используется в ZOI для определения данных параметров, поскольку может быть трудно вывести данную информацию из логического потока.

Отметим, что когда используются только описания, связанные с изображением, поле может быть завершено. Таким образом, нет необходимости представлять описания, несвязанные с изображением, когда они не используются.

5.7.3.1 Поля байтовых диапазонов

Класс описания, не связанный с изображением, позволяет описывать ZOI в байтовых диапазонах. Как правило, 2-й и 3-й элемент таблицы 14 используются для представления байтовых диапазонов для большинства инструментов таких, как аутентификация и шифрование/расшифровка без дополнения битами. Однако некоторые методы защиты такие, как шифрование/расшифровка с дополнением битами, изменяют длину данных. Когда это происходит, необходимо точно определить как байтовый диапазон с дополнениями, так и не дополненный или первоначальный байтовый диапазон. В таком случае байтовый диапазон с дополнениями, определяется 2-м и 3-м элементами таблицы 14 в соответствии с потребностями инструмента защиты. (Отметим, что два элемента не могут использоваться вместе). Кроме того, байтовый диапазон без дополнений определяется 4-м элементом таблицы 14. Байтовый диапазон без дополнений должен быть определен в том же режиме описания, что и байтовый диапазон с дополнениями, и иметь такое же число элементов. Данные элементы должны однозначно соответствовать друг другу в одном и том же порядке.

5.7.3.2 Поле искажений и поле относительной важности

Поля искажений и относительной важности предоставляют возможность сигнализировать о важности участков, определяемых ZOI.

Поле искажений используется для связывания искажения с участком, определяемым ZOI. Значение искажения определяет искажение суммарной квадратичной ошибки (или суммы квадратичных ошибок), которое получится, если связанный участок будет недоступным для расшифровки. Искажение суммарной квадратичной ошибки является основным показателем искажения, используемым при обработке изображений и видео. Оно используется для вычисления общего искажения среднеквадратической ошибки (MSE) и соотношения пикового сигнала-шума (PSNR). Поле искажений выражается при помощи однобайтового и двухбайтового описания, причем данные однобайтовые и двухбайтовые описания описаны ниже. Выбор однобайтового и двухбайтового описания сигнализируется при помощи значения параметра Mzoi, которое определяет длину данного поля. Поле относительной важности можно использовать для описания относительной важности среди различных участков, определенных связанными ZOI, без обязательной привязки к определенному показателю искажения. Длина поля относительной важности также сигнализируется в Mzoi. Данные поля более подробно описываются в нижеследующих пунктах.

5.7.3.2.1 Однобайтовое поле искажения

Суммарное искажение квадратичной ошибки выражается при помощи однобайтового поля искажения с представлением типа псевдоплавающей запятой. 8 битов, доступные в поле искажения, распределяются, как показано на рисунке 15 и в таблице 15, и предоставляют соответствующий компромисс между точностью и динамическим диапазоном. Отметим, что знак бита не нужен, поскольку искажение не является отрицательным. Для покрытия достаточного динамического диапазона, используется база 16, а 4 бита используются в качестве экспоненты (exp). Мантисса (m) выражается при помощи 4 битов. Поэтому суммарное значение искажения D задается формулой:

$$D = m \times 16^{exp},$$

где m имеет значение в диапазоне $0 \le m \le 15$, а exp имеет значение в диапазоне $0 \le exp \le 15$. Значение искажения, равное 0, представлено m = 0 и exp = 0, т. е. когда значение поля искажения равно 0. При распределении 4 битов по мантиссе m точность находится в рамках $1/2 \times (1/2^4) = 1/32$ или около 3%. При 4 битах для экспоненты и использовании основы – 16, динамический диапазон составляет от 0 до max, где max задается m = 15, а = 15, что соответствует искажению $15 \times 16^{15} = 1{,}7 \times 10^{19}$.

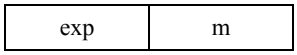


Рисунок 15 – Синтаксис поля искажения

exp: Экспонента значения поля искажения (основа 16)

m: Мантисса значения поля описания

Таблица 15 – Значения параметра поля искажения

Параметр	Размер (биты)	Значения
exp	4	0 ... 15
m	4	0 ... 15

Отметим, что в данном формате для искажения сравнение между двумя искажениями для определения того, какое из них больше, можно осуществить, просто сравнив два значения искажения как символы без знака. В частности для выполнения данного сравнения нет необходимости в конвертировании из формата псевдоплавающей запятой в действительное суммарное искажение для того, чтобы определить, какое из двух значений искажения больше или меньше. Данное свойство может упростить обработку в различных приложениях.

5.7.3.2.2 Двухбайтовое поле искажения

В двухбайтовом формате значения искажения должны выражаться в виде двухбайтового числа в формате псевдоплавающей запятой. Формат псевдоплавающей запятой для искажения определяется следующим образом. Данный формат используется в п. E.1.1.1 (уравнение E.3) Рек. МСЭ-Т Т.800 | ИСО/МЭК 15444-1 для выражения размера шага квантования для JPEG 2000. Каждое 16-битное число содержит экспонент (5 битов) и мантиссу (11 битов) в метрическом значении. В частности, значение плавающей запятой V данного показателя задается следующей формулой:

$$V = 2^{\varepsilon - 15}\left(1 + \frac{\mu}{2^{11}}\right) \quad \text{если } \varepsilon \neq 0,$$
$$V = 0 \quad \text{если } \varepsilon = 0,$$

где ε представляет собой целое число без знака, получаемое из пяти первых наиболее важных битов данного параметра, а μ – целое число без знака, получаемое из оставшихся 11 битов. Особый случай, при котором $V = \infty$ соответствует $\mu = 0$ и $\varepsilon = 31$. Отметим, что не отображаемые значения устанавливаются равными нулю.

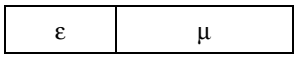


Рисунок 16 – Синтаксис поля искажения

ε: Экспонент значения двухбайтового поля искажения.

μ: Мантисса значения двухбайтового поля искажения.

Таблица 16 – Значения параметра поля искажения

Параметр	Размер (биты)	Значения
ε	5	0 ... 31
μ	11	0 ... $(2^{11} – 1)$

Алгоритм вычисления ε и μ не определяется как обязательная часть данной Рекомендации | Международного стандарта. Одним из возможных методов является следующий (приводится пример преобразования числа 12?25). Если $V = 0$, устанавливаем $\varepsilon = \mu = 0$. В противном случае:

– преобразовать V в двоичное число ($12{,}25_{10} = 1100{,}01_2$);

– стандартизировать число; это означает, что слева от двоичной запятой должна быть 1 цифра, и число должно быть умножено на 2 в соответствующей степени, чтобы в результате получалось первоначальное значение. Стандартизованная форма 1100,01 имеет вид $1{,}10001 \times 2^3$;

– экспонент – это степень числа 2, представленная в дополнительной системе обозначений. Смещение экспонента равно 15; следовательно, для данного примера экспонент представлен как 18_{10} (10010_2);

– мантисса представляет важные биты, *кроме бита, стоящего слева от двоичной запятой,* который всегда равен единице, и поэтому его не нужно хранить; для того чтобы получить 11 битов обычно прибавляются нули. В данном примере мантисса равна 10001000000.

5.7.3.2.3 Поле относительной важности

Поле относительной важности *r* можно использовать для описания относительной важности различных единиц кодирования, без обязательной привязки к определенному показателю искажения. Это позволяет описывать относительную важность или расстановку приоритетов среди единиц кодирования без явного описания того, насколько одна единица важнее другой. Данная относительная важность связанных данных задается в поле n-байта, которое поддерживает 2^{8n} вариантов классификации (расстановки), что показано на рисунке 17 и в таблице 17, где число байтов *n* для данного поля определяется Mzoi. Например, при использовании однобайтового поля относительной важности поддерживается 256 вариантов классификации (расстановки). Увеличение значений соответствует возрастанию важности, также как в поле искажений.

Рисунок 17 – Синтаксис поля относительной важности

r: Значение относительной важности/

Таблица 17 – Значения параметра поля относительной важности

Параметр	Размер (биты)	Значения
r	8 * n	0 ... $(2^{8n} – 1)$

5.7.3.2.4 Дополнительные комментарии, касающиеся поля искажения и поля относительной важности

Поскольку как для однобайтового поля искажений, так и для однобайтового поля относительной важности увеличение значений соответствует возрастанию важности, можно сравнивать две эти единицы данных таким же образом вне зависимости от того, задает ли поле искажений действительное искажение или относительную важность. Данная возможность может упростить использование приложений.

При помощи полей искажения или относительной важности можно определять заголовки. Потеря различных типов данных таких, как основные заголовки и заголовки элемента изображения или заголовок SEC, мешает расшифровке смежных (связанных) данных изображения. Создатель JPSEC может пожелать присвоить искажение этим данным, используя:

1) самое высокое значение искажения (указанное далее) для обозначения заголовка или важных данных; или

2) описать суммарное искажение, которое создастся, если изображение или часть его будет невозможно расшифровать.

Затем у создателя есть несколько возможностей сигнализации о заголовках.

Самым высоким значением искажения для однобайтовых полей является значение "все единицы" (0xFF). Отметим, что данное значения является наибольшим возможным значением искажения, как для однобайтового поля искажения квадратичной ошибки, так и для однобайтового поля относительной важности. Самым большим значением искажения для двухбайтового поля искажения является два байта со значением "все единицы" (0xFFFF). Самым высоким значением важности для поля относительной важности длиной n байтов является значение "все единицы" в n байтах.

5.7.3.2.5 Совместное использование поля искажения и поля относительной влажности

Поле искажения и поле относительной важности можно использовать одновременно для описания участка, определяемого при помощи ZOI. В таком случае оба поля определяют искажение квадратичной ошибки, однако поле искажения определяет сокращение приращения искажения, в то время как поле относительной важности определяет общее искажение. В частности, поле искажения определяет сокращение приращения искажения, которое получится в результате расшифровки ZOI. Это подразумевает, что вся информация, требующаяся для расшифровки ZOI доступна, и фокусируется на сокращении приращения искажения, производимое ZOI. Поле относительной важности определяет общее искажение, появляющееся, если ZOI недоступна. То есть оно определяет общее искажение, которое получится, если данная ZOI недоступна для расшифровки. Причем следует принимать во внимание не только значение самой ZOI (выраженного в поле искажения), но также и появляющееся искажение, так как другие части сжатого битового потока, зависящие от ZOI, не поддаются расшифровке. Общее искажение, связанное с различными ZOI, является полезным показателем для относительной важности различных ZOI. Когда используются оба поля, для искажения они будут использовать одно и то же математическое выражение, как сигнализируется полем искажения.

5.7.3.3 Поле битовой скорости

Поле битовой скорости используется для определения защищенной зоны в области вейвлет-коэффициента. Оно идентифицирует плоскости наиболее важных битов, сжатая битовая скорость которых задается в данном поле. MSB выбираются при помощи процесса оптимизации искажения в зависимости от скорости, описанного в Части 1. Например, если значение битовой скорости равно 2,5, защищенная зона включает MSB всех коэффициентов волн малой амплитуды, сжатая битовая скорость которых составляется 2,5 бит на пиксел. Синтаксис поля битовой скорости показан на рисунке 18 и в таблице 18. Определяемая битовая скорость задается формулой:

$$R = I_R + F_R/16.$$

Например, нулевая битовая скорость представлена $I_R = 0$ и $F_R = 0$; а битовая скорость, равная 2,5, представлена $I_R = 2$ и $F_R = 8$.

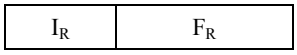


Рисунок 18 – Синтаксис поля битовой скорости

I_R: Целая часть определенной битовой скорости.

F_R: Дробная часть определенной битовой скорости.

Таблица 18 – Значения параметра поля битовой скорости

Параметр	Размер (биты)	Значения
I_R	4	0 ... 15
F_R	4	0 ... 15

5.7.4 Взаимосвязь между многими параметрами

5.7.4.1 Общая взаимосвязь

Когда класс описания, связанный с изображением, имеет многочисленные поля, задаваемые одновременно, зона, получающаяся в результате, должна быть пересечением данных полей. Например, зона может определять самый низкий уровень разрешения во втором элементе изображения. Объединение полей может быть определено при помощи использования многих зон в ZOI.

Класс описания, несвязанный с изображением, может также иметь многочисленные поля, задаваемые одновременно. Когда это происходит, режимы для полей различных параметров должны иметь одно и то же число элементов (за исключением правила, описанного ниже), и данные элементы должны однозначно

соответствовать друг другу. Например, если в данной зоне используются байтовые диапазоны и диапазоны пакетов, каждый из них должен иметь одинаковое число элементов диапазона, причем первый байтовый диапазон соответствует первому диапазону пакета и т. д.

Существует одно исключение из вышеописанного правила, касающегося требования одинакового количества элементов для каждого поля. Это происходит, когда одно из полей f1 содержит 1 элемент, определяющий диапазон элементов (как описано режимом диапазона в п. 5.7.6), где данный диапазон содержит N элементов, когда другое поле f2 определяется списком N элементов. В таком случае поле f1, которое содержит только 1 элемент (диапазон) интерпретируется как список из N элементов. Данные N элементов, определяемые диапазоном в f1, должны однозначно соответствовать N элементам, перечисленным в поле f2. Поэтому диапазон элементов может быть связан либо с одним элементом, либо со многими элементами (один для каждого элемента диапазона).

5.7.4.2 Примеры

Как показано на рисунке 11, структура класса описания зоны может иметь многочисленные поля, задаваемые одновременно, где N полей представляют собой описания, связанные с изображением (D_i^1, D_i^2, ... , D_i^N), а M полей являются описаниями, несвязанными с изображениями (D_n^1, D_n^2, ... , D_n^M). Семантику можно понять как $\{D_i^1 \cap D_i^2 \cap \ldots \cap D_i^N\} = D_n^1 = D_n^2 = ... = D_n^M$, т. е. пересечение N описаний, связанных с изображением, соответствует каждому из M описаний, не связанных с изображением. Кроме того, M описаний, несвязанных с изображением, взаимно соответствуют друг другу. Данная взаимосвязь далее иллюстрируется тремя примерами, приведенными ниже.

В первом примере описание зоны имеет два описания, связанных с изображением: одно для разрешения 2, а другое для слоя 3. В таком случае данные под влиянием представляют собой пересечение разрешения 2 и слоя 3, как показано на рисунке 19.

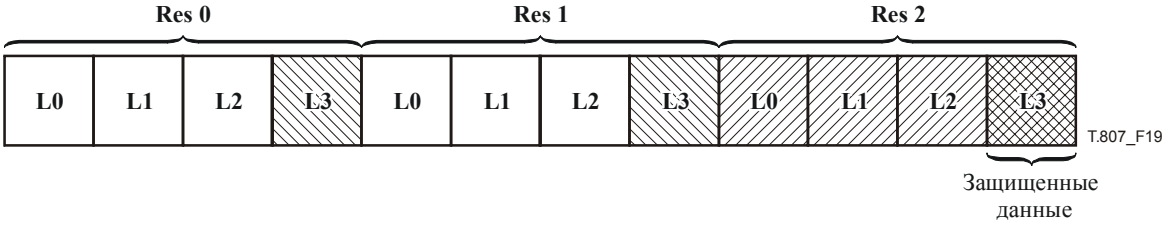


Рисунок 19 – Пример использования зоной ZOI описаний, связанных с изображением

Во втором примере описание зоны имеет два описания, связанных с изображением (разрешение 2 и слой 3) и одно описание, не связанное с изображением (диапазон пакетов 80–100). В таком случае данные под влиянием содержатся в пакетах в диапазоне от 80 до 100.

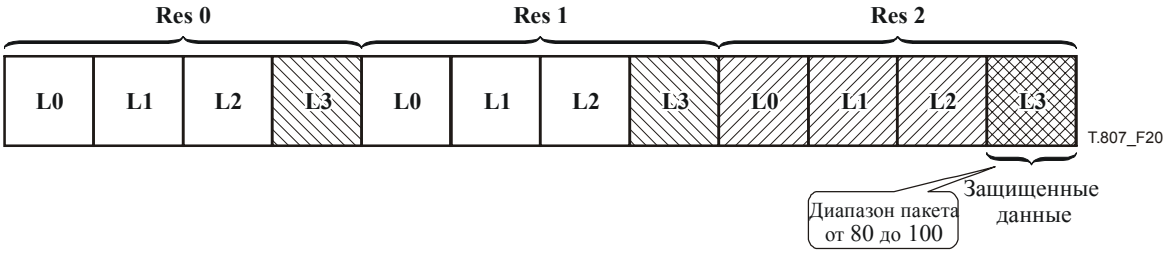


Рисунок 20 – Пример использования зоной ZOI описаний, связанных и несвязанных с изображением

В третьем примере, описание зоны имеет два описания, связанных с изображением (разрешение 2 и слой 3) и два описания, несвязанных с изображением (диапазон пакетов 80–100 и байтовый диапазон 856–1250). И снова данные под влиянием представляют собой пересечение разрешения 2 и слоя 3, и данные под влиянием содержатся в пакетах в диапазоне от 80 до 100. Кроме того, данные пакеты и участки под влиянием расположены в байтовом диапазоне 856–1250.

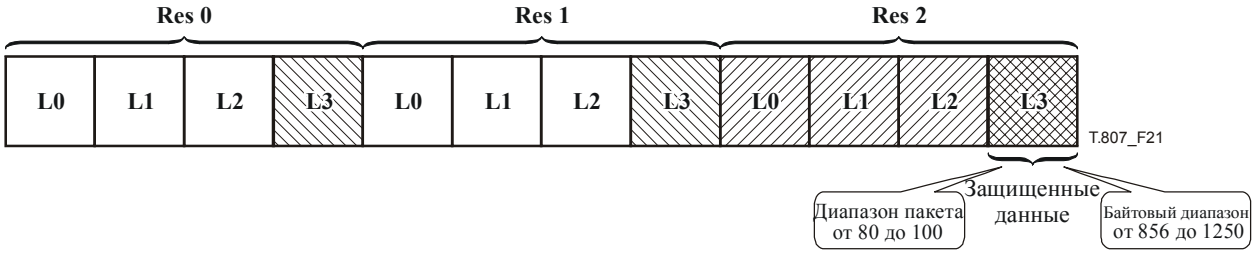


Рисунок 21 – Второй пример использования зоной ZOI описаний, связанных и несвязанных с изображением

5.7.5 Защита любых данных, следующих за маркером SEC

Всестороннее исследование, приведенное выше, главным образом, концентрировалось на обеспечении услуг по защите для кодового потока JPEG 2000. Однако следует защищать многие элементы основного заголовка, включая сигнализацию JPSEC, для этой цели можно также использовать ZOI и методы защиты.

В частности, режим байтового диапазона для класса описания, несвязанного с изображением, можно использовать для определения того, что инструмент JPSEC следует применять к любым данным, которые следуют за маркером SEC. Как было описано ранее, первый байт заголовка SEC – это байт 1 для индексирования байтового диапазона. Данные, которые следуют за маркером SEC и которые можно защитить, включают сегмент SEC и большую часть основного заголовка. Отметим, что весь основной заголовок JPEG 2000 за исключением сегмента маркера SIZ можно разместить после маркера SEC и, таким образом, защитить при помощи подхода, описанного выше. Если необходимо защитить сегмент маркера SIZ JPEG 2000, это нужно сделать на более высоком уровне, например слой формата файла.

Инструменты JPSEC для защиты сегмента SEC главным образом должны быть первыми инструментами в сегменте SEC. Это позволяет потребителю сначала передать данные сегмента SEC, которые затем можно использовать для обработки оставшейся части кодового потока.

5.7.6 Синтаксис параметра описания зоны (Pzoi)

На рисунке 22 показан синтаксис параметра описания ZOI.

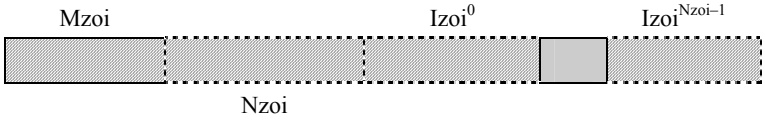


Рисунок 22 – Синтаксис параметра описания ZOI

Mzoi: Режим описания ZOI. В данном поле используется структура FBAS.

Nzoi: Число Izoi. В данном поле используется структура RBAS.

Izoi^{i}: Элемент.

Таблица 19 – Значения параметра Pzoi^{i}

Параметр	Размер (биты)	Значения
Mzoi	Переменный (FBAS)	См. таблицу 20
Nzoi	0 8 + 8 * n (RBAS)	Если число битов 2 Mzoi равно 0 2 ... (2^{7+7*n} – 1)
Izoi^{i}	Переменный	Зависит от режима, определенного в Mzoi

Таблица 20 – Значения параметра Mzoi

Число битов FBAS	Значения (биты)	Семантика
1	0	На заданные зоны оказывает влияние инструмент JPSEC
	1	Влияние оказывается на дополнения к заданным зонам
2	0	Задается один элемент
	1	Задается много элементов
3, 4	00	Режим прямоугольника. Прямоугольный участок, где первая пара значений определяет верхний левый угол, а вторая пара значений определяет нижний правый угол таким образом, что два угла включены. Для каждого угла первое значение должно обозначать горизонтальную позицию, а второе значение должно обозначать вертикальную позицию. Присвоение показателей должно начинаться с 0 и должно использовать координатную сетку, определенную в Части 1 JPEG 2000
	01	Режим диапазона. Диапазон значений, где первое значение определяет начальный показатель, а второе значение определяет конечный показатель, и которые включены
	10	Режим показателя. Определяет одно значение(я)
	11	Режим максимального значения. Определяет максимальное значение
5, 6	00	$Izoi^i$ использует 8-битное целое число
	01	$Izoi^i$ использует 16-битное целое число
	10	$Izoi^i$ использует 32-битное целое число
	11	$Izoi^i$ использует 64-битное целое число
7, 8	00	$Izoi^i$ описывается в одном измерении
	10	$Izoi^i$ описывается в двух измерениях
	01	$Izoi^i$ описывается в трех измерениях
9	0	Смещение не используется в режиме длины
	1	Смещение используется в режиме длины. Задает первоначальное смещение длин смежных байтов, которое следует далее. Существование данного флага должно замещать режимы, определяемые в битах 3 и 4
		Все остальные значения зарезервированы

Когда используются маркеры TRLCP, их размер определяется P_{TRLCP} как показано таблице 4. В таком случае биты 5 и 6 параметра Mzoi заменяются.

Смещение в режиме длины может использоваться для эффективного отображения ряда последовательных сегментов, например, ряда последовательных байтовых диапазонов. Первое значение определяет первоначальное смещение, следующие значения определяют длины каждого последовательного сегмента. Если данное поле используется для представления n сегментов, значение Nzoi должно быть установлено на n + 1.

5.8 Синтаксис шаблона метода защиты (T)

5.8.1 Общие положения

Шаблоны метода защиты содержат параметры для определенных инструментов JPSEC, описанных в п. 5.6.1. Например, они используются в нормативных инструментах JPSEC, описанных в п. 5.6.2. Также их можно использовать в ненормативных инструментах JPSEC, описанных в п. 5.6.3. Существует три типа шаблонов метода защиты: шаблон расшифровки, шаблон аутентификации и шаблон хэш-функции. Шаблон, используемый нормативным инструментом JPSEC, определяется его ID, как показано в таблице 6 и в таблице 21 со ссылками на соответствующие подпункты, в которых они определены.

Как описано в п. 5.6.2, шаблон метода защиты T вместе с областью обработки инструмента PD JPSEC, степенью структурирования G и списком значений V описывает то, как применяется инструмент JPSEC.

Таблица 21 – Значения ID шаблона (ID_T)

Значения	Шаблон метода защиты
0	Зарезервировано
1	Шаблон расшифровки (см. п. 5.8.2)
2	Шаблон аутентификации (см. п. 5.8.3)
3	Шаблон хэш-функции (см. п. 5.8.4)
4	Инструмент NULL
	Все остальные значения зарезервированы для использования ИСО

5.8.2 Шаблон расшифровки (T = T_{decry}, если t = 0 и ID = 1)

Шаблон расшифровки T_{decry} используется для сообщения устройству расшифровки того, как расшифровать полученный кодовый поток. На рисунке 23 показан синтаксис шаблона расшифровки. В таблице 22 показаны размеры и значения символов и параметров для шаблона расшифровки.

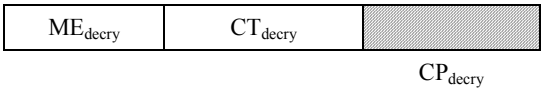


Рисунок 23 – Синтаксис шаблона расшифровки

ME_{decry}: Флаг неверной эмуляции маркера указывает, появилась ли в зашифрованных данных неверная эмуляция маркера. Неверная эмуляция маркера может неблагоприятно повлиять на совместимость с устройствами расшифровки Части 1 JPEG 2000. В данном поле используется структура FBAS.

CT_{decry}: Идентификация типа шифра.

CP_{decry}: Параметр шифра.

Таблица 22 – Значения параметра шаблона расшифровки

Параметр	Размер (биты)	Значения
ME_{decry}	8 + 8 * n (FBAS)	Таблица 23
CT_{decry}	16	Таблица 24
CP_{decry}	Переменный	Если $CT_{decry} < 0x6000$, см. п. 5.8.2.1 Если $0x6000 \le CT_{decry} < 0xC000$, см. п. 5.8.2.2 Если $CT_{decry} \ge 0xC000$, см. п. 5.8.2.3

Таблица 23 – Значения флага эмуляции маркера (ME_{decry})

Значения	Тип метода
01xx xxxx	Зашифрованные данные не содержат неверной эмуляции маркера
00xx xxxx	В противном случае
	Все остальные значения зарезервированы для использования ИСО

По умолчанию значение флага эмуляции маркера равно 0. Значение данного флага может быть установлено на 1 для обозначения того, что зашифрованные данные JPSEC не содержат неверной эмуляции маркера. Создатель JPSEC может предпочесть оставить значение данного флага по умолчанию равным 0.

Таблица 24 – Значения идентификатора шифра (CT_{decry})

Значения	Тип шифра
0 ... 0x5FFF	Блочный шифр (см. таблицу 25)
0x6000 ... 0xBFFF	Потоковый шифр (см. таблицу 26)
0xC000 ... 0xFFFF	Асимметричный шифр (см. таблицу 27)

Таблица 25 – Значения идентификатора блочного шифра (CT_{decry})

Значения	Тип шифра
0x0000	NULL (шифрование не применяется)
0x0001	AES (ИСО/МЭК 18033-3)
0x0002	TDEA (ИСО/МЭК 18033-3)
0x0003	MISTY1 (ИСО/МЭК 18033-3)
0x0004	Camellia (ИСО/МЭК 18033-3)
0x0005	CAST-128 (ИСО/МЭК 18033-3)
0x0006	SEED (ИСО/МЭК 18033-3)
	Все остальные значения зарезервированы для использования ИСО

Таблица 26 – Значения идентификатора потокового шифра (CT_{decry})

Значения	Тип шифра
0x6000	SNOW 2 (ИСО/МЭК 18033-4)
	Все остальные значения зарезервированы для использования ИСО

Таблица 27 – Значения идентификатора асимметричного шифра (CT_{decry})

Значения	Тип шифра
0xC000	RSA-OAEP (ИСО/МЭК 18033-2)
	Все остальные значения зарезервированы для использования ИСО

5.8.2.1 Шаблон блочного шифра (CP_{decry} для блочных шифров)

Шаблон блочного шифра используется для сообщения устройству блочной расшифровки того, как расшифровать полученный кодовый поток. На рисунке 24 показан режим блочного шифра, режим дополнения (битами), размер блока и ключевая информация.

Некоторые режимы блочного шифра могут использовать векторы инициализации. Для этих режимов, векторы инициализации инструмента определяются при помощи поля Степень структурирования инструмента (G), описанного в п. 5.10, и поля списка значений (V), описанного в п. 5.11. В частности векторы инициализации используются только для режимов с ID M_{bc} > 0x80, например, CBC, CFB, OFB, CTR. В случае CTR это на самом деле не IV, а *счетчик*. Значение размера вектора инициализации, задаваемого в поле списка значений V, должно быть установлено на размер блока SIZ_{bc}.

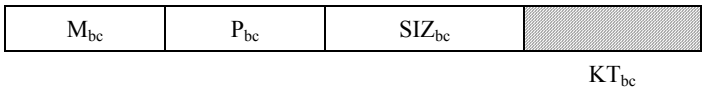


Рисунок 24 – Синтаксис шаблона блочного шифра

M_{bc}: Режим блочного шифра. Первый бит указывает на использование данным инструментом векторов инициализации. Если M_{bc} < 0x8, IV не используются, в противном случае для данного режима требуется один или более значений IV.

P_{bc}: Режим дополнения (битами).

SIZ_{bc}: Размер блока в байтах.

KT_{bc}: Шаблон ключа (см. п. 5.8.5). Содержит информацию о ключах, используемых блочным шифром.

Таблица 28 – Значения шаблона блочного шифра

Параметр	Размер (биты)	Значения
M_{bc}	6	Таблица 29
P_{bc}	2	Таблица 30
SIZ_{bc}	8	1 ... 256
KT_{bc}	Переменный	См. п. 5.8.5

Таблица 29 – Значения режима блочного шифра (M_{bc})

Значения	Тип режима
0	Зарезервировано
0x xxxx	Режимы, используемые без IV
1x xxxx	Режимы, используемые с IV
x0 xxxx	Биты не дополняются
x1 xxxx	Биты дополняются
0x 0001	ECB (ИСО/МЭК 10116)
1x 0010	CBC (ИСО/МЭК 10116)
1x 0011	CFB (ИСО/МЭК 10116)
1x 0100	OFB (ИСО/МЭК 10116)
1x 0101	CTR (ИСО/МЭК 18033-2)
	Все остальные значения зарезервированы для использования ИСО

ПРИМЕЧАНИЕ 1. – Для всех режимов требуются аккуратные реализации, поскольку неподходящая реализация может привести к появлению уязвимых мест. Отметим, что даже при верной реализации ECB присутствует утечка информации, когда появляются идентичные блоки. Указания содержатся в ИСО/МЭК 10116.

ПРИМЕЧАНИЕ 2. – Значения в таблице 30 применяются, только когда M_{bc} в таблице 29 указывает, какие биты дополняются. Когда биты не дополняются, значение P_{bc} должно быть установлено на 00.

Таблица 30 – Режим дополнения битами для блочного шифра (P_{bc})

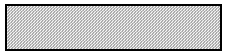
Значения	Тип дополнения
00	Занятие зашифрованного текста (RFC 2040)
01	PKCS#7-дополнение (PKCS#7)
	Все остальные значения зарезервированы для использования ИСО

ПРИМЕЧАНИЕ 3. – При использовании дополнения (битами) во избежание появления потенциально уязвимых мест, таких как избранные атаки на шифр, нужно использовать аккуратную схему системы.

5.8.2.2 Шаблон потокового шифра (CP_{decry} для потоковых шифров)

Шаблон потокового шифра используется для сообщения устройству потоковой расшифровки того, как расшифровать полученный кодовый поток. На рисунке 25 показан синтаксис шаблона потокового шифра. В таблице 31 показаны значения для шаблона потокового шифра.

Векторы инициализации потокового шифра определяются при помощи поля Степень структурирования инструмента (G), описанного в п. 5.10, и поля списка значений (V), описанного в п. 5.11. Значение размера вектора инициализации, задаваемое в списке значений V, должно быть установлено на размер ключа, определенный в шаблоне ключевой информации KT_{sc}.



KT_{sc}

Рисунок 25 – Синтаксис шаблона потокового шифра

KT_{sc}: Шаблон ключевой информации (см. п. 5.8.5). Содержит информацию о ключах, используемых потоковым шифром.

Таблица 31 – Значения шаблона потокового шифра

Параметр	Размер (биты)	Значения
KT_{sc}	Переменный	См. п. 5.8.5

5.8.2.3 Шаблон асимметричного шифра (CP_{decry} для асимметричных шифров)

Шаблон асимметричного шифра используется для сообщения устройству асимметричной расшифровки того, как расшифровать полученный кодовый поток. На рисунке 26 показан синтаксис шаблона асимметричного шифра. В таблице 32 показаны значения шаблона асимметричного шифра.

Для инструментов, которые используют шаблон асимметричного шифра, поле степени структурирования инструмента (G) определяет степень структурирования, с которой применяется данный шифр. Однако поле списка значений (V) не используется для представления каких-либо значений. Таким образом, число элементов (N_v) в поле списка значений должно быть установлено на 0.

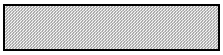


Рисунок 26 – Синтаксис шаблона асимметричного шифра

KT_{sy}: Шаблон ключевой информации (см. п. 5.8.5). Содержит информацию о ключах, используемых асимметричным шифром.

Таблица 32 – Значения шаблона асимметричного шифра

Параметр	Размер (биты)	Значения
KT_{sy}	Переменный	См. п. 5.8.5

5.8.3 Шаблон аутентификации (T = T_{auth}, если t = 0 и ID = 2)

Шаблон аутентификации T_{auth} используется для сообщения верификатору того, как подтвердить подлинность полученного кодового потока. Существует три общих класса методов аутентификации: аутентификация на основе хэш-функции, аутентификация на основе шифра и цифровые подписи. Методы аутентификации на основе как хэш-функции, так и шифра обычно называют кодами аутентификации сообщения (MAC), а их вычисленные значения, используемые для аутентификации, обычно называют значениями MAC. Синтаксис шаблона аутентификации показан на рисунке 27, а в таблице 33 приведены размеры и значения символов и параметров для шаблона аутентификации.

Для многих приложений безопасности аутентификация является наиболее важной услугой безопасности. Даже когда плановой услугой безопасности является конфиденциальность, ее следует дополнить аутентификацией для предотвращения атак. В частности, рекомендуется аутентифицировать части сегмента маркера SEC. Кроме того, аутентификацию следует выполнять как в отношении параметров шаблона аутентификации (T_{auth}), так и сообщения, подлежащего аутентификации. В особенности зона влияния должна определять, что аутентификации подлежат как содержание, так и параметры шаблона аутентификации (T_{auth}).

Рисунок 27 – Синтаксис шаблона аутентификации

M_{auth}: Метод аутентификации.

P_{auth}: Параметры аутентификации.

Таблица 33 – Значение параметра шаблона аутентификации

Параметр	Размер (биты)	Значения
M_{auth}	8	Таблица 34
P_{auth}	Переменный	Если M_{auth} = 0, см. п. 5.8.3.1 Если M_{auth} = 1, см. п. 5.8.3.2 Если M_{auth} =2, см. п. 5.8.3.3

Таблица 34 – Методы аутентификации (M_{auth})

Значения	Метод
0	MAC на основе хэш-функции
1	MAC на основе шифра
2	Цифровая подпись
	Все остальные значения зарезервированы для использования ИСО

5.8.3.1 Аутентификация на основе хэш-функции (P_{auth} для MAC на основе хэш-функции)

MAC аутентификации на основе хэш-функции используется для сообщения верификатору того, как подтверждать подлинность полученного кодового потока. На рисунке 28 показан синтаксис шаблона аутентификации на основе хэш-функции, а в таблице 35 приводятся значения параметров.

Значения MAC определяются при помощи поля Степень структурирования инструмента (G), описанного в п. 5.10, и поле списка значений (V), описанного в п. 5.11. Размер значения MAC, определяемый в списке значений V, должен быть установлен на размер MAC, определяемый SIZ_{HMAC}.

Рисунок 28 – Шаблон аутентификации на основе хэш-функции

M_{HMAC}: Идентификатор метода аутентификации на основе хэш-функции.

H_{HMAC}: Идентификатор хэш-функции.

KT_{HMAC}: Шаблон ключа.

SIZ_{HMAC}: Размер MAC (биты).

Таблица 35 – Значения параметра для шаблона аутентификации на основе хэш-функции

Параметр	Размер (биты)	Значения
M_{HMAC}	8	Таблица 36
H_{HMAC}	8	Таблица 37
KT_{HMAC}	Переменный	См. п. 5.8.5
SIZ_{HMAC}	16	0 ... 65 535

Таблица 36 – Идентификатор метода аутентификации на основе хэш-функции (M_{HMAC})

Значения	Метод аутентификации на основе хэш-функции
0	Зарезервировано
1	HMAC (ИСО/МЭК 9797-2)
	Все остальные значения зарезервированы для использования ИСО

Таблица 37 – Идентификатор хэш-функции (H_{HMAC})

Значения	Хэш-функция
0	Зарезервировано
1	SHA-1 (ИСО/МЭК 10118-3)
2	RIPEMD-128 (ИСО/МЭК 10118-3)
3	RIPEMD-160 (ИСО/МЭК 10118-3)
4	MASH-1 (ИСО/МЭК 10118-4)
5	MASH-2 (ИСО/МЭК 10118-4)
6	SHA-224 (ИСО/МЭК 10118-3)
7	SHA-256 (ИСО/МЭК 10118-3)
8	SHA-384 (ИСО/МЭК 10118-3)
9	SHA-512 (ИСО/МЭК 10118-3)
10	WHIRLPOOL (ИСО/МЭК 10118-3)
	Все остальные значения зарезервированы для использования ИСО

Отметим, что, если SIZ_{HMAC} меньше номинального размера хэш-функции, тогда он представляет собой укороченную версию, соответствующую первым битам SIZ_{HMAC} хэш-функции.

5.8.3.2 Шаблон аутентификации на основе шифра (P_{auth} для MAC на основе шифра)

MAC аутентификации на основе шифра используется для сообщения верификатору того, как подтвердить подлинность полученного кодового потока. На рисунке 29 изображен шаблон, а в таблице 38 приведены размер ключа и закодированная хэш-функция. Примером схемы аутентификации на основе шифра является CBC-MAC. В данных методах блочного шифра для аутентификации, вектор инициализации имеет длину в один размер блока и значение 0. Размер блока по умолчанию задан для блочного шифра. Отметим, что если SIZ_{CMAC} меньше номинального размера MAC аутентификации на основе шифра, тогда он представляет собой укороченную версию, соответствующую первым битам SIZ_{CMAC} MAC.

Отметим, что если число битов данных не является кратным размеру блока шифра, тогда конечный вводимый блок будет частичным блоком данных, выровненным с добавлением нулей до полного блока шифра. Также отметим, что CBC-MAC должно применяться только к данным с фиксированной и известной длиной.

Значения MAC определяются при помощи поля Степень структурирования инструмента (G), определяемого в п. 5.10, и поля списка значений (V), описанного в п. 5.11. Размер значения MAC, задаваемого в списке значений V, должен быть установлен на размер MAC, определяемых в SIZ_{CMAC}.

Рисунок 29 – Синтаксис шаблона аутентификации на основе шифра

CA_{CMAC}: Метод аутентификации на основе шифра.

C_{CMAC}: Значения идентификатора блочного шифра.

KT_{CMAC}: Шаблон ключа.

SIZ_{CMAC}: Размер MAC (биты).

Таблица 38 – Значения шаблона MAC

Параметр	Размер (биты)	Значения
CA_{CMAC}	8	Таблица 39
C_{CMAC}	8	Таблица 25
KT_{CMAC}	Переменный	См. п. 5.8.5
SIZ_{CMAC}	16	0 ... 65 535

Таблица 39 – Метод аутентификации на основе шифра (C_{CMAC})

Значения	Метод
0	CBC-MAC MAC Алгоритм 1 (ИСО/МЭК 9797-1)
1	CBC-MAC MAC Алгоритм 2 (ИСО/МЭК 9797-1)
2	CBC-MAC MAC Алгоритм 3 (ИСО/МЭК 9797-1)
3	CBC-MAC MAC Алгоритм 4 (ИСО/МЭК 9797-1)
	Все остальные значения зарезервированы для использования ИСО

5.8.3.3 Шаблон цифровой подписи (P_{auth} для цифровых подписей)

Цифровая подпись используется для сообщения верификатору того, как подтверждать подлинность полученного кодового потока, а также подтверждать подлинность отправителя для обеспечения целостности и неотказуемости. На рисунке 30 определяется шаблон цифровой подписи, а в таблице 40 перечисляются значения.

Цифровые подписи определяются при помощи поля Степень структурирования инструмента (G), описанного в п. 5.10, и поля списка значений (V), описанного в п. 5.11. Размер значения цифровой подписи, определяемый в списке значений V, должен быть таким, чтобы соответствовать размеру, определяемому SIZ_{DS}. Поскольку размер списка значений выражается в байтах, а не в битах, его размер должен соответствовать минимальному размеру байтов, который может вместить SIZ_{DS}. Каждое значение должно быть представлено наименее важными битами, а значение дополнительных битов MSB должно быть установлено на 0.

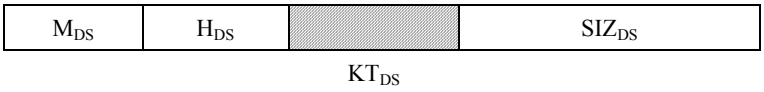


Рисунок 30 – Синтаксис шаблона цифровой подписи

M_{DS}: Метод цифровой подписи.

H_{DS}: Хэш-функция.

KT_{DS}: Шаблон ключа (см. п. 5.8.5). Содержит информацию, связанную с открытым ключом или сертификатом, требующимся для подтверждения подлинности цифровой подписи.

SIZ_{DS}: Размер цифровой подписи (биты).

Таблица 40 – Значения шаблона цифровой подписи

Параметр	Размер (биты)	Значения
M_{DS}	8	Таблица 41
H_{DS}	8	Таблица 37
KT_{DS}	Переменный	См. п. 5.8.5
SIZ_{DS}	16	0 ... 65 535

Таблица 41 – Методы цифровой подписи (M_{DS})

Значения	Метод
1	RSA (ИСО/МЭК 14888-2)
2	Rabin (ИСО/МЭК 14888-2)
3	DSA (ИСО/МЭК 14888-3)
4	ECDSA (ИСО/МЭК 14888-3)
	Все остальные значения зарезервированы для использования ИСО

5.8.4 Шаблон хэш-функции ($T = T_{hash}$, если $t = 0$ и $ID = 3$)

Шаблон хэш-функции T_{hash} используется для сообщения параметров, используемых для вычисления хэш-функции. В таблице 42 показаны размеры и значения символов и параметров для шаблона хэш-функции.

Отметим, что в отличие от шаблона аутентификации на основе хэш-функции, описываемого в п. 5.8.3.1, который включает в себя использование хэш-функции и секретного ключа, данный шаблон хэш-функции не использует ключ. В то время как шаблон хэш-функции может использоваться для обнаружения случайной ошибки или случайного изменения данных, он не предотвращает злонамеренного изменения данных. Для того чтобы предотвратить злонамеренное изменение данных, нужно использовать шаблон аутентификации, поскольку секретный ключ, используемый шаблоном аутентификации, предотвращает незаметное изменение данных.

Значения хэш-функции определяются при помощи поля Степень структурирования инструмента (G), описанного в п. 5.10, и поля списка значений (V), описанного в п. 5.11. Размер значения хэш-функции, заданный в списке значений V, должен соответствовать размеру значения хэш-функции, определяемом SIZ_{hash}.

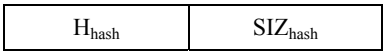


Рисунок 31 – Синтаксис шаблона хэш-функции

H_{hash}: Идентификатор хэш-функции.

SIZ_{hash}: Размер значения хэш-функции (байты).

Таблица 42 – Значения параметра шаблона хэш-функции

Параметр	Размер (биты)	Значения
H_{hash}	8	Таблица 37
SIZ_{hash}	8	0 ... 255

5.8.5 Шаблон информации о ключе (KT)

Шаблон информации о ключе используется для сообщения информации о ключе. На рисунке 32 определяется его шаблон, а в таблице 43 перечисляются значения.

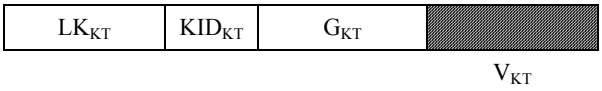


Рисунок 32 – Синтаксис шаблона информации о ключе

LK_{KT}: Длина ключа в битах.

KID_{KT}: Идентификатор информации о ключе. Обозначает смысл значений в списке значений V_{KT}. В шаблоне расшифровки данное значение должно быть установлено на 2 (чтобы URI возвратила секретный ключ). В случае цифровой подписи значение данного поля является свободным.

G_{KT}: Поле Степень структурирования для выражения степени структурирования, с которой изменяется информация о ключе.

V_{KT}: Поле списка значений для отображения меняющегося списка информации о ключе.

Отметим, что в случае секретного ключа (шаблон расшифровки), открытый ключ и сертификат не имеют смысла: шаблон ключа должен хранить некоторую информацию о расположении ключа (например, URI).

Информация о ключе может быть представлена одним или более значениями при помощи поля Степень структурирования инструмента (G_{KT}), описанного в п. 5.10, и поля списка значений (V_{KT}), описанного в п. 5.11. Вместе эти два поля (G_{KT} и V_{KT}) определяют то, как значения ключа в списке значений (V_{KT}) применяются к защищенным данным изображения, как описано в пп. 5.10 и 5.11.

Информация о ключе в списке значений может принимать любую из форм, определенных в таблице 44. Если $KID_{KT} = 1$, тогда каждое значений определяется при помощи шаблона сертификата X.509, описанного в п. 5.8.5.1. Если $KID_{KT} = 2$, тогда каждое значение определяется при помощи URI для сертификата или секретного ключа.

Таблица 43 – Значения шаблона ключа

Параметр	Размер (биты)	Значения
LK_{KT}	16	1 ... 65 535
KID_{KT}	8	Таблица 44
G_{KT}	24	См. п. 5.10
V_{KT}	Переменный	См. п. 5.11

Таблица 44 – Значения идентификатора информации о ключе (KID_{KT})

Значения	Идентификатор информации о ключе
0	Зарезервировано
1	Сертификат X.509 (ИСО/МЭК 9594-8)
2	URI для сертификата или секретный ключ
	Все остальные значения зарезервированы для использования ИСО

5.8.5.1 Шаблон сертификата X.509

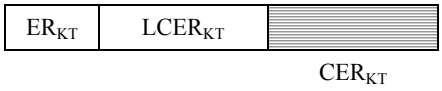


Рисунок 33 – Синтаксис сертификата X.509

ER_{KT}: Правило шифрования для сертификата X.509.

$LCER_{KT}$: Длина сертификата X.509 (CER_{KT}) в байтах.

CER_{KT}: Сертификат X.509.

Таблица 45 – Значения сертификата X.509 (KI_{KT}, если $KID_{KT} = 2$)

Параметры	Размер (биты)	Значения
ER_{KT}	8	0 ... 255 (см. таблицу 46)
$LCER_{KT}$	16	1 ... 65 535
CER_{KT}	Переменный	–

Таблица 46 – Значения правила шифрования (ER_{KT})

Значения	Правило шифрования аутентификатора
0	Зарезервировано
1	DER (RFC 3217)
2	BER (RFC 3394)
	Все остальные значения зарезервированы для использования ИСО

5.9 Синтаксис области обработки (PD)

Синтаксис области обработки используется для обозначения того, к какой области применяется инструмент JPSEC. Возможные области включают область пикселов, область вейвлет-коэффициента, область квантованного вейвлет-коэффициента и область кодового потока.

Рисунок 34 – Синтаксис области обработки

PD: Область обработки. В данном поле используется структура FBAS.

F_{PD}: Поле области обработки для предоставления дальнейшей подробной информации об области обработки. В данном поле используется структура FBAS.

Таблица 47 – Параметры области обработки

Параметр	Размер (биты)	Значения
PD	Переменный (FBAS)	См. таблицу 48
F_{PD}	Переменный (FBAS)	В области вейвлет-коэффициента и квантованного вейвлет-коэффициента см. таблицу 49 В области кодового потока см. таблицу 50

Таблица 48 – Значения параметра области обработки (PD)

Число битов FBAS	Значения	Семантика
1	1	Области пикселов. Метод защиты применяется к пикселам изображения
	0	В противном случае
2	1	Область вейвлет-коэффициента. Метод защиты применяется к вейвлет-коэффициенту
	0	В противном случае
3	1	Область квантованного вейвлет-коэффициента: Метод защиты применяется к квантованному вейвлет-коэффициенту
	0	В противном случае
4	1	Область кодового потока: Метод защиты применяется к кодовому потоку, генерированному из арифметического кодирующего устройства
	0	В противном случае

Отметим, что поле PD должно иметь один и только один бит, установленный на 1, поскольку каждый инструмент JPSEC применяется только к одной области.

В области пикселов изображения, области вейвлет-коэффициента и квантованного вейвлет-коэффициента, для того, чтобы применить инструменты безопасности, двухмерные данные необходимо преобразовать в одномерные. Данное преобразование необходимо выполнить путем сканирования двухмерных данных изображения при помощи метода растрового сканирования.

Таблица 49 – Значения параметра для поля области обработки (F_{PD}) в области вейвлет-коэффициента и области квантованного вейвлет-коэффициента

Число битов FBAS	Значение	Семантика
1	0	Метод защиты применяется к биту знака
	1	Метод защиты применяется к наиболее значимому биту

Таблица 50 – Значения параметров для поля области обработки (F_{PD}) в области кодового потока

Число битов FBAS	Значение	Семантика
1	0	Метод защиты применяется как к заголовку пакета, так и к телу пакета
	1	Метод защиты применяется только к телу пакета

Данное поле (F_{PD}) используется для предоставления дальнейшей информации об обрабатывающей области. При различных значениях PD, данное поле (F_{PD}) имеет различную семантику. Например, в области вейвлет-коэффициента и области квантованного вейвлет-коэффициента, первый бит F_{PD} используется для указания на то, применяется ли инструмент JPSEC к наиболее важному биту. В области кодового потока первый бит F_{PD} используется для указания на то, применяется ли инструмент JPSEC только к телу пакета или к заголовку пакета и к телу пакета; в области пикселов, данное поле (F_{PD}) зарезервировано.

5.10 Синтаксис Степени структурирования (G)

Степень структурирования используется для обозначения единицы защиты для каждого метода защиты. В таблице 53 определяются возможные степени структурирования. На рисунке 35 показан синтаксис Степени структурирования.

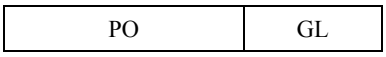


Рисунок 35 – Синтаксис Степени структурирования

PO: Порядок обработки.

GL: Уровень Степени структурирования.

Таблица 51 – Значения параметра Степень структурирования (G)

Параметр	Размер (биты)	Значения
PO	16	См. таблицу 52
GL	8	См. таблицу 53

Таблица 52 –Значения порядка обработки (PO)

Значения MSB LSB	Порядок обработки
0 000 000 000 000 000	Порядок определяется параметрами Зоны влияния, связанными с изображением
1 000 000 000 000 000	Порядок определяется параметрами битового потока в Зоне влияния, несвязанными с изображением
1 000 000 000 000 001	Порядок определяется параметрами пакета в Зоне влияния, несвязанными с изображением
0 000 001 010 011 100	Элемент изображения – разрешение – слой – компонент – граница
0 000 011 100 001 010	Элемент изображения – компонент – граница – разрешение – слой
0 000 010 001 011 100	Элемент изображения – слой – разрешение – компонент – граница
0 000 100 011 001 010	Элемент изображения – граница – компонент – разрешение – слой
0 000 001 100 011 100	Элемент изображения – разрешение – граница – компонент – слой
	Все остальные значения зарезервированы

Таблица 53 – Значения уровня Степени структурирования (GL)

Значения MSB LSB	Степень структурирования
0000 0000	Элемент изображения
0000 0001	Часть элемента изображения
0000 0010	Компонент
0000 0011	Уровень разрешения
0000 0100	Слой
0000 0101	Граница
0000 0110	Пакет
0000 0111	Поддиапазон (субдиапазон)
0000 1000	Блок кода
0000 1001	Весь участок, указанный в ZOI
1000 0000	Элемент, указанный в ZOI, не связанной с изображением
1000 0001	Зона, указанная в ZOI, не связанной с изображением
	Все остальные значения зарезервированы

Для того чтобы обработать всю зону, определенную ZOI, уровень степени структурирования должен быть "зона, определенная в ZOI".

5.11 Синтаксис списка значений (V)

Поле списка значений используется для определения значений, которые изменяются, когда применяется инструмент, и степень структурирования, с которой они изменяются. Оно используется для сигнализации об изменяющихся значениях таких, как ключи, векторы инициализации, значения MAC, цифровые подписи и значения хэш-функции. В поле Списка значений сначала определяется число значений в списке и размер каждого значения. Затем в нем перечисляются сами значения.

Как описывалось в п. 5.6.2, для нормативных инструментов JPSEC в поле Списка значений представлены различные значения для каждого шаблона. Для шаблона расшифровки, в поле представлены векторы инициализации IV_{bc} или IV_{sc} в зависимости от того, используется ли блочный шифр или потоковый шифр. Для шаблона аутентификации, в поле представлено значение MAC VAL_{MAC} для аутентификации на основе хэш-функции и шифра. Для шаблона цифровой подписи, в поле представлена цифровая подпись SIG_{DS}. Для шаблона хэш-функции, в поле представлено значение хэш-функции HV_{hash}. Некоторые виды использования шаблонов не требуют определения значений, например, не все режимы расшифровки используют векторы инициализации. В таких случаях значения N_v и S_v поля Списка значений следует установить равными нулю так, чтобы в списке значений VL не было элементов. Если нужно определить только одно значение, например, если ко всему изображению применяется один ключ, тогда значение N_v будет установлено на один так, чтобы в списке значений содержалось одно значение.

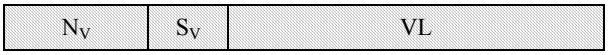


Рисунок 36 – Синтаксис поля списка значений

N_V: Число значений в списке значений VL. Если $N_V = 0$, тогда поле завершается. В данном поле используется структура RBAS.

S_V: Размер каждого значения в списке значений VL в байтах. В данном поле используется структура RBAS.

VL: Список значений.

Таблица 54 – Значения параметра для поля списка значений (V)

Параметр	Размер (биты)	Значения
N_V	16 + 8 * n (RBAS)	0 ... $(2^{15+7*n} - 1)$
S_V	8 + 8 * n (RBAS)	0 ... $(2^{7+7*n} - 1)$
VL	0, если $N_V = 0$ $N_V * S_V$ в противном случае	Неприменимо Определяется шаблоном

5.12 Взаимосвязь между ZOI, Степенью структурирования (G) и Списком значений (VL)

ZOI, PO и GL используются вместе для гарантирования уникального режима работы применяемого(ых) инструмента(ов) JPSEC, вне зависимости от порядка продвижения кодового потока JPEG 2000. Другими словами, получающаяся в результате подпись, значения MAC и зашифрованный кодовый поток не зависят от порядка продвижения кодового потока JPEG 2000. Зона влияния (ZOI) определяет, во всей своей полноте, часть кодового потока JPEG 2000, который будет защищаться при помощи инструмента JPSEC; Порядок обработки (PO), с другой стороны, указывает порядок, в котором инструмент JPSEC обрабатывает кодовый поток; уровень Степени структурирования (GL) определяет защитные единицы, содержащие непрерывную последовательность байтов в переупорядоченном кодовом потоке. И в заключение, каждая единица защиты соответствует значению в Списке значений (VL) в том порядке, в котором они появляются в переупорядоченном кодовом потоке. Данную взаимосвязь можно проиллюстрировать при помощи одного примера, где кодовый поток JPEG 2000 имеет 1 элемент изображения, 3 уровня разрешения и 3 слоя, а число компонентов и границ не существенно. В первоначальном кодовом потоке JPEG 2000 порядок продвижения – RLCP, Зона влияния имеет разрешение 0 и 1, а Порядок обработки (PO) – TRLCP. На рисунках 37 и 38 показано переупорядочение кодового потока и сопоставление каждой единицы защиты со Списком значений (VL), когда уровень Степени структурирования (GL) – разрешение и слой, соответственно.

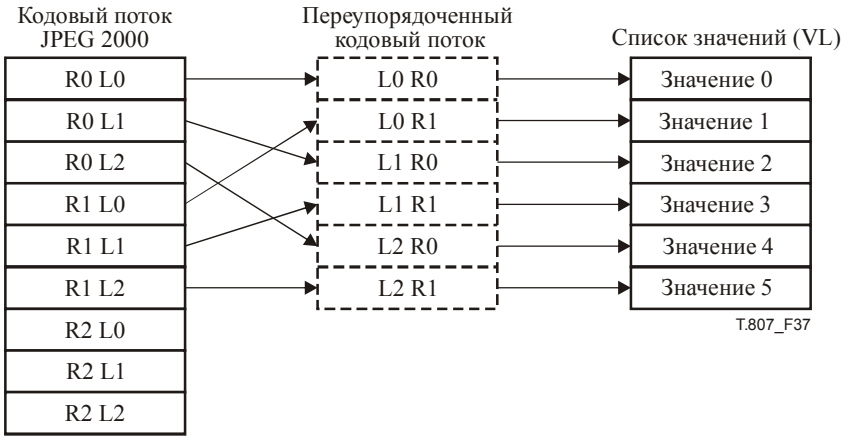


Рисунок 37 – Уровень Степени структурирования (GL) – разрешение

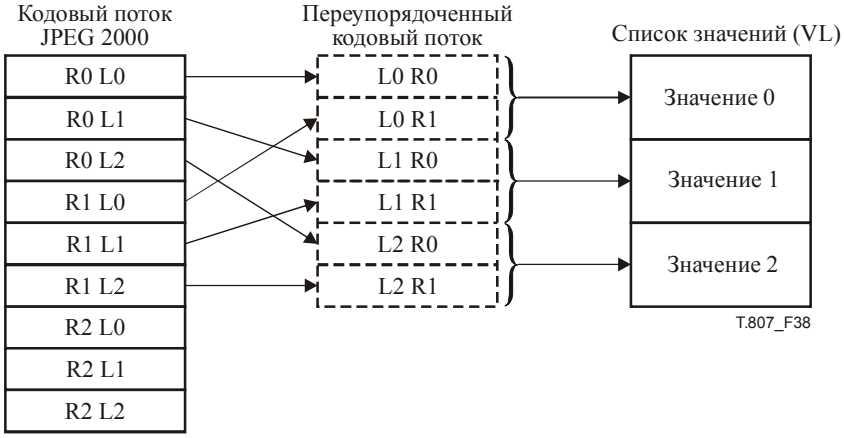


Рисунок 38 – Уровень Степени структурирования (GL) – слой

ПРИМЕЧАНИЕ. – Переупорядоченный кодовый поток используется только для генерирования значений в Списке значений (VL). Конечный кодовый поток JPSEC будет иметь такой же порядок продвижения, как и первоначальный кодовый поток JPEG 2000.

5.13 Маркер безопасности внутри кодового потока (INSEC)

Маркер безопасности внутри кодового потока (INSEC) предоставляет дополнительные средства для передачи информации о безопасности. Он не является обязательным и используется вместе с маркером безопасности SEC. В частности, он используется вместе с ненормативным инструментом JPSEC.

Если быть более точным, маркер SEC присутствует в основном заголовке и дает общую информацию об инструменте JPSEC, применяемом для защиты изображения. Маркер INSEC присутствует в данных битового потока и предоставляет дополнительные или альтернативные параметры для ненормативного инструмента JPSEC, определяемого при помощи параметра указателя экземпляра для инструмента. Поэтому указатель экземпляра инструмента в маркере INSEC должен соответствовать одному из указателей экземпляра инструмента в основном заголовке.

Сегмент маркера INSEC может быть помещен в данные битового потока. Данные сегмент пользуется тем, что арифметическое устройство расшифровки в JPEG 2000 прекращает чтение байтов из битового потока, когда обнаруживает маркер завершения (т. е. два байта со значением больше чем 0xFF8F).

Информация, находящаяся в сегменте маркера INSEC является существенной для предшествующего(их) или последующего(их) защищенного(ых) блока(ов) кода до тех пор, пока не будет обнаружен другой маркер INSEC.

Отметим, что включение маркеров INSEC может привести к тому, что файл не будет соответствовать Части 1 JPEG 2000. Отметим, что у некоторых устройств расшифровки могут быть трудности с обработкой маркера в середине пакета. Вставка в любую часть внутри пакета сделает недействительной длину пакета, обозначенную в заголовке пакета. Также могут возникнуть проблемы с шифрованием и маркерами INSEC из-за:

a) недостаточных ограничений по эмуляции маркера при шифровании; и/или

b) невозможности разместить маркер при наличии шифрования.

Синтаксис маркера INSEC определен на рисунке 39.

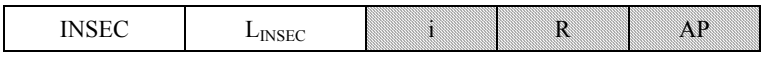


Рисунок 39 – Синтаксис маркера безопасности внутри кодового потока

INSEC: Код маркера. В таблице 55 приведены размеры и значения символов и параметров для сегмента маркера безопасности внутри кодового потока.

L_{INSEC}: Длина сегмента маркера в байтах (за исключением маркера). Отметим, что сегмент маркера INSEC должен быть выровненным по байтам.

i: Указатель экземпляра инструмента, соответствующий одному из параметров указателя экземпляра инструмента в сегменте маркера SEC и, таким образом, определяющий экземпляр инструмента JPSEC, на который ссылается данный маркер INSEC. В данном поле используется структура RBAS.

R: Зона важности для информации INSEC. В данном поле используется структура FBAS.

AP: Дополнительные или альтернативные параметры для метода защиты. Устройство шифрования должно всегда проверять, чтобы оно не эмулировало маркер в данный параметр.

Таблица 55 – Значения параметра безопасности внутри кодового потока (INSEC)

Параметр	Размер (биты)	Значения
INSEC	16	0xFF94
L_{INSEC}	16	2 ... $(2^{16} - 1)$
i	8 + 8 * n (RBAS)	0 ... $(2^{7+7*n} - 1)$
R	Переменный (FBAS)	См. таблицу 56
AP	Переменный	Определяется Органом регистрации или приложением

Таблица 56 – Значения зоны важности (R)

Число битов FBAS	Значения	Зона важности
0	0	Предыдущие блоки кода
	1	Следующие блоки кода

Поскольку INSEC используется с ненормативными инструментами JPSEC, формат дополнительных или альтернативных параметров определяется самим инструментом, который обозначается ID инструмента. В частности, ненормативные инструменты JPSEC определяются органом регистрации или частными приложениями JPSEC. Таким образом, определение данных инструментов должно включать в себя использование INSEC, если оно разрешено.

6 Примеры использования нормативного синтаксиса (информативные)

6.1 Примеры использования ZOI

В данном подпункте содержатся примеры, иллюстрирующие, как можно использовать синтаксис Зоны влияния.

В нижеследующих примерах верхние индексы, используемые в Pzoi, Mzoi и Izoi, соответствуют указателю элементов связанных и несвязанных с изображением, о которых сигнализирует структура BAS в DCzoi для того, чтобы они появились в DCzoi.

6.1.1 Пример 1

В данном подпункте рассматривается пример оказания влияния на уровни разрешения более 3 и участок изображения с левым верхним углом (100, 120) и правым нижним углом (180, 210). В данном примере необходимо 9 байтов.

Таблица 57 – ZOI в примере 1

Параметр			Размер (биты)	Значения (по порядку)	Производное значение (смысл)
NZzoi			8 (RBAS)	1	Число Зон равно 1
Зона^0	DCzoi		1	0_b	Далее не следует сегмент, выровненный по байтам
			1	0_b	Класс описания, связанный с изображением
			6	101000_b	Участки изображения и уровни разрешения определены по порядку
	Pzoi^1	Mzoi^1	1	0_b	Далее не следует сегмент, выровненный по байтам
			1	0_b	На указанные зоны оказывает влияние инструмент JPSEC
			1	0_b	Определен один элемент
			2	00_b	Режим прямоугольника
			2	00_b	Izoi использует 8-битное целое число
			1	1_b	Izoi описывается в двух измерениях
		Izoi^1	8	$0110\ 0100_b$	Xul равно 100
			8	$0111\ 1000_b$	Yul равно 120
			8	$1011\ 0100_b$	Xlr равно 180
			8	$1101\ 0010_b$	Ylr равно 210
	Pzoi^3	Mzoi^3	1	0_b	Далее не следует сегмент, выровненный по байтам
			1	1_b	На дополнение к указанным зонам оказывает влияние инструмент JPSEC
			1	0_b	Определен один элемент
			2	11_b	Максимальный режим
			2	00_b	Izoi использует 8-битное целое число
			1	0_b	Izoi описывается в одном измерении
		Izoi^3	8	$0000\ 0010_b$	Определены уровни разрешения ≤ 2. (То есть уровни разрешения > 3 задаются при помощи Максимального режима и дополнительного коммутатора.)

6.1.2 Пример 2

В данном подпункте рассматривается пример оказания влияния на блоки кода, указатель левого верхнего угла которых равен 5, а указатель правого верхнего угла равен 10 в поддиапазоне 1 при уровне разрешения 0. В данном примере необходимо 10 байтов.

Размер (биты) – ZOI в примере 2

Параметр			Размер (биты)	Значение (по порядку)	Производное значение (смысл)
NZzoi			8 (RBAS)	1	Число Зон равно 1
Зона[0]	DCzoi[1]		1	1_b	Далее следует сегмент, выровненный по байтам
			1	0_b	Класс описания, связанный с изображением
			6	001000_b	Определены уровни разрешения
	DCzoi[2]		1	0_b	Далее не следует сегмент, выровненный по байтам
			1	0_b	Класс описания, связанный с изображением
			6	001100_b	Определены поддиапазоны и блоки кода
	Pzoi[3]	Mzoi[3]	1	0_b	Далее не следует сегмент, выровненный по байтам
			1	0_b	На указанные зоны оказывает влияние инструмент JPSEC
			1	0_b	Определен один элемент
			2	10_b	Режим указателя
			2	00_b	Izoi использует 8-битное целое число
			1	0_b	Izoi описывается в одном измерении
		Izoi[3]	8	$0000\ 0000_b$	Указатель уровня разрешения – 0
	Pzoi[9]	Mzoi[8]	1	0_b	Далее не следует сегмент, выровненный по байтам
			1	0_b	На указанные зоны оказывает влияние инструмент JPSEC
			1	0_b	Определен один элемент
			2	10_b	Режим указателя
			2	00_b	Izoi использует 8-битное целое число
			1	0_b	Izoi описывается в одном измерении
		Izoi[8]	8	$0000\ 0001_b$	Определен поддиапазон 1
	Pzoi[10]	Mzoi[9]	1	0_b	Далее не следует сегмент, выровненный по байтам
			1	0_b	На указанные зоны оказывает влияние инструмент JPSEC
			1	0_b	Определен один элемент
			2	00_b	Режим прямоугольника
			2	00_b	Izoi использует 8-битное целое число
			1	0_b	Izoi описывается в одном измерении
		Izoi[9]	8	$0000\ 0101_b$	Указатель блока кода для левого верхнего угла равен 5
			8	$0000\ 1010_b$	Указатель блока кода для правого нижнего угла равен 10

6.1.3 Пример 3

В данном подпункте рассматривается пример оказания влияния на сегменты данных от 10 до 100 байтов и от 10 000 до 12 000 байтов. В данном примере необходимо 12 байтов.

Таблица 59 – ZOI в примере 3

Параметр			Размер (биты)	Значение (по порядку)	Производное значение (смысл)
NZzoi			8 (RBAS)	1	Число Зон равно 1
Зона^0	DCzoi		1	0_b	Далее не следует сегмент, выровненный по байтам
			1	1_b	Класс описания, не связанный с изображением
			6	010000_b	Определены байтовые диапазоны после маркера SOD
	Pzoi^2	Mzoi^2	1	0_b	Далее не следует сегмент, выровненный по байтам
			1	0_b	На указанные зоны оказывает влияние инструмент JPSEC
			1	1_b	Определено много элементов
			2	01_b	Режим диапазона
			2	01_b	Izoi использует 16-битное целое число
			1	0_b	Izoi описывается в одном измерении
		Nzoi^2	8	$0000\ 0010_b$	Число сегментов данных – 2
		Izoi^{21}	16	$0000\ 0000_b$ $0000\ 1010_b$	Позиция начального байта – 10-я (байты)
			16	$0000\ 0000_b$ $0110\ 0100_b$	Позиция конечного байта – 100-я (байты)
		Izoi^{21}	16	$0010\ 0111_b$ $0001\ 0000_b$	Позиция начального байта – 10 000-я (байты)
			16	$0010\ 1110_b$ $1110\ 0000_b$	Позиция конечного байта – 12 000-я (байты)

6.1.4 Пример 4

В данном подпункте рассматривается пример оказания влияния на уровень разрешения 0 и соответствие байтовых сегментов от 10 до 100 данным для уровня разрешения 0. В данном примере необходимо 10 байтов.

Таблица 60 – ZOI в примере 4

Параметр			Размер (биты)	Значения (по порядку)	Производное значение (смысл)
NZzoi			8 (RBAS)	1	Число Зон равно 1
Зона^0	DCzoi^1		1	1_b	Далее следует сегмент, выровненный по байтам
			1	0_b	Класс описания, связанный с изображением
			6	001000_b	Уровни разрешения определены по порядку
	DCzoi^2		1	0_b	Далее не следует сегмент, выровненный по байтам
			1	1_b	Класс описания, несвязанный с изображением
			6	010000_b	Определены байтовые диапазоны
	Pzoi^1	Mzoi^1	1	0_b	Далее не следует сегмент, выровненный по байтам
			1	0_b	На указанные зоны оказывает влияние инструмент JPSEC
			1	0_b	Определен один элемент
			2	10_b	Режим указателя
			2	00_b	Izoi использует 8-битное целое число
			1	0_b	Izoi описывается в одном измерении
		Izoi^1	8	$0000\ 0000_b$	Уровень разрешения – 0

Таблица 60 – ZOI в примере 4

Параметр			Размер (биты)	Значения (по порядку)	Производное значение (смысл)
Зона[0]	Pzoi[2]	Mzoi[2]	1	0_b	Далее не следует сегмент, выровненный по байтам
			1	0_b	На указанные зоны оказывает влияние инструмент JPSEC
			1	0_b	Определен один элемент
			2	01_b	Режим диапазона
			2	01_b	Izoi использует 16-битное целое число
			1	0_b	Izoi описывается в одном измерении
		Izoi[1]	16	0000 0000 0000 1010_b	Позиция начального байта – 10-я (байты)
			16	0000 0000 0110 0100_b	Позиция конечного байта – 100-я (байты)

6.1.5 Пример 5

В данном подпункте рассматривается пример оказания влияния на уровни разрешения более 3 в элементах изображения, указатель левого верхнего элемента которых равняется 0, а указатель правого нижнего элемента равен 5, число слоев меньше или равно 5 в элементах изображения, указатель левого верхнего элемента которых равен 10, а указатель правого нижнего элемента равен 15. В данном примере необходимо 13 байтов.

Таблица 61 – ZOI в примере 5

Параметр			Размер (биты)	Значение (по порядку)	Производное значение (смысл)
NZzoi			8 (RBAS)	2	Число Зон равно 2
Зона[0]	DCzoi		1	0_b	Далее не следует сегмент, выровненный по байтам
			1	0_b	Класс описания, связанный с изображением
			6	01 1000_b	Элементы изображения уровни разрешения определены по порядку
	Pzoi[2]	Mzoi[2]	1	0_b	Далее не следует сегмент, выровненный по байтам
			1	0_b	На указанные зоны оказывает влияние инструмент JPSEC
			1	0_b	Определен один элемент
			2	00_b	Режим прямоугольника
			2	00_b	Izoi использует 8-битное целое число
			1	0_b	Izoi описывается в одном измерении
		Izoi[2]	8	0000 0000_b	Указатель левого верхнего элемента изображения – 0
			8	0000 0101_b	Указатель правого нижнего элемента изображения – 5
	Pzoi[3]	Mzoi[3]	1	0_b	Далее не следует сегмент, выровненный по байтам
			1	1_b	На дополнение к указанным зонам оказывает влияние инструмент JPSEC
			1	0_b	Определен один элемент
			2	11_b	Максимальный режим
			2	00_b	Izoi использует 8-битное целое число
			1	0_b	Izoi описывается в одном измерении
		Izoi[3]	8	0000 0010_b	Определены уровни разрешения ≤ 2. (То есть уровни разрешения > 3 задаются при помощи Максимального режима и дополнительного коммутатора.)

Таблица 61 – ZOI в примере 5

Параметр			Размер (биты)	Значение (по порядку)	Производное значение (смысл)
Зона[1]	DCzoi		1	0_b	Далее не следует сегмент, выровненный по байтам
			1	0_b	Класс описания, связанный с изображением
			6	010100_b	Элементы изображения и слои определяются по порядку
	Pzoi[2]	Mzoi[2]	1	0_b	Далее не следует сегмент, выровненный по байтам
			1	0_b	На указанные зоны оказывает влияние инструмент JPSEC
			1	0_b	Определен один элемент
			2	00_b	Режим прямоугольника
			2	00_b	Izoi использует 8-битное целое число
			1	0_b	Izoi описывается в одном измерении
		Izoi[2]	8	$0000\ 1010_b$	Указатель левого верхнего элемента равен 10
			8	$0000\ 1111_b$	Указатель правого нижнего элемента равен 15
	Pzoi[4]	Mzoi[4]	1	0_b	Далее не следует сегмент, выровненный по байтам
			1	0_b	На указанные зоны оказывает влияние инструмент JPSEC
			1	0_b	Определен один элемент
			2	11_b	Максимальный режим
			2	00_b	Izoi использует 8-битное целое число
			1	0_b	Izoi описывается в одном измерении
		Izoi[4]	8	$0000\ 0101_b$	Число слоев ≤ 5 определяется при помощи Максимального режима

6.1.6 Пример 6

В данном подпункте рассматривается пример оказания влияния на сегменты заголовка от 10 до 100 байтов. В данном примере необходимо 8 байтов.

Таблица 62 – ZOI в примере 6

Параметр			Размер (биты)	Значение (по порядку)	Производное значение (смысл)
NZzoi			8 (RBAS)	1	Число Зон равно 1
Зона[0]	DCzoi		1	0_b	Далее не следует сегмент, выровненный по байтам
			1	1_b	Класс описания, несвязанный с изображением
			6	001000_b	Определяются байтовые диапазоны после маркера SEC
	Pzoi[3]	Mzoi[3]	1	0_b	Далее не следует сегмент, выровненный по байтам
			1	0_b	На указанные зоны оказывает влияние инструмент JPSEC
			1	0_b	Определен один элемент
			2	01_b	Режим диапазона
			2	01_b	Izoi использует 16-битное целое число
			1	0_b	Izoi описывается в одном измерении
		Izoi[3]	16	$0000\ 0000$ $0000\ 1010_b$	Позиция начального байта – 10-я (байты)
			16	$0000\ 0000$ $0110\ 0100_b$	Позиция конечного байта – 100-я (байты)

6.2 Примеры шаблона информации о ключе

6.2.1 Пример 1

В таблице 63 показан пример использования одного секретного ключа (128 битов) для расшифровки кодового потока, причем идентификация секретного ключа осуществляется при помощи URI и извлекается с сервера ключей, основанного на URI, на стадии расшифровки.

Таблица 63 – Информация о ключе в примере 1

Параметр		Размер (биты)	Значение	Производное значение (смысл)
LK_{KT}		16	128	Длина ключа составляет 128 битов
KID_{KT}		8	2	Определяется URI для секретного ключа
G_{KT}	PO	16	000 001 010 011 100 0_b	Порядок обработки: элемент изображения – разрешение – слой – компонент – граница
	GL	8	0000 1001_b	Единицей защиты является весь участок, определенный в ZOI
V_{KT}	N_V	16 (RBAS)	1	Число значений в списке значений V равно 1
	S_V	8 (RBAS)	19	Длина информации о ключе – 19 байтов
	V1	152	https://server/file	Секретный ключ может быть извлечен с https://server/file

6.2.2 Пример 2

В таблице 64 показан пример использования сертификата X.509 для аутентификации кодового потока, причем сертификат X.509 вложен в KI_{KT} при методе шифрования DER.

Таблица 64 – Информация о ключе в примере 2

Параметр			Размер (биты)	Значение	Производное значение
LK_{KT}			16	1 024	Длина ключа составляет 1 024 бита
KID_{KT}			8	2	Определяется сертификат X.509
G_{KT}	PO		16	000 001 010 011 100 0b	Порядок обработки: элемент изображения – разрешение – слой – компонент – граница
	GL		8	0000 1001b	Единицей защиты является весь участок, определенный в ZOI
V_{KT}	N_V		16 (RBAS)	1	Число значений в списке значений V равно 1
	S_V		8 (RBAS)	Переменный	Длина сертификата X.509
	V1	ER_{KT}	8	1	Сертификат X.509 зашифрован при помощи метода шифрования DER
		$LCER_{KT}$	16	Переменный	Длина CER_{KT}
		CER_{KT}	Переменный	Значение сертификата	Вложен сертификат с открытым ключом на 1 024 бита

6.2.3 Пример 3

В таблице 65 показан пример использования одного открытого ключа для аутентификации кодового потока, причем в KI_{KT} вложен открытый ключ.

Таблица 65 – Информация о ключе в примере 3

Параметр		Размер (биты)	Значение	Производное значение (смысл)
LK_{KT}		16	1 024	Длина ключа составляет 1 024 бита
KID_{KT}		8	1	Определяется открытый ключ
G_{KT}	PO	16	000 001 010 011 100 0b	Порядок обработки: элемент изображения – разрешение – слой – компонент – граница
	GL	8	0000 1001b	Единицей защиты является весь участок, определенный в ZOI
V_{KT}	N_V	16 (RBAS)	1	Число значений в списке значений V равно 1
	S_V	8 (RBAS)	256	Длина открытого ключа составляет 256 байтов
	V1	2 048	Значение открытого ключа	Вложен открытый ключ

6.2.4 Пример 4

В таблице 66 показа пример использования множества секретных ключей для расшифровки кодового потока, причем для разных слоев используются различные секретные ключи.

Таблица 66 – Информация о ключе в примере 4

Параметр		Размер (биты)	Значение	Производное значение (смысл)
LK_{KT}		16	128	Число значений в списке значений V равно 1
KID_{KT}		8	3	Определяется URI для секретного ключа
G_{KT}	PO	16	$000\ 001\ 010\ 011\ 1000_b$	Порядок обработки: элемент изображения – разрешение – слой – компонент – граница
	GL	8	$0000\ 0100_b$	Единицей защиты является слой
V_{KT}	N_V	16 (RBAS)	3	Число значений в списке значений V равно 3
	S_V	8 (RBAS)	16	Длина каждого Vn составляет 16 байтов
	V1	128	https://server/1	Секретный ключ для 1-го уровня может быть извлечен с https://server/1
	V2	128	https://server/2	Секретный ключ для 2-го уровня может быть извлечен с https://server/2
	V3	128	https://server/3	Секретный ключ для 3-го уровня может быть извлечен с https://server/3
	V4	128	https://server/4	Секретный ключ для 4-го уровня может быть извлечен с https://server/4

6.3 Примеры использования нормативного инструмента JPSEC

В нижеследующих примерах описывается, как можно использовать ZOI и шаблоны ключа для оказания основных услуг безопасности таких, как шифрование и аутентификация, в отношении закодированного изображения JPEG 2000.

6.3.1 Пример 1

Изображение кодируется при помощи JPEG 2000 и имеет три разрешения. В данном примере первое разрешение не шифруется для того, чтобы обеспечить возможность предварительного просмотра, а второе и третье разрешения зашифровываются при помощи ключей k1 и k2, соответственно. В данном случае изображение на входе кодируется в порядке продвижения RLCP, имеет 1 элемент изображения, 3 разрешения, 3 слоя, Nc компонентов и Np границ (в данном примере число компонентов и границ не существенно). Шифрование выполняется при помощи AES в режиме CBC без дополнения (битами) (используя занятие зашифрованного текста), для шифрования разрешения 1 используется ключ k0, для шифрования разрешения 2 используется ключ k2, а разрешение 0 остается незашифрованным.

JPSEC сигнализирует о том, как потребителю JPSEC следует расшифровывать JPSEC кодовый поток. Сначала сигнализируется об ID шаблона инструмента для шаблона расшифровки. Для разрешения 1 определяются две ZOI и соответствующий ему байтовый диапазон B0-B1, а для разрешения 2 – соответствующий ему байтовый диапазон B2-B3. Параметры шаблона расшифровки указывают, что шифрование AES применяется без дополнения (битами) (используя занятие зашифрованного текста). Об информации о ключе и том, что к различным разрешениям применяются различные ключи, сигнализируется при помощи параметров информации о ключе. В частности, степень структурирования ключа определена как разрешение, и, таким образом, каждое разрешение имеет отдельный (собственный) ключ, где порядок обработки сигнализируется как TRLCP. Информация о ключе для каждого разрешения содержится в списке значений для ключей. Шифрование выполняется в кодовом потоке, причем зашифровывается как заголовки пакета, так и тело пакета. Степень структурирования шифрования – разрешение, где обработка выполняется в порядке TRLCP, т. е. в том же порядке, что и первоначальный кодовый поток. Поскольку шифрование двух разрешений происходит по-отдельности, требуется два вектора инициализации (IV), они содержатся в списке значений.

Отметим, что получающийся в результате зашифрованный текст пакета определяется порядком обработки и поэтому не зависит от порядка прохождения кодового потока на входе; однако расположение зашифрованных пакетов в кодовом потоке на выходе повторяет порядок расположения пакетов кодового потока на входе.

Таблица 67 – Сегмент маркера SEC для примера 1

Параметр			Размер (биты)	Значения	Значение (смысл)
SEC			16	0xFF65	Маркер SEC
L_{SEC}			16 (RBAS)	0x82	Длина сегмента маркера SEC составляет 130 байтов
Z_{SEC}			8 (RBAS)	0	Указатель данного сегмента маркера SEC
P_{SEC}	F_{PSEC}		1	0_b	Далее не следует структура FBAS
		F_{INSEC}	1	0_b	INSEC не используется
		$F_{multiSEC}$	1	0_b	Используется один сегмент маркера SEC
		F_{mod}	2	00_b	Первоначальные данные JPEG 2000 были изменены
		F_{TRLCP}	1	0_b	В P_{SEC} использование маркера TRLCP не определено
		F_{TRLCP}	3	000_b	
	N_{tools}		8 (RBAS)	0000001_b	Число инструментов безопасности равно 1
	I_{max}		8 (RBAS)	0000000_b	Максимальный указатель экземпляра инструмента равен 0
t			8 (FBAS)	0	Нормативный инструмент JPSEC
i			8 (RBAS)	0	Указатель экземпляра инструмента
ID_T			8	1	Шаблон расшифровки
L_{ZOI}			16 (RBAS)	0x17	Длина ZOI составляет 23 байта
ZOI			184	См. таблицу 68	Зона влияния для данного инструмента
L_{PID}			16 (RBAS)	0x5e	Длина P_{ID} составляет 94 байта
P_{ID}			752	См. таблицу 69	Параметры для данной технологии

Таблица 68 – Пример ZOI

Параметр			Размер (биты)	Значение (по порядку)	Производное значение (смысл)
NZzoi			8 (RBAS)	2	Число Зон равно 1
Зона[0]	DCzoi[1]		1	1_b	Далее следует сегмент, выровненный по байтам
			1	0_b	Класс описания, связанный с изображением
			6	001000_b	Определяется разрешение
	DCzoi[2]		1	0_b	Далее не следует сегмент, выровненный по байтам
			1	1_b	Класс описания, несвязанный с изображением
			6	010000_b	Определяются байтовые диапазоны после маркера SOD
	Pzoi[0,1]	Mzoi[1]	1	0_b	Далее не следует сегмент, выровненный по байтам
			1	0_b	На указанные зоны оказывает влияние инструмент JPSEC
			1	0_b	Определен один элемент
			2	10_b	Режим указателя
			2	00_b	Izoi использует 8-битное целое число
			1	0_b	Izoi описывается в одном измерении
		Izoi	8	$0000\ 0001_b$	Определено разрешение 1
	Pzoi[0,2]	Mzoi[2]	1	0_b	Далее не следует сегмент, выровненный по байтам
			1	0_b	На указанные зоны оказывает влияние инструмент JPSEC
			1	0_b	Определен один элемент
			2	01_b	Режим диапазона
			2	01_b	Izoi использует 16-битное целое число
			1	0_b	Izoi описывается в одном измерении
		Izoi[21]	16	0x31CC	Позиция начального байта – 12 748 (байты). (B0)
			16	0xA3E8	Позиция конечного байта 41 960 (байты). (B1)

Таблица 68 – Пример ZOI

Параметр			Размер (биты)	Значение (по порядку)	Производное значение (смысл)
Зона[1]	DCzoi[1]		1	1_b	Далее следует сегмент, выровненный по байтам
			1	0_b	Класс описания, связанный с изображением
			6	001000_b	Определяется разрешение
	DCzoi[2]		1	0_b	Далее не следует сегмент, выровненный по байтам
			1	1_b	Класс описания, несвязанный с изображением
			6	010000_b	Определяются байтовые диапазоны после маркера SOD
	Pzoi[0,1]	Mzoi[1]	1	0_b	Далее не следует сегмент, выровненный по байтам
			1	0_b	На указанные зоны оказывает влияние инструмент JPSEC
			1	0_b	Определен один элемент
			2	10_b	Режим указателя
			2	00_b	Izoi использует 8-битное целое число
			1	0_b	Izoi описывается в одном измерении
		Izoi[1]	8	$0000\ 0010_b$	Определено Разрешение 2
	Pzoi[0,2]	Mzoi[2]	1	0_b	Далее не следует сегмент, выровненный по байтам
			1	0_b	На указанные зоны оказывает влияние инструмент JPSEC
			1	0_{b2}	Определен один элемент
			2	01_b	Режим диапазона
			2	10_b	Izoi использует 32-битное целое число
			1	0_b	Izoi описывается в одном измерении
		Izoi[2]	32	0xA3EE	Начальная позиция байта – составляет 41 966 (байты). (B2)
			32	0x21101	Конечная позиция байта – 135 425 (байтов). (B3)

Таблица 69 – Пример P_{ID}

Параметр		Размер (биты)	Значения	Значение (смысл)
T_{ID}		432	См. таблицу 70	Шаблоны расшифровки
PD		8 (FBAS)	0_b	Далее не следует сегмент, выровненный по байтам
			0_b	Область пикселов не используется
			0_b	Область вейвлет-коэффициента не используется
			0_b	Область квантованного вейвлет-коэффициента не используется
			1_b	Используется область кодового потока
			000_b	Зарезервировано для использования ИСО
F_{PD}		8 (FBAS)	0_b	Далее не следует байт FBAS
			1_b	Зашифровывается только тело пакета
			000000_b	Зарезервировано для использования ИСО
G	PO	16	$000\ 001\ 010\ 011\ 100\ 0_b$	Порядок обработки: элемент изображения – разрешение – слой – компонент – граница
	GL	8	$0000\ 0011_b$	Единицей защиты является уровень разрешения
V	N_V	16 (RBAS)	2	Число значений в списке значений V равно 2
	S_V	8 (RBAS)	16	Длина каждого Vn составляет 16 байтов
	V1	128	IV0	Значение вектора инициализации для R1
	V2	128	IV1	Значение вектора инициализации для R2

Таблица 70 – Пример шаблона расшифровки

Параметр		Размер	Значение (по порядку)	Производное значение (смысл)
ME_{decry}		8	0	Произошла эмуляция маркера
CT_{decry}		16	0001_b	Блочный шифр (AES)
CP_{decry}	M_{bc}	6	100000_b	Режим CBC. Дополнения битами не происходит
	P_{bc}	2	00_b	Занятие зашифрованного текста
	SIZ_{bc}	8	16	Размер блока (16 байтов, 128 битов)
	KT_{bc}	392	См. таблицу 71	Шаблон ключа

Таблица 71 – Пример шаблона ключа

Параметр		Размер (биты)	Значение	Производное значение (смысл)
LK_{KT}		16	128	Длина ключа равна 128 битов
KID_{KT}		8	2	Для секретного ключа используется URI
G_{KT}	PO	16	$0\ 000\ 001\ 010\ 011\ 100_b$	Порядок обработки: элемент изображения – разрешение – слой – компонент – граница
	GL	8	$0000\ 0011_b$	Единицей защиты является уровень разрешения
V_{KT}	N_V	32 (RBAS)	2	Число значений в списке значений V равно 2
	S_V	8 (RBAS)	19	Длина каждого Vn составляет 19 байтов
	V1	152	https://server/key1	Секретный ключ для уровня разрешения 1 может быть извлечен с https://server/key1
	V2	152	https://server/key2	Секретный ключ для уровня разрешения 2 может быть извлечен с https://server/key2

6.3.2 Пример 2

В данном случае, к закодированному изображению JPEG 2000 из предыдущего пример применяется аутентификация. В данном примере аутентифицируются все три разрешения и три слоя в каждом разрешении, причем для аутентификации каждого разрешения используется отдельный (собственный) ключ. Поскольку существует три разрешения, существует три ключа, и поскольку для каждого разрешения существует три слоя, для каждого разрешения будет существовать три значения MAC. Таким образом, для всего изображения JPSEC будет существовать девять значений MAC. В частности,

- Разрешение 0 имеет значения MAC M0, M1, M2 (по одному для каждого слоя) и использует ключ key0;
- Разрешение 1 имеет значения MAC M3, M4, M5 (по одному для каждого слоя) и использует ключ key1;
- Разрешение 2 имеет значения MAC M6, M7, M8 (по одному для каждого слоя) и использует ключ key2.

В данном примере иллюстрируется, как может происходить аутентификация сигнализации, а также гибкость, предоставляемая ZOI и инструментами степени структурирования. Как и в предыдущем примере, изображение на входе кодируется в порядке продвижения RLCP и имеет 1 элемент изображения, 3 разрешения, 3 слоя, Nc компонентов и Np границ (в данном примере число компонентов и границ не существенно). Аутентификация выполняется при помощи HMAC с SHA-1.

JPSEC сигнализирует, как потребитель JPSEC может подтвердить подлинность или аутентифицировать защищенное содержание JPSEC. Сначала выполняется сигнализация об ID шаблона инструмента для шаблона аутентификации. Затем для того чтобы сигнализировать о том, что существует три разрешения и соответствующие байтовые диапазоны для каждого разрешения, используется ZOI. Параметры шаблона аутентификации сигнализируют о том, что HMAC применяется с использованием SHA-1. Шаблона информации о ключе предоставляет информацию о ключах, включая информацию о том, что степень структурирования ключа – разрешение, и предоставление информации для каждого из трех ключей в списке значений для ключей. Область обработки для аутентификации определена как кодовый поток, включающий заголовки пакетов. Инструмент степени структурирования для аутентификации определен как слой, поэтому существует 3 MAC для каждого разрешения, что в общей сложности составляет 9 значений MAC. Эти девять значений MAC содержатся в списке значений. Порядок обработки всех вышеперечисленных параметров определяется как TRLCP, такой же, как и первоначальный порядок обработки кодового потока.

Отметим, что использование порядка обработки в поле степень структурирования гарантирует, что вне зависимости от порядка продвижения кодового потока, в результате будут получаться такие же значения MAC.

Отметим, что, хотя в данном примере демонстрируется использование MAC, можно использовать этот же подход для сигнализации использования многих цифровых подписей.

Таблица 72 – Сегмент маркера SEC

Параметр			Размер (биты)	Значение (по порядку)	Производное значение (смысл)
SEC			16	0xFF65	Маркер SEC
L_{SEC}			16	0x0099	Длина сегмента маркера SEC
Z_{SEC}			8 (RBAS)	0	Указатель данного сегмента маркера SEC
P_{SEC}	F_{PSEC}		1	0_b	Далее не следует структура FBAS
		F_{INSEC}	1	0_b	Сегмент маркера INSEC не используется
		$F_{multiSEC}$	1	0_b	В данном кодовом потоке только один сегмент маркера SEC
		F_{mod}	1	0_b	Первоначальные данные JPEG 2000 не были изменены
		F_{TRLCP}	1	0_b	Маркер TRLCP не используется
		Дополнение	3	000_b	Маркер TRLCP не используется
	N_{tools}		7	1	В данном кодовом потоке используется только один инструмент
	I_{max}		7	0	Максимальный указатель экземпляра инструмента – 0
Инструмент[0]	t		8 (FBAS)	0	Нормативный инструмент JPSEC
	i		8 (RBAS)	0	Указатель экземпляра инструмента
	ID_T		8	2	Данный нормативный инструмент использует шаблон аутентификации
	L_{ZOI}		16 (RBAS)	0x20	Длина ZOI составляет 32 байта
	ZOI		256	Таблица 73	Охваченная зона изображения
	L_{PID}		16 (RBAS)	0x6c	Длина P_{ID} составляет 108 байтов
	P_{ID}		928	Таблица 74	Параметры для инструмента JPSEC

Таблица 73 – Сигнализация ZOI

Параметр			Размер (биты)	Значение (по порядку)	Производное значение (смысл)
NZzoi			8 (RBAS)	1	Число Зон равно 1
Зона[0]	DCzoi[1]		1	1_b	Далее следует сегмент, выровненный по байтам
			1	0_b	Класс описания, связанный с изображением
			6	001000_b	Уровни разрешения определяются по порядку
	DCzoi[2]		1	0_b	Далее не следует сегмент, выровненный по байтам
			1	1_b	Класс описания, несвязанный с изображением
			6	010000_b	Определяются байтовые диапазоны
	Pzoi[0,1]	Mzoi[1]	1	0_b	Далее не следует сегмент, выровненный по байтам
			1	0_b	На указанные зоны оказывает влияние инструмент JPSEC
			1	0_b	Определен один элемент
			2	01_b	Режим диапазона
			2	00_b	Izoi использует 8-битное целое число
			1	0_b	Izoi описывается в одном измерении
		Izoi[1]	8	0	Начало диапазона – 0
			8	2	Окончание диапазона – 2

Таблица 73 – Сигнализация ZOI

Параметр			Размер (биты)	Значение (по порядку)	Производное значение (смысл)
Зона^{0}	Pzoi^{0,2}	Mzoi^{2}	1	0_b	Далее не следует сегмент, выровненный по байтам
			1	0_b	На указанные зоны оказывает влияние инструмент JPSEC
			1	1_b	Определено много элементов
			2	01_b	Режим диапазона
			2	10_b	Izoi использует 32-битное целое число
			1	0_b	Izoi описывается в одном измерении
		Nzoi	8 (RBAS)	3	Число Izoi составляет 3
		Izoi^{1}	32	104	Позиция начального байта – 104 (байты)
			32	12 762	Позиция конечного байта – 12 762 (байты)
		Izoi^{2}	32	12 768	Позиция начального байта – 12 768 (байты)
			32	41 980	Позиция конечного байта – 41 980 (байты)
		Izoi^{3}	32	41 986	Позиция начального байта – 41 986 (байты)
			32	135 445	Позиция конечного байта – 135 445 (байты)

Таблица 74 – Параметры сигнализации P_{ID}

Параметр					Размер (биты)	Значение (по порядку)	Производное значение (смысл)
T_{auth}	M_{auth}				8	0	Методы аутентификации: аутентификация на основе хэш-функции
	P_{auth}	M_{HMAC}			8	1	Для аутентификации используется HMAC
		H_{HMAC}			8	1	SHA-1 используется для хеширования
		KT_{HMAC}	LK_{KT}		16	128	Длина ключа измеряется в битах
			KID_{KT}		8	3	KI_{KT} содержит URI для частного ключа
			G_{KT}	PO	16	0 000 001 010 011 100_b	Порядок: элемент изображения – разрешение – слой – компонент – граница
				GL	8	00000011_b	Степень структурирования ключа – разрешение
			V_{KT}	N_V	16 (RBAS)	3	В списке существует 3 ключа
				S_V	8 (RBAS)	8	Размер каждого ключа составляет 8 байтов
				VL	64	*Key*0	Первый ключ – это *key*0 при разрешении 0
					64	*Key*1	Второй ключ – это *key*1 при разрешении 1
					64	*Key*2	Третий ключ – это ключ *key*2 при разрешении 2
		SIZ_{HMAC}			16	20	Размер MAC составляет 20
PD					8 (FBAS)	0_b	Далее не следует сегмент, выровненный по байтам
						0_b	Область пикселов не используется
						0_b	Область вейвлет-коэффициента не используется
						0_b	Область квантованного вейвлет-коэффициента не используется
						1_b	Используется область кодового потока
						000_b	Зарезервировано для использования ИСО

Таблица 74 – Параметры сигнализации P_{ID}

Параметр		Размер (биты)	Значение (по порядку)	Производное значение (смысл)
F_{PD}		8 (FBAS)	0_b	Далее не следует байт FBAS
			0_b	Зашифровывается заголовок и тело пакета
			000000_b	Зарезервировано для использования ИСО
G	PO	16	$000001010011 1000_b$	Порядок: элемент изображения – разрешение – слой – компонент – граница
	GL	8	00000100_b	Степень структурирования инструмента – слой
V	N_V	32 (RBAS)	9	Существует 9 MAC (по 3 MAC на каждое разрешение)
	S_V	8 (RBAS)	20	Размер каждого MAC составляет 20 байтов
	VL	160	*M*0	Первый MAC – *M*0
		160	*M*1	Второй MAC – *M*1
		160	*M*2	Третий MAC – *M*2
		160	*M*3	Четвертый MAC – *M*3
		160	*M*4	Пятый MAC – *M*4
		160	*M*5	Шестой MAC – *M*5
		160	*M*6	Седьмой MAC – *M*6
		160	*M*7	Восьмой MAC – *M*7
		160	*M*8	Девятый MAC – *M*8

6.4 Примеры поля искажений

В данном подпункте рассматривается несколько простых примеров использования поля искажения.

6.4.1 Пример 1

Данный пример строится на 3-м примере ZOI в п. 6.1.3, он показывает, как значения искажения могут быть связаны с двумя сегментами данных, о которых сигнализирует ZOI в выбранном примере. Как описывалось ранее, в примере 3 в п. 6.1.3 сигнализируется о двух сегментах данных: (1) байты от 10 до 100 и (2) байты от 10000 до 12000. Связывание полей искажения с этими двумя сегментами данных производится в два этапа. Сначала, о поле искажения сигнализируется в DCzoi. Затем, о значениях искажений сигнализируется при помощи $Pzoi^2$. Поэтому любые изменения 3-го примера ZOI в п. 6.1.3 должны вноситься в поле искажения, но не в DCzoi, и добавляться в $Pzoi^2$ (Последние 9 строк в таблице 75).

Таблица 75 – Связывание поля искажения с двумя сегментами данных (расширение 3-го примера ZOI в п. 6.1.3)

Параметр			Размер (биты)	Значения (по порядку)	Производное значение (смысл)
NZzoi			8 (RBAS)	1	Число Зон равно 1
Зона^0	DCzoi		1	0_b	Далее не следует сегмент, выровненный по байтам
			1	1_b	Класс описания, несвязанный с изображением
			6	010001_b	Определены байтовые диапазоны после маркера SOD, а также связанные поля искажения
	$Pzoi^2$	$Mzoi^2$	1	0_b	Далее не следует сегмент, выровненный по байтам
			1	0_b	На указанные зоны оказывает влияние инструмент JPSEC
			1	1_b	Определено много элементов
			2	01_b	Режим диапазона
			2	01_b	Izoi использует 16-битное целое число
			1	0_b	Izoi описывается в одном измерении

Таблица 75 – Связывание поля искажения с двумя сегментами данных (расширение 3-го примера ZOI в п. 6.1.3)

Параметр			Размер (биты)	Значения (по порядку)	Производное значение (смысл)
		$Nzoi^{2}$	8 (RBAS)	2	Число сегментов данных равно 2
		$Izoi^{2,1}$	16	0000 0000 0000 1010_b	Позиция начального байта – 10-я (байты)
			16	0000 0000 0110 0100_b	Позиция конечного байта – 100-я (байты)
Зона^{0}	$Pzoi^{2}$	$Izoi^{2,2}$	16	0010 0111 0001 0000_b	Позиция начального байта – 10 000-я (байты)
			16	0010 1110 1110 0000_b	Позиция конечного байта – 12 000-я (байты)
	$Pzoi^{6}$	$Mzoi^{6}$	1	0_b	Далее не следует сегмент, выровненный по байтам
			1	0_b	На указанные зоны оказывает влияние инструмент JPSEC
			1	1_b	Определено много элементов
			2	10_b	Режим указателя
			2	00_b	Izoi использует 8 битов для представления каждого значения искажения
			1	0_b	Izoi описывается в одном измерении
		$Nzoi^{6}$	8 (RBAS)	2	Число сегментов данных равно 2
		$Izoi^{6,1}$	8	Значение D1	Значение искажения для первого сегмента
		$Izoi^{6,2}$	8	Значение D2	Значение искажения для второго сегмента

6.4.2 Пример 2

В данном примере описывается, как значения искажения могут быть связаны с пакетами JPEG 2000. DCzoi определяет диапазон из 4 пакетов, также сигнализируется о поле искажений. $Pzoi^{1}$ задает диапазон пакетов, а $Pzoi^{2}$ описывает искажение, связанное с каждым из этих пакетов. Следует обратить внимание на то, что, поскольку $Pzoi^{1}$ определяет диапазон длиной 4, а $Pzoi^{2}$ определяет 4 значения, каждый элемент диапазона связан с одним значением, например, каждый пакет связан с одним искажением.

Таблица 76 – Сигнализация диапазона пакетов и связывание искажений с каждым пакетом

Параметр			Размер (биты)	Значение (по порядку)	Производное значение (смысл)
NZzoi			8 (RBAS)	1	Число Зон равно 1
Зона^{0}	DCzoi		1	0_b	Далее не следует сегмент, выровненный по байтам
			1	1_b	Класс описания, несвязанный с изображением
			6	100001_b	Определены пакеты и связанные поля искажений
	$Pzoi^{1}$	$Mzoi^{1}$	1	0_b	Далее не следует сегмент, выровненный по байтам
			1	0_b	На указанные зоны оказывает влияние инструмент JPSEC
			1	0_b	Определен один элемент
			2	01_b	Режим диапазона
			2	00_b	Izoi использует 8-битное целое число
			1	0_b	Izoi описывается в одном измерении
		$Nzoi^{1}$	8 (RBAS)	1	Число сегментов данных равно 1
		$Izoi^{11}$	8	$0000\ 0000_b$	Начальный пакет имеет номер 0
			8	$0000\ 0011_b$	Конечный пакет имеет номер 3

Таблица 76 – Сигнализация диапазона пакетов и связывание искажений с каждым пакетом

Параметр			Размер (биты)	Значение (по порядку)	Производное значение (смысл)
	Pzoi[6]	Mzoi[6]	1	0_b	Далее не следует сегмент, выровненный по байтам
			1	0_b	На указанные зоны оказывает влияние инструмент JPSEC
			1	1_b	Определено много элементов
			2	10_b	Режим указателя
			2	00_b	Izoi использует 8 битов для представления каждого значения искажения
			1	0_b	Izoi описывается в одном измерении
		Nzoi[6]	8 (RBAS)	4	Число сегментов данных равно 4
		Izoi[6,1]	8	Значение D1	Значение искажения для первого пакета
		Izoi[6,2]	8	Значение D2	Значение искажения для второго пакета
		Izoi[6,3]	8	Значение D3	Значение искажения для третьего пакета
		Izoi[6,4]	8	Значение D4	Значение искажения для четвертого пакета

7 Орган регистрации JPSEC

7.1 Общая информация

Механизм регистрации JPSEC предусматривает однозначную идентификацию ненормативных инструментов безопасности, соответствующих стандарту JPSEC, которые можно далее предложить или развить как ненормативные инструменты JPSEC, в добавление к ненормативным инструментам JPSEC , перечисленным в Приложении B. Данная регистрация выполняется Органом регистрации JPSEC и должна соответствовать Директивам JTC 1. Управление процессом регистрации данных новых инструментов JPSEC осуществляется при помощи процесса, определенного в данном подпункте.

Заявители могут представлять на рассмотрение технологии, которые, по их мнению, необходимо включить в список ссылок JPSEC. Отметим, что использование инструмента JPSEC определяется при помощи маркера JPSEC, присутствующего в кодовом потоке. Когда приложение обнаруживает новый ID JPSEC, оно может связаться с RA JPSEC и получить зарегистрированную информацию о данном инструменте.

7.2 Критерии пригодности заявителей для регистрации

Подходящими заявителями являются организации, признаваемые национальными организациями.

7.3 Заявки на регистрацию

Орган регистрации JPSEC должен публиковать заявки на регистрацию новых инструментов JPSEC на сайте в интернете.

Интернет-сайт должен содержать формы для Заявления на регистрацию, Запроса на обновление, Уведомления о присвоении или модернизации, а также Отклонения заявки.

Все формы должны включать в себя:

- название организации – заявителя;
- адрес организации – заявителя;
- имя, звание, почтовый/электронный адрес, номер телефона/факса контактного лица в организации.

Формы Заявки на регистрацию и Запроса на обновление должны также включать следующие пункты:

- Название инструмента JPSEC (обязательно).
- Тип инструмента JPSEC, например, цифровая подпись, "водяной знак", шифрование, скремблирование, генерирование ключа и управление им, аутентификация (необязательно).
- Описательный технический обзор (обязательно).
- Описательный обзор инструмента (обязательно).

- Описание примеров использования и работы (необязательно).
- Спецификацию синтаксиса параметров, включая возможные значения (необязательно).
- Рекомендации по оптимальному использованию (необязательно).
- Статус IPR, например, владелец, правообладатель (необязательно).
- Условия IPR для использования (обязательно).
- Ограничения использования, например, условия экспорта (необязательно).
- Информацию по загрузке реализаций (необязательно).
- Дополнительные комментарии, мотивировки, ссылки и т. д. (необязательно).
- Требования конфиденциальности отдельных пунктов заявки (необязательно).
- Запрашиваемое время для регистрации инструмента (необязательно).

Орган регистрации JPSEC должен предоставлять заявителям справочный материал в помощь при подготовке заявок.

7.4 Рассмотрение заявки и ответ на нее

Для обеспечения беспристрастности в данном подпункте описывается процесс рассмотрения заявки Органом регистрации JPSEC и предоставление ответа на нее.

Для рассмотрения заявок была создана комиссия по техническому рассмотрению. Данная комиссия состоит из членов ИСО/МЭК JTC 1/SC 29/WG 1 и Органа регистрации JPSEC. Комиссия по рассмотрению изучает заявки на заседании WG 1 в срок не позднее 9 месяцев с момента подачи заявки.

Комиссия по рассмотрению принимает или отклоняет заявку, основываясь на критериях отказа, описанных в п. 7.5.

Если заявка принимается, новому инструменту JPSEC на указанный период времени присваивается идентификатор (ID). Синтаксис ID должен соответствовать п. 5.6.3. Комиссия по рассмотрению утверждает информацию по описанию инструмента JPSEC, приведенную в п. 7.3. Затем ID необходимо использовать для сигнализации в кодовом потоке JPSEC.

После рассмотрения и принятия заявки RA JPSEC уведомляет заявителя о положительном или отрицательном ответе на запрос регистрации. Ответ заявителю должен включать краткое объяснение результатов технического рассмотрения. Ответ должен быть отослан заявителям не позднее чем через 9 месяцев с момента подачи заявки.

Отрицательный ответ можно опротестовать, если лицо, подающее заявку на регистрацию, считает, что при отказе была совершена ошибка, или когда требуется более подробная информация для разъяснения некоторых пунктов или вопросов. Если лицо, подающее заявку, требует дополнительного рассмотрения вне процесса Органа регистрации, он может подать на рассмотрение комиссией WG 1 в большем составе на следующем заседании группы WG 1. Затем по запросу экспертов его могут попросить предоставить дополнительную информацию. Эксперты, под руководством WG 1, предоставят окончательный решающий положительный или отрицательный ответ. Для пересмотра отклоненной заявки группой WG 1, лица, подающие заявку, должны заново подать ее через Национальную Организацию, указав причину, по которой требуется рассмотрение заявки группой WG 1.

7.5 Отклонение заявок

Критериями отклонения заявки являются следующие:

- заявитель не является подходящим;
- не были выплачены необходимые взносы (когда это существенно);
- уже существует утвержденный зарегистрированный элемент, содержание которого идентично содержанию заявки;
- информация в заявке неполная или непонятная;
- доводы для включения в перечень неадекватны. Инструмент JPSEC-претендент должен продемонстрировать, что он оказывает полезную услугу безопасности, и предоставить примеры использования, когда он является существенным;
- Орган решил, что предложенный инструмент не достаточно оригинален, и его можно реализовать, используя существующий утвержденный элемент;
- заявка содержит ошибки или не соответствует нормативным спецификациям или стандарту JPSEC;
- техническое описание не является исчерпывающим;
- условия конфиденциальности не являются соответствующими.

7.6 Присвоение идентификаторов и запись определений объектов

Процесс рассмотрения и вышеописанный синтаксис гарантируют, что присвоенный ID является уникальным для данного перечня, и что такой же ID не присвоен другому объекту.

После выполнения присваивания, ID и связанная информация должны быть включены в перечень, и Орган регистрации JPSEC должен проинформировать заявителя об этом присвоении в течение 9 месяцев.

Определение инструмента JPSEC должно быть записано в перечне при присвоении ID.

7.6.1 Повторное использование ID

Орган регистрации может повторно использовать идентификаторы. Например, идентификаторы можно повторно использовать после истечения срока их действия, или когда их прекращают использовать естественным образом или исправляют.

Владельцы ID могут по своему желанию прекратить использовать свой ID при помощи Запроса на обновление.

7.6.2 Исправление

Орган регистрации JPSEC может исправить идентификатор по техническим причинам или из-за неправильного использования инструмента. В таком случае владельцы будут осведомлены об этом при помощи Уведомления об обновлении.

7.7 Техническое обслуживание

С целью технической поддержки перечня Орган регистрации JPSEC должен реализовывать механизмы по поддержанию целостности перечня, включая соответствующее резервное копирование для сохранения записей.

Владелец ID может обновлять связанную информацию об инструменте JPSEC посредством Запроса на обновление.

Орган регистрации JPSEC должен предоставить механизмы для поддержания конфиденциальности записей, указанных в заявке.

7.8 Публикация перечня

Как правило, интересы сообщества пользователей информационными технологиями удовлетворяются наилучшим образом, если информация перечня становится общедоступной. В определенных случаях, однако, может появиться потребность в конфиденциальности всех или части данных, имеющих отношение к определенной регистрации, полностью или в некоторой части процесса регистрации.

Орган регистрации JPSEC должен публиковать информацию о регистрации так, чтобы она соответствовала требованиям конфиденциальности инструмента JPSEC.

В случаях, когда требуется публикация, обязательно наличие электронной версии, и версии, отпечатанной на бумаге. Если публикацию должен выполнить Орган регистрации JPSEC, он должен вести точные записи распределения, относящиеся к своим публикациям.

7.9 Требования информации перечня

Орган регистрации JPSEC должен публиковать в электронном виде список ненормативных инструментов JPSEC из своего перечня, а также информацию, связанную с ними, удовлетворяя, при этом, требованиям конфиденциальности инструмента JPSEC.

Для каждого инструмента JPSEC в перечне должна содержаться следующая информация:

- присвоенный ID;
- имя первого заявителя;
- адрес первого заявителя;
- дата первоначального присвоения;
- дата последнего повторного присвоения, если разрешено (обновляемый);
- имя текущего владельца (обновляемый);
- адрес текущего владельца (обновляемый);
- фамилия, звание, почтовый/электронный адрес, номер телефона/факса контактного лица в организации (обновляемый);
- дата последнего обновления (обновляемый).

Здесь также должна содержаться информация, предоставляемая заявителем инструмента JPSEC, которая определена в п. 7.3, а также информация об утверждении.

Приложение A

Рекомендации и случаи использования

(Данное приложение является неотъемлемой частью данной Рекомендации | Международного стандарта)

A.1 Класс приложений JPSEC

A.1.1 Введение

В данном подпункте дается схематическое описание того, как можно реализовывать класс приложений JPSEC. Для данного класса приложений приводятся примеры сценариев защищенного распространения изображения JPEG 2000. В нижеследующих подпунктах приводится обзор схематического приложения JPSEC, включая объекты JPSEC и информацию, которой они обмениваются. Данное описание является схематическим и ни в коей мере не определяет какую-либо конкретную реализацию, а также не устанавливает требования к какой-либо реализации; отдельные реализации могут включать или не включать объекты, упоминающиеся в нижеследующем описании.

A.1.2 Обзор защищенного распространения изображений JPEG 2000

На рисунке A.1 приводится обзор класса приложений JPSEC при защищенном распространении изображений JPEG 2000. В данных приложениях, может потребоваться, чтобы приложение JPSEC оказывало различные услуги безопасности для JPEG 2000, например, конфиденциальность обмена изображениями, аутентификация источника и содержания изображений.

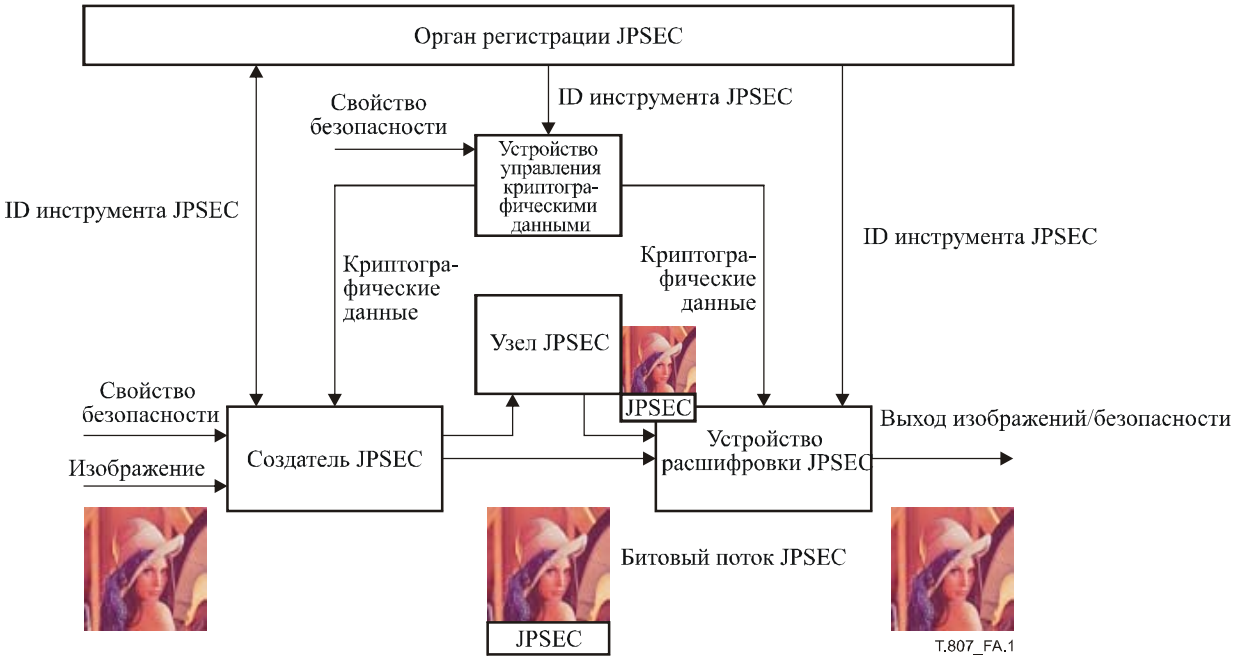


Рисунок A.1 – Обзор приложения защищенного распространения изображения JPEG 2000

При реализации приложения по защищенному распространению изображения JPEG 2000 можно выделить следующие этапы:

Этап 1: Создатель JPSEC создает кодовый поток JPSEC.

Этап 2: Кодовый поток JPSEC распространяется через узел или узлы JPSEC.

Этап 3: Происходит получение кодового потока JPSEC и визуализация его потребителем JPSEC.

Этап 1: Создание кодового потока JPSEC

За создание защищенного кодового потока JPEG 2000 отвечает создатель. Кодовый поток можно сформировать из данных битового отображения графического объекта или из сжатых данных JPEG 2000. Создатель JPSEC применяет к данным изображения различные методы безопасности такие, как шифрование, генерирование подписи и ICV (Значение проверки целостности).

Для обеспечения безопасности данных изображения создатель определяет, какое Свойство параметра безопасности связано с изображением. "Свойство параметра безопасности" включает в себя следующие атрибуты:

- Зону влияния (область охвата каждого метода защиты);
- Область обработки (область, которую будет обрабатывать каждый метод защиты);
- Степень структурирования (единица каждого метода защиты);
- Идентификацию инструмента JPSEC (применяемый криптографический алгоритм и смежные параметры).

Этап 2: Доставка кодового потока JPSEC

Кодовый поток JPSEC может быть передан потребителю JPSEC напрямую через сеть или носители данных (такие, как CD-ROM). Также кодовый поток можно передать через узел JPSEC, который может выполнять различные типы дополнительной обработки кодового потока JPSEC, такие как перекодировка.

Если того требуют методы инструмента безопасности JPSEC в Параметре свойства безопасности кодового потока JPSEC (например, для шифрования или для аутентификации), создатель JPSEC должен распространить соответствующие криптографические данные по независимому ("секретному") каналу потребителю JPSEC. Этими данными такими, как ключ или цифровая подпись, можно управлять либо вручную, либо автоматически при помощи программа управления криптографическими данными.

Этап 3: Визуализация кодового потока JPSEC потребителем

Кодовый поток JPSEC обрабатывается потребителем JPSEC в соответствии с применяемым свойством Параметра безопасности: это подразумевает применение соответствующих методов безопасности таких, как расшифровка, аутентификация и проверка целостности. Кроме того, для каждого метода безопасности инструмента JPSEC создатель JPSEC и потребитель JPSEC могут использовать различные типы криптографических данных.

В результате потребитель JPSEC получает расшифрованные данные изображения и/или выходные данные безопасности такие, как результат проверки подлинности.

Создатель JPSEC, потребитель JPSEC и программа управления криптографическими данными могут обращаться к Органу регистрации JPSEC для получения необходимых рекомендаций по обработке определенного ID инструмента JPSEC.

В нижеследующих подпунктах приводится дополнительная информация о схематическом объекте JPSEC в соответствии с услугой JPSEC. На рисунке A.2 изображена легенда используемого описания.

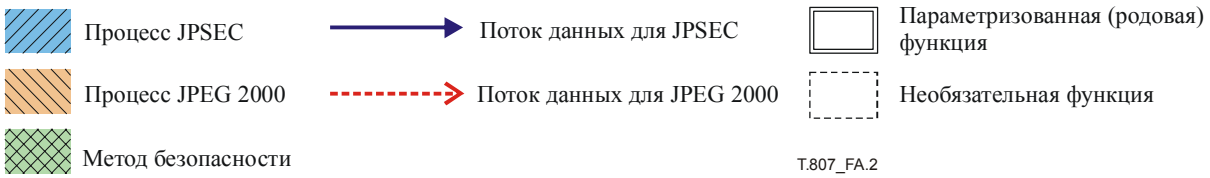


Рисунок A.2 – Описание легенды

- **Процесс JPSEC**: Процесс, использующий инструменты, определенные в данной Рекомендации | Международном стандарте.
- **Процесс JPEG 2000**: Процесс, определенный в Рек. МСЭ-Т Т.800 | ИСО/МЭК 15444-1 (Часть 1 JPEG 2000).
- **Метод безопасности**: Хорошо известный метод обеспечения безопасности, определенный либо в данной Рекомендации | Международном стандарте, либо в каком-либо другом стандарте или документе.
- **Поток данных для JPSEC**: Поток данных, передающий информацию, определенную в данной Рекомендации | Международном стандарте. Пунктирная линия означает, что он не является обязательным.
- **Поток данных для JPEG 2000**: Поток данных, определенный в Рек. МСЭ-Т Т.800 | ИСО/МЭК 15444-1 (Часть 1 JPEG 2000).
- **Параметризованная (родовая) функция**: Функция, которая имеет несколько переменных функций, которые может выбирать приложение.
- **Необязательная функция**: Функция, которую не обязательно применять в приложении JPSEC.

A.1.3 Процедура шифрования и расшифровки

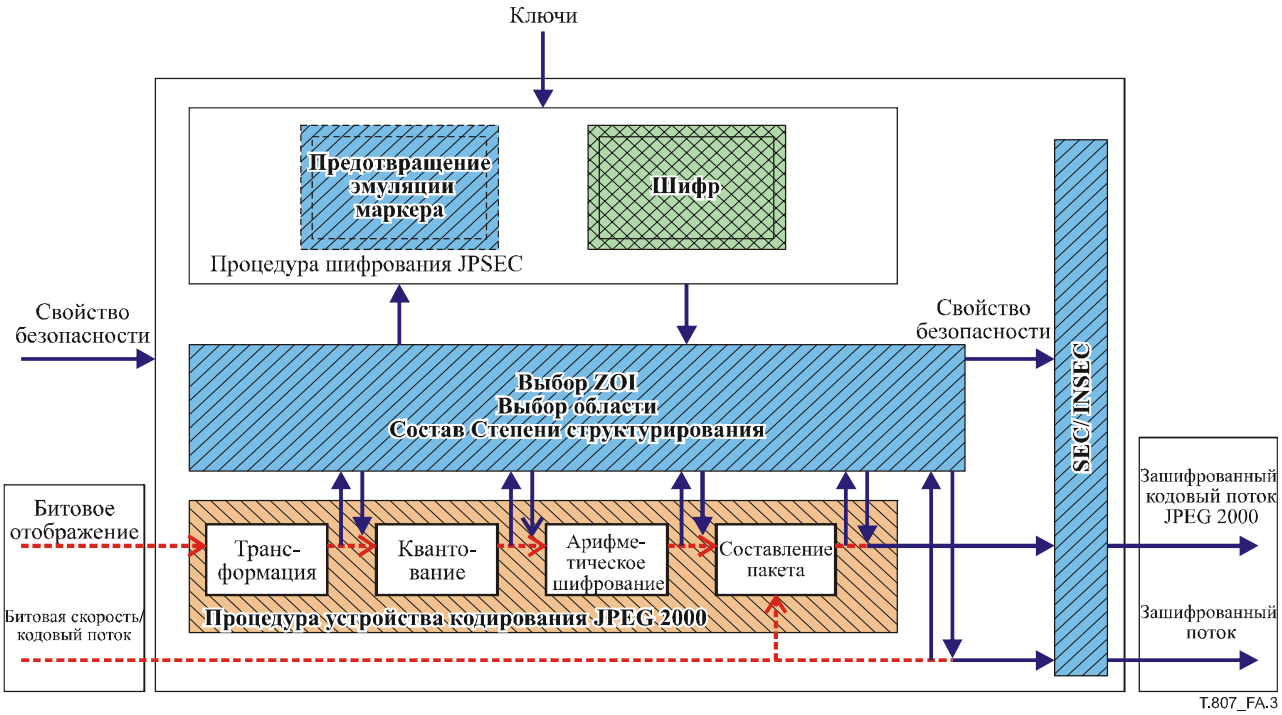


Рисунок A.3 – Процедура шифрования

На рисунке A.3 изображен пример процедуры шифрования для создателя JPSEC. Данная процедура включает в себя следующие процессы:

- извлечение данных в соответствии с указанной Областью обработки;
- выбор части извлеченных данных в соответствии с Зоной влияния (т. е. частичное шифрование);
- зашифровывание выбранных данных при помощи указанного метода. Кроме того, можно зашифровать данные в единице, основанной на Степени структурирования. В таком случае для различных единиц можно использовать различные ключи;
- замена незашифрованных данных зашифрованными данными;
- (необязательно) применение механизма, предотвращающего эмуляцию маркера;
- вставка Свойства параметра безопасности в сегмент маркера SEC и/или INSEC.

Отметим, что, как правило, в результате процедуры шифрования JPSEC генерируется кодовый поток JPSEC, который не является обратно совместимым с Частью 1 JPEG 2000. То, что данные изображения будут проходить через устройство расшифровки, совместимое с Частью 1 после соответствующей расшифровки, не предполагается. Для предотвращения эмуляции сегмента маркера в зашифрованном кодовом потоке можно применять механизм предотвращения эмуляции маркера.

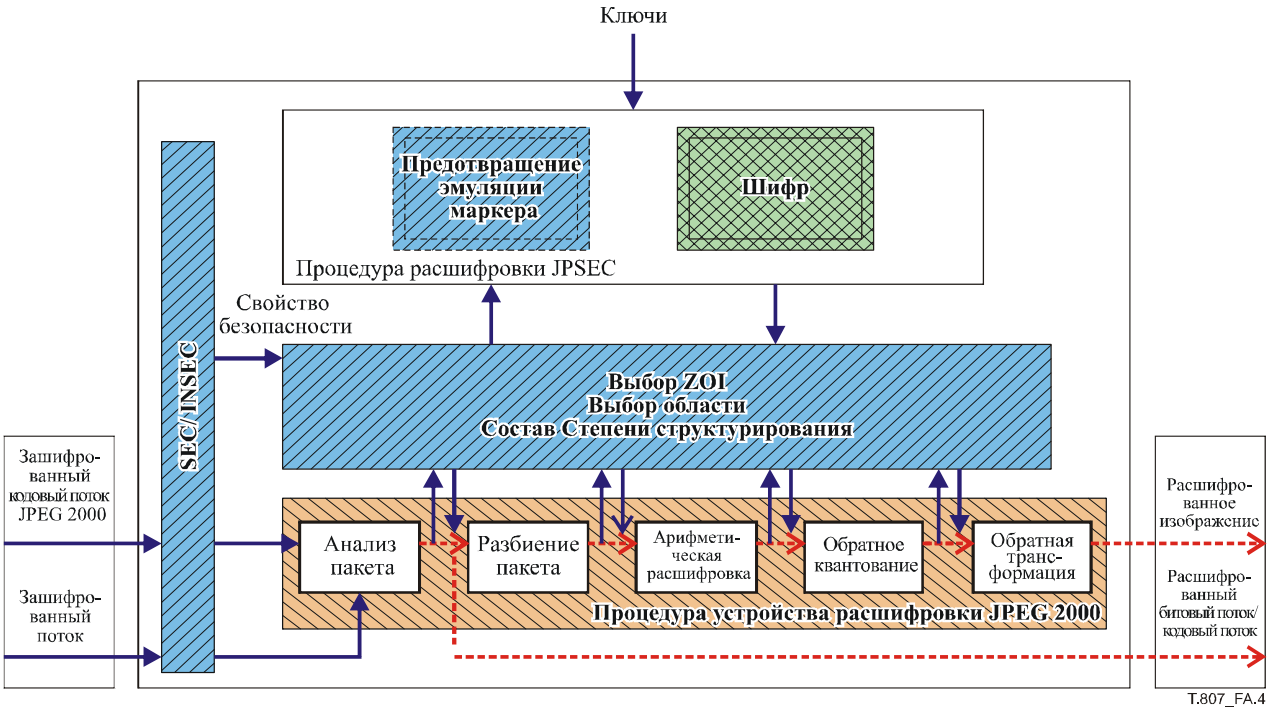


Рисунок А.4 – Процедура расшифровки

На рисунке А.4 изображен пример процедуры расшифровки для потребителя JPSEC. Данная процедура включает в себя следующие процессы:

- анализ Свойства параметра безопасности в сегменте маркера SEC и/или INSEC;
- извлечение данных в соответствии с указанной Областью обработки;
- выбор части извлеченных данных в соответствии с ключами, предназначенными для сохранения (т. е. частичная расшифровка);
- расшифровка выбранных данных при помощи указанного метода безопасности. Кроме того, можно расшифровать данные в единице на основе Степени структурирования;
- замена зашифрованных данных расшифрованными данными;
- применение механизма по предотвращению эмуляции маркера, если он применялся в процессе зашифровывания.

A.1.4 Генерирование подписи и процедура аутентификации

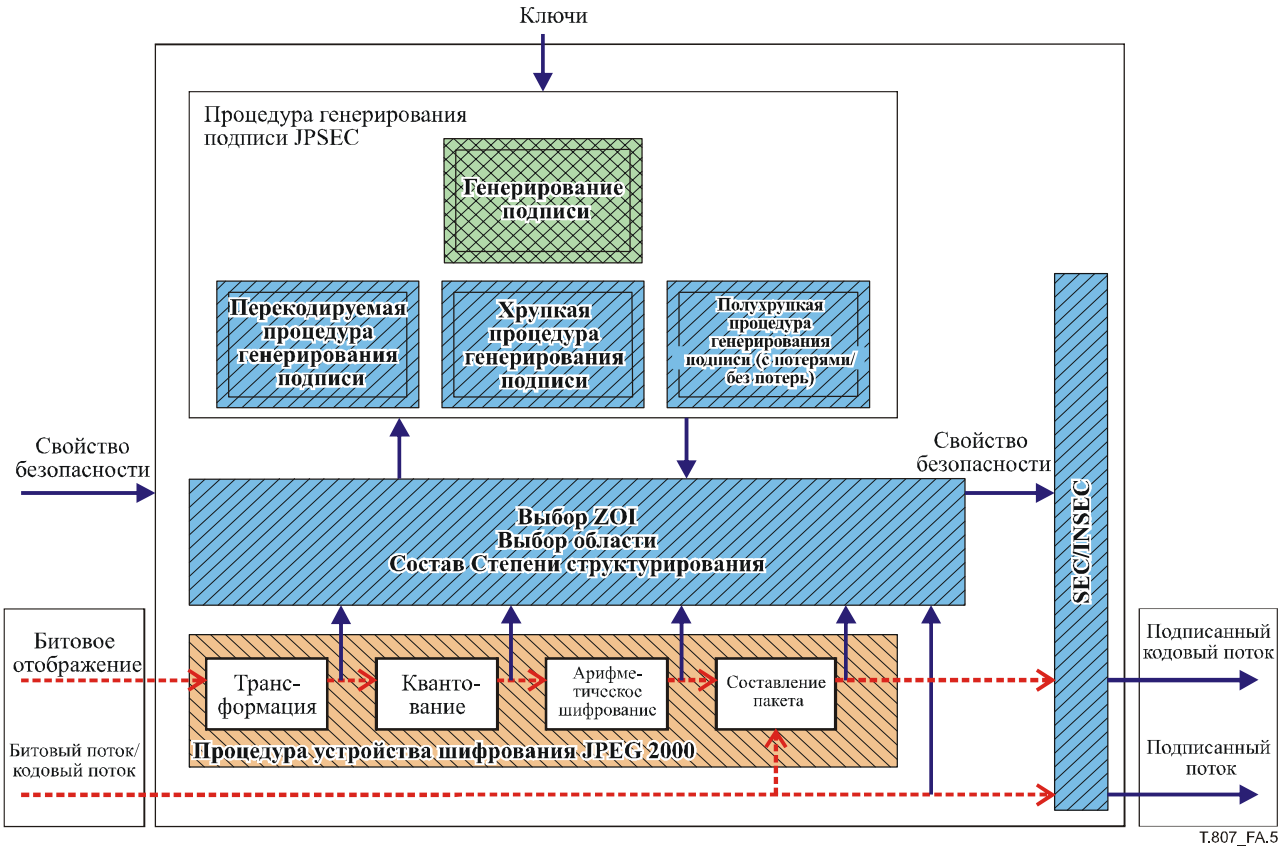


Рисунок A.5 – Процедура генерирования подписи

На рисунке A.5 изображен пример процедуры генерирования подписи для создателя JPSEC. Данная процедура включает в себя следующие процессы:

- извлечение данных в соответствии с указанной Областью обработки;
- выбор части извлеченных данных в соответствии с указанной Зоной влияния (т. е. частичная подпись);
- вычисление цифровых подписей, соответствующих выбранным данным, при помощи указанного метода безопасности. Кроме того, можно генерировать цифровые подписи в единице на основе Степени структурирования;
- вставка Свойства параметра безопасности, включая вычисленные цифровые подписи, в сегмент маркера SEC и/или INSEC.

Отметим, что в JPSEC определяются три режима аутентификации: "хрупкий режим", "полухрупкий режим (с потерями/без потерь)" и "режим перекодировки". Аутентификация "хрупкий режим" может обнаружить любое однобитовое изменение кодового потока, в то время как аутентификация "полухрупкий режим" может обнаружить любое намеренное изменение, но пропустить случайное искажение в заранее определенной степени. Аутентификация "режим перекодировки" может подтвердить подлинность части источника кодового потока.

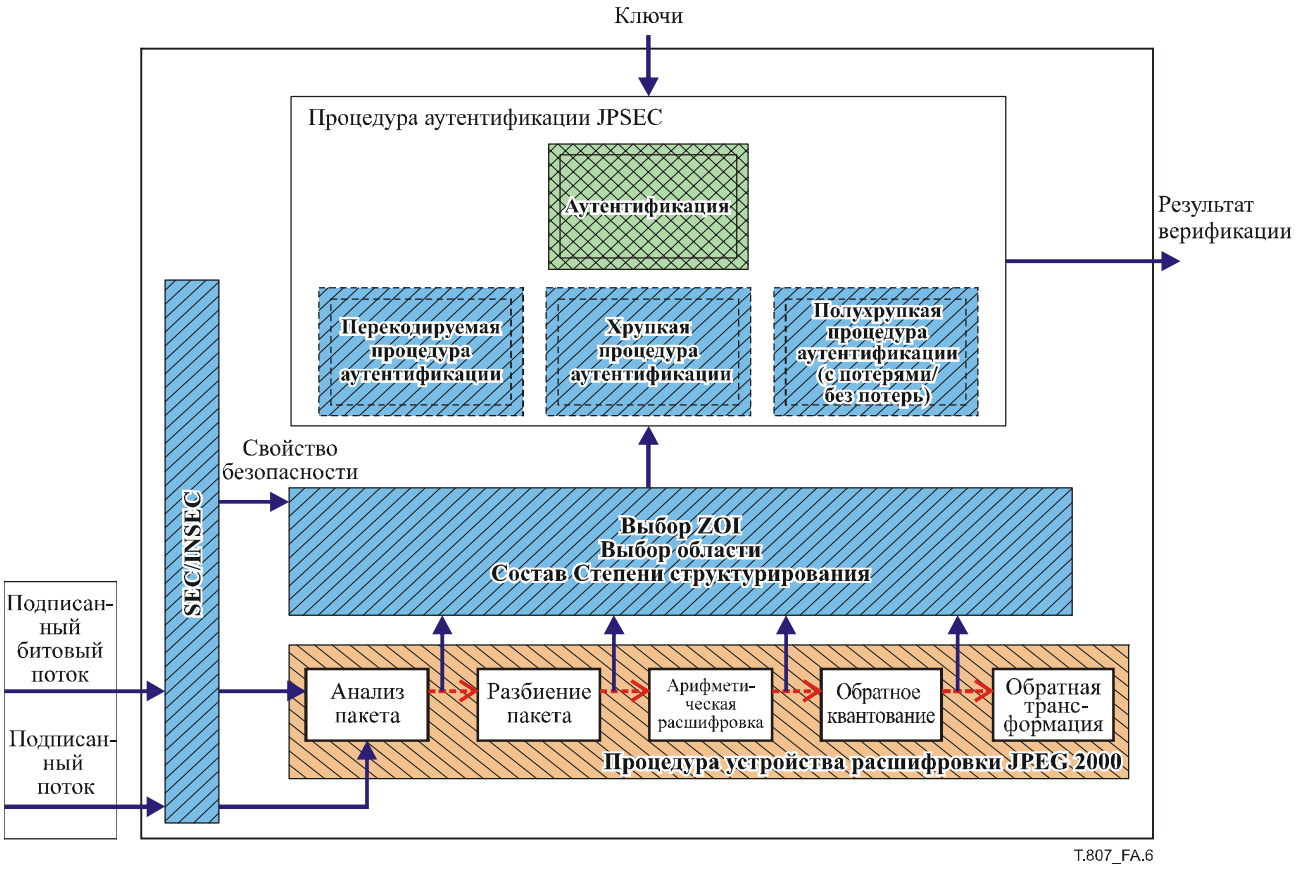


Рисунок А.6 – Процедура аутентификации

На рисунке А.6 изображен пример процедуры аутентификации для потребителя JPSEC. Данная процедура включает в себя следующие процессы:

- извлечение данных в указанной Области обработки;
- выбор части извлеченных данных в соответствии с указанной Зоной влияния;
- проверка подлинности выбранных данных при помощи указанного метода безопасности. Кроме того, можно проверить подлинность выбранных данных в единице на основе Степени структурирования.

A.1.5 Генерирование ICV (Значение проверки целостности) и процедура проверки целостности

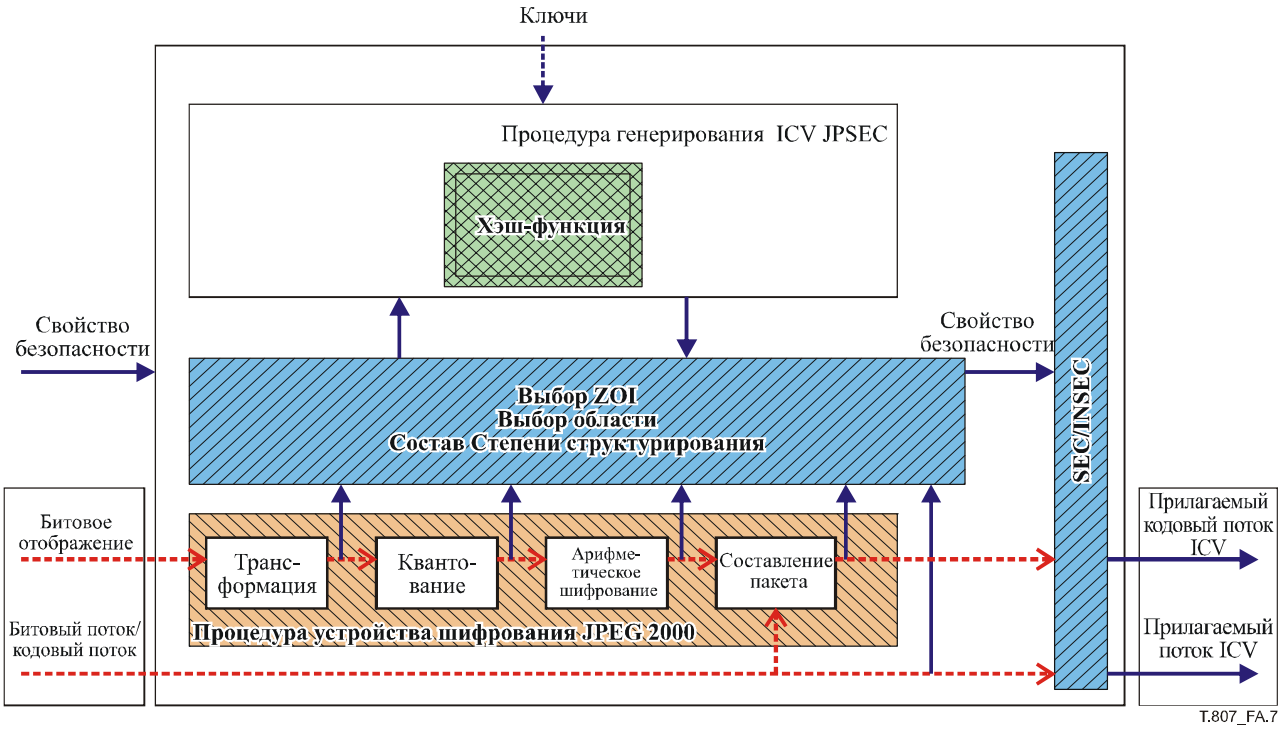


Рисунок A.7 – Процедура генерирования ICV (Значение проверки целостности)

На рисунке A.7 изображен пример процедуры генерирования ICV для создателя JPSEC. Данная процедура включает в себя следующие процессы:

- извлечение данных в указанной Области обработки;
- выбор части извлеченных данных в соответствии с указанной Зоной влияния;
- вычисление ICV, соответствующих выбранным данным, при помощи указанного метода безопасности. Кроме того, можно генерировать ICV в единице на основе Степени структурирования;
- вставка Свойства параметра безопасности, включая вычисленные ICV, в сегмент маркера SEC и/или INSEC.

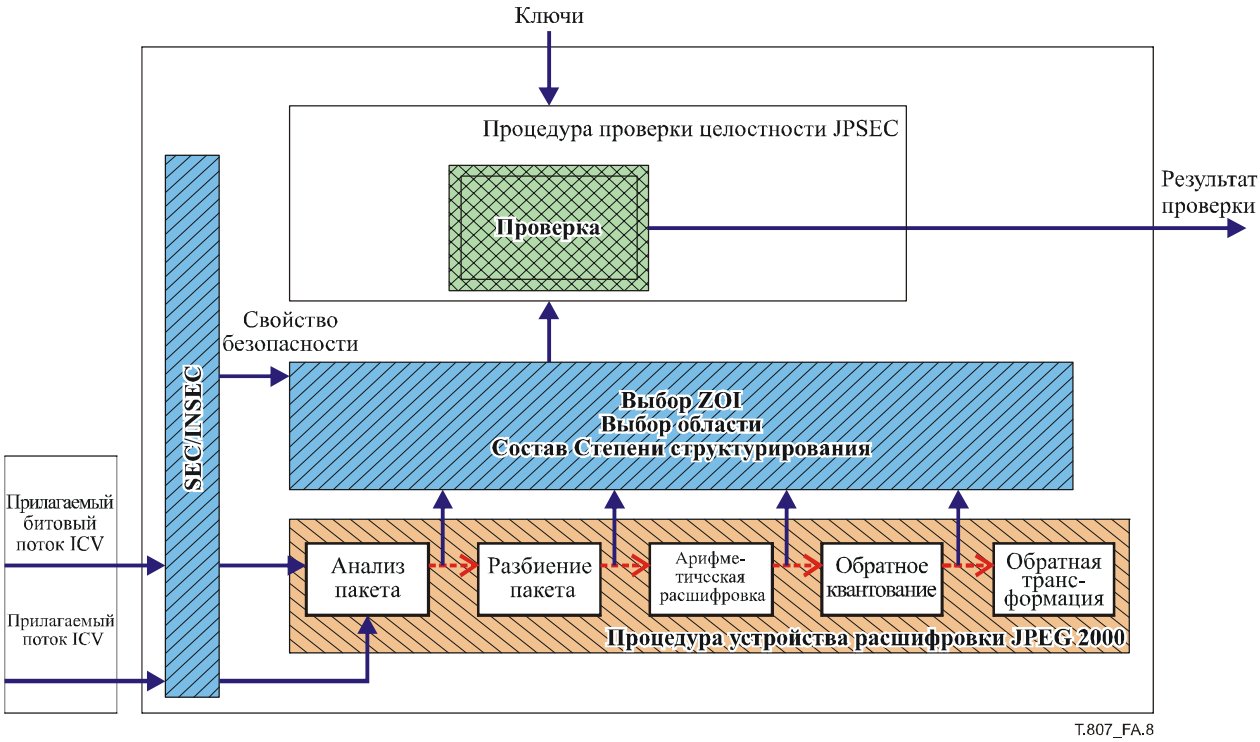


Рисунок A.8 – Процедура проверки целостности

На рисунке A.8 изображен пример процедуры проверки целостности для потребителя JPSEC. Данная процедура включает в себя следующие процессы:

- извлечение данных в соответствии с указанной Областью обработки;
- выбор части извлеченных данных в соответствии с указанной Зоной влияния;
- проверка подлинности выбранных данных при помощи указанного метода безопасности. Кроме того, можно проверить подлинность выбранных данных в единице на основе Степени структурирования.

Приложение B

Технологические примеры

(Данное приложение является неотъемлемой частью данной Рекомендации | Международного стандарта)

B.1 Введение

Синтаксис JPSEC позволяет применять нормативные и ненормативные инструменты безопасности к изображениям JPEG 2000. В данном подпункте приводится десять информативных технологических примеров, демонстрирующих различные варианты использования JPSEC. Данные примеры являются только информативными и не подтверждены стандартом JPSEC. Однако они предоставляются для демонстрации гибкости стандарта.

К технологическим примерам относятся:

- Гибкая схема управления доступом для JPEG 2000;
- Унифицированная структура аутентификации для изображений JPEG 2000;
- Простой метод шифрования на основе пакетов для кодовых потоков JPEG 2000;
- Инструмент шифрования для управления доступом JPEG 2000;
- Инструмент генерирования ключа для управления доступом JPEG 2000;
- Скремблирование вейвлет-области и битового потока для условного управления доступом;
- Прогрессивный доступ для кодового потока JPEG 2000;
- Масштабируемая подлинность кодовых потоков JPEG 2000;
- Конфиденциальность данных JPEG 2000 и система управления доступом на основе разделения данных и создания "приманки";
- Защищенная масштабируемая потоковая передача данных и защищенная перекодировка.

B.2 Гибкая схема управления доступом для кодовых потоков JPEG 2000

B.2.1 Услуга безопасности

Схема управления доступом позволяет визуализировать кодовые потоки JPEG 2000 в соответствии с любым сочетанием разрешений, слоев качества, элементов изображения и границ.

B.2.2 Типичное применение

Данная схема обеспечивает защиту поставки содержания через различные передающие среды, например, интернет, цифровое кабельное ТВ, спутниковое вещание и CD-ROM. Как правило, технология поддерживает приложения, где кодовый поток зашифровывается только один раз со стороны издателя, но защищенный кодовый поток расшифровывается много раз в соответствии с различными правами доступа пользователя.

B.2.3 Мотивировка

В модели Супер-распространение издатель свободно распространяет защищенное содержание, а ключи содержания распространяются защищенным образом. Пользователь, желающий получить доступ к части кодового потока посылает свой запрос на сервер ключей. Сервер ключей, в свою очередь, высылает в ответ соответствующие ключи для расшифровки в соответствии с правами доступа пользователя. Пользователь может получить доступ к разрешенным подизображениям (субизображениям).

B.2.4 Технический обзор

Издатель создает защищенный кодовый поток JPEG 2000 путем зашифровывания каждого пакета. Основой данной технологии является управление деревом ключей, которое состоит из элементов изображения, компонентов, разрешений, слоев, границ и даже блоков кода в любом порядке. Для того чтобы с легкостью описать данную технологию, предположим, что порядок дерева ключей – RLCP (разрешение – слой – компонент – граница), а каждое разрешение имеет одинаковое число границ. Далее, приняв значение однонаправленной хэш-функции за h(.), рассмотрим кодовый поток изображения JPEG 2000 с n_T элементов изображения, n_C компонентов, n_L слоев, n_R разрешений на элемент изображения-компонент, n_P границ на разрешение. Для кодового потока JPEG 2000 главный ключ K. Сконструируем дерево ключей следующим образом.

1) Генерируем ключ $k^t = h(K|"T"|t)$, для каждого элемента изображения $t = 0, 1, \ldots, n_T - 1$, где "|" – это конкатенация, а "*T*" обозначает код ASCII для буквы *T*.

2) Генерируем ключ $k^r = h(k^{r+1})$, для каждого $r = n_R - 2, \ldots, 1, 0$, где $k^{n_R - 1} = h(k^t|"R")$, а "*R*" обозначает код ASCII для буквы *R*.

3) Вычисляем ключ $k^{rl} = h(k^{r(l+1)})$, для каждого $r = n_R - 1, \ldots, 1, 0$, $l = n_L - 2, \ldots, 1, 0$, где $k^{r(n_L - 1)} = h(k^r|"L")$, а "*L*" обозначает код ASCII для буквы *L*.

4) Вычисляем ключ $k^{rlc} = h(k^{rl}|"C"|c)$, для каждого $r = n_R - 1, \ldots, 1, 0$, $l = n_L - 1, \ldots, 1, 0$, $c = 0, 1, \ldots, n_C - 1$, где "*C*" обозначает код ASCII для буквы *C*, а *c* обозначает указатель (индекс) данного компонента.

5) Вычисляем ключи $k^{rlcp} = h(k^{rlc}|"P"|p)$, для каждого $r = n_R - 1, \ldots, 1, 0$, $l = n_L - 1, \ldots, 1, 0$, $c = 0, 1, \ldots, n_C - 1$, $p = 0, 1, \ldots, n_R - 1$, где "*P*" обозначает код ASCII для буквы *P*, а *p* обозначает указатель (индекс) данной границы.

Защищенный кодовый поток получается при зашифровывании каждого тела пакета соответствующим ключом ("лист" дерева ключей).

Для формирования подизображения (субизображения) из защищенного кодового потока, пользователь получает соответствующие ключи доступа (например, с сервера ключей). Данные ключи доступа могут точно восстановить "листья" дерева ключей, соответствующие пакетам запрашиваемого подизображения. Процесс восстановления ключа аналогичен процессу генерирования ключа. "Листья" дерева ключей используются для расшифровки соответствующих пакетов.

B.2.5 Синтаксис кодового потока

В таблице B.1 приводится структура сегмента SEC. Поле ZOI сигнализирует заданные параметры, поле P_{ID} сигнализирует параметры метода защиты для данной схемы управления доступом. Значение поля PM_{ID} всегда устанавливается на 1 и обозначает, что используется шаблон расшифровки. Поле TP_{ID} сигнализирует дополнительные параметры для данной схемы управления доступом. КТО – это порядок генерирования дерева ключей. В поле L_{aki} указывается длина информации о ключе доступа.

Таблица B.1 – Пример параметров для данной схемы

t	i	ID_{RA}	L_{ZOI}	ZOI	L_{PID}	P_{ID}

Параметр		Размер (биты)	Значения	Значение (смысл)
t		8 (FBAS)	1	Инструмент защиты органа регистрации
i		8 (RBAS)	*Значение экземпляра*	Идентификатор экземпляра инструмента
ID_{RA}	$ID_{RA,id}$	32	*Значение ID инструмента*	Зарегистрированный ID
	$ID_{RA,nsl}$	8 (RBAS)	21	Длина $ID_{RA,ns}$ в байтах
	$ID_{RA,ns}$	168	*Пространство имен*	Пространство имен RA, с которым зарегистрирован данный инструмент
L_{ZOI}		16 (RBAS)	$[2 \ldots 2^{16} - 1]$	Длина ZOI
ZOI		Переменный	См. п. 5.7	Зона влияния для данной схемы
L_{PID}		16 (RBAS)	$[2 \ldots 2^{16} - 1]$	Длина L_{PID} + P_{ID}
P_{ID}		Переменный	См. таблицу B.2	Параметры для данной схемы

Таблица B.2 – P_{ID}

$PM_{ID} = 1$	T_{decry}	TP_{ID}

Параметр	Размер (биты)	Значения	Значение (смысл)
$ID_T = 1$	8	Всегда устанавливается на 1	Маркер для шаблона расшифровки
T_{decry}	Переменный	Значения шаблона расшифровки	Шаблон расшифровки
TP_{ID}	Переменный	См. таблицу B.3	Дополнительная информация для данной схемы

Таблица B.3 – TP_{ID}

KTO	L_{aki}	AK_{Info}

Параметр	Размер (биты)	Значения	Значение (смысл)
KTO	8	0 ... (2^8 – 1)	Порядок Дерева ключей. Он может отличаться от порядка продвижения кодового потока, ориентировочно, 0x00: LRCP 0x01: RLCP 0x02: RPCL 0x03: PCRL 0x04: CPRL остальные: зарезервированы
L_{aki}	16	0 ... (2^{16} – 1)	Длина информации о ключе доступа, если L_{aki} = 0, поле AK_{Info} отсутствует
AK_{Info}	Переменный	См. таблицу B.4	Информация о ключе доступа (например, длина ключа, число ключей)

Таблица B.4 – AK_{info}

L_{uk}	UK	E_{ak}	N_{ak}	AK

Параметр	Размер (биты)	Значения	Значение (смысл)
L_{uk}	16	0 ... (2^{16} – 1)	Длина ключа пользователя
UK	L_{uk}	NaN	Информация о ключе пользователя
E_{ak}	16	См. таблицу 24	Шифр, используемый для зашифровывания ключей доступа
N_{ak}	16	0 ... (2^{16} – 1)	Число ключей доступа
AK	N_{ak} * K_{bc}	NaN	Ключи доступа

B.2.6 Заключение

Данная технология позволяет издателю защищать кодовой поток JPEG 2000 при помощи главного ключа. Защищенный кодовый поток можно доставить любому количеству пользователей, однако ключи для пакетов держатся в секрете. Сервер ключей генерирует различные ключи доступа для пользователей в соответствии с их правами доступа. Пользователи генерируют предоставленные ключи пакетов из своих ключей доступа и получают различные изображения. То есть данная технология обладает свойством, которое можно назвать "*зашифровано один раз, доступ множеством способов*".

B.3 Унифицированная структура аутентификации для изображений JPEG 2000

B.3.1 Описание работы

Данный инструмент JPSEC предоставляется следующие услуги JPSEC: проверка целостности данных изображения/содержания и аутентификация источника, т. е. хрупкая/полухрупкая аутентификация для изображений JPEG 2000 на основе схем цифровой подписи.

Поскольку данный инструмент поддерживает как хрупкую, так и полухрупкую аутентификацию, его можно использовать в различных сценариях приложений, включая распространение изображений, потоковую передачу изображений, обработку изображений для медицинских и военных целей, обеспечение правопорядка, электронную коммерцию и электронное правительство.

В среде изображения могут подвергаться различным видам случайных искажений при перекодировке и преобразовании формата. Традиционные методы аутентификации, основанные на криптографии, защищают изображения JPEG 2000 на уровне целостности данных, но не могут предотвратить такие искажения, сохраняющие содержание. Поэтому требуются полухрупкие методы аутентификации для защиты изображений JPEG 2000 на уровне содержания изображения. В данном инструменте объединяются аутентификация данных изображения и аутентификация содержания изображения. Кроме того, предлагается новое понятие, которое называется наименьшая битовая скорость аутентификации (LABR). То есть если перекодировка изображения происходит на битовой скорости, не меньшей, чем LABR, оно будет визуализироваться как подлинное, в противном случае как неподлинное. Данный вид аутентификации может быть хрупкий или полухрупкий. При полухрупкой аутентификации, инструмент может идентифицировать место, где произошло изменение, когда изображение считается неподлинным.

B.3.2 Технический обзор

Для применения хрупкой и полухрупкой аутентификации в данном информативном инструменте JPSEC применяется ряд методов. Они включают в себя выбор характеристики, цифровую подпись, ограничение доступа к данным с потерями и без потерь, а также ECC (коды коррекции ошибок). В соответствии с LABR, указанной пользователями, на основе анализа, применяемого к структуре JPEG 2000, выбираются соответствующие характеристики, а затем генерируется цифровая подпись. При полухрупкой аутентификации для улучшения уровня надежности используется ECC. В изображение в качестве "водяного знака" вставляются биты контроля четности (PCB), он необходимы для выявления мест атаки. Вставку данных можно производить двумя способами: с потерями информации и без потерь. При ограничении доступа к данным с потерями информации, после ограничения доступа к данным восстановить исходное изображение невозможно. При ограничении доступа к данным без потерь информации изображение модифицируется обратимым образом, т. е. исходное изображение можно восстановить при условии, если помеченное изображение не было изменено. Полухрупкая аутентификация без потерь информации полезна для JPEG 2000, поскольку данный стандарт поддерживает сжатие изображения с потерями до изображения без потерь. В частности, это полезно для обработки изображений для медицинских целей и удаленных приложений обработки изображений, где отсутствие потерь является одним из важнейших требований.

Аналогично битовой скорости сжатия изображения, которая используется для управления и измерения силы сжатия, параметр LABR (наименьшая битовая скорость аутентификации) используется для управления силой защиты в количественном отношении. Например, когда защита изображения JPEG 2000 осуществляется при помощи LABR равной 2 bpp (бит на пиксел), любая перекодированная версия данного изображения будет визуализироваться предложенной системой как подлинная, поскольку битовая скорость после перекодировки больше или равна 2 bpp.

На рисунке B.1 показано, как можно использовать данный инструмент для защиты изображений.

Рисунок B.1 – Защита изображения при помощи унифицированной структуры аутентификации для JPEG 2000

Для данного инструмента можно использовать различные синтаксисы сигнализации в зависимости от выбранного метода аутентификации. Для хрупкой аутентификации используется синтаксис нормативного инструмента JPSEC, определенный в п. 5.8.3. Для полухрупкой аутентификации используется синтаксис ненормативного инструмента JPSEC, показанный в таблице B.5. Кроме того, значение F_{INSEC} следует установить на 0, поскольку маркер INSEC этим инструментом не используется, а значение F_{mod} следует установить на 1, поскольку получающийся в результате кодовый поток данного инструмента JPSEC все еще соответствует Части 1 JPEG 2000.

Таблица B.5 – Синтаксис для полухрупкой аутентификации

Параметр		Размер (биты)	Значение	Производное значение (смысл)
t		8 (FBAS)	1	Используется синтаксис ненормативного инструмента
i		8 (RBAS)	0 ... (2^7 – 1)	Указатель (индекс) экземпляра инструмента
ID_{RA}	$ID_{RA,id}$	32	0 ... (2^{32} – 1)	Номер ID присвоенный RA
	$ID_{RA,nsl}$	8 (RBAS)	21	Длина $ID_{RA,ns}$ в байтах
	$ID_{RA,ns}$	168	*Пространство имен*	Пространство имен RA, в котором зарегистрирован данный инструмент

Таблица B.5 – Синтаксис для полухрупкой аутентификации

Параметр				Размер (биты)	Значение	Производное значение (смысл)
$0L_{ZOI}$				16 (RBAS)	0 ... (2^{16} – 1)	Длина ZOI
ZOI				Переменный	*Значения ZOI*	Зона охвата в изображении, защищаемом данным инструментом
L_{PID}				16 (RBAS)	0 ... (2^{16} – 1)	Длина P_{ID} и L_{PID} в байтах
P_{ID}	ID_T			8	2	Шаблон аутентификации используется, как определено в таблице 21
	T_{auth}	M_{auth}		8	2	Метод цифровой подписи используется, как определено в таблице 34
		P_{auth}	M_{DS}	8	См. таблицу 41	Используется алгоритм цифровой подписи такой, как DSA или RSA
			H_{DS}	8	См. таблицу 37	Используется хэш-функция
			KT_{DS}	Переменный	*Значения шаблона ключей*	Открытый ключ хранится в KT_{DS}. Данный инструмент использует только один открытый ключ
			SIZ_{DS}	16	0 ... (2^{16} – 1)	Размер цифровой подписи в байтах
P_{ID}	PD			1	0_b	Структура FBAS завершается
				1	0_b	Область пикселов не используется
				1	0_b	Область вейвлет-коэффициента не используется
				1	1_b	Область квантованного вейвлет-коэффициента используется
				1	0_b	Область кодового потока не используется
				3	000_b	Зарезервировано для использования ИСО
	G	PO		16	*Значения порядка обработки*	Порядок обработки
		GL		8	0000 1001	Уровень Степени структурирования: Единицей защиты является вся область, указанная в ZOI
	V	N_V		16	1	Число цифровых подписей в списке равно 1
		S_V		8 (RBAS)	1 ... (2^8 – 1)	Размер цифровой подписи в байтах
		VL		8* S_V	*Значение цифровой подписи*	Цифровые подписи, генерируемые данным инструментом
	LABR	$LABR_{int}$		8	0 ... (2^8 – 1)	Целая часть LABR
		$LABR_{fra}$		8	0 ... (2^8 – 1)	Дробная часть LABR
	Порог			8	[0 ... 2^8 – 1]	Пороговое значение. (Действительно только для аутентификации без потерь.)
	Перемещение			8	[0 ... 2^8 – 1]	Число перемещений, необходимых для внедрения битов "водяного знака". (Действительно только для аутентификации без потерь.)

Орган регистрации должен присвоить данному инструменту уникальный ID. Описание инструмента можно загрузить с Органа регистрации (RA) при помощи присвоенного ID.

B.3.3 Заключение

В заключение, этот инструмент обладает следующими особенностями:

- Аутентификация изображений JPEG 2000 на уровне данных изображения или на уровне содержания изображения путем интеграции хрупкой и полухрупкой аутентификации в одной структуре. Кроме того, полухрупкая аутентификация включает в себя режимы с потерями информации и без потерь.
- Устойчивость к различным случайным искажениям, возникающим, например, при перекодировке, преобразовании формата, сжатии с потерями информации и мультицикле кодирования JPEG 2000. Поэтому данный инструмент можно использовать для защиты изображений JPEG 2000 во всеобъемлющем окружении.
- Масштабируемая защита изображений JPEG 2000. В частности, данный инструмент может обеспечить защиту любого элемента изображения, компонента, разрешения, слоя, границы или блока кода.

- Совместимость с современной структурой безопасности информации, называемой Инфраструктура открытых ключей (PKI), которая является основой существующих стандартов, таких как X.509.
- Количественная сила защиты, контролируемая одним параметром, называемым LABR, который предоставляет конечным пользователям большие удобства.
- Способность определить возможное место атаки на участках изображения, если изображение считается неподлинным. Эта способность может помочь визуально убедить пользователей.
- Поддержка защиты "с потерями – без потерь", соответствующей сжатию "с потерями – без потерь" стандартов кодирования JPEG 2000. Таким образом, данный инструмент имеет гораздо более широкое применение, включая обработку изображений для медицинских целей и удаленные приложения обработки изображений.

B.4 Простой метод шифрования на основе пакетов для кодовых потоков JPEG 2000

B.4.1 Описание работы

В данном подпункте представлен метод избирательного шифрования для изображений JPEG 2000. Он основывается на шифровании уровня пакета и на стандартных надежных алгоритмах шифра.

Услугой безопасности, которую использует данный метод, является конфиденциальность изображений JPEG 2000, получаемая посредством шифрования кодового потока. Поэтому, используя данный метод, можно достичь защиты IPR, а также защиты частной жизни.

Данный подход поддерживает перекодировку, масштабирование и другие функциональные возможности обработки содержания без необходимости в получении доступа к криптографическому ключу и выполнении расшифровки и повторного зашифровывания. Данный подход не вмешивается в процессы кодирования и декодирования, а также имеет очень ограниченное неблагоприятное влияние на эффективность сжатия и не оказывает неблагоприятного влияния на устойчивость к ошибкам. Такой подход дает максимальную гибкость при реализации сценариев и приложений с различными уровнями безопасности.

Данный метод могут использовать производители содержания для ограничения доступа к содержанию изображения, а также поставщики содержания для гарантирования конфиденциальной поставки содержания конечным пользователям.

B.4.2 Технический обзор

Данный метод состоит в зашифровывании кодового потока после сжатия изображения, как показано на рисунке B.2.

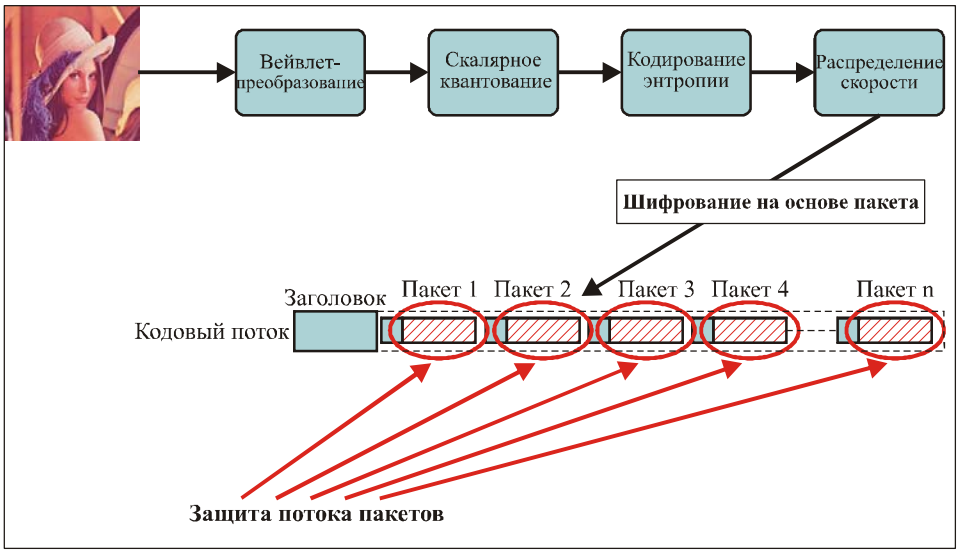


Рисунок B.2 – Принцип шифрования на основе пакетов

Данный инструмент JPSEC может принять в качестве входной информации несколько параметров, связанных с изображением: уровни разрешения, уровни качества, компоненты, границы или элементы изображения. Тогда

обрабатывается только полезная нагрузка пакетов, соответствующих данным входным параметрам. Таким образом, защищенный кодовый поток сохраняет обычную структуру JPEG 2000. После зашифровывания кодового потока, к основному заголовку добавляется сегмент маркера SEC для того, чтобы дать возможность потребителю JPSEC в последствии правильно расшифровать изображение.

Данный метод использует хорошо известные стандартные базовые алгоритмы для выборочного шифрования пакетов: методы DES или AES, связанные с режимами стандарта, описанными в [22] такими, как ECB, CBC, CFB, OFB и CTR. Конечно, можно использовать любые другие алгоритмы блочных шифров. DES и AES приводятся здесь в качестве примеров стандартных шифров.

B.4.2.1 Пример сигнализации

Данный метод может быть сигнализирован при помощи синтаксиса нормативного инструмента, основанного на шаблонах. Ниже приводится пример сигнализации для этого метода (см. таблицу B.6), в котором определяется одна зона для ZOI, но, конечно, их может быть больше, синтаксис остается таким же, как для Зоны^0.

Таблица B.6 – Пример Зоны влияния с пространственными координатами, разрешениями и слоями

Параметр			Размер (биты)	Значение (по порядку)	Производное значение (смысл)
NZzoi			8	1 (RBAS)	Число Зон равно 1
Зона^0	DCzoi		1	0	Далее не следует сегмент, выровненный по байтам
			1	0	Класс описания, связанный с изображением
			6	101100	Участки изображения, уровни разрешения, слои качества и компоненты определены по порядку
	Pzoi^1	Mzoi^1	1	0	Далее не следует сегмент, выровненный по байтам
			1	0	На указанные зоны оказывает влияние метод защиты
			1	0	Определен один элемент
			2	00	Режим прямоугольника
			2	00	Izoi использует 8-битное целое число
			1	1	Izoi описывается в двух измерениях
		Izoi^1	8	0110 0100	Xul – 100
			8	0111 1000	Yul – 120
			8	1011 0100	Xlr – 180
			8	1101 0010	Ylr – 210
	Pzoi^3	Mzoi^3	1	0	Далее не следует сегмент, выровненный по байтам
			1	1	На указанные зоны не оказывает влияния метода защиты
			1	0	Определен один элемент
			2	11	Максимальный режим
			2	00	Izoi использует 8-битное целое число
			1	0	Izoi описывается в одном измерении
		Izoi^3	8	0000 0010	Определены уровни разрешения ≤ 2. (То есть уровни разрешения > 3 определяются при помощи Максимального режима и дополнительного коммутатора.)
	Pzoi^4	Mzoi^4	1	0	Далее не следует сегмент, выровненный по байтам
			1	0	На указанные зоны оказывает влияние метод защиты
			1	0	Определен один элемент
			2	11	Максимальный режим
			2	00	Izoi использует 8-битное целое число
			1	0	Izoi описывается в одном измерении
		Izoi^4	8	0000 0101	Слои ≤ 5 определяются при помощи максимального режима

Таблица B.7 – Описание шаблона расшифровки в случае AES-192/CBC

Параметр					Размер (биты)	Значение	Производное значение (смысл)
P_{PM}	ME_{decry}				8	0000 0000	NULL: метода предотвращения эмуляции маркера нет
	CT_{decry}				16	0x0003	Идентификатор шифра: AES (блочный шифр)
	CP_{decry}	M_{bc}			6	10 0000	Режим шифра: CBC
		P_{bc}			2	01	Режим дополнения (PKCS#7-дополнение)
		SIZ_{bs}			8	0001 0000	Размер блока: 16 байтов (128 битов)
		KT_{bc}	LK_{KT}		16	0x00C0	Размер ключа: 192 бита
			KID_{KT}		8	0000 0011	Информация о ключе – URI
			LKI_{KT}		16	0x0021 (=33)	Длина URI: 33 байта
			KI_{KT}		264	https://server/ path/secretkey .pem	Данный URI является https URL; приложение, использующее JPSEC должно понимать его. Эффективный возврат ключа – за рамками данного стандарта
			G_{KT}	PO	16	0 000 001 010 011 100	Порядок обработки – TRLCP
				GV	8	0000 1001	Степень структурирования ключа – вся область в ZOI
			V_{KT}	N_V	16	0x0001	Одно значение ключа в KI_{KT}; значения в V_{KT} не указаны
				S_V	16	0010 0001	Длина URI: 33 байта
				VL	264	https://server/ path/secretkey .pem	Данный URI является https URL; приложение, использующее JPSEC должно принимать его. Эффективный возврат ключа – за рамками данного стандарта

Таблица B.8 – Синтаксис области обработки

Параметр	Размер (биты)	Значение	Производное значение (смысл)
PD	1	0_b	Далее не следует сегмент, выровненный по байтам
	1	0_b	Не в области пикселов
	1	0_b	Не в области вейвлет-коэффициента
	1	0_b	Не в области квантованного вейвлет-коэффициента
	1	1_b	Обрабатывается в области кодового потока
	3	000_b	Не используется

Таблица B.9 – Синтаксис Степени структурирования и списка значений

Параметр		Размер (биты)	Значение	Производное значение (смысл)
G	PO	16	0 000 001 010 011 100	Порядок обработки TRLCP
	GV	8	0000 0110	Единицей защиты является пакет
V	N_V	16	1	Определено число значений IV
	S_V	8	16	Размер IV в байтах
	VL	128	*Значение*	Значение IV

B.4.3 Заключение

Метод, представленный в данном подпункте, демонстрирует выборочное шифрование для изображений JPEG 2000. Он основывается на шифровании на уровне пакетов, а также на стандартных надежных алгоритмах шифра. Данный метод может быть сигнализирован при помощи шаблонов, определенных в п. 5.8, он поддерживает разные уровни сложности.

B.5 Инструмент шифрования для управления доступом JPEG 2000

B.5.1 Используемые услуги безопасности

Данная технология предоставляет инструмент шифрования, который может предотвратить эмуляцию маркера в зашифрованном кодовом потоке.

B.5.2 Типичные приложения

Данная технология может обеспечить выборочное и полное шифрование кодовых потоков JPEG 2000. Такие методы выборочного шифрования можно использовать для вывода на экран только утвержденного изображения такого, как сильно уменьшенное изображение, изображение низкого качества и частично зашифрованное изображение.

B.5.3 Потенциальные пользователи, модель реализации и мотивировка

В основе данной технологии лежит шифрование кодовых потоков JPEG 2000 на основе пакетов при помощи хорошо известного алгоритма шифра. В частности, данная технология предотвращает эмуляцию маркера в зашифрованном кодовом потоке. Поэтому, даже если получающийся в результате зашифрованный кодовый поток является входящей информацией для устройства расшифровки, совместимого с Частью 1 JPEG 2000, маловероятно, что данное устройство расшифровки получит сбой и может верно воспроизвести защищаемое изображение.

B.5.4 Технический обзор

(1) Шифрование

Этап 1 2 (байта) код временно зашифровывается при помощи хорошо известного алгоритма шифра.

Этап 2 Если временно зашифрованный код или связанный с ним код больше 0xFF8F, тогда данный код 2 (байта) не зашифровывается.

В противном случае временно зашифрованный код является выходной информацией как зашифрованный код.

Этап 3 Переход к следующему 2 (байта) коду, а Этап 1 и Этап 2 продолжаются.

Согласно спецификации Части 1 все 2 (байта) кода в незашифрованном тексте должны быть меньше чем 0xFF90. Кроме того, если временно зашифровываемый код или код, смежный с ним, больше, чем 0xFF8F, тогда 2 (байта) код не зашифровывается. В результате, все 2 (байта) кода в зашифрованном тексте меньше, чем 0xFF90.

Если длина незашифрованного текста является нечетной, необходимо сделать исключение при обработке, последний байт не зашифровывается или дополняется одним дополнительным байтом.

(2) Расшифровка

Этап 1 2 (байта) код временно расшифровывается при помощи того же алгоритма шифра, что использовался при шифровании.

Этап 2 Если временно расшифрованный код или код, смежный с ним, больше, чем 0xFF8F, тогда 2 (байта) код не расшифровывается. В противном случае временно расшифрованный код является выходной информацией как расшифрованный код.

Этап 3 Переход к следующему 2 (байта) коду, Этап 1 и Этап 2 продолжаются.

Весь 2 (байта) код в исходном незашифрованном тексте должен быть меньше, чем 0xFF90. Таким образом, можно придти к выводу, что 2 (байта) код не зашифровывается, если временно расшифрованный код или код, смежный с ним, больше чем 0xFF8F.

B.5.5 Метод сигнализации

В таблице B.10 приводится пример параметров для данной технологии. Любые параметры для данной технологии должны быть сигнализированы в соответствии с синтаксисом, определяемом в JPSEC. В особенности, данная технология должна использовать шаблон "расшифровки", степень структурирования "пакет" и область применения "битовый поток" с соответствующей ZOI.

Таблица B.10 – Пример параметров для данной технологии

Параметр		Размер (биты)	Значение	Значение (смысл)
SEC		16	0xFF65	Маркер SEC
L_{SEC}		16	Переменное	Длина сегмента маркера SEC
Z_{SEC}		8	1 (пример)	Указатель данного сегмента маркера SEC
P_{SEC}		1	0	Далее не следует байт FBAS
	F_{INSEC}	1	1 (пример)	Используется INSEC
	$F_{multiSEC}$	1	0_b	Используется один сегмент маркера SEC
	F_{mod}	1	1_b	Исходные данные JPEG 2000 были изменены
	F_{TRLCP}	1	0_b	Использование маркера TRLCP не определено
	Дополнение	3	000_b	Не используется
	N_{tools}	8 (RBAS)	1	Число инструментов безопасности равно 1
	I_{max}	8 (RBAS)	0	Максимальный указатель экземпляра инструмента равен 0
t		8 (FBAS)	1	Защита RA ненормативного инструмента JPSEC
i		8 (RBAS)	0000000_b	Указатель экземпляра для данного инструмента
ID_{RA}	$ID_{RA,id}$	32	0	Зарегистрированный ID
	$ID_{RA,nsl}$	8 (RBAS)	21	Длина $ID_{RA,ns}$ в байтах
	$ID_{RA,ns}$	168	*Пространство имен*	Пространство имен RA, в котором зарегистрирован данный инструмент
L_{ZOI}		16	9	Длина ZOI равна 9 байтам
ZOI		Переменный	См. таблицу B.11 (пример)	Зона влияния для данного инструмента
L_{PID}		16	Переменное	Длина L + T + PD + G
P_{ID}		Переменный	См. таблицу B.12 (пример)	Параметры для данной технологии

Таблица B.11 – Пример ZOI данного инструмента генерирования ключа

Параметр			Размер (биты)	Значение (по порядку)	Производное значение (смысл)
NDzoi			8	1	Число Зон равно 1
Зона[0]	DCzoi		1	0_b	Далее не следует сегмент, выровненный по байтам
			1	0_b	Класс описания, связанный с изображением
			6	101000_b	Участки изображения и уровни разрешения определены по порядку
	Pzoi[1]	Mzoi[1]	1	0_b	Далее не следует сегмент, выровненный по байтам
			1	0_b	На указанные зоны оказывает влияние метод защиты
			1	0_b	Определен один элемент
			2	00_b	Режим прямоугольника
			2	00_b	Izoi использует 8-битное целое число
			1	1_b	Izoi описывается в двух измерениях
		Izoi[1]	8	$0110\ 0100_b$	Xul – 100
			8	$0111\ 1000_b$	Yul – 120
			8	$1011\ 0100_b$	Xlr – 180
			8	$1101\ 0010_b$	Ylr – 210

Таблица B.11 – Пример ZOI данного инструмента генерирования ключа

Параметр			Размер (биты)	Значение (по порядку)	Производное значение (смысл)
	Pzoi[3]	Mzoi[3]	1	0_b	Далее не следует сегмент, выровненный по байтам
			1	1_b	Метод защиты не оказывает влияния на указанные зоны
			1	0_b	Определен один элемент
			2	11_b	Максимальный режим
			2	00_b	Izoi использует 8-битное целое число
			1	0_b	Izoi описывается в одном измерении
		Izoi[3]	8	$0000\ 0010_b$	Определены уровни разрешения > 3

Таблица B.12 – P_{ID} для данной технологии

Параметр		Размер (биты)	Значение	Значение (смысл)
T		Переменный	См. таблицу B.13	Шаблоны расшифровки
PD		8	$0000\ 1000_b$	Далее не следует байт FBAS. Обрабатывается в области кодового потока
G	PO	16	$0\ 000\ 001\ 010\ 011\ 100\ 0_b$	Порядок обработки – элемент изображения – разрешение – слой – компонент – граница
	GL	8	$0000\ 0110_b$	Единицей защиты является пакет
Skip		8	0	Параметр *Skip* для данного инструмента

Таблица B.13 – Пример шаблона расшифровки для данной технологии

Параметр		Размер (биты)	Значение (по порядку)	Производное значение (смысл)
ME_{decry}		8	1	Эмуляция маркера не произошла
CT_{decry}		16	1	Блочный шифр (AES)
CP_{decry}	M_{bc}	6	$10\ 0010_b$	Используется режим OFB. (Биты не дополняются.)
	SIZ_{bc}	16	128	Размер блока (128 битов)
	KT_{bc}	Переменный	*Значения шаблона ключей*	Шаблон ключей
	IVsc	128	*Первоначальное значение вектора*	Первоначальное значение вектора

B.5.6 Заключение

В данном подпункте описывалась технология шифрования для кодового потока JPEG 2000. Значительным преимуществом данной технологии является предотвращение эмуляции маркера в зашифрованном кодовом потоке.

B.6 Инструмент генерирования ключа для управления доступом JPEG 2000

B.6.1 Используемые услуги безопасности

Данная технология предоставляет управление доступом, связанное с изображением, для JPEG 2000 в соответствии с иерархической структурой JPEG 2000.

B.6.2 Типичные применения

Типичным применением данной технологии является распространение защищенных изображений, где только авторизованный пользователь сможет воспроизвести полученное изображение. Например, сильно уменьшенное изображение можно свободно воспроизводить, а изображение с большим разрешением может быть расшифровано только пользователем, у которого есть ключ.

B.6.3 Потенциальные пользователи, модель реализации и мотивировка

Данная технология поддерживает генерирование ключей для использования при защищенном распространении изображения JPEG 2000. Данная технология основана на управлении доступом, связанным с изображением, таким, как участок изображения, разрешение и качество изображения. Принцип данной технологии – генерирование ключей шифрования и расшифровки в иерархическом порядке при помощи криптографической однонаправленной хэш-функции такой, как хэш-функция.

B.6.4 Технический обзор

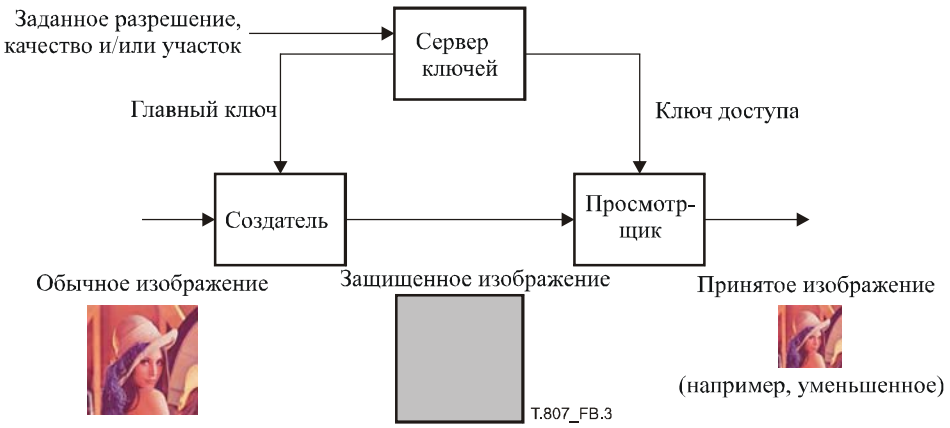


Рисунок B.3 – Обзор данной технологии

На этапе шифрования сервер ключей генерирует главный ключ. Затем создатель зашифровывает изображение, используя ключи пакета, которые генерируются из главного ключа. На этапе расшифровки сервер ключей генерирует ключ доступа в соответствии с заданным разрешением, качеством и/или участком изображения. Затем программа просмотра расшифровывает зашифрованное изображение при помощи ключей пакета, которые генерируются из ключа доступа. Отметим, что данные ключи генерируются последовательно на основе защищенной цепочки хэш-функций.

В частности, в данной технологии используется следующая политика управления доступом: "если пользователь может получить доступ к какому-либо уровню разрешения/слою, тогда данный пользователь может также получить доступ к более низким уровням разрешения/слоям". С другой стороны, даже если пользователь может получить доступ к какому-либо элементу изображения, он не может получить доступ ни к каким другим элементам изображения

Важным преимуществом данной технологии является то, что число ключей, необходимых для перехода от сервера ключей к программе просмотра, гораздо меньше, чем обычно. Это означает, что данная технология позволяет снизить потери при использовании запоминающих устройств.

B.6.5 Метод сигнализации

В таблице B.14 приводятся параметры, рекомендуемые для данной технологии. Любые параметры должны сигнализироваться в соответствии с синтаксисом, определенным в JPSEC. В особенности, данный инструмент должен использовать шаблон "расшифровки", степень структурирования "пакет" и область обработки "битовый поток" с соответствующей ZOI.

Таблица B.14 – Параметры, рекомендуемые для данной технологии

Параметр		Размер (биты)	Значения	Значение (смысл)
SEC		16	0xFF65	Маркер SEC
L_{SEC}		16	0 ... 255	Длина сегмента маркера SEC
Z_{SEC}		8	0	Указатель данного сегмента маркера SEC
P_{SEC}		1	0	Далее не следует байт FBAS
	F_{INSEC}	1	1	Используется INSEC
	$F_{multiSEC}$	1	0_b	Используется один сегмент маркера SEC

Таблица B.14 – Параметры, рекомендуемые для данной технологии

Параметр		Размер (биты)	Значения	Значение (смысл)
	F_{mod}	1	1_b	Исходные данные JPEG 2000 были изменены
	F_{TRLCP}	1	0_b	Использование маркера TRLCP не определено
	Дополнение	3	000_b	Не используется
	N_{tools}	8 (RBAS)	1	Число инструментов безопасности равно 1
	I_{max}	8 (RBAS)	0	Максимальный указатель экземпляра инструмента равен 0
t		8 (RBAS)	1	Ненормативный инструмент JPSEC
i		8 (RBAS)	0	Указатель экземпляра для данного инструмента
ID_{RA}	$ID_{RA,id}$	32	5	Зарегистрированный ID для данного инструмента
	$ID_{RA,nsl}$	8 (RBAS)	21	Длина $ID_{RA,ns}$ в байтах
	$ID_{RA,ns}$	168	*Пространство имен*	Пространство имен RA, в котором зарегистрирован данный инструмент
L_{ZOI}		16	Переменное	Длина ZOI для данного инструмента
ZOI		Переменный	*Значение ZOI*	Зона влияния для данного инструмента
L_{PID}		16	Переменное	Длина L + T + PD + G
P_{ID}		Переменный	См. таблицу B.16	Параметры для данной технологии

Таблица B.15 – Пример ZOI данного инструмента генерирования ключа

Параметр			Размер (биты)	Значение (по порядку)	Производное значение (смысл)
NDzoi			8	1	Число Зон равно 1
Зона[0]	DCzoi		1	0_b	Далее не следует сегмент, выровненный по байтам
			1	0_b	Класс описания, связанный с изображением
			6	101000_b	Участки изображения и уровни разрешения определены по порядку
	Pzoi[1]	Mzoi[1]	1	0_b	Далее не следует сегмент, выровненный по байтам
			1	0_b	На указанные зоны оказывает влияние метод защиты
			1	0_b	Определен один элемент
			2	00_b	Режим прямоугольника
			2	00_b	Izoi использует 8-битное целое число
			1	1_b	Izoi описывается в двух измерениях
		Izoi[1]	8	$0110\ 0100_b$	Xul – 100
			8	$0111\ 1000_b$	Yul – 120
			8	$1011\ 0100_b$	Xlr – 180
			8	$1101\ 0010_b$	Ylr – 210
	Pzoi[3]	Mzoi[3]	1	0_b	Далее не следует сегмент, выровненный по байтам
			1	1_b	Метод защиты не оказывает влияния на указанные зоны
			1	0_b	Определен один элемент
			2	11_b	Максимальный режим
			2	00_b	Izoi использует 8-битное целое число
			1	0_b	Izoi описывается в одном измерении
		Izoi[3]	8	$0000\ 0010_b$	Определены уровни разрешения > 3

Таблица B.16 – P_{ID} для данной технологии

Параметр		Размер (биты)	Значения	Значение (смысл)
T		Переменный	См. таблицу B.17	Шаблоны расшифровки
PD		8	$0000\ 1000_b$	Далее не следует байт FBAS. Обрабатывается в области кодового потока
G	PO	16	$0\ 000\ 001\ 010\ 011\ 100_b$	Порядок обработки – элемент изображения – разрешение – слой – компонент – граница
	GL	8	$0000\ 0110_b$	Единицей защиты является пакет
H		16	См. таблицу 37 в п. 5.8.3.1	Хэш-функция для данного инструмента генерирования ключа
L_k		8	0 ... 255	Длина информации о ключе доступа
AK_{info}		Переменный	*Значение ключа доступа*	Информация о ключе доступа (данная информация зашифровывается при помощи KT_{bc} в T)

Таблица B.17 – Пример шаблона расшифровки для данной технологии

Параметр		Размер (биты)	Значение (по порядку)	Производное значение (смысл)
ME_{decry}		8	1	Эмуляция маркера не произошла
CT_{decry}		16	3	Блочный шифр (AES)
CP_{decry}	M_{bc}	6	10 0010	Используется режим OFB. (Биты не дополняются.)
	SIZ_{bc}	16	128	Размер блока (128 битов)
	KT_{bc}	Переменный	См. п. 5.8.5	Шаблон ключей
	IVsc	128	*Первоначальное значение вектора*	Первоначальное значение вектора

B.6.6 Заключение

В данном подпункте описывалась технология управления доступом, связанная с изображением для кодового потока JPEG 2000. Значительным преимуществом данной технологии является то, что число ключей, которыми необходимо управлять и к которым необходимо получать доступ, меньше, чем обычно.

B.7 Скремблирование вейвлет-области и битового потока для условного управления доступом

B.7.1 Резюме

Управление доступом к изображению является важной функцией в защищенной передаче изображений. Часто возникает необходимость предоставить доступ только к сильно уменьшенному изображению или к изображению низкого качества, в то время как доступ к более высоким разрешениям или лучшему качеству подлежит авторизации. В данном подпункте рассматривается метод условного управления доступом. Первоначально данный метод был представлен в [23]. Метод состоит в том, что к изображению добавляются псевдослучайные помехи. Авторизованным пользователям известна эта псевдослучайная последовательность, и, таким образом, они могут удалить эти помехи. С другой стороны, неавторизованные пользователи имеют доступ только к сильно искаженным изображениям. Система состоит их трех основных компонентов: скремблирование, генератор псевдослучайных чисел и алгоритм шифрования. Для того чтобы полностью использовать и сохранить свойства JPEG 2000, к блокам кода, составляющим кодовый поток, выборочно применяется скремблирование. Следовательно, можно управлять уровнем искажений, вводимых в определенные части изображения. Это позволяет управлять доступом к разрешению, качеству или интересным участкам изображения.

B.7.2 Технический обзор

Данная система состоит из трех основных компонентов:

- Скремблирование: предусматривается два подхода. Скремблирование выполняется либо над квантованными вейвлет-коэффициентами, либо непосредственно над битами кодового потока. В первом случае, знаки коэффициентов в каждом блоке кода инвертируются псевдослучайным образом. Во втором случае, биты кодового потока инвертируются псевдослучайным образом.

- Генератор псевдослучайных чисел (PRNG): PRNG используется для приведения скремблирования в движение. Он основывается на значении начального числа. В более предпочтительном варианте реализации данного метода для генератора псевдослучайных чисел (PRNG) используется алгоритм SHA1PRNG [24] с 64-битным начальным числом. Отметим, что также можно использовать другие алгоритмы PRNG.
- Алгоритм шифрования: для того чтобы сообщить начальные числа авторизованным пользователям, их зашифровывают и вставляют в кодовый поток. В более предпочтительном варианте реализации данного метода для шифрования используется алгоритм RSA [25]. Можно также использовать другие алгоритмы шифрования. Длину ключа можно выбрать в момент защиты изображения.

Рисунки B.4 и B.5 соответствуют двум случаям скремблирования вейвлет-области и битового потока.

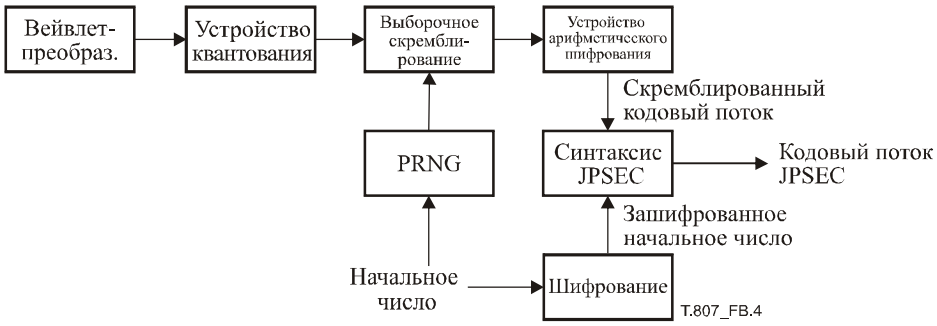


Рисунок B.4 – Блок-схема для скремблирования вейвлет-области

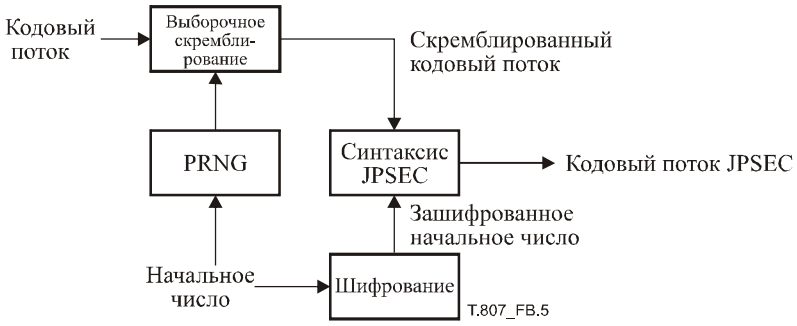


Рисунок B.5 – Блок-схема для скремблирования области битового потока

Для усиления безопасности системы можно изменять начальное число от одного блока кода к другому. Также, используя различные ключи шифрования, можно определить несколько уровней доступа. Синтаксис, приведенный ниже, является очень гибким и предусматривает использование нескольких начальных чисел и многих ключей.

B.7.3 Синтаксис кодового потока

В данном примере используются сегменты маркеров SEC и INSEC. Синтаксис кодового потока определен ниже. В сегменте маркера SEC используется синтаксис инструмента для ненормативных инструментов. Сегмент маркера INSEC используется для сигнализации того, какие блоки кода скремблируются, и какие начальные числа используются.

B.7.3.1 Синтаксис сегмента маркера SEC

Используется синтаксис инструмента для ненормативных инструментов. В случае использования нескольких ключей в сегменте маркера SEC используются несколько экземпляров инструмента. А именно, присутствуют несколько экземпляров i = 0, 1, 2, ... с одинаковым ID, причем каждый экземпляр соответствует различному идентификатору ключа $KeyID^{(i)}$ (рисунок B.6).

t	i = 0	ID	$L_{ZOI}^{(0)}$	$ZOI^{(0)}$	$L_{PID}^{(0)}$	$N_S^{(0)}$	$KeyID^{(0)}$	Данные
t	i = 1	ID	$L_{ZOI}^{(1)}$	$ZOI^{(1)}$	$L_{PID}^{(1)}$	$N_S^{(1)}$	$KeyID^{(1)}$	Данные
t	i = 2	ID	$L_{ZOI}^{(2)}$	$ZOI^{(2)}$	$L_{PID}^{(2)}$	$N_S^{(2)}$	$KeyID^{(2)}$	Данные

Рисунок B.6 – Синтаксис ненормативного инструмента защиты в случае с множеством ключей

P_{ID} имеет следующую семантику:

Таблица B.18 – Синтаксис и семантика для P_{ID}

Параметры	Размер (биты)	Значение
N_S	16	Число начальных чисел, используемых данным экземпляром
KeyID	32	Идентификация ключа, используемого для расшифровки
Данные	Переменный	Зашифрованные начальные числа

B.7.3.2 Синтаксис сегмента маркера INSEC

Для передачи информации о том, какое начальное число используется для защиты блоков кода, также используется маркер безопасности внутри кодового потока (INSEC). В данном примере он вставляется перед защищенным(и) блоком(ами) кода для указания на то, Какое начальное число используется для защиты данного(ых) блока(ов) кода. Вместо указания на само начальное число, маркер содержит указатель, относящийся к начальным числам в основном заголовке сегмента маркера SEC. В данном примере информация INSEC применяется к последующим блокам кода, R всегда равно 1. В случае вейвлет-скремблирования и скремблирования битового потока синтаксис AP различается:

S_{idx}

Off	S_{idx}

Рисунок B.7 – Синтаксис AP: Скремблирование вейвлет-области (слева), скремблирование области битового потока (справа)

Семантика следующая:

Таблица B.19 – Синтаксис и семантика AP

Параметр	Размер (биты)	Значение
Off	16	Смещение первого скремблируемого байта в битовом потоке блока кода
S_{idx}	16	Указатель начального числа для блока кода

В случае использования нескольких ключей, комбинация экземпляра инструмента i и указателя начального числа S_{idx} уникальным образом идентифицирует, на какое начальное число/ключ ссылается сегмент маркера INSEC.

B.7.4 Заключение

В данном подпункте был представлен инструмент безопасности для условного управления доступом к изображениям JPEG 2000. Данный метод предусматривает вставку псевдослучайных помех в выбранные части кодового потока. Следовательно, для неавторизованного устройства расшифровки, которое не знает, как удалить эти помехи, расшифрованное изображение имеет большое количество искажений,

Безопасность данного метода зависит от защищенности определенных алгоритмов для генерирования псевдослучайного числа и шифрования начальных чисел, при более предпочтительной реализации данного метода это SHA1PRNG и RSA, соответственно. SHA1PRNG – это защищенный PRNG, поскольку даже зная некоторые числа последовательности, вычислить саму последовательность невозможно. В данном примере начальное число PRNG имеет 64 бита, что не позволяет осуществить атаку грубой силой. Начальные числа зашифровываются при помощи RSA, используя длину ключа, задаваемую пользователем. RSA считается безопасным алгоритмом, при условии если используется ключ достаточной длины.

B.8 Прогрессивный доступ для кодового потока JPEG 2000

B.8.1 Используемые услуги безопасности

Данный метод обеспечивает управление доступом, не связанным с изображением, для JPEG 2000 в соответствии с порядком продвижения в кодовом потоке.

B.8.2 Типичное применение

Типичным способом применения данной технологии является защищенное распространение изображения, при котором только авторизованный пользователь может воспроизвести принятое изображение. В частности, данная технология подходит для управления доступом в соответствии с порядком продвижения в кодовом потоке.

B.8.3 Потенциальные пользователи, модель реализации и мотивировка

Основной проблемой при разработке схемы управления доступом является достижение равновесия между безопасностью, эффективностью и гибкостью. Данный метод управления доступом для кодового потока JPEG 2000 конструирует цепочку хэш-функций для генерирования ключей для каждого пакета с целью зашифровать пакеты в кодовом потоке. Поэтому расшифровать пакеты, соответствующие данному изображению в кодовом потоке могут только пользователи, имеющие верную категорию допуска.

B.8.4 Технический обзор

На этапе шифрования сервер ключей генерирует главный ключ. Затем создатель зашифровывает кодовый поток при помощи ключей пакета, которые генерируются из главного ключа. На этапе расшифровки сервер ключей генерирует ключ доступа в соответствии с заданным пакетом. Затем программа просмотра расшифровывает зашифрованный кодовый поток при помощи ключей пакета, которые генерируются из ключа доступа.

В частности, данная технология использует следующую политику управления доступом: "если пользователь может получить доступ к какому-либо пакету, тогда этот пользователь может также получить доступ к предшествующим пакетам в данном кодовом потоке". Поэтому мы можем назвать такой вид управления доступом "Прогрессивный доступ".

Существенным преимуществом данной технологии является то, что число ключей, необходимых для перехода от сервера ключей к программе просмотра, гораздо меньше, чем обычно. Это означает, что данная технология позволяет снизить потери при использовании запоминающих устройств.

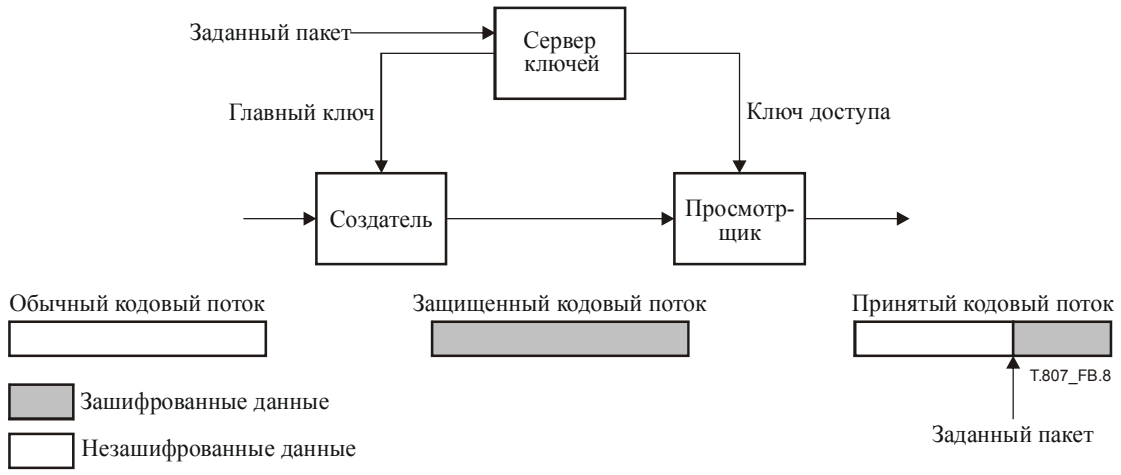


Рисунок B.8 – Технический обзор данной технологии

B.8.5 Метод сигнализации

В таблице B.20 приводятся параметры, рекомендуемые для данной технологии. Любые параметры должны сигнализироваться в соответствии с синтаксисом, определенным в JPSEC. В особенности, данный инструмент должен использовать шаблон "расшифровки", степень структурирования "пакет" и область обработки "битовый поток" с соответствующей ZOI.

Таблица B.20 – Пример параметров для данного инструмента

Параметр		Размер (биты)	Значения	Значение (смысл)
SEC		16	0xFF65	Маркер SEC
L_{SEC}		16	Переменное 0 ... 255	Длина сегмента маркера SEC
Z_{SEC}		8	0	Указатель данного сегмента маркера SEC
P_{SEC}		1	0	Далее не следует байт FBAS
	F_{INSEC}	1	1_b	Используется INSEC
	$F_{multiSEC}$	1	0_b	Используется один сегмент маркера SEC
	F_{mod}	1	1_b	Исходные данные JPEG 2000 были изменены
	F_{TRLCP}	1	0_b	Использование маркера TRLCP не определено
	Дополнение	3	000_b	Не используется
	N_{tools}	8 (RBAS)	1	Число инструментов безопасности равно 1
	I_{max}	8 (RBAS)	0	Максимальный указатель экземпляра инструмента равен 0
t		8 (RBAS)	1	Инструмент защиты RA
i		8 (RBAS)	0	Указатель экземпляра
ID_{RA}	$ID_{RA,id}$	32	7	Зарегистрированный ID
	$ID_{RA,nsl}$	8 (RBAS)	21	Длина $ID_{RA,ns}$ в байтах
	$ID_{RA,ns}$	168	*Пространство имен*	Пространство имен RA, в котором зарегистрирован данный инструмент
L_{ZOI}		16 (RBAS)	Переменное	Длина ZOI
ZOI		Переменный	См. таблицу B.21 (пример)	Зона влияния для данного инструмента
L_{PID}		16 (RBAS)	Переменное	Длина L + T + PD + G
P_{ID}		Переменный	См. таблицу B.22 (пример)	Параметры для данного инструмента

Таблица B.21 – Пример ZOI данной технологии

Параметр			Размер (биты)	Значение (по порядку)	Производное значение (смысл)
NDzoi			8	1	Число Зон равно 1
$Зона^0$	DCzoi		1	0	Далее не следует сегмент, выровненный по байтам
			1	1	Класс описания, несвязанный с изображением
			6	000100	Пакеты определены
	$Pzoi^4$	$Mzoi^4$	0	1	Далее не следует сегмент, выровненный по байтам
			1	1	Метода защиты не оказывает влияния на указанные зоны
			1	1	Определено много элементов
			11	2	Максимальный режим
			00	2	Izoi использует 8-битное целое число
			00	2	Izoi описывается в одном измерении
		$Izoi^{11}$	8	0000 1010	Определяется индекс пакета > 10

Таблица B.22 – P_{ID} для данной технологии

Параметр		Размер (биты)	Значения	Значение (смысл)
T		Переменный	См. таблицу B.23	Шаблоны расшифровки
PD		8	$0000\ 1000_b$	Последующий байт BAS не существует. Область кодового потока
G	PO	16	$0\ 000\ 001\ 010\ 011\ 100_b$	Порядок обработки – элемент изображения – разрешение – слой – компонент – граница
	GL	8	$0000\ 0110_b$	Единицей защиты является пакет
H		16	См. таблицу 37 в п. 5.8.3.1	Хэш-функция для данного инструмента генерирования ключа
L_k		8	0 ... 255	Длина информации о ключе доступа
AK_{info}		Переменный	*Значение ключа доступа*	Информация о ключе доступа (данная информация зашифровывается при помощи KT_{bc} в T)

Таблица B.23 – Пример шаблона расшифровки для данной технологии

Параметр		Размер (биты)	Значение (по порядку)	Производное значение (смысл)
ME_{decry}		8	1	Эмуляция маркера не произошла
CT_{decry}		16	3	Блочный шифр (AES)
CP_{decry}	M_{bc}	6	10 0010	Используется режим OFB. (Биты не дополняются.)
	SIZ_{bc}	16	128	Размер блока (128 битов)
	KT_{bc}	Переменный	*Значения шаблона ключей*	Шаблон ключей
	IVsc	128	*Первоначальное значение вектора*	Первоначальное значение вектора

B.8.6 Заключение

В данном подпункте описывалась технология управления доступом для кодового потока JPEG 2000. Значительным преимуществом данной технологии является то, что число ключей, которыми необходимо управлять и к которым необходимо получать доступ, меньше, чем обычно. Данная технология обеспечивает гибкое и эффективное управление доступом JPEG 2000 в соответствии с порядком продвижения в кодовом потоке.

B.9 Масштабируемая подлинность кодовых потоков JPEG 2000

B.9.1 Услуга безопасности

В данном подпункте представлен гибкий механизм аутентификации для кодовых потоков JPEG 2000. Он позволяет пользователям подтверждать подлинность и целостность различных подизображений (субизображений) при помощи одной цифровой подписи.

B.9.2 Типичное применение

В важных областях деятельности таких, как управление, финансы, здравоохранение и право, клиентам обычно необходимо подтверждение подлинности полученного содержания. Следовательно, для аутентификации документа при распространении содержания требуется механизм масштабируемой безопасности.

B.9.3 Мотивировка

В издательских приложениях третьих сторон производитель изображения генерирует кодовый поток и его подпись. Затем производитель поставляет кодовый поток и его подпись издателю третьей стороны. Из-за ограниченности ресурсов (например, пропускной способности, вычислительных возможностей) пользователи могут запросить у издателя перекодированный кодовый поток. Издатель поставит пользователю данные подизображения (субизображения) и доказательство их подлинности.

B.9.4 Технический обзор

Данная схема предоставляет гибкий механизм аутентификации для кодовых потоков JPEG 2000. Он включает в себя 3 модуля: Подпись, Перекодировка и Подтверждение подлинности. Основной технологией является дерево Меркле (Merkle), которая организует пакеты JPEG 2000.

B.9.4.1 Модуль подписи

Модуль подписи генерирует подпись на входе кодового потока JPEG 2000 в соответствии с предпочтительной схемой цифровой подписи. Защищенный кодовый поток получается при вставке маркера SEC в исходный кодовый поток. В частности, производитель:

- читает кодовый поток JPEG 2000;
- конструирует дерево хэш-функции для вычисления *корневого* значения. Значение каждого "листа" представляет собой значение хэш-функции пакета. Значение каждого внутреннего узла представляет собой значение хэш-функции дочерних узлов. Структура дерева аналогична порядку продвижения кодового потока;
- подписывает *корневое* значение дерева хэш-функций при помощи частного ключа, основанного на алгоритме подписи;
- создает параметры SEC. Вставляет данные параметры в сегмент SEC для получения подлинного кодового потока.

B.9.4.2 Модуль перекодировки

Генерирует Второстепенные Метки целостности (SIT) и перекодированный кодовый поток, основанный на запрашиваемом разрешении, слое, компоненте и участке. SEC нового кодового потока включает в себя SIT и некоторые другие параметры. В частности, издатель и/или прокси:

- читает отброшенные пакеты, не включенные в перекодированный кодовый поток;
- конструирует поддеревья хэш-функции при помощи отброшенных пакетов;
- вставляет корневые значения поддеревьев в сегмент SEC.

Перекодированный кодовый поток включает в себя обновленный сегмент SEC и кодовый поток без отброшенных пакетов.

B.9.4.3 Модуль проверки

Модуль проверки проверяет подлинность защищенного кодового потока. В соответствии с предпочтительной схемой цифровой подписи, верификатор получает открытый ключ, затем:

- читает полученный кодовый поток;
- конструирует дерево хэш-функции при помощи полученных пакетов и заголовков кодовых потоков снизу вверх. Если некоторые пакеты отбрасываются, заменяет данное поддерево (поддерево) соответствующим SIT. Таким образом, конструируется *корневое'* значение;
- проверяет *корневое'* значение по отношению к подписи в сегменте SEC на основе определенной системы подписи. Если они совпадают, кодовый поток принимается; в противном случае полученные пакеты отклоняются.

B.9.5 Синтаксис кодового потока

Структура SEC показана в таблице B.24. Она включает в себя маркер SEC, ID инструмента и ZOI, шаблон аутентификации, а также параметры безопасности для подтверждения подлинности. Параметры безопасности включают в себя данные для восстановления заголовков кодовых потоков.

Таблица B.24 – Синтаксис ненормативного инструмента

t	i	ID	L_{ZOI}	ZOI_{ID}	L_{ID}	PM_{ID}	T	TP_{ID}

Параметр		Размер	Значения	Семантика
t		8 (RBAS)	1	Инструмент защиты органа регистрации
i		8 (RBAS)	*Значение экземпляра*	Идентификатор экземпляра инструмента
ID_{RA}	$ID_{RA,id}$	32	*Значение ID*	Зарегистрированный ID
	$ID_{RA,nsl}$	8 (RBAS)	21	Длина $ID_{RA,ns}$ в байтах
	$ID_{RA,ns}$	168	*Пространство имен*	Пространство имен RA, в котором зарегистрирован данный инструмент
L_{ZOI}		16	$[0 \ldots 2^{16} - 1]$	Длина параметров для ZOI
ZOI_{ID}		Переменный	Значения ZOI	Параметры Зоны
L_{ID}		16	$[19 \ldots 2^{16} - 1]$	Длина параметров
ID_T		8	2	id класса для шаблона аутентификации
T		Переменный	*Значения шаблона аутентификации*	Шаблон аутентификации/MAC
TP_{ID}		Переменный	См. таблицу B.25	Параметры безопасности

Таблица B.25 – Параметры безопасности

Параметр	Размер (биты)	Значения	Значение (смысл)
HashTree	8	0 ... (2^8 – 1)	Порядок Hash Tree. Может отличаться от порядка продвижения кодового потока. Ориентировочно, 0x00: LRCP 0x01: RLCP 0x02: RPCL 0x03: PCRL 0x04: CPRL другие: зарезервированы
L_{SIT}	16	0 ... (2^{16} – 1)	Число SIT
SIT	Переменный: L_{hash}*L_{SIT}	NaN	Второстепенная метка целостности
L_{SMH}	16	0 ... (2^{16} – 1)	Длина SMH
SMH	Переменный		Параметры для восстановления основного заголовка
L_{STH}	16	0 ... (2^{16} – 1)	Длина STH
STH	Переменный		Параметры для восстановления заголовка элемента изображения
a) Для аутентификации Keyed-MAC ключ (подтверждения подлинности) следует поставлять отдельно. b) NaN: Не является числом. c) L_{hash} – это размер значения хэш-функции, например 160 для SHA-1.			

B.9.6 Заключение

Данная технология обеспечивает гибкий механизм аутентификации для кодового потока JPEG 2000. Она обладает свойством "подписав один раз, подтверждать подлинность много раз". То есть после подписания исходного кодового потока JPEG 2000, различные кодовые потоки, получающиеся из исходного кодового потока в результате перекодировки, можно верифицировать, полагаясь только на производителя. Данное свойство прекрасно дополняет функциональную возможность "сжать один раз, восстанавливать по-разному". Данная технология противоположна традиционному методу аутентификации, которая позволяет одной подписи аутентифицировать только одно изображение.

B.10 Конфиденциальность данных JPEG 2000 и система управления доступом на основе разделения данных и создания "приманки"

Система, описанная в данном подпункте, основана на разделении в ходе процесса, который называется *Data_Splitting and Luring*, исходного файла JPEG 2000 на два новых файла, называющихся, соответственно *Lured_jp2file*, передающего защищенное содержание, и *Control_File*, передающего информацию, необходимую для получения доступа к защищенному содержанию. Восстановить исходный файл JPEG 2000 можно только при помощи комбинации данных двух файлов в режиме реального времени в ходе процесса *Live_Composing*. Управление процессом Live_Composing осуществляется в соответствии с правилами управления доступом и управлением правами. Описанная система обеспечивает высокий уровень надежности и гибкости в области конфиденциальности данных JPEG 2000 и управления доступом. Кроме того, в ее основе лежит низкое потребление времени и низкозатратные операции по вычислению.

B.10.1 Описание работы

B.10.1.1 Используемые услуги безопасности

– Конфиденциальность: Файл Lured_jp2file передает защищенное содержание. При декодировании только файла Lured_jp2file, визуализируемое содержание визуально скремблируется, таким образом предотвращая доступ к первоначальному содержанию. Получение доступа к

первоначальному содержанию возможно только при восстановлении данных, хранящихся в файле Control_File, в ходе Процесса Live_Composing в режиме реального времени.

– Управление доступом: Данную систему можно использовать для выполнения управления доступом к содержанию изображения: несколько пользователей, имеющих один и тот же файл Lured_jp2file, но обладающие разными правами доступа не смогут получить доступ к одним и тем же частям содержания.

Обратите внимание на защиту IPR: связывая доступ к содержанию с аутентификацией и управлением правами, можно обеспечить эффективное управление и отслеживание передачи и использования защищенного содержания в соответствии с желанием и исключительными правами владельца содержания, возможно, комбинируя данную систему с "водяными знаками" и контрольной суммой файла.

B.10.1.2 Типичное применение

Одной из ключевых идей описанной системы является разделение исходного файла JPEG 2000 на два файла, причем первый (Lured_jp2file) передает только 99% исходных данных, а 1% фиктивных данных, называемых "приманка", можно свободно распространять, вещать, обмениваться или копировать посредством любых классических сетей или сред передачи. Второй файл (Control_File) передает 1% исходных данных плюс некоторая информация. Данные второго файла абсолютно необходимы для получения доступа к защищенному содержанию, передаваемому в файле Lured_jp2file.

Другой ключевой идеей является связывание доступа к защищенному содержанию, передаваемому в файле Lured_jp2file, с этапами идентификации и управления правами, результаты которых запустят потоковую передачу необходимой информации, используемой для восстановления нескремблированного содержания только в режиме реального времени.

В заключение, эффективно отслеживать использование и сообщать об использовании можно посредством статистических данных, собираемых из защищенных журналов регистрации серверов Control_files.

B.10.1.3 Потенциальные пользователи, модель реализации и мотивировка

Потенциальными пользователями описываемой системы являются создатели, владельцы и поставщики содержания, поскольку данная система гарантирует, что после защиты содержания и передачи его в файле Lured_jp2file, получить доступ к исходному содержанию смогут только аутентифицированные и разрешенные пользователи. Важно отметить, что только 99% первоначального содержания предоставляется бесплатно, в то время как 1%, необходимый для получения доступа к исходному содержанию, будет распространяться только после прохождения протоколов аутентификации и управления правами.

B.10.2 Технический обзор

На рисунке B.9 представлен обзор данной системы.

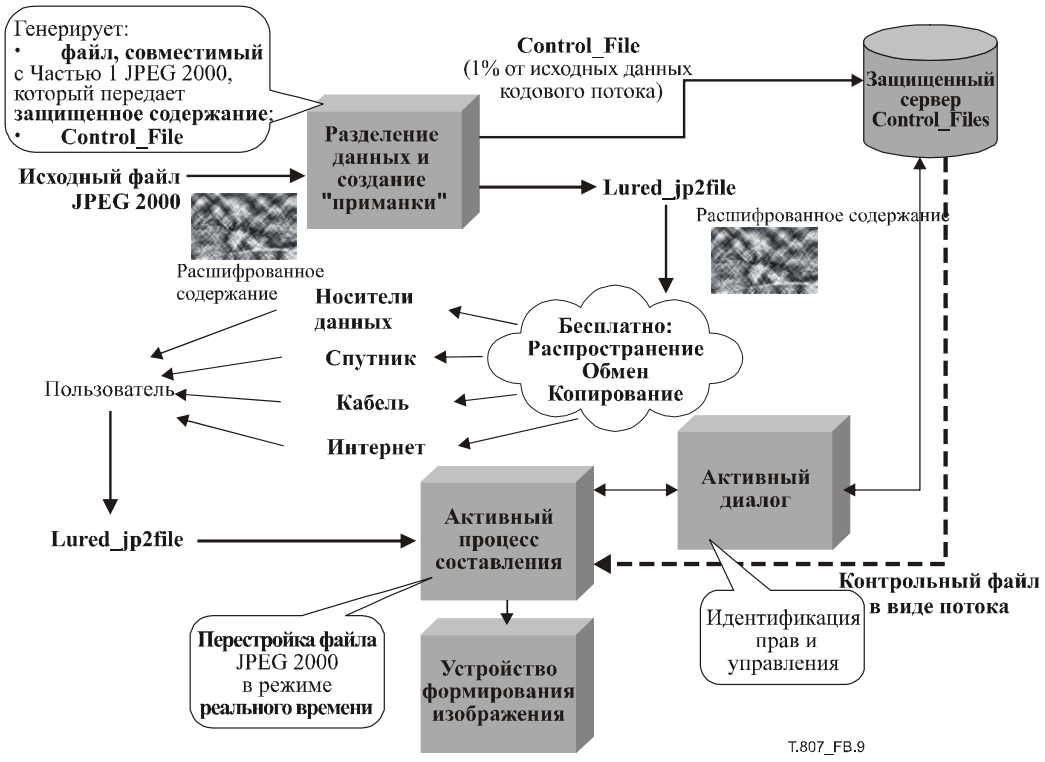


Рисунок B.9 – Обзор системы

Входной файл JPEG 2000 разделяется на два новых файла в ходе операции, называемой *Data Splitting and Luring*. Затем генерируется два новых файла: *Lured_jp2file*, передающий защищенное содержание (содержание JPSEC) и *Control_File*.

В ходе процесса Data Splitting and Luring, некоторые части исходного файла JPEG 2000 извлекаются и заменяются "приманкой". Файл Lured_jp2file передает 99% исходного содержания, в то время как последний 1% представляет собой фиктивные данные, которые называются "приманкой", т. е. данные без заранее известной связи с исходными данными. В отличие от классического шифрования, процесс создания "приманки" не основан на ключе. Любой пользователь может свободно распространять, обмениваться и копировать файл Lured_jp2file. Файл Control_File содержит 1% исходных данных, извлеченных из исходного файла. Он хранится на *Защищенном сервере Control_Files*.

Когда любое совместимое с Частью 1 JPEG 2000 устройство расшифровки расшифровывает файл Lured_jp2file, кажется, что происходит визуальное скремблирование содержания. Единственным способом получить доступ к исходному содержанию является восстановление извлеченный исходных данных благодаря Control_File. Устройство *Live_Composing* соединяется с Защищенным Сервером Control_Files посредством протокола *Live_Dialog,* затем происходит идентификация и используется протокол управления правами:

- если пользователь обладает правами или соглашается с условиями доступа к содержанию (например, оплата или подписка), извлеченные данные восстанавливаются из Control_File и исходный файл JPEG 2000 восстанавливается в режиме реального времени. Однако в соответствии с правами пользователя, восстановление исходного файла JPEG 2000 может быть частичным (например, разрешено получение доступа только к определенному элементу изображения и/или цветовому компоненту и/или к разрешению и/или границе и/или слоям качества) или полным;
- если пользователь не обладает правами или не соглашается с условиями, отображается только скремблированное содержание.

Основными чертами описанной системы являются:

- *разделение исходного файла* JPEG 2000 на два файла, причем первый передает защищенное содержание JPEG 2000 из 99% исходных данных плюс 1% фиктивных данных, называемых "приманками" (Lured_jp2file), а второй передает некоторые данные исходной информации (1%) необходимые для восстановления исходного содержания JPEG 2000;
- *визуальное скремблирование* содержания;
- *совместимость* с Частью 1 JPEG 2000 и *сохранение размера файла*;
- система защиты *с низкой битовой скоростью и низкими затратами на вычисление*.

Описываемую систему можно использовать в любом окружении и/или операционной системе. Каких-либо жестких требований к аппаратному и программному обеспечению не требуется.

Процесс Luring вставит следующий маркер SEC в файл Lured_jp2file:

Таблица B.26 – Значения параметров для данного инструмента

Параметр		Размер (биты)	Значение (по порядку)	Производное значение (смысл)
SEC		16	0xFF65	Маркер SEC
L_{SEC}		16	0xXXXX	Длина сегмента маркера SEC
Z_{SEC}		8	1 ... 255	Указатель сегмента маркера
P_{SEC} (если $Z_{SEC} = 1$)	F_{INSEC}	1	0	INSEC не используется
	$F_{multiSEC}$	1	0	Используется один сегмент маркера SEC
	F_{J2K}	2	1	Поток JPSEC, совместимый с Частью 1 JPEG 2000
	F_{TRLCP}	1	0	В данном поле не определяется использование маркера TRLCP
	N_{tools}	7	1	В кодовом потоке используется один инструмент безопасности
	I_{max}	7	1	Используется максимальный указатель экземпляра инструмента
	Дополнение	5	0	Дополнение

Таблица B.26 – Значения параметров для данного инструмента

Параметр					Размер (биты)	Значение (по порядку)	Производное значение (смысл)
Инстру-мент$^{(0)}$	t				8 (RBAS)	1	Ненормативный инструмент защиты
	i				8 (RBAS)	0	Указатель экземпляра инструмента
	ID_{RA}	$ID_{RA,id}$			32	ID	Для поставки номера ID используется RA
		$ID_{RA,nsl}$			8 (RBAS)	21	Длина $ID_{RA,ns}$ равна 21 байт
		$ID_{RA,ns}$			168	*Пространство имен*	Пространство имен RA, в котором зарегистрирован данный инструмент
	L_{ZOI}				16	*Значение длины*	Длина L_{ZOI} + ZOI
	ZOI	NZ_{ZOI}			8	0...254	Число Зон
		Зона^0	DC_{ZOI}		1	0	Далее не следует сегмент, выровненный по байтам
					1	1	Класс описания, не связанный с изображением
					6	000010	Определены указатели пакетов
			$Pzoi^{0,0}$	Mzoi	1	0	Далее не следует сегмент, выровненный по байтам
					1	0	На указанные зоны оказывает влияние метод защиты
					1	1	Определены многие элементы
					2	10	Режим указателя
					2	xx	Izoi использует 8- или 16- или 32-битное целое число
					1	0	Izoi описывается в одном измерении
				Nzoi	8	Переменное	2 ... 255 (число указателей пакетов)
				$lzoi^i$	xxx Nzoi	Переменное	Указатель пакета
	L_{PID}				16	0 ... (2^{16} – 1)	Длина L_{PID} + P_{ID} в байтах
	P_{ID}				Переменный	Переменное	ID контрольного файла , URL сервера контрольного файла и т. д.; полный синтаксис предоставляется RA

Инструменты, необходимые для выполнения процессов Data Splitting и Luring и/или Live Composing, возможно, будут предоставлены через соединение с Органом регистрации и загружены с него.

B.11 Защищенная масштабируемая потоковая передача данных и защищенная перекодировка

B.11.1 Резюме и мотивировка

В данном подпункте описывается метод для предоставления услуг защиты таких, как конфиденциальность и аутентификация кодовый потоков JPEG 2000 таким образом, который:

1) позволяет объекту (потенциально ненадежному) безопасным образом перекодировать или адаптировать защищенные потоки JPSEC, не требуя от объекта снятия защиты или расшифровки содержания; и

2) позволяет клиенту подтверждать выполнение операции по перекодировке действительным и допустимым образом.

Часто требуется, чтобы после перекодировки закодированное содержание JPEG 2000 было адаптировано к требованиям клиентов с отличающимися возможностями устройств (например, небольшой размер дисплея или сетевые соединения с низкой битовой скоростью) и сетевыми условиями изменяющегося времени. Однако если кодовые потоки JPEG 2000 не были защищены достаточно тщательно, свойство масштабируемости может быть потеряно. Например, это происходит, когда весь кодовый поток JPEG 2000 зашифровывается в один файл. В таком случае единственный способ перекодировать защищенный кодовый поток – это сначала расшифровать его, а затем перекодировать или адаптировать расшифрованный поток. Поскольку устройство перекодировки должно расшифровать содержание, это нарушает сквозную безопасность системы.

Стандарт JPSEC был разработан для обеспечения защищенной перекодировки защищенного содержания JPSEC, где защищенная перекодировка определяется как *перекодировка без снятия защиты (расшифровки) содержания*. Этого можно достичь при помощи защищенной масштабируемой потоковой передачи, которая сочетает в себе масштабируемое кодирование, шифрование, и сигнализацию таким образом, который позволяет снизить сложность, обеспечить безопасность перекодировки (потенциально ненадежным) сервером или узлом в середине сети или прокси. Это позволит JPSEC достичь казалось бы противоречащих друг другу свойств перекодировки в середине сети и сквозной безопасности. Например, На рисунке B.10 среда передачи зашифровывается у отправителя и расшифровывается только у получателя, и остается зашифрованной во всех точках между ними: (слева) узел в середине сети защищенным образом перекодирует защищенное содержание для каждого клиента JPSEC, (справа) ненадежный сервер защищенным образом осуществляет перекодировку и потоковую передачу содержания JPSEC без снятия с него защиты.

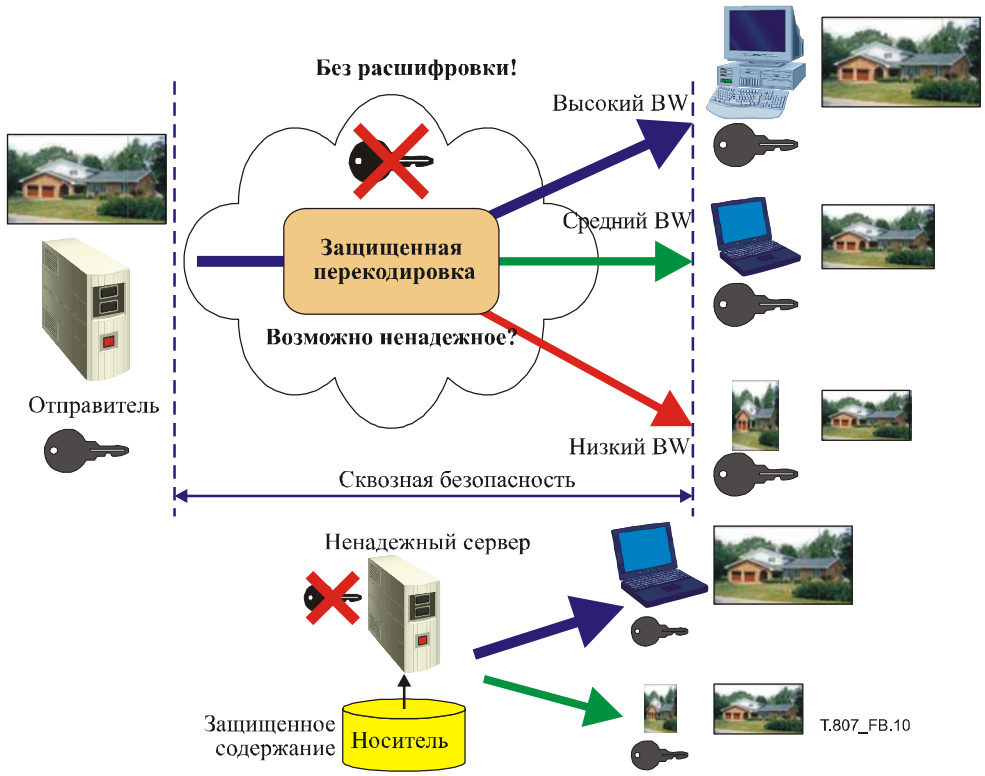


Рисунок B.10 – JPSEC активирует сквозную безопасность и безопасную перекодировку в середине сети

B.11.2 Описание работы и два примера использования

В первом примере исходный кодовый поток JPEG 2000 имеет порядок RLCP. Цель – защитить данный поток при помощи шифрования и аутентификации, обеспечив при этом защищенную перекодировку разрешения в защищенном кодовом потоке. Поскольку исходный кодовый поток JPEG 2000 используется в порядке RLCP, каждый компонент разрешения представлен смежными сегментами данных. Можно выполнить шифрование каждого из трех смежных сегментов данных. Затем в заголовке JPSEC указывается три зоны влияния, описывающие компонент разрешения, сегмент кодового потока и шаблон шифрования для каждого сегмента. Также выполняется аутентификация каждого из трех сегментов данных либо до, либо после шифрования в зависимости от требуемых функциональных возможностей. Это также указывается в заголовке SEC при помощи шаблона аутентификации.

Для того чтобы выполнить защищенное перекодирование кодового потока JPSEC, устройство перекодировки просто читает и анализирует заголовок SEC, определяет местоположение сегментов разрешения, а затем сохраняет или удаляет соответствующие сегменты данных/разрешения. Отметим, что данная операция по перекодировке соответствует простой операции анализа и не требует снятия защиты с данных. Аутентификация выполняется путем аутентификации полученных перекодированных данных со значениями MAC, которые помещаются в заголовок SEC во время процесса защиты JPSEC.

Во втором примере целью снова является обеспечение защиты кодового потока, при этом допускается перекодировка разрешения; однако данный пример несколько более сложен тем, что исходный кодовый поток JPEG 2000 имеет порядок PCRL, а не RLCP, поэтому сегменты данных, соответствующие трем компонентам разрешения, не являются смежными в исходном кодовом потоке. JPSEC позволяет осуществить защищенную перекодировку или масштабирование разрешения несколькими способами. Один из методов – зашифровать

отдельные пакеты, оставив при этом заголовки пакетов незашифрованными. Это позволит сохранить самый высокий уровень масштабируемости в потоке, но также потребует самой сложной операции по защищенной перекодировке, поскольку устройство перекодировки должен проанализировать поток JPSEC на уровне потока. Противоположной ситуацией, которая получается в ходе самой простой операции по перекодировке, является переупорядочение данных таким образом, что компоненты разрешения снова находятся в смежных сегментах, смещение которых сигнализируется в заголовке SEC. Этого можно достичь совместимым с JPEG 2000 способом путем переупорядочивания пакетов JPEG 2000 из PCRL к порядку RLCP и сигнализации нового порядка продвижения в сегменте маркера COD или изменении порядка продвижения в сегменте маркера (POC). Получающееся в результате переупорядочивание данных и защита информации показаны на рисунке B.11. И снова основной заголовок SEC содержит параметры ZOI, которые описывают соответствующие параметры, связанные с изображением и битовым потоком, соединенные с каждым сегментом данных, но на этот раз в переупорядоченном кодовом потоке.

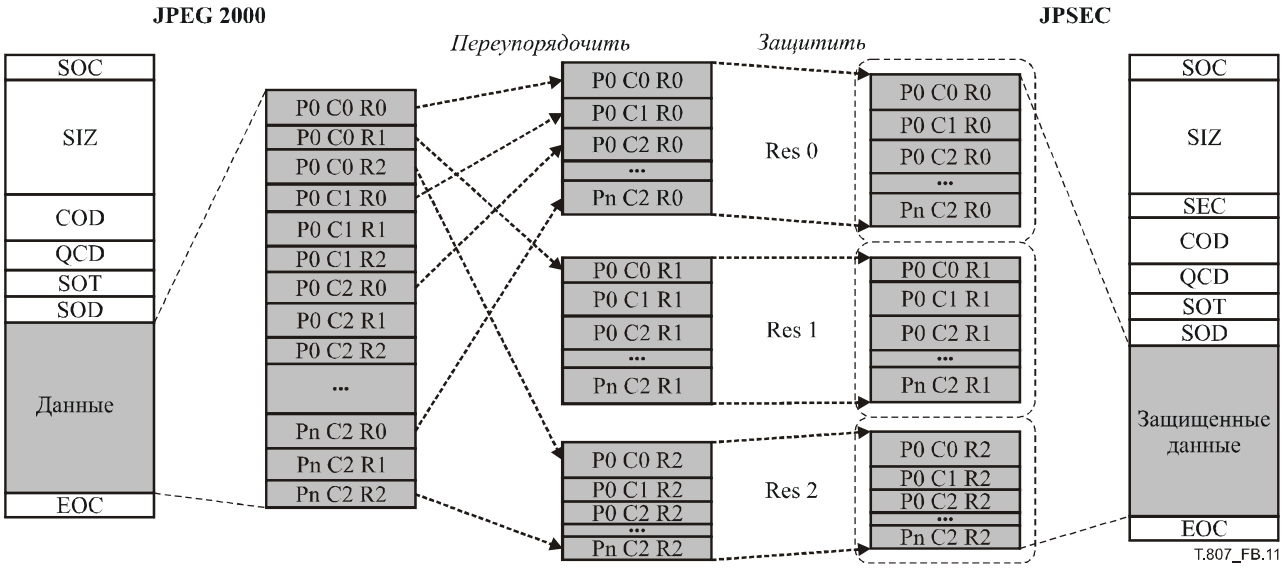


Рисунок B.11 – Пример формирования кодового потока JPSEC

B.11.3 Синтаксис кодового потока

Синтаксис JPSEC можно использовать для создания системы защищенной масштабируемой потоковой передачи и защищенной перекодировки при помощи инструмента защиты шаблона. В частности, Зону влияния (ZOI) можно использовать с шаблоном расшифровки, областью обработки и степенью структурирования для того, чтобы полностью определить процесс расшифровки, который разрешенному потребителю JPSEC следует использовать для расшифровки потока. Кроме того, параметры ZOI сигнализируют информацию, которую могут использовать узлы перекодировки для выполнения защищенной перекодировки.

ZOI определяет три зоны, по одной для каждого разрешения, и байтовые диапазоны, связанные с зашифрованными битами для каждой зоны. Синтаксис сигнализации для шаблона защиты расшифровки, области обработки и степени структурирования показан в таблице B.27. Метод расшифровки сигнализируется при помощи шаблона защиты расшифровки. В таком случае метод определяет шифрование AES в режиме CTR, а также размер блока и длина ключа. В области обработки и степени структурирования далее указывается, как выполняется расшифровка. Сигнализируется, что областью обработки является сам битовый поток, и что зашифровываются заголовки пакетов и тела пакетов. Изменяя область обработки и степень структурирования, можно задать разные методы расшифровки. Например, степенями структурирования шифрования могут быть отдельные пакеты или тела пакетов. Кроме того, в той же ZOI, что и выше, определяется метод аутентификации, но со следующим шаблоном аутентификации. Синтаксис шаблона аутентификации показан в таблице B.28, для аутентификации здесь используется HMAC с SHA-1. Конечно, можно также использовать шифры JPSEC и MAC. Кроме того, предложенное решение можно использовать с другой цифровой подписью, инструментами управления доступом и управления ключами. Кроме того, с каждым пакетом (или с другой зоной данных) может быть связано искажение при помощи поля искажений (см. п. 5.7.3.2) для обеспечения защищенной потоковой передачи, оптимизированной по уровню искажений (R-D), и защищенной перекодировки [26], [27] и [28].

Таблица B.27 – Значения параметров для инструмента защиты шаблона, области обработки и степени структурирования

Параметр			Размер (биты)	Значение (по порядку)	Производное значение (смысл)
T_{decry}	ME_{decry}		8	0	Флаг эмуляции маркера равен NULL
	CT_{decry}		16	1	Шифрование AES
	CP_{decry}	M_{bc}	6	$10\ 0101_b$	CTR и отсутствие дополнения
		P_{bc}	2	0	Для режима CTR дополнение (битами) не используется
		SIZ_{bc}	8	128	Размер блока равен 128 бита
		KT_{bc}	Переменный	*Шаблон ключей*	Шаблон информации о ключе
PD			1	0_b	Далее не следует сегмент, выровненный по байтам (BAS)
			1	0_b	Не в области пикселов
			1	0_b	Не в области вейвлет-коэффициента
			1	0_b	Не в области квантованного вейвлет-коэффицента
			1	1_b	Обрабатывается в области кодового потока
			3	000_b	Не используется
G		PO	16	$0\ 0000\ 0101\ 0011\ 100_b$	Порядок обработки – TRLCP
		GL	8	$0000\ 1001_b$	Степень структурирования – это весь участок, определяемый ZOI
V		N_V	16	1	Определено одно значение
		S_V	8	16	Размер равен 16 байтам
		VL	128	*Текущее значение*	Значение счетчика для режима CTR

Таблица B.28 – Значения параметров для инструмента защиты шаблона аутентификации

Параметр			Размер (биты)	Значение (по порядку)	Производное значение (смысл)
T_{auth}	M_{auth}		8	0	MAC на основе хэш-функции
	P_{auth}	M_{HMAC}	8	1	HMAC
		H_{HMAC}	8	1	ID хэш-функции – SHA-1
		KT_{HMAC}	Переменный	*Значение ключа*	См. шаблон ключей
		SIZ_{HMAC}	16	80	Размер MAC равен 80 битам (укороченное 160)

B.11.4 Заключение

В данном подпункте описывается защищенная масштабируемая потоковая передача и защищенная перекодировка при помощи JPSEC, что позволяет совместить два казалось бы противоречащих друг другу свойства сквозной безопасности и защищенной перекодировки в узлах в середине сети. Это позволяет перекодировать кодовый поток JPSEC *без необходимости расшифровки*. Кроме того, данный метод предоставляет аутентификацию того, что перекодировка осуществлялась только действительным и допустимым образом, и какого-либо случайного или злонамеренного изменения не произошло. Это позволяет (потенциально ненадежному) серверу или узлу в середине сети такому, как прокси, выполнять защищенную перекодировку, позволяя при этом потребителю JPSEC аутентифицировать, что полученное содержание было перекодировано действительным и допустимым образом.

Приложение C

Функциональная совместимость

(Данное приложение является неотъемлемой частью данной Рекомендации | Международного стандарта)

C.1 Часть 1

Для создания кодовых потоков JPSEC, которые точно соответствуют Части 1 JPEG 2000, к кодовому потоку JPEG 2000 можно применить несколько методов защиты. Мы используем термин "совместимость с Частью 1" для обозначения кодовых потоков JPSEC, которые имеют четко определенный режим работы для устройств расшифровки Части 1 JPEG 2000, включая те, которые не осведомлены о JPSEC.

Устройство расшифровки Части 1 JPEG 2000 будет пропускать сегменты маркера, которые оно не распознает. Инструмент JPSEC такой, как нормативный инструмент JPSEC для аутентификации, вставляет значения кода аутентификации сообщения, которые вычисляются из данных JPEG 2000, в сегмент маркера SEC наряду с параметрами, описывающими определенные методы аутентификации, которые может использовать потребитель JPSEC. Данные параметры и значения сообщают потребителю JPSEC, как подтверждать подлинность полученного кодового потока JPSEC. Отметим, что инструмент аутентификации JPSEC не манипулирует данными JPEG 2000. Таким образом, устройство расшифровки Части 1 JPEG 2000, получающее данный кодовый поток JPSEC, начнет расшифровку потока JPSEC, затем оно пропустит сегмент маркера SEC и продолжит расшифровывать поток JPSEC, как если бы он был потоком Части 1 JPEG 2000. Нормативный инструмент JPSEC для аутентификации также использует данные характеристики, что, таким образом, также приводит к получению кодового потока, совместимого с Частью 1.

JPSEC позволяет выполнять шифрование и расшифровку кодовых потоков JPEG 2000 и JPSEC. Когда используется шифрование, данные JPEG 2000, конечно, изменяются. Строго говоря, совместимость с Частью 1 невозможна при зашифрованных потоках, поскольку, скорее всего, в результате устройство расшифровки Части 1 JPEG 2000 будет видеть неверные значения. Одним из возможных способов преодоления или, по крайней мере, смягчения данной проблемы является использование возможностей устойчивости к ошибкам JPEG 2000. Используя устойчивость к ошибкам, можно получить зашифрованные кодовые потоки JPSEC, имеющие определенный режим работы для устройств расшифровки Части 1 JPEG 2000.

В JPSEC имеется поле параметра P_{SEC}, которое содержит параметры безопасности для всего кодового потока. Это поле включает в себя флаг F_{J2K}, который может быть установлен на 1 для обозначения того, что кодовый поток JPSEC не поддается расшифровке устройствами расшифровки Части 1 JPEG 2000. Создатель JPSEC может установить данный параметр при применении инструментов JPSEC к кодовому потоку JPEG 2000. Как уже было сказано, создатель JPSEC может принять защищенный кодовый поток JPSEC в качестве входных данных. Если создатель получает в качестве входных данных кодовый поток JPSEC, который имеет флаг, который указывает на совместимость с Частью 1, а затем применяет инструмент JPSEC, который теряет часть совместимости с Частью 1, флаг F_{J2K} должен быть установлен на 0.

Для потоков JPSEC, которые не являются совместимыми с Частью 1, рекомендуется использовать расширение файла .jp2s для обозначения того, что устройство расшифровки Части 1 JPEG 2000 не сможет расшифровать защищенный кодовый поток.

C.2 Часть 2

Поправку 2 к Части 2 JPEG 2000 по сегменту маркера с расширенными возможностями (CAP) можно использовать для обозначения того, что используется JPSEC. В частности, в Части 2 для обозначения присутствия сегмента маркера CAP, который содержит параметр C_{cap}, используется параметр R_{siz}. Данный параметр можно использовать для сигнализации того, какие части JPEG 2000 используются в кодовом потоке. Путем установки соответствующего бита в параметре C_{cap} можно определить, что используется Часть 8 JPEG 2000 (JPSEC).

Таким образом, создатель JPSEC может установить параметр R_{siz} таким образом, чтобы он обозначал присутствие сегмента маркера CAP. Он может вставить или редактировать сегмент маркера CAP так, чтобы параметр C_{cap} указывал на использование Части 8.

C.3 JPIP

C.3.1 Общая взаимосвязь между JPIP и JPSEC

JPIP определяет протокол, состоящий из структурированных серий взаимодействий между клиентом и сервером, посредством которых может осуществляться полный или частичный обмен метаданными файла, структурой или потоками кода изображения.

JPIP также можно адаптировать при помощи различных расширений к формату файла JPEG 2000, как определено в Рек. МСЭ-Т Т.801 | ИСО/МЭК 15444-2, Рек. МСЭ-Т Т.802 | ИСО/МЭК 15444-3 и Рек. МСЭ-Т Т.805 | ИСО/МЭК 15444-6. Однако для достижения простого уровня согласованности действий, который позволяет передавать отдельный файлы JPEG 2000 или кодовые потоки, данные дополнительные возможности не являются обязательными.

Для поддержки современных стандартов Рек. МСЭ-Т Т.802 | ИСО/МЭК 15444-3, стандарта Motion JPEG 2000 и Рек. МСЭ-Т Т.805 | ИСО/МЭК 15444-6, Составных Документов и будущих частей JPEG 2000 (сейчас JP3D, JPSEC и JPWL) в JPEG 2000 были включены возможности расширения протокола JPIP.

JPSEC предоставляет услуги безопасности для изображений JPEG 2000. Синтаксис JPSEC поддерживает два типа маркеров: SEC и INSEC. В основном заголовке битового потока JPSEC появляется один или несколько маркеров SEC. Другими словами, JPSEC потребляет кодовый поток JPEG 2000, изменяет основной заголовок JPEG 2000 и формирует новый "основной заголовок" JPSEC, а затем модифицирует соответствующий поток данных JPEG 2000, в результате чего получается новый защищенный поток данных. Маркеры INSEC могут необязательно появляться в "части данных" потока данных. По сравнению с маркером SEC они определяют параметры "меньшего размера" или "ограниченной области", их можно использовать для дополнения маркера SEC.

Было замечено, что JPIP находится чуть ниже транспортного уровня, в то время как JPSEC находится на уровне приложений. С этой точки зрения JPIP оказывает транспортные услуги JPSEC. То есть JPIP предлагает эффективные инструменты для передачи между серверами и клиентами информации об изображении, включая основной заголовок (всех маркеров) и кодовые потоки. В данном подпункте рассматривается использование JPIP для передачи содержания JPSEC.

C.3.2 Определенные вопросы взаимодействия между JPIP и JPSEC

В данном подпункте описываются проблемы, которые должны учитывать отправитель и получатель JPIP при передаче содержания JPSEC.

В п. A.3.5 "Буфер данных основного заголовка" Рек. МСЭ-Т Т.808 | ИСО/МЭК 15444-9 типы сред передачи потоков JPP- и JPT- используют буфер данных основного заголовка. Этот буфер данных состоит из объединенного списка всех маркеров и сегментов маркеров в основном заголовке, начиная с маркера SOC. Буфер не содержит маркеров SOT, SOD или EOC. Однако основной заголовок JPEG 2000 не включает в себя маркер SEC и его сегмент. В результате в п. A.3.5 JPIP FCD 2.0 не определяется поддержка сегмента маркера SEC, определенного в JPSEC. Таким образом, отправитель и получатель JPIP должны быть изменены таким образом, чтобы они могли распознавать сегмент(ы) маркера SEC, которые появляются в основном заголовке кодового потока JPSEC.

В п. A.3.2 "Буферы данных о границе" Рек. МСЭ-Т Т.808 | ИСО/МЭК 15444-9 описывается поддержка данных о границе. Однако п. A.3.2 JPIP FCD 2.0 не определяет поддержку маркера INSEC и его сегмента, определенного в JPSEC. Таким образом, отправитель и получатель JPIP должны быть изменены таким образом, чтобы они могли распознавать сегмент(ы) маркера INSEC, которые могут появиться в части данных кодового потока JPSEC.

В п. A.3.3 "Буферы данных о заголовке элемента изображения" Рек. МСЭ-Т Т.808 | ИСО/МЭК 15444-9 буферы данных о заголовке элемента изображения появляются только в типе среды передачи потока JPP. Для буферов данных, принадлежащих к этому классу, внутриклассовый идентификатор содержит указатель (начинающийся с 0) элемента изображения, к которому относится буфер данных. Этот буфер данных состоит из маркеров и сегментов маркеров для элемента изображения n. Он не должен содержать сегмент маркера SOT. Включение маркеров SOD не является обязательным. Этот буфер данных может быть сформирован из разрешенного кодового потока путем объединения всех сегментов маркеров, кроме SOT и POC во всех заголовках части элемента изображения для элемента изображения n.

В п. A.3.4 "Буферы данных об элементе изображения" Рек. МСЭ-Т Т.808 | ИСО/МЭК 15444-9 буферы данных об элементе изображения должны использоваться только вместе с типом среды передачи потока JPT. Для буферов данных, принадлежащих к этому классу, внутриклассовый идентификатор содержит указатель (начинающийся с 0) элемента изображения, к которому относится буфер данных. Каждый буфер данных об элементе изображения соответствует строке байтов, сформированной путем объединения по порядку всех частей элементов изображения, принадлежащих данному элементу изображения, вместе с SOT, SOD и всеми остальными важными сегментами маркеров.

Как было упомянуто выше, в пп. A.3.4 и A.3.5 Рек. МСЭ-Т Т.808 | ИСО/МЭК 15444-9 описывается поддержка заголовка части элемента изображения и данных части элемента изображения. Однако в пп. A.3.4 и A.3.5 Рек. МСЭ-Т Т.808 | ИСО/МЭК 15444-9 не указывается, поддерживают ли они сегменты маркеров SEC и INSEC. Таким образом, отправитель и получатель JPIP должны быть изменены таким образом, чтобы распознавать и передавать данные сегменты маркеров наряду с защищенными данными.

C.3.3 Резюме

Как правило, JPSEC подходит для передачи посредством JPIP. Маркер INSEC используется в кодовом потоке для описания некоторой "небольшой" части определенных данных, защищаемых при помощи инструмента(ов) безопасности. Это делает JPSEC более гибким. Чтобы повысить надежность INSEC, служебному уровню (в данный момент мы имеем в виду JPIP) следует обеспечить хорошее Качество обслуживания или защиту маркера INSEC и его сегмента. Для того чтобы достичь этой цели, JPIP и JPSEC необходимо проработать некоторые вопросы и удостовериться в согласованности действий между JPIP и JPSEC.

C.4 JPWL

Стандарт Беспроводной JPEG 2000 или JPWL (Рек. МСЭ-Т Т.810 | ИСО/МЭК 15444-11) расширяет основную спецификацию JPEG 2000 для достижения эффективной передачи изображений JPEG 2000 через подверженную ошибкам среду передачи. В частности, JPWL определяет набор инструментов и методов для защиты кодового потока от ошибок при передаче. Данный стандарт также определяет средства для описания чувствительности кодового потока к ошибкам при передаче, а также для описания мест кодового потока с остаточными ошибками при передаче.

JPWL особенно направлено на защиту заголовка изображения, коды Упреждающей коррекции ошибок (FEC), Неравномерной защиты от ошибок (UEP), объединенное кодирование канала-источника, разделение и чередование данных, а также надежное арифметическое кодирование. JPWL не связан с определенной сетью или транспортным протоколом, но предоставляет общее решение для надежной передачи изображений JPEG 2000 через подверженные ошибкам сети.

Основными функциональными возможностями JPWL являются:

- защита кодовых потоков от ошибок при передаче;
- описание степени чувствительности различных частей кодового потока к ошибкам при передаче;
- описание мест остаточных ошибок в кодовом потоке.

JPWL определяет четыре сегмента маркера: Возможность защиты от ошибок (EPC), Блок защиты от ошибок (EPB), Дескриптор чувствительности к ошибкам (ESD) и Дескриптор остаточных ошибок (RED).

Сегмент маркера EPC указывает на то, какие нормативные и информативные инструменты JPWL используются в данном кодовом потоке. В частности, EPC сигнализирует, присутствуют ли в данном кодовом потоке остальные три нормативных сегмента маркера, определенные JPWL, а именно Дескриптор чувствительности к ошибкам (ESD), Дескриптор остаточных ошибок (RED) и Блок защиты от ошибок (EPB). Кроме того, EPC сигнализирует об использовании информативных инструментов, которые ранее были зарегистрированы в RA JPWL. Наличие EPC является обязательным для кодового потока JPWL.

Основной функцией EPB является защита Основного заголовка и Заголовка части элемента изображения. Однако его также можно использовать для защиты оставшейся части кодового потока. Сегмент маркера EPB содержит информацию о параметрах защиты от ошибок и данные об избыточности, используемые для защиты кодового потока от ошибок.

Сегмент маркера ESD содержит информацию о чувствительности кодового потока к ошибкам. Данную информацию можно использовать при применении метода Неравномерной защиты от ошибок (UEP). Для защиты самой чувствительной части кодового потока используются более мощные коды. Данную информацию можно также использовать для выборочной передачи. И, наконец, информацию, передаваемую в ESD, можно также использовать для других приложений не-JPWL таких, как эффективная перекодировка скорости или интеллектуальная предварительная выборка.

Сегмент маркера RED сигнализирует о присутствии в кодовом потоке остаточных ошибок. В действительности устройство расшифровки JPWL может не суметь скорректировать все ошибки в кодовом потоке. RED позволяет сигнализировать о месторасположении таких остаточных ошибок. Затем данную информацию может использовать устройство расшифровки JPEG 2000 для того, чтобы лучше справляться с ошибками. Например, устройство расшифровки может запросить повторную передачу, замаскировать ошибки или удалить поврежденную информацию.

C.4.1 Общая взаимосвязь между JPWL и JPSEC

Комбинация JPWL и JPSEC требуется, когда нужно обеспечить безопасность и передачу изображений JPEG 2000 по подверженному ошибкам беспроводному каналу.

Со стороны передатчика чувствительность к ошибкам JPWL обычно генерируется во время шифрования JPEG 2000. Затем к кодовому потоку применяются инструменты JPSEC для того, чтобы защитить его. В конце, для того чтобы сделать кодовый поток более устойчивым к ошибкам при передаче, применяются инструменты шифрования JPWL.

Со стороны получателя сначала применяются инструменты расшифровки JPWL для коррекции возможных ошибок при передаче. Во время этого этапа JPWL может также генерировать информацию об остаточных ошибках. В конце, для того чтобы оказать выбранные услуги безопасности, применяются инструменты JPSEC.

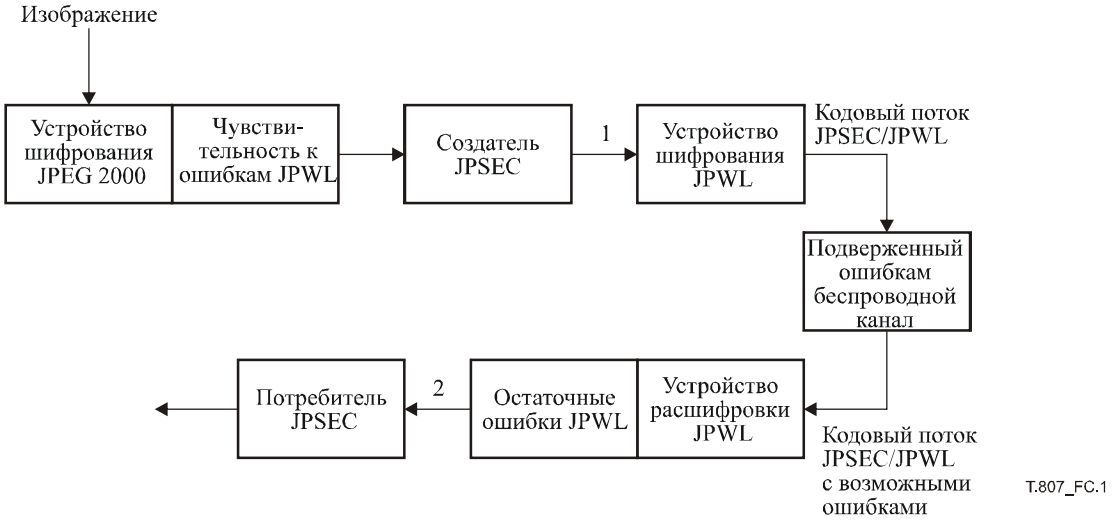


Рисунок C.1 – Типичная комбинация JPWL и JPSEC

C.4.2 Определенные вопросы взаимодействия между JPWL и JPSEC

При взаимодействии JPWL и JPSEC следует учитывать несколько аспектов:

1) Возможность защиты от ошибок JPWL (EPC): Присутствие данного сегмента маркера повлияет на байтовые диапазоны. Отметим, что данный сегмент маркера является обязательным в кодовом потоке JPWL.

2) Блок защиты от ошибок JPWL (EPB): Данный сегмент маркера обычно добавляется на последнем этапе на передатчике и удаляется на первом этапе на приемнике. В принципе, данный сегмент маркера не должен влиять на JPSEC.

3) Дескриптор чувствительности к ошибкам JPWL (ESD): Данный сегмент маркера обычно добавляется во время шифрования Части 1 JPEG 2000. В таком случае он будет прозрачным для последующих операций JPSEC. Однако JPSEC может негативно влиять на использование ESD в JPWL. В частности, JPSEC не должен менять байтовые диапазоны при использовании ESD байтовых диапазонов. Кроме того, операции JPSEC не должны влиять на значения искажения; в противном случае информация, передаваемая в ESD, становится нерелевантной. В последнем случае создатель JPSEC имеет возможность удалить сегмент маркера ESD.

4) Дескриптор остаточных ошибок JPWL (RED): Данный сегмент маркера может быть вставлен после расшифровки JPWL. Поэтому он может повлиять на байтовые диапазоны JPSEC. Также он может оказывать влияние на методы аутентификации JPSEC. В случае появления искажений в кодовом потоке информация RED может оказаться полезной потребителю JPSEC для соответствующей обработки искаженного кодового потока.

5) SEC JPSEC: Присутствие данного сегмента маркера повлияет на байтовые диапазоны. Отметим, что данный сегмент маркера является обязательным в кодовом потоке JPSEC.

6) INSEC JPSEC: Присутствие данного сегмента маркера повлияет на байтовые диапазоны. Отметим, что данный сегмент маркера появляется в данных кодового потока.

В случае отсутствия остаточных ошибок, устройства шифрования и расшифровки JPWL в идеале должны быть прозрачными. Другими словами, в таком случае, потоки в точках 1 и 2 на рисунке, приведенном выше, должны быть строго идентичными.

В качестве общей рекомендации, при использовании в комбинации с JPWL, предпочтительно, чтобы JPSEC использовал байтовые диапазоны, начинающиеся после маркера SOD, для того чтобы минимизировать проблемы с байтовыми диапазонами. Кроме того, предпочтительнее ограничить присутствие сегментов маркера JPWL до Основного заголовка и избежать их присутствия в Заголовках части элемента изображения.

Приложение D

Заявление о выдаче патента

(Данное приложение не является неотъемлемой частью данной Рекомендации | Международного стандарта)

ПРИМЕЧАНИЕ. – Приложение D является приложением только к ИСО/МЭК. Компании, подающие в МСЭ заявки на выдачу патента, касающиеся данного текста, перечислены в базе данных IPR. Смотрите: http://itu.int/ITU-T/ipr/.

Международная организация по стандартизации (ИСО) и Международная электротехническая комиссия (МЭК) обращают внимание на то, что совместимость с данной частью ИСО/МЭК 15444 может подразумевать использование патентов.

У ИСО и МЭК нет определенной позиции, касающейся доказательства, действительности и области применения данных патентных прав.

Обладатели данных патентных прав уверили ИСО и МЭК, что они готовы вести переговоры о выдаче лицензии на разумных и непредвзятых условиях с заявителями со всего мира. В этом отношении утверждения обладателями данных патентных прав регистрируются в ИСО и МЭК. Информацию можно получить в компаниях, перечисленных ниже.

Обращаем Ваше внимание на то, что возможно подпадание некоторых элементов данной части ИСО/МЭК 15444 под патентные права, не обозначенные в данном приложении. ИСО и МЭК не несут ответственности за определение каких-либо или всех подобных патентных прав.

Таблица D.1 – Список утверждений

Число	Объекты, подающие заявления о выдаче патента
1	Корпорация Canon
2	Колумбийский университет
3	EMITALL Surveillance
4	HP
5	Институт исследований Infocomm
6	MediaLive
7	Технологический институт Нью-Джерси

БИБЛИОГРАФИЯ

[1] ITU-T Recommendation X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications.*

ISO/IEC 7498-2:1989, *Information Processing Systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture*.

[2] ISO/IEC 9796-2:2002, *Information technology – Security techniques – Digital signature schemes giving message recovery – Part 2: Integer factorization based mechanisms*.

[3] ISO/IEC 9797-1:1999, *Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher*.

[4] ISO/IEC 9798-1:1997, *Information technology – Security techniques – Entity authentication – Part 1: General*.

[5] ISO/IEC 10118-1:2000, *Information technology – Security techniques – Hash-functions – Part 1: General*.

[6] ISO/IEC 10118-2:2000, *Information technology – Security techniques – Hash-functions – Part 2: Hash-functions using an n-bit block cipher*.

[7] ISO/IEC 10118-3:2004, *Information technology – Security techniques – Hash-functions – Part 3: Dedicated hash-functions*.

[8] ISO/IEC 10118-4:1998, *Information technology – Security techniques – Hash-functions – Part 4: Hash-functions using modular arithmetic*.

[9] ISO/IEC 11770-1:1996, *Information technology – Security techniques – Key management – Part 1: Framework*.

[10] ISO/IEC 11770-2:1996, *Information technology – Security techniques – Key management – Part 2: Mechanisms using symmetric techniques*.

[11] ISO/IEC 11770-3:1999, *Information technology – Security techniques – Key management – Part 3: Mechanisms using asymmetric techniques*.

[12] ISO/IEC 13335-1:2004, *Information technology – Security techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management*.

[13] ISO/IEC TR 13335-4:2000, *Information technology – Guidelines for the management of IT Security – Part 4: Selection of safeguards*.

[14] ISO/IEC 14888-1:1998, *Information technology – Security techniques – Digital signatures with appendix – Part 1: General*.

[15] ISO/IEC 14888-3:1998, *Information technology – Security techniques – Digital signatures with appendix – Part 3: Certificate-based mechanisms*.

[16] ISO/IEC 15946-2:2002, *Information technology – Security techniques – Cryptographic techniques based on elliptic curves: Part 2 – Digital signatures*.

[17] ISO/IEC 15946-3:2002, *Information technology – Security techniques – Cryptographic techniques based on elliptic curves: Part 3 – Key establishment*.

[18] ISO/IEC 15946-4:2004, *Information technology – Security techniques – Cryptographic techniques based on elliptic curves: Part 4 – Digital signatures giving message recovery*.

[19] ISO/IEC 18033-2:2006, *Information technology – Security techniques – Encryption algorithms – Part 2: Asymmetric ciphers*.

[20] ISO/IEC 18033-3:2005, *Information technology – Security techniques – Encryption algorithms – Part 3: Block ciphers*.

[21] ISO/IEC 18033-4:2005, *Information technology – Security techniques – Encryption algorithms – Part 4: Stream ciphers*.

[22] DWORKIN (Morris): Recommendation for Block Cipher Modes of Operation, Methods and Techniques, *NIST Special Publication 800-38A*.

[23] GROSBOIS (R.), GERBELOT (P)., EBRAHIMI (T.): Authentication and access control in the JPEG 2000 compressed domain, *In Proc. of the SPIE 46th Annual Meeting, Applications of Digital Image Processing XXIV*, San Diego, 29 July–3 August, 2001.

[24] http://java.sun.com/j2se/1.4.2/docs/guide/security/CryptoSpec.html, Java Cryptography Architecture API Specification and reference.

[25] RIVEST (R.L.), SHAMIR (A.), ADLEMAN (L.M.): A method for obtaining digital signatures and public-key cryptosystems, *Communications of the ACM (2) 21*, 1978, Page(s): 120–126.

[26] WEE (S.), APOSTOLOPOULOS (J.): Secure Scalable Video Streaming for Wireless Networks, *IEEE Inter. Conf. on Acoustics, Speech, and Signal Processing (ICASSP)*, March 2001. Also available at www.hpl.hp.com/personal/John_Apostolopoulos/papers/SecureScalableStreaming_ICASSP01.pdf.

[27] WEE (S.), APOSTOLOPOULOS (J.): Secure Scalable Streaming Enabling Transcoding Without Decryption, *IEEE Inter. Conf. on Image Processing (ICIP)*, http://lib.hpl.hp.com/techpubs/2001/HPL_2001_320.html Sept. 2001.

[28] WEE (S.), APOSTOLOPOULOS (J.): Secure Scalable Streaming and Secure Transcoding with JPEG 2000, *IEEE Inter. Conf. on Image Processing (ICIP)*, Sept. 2003. http://lib.hpl.hp.com/techpubs/2003/HPL-2003-117.html.

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия A	Организация работы МСЭ-Т
Серия D	Общие принципы тарификации
Серия E	Общая эксплуатация сети, телефонная служба, функционирование служб и человеческие факторы
Серия F	Нетелефонные службы электросвязи
Серия G	Системы и среда передачи, цифровые системы и сети
Серия H	Аудиовизуальные и мультимедийные системы
Серия I	Цифровая сеть с интеграцией служб
Серия J	Кабельные сети и передача сигналов телевизионных и звуковых программ и других мультимедийных сигналов
Серия K	Защита от помех
Серия L	Конструкция, прокладка и защита кабелей и других элементов линейно-кабельных сооружений
Серия M	Управление электросвязью, включая СУЭ и техническое обслуживание сетей
Серия N	Техническое обслуживание: международные каналы передачи звуковых и телевизионных программ
Серия O	Требования к измерительной аппаратуре
Серия P	Качество телефонной передачи, телефонные установки, сети местных линий
Серия Q	Коммутация и сигнализация
Серия R	Телеграфная передача
Серия S	Оконечное оборудование для телеграфных служб
Серия T	**Оконечное оборудование для телематических служб**
Серия U	Телеграфная коммутация
Серия V	Передача данных по телефонной сети
Серия X	Сети передачи данных, взаимосвязь открытых систем и безопасность
Серия Y	Глобальная информационная инфраструктура, аспекты межсетевого протокола и сети последующих поколений
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Отпечатано в Швейцарии
Женева, 2007 г.