Министерство образования и науки Украины
Харьковский национальный университет радиоэлектроники

На правах рукописи

КОМОЛОВ ДМИТРИЙ ИВАНОВИЧ

УДК 621.327: 681.5

МЕТОД ПОВЫШЕНИЯ ПРОПУСКНОЙ СПОСОБНОСТИ ЗАКРЫТОГО ВИДЕОКАНАЛА ДЛЯ ВЕДОМСТВЕННЫХ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ

05.12.02 – телекоммуникационные системы и сети

Диссертация на соискание ученой степени
кандидата технических наук

Научный руководитель:
Баранник Владимир Викторович
доктор технических наук, профессор

Ідентичність всіх примірників дисертації
ЗАСВІДЧУЮ:
Вчений секретар спеціалізованої
вченої ради Д 35.052.10

/І.В. Демидов/

Харьков – 2016

СОДЕРЖАНИЕ

ПЕРЕЧЕНЬ УСЛОВНЫХ СОКРАЩЕНИЙ

JPEG (Joint Photographic Experts Group) – Метод сжатия изображений и соответствующий графический формат;

MPEG (Moving Picture Experts Group) – Стандарт сжатия и передачи цифровой видео и аудио информации;

PSNR (Peak signal-to-noise ratio) – Пиковое отношение сигнал/шум;

HD (High Definition) – Широкоэкранный формат видеоизображения;

RGB (Red, Green, Blue) – Аддитивная цветовая модель, как правило, описывающая способ синтеза цвета для цветовоспроизведения;

RLE (Rn-Length Encoding) – Групповое кодирование;

YCrCb – Цветовое пространство, которое используется для передачи цветных изображений в компонентном видео и цифровой фотографии;

ДКП – Дискретно косинусное преобразование;

ТКС – Телекоммуникационная система;

ВКС – Видеоконференцсвязь;

МВД – Министерство внутренних дел;

ОВД – Органы внутренних дел;

ЕЦВТС – Единая цифровая ведомственная телекоммуникационная сеть.

ВВЕДЕНИЕ

Актуальность темы. Информационные системы, используемые в органах внутренних дел Украины, позволяют повысить эффективность управления, раскрываемость преступлений и оказание услуг населению. Они должны обеспечивать сотрудников необходимой актуальной, систематизированной информацией. Ключевой составляющей информационного обеспечения является видеоинформационная составляющая. В состав видеоинформационной составляющей входят системы видеонаблюдения и видеоконференцсвязи. Так в 2012 году в МВД была построена ведомственная система видеоконференцсвязи на базе ЕЦВТС, которая постоянно модернизируется и расширяется. А в 2013 году построена система видеоконференцсвязи между подразделениями МВД, прокуратуры и судами для трансляции проведения следственных действий. В поддержку внедрения техники видеонаблюдения и видеоконференцсвязи в органах внутренних дел Украины принят ряд нормативно-правовых актов, которые регламентируют законность, порядок применения и функционирования, а также требования, предъявляемые к этим системам. В соответствии с законом Украины «О защите информации в информационно-телекоммуникационных системах» вся информация, которая является собственностью государства, или информация с ограниченным доступом, требования относительно защиты которой, установлены законом, должна обрабатываться в системе с применением комплексной системы защиты информации с подтвержденным соответствием. В силу того, что вся информация, обрабатываемая в МВД, в том числе аудио и видео, является служебной, она требует обеспечения надежной защиты. На основе нормативно-правовых документов разработаны требования, предъявляемые к ведомственным видеоинформационным системам. Основными требованиями являются: обеспечение качественного предоставления видеосервиса, оперативная доставка видеоинформационных потоков, обеспечение необходимого уровня надежной защиты. В то же время существуют проблемы, которые необходимо решать для обеспечения выполнения

ведомственных требований к видеоинформационным сервисам. К ним относятся: использование низкоскоростных каналов связи, использование видеооборудования низкого качества, отсутствие систем технической защиты информации.

Выполнение ведомственных требований с помощью используемого видеооборудования и передача закрытых видеоинформационных потоков по существующим низкоскоростным каналам связи обеспечивается необходимый уровень конфиденциальности только для проведения сеансов видеоконференцсвязи низкого качества. Значит, существует противоречие, обусловленное наличием дисбаланса между требованиями к ведомственным видеоинформационным сервисам и пропускной способностью сети. Поэтому повышение качества видеоинформационного сервиса для ведомственных инфокоммуникационных сетей в условиях обеспечения заданной конфиденциальности является ***актуальной научно-прикладной задачей***.

Преодоление дисбаланса между реальной интенсивностью закрытого видеопотока и пропускной способностью сети достигается за счет снижения интенсивности видеопотока и применения надежных и простых в реализации методов скрытия, обеспечивающих требуемый уровень конфиденциальности.

В зависимости от доступной скорости передачи данных и качества реконструируемых видеоинформационных потоков интенсивность передаваемых закрытых видеоданных необходимо снизить в среднем на 10 – 50 %. Следовательно, ***цель исследований*** заключатся в разработке метода повышения пропускной способности закрытого видеоканала для ведомственных телекоммуникационных систем в условиях обеспечения заданной конфиденциальности.

Для этого требуется создать метод закрытия видеопотока, характеризующийся такой функциональной зависимостью, для которой обеспечивается требование по снижению интенсивности при выполнении условий по достоверности и конфиденциальности.

Отсюда **тематика диссертационных исследований,** заключающаяся в создании метода повышения пропускной способности закрытого видеоканала для ведомственных инфокоммуникационных систем, является актуальной.

Связь работы с научными программами, планами, темами. Диссертационные исследования связаны со следующими программами и нормативными документами: Закона Украины «Про Концепцію Національної програми інформатизації» от 04.02.1998 № 75/98-ВР, Концепции развития связи Украины от 9.12.1999 р. N 2238, Национальных космических программ Украины от 30.09.2008 N 608-VI, планами научной, научно-технической деятельности Харьковского национального университета радиоэлектроники, в рамках которых была виполнена НДР “Технології створення інтегрованих інформаційних систем на основі мереж цифрового мобільного зв’язку” (№ 0113U000360), в которой автор диссертации был исполнителем.

Цель работы: разработка метода повышения пропускной способности закрытого видеоканала для ведомственных телекоммуникационных систем в условиях обеспечения заданной конфиденциальности.

Задачи исследований:

1. Обоснование направления совершенствования селективной технологии закрытия видеопотока для повышения качества видеосервисов в ведомственных инфокоммуникационных системах;
2. Разработка метода повышения пропускной способности закрытого видеоканала на основе шифрования энергетически значимых структурных единиц базового видеокадра;
3. Разработка метода реконструкции закрытого видеопотока на основе учета требований относительно особенностей формирования кодовых конструкций компрессионного представления и кодограмм блочных симметричных шифров;
4. Разработка программной реализации созданных методов и проведение сравнительной оценки их эффективности с учетом уровня интенсивности кодированного видеопотока.

Объект исследования: процесс повышения качества предоставления видеосервисов с учетом обеспечения необходимого уровня конфиденциальности в ведомственных инфокоммуникационных системах.

Предмет исследования: методы повышения пропускной способности закрытого видеоканала на основе технологий кодирования и цифровой

обработки видеопотока для ведомственных систем предоставления видеосервисов.

Методы исследований. Обоснование направления повышения качества предоставления видеоинформационных услуг с использованием ведомственных телекоммуникационных систем и закрытия базового видеокадра осуществлялось на основе методов системного анализа, теории исследования операций. Разработка метода повышения пропускной способности закрытого видеоканала проводилась с использованием методов теории кодирования и цифровой обработки изображений. Оценка адекватности теоретических и практических результатов проводилась на основе методов математической статистики.

Научная новизна полученных результатов:

1. Получил дальнейшее развитие метод выявления значимых фрагментов кадра на основе использования информации в спектральном пространстве. Отличительные характеристики метода заключаются в определении энергетической значимости для структурных единиц базового кадра видеопотока с учетом каскадных пороговых оценок интегрированных по всему трансформированному макроблоку. Это позволяет создать условия для снижения интенсивности видеопотока и сохранения семантической информации об объектах интереса.

2. Впервые разработан метод оценки информационной интенсивности закрытого видеопотока на основе выявления семантически значимых фрагментов базового кадра. Отличительные характеристики метода состоят в том, что интенсивность битового потока оценивается на основе того, что криптографической защите подлежат только значимые структурные единицы базового кадра с учетом степени их влияния на характеристики интенсивности и конфиденциальности предсказываемых кадров видеоинформационного потока. Это позволяет провести оценку пропускной способности закрытого видеоканала с учетом обеспечения ведомственных требований относительно качества видеосервиса.

3. Впервые разработан метод повышения пропускной способности закрытого видеоканала на основе селективной обработки видеоинформационного потока. Отличительные особенности метода

заключаются в: автоматической селекции значимых фрагментов видеопотока только по базовому кадру с использованием каскадных решающих правил в спектральном пространстве; дифференцированной обработке базового кадра с учетом выявления и закрытия значимых структурных единиц; согласовании кодовых конструкций значимых структурных единиц кадра с условиями блочного симметричного шифрования без внесения избыточности. Это обеспечивает повышение пропускной способности видеоканала с учетом ведомственных требований относительно конфиденциальности и качества видеоинформационного потока.

4. Впервые создан метод реконструкции закрытого видеоинформационного потока на основе внутрикадровой селекции ключевых компонент кадра. Отличие данного метода от существующих состоит в том, что дешифрование проводится в процессе восстановления с учетом идентификации закрытых структурных единиц базового кадра в общем кодовом потоке на основе использования установленных меток и взаимной согласованности требований относительно формирования кодовых конструкций. Это позволяет обеспечить требуемое качество ведомственного видеоинформационного сервиса для закрытых информационных ресурсов.

Новизна полученных результатов подтверждается отсутствием разработанных моделей и методов в существующих положениях теории и практики кодирования и шифрования видеоинформационных потоков.

Практическое значение полученных результатов заключается во внедрении технологии повышения пропускной способности закрытого видеоканала в ведомственные инфокоммуникационные системы, что, в частности, позволяет обеспечить следующие результаты:

1. Для разработанного метода достигается выявление и сокрытие до 90% семантически значимых областей видеодокументов, представляющих оперативный интерес, что обеспечивает выполнение ведомственных требований по конфиденциальности видеоинформационного потока. При этом прирост по интенсивности в условиях обеспечения высокого качества ведомственных видеоинформационных сервисов за счет закрытия только значимых структурных единиц базового кадра не превышает 7 %, относительно случая передачи видеоинформации в открытом виде.

2. Оценка степени закрытия видеоинформационного потока по базовому кадру для созданного метода показала, что обеспечивается необходимый уровень конфиденциальности для ведомственного информационного ресурса. Соответственно, средние значения пикового отношения сигнал/шум для предсказываемых кадров в группе при попытке несанкционированного доступа в зависимости от режимов обработки видеопотока находятся в пределах от 5 до 9 дБ.

3. Для разработанного метода обеспечивается наибольшая пропускная способность закрытого видеоканала относительно известных методов в случае использования единой ведомственной цифровой телекоммуникационной сети в видеоформате Full HD и достигает 407 Мбит/с.

4. Разработанный метод обеспечивает пропускную способность закрытого видеоканала на уровне 59 Мбит/с (25 кадров/с в пересчете на исходный видеопоток) в условиях использования полевых узлов для проведения сеансов ведомственной видеоконференцсвязи в видеоформате SD при выполнении ведомственных требований по оперативности, достоверности $PSNR_{с} > 21$ дБ и конфиденциальности $PSNR_{нсд} < 10$ дБ.

5. В случае использования разработанного метода селекции значимых структурных единиц базового видеокадра для видеоформата Full HD обеспечивается выигрыш по пропускной способности закрытого видеоканала от 23% до 51%, по сравнению с известными методами последовательного шифрования (кодирование видеоданных с последующим их шифрованием) и от 26% до 42%, по сравнению с методами селекции всех структурных единиц базового видеокадра, в зависимости от качества передаваемых видеоданных. Это позволяет повысить качество предоставления видеоинформационных услуг для инфокоммуникационных систем с высокой разрешающей способностью при выполнении ведомственных условий по конфиденциальности, оперативной доставке и достоверности.

Результаты диссертации использовались при выполнении госбюджетной НИР № 276-4 «Технологии создания интегрированных информационных систем на основе сетей цифрового мобильной связи» (номер государственной регистрации № 0113U000360), которая выполнялась

согласно тематического плана НИР Харьковского национального университета радиоэлектроники, и в Главном управлении Национальной полиции в Харьковской области (акт реализации от 07.10.2015 г.).

Личный вклад соискателя. Основные результаты работы были получены автором самостоятельно и достаточно полно отражены в публикациях: в работе [29] - проводится анализ структуры видеоинформационных систем в Министерстве внутренних дел Украины; в работе [46] - исследованы системы видеоконференцсвязи, применяемые в органах внутренних дел Украины, представлены основные результаты исследований показателей эффективности применения ведомственных систем и требования, предъявляемые к ним; в работах [77; 79; 17] - проанализированы основные характеристики политики видеопотока при различных вариантах сокрытия для поиска наилучшего метода закрытия видеоинформационную ресурса в ведомственных телекоммуникационных системах; в работах [18; 87; 13] - проведены экспериментальные исследования по восстановлению видеопотока при зашифрованном базовом кадре с учетом различных пиковых отношений сигнал/шум и коэффициентов снижения интенсивности; в работах [14, 16; 78; 98] - разработан селективный метод шифрования, основанный на сокрытии базового кадра, представлены алгоритмы и схемы кодирования и декодирования видеопотока; в работах [11, 8, 48, 9; 115] - создается метод повышения пропускной способности закрытого видеоканала, который основан на закрытии наиболее значимых составляющих базового видеокадра; в работах [10; 49, 98; 114] - построена технология совместимости кодовой конструкции энергетически значимой структурной единицы требованиям методов блочного симметричного шифрования для закрытия потоковых видеоданных на основе технологии внутрикадрового селекции базового видеокадра; в работах [12; 101] - разработана методологическая база для расчета битовой скорости зашифрованной структурной единицы базового видеокадра.

Апробация работы. Основные результаты и положения диссертационной работы были представлены и обсуждены на 10 научно-технических конференциях: The 4th International Scientific Conference ″ITSEC″ (Київ, 20 – 23 травня 2014 р.); Четверта міжнародна науково-

практична конференція [«Інформаційні технології та комп'ютерна інженерія»], (Вінниця, 28 – 30 травня 2014 р.); V Міжнародна науково-практична конференція [«Інформаційні технології та комп'ютерна інженерія» (ІТКІ-2015)] (Івано-Франківськ – Ворохта – Винниця, 27 – 29 травня 2015 р.); The XIIIth International Conference The Experience of Designing and Application of CAD Systems in Microelectronics CADSM'2015 (24-27 February 2015 Polyana-Svalyava (Zakarpattya); Науково-технічна конференція [«Інформаційна безпека України»] (Київ, 12-13 березня 2015 р.); VI Международная научно-практическая конференция [«Проблеми і перспективи розвитку ІТ-індустрії»], (Харків, 17 - 18 квітня 2014 р.); Науково-методична конференція [«Сучасні проблеми телекомунікації і підготовка фахівців в галузі телекомунікацій – 2014»] (Львів, 1-4 листопада 2014р.); VI Международная научно-практическая конференция [«Проблеми і перспективи розвитку ІТ-індустрії»], (Харьков, 17 - 18 апреля 2014 р.); XXII Міжнародна науково-практична конференція [«Інформаційні технології: наука, техніка, технологія, освіта, здоров'я»], (Харків, 21 - 23 травня 2014 р.); The XIIIth International Conference The Experience of Designing and Application of CAD Systems in Microelectronics CADSM'2015 (24-27 February 2015 Polyana-Svalyava (Закарпатская обл.), Ukraine).

Публикации. Основные положения и результаты исследований опубликованы в 23 научных работах, в том числе, 10 статей в научных фаховых изданиях Украины, 1 из которых без соавторов, 5 – включены в международные научно-метрические базы. Кроме того, материалы диссертационной работы представлены в 13 тезисах докладов на научно-технических конференциях, выполнены 5 апробаций на конференциях, которые проходили под эгидой международной организации IEEE.

РАЗДЕЛ 1
ОБОСНОВАНИЕ НЕОБХОДИМОСТИ ПОВЫШЕНИЯ ПРОПУСКНОЙ СПОСОБНОСТИ ЗАКРЫТОГО ВИДЕОКАНАЛА ДЛЯ ОБЕПЕЧЕНИЯ КАЧЕСТВА ВИДЕОИНФОРМАЦИОННОГО СЕРВИСА В ВЕДОМСТВЕННЫХ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМАХ

Развитие инфокоммуникационных технологий, которые определяются ростом трафика и потребностью потребителей в появлении новых услуг, приводит к необходимости постоянного роста и модернизации телекоммуникационных систем и сетей. Наиболее востребованными в последние годы становятся видеоинформационные услуги, такие как IP-видеонаблюдение, видеотелефония, видеоконференцсвязь, on-line трансляции, видео «по запросу». Особенностью таких видеоинформационных услуг являются большие объемы передаваемых видеоданных, чувствительность к времени обработки и потерям пакетов при передаче по каналу связи. С учетом приведенных ведомственных требований необходимо особое внимание уделять качеству предоставляемых видеосервисов и уровню их конфиденциальности.

1.1. Роль и место видеоинформационных ресурсов в системе функционирования подразделений Министерства внутренних дел Украины

Министерство внутренних дел (МВД) Украины, является центральным отраслевым органом государственной исполнительной власти. Министерство реализует государственную политику в сфере защиты прав и свобод граждан, интересов общества и государства от противоправных посягательств, организует и координирует деятельность органов внутренних дел по борьбе с

преступностью, охране общественного порядка и обеспечению общественной безопасности.

Основные задачи МВД Украины вытекают из общих задач, возложенных на органы внутренних дел, в них программируются содержание руководства внутренними делами, осуществляемого МВД, и основные направления деятельности министерства. Содержание деятельности МВД Украины как центрального органа управления в области внутренних дел состоит:

– в организации и координации деятельности органов внутренних дел Украины по защите прав и свобод граждан, интересов общества и государства от противоправных посягательств, охране общественного порядка и обеспечении общественной безопасности;

– в участии, разработке и реализации государственной политики борьбы с преступностью;

– в предупреждении преступлений, их пресечении, раскрытии и расследовании, розыске лиц, совершивших преступления, принятии мер по устранению причин и условий, способствующих совершению правонарушений;

– в определении основных направлений совершенствования работы ОВД, оказании им организационно-методической и практической помощи;

– в организации работы по обеспечению безопасности дорожного движения и пожарной безопасности;

В соответствии с основными задачами МВД Украины осуществляет и основные направления деятельности:

– обеспечивает государственную политику борьбы с преступностью;

– определяет основные направления деятельности подчиненных органов, подразделений и учреждений, а также эффективные способы и методы выполнения возложенных на них задач;

– организует работу органов внутренних дел по охране общественного порядка на улицах и других общественных местах, предупреждению и пресечению административных правонарушений; [45]

– организует осуществление ОВД профилактических и оперативно-розыскных мероприятий по предупреждению, выявлению, пресечению и раскрытию преступлений, производства дознания и предварительного следствия;

– непосредственно осуществляет работу по выявлению, раскрытию и расследованию преступлений, имеющих межрегиональный и международный характер, ведет борьбу с организованной преступностью и наркобизнесом, с преступлениями в сфере экономики;

– обеспечивает профилактику правонарушений, вносит в центральные и местные органы государственной власти, предприятия, учреждения и организации представления о необходимости устранения причин и условий, способствующих совершению правонарушений;

– принимает участие в научных, криминологических и социологических исследованиях, в разработках на их основе государственных программ борьбы с преступностью и охране правопорядка;

– организует и осуществляет розыск граждан в случаях, предусмотренных законодательством и международными договорами;

– организует информационно-аналитическое обеспечение деятельности ОВД формирует центральные справочно-информационные фонды, оперативно-поисковый учет, в пределах полномочий ведет государственную статистику;

– организует проведение экспертиз по уголовным делам и криминалистические исследования по материалам оперативно-розыскной деятельности, обеспечивает в установленном порядке участие специалистов криминалистической службы в следственных действиях;

– обеспечивает функционирование разрешительной системы и осуществляет контроль за приобретением, хранением, ношением и перевозкой оружия, боеприпасов, взрывчатых веществ и материалов, иных предметов и веществ, хранение и использование которых предусмотрено специальными правилами, а также за открытием и функционированием объектов, где они используются;

– принимает меры по обеспечению безопасности дорожного движения;

– контролирует работы, направленные на предупреждение дорожно-транспортных происшествий;

Для выполнения возложенных на Министерство внутренних дел Украины функций, в соответствии с действующим законодательством, ему предоставлены определенные полномочия. Так, МВД имеет право:

– принимает меры, направленные на устранение угроз жизни и здоровью физических лиц и общественной безопасности, возникших в результате совершения уголовного, административного правонарушения;

– осуществляет досудебное расследование уголовных правонарушений в пределах определенной подследственности;

– разыскивает лиц, скрывающихся от органов досудебного расследования, следственного судьи, суда, уклоняющихся от исполнения уголовного наказания, пропавших без вести;

– доставляет в случаях и порядке, определенных законом, задержанных лиц, подозреваемых в совершении преступления, и лиц, совершивших административное правонарушение;

– принимает меры по обеспечению общественного порядка и общественной безопасности на улицах, площадях, парках, скверах, стадионах, вокзалах, аэропортах, морских и речных портах, других общественных местах;

– регулирует дорожное движение и осуществляет контроль за соблюдением правил дорожного движения;

– обеспечивает безопасность взятых под защиту лиц по основаниям и в порядке, определенных законом;

– принимает меры для предотвращения и пресечения насилия в семье.

С 2015 года начата реформа системы МВД Украины, которая продолжается до сих пор. В результате реформирования изменена (расширена) структура органов внутренних дел. Новая структура МВД Украины представлена на рис. 1.1.

Рис. 1.1. Структура Министерства внутренних дел Украины.

В результате процесса реформирования проводятся не только изменения в структуре органов внутренних дел, но и координально меняется подход к материальному, техническому и информационному обеспечению сотрудников МВД. В результате внедрения комплексных информационно-технических решений планируется повышению качества работы органов полиции, что в целом позитивно отразится на состоянии криминогенной обстановки в государстве. Для качественного и эффективного выполнения задач, возложенных на структурные подразделения МВД Украины, разработан ряд программ по развитию информационного обеспечения. Среди них: проведение работ по оборудованию мест массового скопления граждан системами видеонаблюдения и кнопками тревожной сигнализации, финансирование программ по безопасности дорожного движения, разработке межведомственных мероприятий по реабилитации лиц, ранее судимых и лиц, ранее совершавших преступления.

Под информационным обеспечением органов внутренних дел Украины следует понимать деятельность по разработке, организации функционирования и совершенствованию информационных систем, направленную на организацию обеспечения подразделений совокупностью

сведений в виде систематизированной информации, необходимой им для осуществления возложенных на них задач и функций процесса управления.

Информационное обеспечение крайне важно для руководителей всех уровней органов внутренних дел, координирующих действия подчиненных, эффективность деятельности которых находится в прямой зависимости от имеющихся в их распоряжении и удовлетворяющих их информационные потребности информационных систем.

Исходя из вышесказанного, задачи информационного обеспечения и информационной системы органов внутренних дел Украины можно сформулировать следующим образом:

– определение необходимых для управления видов и объектов информации, форм ее представления и сроков поступления в систему, а также ответственных за это компонентов системы;

– обеспечение информационного взаимодействия служб и подразделений органов внутренних дел с объектами внутриорганизационного управления и иными организациями;

– организация регистрации заданных параметров (показателей) функционирования системы и состояния объектов в неведомственных организациях;

– обработка первичной информации, поступившей в систему, ее систематизация и обобщение в виды и формы, необходимые для осуществления процесса управления;

– распределение поступившей и обработанной информации между звеньями системы управления (службами, подразделениями, исполнителями) согласно выполняемым ими функциям или конкретно решаемым задачам;

– обеспечение хранения поступившей информации, ее своевременный и релевантный поиск и выдача, согласно запросам, компонентов системы и с других источников;

– организация своевременной передачи информации между объектами внутриорганизационного управления, а также другими организациями;

– внедрение технических средств сбора, обработки, хранения и выдачи информации в целях ускорения этих процессов и улучшения их качества.

Таким образом, информационные системы, используемые в органах внутренних дел Украины, должны обеспечивать сотрудника необходимой, актуальной, систематизированной информацией.

Ключевой составляющей информационного обеспечения является видеоинформационная составляющая. В состав видеоинформационной составляющей входят системы видеонаблюдения и видеоконференцсвязи.

Видеосвязь в органах внутренних дел (ОВД) имеет большую актуальность, об этом свидетельствует анализ решаемых задач по информационному обеспечению.

Системы видеосвязи в органах внутренних дел можно разделить на две группы:

1. Системы видеонаблюдения используются для передачи визуализированной информации в процессе визуального контроля, осуществляемого с помощью видеокамер.

2. Системы видеоконференцсвязи используются как интерактивный инструмент, который включает в себя аудио, видео, компьютерные и коммуникационные технологии для осуществления связи территориально удаленных подразделений полиции «лицом к лицу» в реальном времени.

Первая группа включает в себя системы видеонаблюдения, которые находят свое применение:

- на автомобильных и железнодорожных вокзалах, аэропортах;
- на дорогах и в местах наиболее частого совершения дорожно-транспортных происшествий;
- в наиболее критичных местах с позиции совершения правонарушений (в местах наиболее частого совершения правонарушений);
- в местах массового скопления граждан и проведения массовых мероприятий;
- при проведении обзора, обыска, воссоздании обстановки и обстоятельств события и при проведении других следственных действий;

- в процессе оперативной видеосъемки.

Системы видеонаблюдения решают такие задачи структурных подразделений органов внутренних дел, как:

- обеспечение безопасности граждан;
- соблюдению прав человека;
- охрана общественного порядка;
- способствуют оперативности реагирования на правонарушения, а также их документированию;
- увеличивают скорость установления лиц, совершивших правонарушения;
- помогают осуществлять контроль за криминогенной ситуацией;
- фиксация нарушений правил дорожного движения;
- позволяют уменьшить количество сотрудников полиции на улицах, что делает их работу более эффективной.

Мировой опыт показывает, что наличие систем видеонаблюдения является сдерживающим фактором при желании совершить правонарушение, даже при отсутствии сотрудников полиции. Установка систем видеонаблюдения позволяет снизить количество совершаемых преступлений на 60%, повысить раскрываемость на 65%, уменьшить количество сотрудников полиции на 15%.

В поддержку внедрения техники видеонаблюдения в Украине принят ряд нормативно-правовых актов, которые регламентируют законность и порядок применения систем видеонаблюдения:

- законопроект № 11104, принятый как Закон Украины, которым предусматривается, что системы видеонаблюдения будут использоваться во время голосования и подсчета голосов на парламентских выборах в Украине 28 октября 2012 г.; [74]
- ст. 307 Гражданского Кодекса Украины – гарантией невмешательства в личную и семейную жизнь является и защита интересов физического лица при проведении фото-, кино-, теле- и видеосъемок. При проведении фото-, кино-, теле- и видеосъемок согласие физического лица на съемку

обязательно. Это общее правило. Съемка физического лица на фото-, кино-, теле- или видеопленку, в том числе тайная, без согласия лица может быть проведена лишь в случаях, установленных законом (ч. 3 ст. 307 Гражданского Кодекса Украины). [89]

Эти документы регламентируют общие правила применения систем видеонаблюдения.

Таким образом, на законодательном уровне прописано то, что в органах внутренних дел Украины возможно использование открытой и скрытой видеосъемки.

Так, случаями отрытой съемки без согласия физического лица являются:

- киносъемка, видеозапись при проведении обзора, обыска, воссоздании обстановки и обстоятельств события и при проведении других следственных действий (85-2 Уголовно-процессуального кодекса); [58]

- в судебном процессе (ст. 6 Гражданского процессуального кодекса, ст. 12 Кодекса административного судопроизводства, ст. 87-1 Уголовно-процессуального кодекса, ст.ст. 4-4, 81-1 Хозяйственного процессуального кодекса); [33]

- в соответствии с Законом Украины «Про Национальную полиции», полиции предоставлено право проводить фотографирование, звукозапись, кино- и видеосъемку, дактилоскопию лиц, которые задержаны по подозрению в совершении преступления или за бродяжничество, взятые под стражу, обвиняются в совершении преступления, а также лиц, подданных административному аресту; а также проводить кино-, фото- и звукофиксацию как вспомогательное средство предупреждения противоправных действий и раскрытия правонарушений. [72]

Право тайной (скрытой) съемки определено Законом Украины «Об оперативно-розыскной деятельности». В соответствии с указанным Законом (п.11 ст. 8), осуществлять визуальное наблюдение в общественных местах с применением фото-, кино- и видеосъемки, оптических и радиоприборов, других технических средств имеют право оперативные подразделения при наличии определенных Законом оснований. Важно отметить, что проведение

оперативно-розыскной деятельности, в том числе проведение фото-, кино- и видеосъемки, другими (неоперативными) подразделениями, общественными, частными организациями и лицами запрещается. [73]

Другой стороной видео-взаимодействия являются системы цифровой видеоконференцсвязи с использованием телекоммуникаций для приема и передачи видеоинформации в реальном времени. Такие системы широко используются в органах внутренних дел Украины, а именно для:

- проведения селекторных совещаний между министром внутренних дел Украины и начальниками областных ГУНП, УНП в областях (введена в эксплуатацию в 2012 году);
- проведения селекторных совещаний между руководством МВД Украины и областными аппаратами, службами по направлениям (введена в эксплуатацию в 2011 году);
- для видеотрансляции проведения следственных действий в территориально отдаленные органы и подразделения МВД Украины, суды и прокуратуру (введена в эксплуатацию в 2013 году и продолжает развиваться).

Положительными аспектами применения систем ВКС в структуре МВД Украины являются:

- повышение оперативности при принятии решений в чрезвычайных ситуациях;
- проведение совещаний в любое время и в кротчайшие сроки;
- обеспечение проведения дистанционного обучения сотрудников;
- уменьшение расходов и времени, связанных с отрывом сотрудников МВД от работы на время переезда в аппарат МВД (Киев) или областные центры;
- возможность принятия более обоснованных решений за счёт привлечения при необходимости дополнительных экспертов;
- обеспечение более прочного взаимодействия между сотрудниками, так как в ходе видеоконференции задействовано большее число органов чувств, чем во время телефонного разговора.

Таким образом, все видеоинформационные ресурсы, обрабатываемые в органах внутренних дел Украины можно поделить на открытые и скрытые (тайные). Это представлено на рис. 1.2.

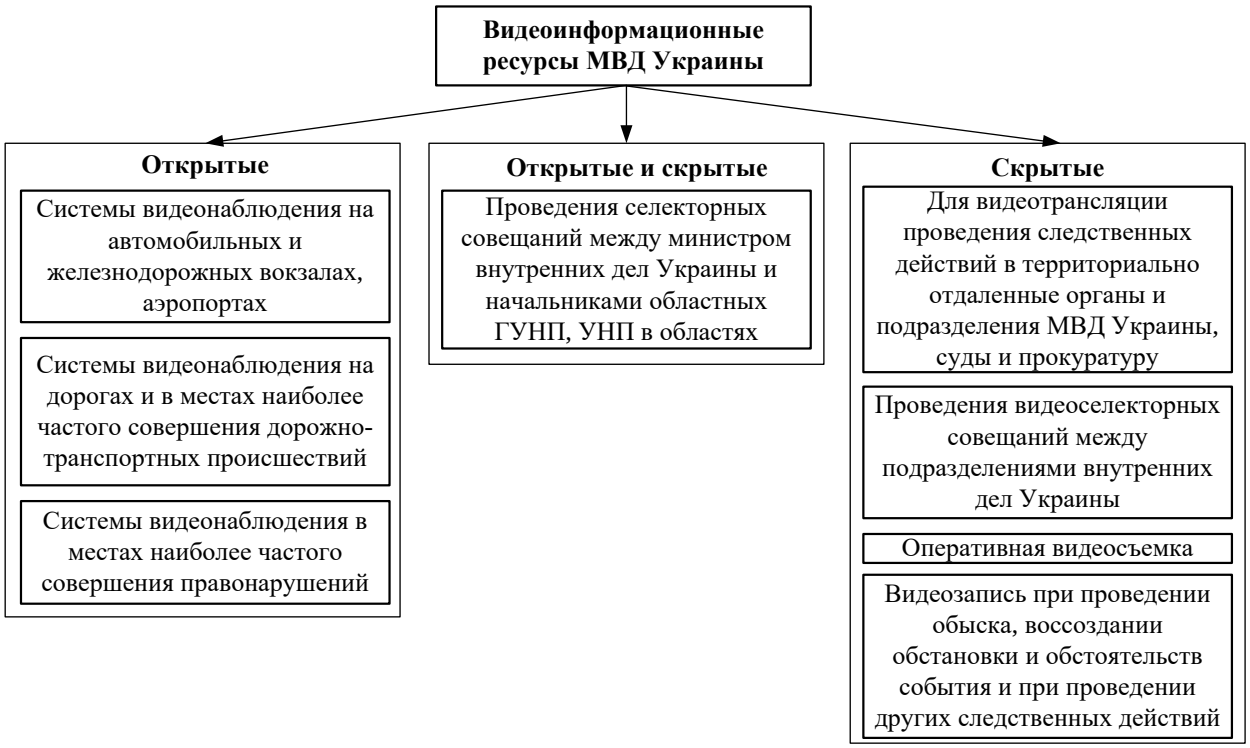


Рис. 1.2. Виды видеоинформационных ресурсов, обрабатываемых в органах внутренних дел Украины.

Как видно из рис. 1.2, вся информация (в том числе и видеоконтент), обрабатываемая в МВД, может быть как открытой, так и скрытой, поэтому является служебной, соответственно приобретает статус государственной. Она имеет важную роль для обеспечения эффективного функционирования структурных подразделений МВД Украины. Отсюда вытекает, что информация, обрабатываемая в органах внутренних дел Украины должна обеспечивать выполнение ведомственных требований по оперативности, достоверности и конфиденциальности.

1.2. Формирование системы показателей для оценки качества ведомственного видеосервиса

Видеоинформационные ресурсы в органах внутренних дел Украины созданы для эффективной работы подразделений и качественного, объективного и своевременного принятия управленческих решений.

Обобщенная схема процесса доставки ведомственной видеоинформации в органах внутренних дел Украины представлена на рис. 1.3.

Рис. 1.3. Обобщенная схема процесса доставки видеоинформации в органах внутренних дел Украины.

Основными показателями эффективности, определяющими качество ведомственного видеосервиса, и функционирования систем доставки видеоинформационного потока для ведомственных систем являются оперативность и достоверность. [46]

Под оперативностью, как характеристикой качества видеосервиса, в ведомственных видеоинформационных системах понимается время на доставку видеоинформационного потока. Время $T_д$ доставки видеопотока в ведомственных телекоммуникационных системах включает в себя время на кодирование исходного видеопотока, его передачу и декодирование принятых видеоданных. Время $T_д$ доставки определяется как:

$$T_д = T_к + T_п + T_{дк},$$

где $T_к$ – время кодирования исходного видеопотока;

$T_п$ – время передачи кодированного видеопотока по инфокоммуникационным системам;

$T_{дк}$ – время, затраченное на декодирования принятого видеопотока.

Достоверность, как характеристика качества видеосервиса определяет уровень соответствия принятых видеоданных по отношению к исходным. Основным показателем достоверности является качество видеоинформационного сервиса. [15] Основным показателем оценки качества видеосервиса является пиковое отношению сигнал/шум PSNR :

$$PSNR = 20\lg(\frac{I_{max}}{MSE}),$$

где $I_{max} = 255$ – максимальное значение 8-битного сигнала.

MSE – среднеквадратические отклонение, которое определяется как:

$$MSE = \sqrt{\frac{1}{mn}\sum_{i=1}^{m}\sum_{j=1}^{n}[a_{i,j} - a'_{i,j}]^2},$$

где m – количество строк в видеокадре;

n – количество столбцов в видеокадре;

$a_{i,j}$ – $(i;j)$-й исходный элемент видеокадра;

$a_{i,j}$ – $(i;j)$-й восстановленный элемент видеокадр авторизированным пользователем.

1.3. Обоснование требований для видеоинформационных сервисов, применяемых в органах внутренних дел Украины

В законе Украины «О защите информации в информационно-телекоммуникационных системах» написано, что информация, которая является собственностью государства, или информация с ограниченным доступом, требование относительно защиты которой, установлено законом, должна обрабатываться в системе с применением комплексной системы защиты информации (КСЗИ) с подтвержденным соответствием. В силу того, что вся информация, обрабатываемая в МВД, в том числе аудио и видео, является служебной, она требует обеспечения надежной защиты. Это достигается созданием КСЗИ, которая включает в себя применение, как аппаратных, так и программных средств. Требования КСЗИ не выполняется в силу их дороговизны. К ним относятся как закупка профессионального оборудования защиты информации, так и разработка нормативной документации, которая выполняется организациями, имеющими лицензию в области технической защиты информации. Оборудование, которое сейчас применяется для этих целей, не обеспечивает выполнение в полной мере задач по защиты передаваемых видеоданных. К тому же, его применение вызывает задержки в процессе обработки видеопотока, которые способствует появлению ошибок в канале связи и видеокодеке. Это приводит к негативным последствиям, начиная от потери фрагментов видеокадров до обрыва видеопотока. [2]

В декабре 2012 года в МВД были разработаны «Ведомственные технические требования для систем видеоконференцсвязи в органах досудебного расследования». В этом документе формируются требования к программно-аппаратной части ведомственных систем ВКС. Они представлены в таб. 1.1.

Таблица 1.1

Основные требования к программно-аппаратной части систем ВКС в МВД Украины.

№ п/п	Характеристика	Минимальное требуемое значение
1.	Использование видеоформата	Не менее 720 HD (использование прогрессивной развертки)
2.	Параметры видеокамеры	Не менее 720 HD
3.	Поддержка общих стандартов обработки видеопотоков	H.263, H.263+, H.264
4.	Поддержка видеопротоколов	H.323, SIP
5.	Применение средств защиты информации	Обязательное применение средств защиты информации, которые имеют соответствующие экспертные документы Государственной службы специальной связи и защиты информации Украины.
6.	Применение сетевых технологий для предотвращения несанкционированного доступа	Возможность работы через Firewall, NAT или прокси-сервер из локальной сети организации.
7.	Стойкость к неравномерности и разрывам соединения канала связи	задержка при передаче пакетов - не больше 50 мс, процент допустимых потерь пакетов – не больше 5%
8.	Технологии маскирования субъектов видеоконференцсвязи	Возможность изменения голоса и видео с целью невозможности определения лица абонента на другом конце.

Технические требования для серверного оборудования видеоконференцсвязи представлены в таб. 1.2.

Таблица 1.2

Основные требования для серверного оборудования систем ВКС в МВД Украины.

№ п/п	Характеристика	Минимальное требуемое значение
1.	Количество устойчивых подключений	не меньше 100 видео- и аудио-абонентов одновременно
2.	Количество одновременных видеоконференций точка-точка	не меньше 50
3.	Возможность проведения нескольких одновременных видеоконференций	3 групповые и 10 персональных конференций
4.	Использование видеоформата	не меньше 720 HD
5.	Пропускная способность	не меньше 15 кадров в секунду с синхронизацией видео и звука
6.	Использование методов повышения качества видео	Обеспечение фильтрации шумов видеокамеры
7.	Степень масштабирования	не меньше 2000 пользователей
8.	Использование дополнительных функций	передача файлов, электронная доска, просмотр слайдов

Продолжение таблицы 1.2.

№ п/п	Характеристика	Минимальное требуемое значение
9.	Хранение видеоинформации	Возможность автоматического или ручного способа записи и сохранения видеоконференций
10.	Формирование списка абонентов	Использование единой адресной книги для всех пользователей. При добавлении нового пользователя на сервере его имя автоматически добавляется в адресные книги всех зарегистрированных на сервере пользователей
11.	Изменение списка абонентов	Возможность внесения изменений в адресную книгу конечного пользователя администратором сервера непосредственно на самом сервере
12.	Использование низкоскоростных каналов	Обеспечение видеоконференцсвязи на низкоскоростных (от 128 кбит/с) каналах передачи данных
13.	Использование устройств ВКС	использование устройств, которые работают по протоколу H.323/SIP
14.	Согласование протоколов	совершение перекодирования видео и аудио потоков в форматы, которые использует данная система
15.	Техническая поддержка	Проверка работоспособности системы в режиме «горячая» линия

Исходя из требований к ведомственных систем видеоконференцсвязи (таб. 1.1, таб. 1.2), интенсивности информационных видеопотоков должна быть 398 Мбит/с для формата 720P и 177 Мбит/с для формата 1080P.

Из анализа таблиц 1.1. и 1.2. можно заключить, что разработаны ведомственные требования относительно предоставления видеоуслуг для структурных подразделений МВД Украины. Они отличаются повышенными требованиями относительно обеспечения оперативности, достоверности и различных режимов конфиденциальности. Для выполнения этих требований необходимо развивать существующие сети и технологии обработки видеоконтента.

1.4. Обоснование проблемных сторон инфокоммуникационных сетей, используемых в Министерстве внутренних дел Украины, с позиции обеспечения качества видеосервиса

Для обеспечения качества видеоинформационных сервисов в системе органов внутренних дел Украины используется специализированная телекоммуникационная система. Приказом МВД Украины от 02.02.2006 № 112 утверждена программа создания ЕЦВТС. Общая структура единой цифровой ведомственной телекоммуникационной сети МВД Украины представлена на рис. 1.4. [11]

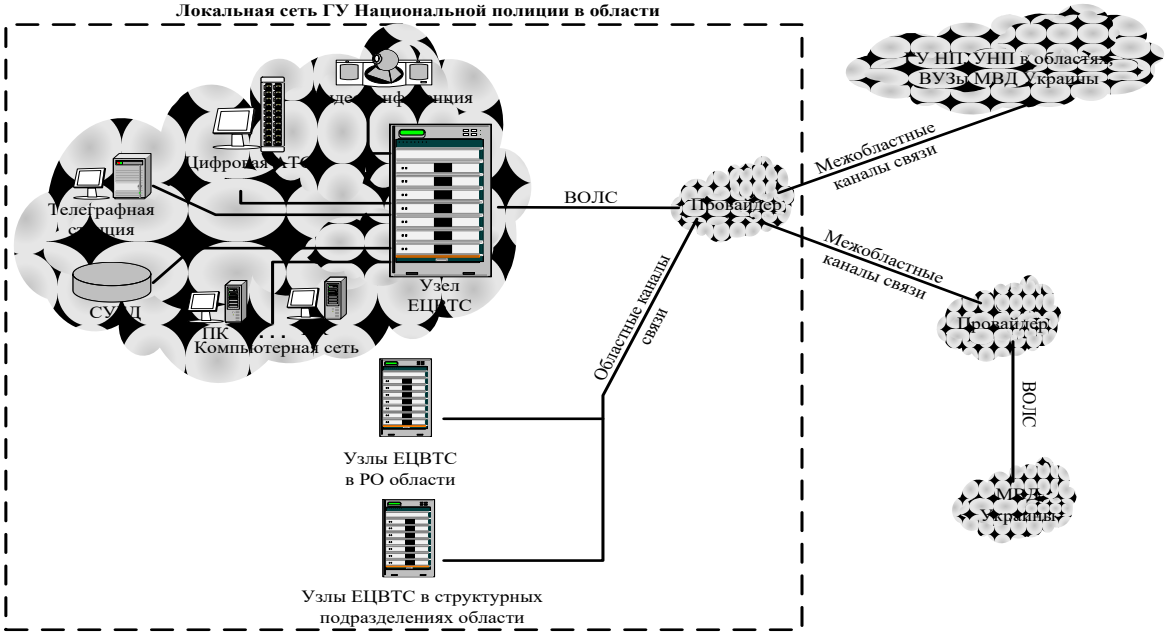


Рис. 1.4. Структурная схема построения ЕЦВТС МВД Украины.

Системы видеоконференцсвязи в органах внутренних дел Украины строятся на различных каналах связи и локальных сетях – единой цифровой ведомственной телекоммуникационной сети (ЕЦВТС) МВД Украины. Структурная схема построения ведомственной системы видеоконференцсвязи представлена на рис. 1.5. [29]

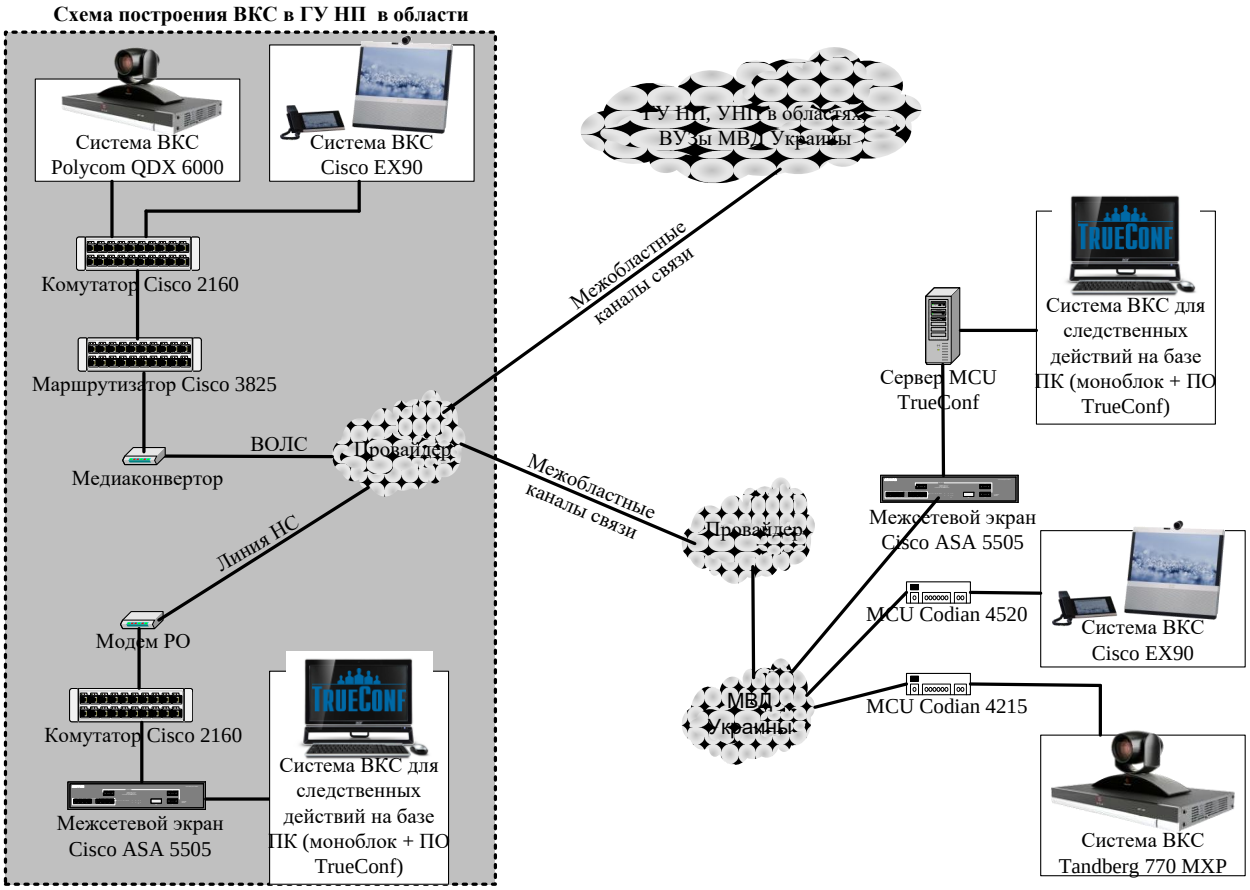


Рис. 1.5. Структурная схема построения ведомственной системы видеоконференцсвязи.

Для повышения оперативности и эффективной борьбы с преступностью в кризисных ситуациях МВД Украины в 2015 году закупило мобильные системы спутниковой связи (рис. 1.6). Организация рабочего места такой системы занимает до 20 минут.

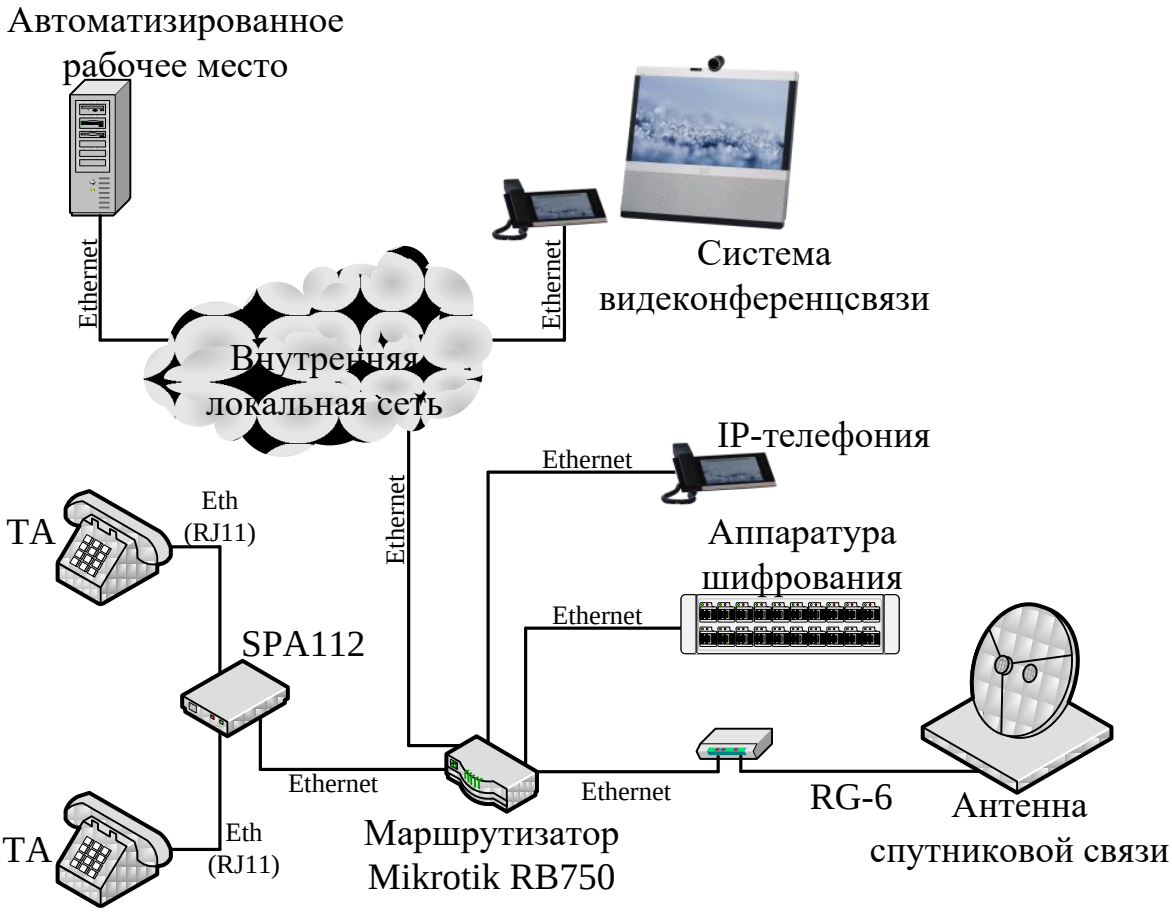


Рис. 1.6. Структурная схема построения спутникового узла ЕЦВТС МВД Украины.

Использование беспроводных сетей имеет ограниченное развитие по причине их меньшей защищенности.

В зависимости от участков построения единой цифровой ведомственной телекоммуникационной сети МВД Украины, в ней используются различные каналы связи: оптические, спутниковые, непосредственные связи, по витой паре. Характеристики и места использования этих каналов связи представлены в таб. 1.3.

Таблица 1.3

Характеристики и места использования каналов связи в системе МВД Украины.

№ п/п	Тип канала связи	Место применения	Скорость передачи
1.	Отический канал	Между областными Управлениями ГУ НП и МВД Украины	20 Мбит/с
2.	Спутниковы канал	Между полевыми (оперативными) командными пунктами и подразделениями МВД Украины	5 Мбит/с
3.	Каналы непосредственной связи	Между районными подразделениями и ГУ НП в области	2 Мбит/с
4.	По витой паре	Внутри подразделений и между близко расположенными подразделениями	100 Мбит/с

Оценки интенсивности $V_{гк}^{(сж)}$ группы кадров при заданной достоверности PSNR для ведомственных систем видеоконференцсвязи представлены на диаграмме (рис.1.7). [14]

Из анализа диаграммы (рис. 1.7) видно, что существующая интенсивность $V_{гк}^{(сж)}$ при заданном уровне достоверности PSNR даже после применения MPEG-технологий превышает пропускную способность единой цифровой ведомственной сети МВД Украины. К тому же, основная часть видеопотока подлежит защите (шифрованию). В результате чего интенсивность передаваемых видеоданных будет расти. Поэтому ***актуальной научно-прикладной задачей является повышение качества видеоинформационного сервиса для ведомственных***

инфокоммуникационных сетей в условиях обеспечения заданной конфиденциальности.

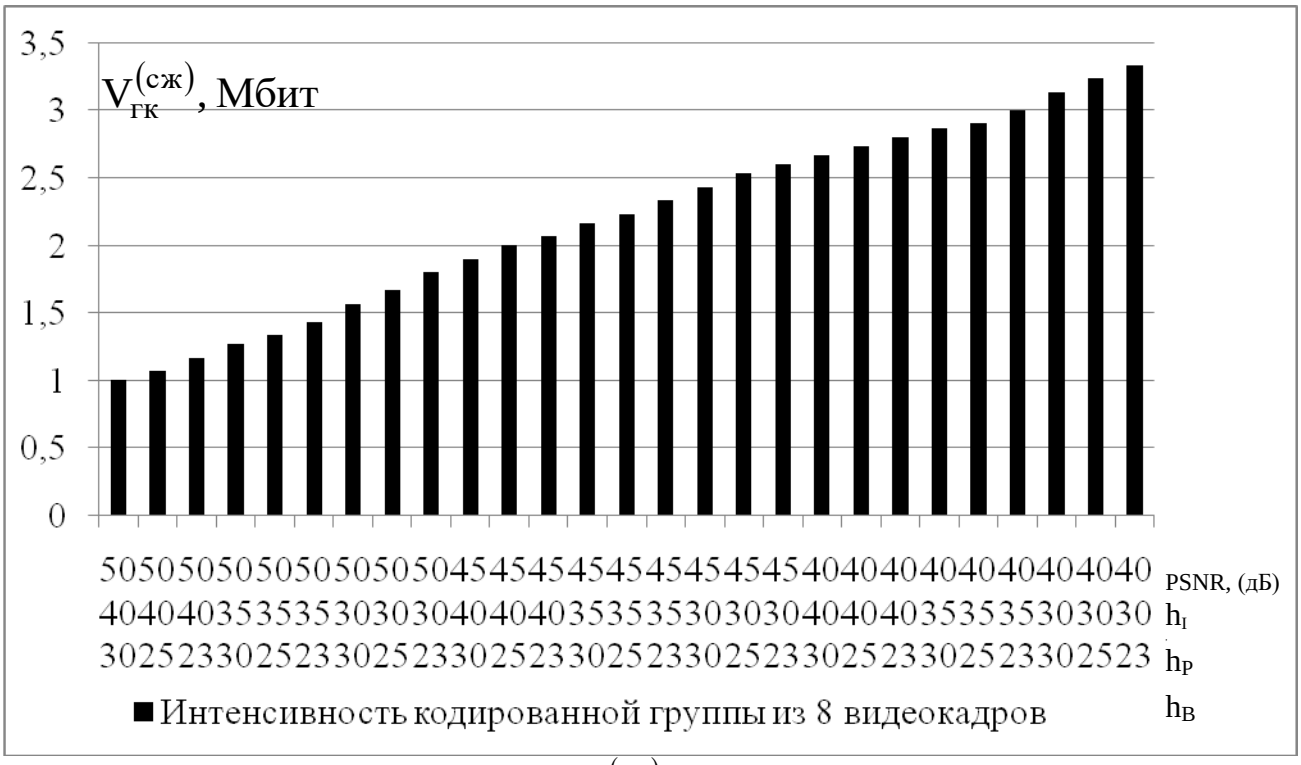


Рис. 1.7. Значения интенсивности $V_{гк}^{(сж)}$ при заданной достоверности PSNR для ведомственных систем видеоконференцсвязи.

В то же время основными проблемными вопросами, которые приходится решать в процессе построении систем видеоинформационного обеспечения, являются:

1. Построение новых каналов передачи данных. С установкой новых и более профессиональных систем видеонаблюдения возникает необходимость в создании новых сетей и каналов передачи данных. Данная проблема решается заменой старого каналообразующего оборудования на современное, построением новых каналов связи с применением оптоволоконных и беспроводных технологий. Это достаточно трудно реализовать в современных условиях мегаполисов и при ограничениях на использование беспроводных технологий по причине их незащищенности.

2. Повышение качества получаемого видеоконтента. Оборудование видеонаблюдения, применяемое сегодня в подразделениях МВД Украины в своей деятельности, в своем большинстве является аналоговым и, имеющим не достаточные характеристики. Это позволяет только зафиксировать факт совершения правонарушения и в редких случаях позволяет зафиксировать моменты, которые способствуют быстрому его раскрытию. Приобретение цифровых камер формата HD (720P) и Full HD (1080P) с высокими характеристиками решает эти проблемы, но их высокая стоимость и большая интенсивность передаваемых видеоданных пока не позволяют их внедрять в полной мере в структуру ОВД.

3. Пропускные способности каналов. Современные требования, предъявляемые к оборудованию ВКС и к самому видеоконтенту очень высоки, это влечет за собой повышение интенсивности передаваемых видеоданных. При этом увеличивается интенсивности других данных, используемых в ЕВЦТС МВД Украины. Соответственно каналы связи, используемые ЕВЦТС, не обеспечивают необходимую пропускную способность видоепотока для эффективного и качественного функционирования органов внутренних дел Украины.

4. Согласование протоколов. Распространение видеоинформационных систем в МВД Украины сегодня находится на активной стадии своего развития – происходит расширение существующих и внедрение новых (более современных) систем. Поэтому возникают сложности при интеграции разных по своим характеристикам систем, которые используют различные стандарты и протоколы согласования.

Из анализа структуры единой ведомственной цифровой сети МВД Украины (рис. 1.4, рис. 1.5, рис. 1.6), применяемого оборудования (таб. 1.3) и требований для ведомственных систем видеоконференцсвязи (таб. 1.1, таб. 1.2), видно, что в органах внутренних дел используются низкоскоростные каналы связи (от 128 кбит/с), по которым необходимо передавать видеоданные высокого качества формата 720P (1280x720).

Поэтому пропускные способности каналов связи в органах внутренних дел Украины не всегда (в случае использования спутниковых терминалов; каналы связи к районным подразделениям МВД) могут обеспечить необходимую пропускную способность для трансляции видеоданных.

1.5. Обоснование направления для повышения качества видеосервиса в условиях требуемой конфиденциальности с использованием ведомственных системах видеоконференцсвязи

Для решения задач по повышению оперативности и достоверности видеоинформационного ресурса применяются различные технологии обработки видеопотока. Наиболее популярной технологией обработки видео является MPEG. В настоящее время существуют три его спецификации: MPEG-1, MPEG-2 и MPEG-4. Стандарта MPEG позволяет менять в широких пределах значения большинства его параметров. MPEG использует следующие основные идеи:

– устранение временной избыточности видео, учитывающее тот факт, что в пределах коротких интервалов времени большинство фрагментов видеосцены оказываются неподвижными или незначительно смещаются по полю;

– устранение пространственной избыточности изображений подавлением мелких деталей видеосцены, несущественных для визуального восприятия человеком;

– использование более низкого цветового разрешения;

– повышение информационной плотности результирующего цифрового потока путем выбора оптимального математического кода для его описания (на пример, использование более коротких кодовых слов для наиболее часто повторяемых значений).

В технологии Motion JPEG каждый видеокадр изображения сжимается отдельно с использованием стандарта JPEG. Никаких других

дополнительных алгоритмов при этом не используется. Безусловным достоинством этого метода является возможность редактирования видео без потерь качества, так как кадры являются независимыми. Этим определяется использование данного метода именно как механизма хранения видео, служащего для его редактирования, а не для распространения. Motion JPEG использует алгоритм блокового ДКП для сжатия изображений. [3]

Editable MPEG, так же как и M-JPEG, используется для редактирования цифрового видео представляет собой AVI-файл, состоящий только из кадров MPEG типа I. Однако все другие механизмы сжатия MPEG тут задействованы. [7]

Характеризуя эту группу видеокодеков, можно отметить, что они проектировались и создавались в первую очередь как средства сжатия видео- и аудиоданных, хранящихся на жестких дисках и компакт-дисках, а это, в свою очередь, свидетельствует об их небольших возможностях при сжатии и относительно высоком качестве при воспроизведении. [1]

С приходом Интернета все большую популярность получают методы и средства сжатия видео- и аудиоданных, позволяющих, применяя передовые технологии (sophisticated motion estimation and compensation, wavelets, fractals и другие), достичь наибольшую пропускную способность, позволивших проводить, например, сеансы видеоконференций средствами Интернета. Такие методы сжатия обеспечивают большую степень сжатия, при относительно низком качестве. [11]

В 1997 году была официально зарегистрирована новая серия видеокодеков цифрового видео, определяющая тенденции развития механизмов сжатия видео. Некоторые видеокодеки семейства H.XXX, например H.261, довольно популярны, другие малоизвестны и используют такие передовые и улучшенные технологии, как wavelets. [20]

Отличительной особенностью видеокодеков семейства H.XXX является их нацеленность на уменьшение потока цифрового видео через Интернет, что естественно приводит к отходу фактора качества на второй план. Некоторые

продукты семейства H.XXX совершенствуется, а некоторые уже входят в состав таких пакетов телеконференций, как NetShow и NetMeeting. [27]

Для построения систем видеоконференцсвязи применяется оборудование таких производителей как:

- Cisco (Tandberg) (система видеоконференцсвязи между министром и начальниками областных управлений);

- Cisco (Tandberg) и Polycom (видеоселектор между руководством МВД Украины и областными аппаратами);

- вандолозащищенные видеотерминалы на базе моноблочного персонального компьютера с использованием ПО TrueConf и оборудования технической защиты информации по каналам связи (межсетевого экрана Cisco Asa 5505) согласно разработанных МВД технических требований (видео селектор для проведения следственных действий).

Системы видеоконференцсвязи в МВД Украины начали создаваться с 2011 года и продолжают развиваться сегодня. Улучшение предоставляемых провайдерами услуг (повышение скорости в каналах связи), позволяет использовать более профессиональное и высококачественное оборудование. Это можно заметить, проанализировав характеристики внедряемого оборудования ВКС, представленные в таб. 1.4.

Из таб. 1.3 видно, что видеоконференцсвязь в органах внутренних дел Украины является новым (внедрение с 2011 года), актуальным и перспективным направлением, которое постоянно развивается. С одной стороны, характеристики представленного оборудования соответствуют техническим требованиям, предъявляемым МВД Украины, а с другой – не все представленное оборудование обладает высококачественными параметрами видео (HD разрешение 1920*1080).

Перечисленное в таб. 1.4 оборудование, входящее в состав систем видеоконференцсвязи, обеспечивает выполнение ведомственных требований МВД Украины только по оперативности и доступности. При этом комплекс мер по обеспечению конфиденциальности используется только в системе

видеоконференцсвязи для проведения следственных действий. Он представлен в виде межсетевого экрана Cisco ASA 5505.

Таблица 1.4

Основные характеристики оборудования ВКС в МВД Украины.

№ п/п	Название системы ВКС	Год внед-рения	Видео-формат	Видео-стандарт	Протокол передачи видео	Скорость передачи
1.	Tandberg 770 MXP	2011	XGA (1024*768)	H.261, H.263, H.263+, H.263++(Natural Video), H.264	H.320, H.323, SIP	от 128 до 2048 кбит/с
2.	Polycom QDX 6000	2011	XGA (1024*768)	H.261, H.263, H.264	H.323	от 128 до 4096 кбит/с
3.	Cisco EX90	2012	1080p (1920*1080)	H.261, H.263, H.263+, H.264	H.323, SIP	от 128 до 6144 кбит/с
4.	Комплекс ПК + ПО TrueConf	2013	1080p (1920*1080)	H.261, H.263, H.263+, H.264	H.323, SIP	от 128 до 6144 кбит/с
5.	LifeSize HD	2017	1080p (1920*1080)	H.261, H.263, H.263+, H.264	H.323, SIP	от 128 до 8172 кбит/с

Анализ применяемых технологий обработки видеоданных показал, что некоторые из них позволяют обеспечить выполнение требований по оперативности и достоверности для ведомственных видеоинформационных

систем. Но не одна из этих технологий не обеспечивает выполнение ведомственных требований по конфиденциальности.

Выполнение ведомственных требований с помощью современного импортного оборудования видеоконференцсвязи (таб. 1.1, таб. 1.2) приводит к существенному увеличению времени обработки и передачи закрытых видеоданных. Откуда можно заключить, что выполнение требований к ведомственным системам видеоконференцсвязи по своевременной доставке закрытого видеопотока обеспечивается только в случае передачи закрытых видеоданных с низким пространственным разрешением. Значит, существует противоречие, обусловленное наличием дисбаланса между требованиями к ведомственным видеоинформационным сервисам и пропускной способностью сети.

В то же время:

– с одной стороны проведенные оценки не учитывают требования относительно обеспечения конфиденциальности;

– с другой стороны существуют угрозы, влияющие на снижение конфиденциальности.

В то же время существует целый комплекс угроз и уязвимостей системы обеспечения информации. Они представлены на рис. 1.8.

Из анализа рис. 1.8 видно, что важным является обеспечение конфиденциальности для ведомственных видеоинформационных ресурсов, используемых в органах внутренних дел Украины. Под конфиденциальностью в ведомственных видеоинформационных системах понимается обязательное требование для лиц, получивших доступ к ведомственной видеоинформации, не передавать ее третьим лицам без получения разрешения руководством.

Рис. 1.8. Угрозы конфиденциальности видеоинформационного ресурса в системе управления МВД Украины

1.6. Постановка цели и задач на исследование

Для выполнения требований по опертивности, достоверности и конфиденциальности в ведомственных инфокоммуникационных системах необходимо разработать метод повышения качества видеосервиса в условиях обеспечения конфиденциальности с использованием стандартизированных MPEG технологий и ГОСТированных алгоритмов криптографической защиты. Здесь обобщающим показателем, учитывающим требования по оперативности, достоверности и конфиденциальности ведомственной сети, является пропускная способность закрытого канала.

Дадим определение пропускная способность закрытого канала с позиции исходного потока:

Определение 1. Под пропускной способностью $H_{зк}$ закрытого видеоканала для ведомственной видеоинформационной системы подразумевается суммарная интенсивность $V_{гк_з}$ закрытого видеопотока, который обрабатывается и передается за требуемое время $T_{тр,д}$ при выполнении условий по конфиденциальности $PSNR_{нсд} \le PSNR_{тр,нсд}$ и достоверности $PSNR_{с} \ge PSNR_{тр,с}$.

Определение 2. Другими словами, под пропускной способностью $H_{зк}$ закрытого видеоканала понимается количество N_K исходных кадров $V_{К_{исх}}$, для которых система обеспечивает закрытие и доставку (обработку $T_{обр}$ и передачу $T_{п}$) за требуемое время $T_{тр,д}$ с необходимой достоверностью $PSNR_{тр,с}$.

С позиции технологии обработки (кодирование, шифрование) и передачи:

Определение 3. Под пропускной способностью $H_{зк}$ закрытого видеоканала для ведомственной видеоинформационной системы подразумевается интенсивность $V_{гк_{код}}$ скрытых кодированных видеоданных, соответствующая такому количеству N_K кадров, которые необходимо обработать $T_{тр,обр}$ и передать $T_{тр,п}$ за требуемое время $T_{тр,д} = T_{тр,обр} + T_{тр,п}$ при обеспечении ведомственных требований по конфиденциальности $PSNR_{нсд} \le PSNR_{тр,нсд}$ и достоверности $PSNR_{с} \ge PSNR_{тр,с}$ с учетом пропускной способности $L_{сети}$ сети.

Пропускная способность закрытого видеоканала зависит от:

1) времени обработки $T_{р,обр}$ (кодирование и шифрование) и передачи $T_{р,п}$ видеопотока. Чем меньше время доставки $T_{р,д}$ кодированного потока, тем больше количество N_K кадров, которые будут обработаны и закрыты за требуемое время $T_{тр,д}$;

2) достоверности $PSNR_с$. Чем меньше значение пикового отношения сигнал/шум $PSNR_с$ при авторизированном доступе, тем меньше интенсивность $V_{гк_{код}}$ кодированного потока и меньше время $T_{р,д}$ доставки. Но при этом нарушается требование $PSNR_с < PSNR_{тр,с}$ по обеспечению заданного уровня $PSNR_{тр,с}$ достоверности;

3) степени $PSNR_{нсд}$ закрытия. Чем меньше значение пикового отношения сигнал/шум $PSNR_{нсд}$ при неавторизированном доступе, тем выше степень закрытия $PSNR_{нсд} \to PSNR_{тр,нсд}$. Чем больше степень скрытия $PSNR_{нсд}$, тем больше разрушаются закономерности при кодировании и поэтому меньше избыточности устраняется, соответственно возрастает интенсивность $V_{гк_{код}}$. Это приводит к снижению пропускной способности $H_{зк}$ закрытого видеоканала.

4) степени насыщенности видеокадров (динамика видеосцены). Чем выше степень насыщенности, тем больше количество структурных единиц $S_{зн}^{(\xi,\gamma)}$, которые закрываются и меньше количество структурных единиц $S_{незн}^{(\xi,\gamma)}$, которые кодируются по стандартному алгоритму. Это приводит к повышению суммарной интенсивности $V_{гк_{код}}$ скрытых видеоданных, а следовательно, к снижению пропускной способности $H_{зк}$ закрытого видеоканала.

Отсюда, для выполнения ведомственных требований к пропускной способности $H_{зк}$ закрытого видеоканала необходимо снизить интенсивность

$N_K \cdot V_{K_{исх}}$ видеоданных в контексте снижения времени передачи, обеспечить их скрытие и доставку за требуемое время $T_{р,д} \le T_{тр,д}$ при необходимых условиях по достоверности $PSNR_с \ge PSNR_{тр,с}$ и конфиденциальности $PSNR_{нсд} \le PSNR_{тр,нсд}$. Тогда формула для оценки пропускной способности $H_{зк}$ закрытого видеоканала в пересчете на исходный поток запишется следующим образом:

$$H_{зк} = N_K \cdot V_{K_{исх}} : T_{р,д} \le T_{тр,д}; PSNR_с \ge PSNR_{тр,с}; PSNR_{нсд} \le PSNR_{тр,нсд},$$

где $V_{K_{исх}}$ – интенсивность исходного видеокадра;

N_K – количество видеокадров, которые передаются при заданных условиях по оперативности, достоверности и конфиденциальности;

$T_{тр,д}$ – требуемое время доставки, приходящееся на группу кадров;

$T_{р,д}$ – реальное время доставки, которое включает в себя время на кодирование, скрытие и передачу видеоданных;

$PSNR_с$ – значение пикового отношения сигнал/шум для доставленного видеокадра при санкционированном доступе;

$PSNR_{нсд}$ – значение пикового отношения сигнал/шум для доставленного видеокадра при несанкционированном доступе;

$PSNR_{тр,с}$ – требуемое значение пикового отношения сигнал/шум для доставленного видеокадра при санкционированном доступе;

$PSNR_{тр,нсд}$ – требуемое значение пикового отношения сигнал/шум для видеокадра при несанкционированном доступе, $L_{сети}$ – пропускная способность сети.

Формула для оценки пропускной способности $H_{зк}$ закрытого видеоканала в пересчете на кодированный поток, соответствующий группе кадров, будет записываться так:

$$H_{зк} = V_{гк_{код}} : T_{р,д} \le T_{тр,д}; PSNR_{с} \ge PSNR_{тр,с}; PSNR_{нсд} \le PSNR_{тр,нсд},$$

где $V_{гк_{код}}$ – интенсивность кодированной группы видеокадров.

С учетом обобщающего показателя, учитывающего требования по оперативности, достоверности и конфиденциальности ведомственной сети, можно сформулировать цель исследования. ***Целью исследования является разработка метода повышения пропускной способности закрытого видеоканала для ведомственных телекоммуникационных систем.***

Частными задачами исследования являются:

– обоснование совершенствования селективной технологии закрытия видеопотока;

– разработка метода повышения пропускной способности закрытого канала на основе внутрикадровой селекции структурных единиц базового кадра для снижения интенсивности передаваемых видеоданных;

– разработка метода декодирования закрытого видеопотока на основе внутрикадровой селекции структурных единиц базового кадра;

– разработка метода оценки пропускной способности закрытого видеоканала на основе на основе интенсивности видеопотока.

Выводы

На основе анализа, проведеного в первом разделе, можно сделать следующие выводы:

1. Обоснована необходимость использования видеоинформационных ресурсов для эффективной работы подразделений и качественного, объективного и своевременного принятия управленческих решений в системе функционирования Министерства внутренних дел Украины. Доказана необходимость применения средств защиты информации для

обеспечения требуемого уровня конфиденциальности в ведомственных системах видеоконференцсвязи.

2. Выявлены проблемные вопросы при организации и проведении сеансов видеоконференцсвязи. К ним относятся:

- отсутствие каналов передачи данных в местах применения систем видеонаблюдения (густо застроенные центральные части больших городов), невозможность прокладки новых проводных каналов связи, сложности с построением беспроводных каналов связи из-за архитектурных особенностей современных зданий и густотой застройки;

- использование низкоскоростных каналов связи и устаревшего каналообразующего оборудования, применяемого между областными и районными подразделениями ОВД, что не позволяет повышать качество передаваемого видеоконтента;

- не обеспечивается выполнение ведомственных требований по конфиденциальности для оборудования, применяемого в ОВД для проведения сеансов ВКС;

3. Обосновано, что для ведомственных телекоммуникационных систем необходимо разработать метод снижения интенсивности закрытых видеоданных в условиях ограничений по достоверности и конфиденциальности.

РАЗДЕЛ 2
ОБОСНОВАНИЕ НАПРАВЛЕНИЯ СОЗДАНИЯ ТЕХНОЛОГИИ СКРЫТИЯ ВИДЕОПОТОКА В ИНФОКОММУНИКАЦИОННЫХ СИСТЕМАХ

Основной задачей при построении ведомственных систем видеоконференцсвязи является обеспечение выполнения требований к этим системам. Сложностью при работе с видеоданными является увеличение интенсивности и времени обработки передаваемой информации при обеспечении необходимого уровня конфиденциальности. Поэтому для повышения эффективности предоставляемых видеоуслуг проводится анализ существующих методов закрытия видеоданных и выявляются недостатки при их интеграции в ведомственные видеоинформационные системы.

Для устранения максимального количества избыточности при закрытии видеопотока используется базовый кадр. На основании этого разрабатывается метод скрытия видеоданных, который базируется на скрытии только I-кадров Таким образом, обеспечивается полное скрытие всей видеопоследовательности при минимальной избыточности.

2.1. Обоснование подхода для обеспечения повышения пропускной способности закрытого видеоканала в системе обработки видеопотока

Существуют различные технологии и решения, которые применяются для защиты видеоданных. Процесс скрытия может быть реализован на разных этапах формирования, обработки и передачи видеоданных, а именно:

1) до кодирования видеопотока (алгоритмы шифрования применяются к вновь созданным (не кодированным) исходным видеоданным; все операции по снижению интенсивности и помехоустойчивому кодированию выполняются с уже скрытыми видеоданными);

2) после того, как сформировано компрессионное представление видеоданных (скрытие видеопотока выполняется после всех операции по снижению интенсивности и помехоустойчивого кодирования, перед тем, как кодированный видеопоток попадает в канал связи);

3) в процессе кодирования (алгоритмы шифрования интегрируются в стандартизированный процесс по обработке исходных видеоданных для снижения их интенсивности (на различных стадиях компрессии MPEG-кодека)).

На рис. 2.1 представлена структурно-функциональная схема обработки видеоданных в инфокоммуникационных сетях с возможными вариантами применения алгоритмов шифрования. [8]

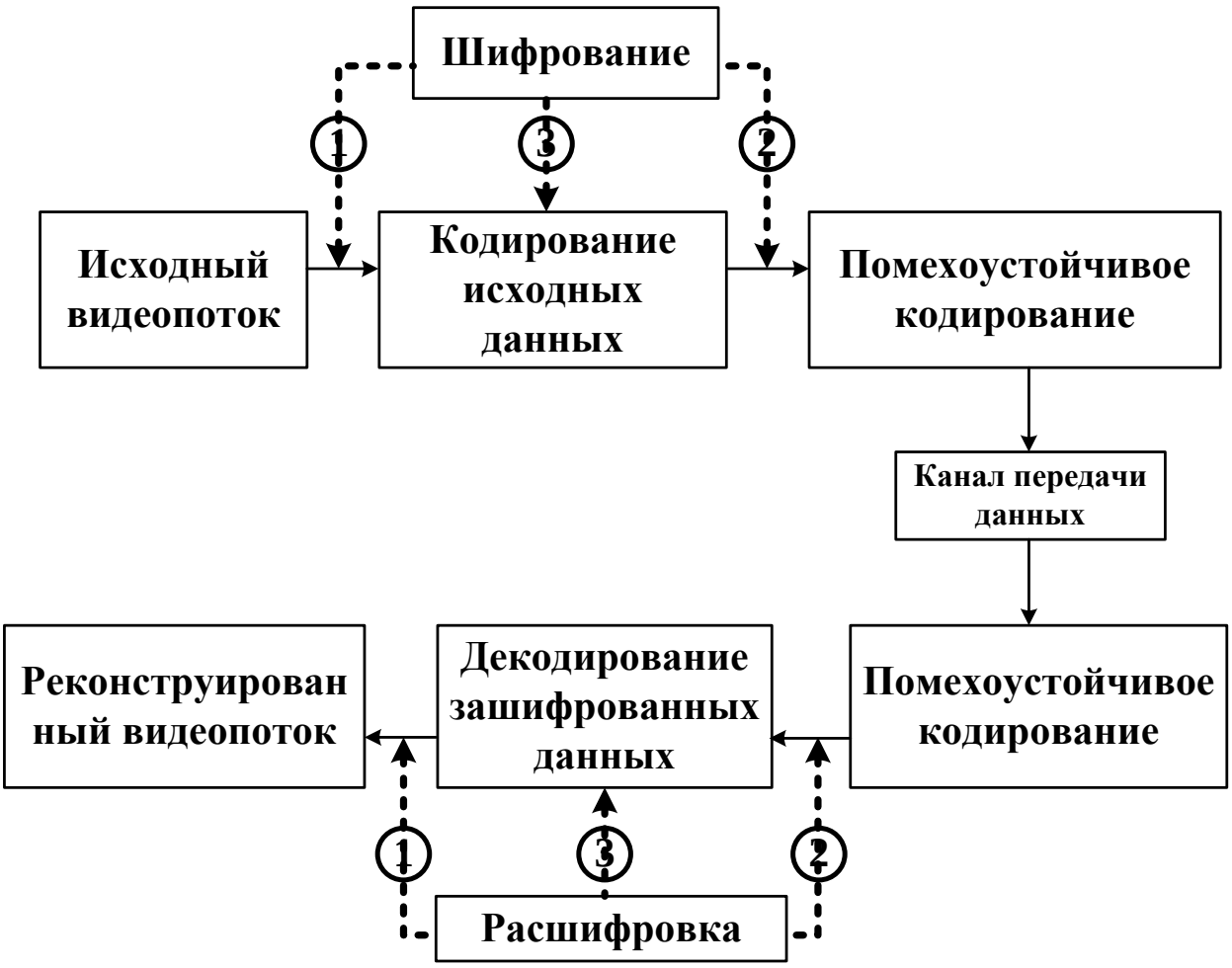


Рис. 2.1. Структурно-функциональная схема обработки видеоданных в инфокоммуникациях с возможными вариантами применения алгоритмов шифрования.

Рассмотрим более подробно варианты возможного применение алгоритмов шифрования к видеопотоковым данным.

Процесс обработки и закрытия видеопотока в ведомственных телекоммуникационных системах определяется временем обработки, которое включает в себя процессы шифрования и кодирования. [16]

Время $T^{(1)}_{\text{шид}}$ шифрования исходного видеопотока рассчитывается по формуле:

$$T^{(1)}_{\text{шид}} = \frac{\partial(N; R_k; G_k)^{(r)}_{\text{ш}}}{S_{\text{вк}}},$$

где $S_{вк}$ – производительность вычислительного комплекса, оцениваемая как количество операций в секунду; $\partial(N; R_k; G_k)^{(r)}_{\text{ш}}$ – количество операций на шифрование, которое зависит от используемого алгоритма r шифрования.

Время на кодирование $T^{(1)}_{\text{сшд}}$ шифрованного видеопотока рассчитывается по формуле:

$$T^{(1)}_{\text{сшд}} = \frac{\partial(V_{\text{шд}})^{(\alpha)}_{\text{сж}}}{S_{\text{вк}}},$$

где $\partial(V_{\text{шд}})^{(\alpha)}_{\text{сж}}$ – количество операций кодирования, которое зависит от используемого алгоритма α кодирования.

Вариант с шифрованием исходных данных до кодирования обладает следующими недостатками:

– не учитывается сокращение избыточности в исходных видеоданных;

– после кодирования происходит увеличение первоначальной интенсивности видеопотока в результате разрушения его структуры за счет предварительного шифрования, это описывает следующее неравенство:

$$V^{(1)}_{\text{сшд}} > V_{\text{сид}},$$

где $V_{сид}$ – интенсивность кодированного видеопотока;

$V^{(1)}_{сшд}$ – интенсивность компактно представленных зашифрованных видеоданных.

– увеличение интенсивности $V^{(1)}_{сшд}$ кодированных шифрованных видеоданных влечет за собой увеличение времени $T^{(1)}_{псш}$ на передачу этих данных в канале связи, что описано неравенством:

$$T^{(1)}_{псш} > T_{псд},$$

где $T_{псд}$ – время передачи кодированного исходного видеопотока.

Для устранения недостатков, которые присутствую в варианте шифрования видеоданных до их компрессии, рассмотрим вариант скрытия видеопотока после его компрессии.

Такой вариант с применением технологии обеспечения конфиденциальности к уже кодированным видеоданным позволяет сократить предварительную избыточность исходного видеопотока и снизить время на шифрование. Он обеспечивает высокий уровень закрытия информации, но при этом обладают существенными недостатками:

1) при ошибках в канале связи происходит размножение ошибок;

2) криптографической обработке подлежит весь видеоинформационный поток, из-за чего увеличивается суммарное время обработки формируемых видеоданных на передающей стороне и время обработки видеоданных на принимающей стороне.

Рассмотренные варианты обладают такими недостатками как:

а) закрытие видеопотока происходит не в он-лайн режиме;

б) ограничения, накладываемые на производительность вычислительных систем, не позволяют применять современные методы компрессии и шифрования;

в) интенсивность закрытого видеопотока зачастую значительно превышает интенсивность исходного.

Поэтому для устранения недостатков предлагается использовать вариант, в котором данные закрываются в процессе их кодирования – селективный подход. Такая реализация представлена на рис.2.2 и применяется в случаях обработки и передачи данных в системах реального времени (например, ВКС, где возможна дополнительная программная и аппаратная интеграция в видеокодек). Для такого варианта кодирование и шифрование выполняются для исходных данных по мере поступления их на обработку. [77]

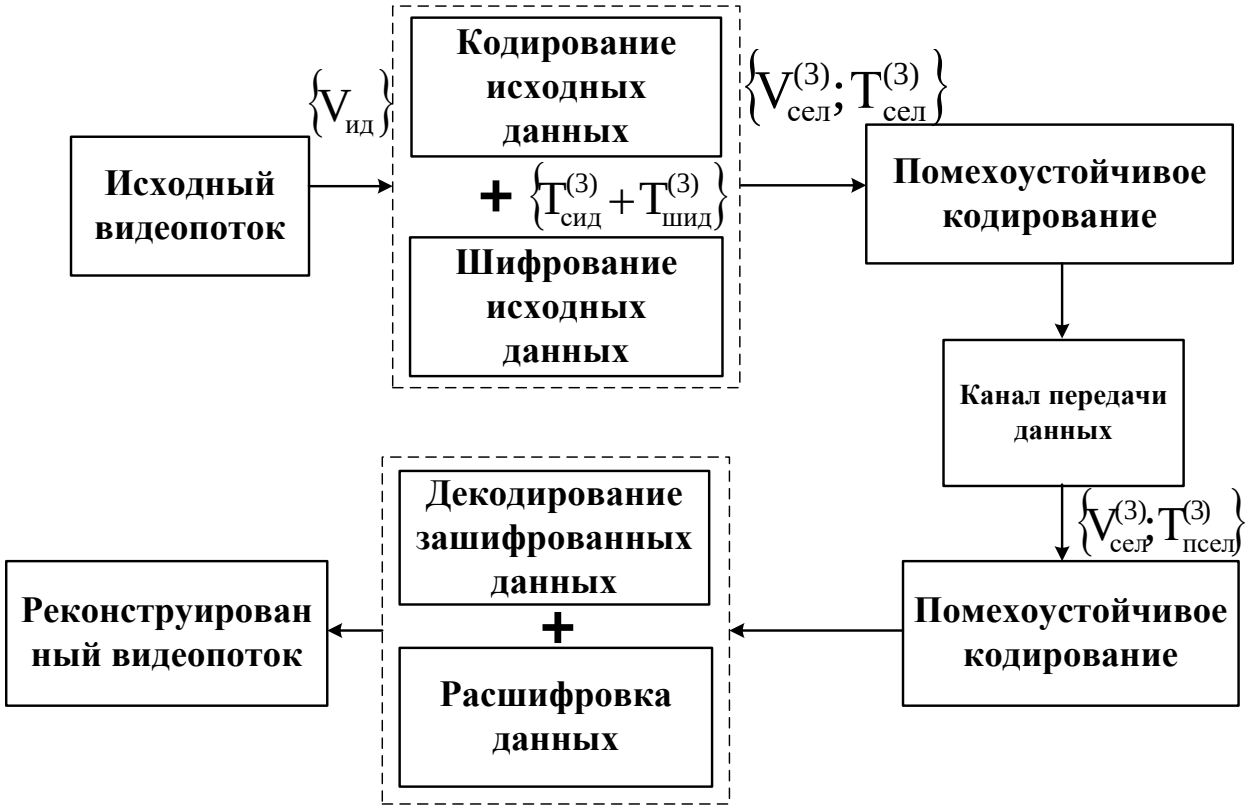


Рис. 2.2. Структурно-функциональная схема обработки данных в инфокоммуникациях с применением алгоритмов шифрования в процессе кодирования (селективный подход).

В процессе формирования видеоинформационного потока достигается повышение информативности передаваемых конструкций и сокращение первоначальной интенсивности. Это позволяет:

– устранить избыточность, которая свойственна любому исходному видеопотоку, а следовательно, снизить количество информации, которая может использоваться при криптоанализе;

– снизить время шифрования за счет уменьшения длины обрабатываемых сообщений.

Из общей структуры видеопотока следует то, что интенсивность $V_{сел}^{(3)}$ обрабатываемых данных с применением селективного подхода шифрования будет превышать интенсивность $V_{сшд}^{(1)}$ кодированных исходных данных, но меньше интенсивности $V_{ид}$ исходных видеоданных:

$$V_{сид} < V_{сел}^{(3)} < V_{ид}.$$

Интенсивность $V_{сел}^{(3)}$ обрабатываемых данных с применением селективного шифрования будет больше интенсивности $V_{сшд}^{(1)}$ зашифрованных кодированных исходных данных и меньше интенсивности $V_{шсд}^{(2)}$ кодированных зашифрованных видеоданных из-за внедрения алгоритмов шифрования:

$$V_{сшд}^{(1)} > V_{сел}^{(3)} > V_{шсд}^{(2)}.$$

Рассмотрев вышеизложенный материал, можно сделать вывод о том, что селективный подход обладает рядом преимуществ при закрытии и передаче видеоданных, а именно:

1) время $T_{сел}$ на обработку и передачу видеоданных с применением селективного шифрования затрачивается меньше, чем при шифровании до процедуры кодирования $T_{обр}^{(1)}$:

$$T_{сел} < T_{обр}^{(1)};$$

2) интенсивность $V_{сел}^{(3)}$ данных с применением селективного шифрования будет меньше интенсивности данных, которые сначала шифруются, а потом кодируются:

$$V_{сел}^{(3)} < V_{сшд}^{(1)}.$$

В то же время в селективном подходе существуют такие недостатки:

–время $T_{сел}$ на передачу скрытых видеоданных увеличивается по сравнению с методом, в котором шифрование применяется после процедуры кодирования $T_{обр}^{(2)}$:

$$T_{сел} < T_{обр}^{(2)};$$

– интенсивность $V_{сел}^{(3)}$ поступающих в канал связи видеоданных больше, чем интенсивность $V_{шсд}^{(2)}$ данных, которые сначала кодируются, а потом шифруются:

$$V_{сел}^{(3)} > V_{шсд}^{(2)}.$$

Внедрение алгоритмов шифрования в процессе кодирования способствует уменьшению эффективности процесса снижения интенсивности:

$$\kappa_{сел} < \kappa_{исх}.$$

где $\kappa_{сел}$ – коэффициент снижения интенсивности при использовании селективной обработки видеопотока;

$\kappa_{исх}$ – коэффициент снижения интенсивности при обработке видеоинформационных потоков стандартизированными алгоритмами компрессии.

Результатом этого является увеличение интенсивности поступающих в канал видеоинформационных потоков. [79]

Селективные методы шифрования имеют простую реализацию, не требуют значительных вычислительных ресурсов, повышают помехоустойчивость всего видеопотока. При несанкционированном перехвате такого видеопотока с ошибками, в процессе расшифровке количество этих ошибок будет только увеличиваться. [59]

Рассмотрены варианты реализации процесса скрытия на разных этапах формирования, обработки и передачи видеоинформационного потока. Обосновано, что наиболее эффективным является применение селективных методов скрытия для ведомственных видеоинформационных систем с позиции обеспечения требований по оперативности, достоверности и конфиденциальности является селективный метод, где обработка и передача видеоданных осуществляется в реальном времени.

2.2. Разработка рекомендаций относительно развития селективных методов обработки информационных потоков на основе скрытия базового видеокадра

Видеопоток имеет определенную структуру, которая состоит из нескольких уровней: собственно сам видеопоток (sequence), группа кадров

(GOP –GroupOfPictures), слайс (slice), макроблок (macroblock) и блок (block). Структура видеопотока представлена на рис. 2.3. [35]

Как видно из структуры (рис. 2.3), процесс формирования видеопотока основан на последовательном построении цепочки видекадров разного типа. Под типом кадров видеопотока подразумевается способ кодирования и хранения информации об очередном кадре, отличающемся друг от друга наличием или отсутствием зависимостей этого кадра от предыдущего и последующего.

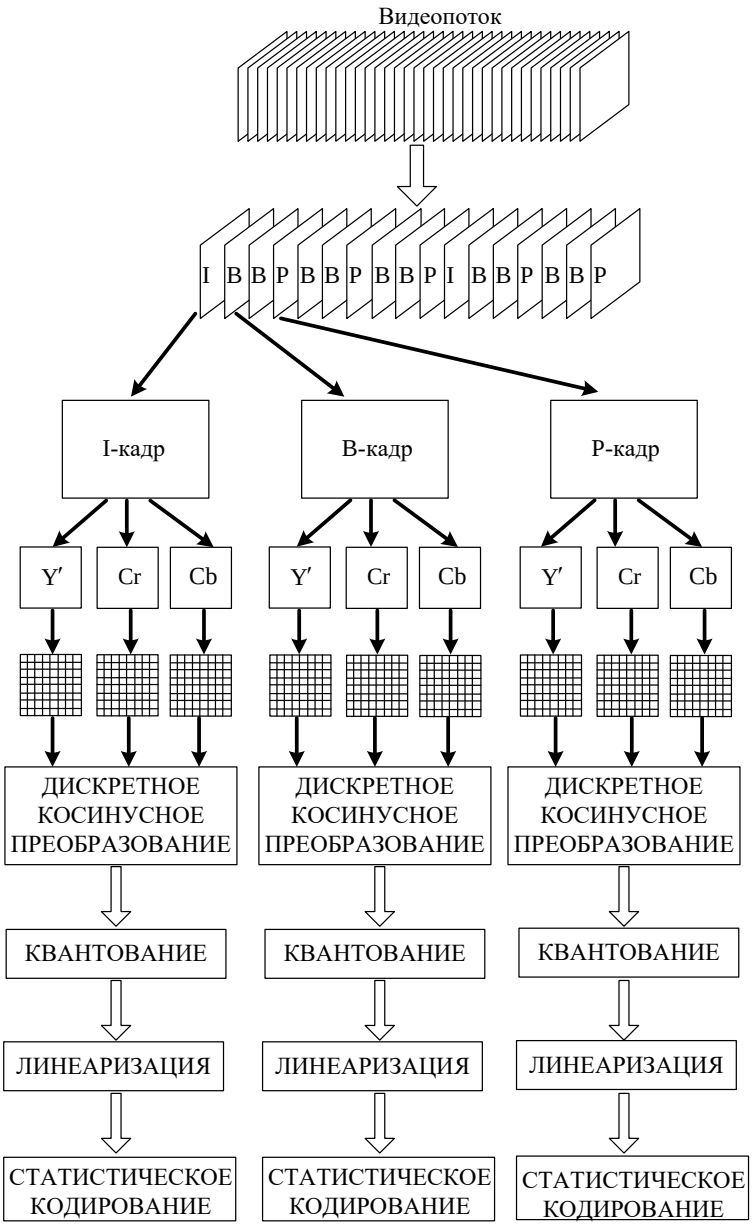


Рис. 2.3. Структурная схема видеопотока MPEG.

Весь видеопоток состоит из последовательно сформированных групп видеокадров. [42] Группа может состоять из разного количества видеокадров. Каждая группа видеокадров в соответствии с MPEG-стандартом состоит из трех типов видеокадров:

- I-кадры (intra) называются ключевыми (keyframes) или «базовыми» и содержат только независимо сжатые макроблоки.

- P-кадры (predicted) называются «разностными» и могут содержать как независимо сжатые макроблоки, так и макроблоки со ссылкой на другой I- или P-кадр.

- B-кадры (bi-predicted) – «двунаправленные», «обратные» кадры могут содержать следующие макроблоки: независимые, со ссылкой на один кадр или со ссылкой на 2 кадра. B-кадры ссылаются на ближайшие I-,P или B-кадры.

Наиболее часто, используются сложные последовательности кадров, которые обеспечивают более сильную компрессию видео. [4] Например, она может быть такой: IBBPBBPBB или IBBPBBPBBPBBPBBPBBPBBPBBP, или иной в зависимости от метода обработки. Базовой схемой построения MPEG-видеопотока является последовательность групп кадров, состоящих из 8 или 12 кадров и имеющих вид IBBPBBPB (1 I-кадр, 2 P-кадра, 5 B-кадров) или IBBPBBPBBPBB (1 I-кадр, 3 P-кадра, 8 B-кадров). [49] Количество кадров $N_{гк}$ в группе кадров можно описать следующим образом:

$$N_{гк} = N_I + N_P + N_B,$$

где N_I – количество I-кадров в группе кадров;

N_P – количество P-кадров в группе кадров;

N_B – количество B-кадров в группе кадров.

До кодирования все кадры в группе кадров имеют одинаковый объем, так как он зависит от глубины цвета, используемых для кодирования цвета пикселя и размера изображения. Поэтому имеет место равенство:

$$V_k = V_I = V_P = V_B,$$

где V_k – интенсивность видеокадра;

V_I – интенсивность I-кадра;

V_P – интенсивность P-кадра;

V_B – интенсивность B-кадра.

Наиболее значимым является I-кадр, так как в нем содержится максимальное количество информации, а кадры других типов содержат до 70% ссылок на него. Поэтому к дальнейшему рассмотрению предлагается проводить обработку базового I-кадра. [6]

Реализация селективного метода шифрования возможна на различных уровнях формирования базового видеокадра. Иерархия формирования кадра выделяет несколько уровней: собственно сам кадр, слайс, макроблок и блок. Внедрение алгоритмов селективного шифрования возможно на различных уровнях формирования видеокадра. Это представлено на рис. 2.4. [10]

Рассмотрим различные варианты интеграции алгоритмов селективного шифрования на различных уровнях формирования видеокадра:

– шифрование всего I-кадра;

– шифрование слайсов. Слайсы содержат заголовоки об одном или более смежных макроблоках, которые упорядочены слева-направо и сверху вниз. Группирование макроблоков в слайс позволяет усилить устойчивость к сбоям и ошибкам в потоке;

– шифрование макроблока (представляет собой квадратный фрагмент кадра размером 16x16 пикселей и состоит из четырех Y, Cb, Cr блока. В свей структуре он также имеет заголовок, вектор движения и параметры формата субдискретизации). [85]

На данном этапе формирования видеокадра возможно применение таких методов как:

1) шифрование макроблоков;

2) шифрование вектора движения (данное решение скрывает алгоритм изменения блоков в видеопотоке);

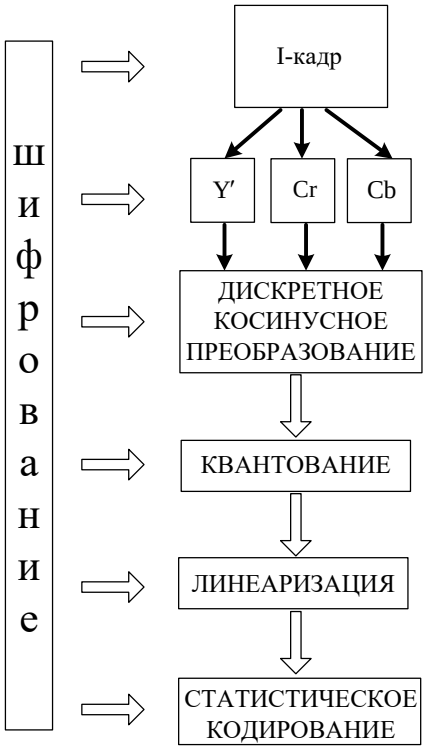


Рис. 2.4. Структурно-функциональная схема интеграции алгоритмов селективного шифрования на различных уровнях формирования видеокадра.

– шифрование макроблока. На этом уровне блок представляет собой квадратную матрицу 8x8 пикселей яркости или насыщенности. [93] Над матрицами производится прямое дискретное косинус-преобразование (ДКП) каждого блока (разложение в спектр). Одномерное ДКП по дискретным значениям амплитуды сигнала формирует вектор длины, состоящий из коэффициентов разложения. [117] То есть, рассматривая строку матрицы как вектор значений амплитуды некоего сигнала, можно применить одномерное ДКП. В результирующем векторе сначала будут находиться низкочастотные, а в конце – высокочастотные компоненты сигнала. [9] После обработки строк матриц, ДКП применяется для столбцов. В итоге получается матрица коэффициентов разложения, которая в левом верхнем углу содержит низкочастотные составляющие, а правом нижнем – высокочастотные. Далее идет процесс квантования коэффициентов разложения, а по сути уменьшение динамического диапазона, путем деления на матрицы квантования. [91] В связи с тем, что цветовая характеристика элементов изображения имеет

сильную пространственную корреляцию (то есть соседние пиксели обычно не очень сильно отличаются друг от друга), в полученном спектре будут преобладать низкочастотные составляющие. [108] Поэтому появляется возможность провести не статическое квантование, а адаптированное, то есть не делить на матрицы из одинаковых элементов, а подобрать коэффициенты наиболее удобным образом, чтобы исключить излишнюю информацию о высокочастотной составляющей. В связи с этим матрицы квантования в левом верхнем углу содержат минимальные по модулю делители, а в правом нижнем – максимальные. После квантования часть коэффициентов из-за выравнивания сравняется, а большинство малых коэффициентов округлится до нуля, образовав подобласти с нулевым значением. [12] Это обстоятельство позволяет произвести упаковку длинных цепочек одинаковых значений методом группового кодирования (RLE, RunLengthEncoding). Для этого квадратная матрица преобразуется зиг-заг обходом в вектор, и цепочки повторяющихся коэффициентов упаковываются в пары (длина, значение). [13] На данном этапе возможно реализовать:

1) шифрование высокочастотных и среднечастотных составляющих;

2) шифрование длин нулевых цепочек;

– шифрование на уровне статистического кодирования. Здесь возможно применение таких методов, как:

1) замена таблиц Хаффмана;

2) использование алгоритма нарушения префиксности.

Анализ различных вариантов селективного шифрования показал, что наиболее эффективным является шифрование после этапа дискретного косинусного преобразования. [44]

К рассмотрению предлагается разработка селективного метода скрытия видеоданных на основе шифрования базового видеокадра. Структурная схема кодирования видеопотока для селективного подхода с закрытием базового I-кадра представлена на рис. 2.5.

Ниже представлены этапы кодирования исходного видеопотока в селективном подходе:

1. Покадровое распределение исходного видеопотака (выделение кадров I, P и B типов из группы кадров для дальнейшей обработки).

2. Преобразование исходного видеокадра в цветовое пространство YUV. В результате применения разложения цветового пространства на яркостную и цветовые составляющие достигается лучшая степень сжатия. [92] На данном этапе кодирования с помощью соответствующих соотношений цветовая модель RGB преобразуется в YCbCr:

3. Субдискретизация компонентов яркости и цветности (рис. 2.6). Составляющие цветности (Cb и Cr) содержат высокочастотную цветовую информацию, к которой глаз человека менее чувствителен. Поэтому определенная ее часть может быть отброшена и, тем самым, можно уменьшить количество учитываемых пикселей для каналов цветности.

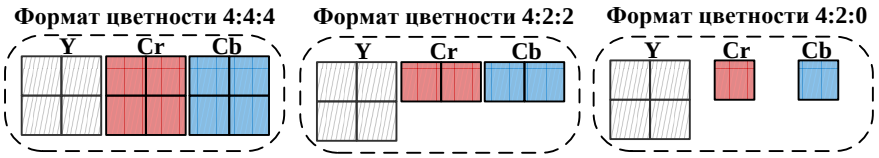


Рис. 2.7. Схема субдискретизации компонентов яркости и цветности.

4.1. Предсказание вперед по предыдущему I или P кадру. P-кадры сжимаются с использованием предшествующих I- или P-кадров с помощью предсказывающего кодирования и компенсации движения (так называемое предсказание вперед, устраняющее временную избыточность), что обеспечивает увеличение степени сжатия. [5]

4.2. Предсказание вперед или назад по I или P кадру. B-кадры сжимаются с использованием двунаправленного предсказания, т.е. с привлечением предшествующих и последующих I- и P-кадров.

5.1. Формирование разностного кадра с применением алгоритма дифференциальной импульсно-кодовой модуляции. [112]

5.2. Формирование промежуточного кадра с использованием метода интерполирования.

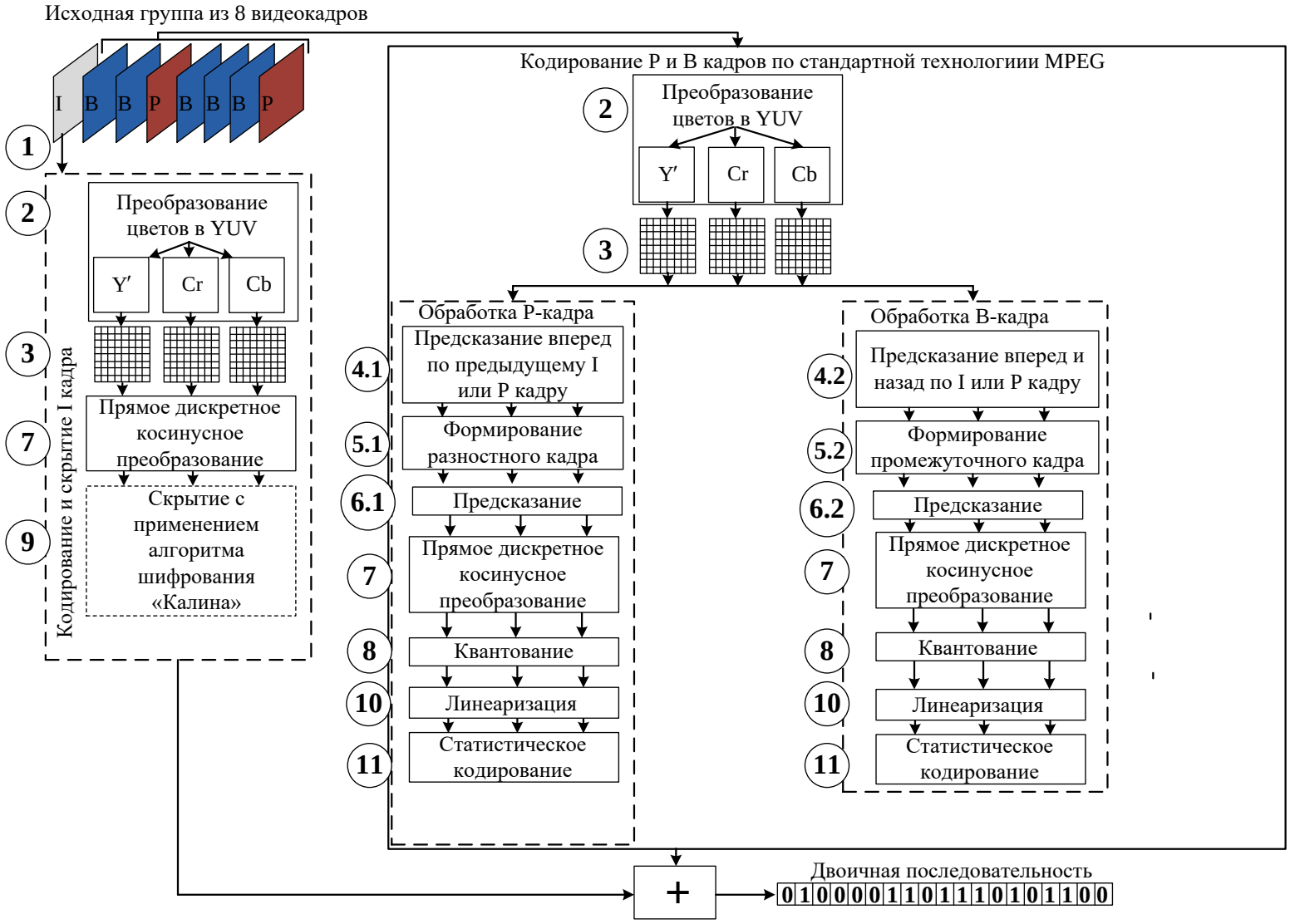


Рис. 2.5. Схема кодирования видеопотока в селективном подходе со скрытием I-кадра.

6.1. Кодирование P-кадров с использованием алгоритмов компенсации движения и предсказания вперед по предшествующим I или P кадрам. Для такого кодирования применяется дифференциальная импульсно-кодовая модуляция (ДИКМ) – метод кодирования, который основывается на предположении наличия корреляционной связи между соседними отсчетами изображения. [24]

6.2. При кодирования B-кадров применяется компенсация движения и предсказание вперед по ближайшим предшествующим опорным I или P кадрам. При интерполяционном (двунаправленном) предсказании оценка выполняется по известным значениям предшествующих и последующих отсчетов с применением алгоритмов интерполяции.

7. Применение дискретных косинусных преобразований для уменьшения избыточности изображения.

8. Для скрытия I-кадра к нему применяется гарантированное шифрование по алгоритму «Калина». [124]

9. Линеаризация матриц квантовая.

$$[M * N] \Rightarrow (M_0, N_0), (M_0, N_1), (M_1, N_0), (M_2, N_0) \ldots (M_7, N_7),$$

где $[M * N]$ – размер матрицы квантования.

10. Статистическое кодирование результирующих коэффициентов с применением алгоритмов группового кодирования и алгоритма Хаффмана для удаления избыточности информации. [57]

Структурная схема декодирования видеопотока в селективном подходе с закрытием базового I-кадра представлена на рис. 2.8.

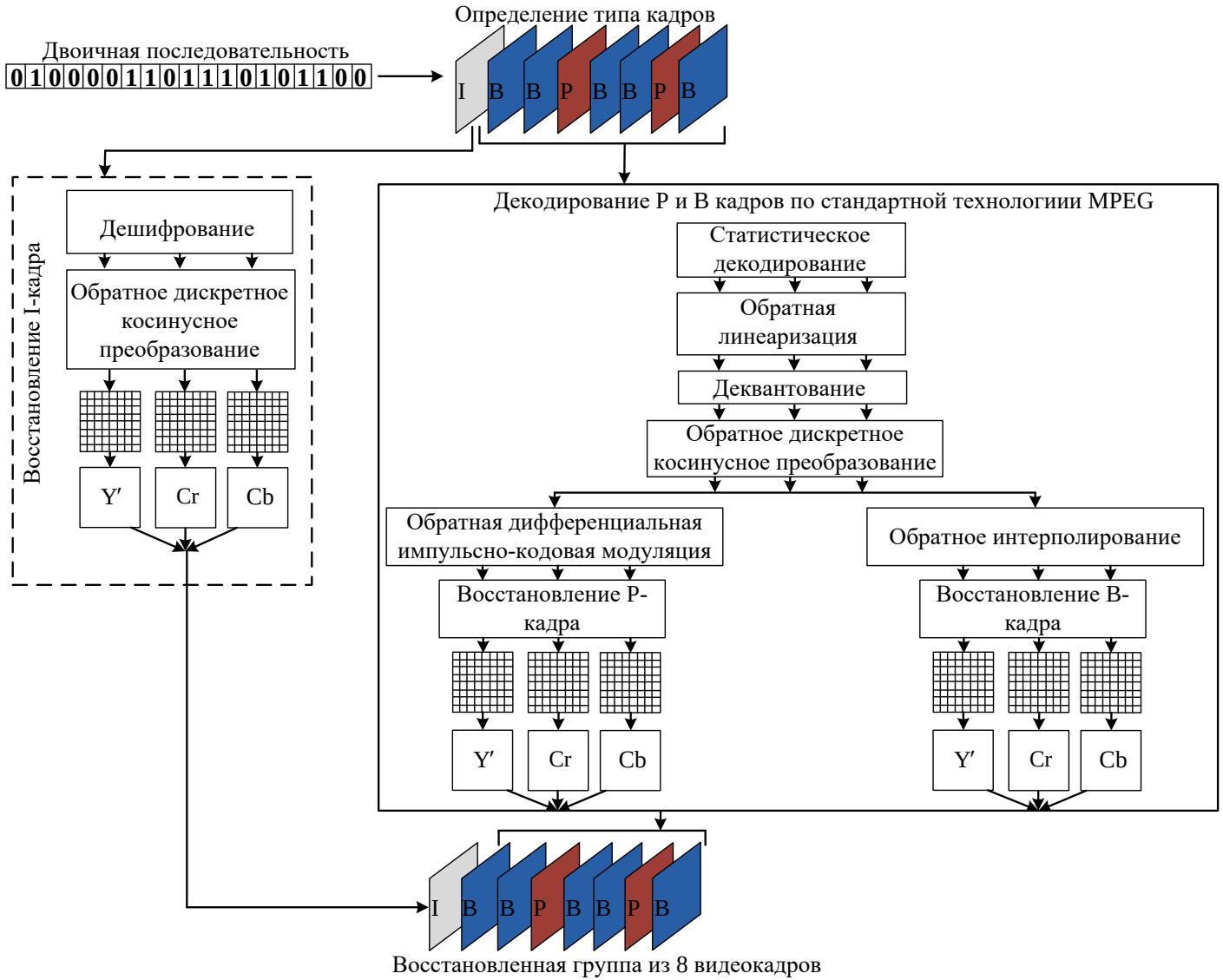


Рис. 2.8. Схема декодирования видеопотока в селективном подходе со скрытием I-кадра.

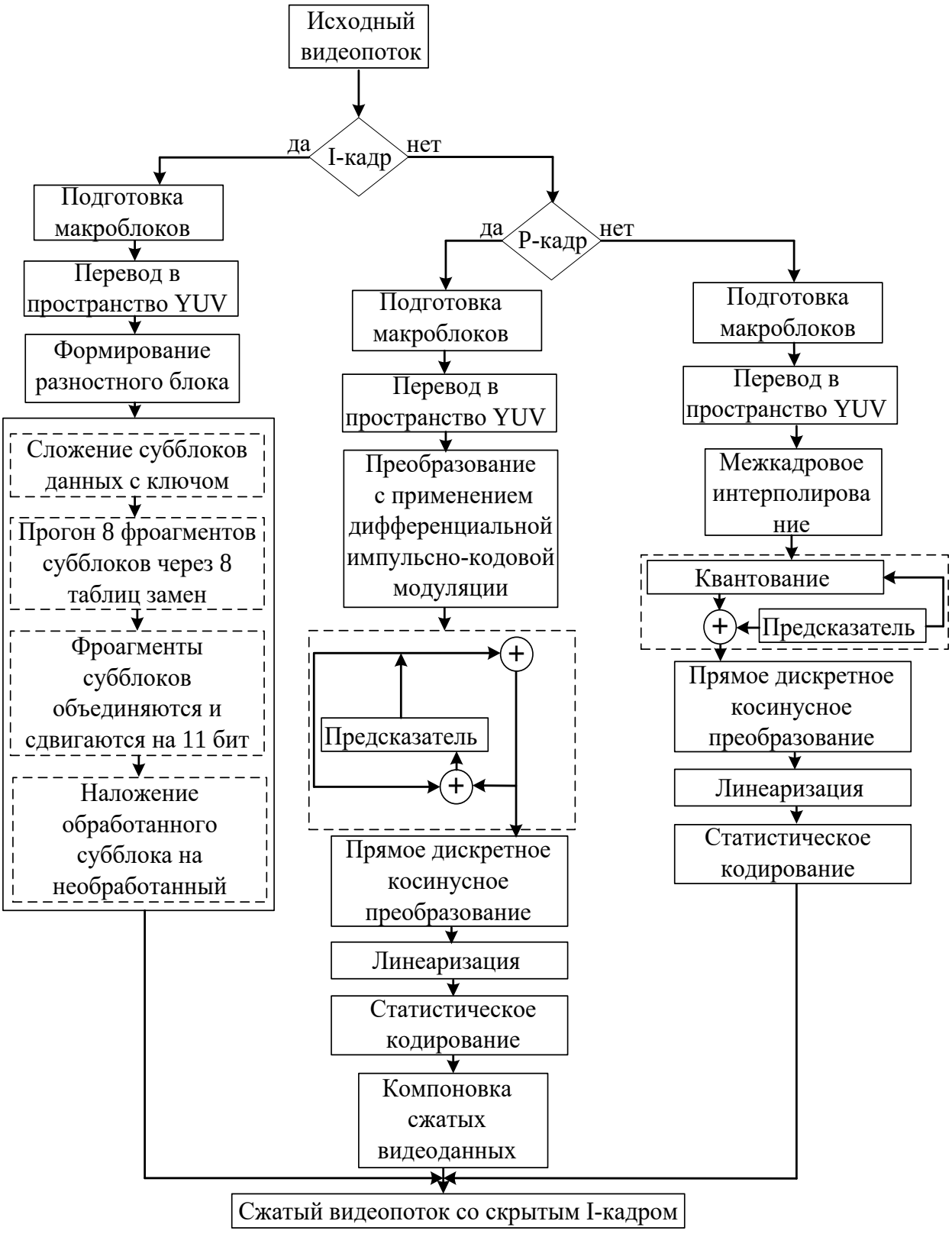


Рис. 2.9. Алгоритм кодирования видеопотока в селективном подходе со скрытием I-кадра.

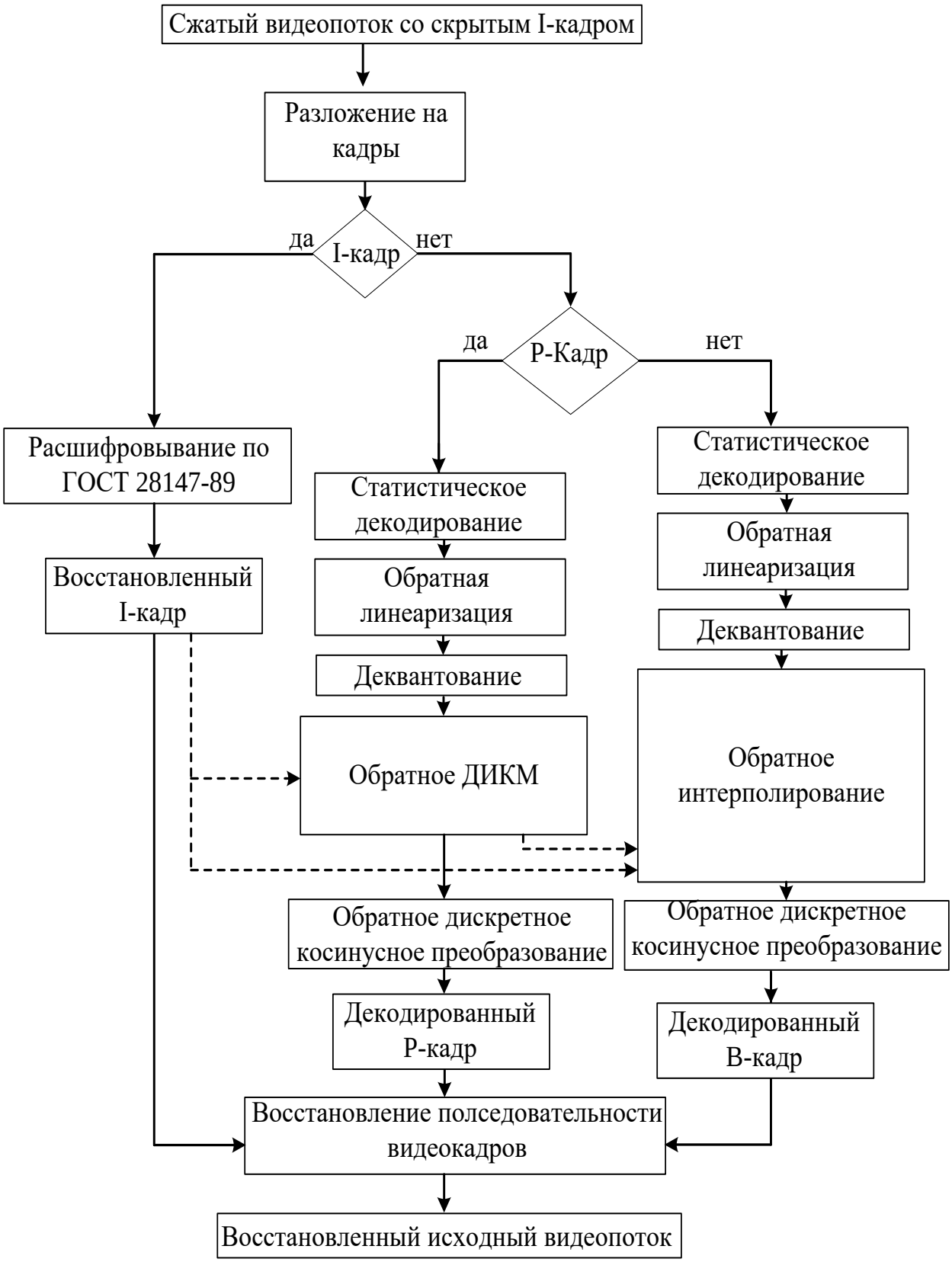


Рис. 2.10. Алгоритм декодирования видеопотока в селективном подходе со скрытием I-кадра.

Проведен анализ вариантов интеграции алгоритмов селективного шифрования на различных уровнях формирования видеокадра. В результате чего разработан метод селективной обработки видеоданных на основе скрытия базового видеокадра после этапа дискретного косинусного преобразования.

2.3 Оценки степени скрытия видеопотока для селективного метода обработки для базового видеокадра

Проведем экспериментальные исследования по селективному методу скрытия базового кадра. Целью эксперимента является:

– оценка влияния базового кадра на другие кадры в группе видеокадров;

– оценка восстановленного B-кадра при скрытом базовом видеокадре в случае несанкционированного доступа.

В ходе эксперимента обрабатывался I-кадр с различным качеством (34%, 67%, 100%), которое определяется значениями пикового отношения сигнал/шум ($PSNR = 6.0912$, $PSNR = 6.1062$, $PSNR = 6.1798$). Базовый видеокадр подвергался шифрованию алгоритмом гарантированной защиты «Калина» после этапа дискретного косинусного преобразования перед этапом квантования (в процессе кодирования). После чего предпринимались попытки восстановления его дифференцированного представления (B-кадра) при закрытом базовом I-кадре. Результаты экспериментов представлены на рисунках 2.11, 2.12, 2.13, где а) это базовый видеокадр при авторизированном доступе; б) дифференцированное представления базового кадра (B-кадра) при авторизированном доступе; в) восстановленое дифференцированное представление (B-кадра) при закрытом базовом I-кадре при неавторизированном доступе.

а) б) в)

Рис. 2.11. Восстановление дифференцированного представления базового кадра при зашифрованном базовом с качеством 34%, $\kappa = 2.1086$, $PSNR = 6.0912$.

а) б) в)

Рис. 2.12. Восстановление дифференцированного представления базового кадра при зашифрованном базовом с качеством 67%, $\kappa = 2.0557$, $PSNR = 6.1062$.

а) б) в)

Рис. 2.13. Восстановление дифференцированного представления базового кадра при зашифрованном базовом с качеством 100%, $\kappa = 1.6328$, $PSNR = 6.1798$.

По результатам эксперимента (рис. 2.11, 2.12, 2.13.) видно, что при неавторизированном доступе происходит полное разрушение фона изображения B-кара, а разрушение наиболее значимых объектов происходит за

счет размытия их контуров. В целом видно, что только при закрытии базового I-кадра обеспечивается достаточная конфиденциальность всего видеопотока.

Интенсивность $V_{гк}$ закодированной группы кадров будет состоять из суммы интенсивностей закодированного представления кадров всех типов, и будет иметь вид:

$$V_{гк} = V_{I,\Sigma} + V_{P,\Sigma} + V_{B,\Sigma}, \quad (2.1)$$

где $V_{I,\Sigma}$ – суммарная интенсивность закодированного представления I-кадров в группе кадров;

$V_{P,\Sigma}$ – суммарная интенсивность закодированного представления P-кадров в группе кадров;

$V_{B,\Sigma}$ – суммарная интенсивность закодированного представления B-кадров в группе кадров.

Интенсивность закодированных видеоданных зависит от коэффициента снижения интенсивности [97], который является основной характеристикой алгоритма кодирования и определяется как отношение интенсивность исходных не кодированных данных к интенсивности кодированных, т.е.:

$$к = \frac{V_{ид}}{V_{сж}}, \quad (2.2)$$

где к – коэффициент снижения интенсивности;

$V_{ид}$ – интенсивность исходного видеопотока;

$V_{сж}$ – интенсивность закодированного видеопотока.

Таким образом, чем выше коэффициент снижения интенсивности, тем алгоритм эффективнее. Следует отметить, что:

если $\kappa=1$, то алгоритм не производит компрессии, то есть выходные данные оказываются по интенсивности равными входными;

если $\kappa<1$, то алгоритм порождает данные большего размера, нежели несжатые, то есть, совершает не эффективную работу.

Коэффициент снижения интенсивности для кадров разных типов будет различным из-за использования разных технологий компрессии. [126] Соответственно коэффициент снижения интенсивности κ_I для I-кадров будет самым низким из-за их большой насыщенности, $\kappa_i \to 1$. Коэффициент снижения интенсивности κ_P для P-кадров выше, чем для I-кадров, но меньше, чем для B-кадров. Коэффициент снижения интенсивности κ_B для B-кадров будет самым высоким из-за меньшей степени квантизации и формата цветового представления. [52]

Интенсивность $V^{сж}$ кодированного представления для кадра, в зависимости от его типа, будет иметь следующий вид:

$$V_I^{сж} = \frac{V_I}{\kappa_I},\ V_P^{сж} = \frac{V_P}{\kappa_P},\ V_B^{сж} = \frac{V_B}{\kappa_B},$$

где $V_I^{сж}$ – интенсивность кодированного I-кадра;

$V_P^{сж}$ – интенсивность кодированного P-кадра;

$V_B^{сж}$ – интенсивность кодированного B-кадра;

κ_I – коэффициент сжатия для I-кадров;

κ_P – коэффициент сжатия для P-кадров;

κ_B – коэффициент сжатия для B-кадров.

Суммарная интенсивность кодированного представления кадров каждого типа в группе кадров будет иметь вид:

$$V_{I,\Sigma}^{сж} = N_I \cdot V_I^{сж},\ V_{P,\Sigma}^{сж} = N_P \cdot V_P^{сж},\ V_{B,\Sigma}^{сж} = N_B \cdot V_B^{сж},$$

где $V_{I,\Sigma}^{сж}$ – суммарная интенсивность кодированного представления I-кадра в группе кадров;

$V_{P,\Sigma}^{сж}$ – суммарная интенсивность кодированного представления P-кадров в группе кадров;

$V_{B,\Sigma}^{сж}$ – суммарная интенсивность кодированного представления B-кадров в группе кадров.

Формулы для расчета суммарной интенсивности кодированного представления кадров каждого типа с учетом выражения (2.2) будут иметь вид:

$$V_{I,\Sigma}^{сж} = N_I \cdot \frac{V_I}{\kappa_I},\ V_{P,\Sigma}^{сж} = N_P \cdot \frac{V_P}{\kappa_P},\ V_{B,\Sigma}^{сж} = N_B \cdot \frac{V_B}{\kappa_B}.$$

Тогда формула для определения интенсивности $V_{гк}^{сж}$ кодированного представления группы кадров будет иметь вид:

$$V_{гк}^{сж} = V_{I,\Sigma}^{сж} + V_{P,\Sigma}^{сж} + V_{B,\Sigma}^{сж} = N_I \cdot V_I^{сж} + N_P \cdot V_P^{сж} + N_B \cdot V_B^{сж},$$

$$V_{гк}^{сж} = \sum^{N_I} \frac{V_I}{\kappa_I} + \sum^{N_P} \frac{V_P}{\kappa_P} + \sum^{N_B} \frac{V_B}{\kappa_B} = N_I \cdot \frac{V_I}{\kappa_I} + N_P \cdot \frac{V_P}{\kappa_P} + N_B \cdot \frac{V_B}{\kappa_B}.$$

С учетом того, что исходные интенсивности всех кадров равны (2.1) формула для определения интенсивности $V_{гк}^{сж}$ кодированного представления группы кадров будет иметь вид:

$$V_{гк}^{сж} = V_k \left(\frac{N_I}{\kappa_I} + \frac{N_P}{\kappa_P} + \frac{N_B}{\kappa_B} \right).$$

Для определения влияния потерь на степень снижения интенсивности базового I-кадра в группе кадров необходимо рассчитать его интенсивность в группе кадров. [31] В процентном соотношении $V_I^{сж\%}$ интенсивность кодированного представления I-кадров в группе кадров имеет вид:

$$V_I^{сж\%} = \frac{V_{I,\Sigma} \cdot 100\%}{V_{гк}} = \frac{N_I \cdot \frac{V_I}{\kappa_I} \cdot 100\%}{N_I \cdot \frac{V_I}{\kappa_I} + N_P \cdot \frac{V_P}{\kappa_P} + N_B \cdot \frac{V_B}{\kappa_B}}. \quad (2.3)$$

С учетом выражения (2.1) и количества I-кадров в группе кадров $N_I = 1$, выражение (2.3) будет иметь вид:

$$V_I^{сж\%} = \frac{100\%}{1 + \frac{\kappa_I}{\kappa_P} N_P + \frac{\kappa_I}{\kappa_B} N_B},$$

где $$1 > \frac{\kappa_I}{\kappa_P} > \frac{\kappa_I}{\kappa_B}.$$

Данное выражение для группы из 8 кадров будет иметь вид:

$$V_{I(8)}^{сж\%} = \frac{100\%}{1 + 2\frac{\kappa_I}{\kappa_P} + 5\frac{\kappa_I}{\kappa_B}}.$$

С учетом зависимости коэффициентов κ снижения интенсивности от PSNR пикового отношения сигнал/шум для реалистических изображений

(таб. 2.1.) интенсивность $V_I^{сж\%}$ кодированного представления I-кадров в $V_{гк}$ группе из 8 кадров будет иметь значения, указанные на графике (рис. 2.6).

Из выражения (2.3) видно, что суммарная интенсивность конкретного типа кадров в группе кадров зависит от их количества в группе кадров и от коэффициента сжатия, и не зависит от интенсивности этих кадров. [101]

В таб. 2.1 указаны коэффициенты κ снижения интенсивности для реалистического средненасыщенного кадра без учета компенсации движения при определенных значениях PSNR пикового отношения сигнал/шум. [65]

Таблица 2.1

Зависимость κ коэффициента степени сжатия от PSNR пикового отношения сигнал/шум для реалистических изображений средней насыщенности.

	Пиковое отношение сигнал/шум, PSNR (дБ)						
	50	45	40	35	30	25	23
Коэффициент κ снижения интенсивности	1,3	2,1	2,9	4,5	6,8	16	28

Так как при больших отношениях сигнал/шум возрастает погрешность, то для расчета коэффициента снижения интенсивности будут использоваться следующие значения:

– для определения коэффициента снижения интенсивности κ_I I-кадров будет использоваться пиковое отношение сигнал/шум $PSNR = 50;45;40$ дБ;

– для определения коэффициента снижения интенсивности κ_P P-кадров будет использоваться пиковое отношение сигнал/шум $PSNR = 40;35;30$ дБ;

– для определения коэффициента снижения интенсивности κ_B B-кадров будет использоваться пиковое отношение сигнал/шум $PSNR = 30;25;23$ дБ.

В процессе шифрования разрушается структура видеокадра, поэтому стандартизированный алгоритм обработки кадра не производит компресии и является неэффективным [17]. В таком случае исходные данные оказываются по интенсивности равными закодированным, тогда коэффициент снижения интенсивности $\kappa=1$. Следовательно, интенсивность зашифрованного кодированного представления видеокадра будет больше интенсивности исходного кодированного представления видеокадра. [48] На рис. 2.14 представлен сравнительный график селективно обработанного и кодированного представления видеокадра в зависимости от пикового значения сигнал/шум.

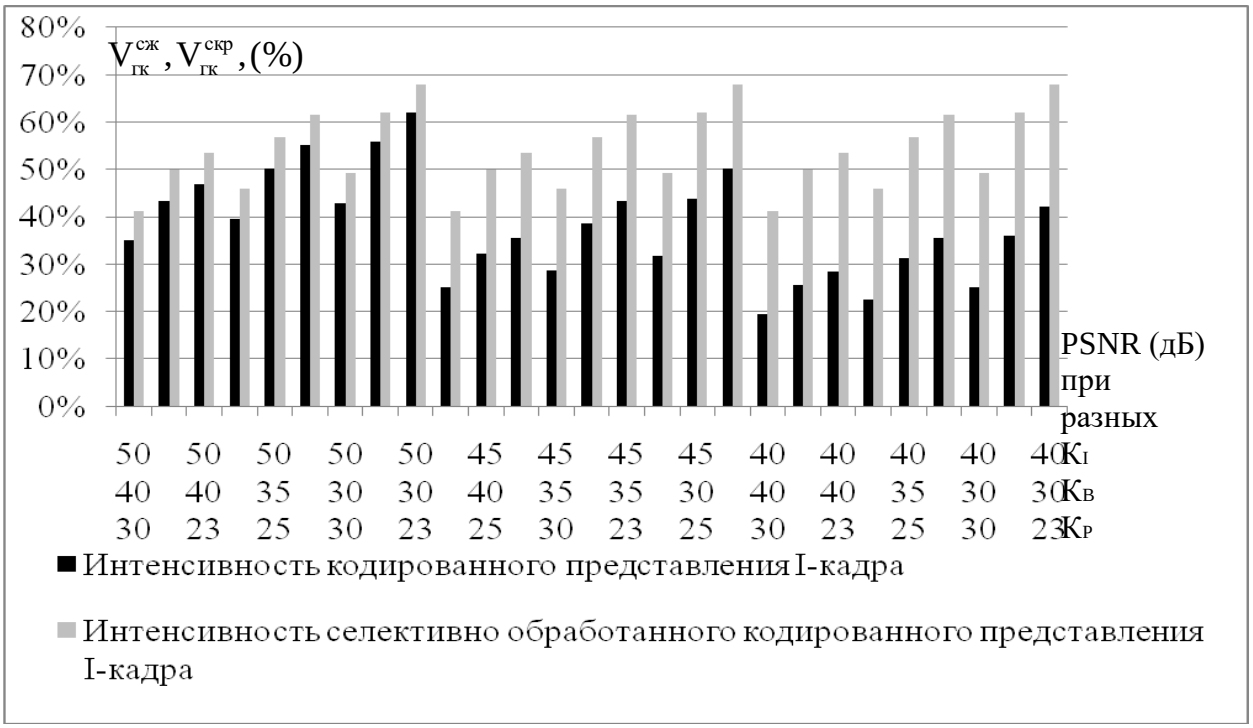


Рис. 2.14. Интенсивность $V_{I(8)}^{скр\%}$ селективно обработанного и $V_{I(8)}^{сж\%}$ закодированного представления I-кадра относительно интенсивности $V_{гк}^{сж}$ группы кадров из 8 видеокадров в зависимости от пикового отношения сигнал/шум для средненасыщенных изображений в процентном соотношении.

Исследования показали, что интенсивность базовых I-кадров занимает от 20% до 60% всей интенсивности видеопотока в зависимости от пиковых отношений сигнал/шум, а прирост интенсивности скрытого кадра в процентном

соотношении относительно интенсивности кодированного не скрытого кадра в группе кадров в зависимости от значений PSNR составляет 7% – 25%. Это обусловлено скрытием базового I-кадра относительно варианта кодирования I-кадра без скрытия. Также видно, что с понижением значений пикового отношения сигнал/шум вес (в процентах) скрытого I-кадра в группе кадров увеличивается. Таким образом, закрыв около от 20% до 60% видеоданных, достигается скрытие 100% передаваемой информации. При этом достигается экономия времени на обработку и передачу видеоданных.

Ниже представлена диаграмма величины прироста $D(h_I; h_B; h_P)$ интенсивности $V_{гк,з}^{(сж)}$ кодированной группы кадров со скрытым I-кадром по отношению к интенсивности $V_{гк,з}^{(сж)}$ кодированной группы кадров без скрытия в процентном соотношении с учетом пикового отношения сигнал/шум для средненасыщенных изображений (рис. 2.15), которая рассчитывается по формуле:

$$D(h_I; h_P; h_B) = \left(1 - \frac{V_{гк,з}^{(сж)}}{V_{гк}^{(сж)}}\right) \cdot 100\% .$$

Анализ диаграммы на рис. 2.15 показывает:

- увеличение процентного соотношения интенсивности кодированного представления группы кадров со скрытым I-кадром в зависимости от кодированного представления группы кадров без скрытия I-кадра в среднем на 12% при понижении пикового отношения сигнал/шум для I-кадра на 5дБ;

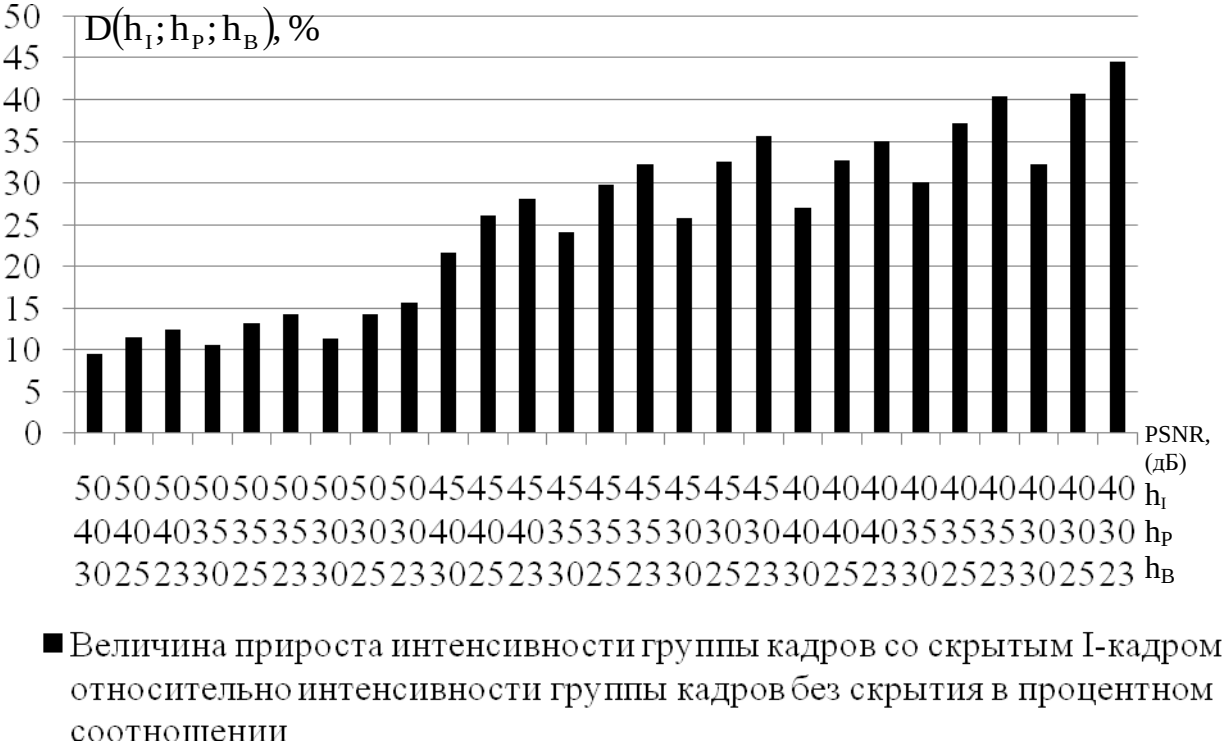


Рис. 2.15. Диаграмма изменения величины прироста $D(h_I; h_P; h_B)$ интенсивности $V_{гк,з}^{(сж)}$ кодированной группы кадров со скрытым I-кадром по отношению к интенсивности $V_{гк,з}^{(сж)}$ кодированной группы кадров без скрытия в процентном соотношении с учетом пикового отношения сигнал/шум для средненасыщенных изображений.

- увеличение интенсивности кодированного представления группы кадров со скрытым I-кадром напрямую зависит от пикового отношения сигнал/шум. С уменьшением пикового отношения сигнал/шум ухудшается визуальное качество изображения, но увеличивается его степень сжатия;

- при максимальных пиковых отношениях сигнал/шум для средненасыщенных изображений (высокое качество изображений) величина прироста $D(h_I; h_P; h_B)$ интенсивности $V_{гк,з}^{(сж)}$ кодированной группы кадров со скрытым I-кадром по отношению к интенсивности $V_{гк,з}^{(сж)}$ кодированной группы кадров без скрытия в процентном соотношении составляет около 10%-15%, а

при минимальных значениях PSNR величина прироста увеличивается до 40%-44%.

В селективном подходе скрытию подвергается только I-кадр, который является базовым и имеет максимальную интенсивность в группе кадров. [40] Поэтому с уменьшением значений пикового отношения сигнал/шум степень сжатия для I-кадра будет постоянной ($\kappa_I = 1$), а для P и B кадров степень сжатия будет расти. В результате чего интенсивность I-кадра относительно интенсивности группы кадров в процентном соотношенни с применением селективного шифрования в зависимости от пикового отношения сигнал/шум может колеблется от 41% до 68%. [76]

Следует отметить то, что при использовании алгоритмов шифрования после квантования структура промежуточного представления разрушается. Изменяются структурные характеристики (значения компонент и зависимость между ними) в матрицах дискретного косинусного преобразования. [127] Это разрушает вероятностные и статистические характеристики, приводит к отсутствию цепочек нулевых значений при загзаг-сканировании. [39] В результате чего степень сжатия I-кадра уменьшается. Поэтому различия между значениями интенсивностей кодированного представления группы кадров со скрытием базового I-кадра и без скрытия в процентном соотношении становятся явно выраженными и могут достигать 35%.

Для определения изменения визуального качества изображений при разных режимах обработки проведем оценку средних значений пикового отношения сигнал/шум $\mathrm{PSNR}(8)_{\mathrm{ср}}$ для 8 видеокадров средненасыщенных изображений, которые определяются следующим образом:

$$\mathrm{PSNR}(8)_{\mathrm{ср}} = \frac{\mathrm{PSNR}(\mathrm{K_I}) + 2 \cdot \mathrm{PSNR}(\mathrm{K_B}) + 5 \cdot \mathrm{PSNR}(\mathrm{K_P})}{8}. \qquad (2.4)$$

Зависимость среднего значения пикового отношения $\mathrm{PSNR}(8)_{\mathrm{ср}}$ сигнал/шум в группе из 8 кадров для средненасыщенных изображений от

коэффициентов сжатия к при разных режимах обработки рассчитана по формуле (2.4) и представлена в виде диаграммы на рис. 2.16.

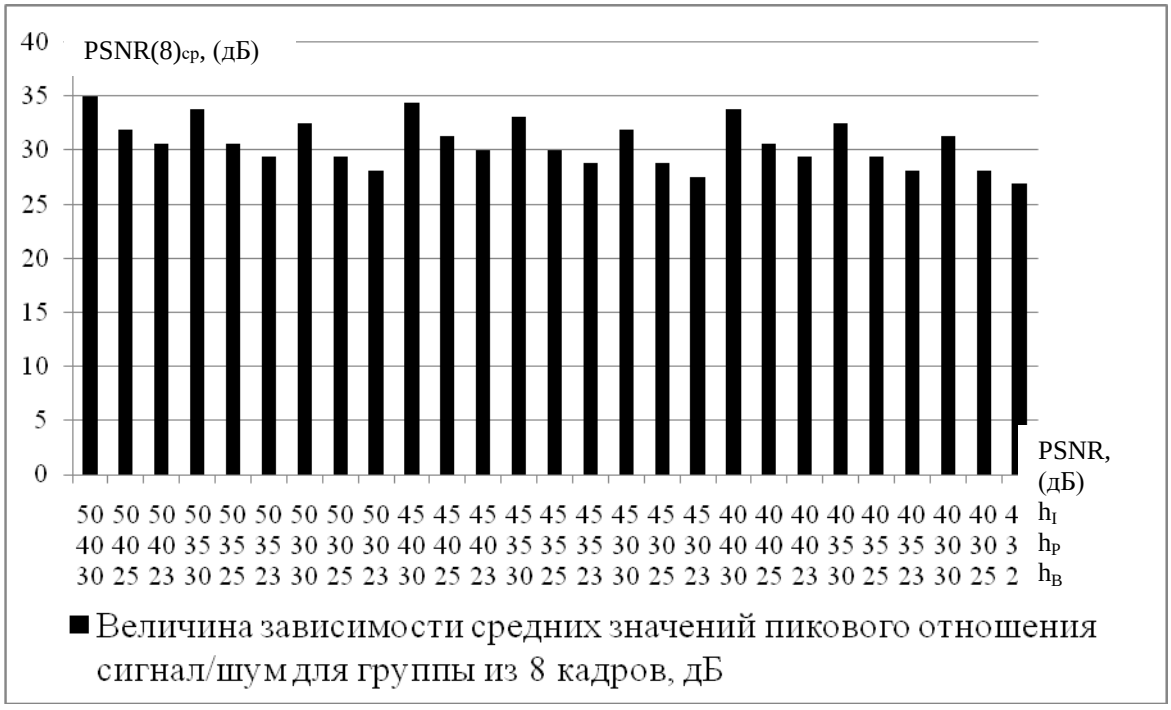


Рис. 2.16. Средние значения $PSNR(8)_{ср}$ по группе из 8 кадров для разных режимов обработки кадров в средненасыщенных изображениях при авторизированном доступе.

Из анализа диаграммы на рис. 2.16 видно, что:

- средние значения $PSNR(8)_{ср}$ для группы из 8 кадров при разных режимах обработки кадров в средненасыщенных изображениях колеблются в пределах 27-35дБ. Это свидетельствует о значительных изменениях качества изображений при разных режимах обработки;

- при изменении PSNR для I-кадра на 5дБ среднее пиковое значение отношения сигнал/шум для группы кадров уменьшается на 1дБ. При этом такие изменения незначительно влияют на интенсивность кодированного представления группы кадров;

- на средний PSNR группы кадров существенно влияют значения отношений сигнал/шум для P и B-кадров.

Выводы

1. Проведен анализ различных вариантов шифрования видеоинформационного потока. Обосновано, что наиболее эффективным является селективный метод скрытия для ведомственных видеоинформационных систем, где обработка и передача видеоданных осуществляется в реальном времени.

2. Разработаны рекомендации по селективному шифрованию в процессе кодирования видеопотока. Они основаны на скрытии базового I-кадра. Это позволяет обеспечить скрытие группы кадров в условиях минимизации потерь по степени снижения интенсивности.

3. Разработан метод оценки интенсивности скрытого I-кадра и без скрытия относительно группы кадров в процентном соотношении. Проведен анализ изменения интенсивности открытого I-кадра и скрытого I-кадра относительно группы кадров в процентном соотношении. Результаты анализа показали, что в зависимости от пикового отношения сигнал/шум интенсивность скрытого I-кадра по сравнению с открытым относительно группы кадров увеличивается от 7% до 20%. В результате увеличение интенсивности скрытого базового кадра не выполняются ведомственные требования по оперативной доставке видеопотока.

4. Проведена оценка интенсивности кодированных видеоданных без скрытия и со скрытием I-кадра. В случае скрытия видеопотока высокого качества с применением селективного метода во время обработки, интенсивность видеоданных увеличивается незначительно (10%). С уменьшением значений пикового отношения сигнал/шум на 5-15 дБ для всех типов кадров, интенсивность скрытых видеоданных (со скрытым I-кадром) увеличивается на 10-44% по сравнению с открытым видеопотоком. Следовательно, при уменьшении качества видеоконтента с использованием селективного метода скрытия его интенсивность растет. Проведенные оценки по интенсивности показали, что данный метод не обеспечивает требований по оперативности для ведомственных инфокоммуникационных систем.

Таким образом, рассмотрен метод по обеспечению безопасности видеоданных путем закрытия базового I-кадка, в результате чего закрывается вся последовательность видеокадров в группе кадров. Эффективность такого подхода рассматривалась со стороны изменения интенсивности скрытого I-кадра относительно интенсивности группы кадров. Поэтому при использовании селективного метода, основанного на закрытии базового I-кадра, с одной стороны выполняются требования по обеспечению конфиденциальности и целостности видеоинформационного ресурса. Но с другой стороны, реализация такого подхода приводит к увеличению интенсивности передаваемых закрытых видеоданных, в результате чего снижается пропускная способность закрытого видеоканала. Это приводит к невозможности выполнения требований, установленных для ведомственных систем видеоконференцсвязи по обеспечению необходимой пропускной способности скрытого канала. В этом случае снижается эффективность проведения ведомственных сеансов видеоконференцсвязи.

Значит, необходимо дополнительно снизить интенсивность закрытого видеопотока в условиях обеспечения требуемой достоверности и конфиденциальности. Таким образом, необходимо разработать метод, обеспечивающий повышение пропускной способности закрытого видеоканала для систем ведомственной видеоконференцсвязи.

Результаты исследований, изложенные в данном разделе, опубликованы в научных трудах [14, 16; 78; 98].

РАЗДЕЛ 3
РАЗРАБОТКА МЕТОДА ПОВЫШЕНИЯ ПРОПУСКНОЙ СПОСОБНОСТИ ЗАКРЫТОГО ВИДЕОКАНАЛА В ИНФОКОММУНИКАЦИОННЫХ СИСТЕМАХ

Разрабатывается метод повышения пропускной способности закрітого видеоканала, основанный на внутрикадровой селекции структурных единиц базового кадра. Данный метод в отличии от других методов осуществляет закрытие видеопотока на основе технологии кодирования базовых кадров с использованием селективной обработки структурных единиц в зависимости от их энергетической значимости.

Для оценки энергетической значимости структурных единиц базового видеокадра разрабатывается технология выявления структурных единиц по степени их структурной и семантической информативности. Она позволяет определять наиболее значимые блоки яркостной составляющей в структурных единицах базового видеокадра на основе оценки информации показателей по совокупности низкочастотных значений компонент трансформанты ДКП.

В результате применения данной технологии значимыми считаются структурные единицы, которые:

1. Обладают выраженными структурными переходами, текстурными и яркостными перепадами;

2. Имеют выраженные текстурные перепады;

3. Обладают множеством контрастных незначимых мелких деталей.

Это позволяет эффективно закрывать видеопоток на основе технологии внутрикадровой селекции базовых видеокадров в условиях ограничения по времени обработки и конфиденциальности.

3.1 Методологическая база для определения энергетической значимости структурной единицы видеокадра

Селективный метод, основанный на закрытии I-кадра, относится к варианту межкадровой селекции. Межкадровая селекция находится на уровне структуры потока видеокадров, где закрытию подлежит не весь видеоряд, а определенное количество кадров. В таком методе закрытия основным недостатком является увеличение интенсивности (снижение пропускной способности видеоданных до 70%). [41] Поэтому для повышения пропускной способности предлагается дополнительно рассматривать метод, основанный на закрытии видеопотока на базе внутрикадровой селекции.

Под понятием внутрикадровой селекции подразумевается закрытие не всего видеокадра, а только значимых $S_{зн}$ его составляющих. [107]

Под значимой $S_{зн}$ составляющей понимается такая составляющая видеокадра K_I, которая несет в себе наибольшую семантическую и структурную информативность. В процессе автоматической селекции значимых $S_{зн}$ составляющих предлагается учитывать структурные особенности формирования видеопотока. [18]

Для селекции значимых структурных единиц $S_{зн}$ предлагается выявлять наиболее информативные, в плане структурного и семантического содержания, составляющие базового кадра. [109] Поскольку наиболее полную информацию несет яркостная составляющая видеокадра K_I, то значимые структурные единицы предлагается выявлять на базе яркостных компонент. Поэтому принятие решения по закрытию структурной единицы предлагается осуществлять по результатам анализа информационной составляющей совокупности блоков $B(Y)_{\varphi}^{(\xi,\gamma)}$ яркостной составляющей. [119]

Для определения энергетической насыщенности блоков $B(Y)_{\varphi}^{(\xi,\gamma)}$ предлагается ввести понятии блоков трех типов:

- слабонасыщенные блоки (блоки, в которых присутствуют равномерные участки изображения);

- средней насыщенности (блоки, в которых имеются незначительные отличия между пикселями, соответственно присутствуют плавные переходы контрастности);

- сильнонасыщенные блоки (блоки, в которых присутствуют резкие переходы яркости и контрастности изображения). [19]

Определение энергетической насыщенности блоков предлагается осуществлять после ДКП. С помощью дискретного косинусного преобразования осуществляется переход от пространственно-временного представления видеокадра в пространственно-спектральное. Компоненты трансформанты ДКП являются интегральными характеристиками структурного содержания фрагмента изображения. Причем интегральные свойства компонент зависят от их положения в трансформанте). На рис. 3.1 представлено расположение низкочастотных компонент трансформанты ДКП в блоках $B(Y)_{\varphi}^{(\xi,\gamma)}$ яркостной составляющей макроблока. [80]

Из рис. 3.1 видно, что низкочастотные компоненты находятся в области первых пяти диагоналей.

Интегральная зависимость компонент трансформанты ДКП выглядит следующим образом:

1. Значение компоненты в верхнем левом углу трансформанты ДКП пропорциональны средней яркости изображения. Они характеризуют степень насыщенности блока изображения низкочастотными перепадами. К низкочастотным перепадам относят ступенчатые изменения уровня яркости или координаты цвета. [66]

2. Компоненты в средней части трансформанты определяют степень насыщенности блока изображения линейными, равномерными изменениями уровня яркости.

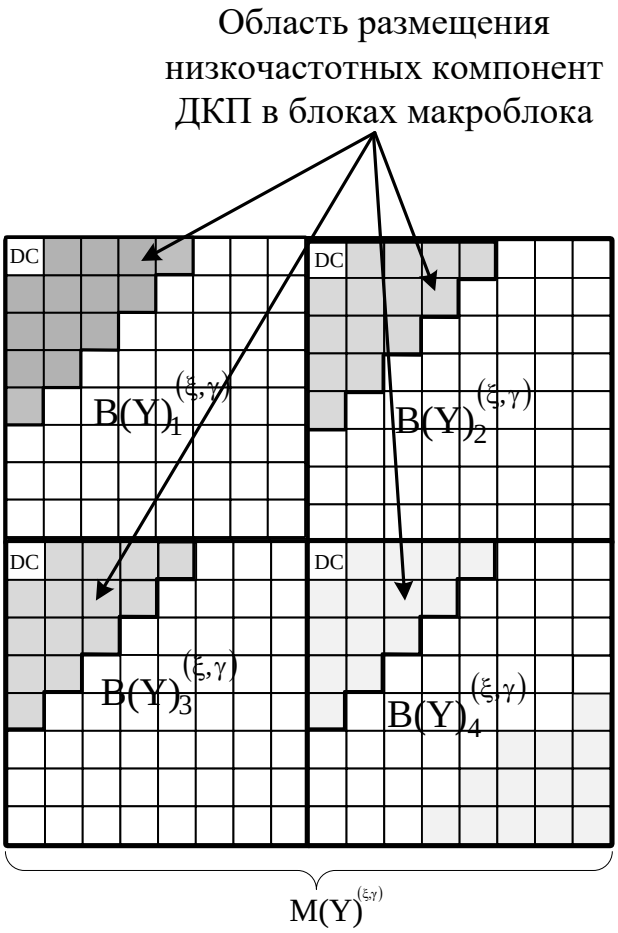


Рис. 3.1. Схема расположения низкочастотных трансформанты ДКП в блоках $B(Y)_{\varphi}^{(\xi,\gamma)}$ яркостной составляющей макроблока.

3. Значения компонент в нижней правой области трансформанты ДКП характеризуют степень насыщенности высокочастотными перепадами блока изображения. К высокочастотным перепадам относят импульсные изменения значений элементов изображений.

Поэтому можно сделать вывод о том, что энергией блока называется величина, характеризующая наличие неоднородно визуальных контуров блока изображения.

Значения компонент изменяются по мере преобладания в изображении различных структурных особенностей. [125]

Широкий класс изображений содержит в основном линейные, монотонные и ступенчатые структурные изменения уровня яркости.

Импульсные изменения занимают меньшую площадь изображения. [21] Кроме того, они могут быть вызваны шумами дискретизации. Поэтому наибольшие значения имеют компоненты расположенные в верхней левой части трансформанты. Компоненты в нижней части трансформанты соответствуют высокочастотным изменениям и поэтому имеют меньшие значения. [60]

На рис. 3.2 показано расположение компонент в трансформанте ДКП блока яркостной составляющей видеокадра.

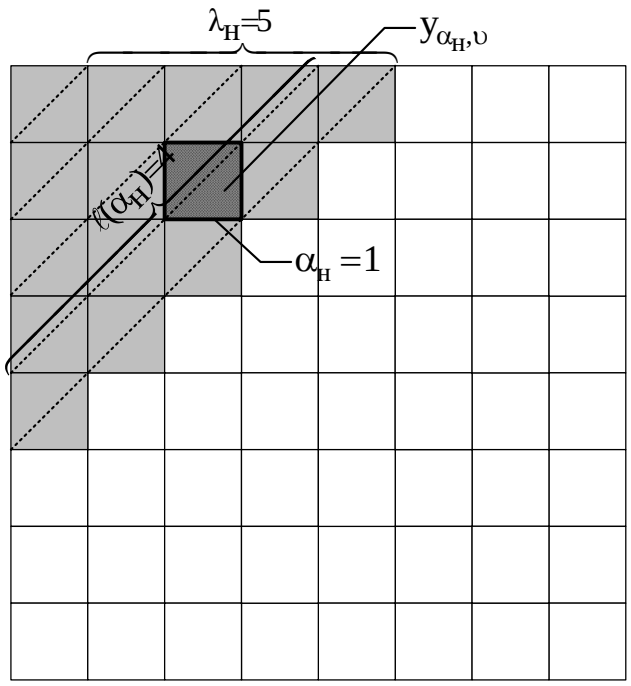


Рис. 3.2. Схема расположения низкочастотных компонент в трансформанте ДКП блока яркости видеокадра.

Для трансформанты ДКП в сильнонасыщенных блоках изображениях характерны следующие особенности:

- значения компонент ДКП уменьшается по диагональному зигзагу слева - направо, сверху – вниз;

- компоненты ДКП с большими значениями сконцентрированы в относительно малой области трансформанты. Компоненты с минимальными значениями занимают большую площадь трансформанты;

- при большой площади изображения, имеющей мало изменяющуюся яркость, размер области трансформанты с большими значениями компонент имеет маленькую площадь.

Предлагается оценивать структурную и семантическую информативность структурной единицы с позиции спектральных характеристик. [120] Очевидно, что чем больше площадь однородной яркостной площади, и чем меньше площадь, заполненная мелкими деталями, тем меньше степень структурной и семантической информативности обрабатываемого блока видеокадра. Наоборот, чем чаще яркостные перепады, и чем больше площадь, отводимая под мелкие детали и контурные перепады, тем выше структурная и семантическая информативность. [25] В связи с чем, для оценки значимости структурных единиц предлагается использовать информацию, содержащуюся в спектральном представлении изображения. [56]

Для определения блоков с выраженными яркостными ступенчатыми перепадами предлагается использовать информацию, содержащуюся в совокупности низкочастотных компонент. [38] Такую информацию предлагается оценивать с помощью показателя $Z(B_н)_φ^{(ξ,γ)}$ суммарных значений низкочастотных компонент, которые находятся в первых 4-х диагоналях ($1 \le \lambda_н \le 5$). Показатель $Z(B_н)_φ^{(ξ,γ)}$ рассчитывается по следующей формуле:

$$Z(B_н)_φ^{(ξ,γ)} = \frac{\log_2 \sum_{\alpha_н=1}^{\lambda_н} \sum_{\upsilon=1}^{\ell(\alpha_н)} y^2_{\alpha_н,\upsilon}}{\sum_{\alpha_н=1}^{\lambda_н} \ell(\alpha_н)}, \qquad (3.1)$$

где $Z(B_н)_φ^{(ξ,γ)}$ – показатель, который определяет суммарное значение низкочастотных компонент ДКП блока $B(Y)_φ^{(ξ,γ)}$ яркости;

$y_{\alpha_н,\upsilon}$ – значение компоненты трансформанты;

$\lambda_н$ – количество диагоналей с низкочастотными компонентами в трансформанте;

υ – индекс элемента внутри $\alpha_н$-ой диагонали;

$\alpha_н$ – индекс низкочастотной $\lambda_н$-ой диагонали;

$\ell(\alpha_н)$ – длина низкочастотной $\alpha_н$-ой диагонали.

Таким образом, разработана система показателей (метрика) для выявления наиболее значимых блоков яркостной составляющей видеокадра по степени семантической и структурной насыщенности на основе оценки информации, содержащейся в суммарных значений низкочастотных компонент трансформанты ДКП.

3.2 Методологическая база, базирующаяся на системе правил для принятия решения по энергетической значимости структурных единиц с помощью показателей низкочастотных компонент блока яркостной составляющей.

Оценку значимости структурной единицы $S^{(\xi,\gamma)}$ предлагается осуществлять на основе энергетической значимости макроблока $M(Y)^{(\xi,\gamma)}$ яркостной составляющей. [102] В свою очередь, оценку значимости макроблока $M(Y)^{(\xi,\gamma)}$ яркостной составляющей предлагается проводить на основе структурной и семантической насыщенности блока $B(Y)_{\varphi}^{(\xi,\gamma)}$. Для этого необходимо разработать метод, базирующийся на системе правил для принятия решения по энергетической значимости структурных единиц и макроблоков на основе информации о значимости блоков яркостной составляющей.

В основе правил лежит система сравнения показателя $Z(B_н)_{\varphi}^{(\xi,\gamma)}$ совокупности значений низкочастотных компонент с пороговыми значениями $\delta_{min_н}$ и $\delta_{max_н}$. Будем считать, что $\delta_{max_н}$ – верхний предел для оценки

показателя $Z(B_н)_φ^{(ξ,γ)}$ совокупности значений низкочастотных компонент блока $B(Y)_φ^{(ξ,γ)}$ яркостной составляющей. $δ_{min_н}$ – нижний предел для оценки показателя $Z(B_н)_φ^{(ξ,γ)}$ совокупности значений низкочастотных компонент блока $B(Y)_φ^{(ξ,γ)}$ яркостной составляющей. [28]

Предлагается проводить оценку энергетической значимости макроблока $M(Y)^{(ξ,γ)}$ яркостной составляющей базового видеокадра K_I. Макроблок $M(Y)^{(ξ,γ)}$ яркостной составляющей будет считаться энергетически значимым в двух случаях:

1. Если в состав макроблока $M(Y)^{(ξ,γ)}$ яркостной составляющей входит один и больше блоков $B(Y)_φ^{(ξ,γ)}$ с высокой степенью семантической и структурной насыщенности. Это можно описать следующим выражением:

$$M(Y)^{(ξ,γ)} = M(Y)_{зн}^{(ξ,γ)} \text{ и } M=1, \text{ если } Z(B_н)_φ^{(ξ,γ)} > δ_{max_н}.$$

2. Если в состав макроблока $M(Y)^{(ξ,γ)}$ яркостной составляющей входят два $N_{sr} = 2$ и больше $N_{sr} > 2$ блоков $B(Y)_φ^{(ξ,γ)}$ со средней степенью семантической и структурной насыщенности, то есть выполняется неравенство:

$$(δ_{min_н} \le Z(B_н)_φ^{(ξ,γ)} \le δ_{max_н}),$$

тогда:

$$M(Y)^{(ξ,γ)} = M(Y)_{зн}^{(ξ,γ)} \text{ и } M=1 \text{ если } N_{sr} \ge 2,$$

$$N_{sr} = N_{sr} + 1, \text{ если } (δ_{min_н} \le Z(B_н)_φ^{(ξ,γ)} \le δ_{max_н})$$

где N_{sr} – количество блоков со средней структурной и семантической насыщенности.

Остальные структурные единицы обрабатываются по стандартному алгоритму видеокомпрессии.

Структурная схема метода селекции значимых структурных единиц $S_{зн}^{(\xi,\gamma)}$ с использованием информации по совокупности значений низкочастотных компонент трансформанты ДКП блоков $B(Y)_{\varphi}^{(\xi,\gamma)}$, $\varphi = \overline{1,4}$ яркостной составляющей представлена на рис. 3.3.

Процесс выбора значимого макроблока $M(Y)^{(\xi,\gamma)}$ яркостной составляющей (рис. 3.7) происходит следующим образом:

1. В начале проверки значимого макроблока $M(Y)^{(\xi,\gamma)}$ яркостной составляющей переменная N_{sr} для подсчета средненасыщенных блоков $B(Y)_{\varphi}^{(\xi,\gamma)}$ яркостной составляющей, принимает значение

$$N_{sr} = 0,$$

а переменная φ, которая определяет номер блока $B(Y)_{\varphi}^{(\xi,\gamma)}$ яркостной составляющей для проверки, принимает значение $\varphi = 1$.

2. После образования трансформант ДКП блоков $B(Y)_{\varphi}^{(\xi,\gamma)}$ яркостной составляющей их проверка осуществляется по очереди с 1-го по 4-й блок.

3. Для блока $B(Y)_{\varphi}^{(\xi,\gamma)}$ яркостной составляющей производится расчет показателя $Z(B_{н})_{\varphi}^{(\xi,\gamma)}$ для совокупности значений низкочастотных компонент с учетом выражения (3.1).

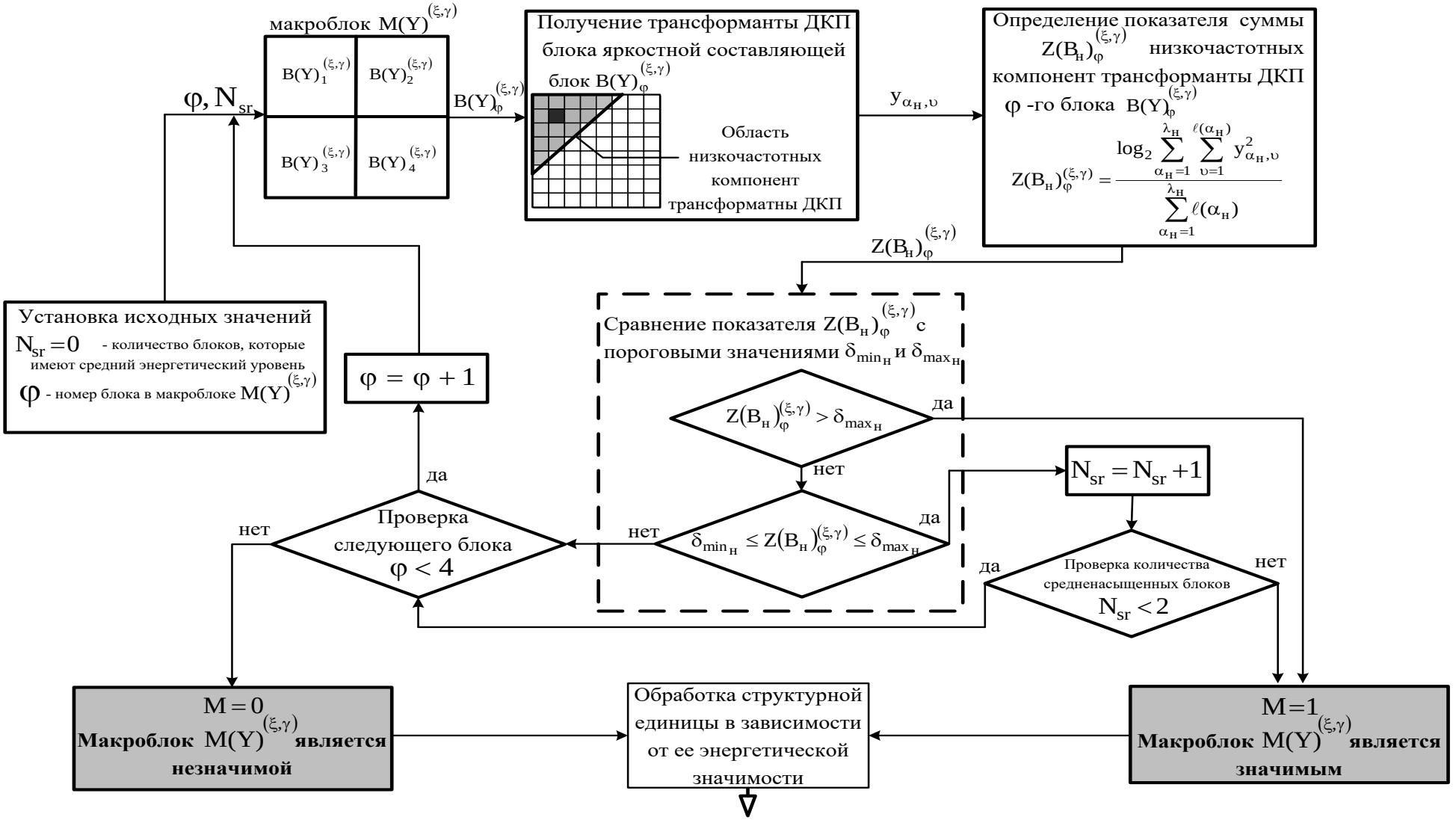


Рис. 3.3. Структурная схема метода селекции значимых структурных единиц $S_{зн}^{(\xi,\gamma)}$ с использованием информации по совокупности значений низкочастотных компонент трансформанты ДКП блоков $B(Y)_\varphi^{(\xi,\gamma)}$ яркостной составляющей.

4. Показатель $Z(B_н)_φ^{(ξ,γ)}$ сравнивается с пороговыми значениями $δ_{min_н}$ и $δ_{max_н}$ для определения энергетической насыщенности блока $B(Y)_φ^{(ξ,γ)}$. Если значения показателя $Z(B_н)_φ^{(ξ,γ)}$ для блока $B(Y)_φ^{(ξ,γ)}$ яркостной составляющей превышает верхний порог $δ_{max_н}$, то блок считается энергетически значимым по степени структурной и семантической насыщенности

$$Z(B_н)_φ^{(ξ,γ)} > δ_{max_н}.$$

В этом случае метка M принимает значение M=1, соответственно макроблок $M(Y)^{(ξ,γ)}$ яркостной составляющей будет считаться энергетически значимым. В результате чего алгоритм проверки останавливается.

6. Если показатель $Z(B_н)_φ^{(ξ,γ)}$ суммарных значений низкочастотных компонент блока $B(Y)_φ^{(ξ,γ)}$ яркостной составляющей находится между пороговыми значениями

$$δ_{min_н} \le Z(B_н)_φ^{(ξ,γ)} \le δ_{max_н},$$

то блок $B(Y)_φ^{(ξ,γ)}$ яркостной составляющей будет средненасыщенным, а переменная N_{sr} для подсчета средненасыщенных блоков $B(Y)_φ^{(ξ,γ)}$ яркостной составляющей, примет значение

$$N_{sr} = N_{sr} + 1.$$

Для того, чтобы считать, что макроблок $M(Y)^{(ξ,γ)}$ яркостной составляющей обладает высокой энергетической значимостью, необходимо

наличие двух и более блоков $B(Y)_{\varphi}^{(\xi,\gamma)}$ яркостной составляющей, входящих в его состав.

7. После чего проверяется количество средненасыщенных блоков $B(Y)_{\varphi}^{(\xi,\gamma)}$ яркостной составляющей. Если количество блоков со средней степенью семантической и структурной насыщенности больше или равно двум: ($N_{sr} \geq 2$), то макроблок $M(Y)^{(\xi,\gamma)}$ яркостной составляющей будет считаться энергетически значимым. В этом случае также метка M принимает значение M=1, а макроблок $M(Y)^{(\xi,\gamma)}$ яркостной составляющей будет считаться энергетически значимым. После чего дальнейшая проверка блоков яркостной составляющей прекращается. Если в результате проверки всех 4-х блоков $B(Y)_{\varphi}^{(\xi,\gamma)}$ яркостной составляющей значение показателя $Z(B_{н})_{\varphi}^{(\xi,\gamma)}$ блоков оказалось меньше нижнего порогового значения $\delta_{\min_{н}} > Z(B_{н})_{\varphi}^{(\xi,\gamma)}$, или количество средненасыщенных блоков меньше $N_{sr} < 2$, то метка M принимает значение M=0. Соответственно, такой макроблок $M(Y)^{(\xi,\gamma)}$ яркостной составляющей будет считаться энергетически значимым.

В результате чего энергетическая значимость структурной единицы $S^{(\xi,\gamma)}$ определяется на основе энергетической значимости макроблока $M(Y)^{(\xi,\gamma)}$. [68] Таким образом, структурная единица считается значимой $S^{(\xi,\gamma)} = S_{зн}^{(\xi,\gamma)}$ если в результате проверки макроблока $M(Y)^{(\xi,\gamma)}$ яркостной составляющей по информации о совокупности значений низкочастотных компонент трансформанты ДКП блоков $B(Y)_{\varphi}^{(\xi,\gamma)}$ метка приняла значение M=1.

На рис. 3.4 представлен алгоритм селекции значимых структурных единиц $S_{зн}^{(\xi,\gamma)}$ с использованием информации по совокупности значений низкочастотных компонент трансформанты ДКП блоков $B(Y)_{\varphi}^{(\xi,\gamma)}$ яркостной составляющей.

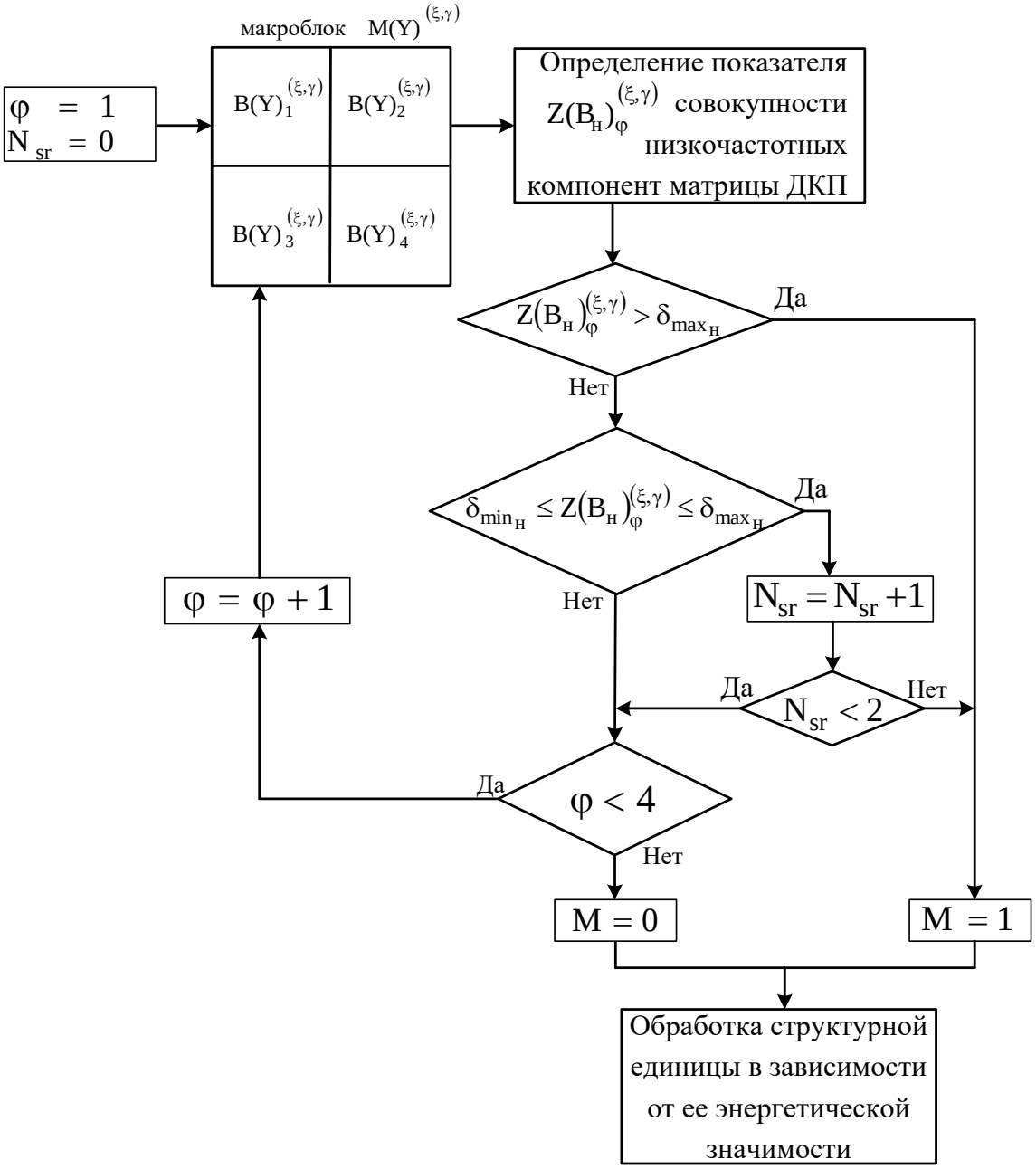


Рис. 3.4. Алгоритм значимых структурных единиц $S^{(\xi,\gamma)}$ с использованием информации по совокупности значений низкочастотных компонент трансформанты ДКП блоков $B(Y)_\varphi^{(\xi,\gamma)}$ яркостной составляющей.

Разработанный метод позволяет выявлять (селекционировать) значимые структурные единицы $S_{зн}$ базового видеокадра K_I на основе оценки показателя $Z(B_н)_\varphi^{(\xi,\gamma)}$ по совокупности значений низкочастотных компонент

блока $B(Y)_{\varphi}^{(\xi,\gamma)}$ яркостной составляющей с пороговыми значениями. В результате работы такого метода происходит выявления участков изображения базового видеокадра, которые обладают выраженными структурными переходами, текстурными и яркостными перепадами. [84]

Таким образом, разработана методологическая база для определения энергетической значимости структурной единицы базового видеокадра, базирующаяся на системе правил для оценки структурной и семантической насыщенности блоков $B(Y)_{\varphi}^{(\xi,\gamma)}$ яркостной составляющей. Здесь учитывается значение показателя по совокупности низкочастотных компонент трансформанты ДКП блока $B(Y)_{\varphi}^{(\xi,\gamma)}$ яркостной составляющей. Это позволяет производить оценку блоков и макроблоков яркостной составляющей видеокадра по низкочастотным компонентам трансформанты ДКП для выявления участков изображения, которые обладают выраженными структурными переходами, текстурными и яркостными перепадами.

3.3 Разработка технологии формирования кодовой конструкции структурной единицы для метода повышения пропускной способности закрытого видеоканала.

Структура кодовой конструкции представления скрытой группы видеокадров представлена на рис. 3.5.

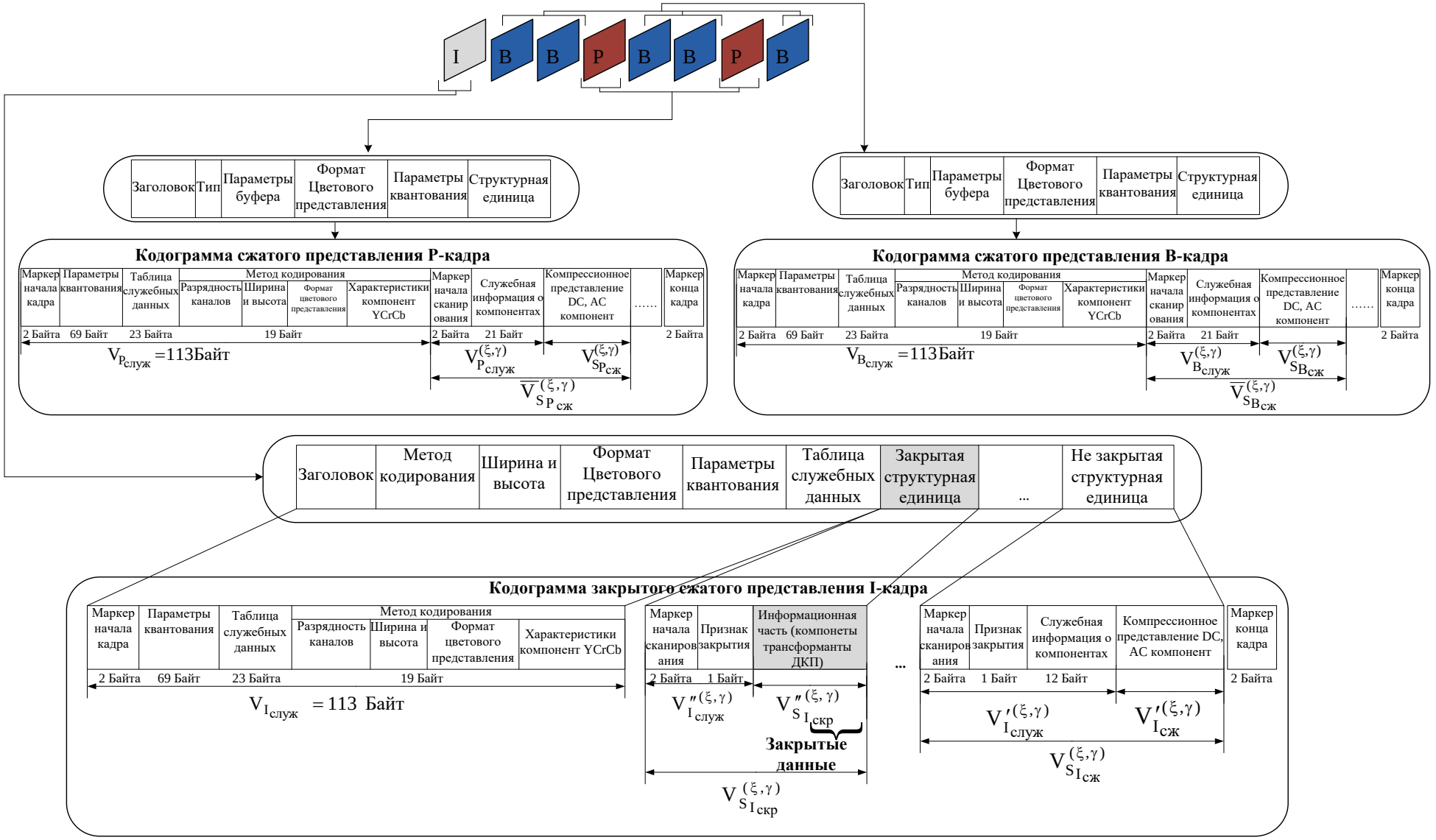


Рис. 3.5. Структура кодовой конструкции представления скрытой группы видеокадров.

Из рис. 3.5 видно, что кодограмма скрытого базового видеокадра формируется следующим образом:

1. Сначала располагается общая служебная информация о базовом видеокадре ($V_{I_{служ}}$ =113 байт), которая включает в себя такие данные:

– маркер начала кадра [FF D8] (2 байта);

– маркер параметров квантования [FF DB] (2 байта) и сами параметры (67 байт);

– маркер таблицы служебных данных [FF C4] (2 байта), длина параметров (2 байта), идентификатор таблиц (1 байт), длины кодов таблиц;

– маркер метода кодирования [FF C0] (2 байта), длина информационного кода о методе кодирования (2 байта), информация о методе кодирования (размер видеокадра, разрядность значений каналов, формат цветового представления, параметры вертикального и горизонтального прореживания компонент) (17 байт);

2. После чего идут поля кодовой конструкции, которые соответствуют информации о структурных единицах базового видеокадра. [90] Интенсивность кодового потока зашифрованной структурной единицы определяется как $V_{S_{I_{скр}}}^{(\xi,\gamma)}$, и включает в себя следующие составляющие:

– служебная часть информации о скрытой структурной единице, которая включает в себя маркер начала сканирования структурной единицы [FF DA] и признак закрытия ($V_{I_{служ}}^{\prime\prime(\xi,\gamma)}$ = 3 байта);

– кодограмма информационной части (значения компонент матриц ДКП), интенсивность которой определяется как $V_{S_{I_{скр}}}^{\prime\prime(\xi,\gamma)}$.

В селективном методе обработки видеоданных кодовые конструкции служебной информация о компонентах и информационной части энергетически значимых структурных единиц $S_{зн}^{(\xi,\gamma)}$ подлежат шифрованию. [61]

3. Кодовая конструкция открытой структурной единицы, которая состоит из следующих составляющих:

– кодограмма информационной части об открытой структурной единицы $V'^{(\xi,\gamma)}_{I_{служ}}$, которая включает в себя маркер начала сканирования структурной единицы [FF DA] (2 байта) и признак закрытия (1 байт), длину заголовка, количество компонент сканирования, номера компонент сканирования;

– двоичный код $V'^{(\xi,\gamma)}_{I_{сж}}$ компрессионного представления DC, AC-компонент.

Кодовая конструкция Р-кадра состоит из такой информации:

1. Служебная информация о Р-кадре ($V_{P_{служ}}$ =113 байт), которая включает в себя такие данные:

– маркер начала кадра [FF D8] (2 байта);

– маркер параметров квантования [FF DB] (2 байта) и сами параметры (67 байт);

– маркер таблицы служебных данных [FF C4] (2 байта), длина параметров (2 байта), идентификатор таблиц (1 байт), длины кодов таблиц;

– маркер метода кодирования [FF C0] (2 байта), длина информационного кода о методе кодирования (2 байта), информация о методе кодирования (размер видеокадра, разрядность значений каналов, формат цветового представления, параметры вертикального и горизонтального прореживания компонент) (17 байт);

2. Потом идут поля кода, которые включают в себя информации о структурных единицах Р-кадра. [103] Интенсивность битового кода структурной единицы Р-кадра определяется как $\overline{V}^{(\xi,\gamma)}_{S_{P_{сж}}}$, и включает в себя такие составляющие:

– служебная информация о компонентах (длина заголовка, количество компонент сканирования, номера компонент сканирования), $V^{(\xi,\gamma)}_{P_{служ}}$ – длина кода служебной части (ξ,γ)-ой сжатой структурной единицы Р-кадра;

– двоичный код компрессионного представления DC, AC-компонент структурных единиц P-кадра, $V_{S_{P_{сж}}}^{(\xi,\gamma)}$ – длина кода компрессионного представления DC, AC-компонент ξ,γ -ой структурной единицы P-кадра.

Двоичный код B-кадра состоит из такой информации:

1. Служебная информация о B-кадре ($V_{B_{служ}}$=113 байт), которая включает в себя такие данные:

– маркер начала кадра [FF D8] (2 байта);

– маркер параметров квантования [FF DB] (2 байта) и сами параметры (67 байт);

– маркер таблицы служебных данных [FF C4] (2 байта), длина параметров (2 байта), идентификатор таблиц (1 байт), длины кодов таблиц;

– маркер метода кодирования [FF C0] (2 байта), длина информационного кода о методе кодирования (2 байта), информация о методе кодирования (размер видеокадра, разрядность значений каналов, формат цветового представления, параметры вертикального и горизонтального прореживания компонент) (17 байт);

2. Потом идут поля кода, которые включают в себя информации о структурных единицах B-кадра. [53] Интенсивность кодового потока структурной единицы B-кадра определяется как $\overline{V}_{S_{B_{сж}}}^{(\xi,\gamma)}$, и состоит из следующих составляющих:

– служебная информация о компонентах (длина заголовка, количество компонент сканирования, номера компонент сканирования), $V_{B_{служ}}^{(\xi,\gamma)}$ – длина кода служебной части (ξ,γ)-ой сжатой структурной единицы B-кадра;

– двоичный код компрессионного представления DC, AC-компонент структурных единиц B-кадра, $V_{S_{B_{сж}}}^{(\xi,\gamma)}$ – длина кода компрессионного представления DC, AC-компонент ξ,γ -ой структурной единицы B-кадра. [118]

Длина кодовой конструкции закрытого базового видеокадра $V_I^{скр}$ – это сумма интенсивностей битового потока скрытых и компрессионно представленных структурных единиц. Данное определение можно представить следующим образом:

$$V_I^{скр} = V_{I_{служ}} + \frac{V_{S_{I_{незн}}}}{k_I} + \frac{V_{S_{I_{зн}}}}{k_{I_з}} = V_{I_{служ}} + V_{S_{I_{сж}}} + V_{S_{I_{скр}}},$$

где $V_{S_{I_{незн}}}$ – интенсивность всех незначимых структурных единиц I-кадра;

$V_{S_{I_{зн}}}$ – интенсивность всех значимых структурных единиц I-кадра;

k_I – коэффициент сжатия для незначимых структурных единиц I-кадра;

$k_{I_з}$ – коэффициент сжатия для значимых структурных единиц I-кадра;

$V_{S_{I_{сж}}}$ – длина кода всех компрессионно представленных структурных единиц I-кадра;

$V_{S_{I_{скр}}}$ – длина кода всех скрытых структурных единиц I-кадра;

$V_{I_{служ}}$ – длина кода служебной информации базового видеокадра.

Кодовое представление $V_{S_{I_{сж}}}^{(\xi,\gamma)}$ не скрытой структурной единицы базового видеокадра K_I определяется как:

$$V_{S_{I_{сж}}}^{(\xi,\gamma)} = V'^{(\xi,\gamma)}_{I_{служ}} + V'^{(\xi,\gamma)}_{S_{I_{сж}}},$$

где $V_{S_{I_{служ}}}^{(\xi,\gamma)}$ – длина кода служебной информации (ξ,γ)-ой структурной единицы базового видеокадра;

$V'^{(\xi,\gamma)}_{S_{I_{сж}}}$ – длина битового потока компрессионного представления (ξ,γ)-ой структурной единицы базового видеокадра.

Интенсивность кода всех открытых структурных единиц $V_{S_{I_{сж}}}$ базового кадра K_I будет рассчитываться как:

$$V_{S_{I_{сж}}} = \sum_{s=1}^{|\Psi_{незн}|} (V'^{(s)}_{I_{служ}} + V'^{(s)}_{S_{I_{сж}}}),$$

где $|\Psi_{незн}|$ – количество незначимых структурных единиц.

Интенсивность $V^{(\xi,\gamma)}_{S_{I_{скр}}}$ зашифрованной структурной единицы определяется по формуле:

$$V^{(\xi,\gamma)}_{S_{I_{скр}}} = V''^{(\xi,\gamma)}_{I_{служ}} + V''^{(\xi,\gamma)}_{S_{I_{скр}}},$$

где $V''^{(\xi,\gamma)}_{I_{служ}}$ – длина кода открытой части служебной информации (ξ,γ)-ой зашифрованной структурной единицы базового видеокадра; $V''^{(\xi,\gamma)}_{S_{I_{скр}}}$ – длина битового потока зашифрованной информационной части (ξ,γ)-ой структурной единицы базового видеокадра.

Интенсивность кода всех зашифрованных структурных единиц $V_{S_{I_{скр}}}$ базового кадра K_I будет рассчитываться таким образом:

$$V_{S_{I_{скр}}} = \sum_{s=1}^{|\Psi_{зн}|} (V''^{(s)}_{I_{служ}} + V''^{(s)}_{S_{I_{скр}}}),$$

где $|\Psi_{зн}|$ – количество значимых структурных единиц.

Таким образом, длина кодового потока $V_{I_{скр}}$ закрытого базового видеокадра будет определяться по следующей формуле:

$$V_{I_{скр}} = V_{I_{служ}} + \sum_{s=1}^{|\Psi_{зн}|} \frac{V_{S_{I_{незн}}}^{(s)}}{k_I} + \sum_{s=1}^{|\Psi_{незн}|} \frac{V_{S_{I_{зн}}}^{(s)}}{k_{I_з}} =$$

$$= V_{I_{служ}} + \sum_{s=1}^{|\Psi_{зн}|} (V_{I_{служ}}^{(s)} + V_{S_{I_{сж}}}^{(s)}) + \sum_{s=1}^{|\Psi_{незн}|} (V_{I_{служ}}^{(s)} + V_{S_{I_{скр}}}^{(s)}).$$

Длина кода компрессионного представления $\overline{V}_{S_{P_{сж}}}^{(\xi,\gamma)}$ структурной единицы Р-кадра определяется так:

$$\overline{V}_{S_{P_{сж}}}^{(\xi,\gamma)} = V_{S_{P_{служ}}}^{(\xi,\gamma)} + \frac{V_{S_{P_{исх}}}}{k_P} = V_{S_{P_{служ}}}^{(\xi,\gamma)} + V_{S_{P_{сж}}}^{(\xi,\gamma)},$$

где $V_{S_{P_{исх}}}$ – интенсивность исходной (ξ,γ)-ой структурной единицы Р-кадра;

k_P – коэффициент сжатия для структурных единиц Р-кадра;

$V_{S_{P_{служ}}}^{(\xi,\gamma)}$ – длина кода служебной информации (ξ,γ)-ой структурной единицы Р-кадра;

$V_{S_{P_{сж}}}^{(\xi,\gamma)}$ – длина битового потока компрессионного представления (ξ,γ)-ой структурной единицы Р-кадра.

Интенсивность кодового потока компрессионного представления Р-кадра $V_{P_{сж}}$ определяется как сумма битового потока компрессионного представления всех структурных единиц Р-кадра. [36] Это описывается следующим выражением:

$$V_{P_{сж}} = V_{S_{P_{служ}}} + \sum_{s=1}^{Ns_p} \frac{V_{S_{P_{исх}}}^{(s)}}{k_P} = V_{P_{служ}} + \sum_{s=1}^{Ns_p} (V_{S_{P_{служ}}}^{(s)} + V_{S_{P_{сж}}}^{(s)}),$$

где Ns_p – количество структурных единиц в P-кадре.

Длина кода компрессионного представления (ξ,γ)-ой структурной единицы $\overline{V}_{S_{B_{сж}}}^{(\xi,\gamma)}$ B-кадра определяется так:

$$\overline{V}_{S_{B_{сж}}}^{(\xi,\gamma)} = V_{S_{B_{служ}}}^{(\xi,\gamma)} + \frac{V_{S_{B_{исх}}}}{k_B} = V_{S_{B_{служ}}}^{(\xi,\gamma)} + V_{S_{B_{сж}}}^{(\xi,\gamma)},$$

где $V_{S_{B_{исх}}}$ – интенсивность исходной (ξ,γ)-ой структурной единицы B-кадра;

k_B – коэффициент сжатия для структурных единиц B-кадра;

$V_{S_{B_{служ}}}^{(\xi,\gamma)}$ – длина кода служебной информации (ξ,γ)-ой структурной единицы B-кадра;

$V_{S_{B_{сж}}}^{(\xi,\gamma)}$ – длина битового потока компрессионного представления (ξ,γ)-ой структурной единицы B-кадра.

Интенсивность компрессионного представления B-кадра $V_{B_{сж}}$ определяется как сумма всех кодовых последовательностей компрессионного представления структурных единиц B-кадра. [104] Это описывается таким выражением:

$$V_{B_{сж}} = V_{S_{B_{служ}}} + \sum_{s=1}^{Ns_B} \frac{V_{S_{B_{исх}}}^{(s)}}{k_B} = V_{B_{служ}} + \sum_{s=1}^{Ns_b} (V_{S_{B_{служ}}}^{(s)} + V_{S_{B_{сж}}}^{(s)}),$$

где Ns_b – количество структурных единиц в B-кадре.

Соответственно, интенсивность V_{GOP} скрытой группы видеокадров определяется как сума битовых последовательностей всех видеокадров в группе и описывается выражением:

$$V_{GOP} = V_{служ}^{GOP} + V_{I_{скр}} + \sum_{s=1}^{N_B} V_{B_{сжs}} + \sum_{s=1}^{N_P} V_{P_{сжs}} .$$

где $V_{служ}^{GOP}$ – длина кода служебной информации группы видеокадров;

N_P – количество P-кадров в группе видеокадров;

N_B – количество B-кадров в группе видеокадров.

Тогда формула для вычисления интенсивности V_{GOP} скрытой группы видеокадров с учетом коэффициентов сжатия будет иметь вид:

$$V_{GOP} = V_{служ}^{GOP} + V_{I_{служ}} + V_{I_{служ}} + \sum_{s=1}^{|\Psi_{зн}|} \frac{V_{S_{I_{незн}}}^{(s)}}{k_I} + \sum_{s=1}^{|\Psi_{незн}|} \frac{V_{S_{I_{зн}}}^{(s)}}{k_{I_з}} +$$

$$+ V_{P_{служ}} + V_{S_{P_{служ}}} + \sum_{s=1}^{Ns_p} (V_{S_{P_{служ}}}^{(s)} + \frac{V_{S_{P_{исх}}}^{(s)}}{k_P}) + V_{B_{служ}} + \sum_{s=1}^{Ns_b} (V_{S_{B_{служ}}}^{(s)} + \frac{V_{S_{B_{исх}}}^{(s)}}{k_B})$$

или через интенсивность структурных единиц:

$$V_{GOP} = V_{служ}^{GOP} + V_{I_{служ}} + \sum_{s=1}^{|\Psi_{незн}|} (V_{I_{служ}}^{(s)} + V_{S_{I_{сж}}}^{(s)}) + \sum_{s=1}^{|\Psi_{зн}|} (V_{I_{служ}}^{(s)} + V_{S_{I_{скр}}}^{(s)}) +$$

$$+ V_{P_{служ}} + \sum_{s=1}^{Ns_p} (V_{S_{P_{служ}}}^{(s)} + V_{S_{P_{сж}}}^{(s)}) + V_{B_{служ}} + \sum_{s=1}^{Ns_b} (V_{S_{B_{служ}}}^{(s)} + V_{S_{B_{сж}}}^{(s)}).$$

Отсюда, по вышеизложенному можно заключить:

– разработана технология формирования кодовой конструкции для селективного метода обработки видеоданных, которая базируется на оценке кодового представления структурных единиц видеокадров с учетом их энергетической значимости;

– разработана методологическая база для оценки битовой скорости видеопотока с учетом наличия выделенных структурных единиц для закрытия видеоинформационного ресурса. При расчетах интенсивности группы видеокадров учитывается длина двоичного кода энергетически значимых структурных единиц базового видеокадра.

Научная новизна:

1. Впервые разработана технология формирования битового кода в селективном методе шифрования видеоинформационного ресурса с учетом энергетически значимых структурных единиц базового видеокадра. Отличительной особенностью этой технологии от стандартной является то, что при формировании битового потока для скрытия видеоинформационного ресурса вводится уровень структурных единиц в базовом видеокадре. Из них выделяются значимые структурные единицы по степени семантической и структурной информативности. Они влияют на дальнейшее формирование P и B-кадров. Применение такой технологии позволяет скрывать значимые структурные единицы базового видеокадра с помощью внедрения маркера признака закрытия в кодовую конструкцию видеопотока.

2. Получил дальнейшее развитие метод оценки интенсивности закрытого видеоинформационного ресурса на основе оценки энергетической значимости структурных единиц базового видеокадра. Главным его отличием является то, что при расчетах учитывается влияние отбора селективных структурных единиц со значимой семантической и структурной информативностью на битовую скорость закрытого видеоинформационного ресурса. Данный метод позволяет рассчитать пропускную способность закрытого видеоинформационного канала связи с учетом интенсивности битового потока зашифрованных и открытых структурных единиц.

3.4. Разработка метода совмещения технологии кодирования значимой структурной единицы и алгоритма блочного симметричного шифрования для метода повышения пропускной способности закрытого видеоканала.

Для реализации метода повышения пропускной способности закрытого видеоканала в работе используется алгоритм симметричного блочного шифрования «Калина». [22] Данный алгоритм был принят в национальном стандарте Украины ДСТУ 7624:2014 «Информационные технологии. Криптографическая защита информации. Алгоритм симметричного блочного преобразования» (введен в действие 1 июля 2015 г.). [100] Это позволяет применять его в ведомственных телекоммуникационных системах Украины. Криптографические преобразования, применяемые в алгоритме, соответствуют современным требованиям к уровню криптографической стойкости и быстродействию. [123] Алгоритм разработан с учетом существующих и потенциальных угроз, дальнейшего интенсивного развития информационных технологий и необходимости активного использования в течение нескольких следующих десятилетий. [23] Алгоритм ДСТУ «Калина» является результатом многолетнего плодотворного сотрудничества Государственной службы специальной связи и защиты информации Украины и ведущих украинских ученых, учитывает опыт и результаты проведения международных и открытых национальных конкурсов криптографических алгоритмов. По сравнению с известным международным стандартом AES (ISO/IEC 18033-3:2010), алгоритм «Калина» обеспечивает высокий уровень криптографической стойкости и аналогичное или более высокое быстродействие на современных и перспективных программных и программно-аппаратных платформах. [122] Алгоритм «Калина» обеспечивает:

- высокий уровень стойкости с запасом на случай появления новых атак и усовершенствования криптоаналитических комплексов на протяжении долгого времени;

- высокую скорость программной реализации на современных и перспективных платформах;

- более высокую или аналогичную эффективность по сравнению с лучшими мировыми решениями;

- наличие режимов работы, необходимых для эффективной реализации современных средств криптографической защиты;

- возможность эффективной интеграции двух национальных алгоритмов в одном средстве криптографической защиты;

- удобство реализации для разработчиков средств криптографической защиты.

На рис. 3.6 представлен сравнительный анализ быстродействия алгоритма шифрования «Калина» с другими алгоритмами.

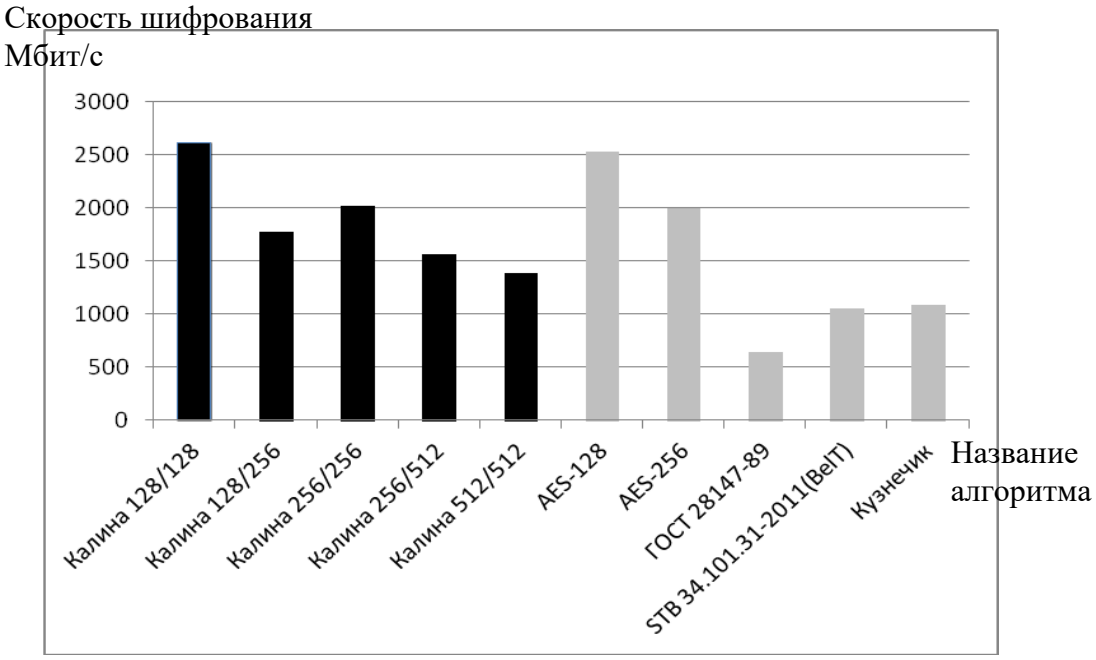


Рис. 3.6. Сравнительный анализ быстродействия алгоритма шифрования «Калина» с другими алгоритмами.

Из рис. 3.6 видно, что алгоритма шифрования «Калина» с длиной ключа в 128 бит является одним из самых быстрых по скорости шифрования. Показатель скорости шифрования данного алгоритма превышает 2500 Мбит/с. Поэтому для шифрования значимых структурных единиц предлагается

использование алгоритм «Калина» с длиной ключа в 128 бит. Такой ключ выбран по тому, что его длины достаточно для обеспечения требуемого уровня конфиденциальности для ведомственных систем видеоконференцсвязи.

Рассмотрим совместимость кодовой конструкции энергетически значимой структурной единицы с алгоритмом шифрования «Калина». Она заключается в создании механизма наложения криптоключа на кодовую конструкцию, подлежащую шифрованию, без образования избыточной информации. [67] Для этого необходимо разработать основные этапы формирования двоичного кода зашифрованной значимой структурной единицы, которые базируются на трех технологических составляющих.

Первая технологическая составляющая заключается в формировании двоичного кода значения компоненты трансформанты ДКП для блока изображения**.**

Значения DC-компоненты трансформанты ДКП размером 8*8 элементов может меняться от 0 до 2047 (-1024 до 1023, так как в JPEG производится вычитание 128 из всех исходных значений, что соответствует вычитанию 1024 из DC). [121] Поэтому на кодирование каждого значения компоненты $y_{\mu,\eta}$ трансформанты $T_{\varphi}^{(\xi,\gamma)}$ ДКП будет выделяться по 11 бит. Это определяется следующим выражением:

$$v(\varphi)_{\mu,\eta}^{(\xi,\gamma)} = \max_{\substack{1\le\mu\le8\\1\le\eta\le8}}(\log_2 y_{\mu,\eta}) = 11\,\text{бит},$$

где $v(\varphi)_{\mu,\eta}^{(\xi,\gamma)}$ – длина битового представления значения компоненты $y_{\mu,\eta}$ трансформанты $T_{\varphi}^{(\xi,\gamma)}$ ДКП φ-го блока $B_{\varphi}^{(\xi,\gamma)}$ (ξ,γ)-ой структурной единицы $S_{\text{зн}}^{(\xi,\gamma)}$ изображения.

Однако здесь требуется учитывать следующие условия:

1. Длина ключа шифрования является четным числом. Поэтому для обеспечения совместимости битового представления значения компоненты $y_{\mu,\eta}$ трансформанты $T_{\varphi}^{(\xi,\gamma)}$ ДКП с ключом шифрования, необходимо, чтобы длина кода значение компоненты $y_{\mu,\eta}$ тоже была четной. [30]

2. Значение компоненты $y_{\mu,\eta}$ трансформанты $T_{\varphi}^{(\xi,\gamma)}$ ДКП может быть как положительным, так и отрицательным. [55]

Поэтому для обеспечения этих условий предлагается использовать дополнительный указатель знака компоненты $y_{\mu,\eta}$ трансформанты $T_{\varphi}^{(\xi,\gamma)}$ ДКП. Длина его кодового представления равна 1 бит. Данный указатель будет использоваться непосредственно в битовой последовательности значения компоненты $y_{\mu,\eta}$ трансформанты $T_{\varphi}^{(\xi,\gamma)}$ ДКП для обеспечения четной длины кода значение компоненты $y_{\mu,\eta}$. Тогда при размере трансформанты $T_{\varphi}^{(\xi,\gamma)} = \{8,8\}$ длина кодового представления компонента в двоичном описании будет равна 12 битам. Это представлено на рис. 3.7.

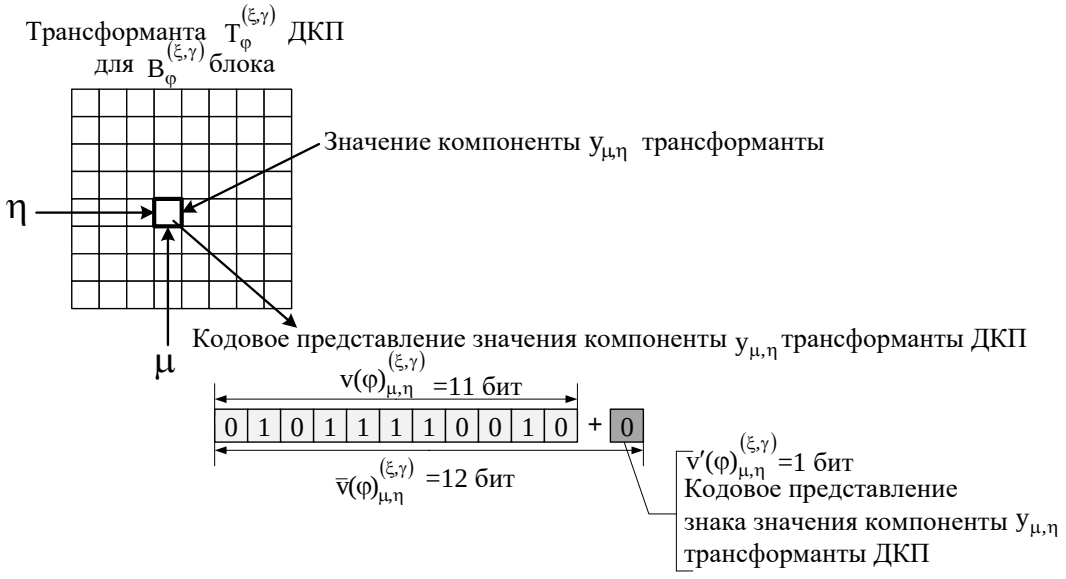


Рис. 3.7. Схема формирования кодового представления $\bar{v}(\varphi)_{\mu,\eta}^{(\xi,\gamma)}$ значения компоненты $y_{\mu,\eta}$ трансформанты $T_{\varphi}^{(\xi,\gamma)}$ ДКП для блока $B_{\varphi}^{(\xi,\gamma)}$ изображения.

На рис. 3.7 изображено сформированное кодовое представление компоненты $y_{\mu,\eta}$ трансформанты $T_{\varphi}^{(\xi,\gamma)}$ ДКП длиной $\bar{v}(\varphi)_{\mu,\eta}^{(\xi,\gamma)}$ в 12 бит для дальнейшего шифрования. В первых 11 битах длины $v(\varphi)_{\mu,\eta}^{(\xi,\gamma)}$ кода записано значение компоненты трансформанты ДКП $y_{\mu,\eta} = 754$. В 12-ый бит записывается значение 0 или 1, которое учитывает знак компоненты. Это представлено в следующем выражении:

$$\bar{v}(\varphi)_{\mu,\eta}^{(\xi,\gamma)} = v(\varphi)_{\mu,\eta}^{(\xi,\gamma)} + v'(\varphi)_{\mu,\eta}^{(\xi,\gamma)}.$$

Тогда интенсивность $V(\varphi)_{\text{скр}}^{(\xi,\gamma)}$ битового потока трансформанты $T_{\varphi}^{(\xi,\gamma)}$ ДКП рассчитывается так:

$$V(\varphi)_{\text{скр}}^{(\xi,\gamma)} = \sum_{i=1}^{\mu\cdot\eta} \bar{v}(\varphi)_{i}^{(\xi,\gamma)} = 768 \text{ бит} = 96 \text{ байт},$$

где $\bar{v}(\varphi)^{(\xi,\gamma)}$ – длина кодового представления (μ,η)-ой компоненты трансформанты $T_{\varphi}^{(\xi,\gamma)}$ ДКП φ-го блока $B_{\varphi}^{(\xi,\gamma)}$ (ξ,γ)-ой структурной единицы $S_{\text{зн}}^{(\xi,\gamma)}$ изображения.

Таким образом, длина $V(\varphi)_{\text{скр}}^{(\xi,\gamma)}$ кодового слова трансформанты ДКП из 64 компонент $T_{\varphi}^{(\xi,\gamma)} = \{y1,\ldots,y64\}$ будет занимать 768 бит = 96 байт (рис. 3.8).

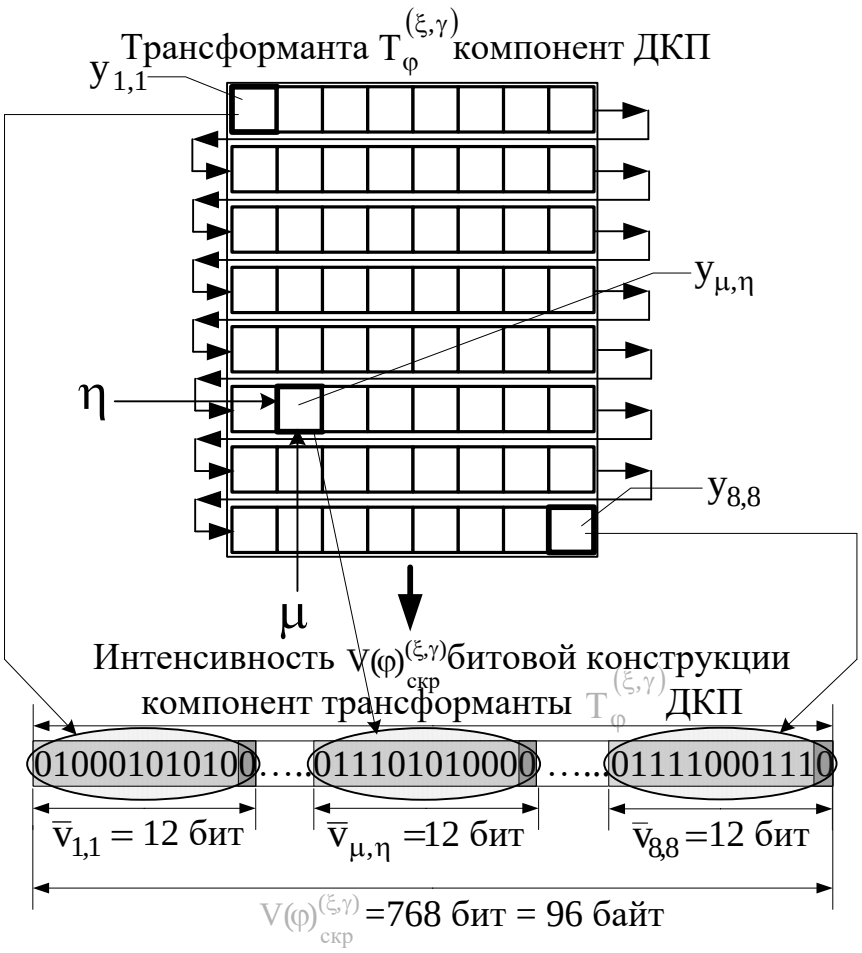


Рис. 3.8. Схема формирования кодового представления $\tilde{V}(\varphi)_{скр}^{(\xi,\gamma)}$ значений компонент трансформанты $T_{\varphi}^{(\xi,\gamma)}$ ДКП блока $B_{\varphi}^{(\xi,\gamma)}$ изображения.

Вторая технологическая составляющая заключается в формировании кодовой конструкции структурной единицы базового видеокадра, подлежащей шифрованию.

Структурная единица базового видеокадра состоит из 6 блоков (4 блока яркости и 2 цветности). [116] Длины кодового представления блоков яркости и цветности, подлежащих шифрованию, равны. Это представлено следующим выражением:

$$V_{B(Y)скр}^{(\xi,\gamma)} = V_{B(Cr)скр}^{(\xi,\gamma)} = V_{B(Cb)скр}^{(\xi,\gamma)} = V(\varphi)_{скр}^{(\xi,\gamma)} = 768\,\text{бит} = 96\,\text{байт},$$

где $V^{(\xi,\gamma)}_{B(Y)_{скр}}$ – длина кодового представления трансформанты ДКП блока яркости;

$V^{(\xi,\gamma)}_{B(Cr)_{скр}}$ – длина кодового представления трансформанты ДКП блока красного цвета;

$V^{(\xi,\gamma)}_{B(Cb)_{скр}}$ – длина кодового представления трансформанты ДКП блока синего цвета.

Интенсивность $V''^{(\xi,\gamma)}_{S_{I_{скр}}}$ структурной единицы, подлежащей шифрованию, определяется так:

$$V''^{(\xi,\gamma)}_{S_{I_{скр}}} = \sum_{\varphi=1}^{N_b} V(\varphi)^{(\xi,\gamma)}_{скр} = 4608 \text{ бит} = 576 \text{ байт},$$

где N_b – количество блоков в структурной единице.

Тогда интенсивность $V_{S_{скр}}$ битового потока закрытой структурной $S^{(\xi,\gamma)}_{зн}$ единицы рассчитывается как:

$$V_{S_{I_{скр}}} = V''^{(\xi,\gamma)}_{I_{служ}} + V''^{(\xi,\gamma)}_{S_{I_{скр}}} = V''^{(\xi,\gamma)}_{I_{служ}} + \sum_{\varphi=1}^{N_b} V(\varphi)^{(\xi,\gamma)}_{скр} =$$

$$= 24 \text{ бита} + 4608 \text{ бит} = 4632 \text{ бита} = 3 \text{ байта} + 576 \text{ байт} = 579 \text{ байт}.$$

Таким образом, структура кодовой конструкции закрытой структурной единицы будет иметь вид, представленный на рис 3.9.

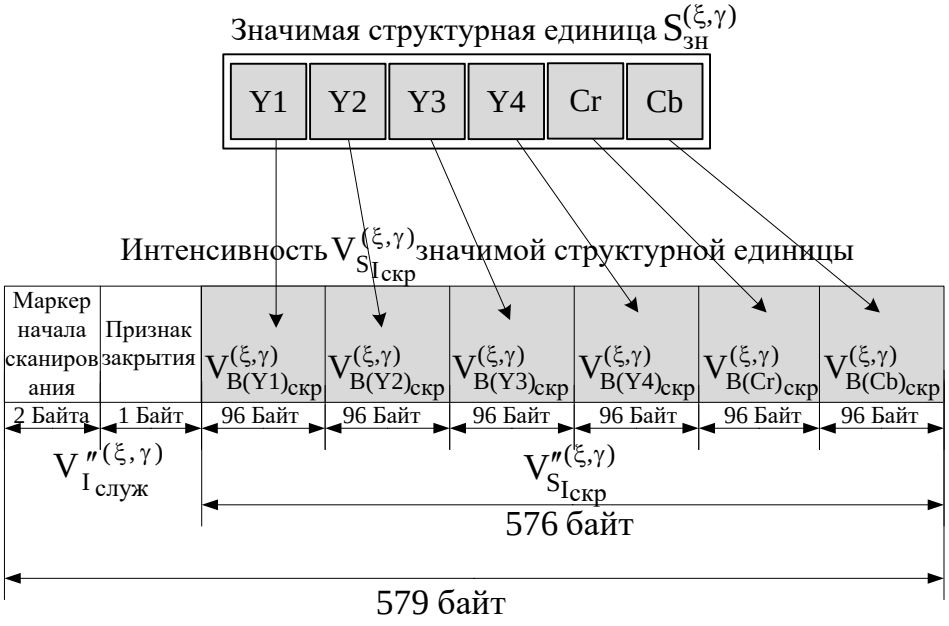


Рис. 3.9. Структура кодовой конструкции закрытой структурной единицы базового видеокадра.

Из рис. 3.9 видно, что структурная единица, подлежащая шифрованию, имеет длину $V_{S_{I_{скр}}}^{(\xi,\gamma)}$ 576 байт (96 байт*6=576 байт) при условии, что размер блока $B_{\varphi}^{(\xi,\gamma)}$ видеоизображения равен 64 пикселям ($\mu = 8, \eta = 8$). Длина кода $V_{S_{I_{исх}}}$ исходного изображения размером в 256 пикселей ($m = 16, n = 16$), где размер одного пикселя равен 1 байту, представленного в трех плоскостях (YCrCb) будет равна 768 байт:

$$V_{S_{I_{исх}}} = V_{B(Y_{m,n})_{исх}} + V_{B(Cr_{m,n})_{исх}} + V_{B(Cb_{m,n})_{исх}} =$$
$$= 16 \cdot 16 \text{ бит} + 16 \cdot 16 \text{ бит} + 16 \cdot 16 \text{ бит} = 786 \text{ байт}$$

где $V_{B(Y_{m,n})_{исх}}$ – битовая интенсивность кода яркостной составляющей исходного изображения;

$V_{B(Cr_{m,n})_{исх}}$ – битовая интенсивность составляющей красного цвета исходного изображения;

$V_{B(Cb_{m,n})исх}$ – битовая интенсивность составляющей синего цвета исходного изображения.

Отсюда следует, что в результате применения внутрикадрового метода селективного шифрования за счет использования формата цветового представления 4:2:0 интенсивность битового потока структурной единицы после шифрования снизится на 25% по сравнению с битовым потоком исходного видеоизображения.

Третья технологическая составляющая заключается в формировании матриц двоичного кода значимой структурной единицы такого же размера, что и ключ шифрования.

Ключ алгоритма шифрования «Калина» длиной в 128 бит (16 байт) представлен в виде матрицы К, которая состоит из 16 элементов по 8 бит (1 байт) каждый:

$$K = \begin{bmatrix} k1 & k2 & k3 & k4 \\ k5 & k6 & k7 & k8 \\ k9 & k10 & k11 & k12 \\ k13 & k14 & k15 & k16 \end{bmatrix}.$$

$$K = \{k_i\}, \text{ где } i = \overline{1,16},$$

где k_i – 8-битный элемент матрицы шифрования К;

i – номер 8-битного элемента в матрице шифрования К.

Для битового согласования элементов матрицы шифрования $K = \{k1,...k16\}$ с битовым потоком компонент трансформанты $T_{\varphi}^{(\xi,\gamma)}$ предлагается битовый поток $V(\varphi)_{скр}^{(\xi,\gamma)}$ поделить на элементы такой же длины как элементы матрицы шифрования К. [95] Таким образом, весь битовый поток

$V^{(\xi,\gamma)}_{B(\varphi)скр}$ компонент трансформанты $T^{(\xi,\gamma)}_{\varphi}$ (ξ,γ)-ой структурной единицы разделяется на 96 элементов по 8 бит. Это выражено следующей формулой:

$$b_i = \frac{V^{(\xi,\gamma)}_{B(\varphi)скр}}{8\ бит} = \frac{768\ бит}{8\ бит} = 96, \text{ где } i = \overline{1, 96},$$

где b_i – 8-битный элемент переформатированного потока компонент трансформанты $T^{(\xi,\gamma)}_{\varphi}$ (ξ,γ)-ой структурной единицы;

i – номер 8-битного элемента переформатированного потока компонент трансформанты $T^{(\xi,\gamma)}_{\varphi}$ (ξ,γ)-ой структурной единицы.

Схема формирования элементов по 8 бит из битового потока компонент трансформанты $T^{(\xi,\gamma)}_{\varphi}$ (ξ,γ)-ой структурной единицы базового видеокадра представлена на рис. 3.10.

Так как длина ключа алгоритма шифрования «Калина» представлена в виде матрицы из 16 элементом (4*4) длиной в 128 бит, то для ее согласования с битовым потоком компонент трансформанты $T^{(\xi,\gamma)}_{\varphi}$ необходимо этот битовый поток разделить на фрагменты по 128 бит. [26] Для этого предлагается разделить битовый поток компонент трансформанты $T^{(\xi,\gamma)}_{\varphi}$ на 8 равных частей (d1…d8), длина каждой из них равна 96 битам (12 байтам). [110]

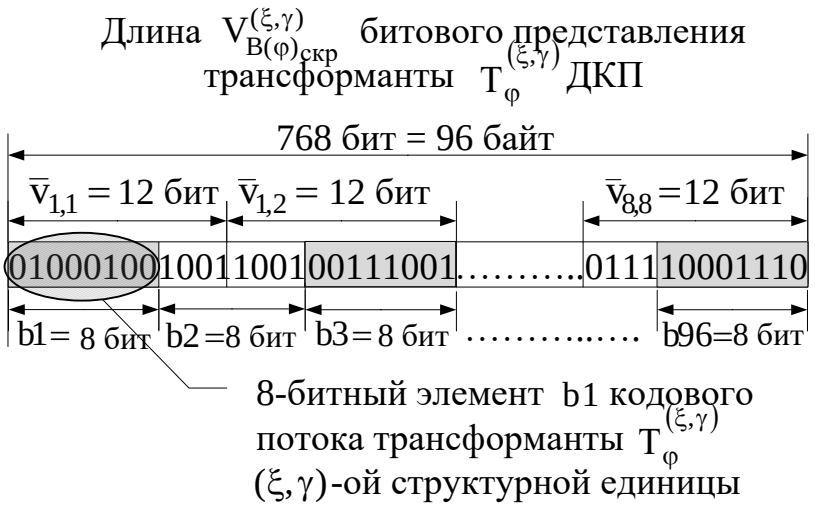


Рис. 3.10. Схема формирования элементов по 8 бит из битового потока компонент трансформанты $T^{(\xi,\gamma)}_{\varphi}$ (ξ,γ)-ой структурной единицы базового видеокадра.

Полученные фрагменты (d1,…,d8) по 12 байт располагаются по очереди сверху вниз. В результате чего формируется матрица $\overline{T}^{(\xi,\gamma)}_{\varphi} = \{b1,...,b96\}$ 8-битных элементов машинного кода компонент трансформанты $T^{(\xi,\gamma)}_{\varphi}$ ДКП. [43] Таким образом, матрица $\overline{T}^{(\xi,\gamma)}_{\varphi}$ будет иметь 12 элементов по горизонтали и 8 элементов по вертикали. Это представлено на рис. 3.11.

Далее предлагается полученную матрицу $\overline{T}^{(\xi,\gamma)}_{\varphi}$ двоичного кода φ-го блока $B^{(\xi,\gamma)}_{\varphi}$ (ξ,γ)-ой структурной единицы $S^{(\xi,\gamma)}_{зн}$ разделить на 6 матриц (T1,…,T6) по 128 бит (16 байт) [105]. Это выражено следующей формулой:

$$\overline{T}^{(\xi,\gamma)}_{\varphi} = T1 \cup T2 \cup T3 \cup T \cup T5 \cup T6.$$

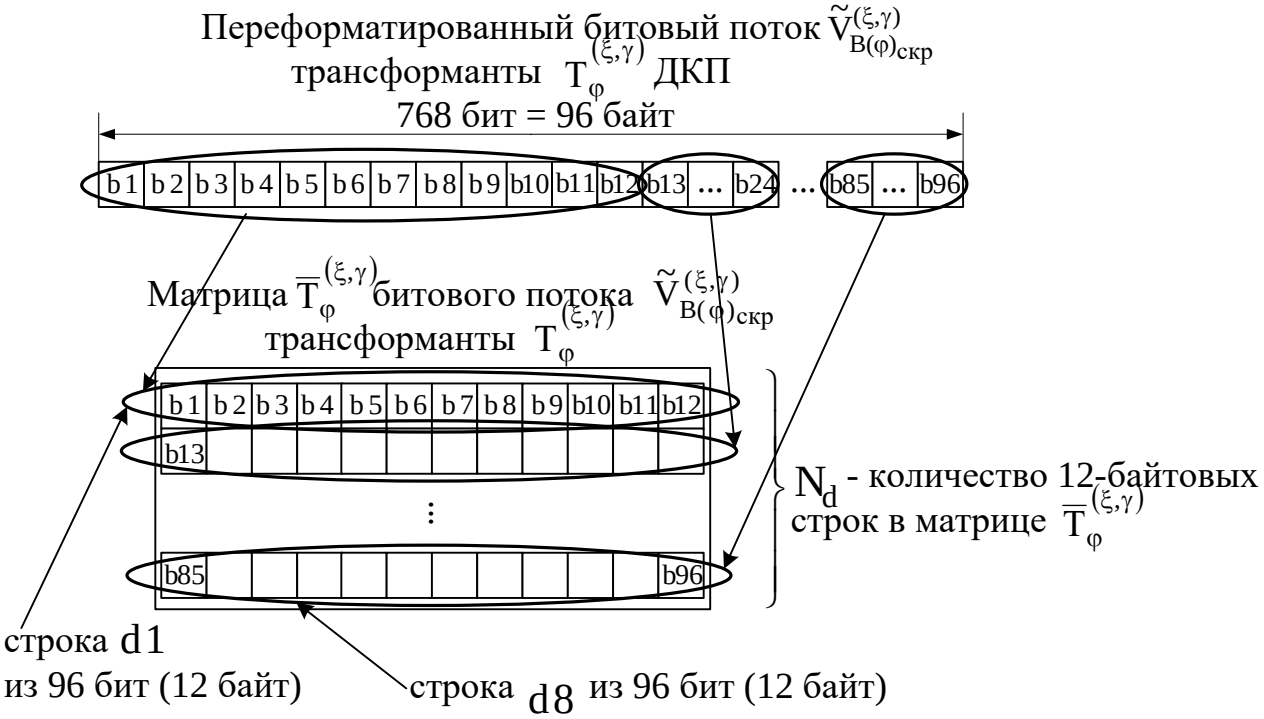


Рис. 3.11. Формирование матрицы $\overline{T}^{(\xi,\gamma)}_{\varphi}$ двоичного кода, состоящей из 8 строк по 12 байт.

Формирование матриц происходит путем деления строк d1, d2, d3 d4 и d5, d6, d7, d8 на три равные части по 4 байта (16 бит). Это представлено на рис. 3.12.

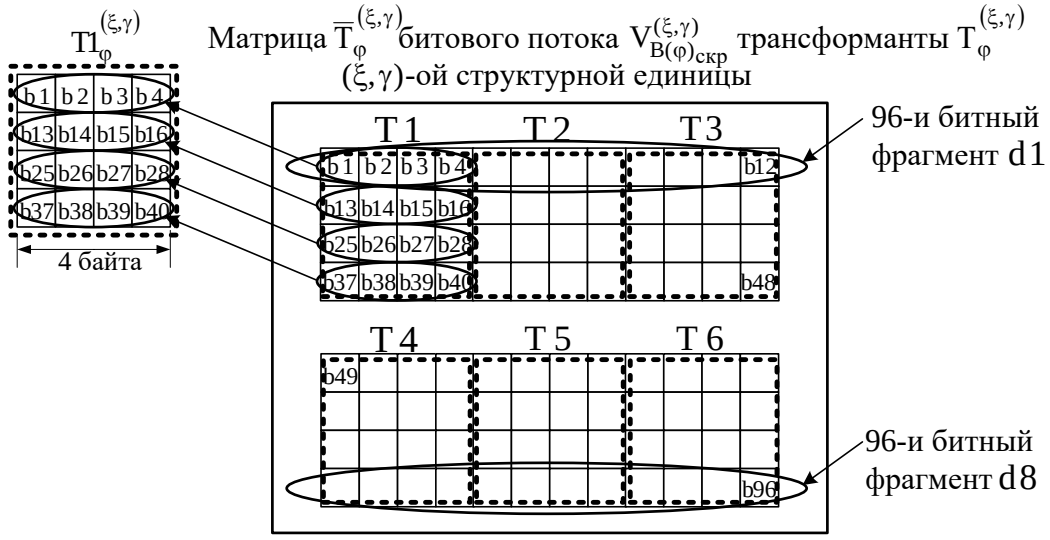


Рис. 3.12. Формирование матриц T1,…,T6 двоичного кода для наложения на них шифроключа К.

Из рис. 3.12 видно, что в результате скремблирования 8-ми битных элементов (b1,…,b96) матрицы $\overline{T}_{\varphi}^{(\xi,\gamma)}$ битового кода дополнительно повышается помехоустойчивость и степень защиты передаваемых закрытых видеоданных.

Таким образом для шифрования битового потока трансформанты $T_{\varphi}^{(\xi,\gamma)}$ ДКП блока $B_{\varphi}^{(\xi,\gamma)}$ изображения (ξ,γ)-ой структурной единицы базового видеокадра сформировано 6 матриц (T1,…,T6) такого же размера, как шифроключ (128 бит):

$$T1=\begin{bmatrix} b1 & b2 & b3 & b4 \\ b13 & b14 & b15 & b16 \\ b25 & b26 & b27 & b28 \\ b37 & b38 & b39 & b40 \end{bmatrix} T2=\begin{bmatrix} b5 & b6 & b7 & b8 \\ b17 & b18 & b19 & b20 \\ b29 & b30 & b31 & b32 \\ b41 & b42 & b43 & b44 \end{bmatrix} T3=\begin{bmatrix} b9 & b10 & b11 & b12 \\ b21 & b22 & b23 & b24 \\ b33 & b34 & b35 & b36 \\ b45 & b46 & b47 & b48 \end{bmatrix}$$

$$T4=\begin{bmatrix} b49 & b50 & b51 & b52 \\ b61 & b62 & b63 & b64 \\ b73 & b74 & b75 & b76 \\ b85 & b86 & b87 & b88 \end{bmatrix} T5=\begin{bmatrix} b53 & b54 & b55 & b56 \\ b65 & b66 & b67 & b68 \\ b77 & b78 & b79 & b80 \\ b89 & b90 & b91 & b92 \end{bmatrix} T6=\begin{bmatrix} b57 & b58 & b59 & b60 \\ b69 & b70 & b71 & b72 \\ b81 & b82 & b83 & b84 \\ b93 & b94 & b95 & b96 \end{bmatrix}$$

Ключ шифрования К длиной в 128-бит накладывается на каждую матрицу (T1,…,T6) битового кода отдельно. [111] Это представлено в следующих выражениях:

$$T'1=E_K(T1);\ T'2=E_K(T2);\ T'3=E_K(T3);$$
$$T'4=E_K(T4);\ T'5=E_K(T5);\ T'6=E_K(T6),$$

где E_K – функция шифрования матриц $T_i=T1,...,T6$ матрицей ключей К.

Функция шифрования E_K с помощью матрицы $K=\{k1,...k16\}$ проводит шифрование матрицы T_i. [32] Алгоритм шифрования «Калина» выполняет шифрование каждого из 16 элементов матрицы T_i с помощью 16 элементов

матрицы ключей $K = \{k1,...k16\}$. Длина каждого элемента в матрице шифрования К и матрице T_i равна 8 битам. [99] В результате чего формируются 6 матриц $(T'1,...,T'6)$ битовых зашифрованных компонент трансформанты ДКП блока видеокадра:

$$T'1 = \begin{bmatrix} c1 & c2 & c3 & c4 \\ c13 & c14 & c15 & c16 \\ c25 & c26 & c27 & c28 \\ c37 & c38 & c39 & c40 \end{bmatrix} T'2 = \begin{bmatrix} c5 & c6 & c7 & c8 \\ c17 & c18 & c19 & c20 \\ c29 & c30 & c31 & c32 \\ c41 & c42 & c43 & c44 \end{bmatrix} T'3 = \begin{bmatrix} c9 & c10 & c11 & c12 \\ c21 & c22 & c23 & c24 \\ c33 & c34 & c35 & c36 \\ c45 & c46 & c47 & c48 \end{bmatrix}$$

$$T'4 = \begin{bmatrix} c49 & c50 & c51 & c52 \\ c61 & c62 & c63 & c64 \\ c73 & c74 & c75 & c76 \\ c85 & c86 & c87 & c88 \end{bmatrix} T'5 = \begin{bmatrix} c53 & c54 & c55 & c56 \\ c65 & c66 & c67 & c68 \\ c77 & c78 & c79 & c80 \\ c89 & c90 & c91 & c92 \end{bmatrix} T'6 = \begin{bmatrix} c57 & c58 & c59 & c60 \\ c69 & c70 & c71 & c72 \\ c81 & c82 & c83 & c84 \\ c93 & c94 & c95 & c96 \end{bmatrix}$$

где $c1,...,c96$ – 8-битные элементы зашифрованного потока компонент трансформанты $T_\varphi^{(\xi,\gamma)}$ (ξ,γ)-ой структурной единицы;

Процесс наложения шифроключа К на матрицу Т1 представлен на рис. 3.13.

Рис. 3.13. Схема шифрования двоичных данных матрицы Т1 из матрицы $\overline{T}_\varphi^{(\xi,\gamma)}$ битового кода компонент трансформанты $T_\varphi^{(\xi,\gamma)}$ ДКП блока $B_\varphi^{(\xi,\gamma)}$ изображения.

Из рис. 3.13 видно, что в результате наложения 16-байтового ключа К на 16-байтовую матрицу Т1 двоичных данных формируется 16-байтовая матрица Т′1 зашифрованных компонент трансформанты $T_{\varphi}^{(\xi,\gamma)}$ ДКП. Таким образом, происходит шифрование всех битовых матриц значимой структурной единицы без образования избыточных битов данных.

На рис. 3.14 представлена схема формирования битового потока из матрицы $\overline{T}_{\varphi}^{(\xi,\gamma)}$ зашифрованного двоичного кода.

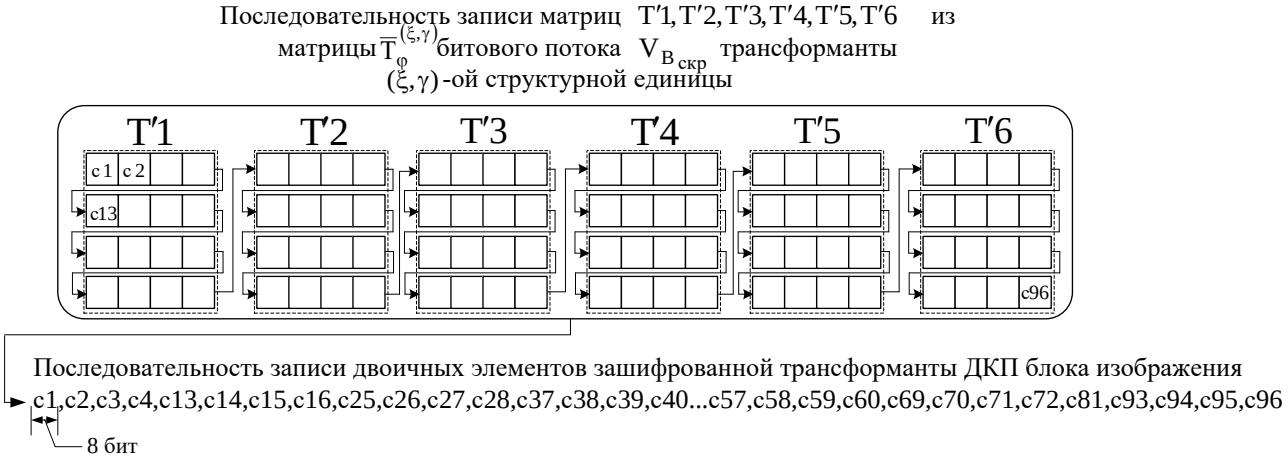


Рис. 3.14. Схема формирования битового потока из матрицы $\overline{T}_{\varphi}^{(\xi,\gamma)}$ зашифрованного двоичного кода.

На рис. 3.15 представлен процесс шифрования алгоритмом «Калина» и схема формирования машинного кода зашифрованной энергетически значимой структурной единицы $S_{зн}^{(\xi,\gamma)}$ видеокадра. В результате чего происходит шифрование всего битового потока энергетически значимых структурных единиц $S_{зн}^{(\xi,\gamma)}$ видеоизображения без остатка и избытка битовых последовательностей.

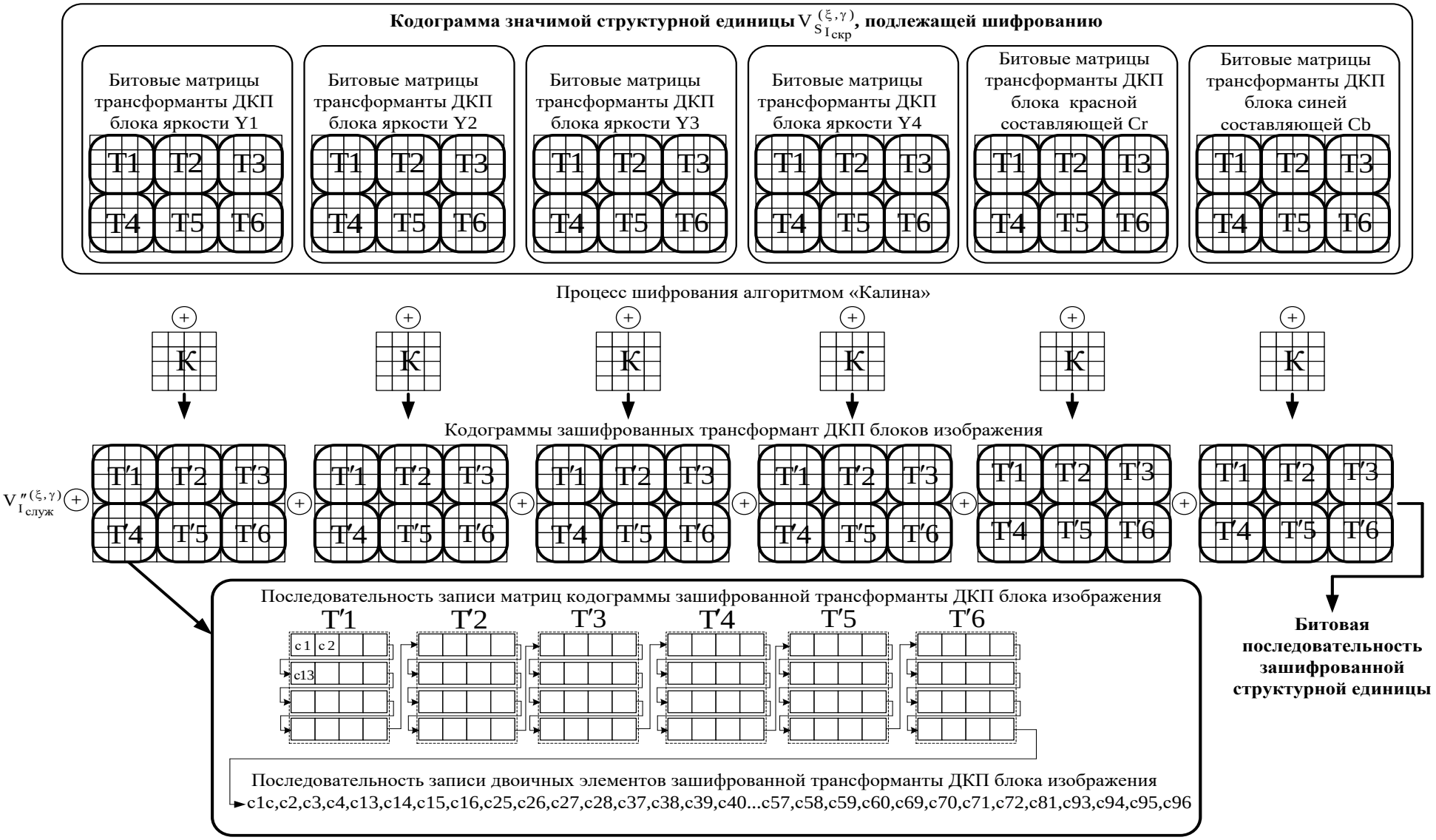


Рис. 3.15. Процесс шифрования кодовой конструкции и схема формирования двоичного кода зашифрованной структурной единицы.

Таким образом, разработан метод совместимости кодовой конструкции энергетически значимой структурной единицы и ключевой последовательности алгоритма шифрования «Калина». Он базируется на следующих технологических составляющих:

1. Формирование 12-битового кодового представления значения компоненты трансформанты ДКП из 11-битового значения компоненты трансформанты ДКП и 1-битового элемента, который определяет знак значения этой компоненты. [106] В результате чего образуется машинное слово четной длины. Таким образом, достигается дальнейшая совместимость битового потока энергетически значимой структурной единицы со 128-битным ключом шифрования.

2. Формирование кодовой конструкции значимой структурной единицы базового видеокадра, подлежащей шифрованию. В результате чего записывается определенным образом 579-битная последовательность служебных данных и цифровых описаний блоков яркости и цветности структурной единицы.

3. Формирование матриц двоичного кода значимой структурной единицы такого же размера, что и ключ шифрования. В результате чего происходит скремблирование битового потока, что дополнительно повышает степень защиты и помехоустойчивости передаваемых закрытых видеоданных. [54]

При шифровании сформированных матриц кодового представления структурной единицы с помощью алгоритма «Калина» достигается полная совместимость 128-битного шифроключа со 128-битными фрагментами потока структурной единицы без образования избыточных битов данных. После чего из полученных матриц двоичного кода зашифрованной структурной единицы формируется битовая последовательность закрытых видеоданных. [51]

В результате применения метода совместимости кодовой конструкции энергетически значимой структурной единицы и ключевой последовательности алгоритма шифрования «Калина» при использовании внутрикадровой селективной обработке базового видеокадра происходит увеличение

интенсивности закрытого базового видеокадра на 20-45% по сравнению с компрессионным базовым видеокадром. При этом достигается уменьшение интенсивности зашифрованной структурной единицы по сравнению с исходной на 25% за счет использования формата цветового представления 4:2:0.

3.5. Создание метода декодирования закрытого видеопотока на основе технологии внутрикадровой селекции.

Предлагается разработать метод декодирования закрытого видеопотока на основе внутрикадровой селекции, которая базируется на выявлении закрытых значимых структурных единиц базового видеокадра. Для этого предлагается декодировать закрытый базовый видеокадр K_I с учетом определения значимых $S_{зн}^{(\xi,\gamma)}$ структурных единиц. [71] Структурная схема метода декодирования закрытого видеопотока представлена на рис. 3.16.

Метод декодирования закрытого видеопотока включает в себя следующие базовые этапы:

1. Выделение кодовой конструкции группы кадров из двоичной последовательности потока видеоданных.

2. Определение типа видеокадров в группе кадров.

3. Выделение цифрового представления закрытого базового видеокадра K_I из цифрового представления группы кадров.

4. Определение закрытых $S_{зн}^{(\xi,\gamma)}$ и не закрытых $S_{незн}^{(\xi,\gamma)}$ структурных единиц. Это происходит в результате анализа метки M, значение которой хранится в дополнительных данных цифровом описании структурной единицы. [98] Если значение метки M=1, то структурная единица определяется как значимая $S^{(\xi,\gamma)} = S_{зн}^{(\xi,\gamma)}$. Если значение метки M=0, то структурная единица определяется как незначимая $S^{(\xi,\gamma)} = S_{незн}^{(\xi,\gamma)}$.

5. Дешифровка закрытых значимых $S_{зн}^{(\xi,\gamma)}$ структурных единиц, при которой расшифровываются значения компонент трансформант ДКП блоков $B(Y)_{m,n}^{(\xi,\gamma)}$, $B(Cr)_{m,n}^{(\xi,\gamma)}$ и $B(Cb)_{m,n}^{(\xi,\gamma)}$.

6. Декодирование незначимых $S_{незн}^{(\xi,\gamma)}$ структурных единиц, которое включает в себя такие этапы:

6.1. Обратная линеаризация трансформант ДКП блоков составляющей яркости и цветности $B(Y)_{m,n}^{(\xi,\gamma)}$, $B(Cr)_{m,n}^{(\xi,\gamma)}$ и $B(Cb)_{m,n}^{(\xi,\gamma)}$ незначимых структурных единиц. [34]

6.2. Деквантование трансформант ДКП незначимых блоков.

7. Обратное ДКП значимых и незначимых блоков составляющей яркости и цветности $B(Y)_{m,n}^{(\xi,\gamma)}$, $B(Cr)_{m,n}^{(\xi,\gamma)}$ и $B(Cb)_{m,n}^{(\xi,\gamma)}$.

8. Построение композиции структурных единиц $S^{(\xi,\gamma)}$ базового видеокадра K_I, которое включает в себя следующие этапы:

8.1. Декодирование служебной информации для формирования структурных единиц $S^{(\xi,\gamma)}$.

8.2. Формирование композиций макроблоков $M(Y)^{(\xi,\gamma)}$, $M(C_r)^{(\xi,\gamma)}$ и $M(C_b)^{(\xi,\gamma)}$. [62]

8.3. Формирование видеоизображения из блоков $B(Y)_{m,n}^{(\xi,\gamma)}$, $B(Cr)_{m,n}^{(\xi,\gamma)}$ и $B(Cb)_{m,n}^{(\xi,\gamma)}$.

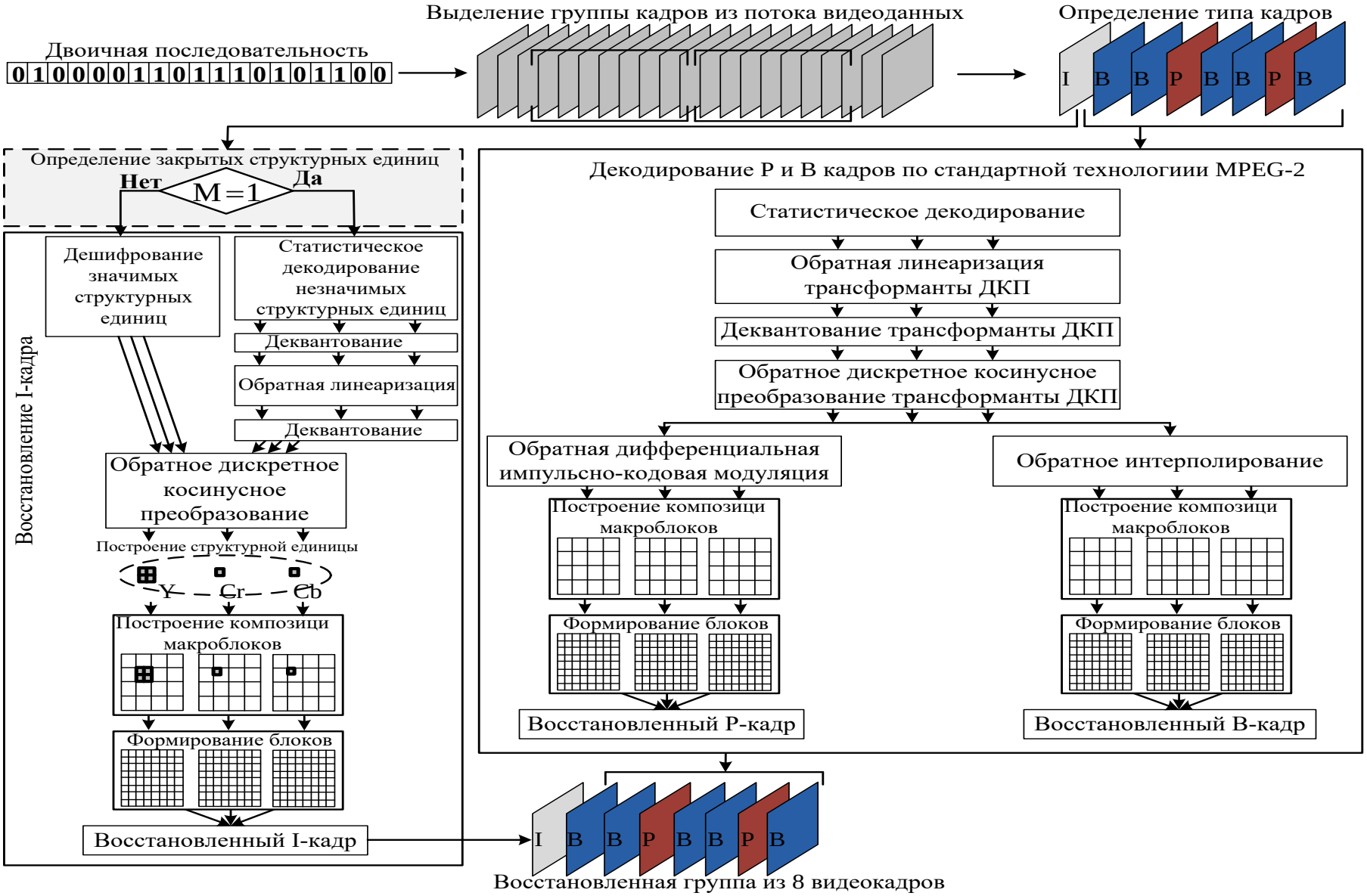


Рис. 3.16. Блок-схема восстановления закрытой группы видеокадров, зашифрованной селективным методом.

9. Преобразование цифровых плоскостей видеоизображения I-кадра из формата YUV в формат RGB (формирование одного видеоизображения из 3-х цифровых плоскостей YCrCb). [47]

10. Обратная дифференциальная импульсно-кодовая модуляция для восстановления P-кадров.

11. Обратное интерполирование для восстановления B-кадров.

12. Преобразование цифровых плоскостей видеоизображений P и B-кадров из формата YUV в формат RGB. [96]

13. Формирование группы видеокадров из восстановленных I, P и B-кадров.

14. Формирование восстановленной видеопоследовательности из групп видеокадров.

После выделения базового кадра из битового потока группы видеокадров происходит определение значимых $S_{зн}^{(\xi,\gamma)}$ и незначимых $S_{незн}^{(\xi,\gamma)}$ структурных единиц. Выявление значимых $S_{зн}^{(\xi,\gamma)}$ структурных единиц заключается в определении значения бита признака закрытия M, который находится в служебной части кодовой конструкции всех структурных единиц базового видеокадра. Если значение бита признака закрытия M=1, то осуществляется стандартное декодирование структурной единицы. Если значение бита признака закрытия M=0, то такая структурная единица определяется как значимая, и она подлежит расшифровке.

Процесс расшифровывания $S_{зн}^{(\xi,\gamma)}$ структурных единиц происходит следующим образом:

1. Информационная часть битовой последовательности значимой $S_{зн}^{(\xi,\gamma)}$ структурной единицы делится на 6 равных фрагментов кода. Таким образом формируются 6 битовых потоков $\tilde{V}_{B(\varphi)скр}^{(\xi,\gamma)}$ трансформант $T_{\varphi}^{(\xi,\gamma)}$ ДКП блоков $B_{\varphi}^{(\xi,\gamma)}$ (ξ,γ)-ой структурной единицы $S_{зн}^{(\xi,\gamma)}$.

2. Формирование битовых матриц $T'1_{\varphi}^{(\xi,\gamma)},...,T'6_{\varphi}^{(\xi,\gamma)}$ из битового потока $\tilde{V}_{B(\varphi)_{скр}}^{(\xi,\gamma)}$ трансформант $T_{\varphi}^{(\xi,\gamma)}$ ДКП. Это происходит делением битового потока $\tilde{V}_{B(\varphi)_{скр}}^{(\xi,\gamma)}$ на строки длиной 4 байта. Каждые 4 строки битового потока $\tilde{V}_{B(\varphi)_{скр}}^{(\xi,\gamma)}$ формируют матрицу из 16 элементов. Это представлено на рис. 3.17.

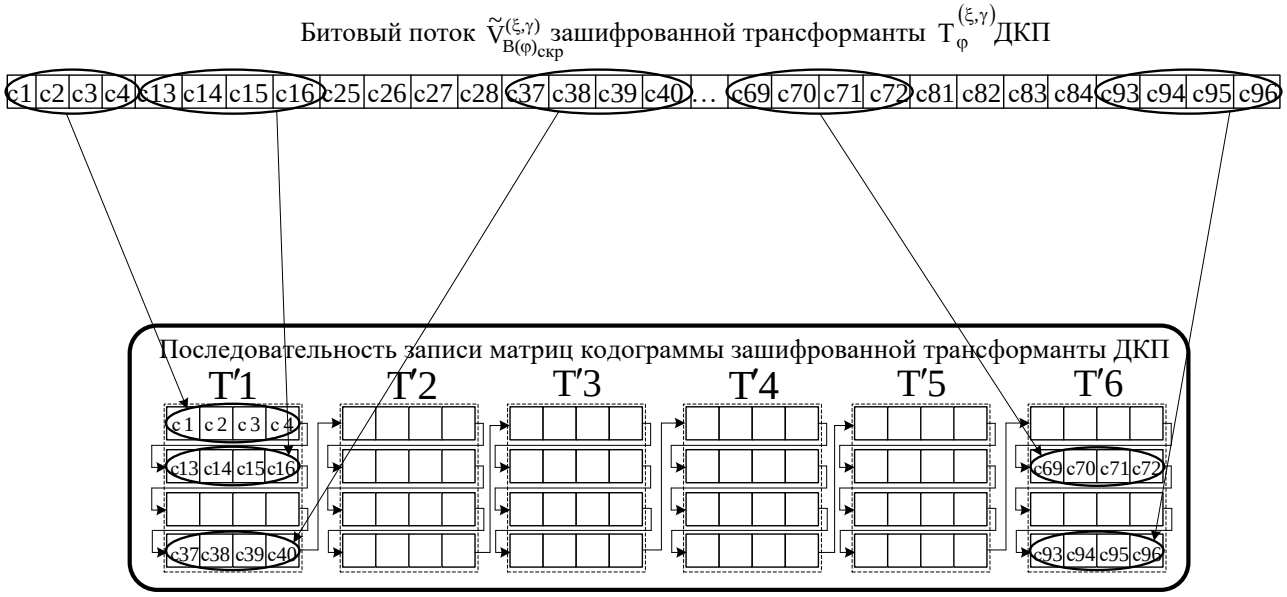


Рис. 3.17. Схема формирования 6 матриц ($T'1_{\varphi}^{(\xi,\gamma)},...,T'6_{\varphi}^{(\xi,\gamma)}$) по 16 байт из битового потока $\tilde{V}_{B(\varphi)_{скр}}^{(\xi,\gamma)}$ зашифрованной трансформанты ДКП.

На рис. 3.17 представлен процесс формирования 6 матриц ($T'1_{\varphi}^{(\xi,\gamma)},...,T'6_{\varphi}^{(\xi,\gamma)}$) из битового потока $\tilde{V}_{B(\varphi)_{скр}}^{(\xi,\gamma)}$ зашифрованной трансформанты ДКП. В результате чего сформированы матрицы такого же размера (16 байт), что и матрица ключей дешифрования K'.

3. Расшифровывание битового представления значений компонент трансформанты $T_{\varphi}^{(\xi,\gamma)}$ ДКП. Это происходит путем наложения матрицы ключей K' длиной в 128-бит на каждую матрицу ($T'1_{\varphi}^{(\xi,\gamma)},...,T'6_{\varphi}^{(\xi,\gamma)}$) битового потока (рис. 3.18).

Процесс расшифровывания матриц $T'1_{\varphi}^{(\xi,\gamma)},...,T'6_{\varphi}^{(\xi,\gamma)}$ битового кода $\tilde{V}_{B(\varphi)скр}^{(\xi,\gamma)}$ компонент зашифрованной трансформанты $T_{\varphi}^{(\xi,\gamma)}$ ДКП представлен в следующих выражениях:

$$T1 = D_{K'}(T'1); T2 = D_{K'}(T'2); T3 = D_{K'}(T'3);$$
$$T4 = D_{K'}(T'4); T5 = D_{K'}(T'5); T6 = D_{K'}(T'6),$$

где $D_{K'}$ – функция расшифровывания матриц $T'1,...,T'6$ матрицей ключей K'.

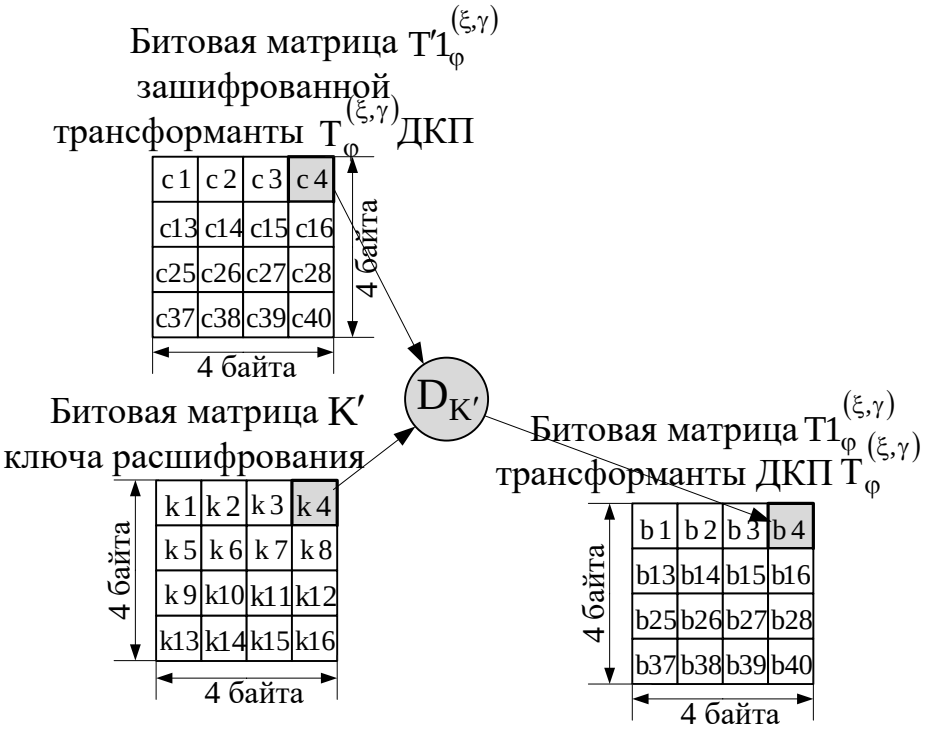
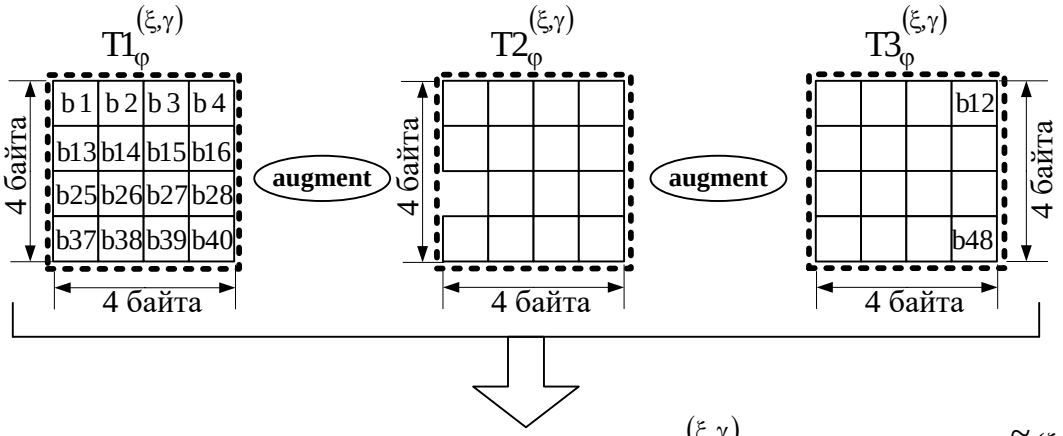


Рис. 3.18. Схема расшифровывания двоичных данных матрицы $T'1_{\varphi}^{(\xi,\gamma)}$ из битового кода $\tilde{V}_{B(\varphi)скр}^{(\xi,\gamma)}$ компонент зашифрованной трансформанты $T_{\varphi}^{(\xi,\gamma)}$ ДКП блока $B_{\varphi}^{(\xi,\gamma)}$ изображения.

Функция шифрования $D_{K'}$ с помощью матрицы расшифровывания $K' = \{k1,...k16\}$ проводит расшифровывание шифрование матриц $T'1,...,T'6$.

Алгоритм шифрования «Калина» выполняет шифрование каждого из 16 элементов матриц T′1,...,T′6 с помощью 16 элементов матрицы ключей K′. Длина каждого элемента в матрице шифрования K′ и матриц T′1,...,T′6 равна 8 битам. В результате чего формируются 6 битовых матриц (T1,...,T6) расшифрованных компонент трансформанты ДКП блока видеокадра.

4. Формирование битовой матрицы $\overline{T}_{\varphi}^{(\xi,\gamma)}$ компонент трансформанты $T_{\varphi}^{(\xi,\gamma)}$ ДКП. Это происходит путем слияния матриц-аргументов элементов битовых матриц T1, T2, T3 слева направо. Процесс слияния матриц-аргументов элементов битовых матриц T1, T2, T3 представлен на рис. 3.19.



Матрица A1 - верхняя половина матрицы $\overline{T}_{\varphi}^{(\xi,\gamma)}$ битового потока $\tilde{V}_{B(\varphi)скр}^{(\xi,\gamma)}$ трансформанты (ξ,γ) -ой структурной единицы

b1	b2	b3	b4	b5	b6	b7	b8	b9	b10	b11	b12
b13	b14	b15	b16	b17	b18	b19	b20	b21	b22	b23	b24
b25	b26	b27	b28	b29	b30	b31	b32	b33	b34	b35	b36
b37	b38	b39	b40	b41	b42	b43	b44	b45	b46	b47	b48

Рис. 3.19. Схема слияния двоичных матриц $T1_{\varphi}^{(\xi,\gamma)}$, $T2_{\varphi}^{(\xi,\gamma)}$ и $T3_{\varphi}^{(\xi,\gamma)}$ из битового кода $\tilde{V}_{B(\varphi)скр}^{(\xi,\gamma)}$ компонент трансформанты $T_{\varphi}^{(\xi,\gamma)}$ ДКП в матрицу A1.

В результате слияния битовых матриц T1, T2, T3 образуется матрица A1, которая состоит из 4 строк длиной в 12 бит. Это представлено следующей функцией:

$$A1 = \text{augment}(T1, T2, T3) =$$

$$= \begin{bmatrix} b1 & b2 & b3 & b4 & b5 & b6 & b7 & b8 & b9 & b10 & b11 & b12 \\ b13 & b14 & b15 & b16 & b17 & b18 & b19 & b20 & b21 & b22 & b23 & b24 \\ b25 & b26 & b27 & b28 & b29 & b30 & b31 & b32 & b33 & b34 & b35 & b36 \\ b37 & b38 & b39 & b40 & b41 & b42 & b43 & b44 & b45 & b46 & b47 & b48 \end{bmatrix},$$

где $\text{augment}(T1, T2, T3)$ – матричная функция, в результате которой происходит слияние матриц-аргументов T1, T2, T3 слева направо.

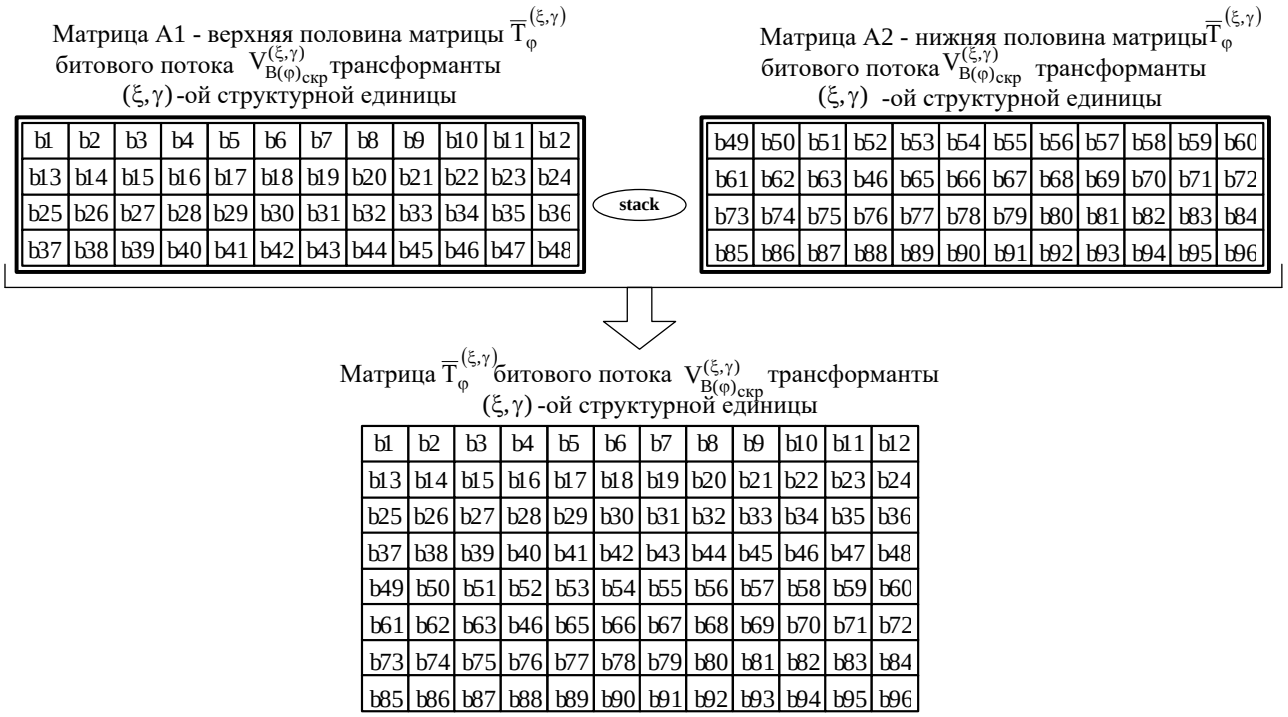
Матрица A1 является верхней половиной матрицы $\overline{\overline{T}}_{\varphi}^{(\xi,\gamma)}$. Нижняя часть матрицы $\overline{\overline{T}}_{\varphi}^{(\xi,\gamma)}$ формируется таким же образом как и матрица A1, из слияния битовых матриц T4, T5, T6 слева направо. Это описано следующим выражением:

$$A2 = \text{augment}(T4, T5, T6) =$$

$$= \begin{bmatrix} b49 & b50 & b51 & b52 & b53 & b54 & b55 & b56 & b57 & b58 & b59 & b60 \\ b61 & b62 & b63 & b46 & b65 & b66 & b67 & b68 & b69 & b70 & b71 & b72 \\ b73 & b74 & b75 & b76 & b77 & b78 & b79 & b80 & b81 & b82 & b83 & b84 \\ b85 & b86 & b87 & b88 & b89 & b90 & b91 & b92 & b93 & b94 & b95 & b96 \end{bmatrix}$$

В результате чего формируется матрица A2, которая состоит из 4 строк длиной в 12 бит. Она является нижней частью битовой матрицы $\overline{\overline{T}}_{\varphi}^{(\xi,\gamma)}$.

Далее выполняется слияние матриц A1 и A2 сверху вниз. В результате чего формируется матрица $\overline{\overline{T}}_{\varphi}^{(\xi,\gamma)}$. Это представлено на рис. 3.20.



b1	b2	b3	b4	b5	b6	b7	b8	b9	b10	b11	b12
b13	b14	b15	b16	b17	b18	b19	b20	b21	b22	b23	b24
b25	b26	b27	b28	b29	b30	b31	b32	b33	b34	b35	b36
b37	b38	b39	b40	b41	b42	b43	b44	b45	b46	b47	b48

b49	b50	b51	b52	b53	b54	b55	b56	b57	b58	b59	b60
b61	b62	b63	b46	b65	b66	b67	b68	b69	b70	b71	b72
b73	b74	b75	b76	b77	b78	b79	b80	b81	b82	b83	b84
b85	b86	b87	b88	b89	b90	b91	b92	b93	b94	b95	b96

b1	b2	b3	b4	b5	b6	b7	b8	b9	b10	b11	b12
b13	b14	b15	b16	b17	b18	b19	b20	b21	b22	b23	b24
b25	b26	b27	b28	b29	b30	b31	b32	b33	b34	b35	b36
b37	b38	b39	b40	b41	b42	b43	b44	b45	b46	b47	b48
b49	b50	b51	b52	b53	b54	b55	b56	b57	b58	b59	b60
b61	b62	b63	b46	b65	b66	b67	b68	b69	b70	b71	b72
b73	b74	b75	b76	b77	b78	b79	b80	b81	b82	b83	b84
b85	b86	b87	b88	b89	b90	b91	b92	b93	b94	b95	b96

Рис. 3.20. Схема слияния двоичных матриц A1 и A2 из битового кода $\tilde{V}_{B(\varphi)_{скр}}^{(\xi,\gamma)}$ в битовую матрицу $\overline{T}_{\varphi}^{(\xi,\gamma)}$ компонент трансформанты $T_{\varphi}^{(\xi,\gamma)}$ ДКП.

Слияние матриц A1 и A2 происходит в результате выполнения следующей функции:

$$\overline{T}_{\varphi}^{(\xi,\gamma)} = \text{stack}(A1, A2) =$$

$$= \begin{bmatrix} b1 & b2 & b3 & b4 & b5 & b6 & b7 & b8 & b9 & b10 & b11 & b12 \\ b13 & b14 & b15 & b16 & b17 & b18 & b19 & b20 & b21 & b22 & b23 & b24 \\ b25 & b26 & b27 & b28 & b29 & b30 & b31 & b32 & b33 & b34 & b35 & b36 \\ b37 & b38 & b39 & b40 & b41 & b42 & b43 & b44 & b45 & b46 & b47 & b48 \\ b49 & b50 & b51 & b52 & b53 & b54 & b55 & b56 & b57 & b58 & b59 & b60 \\ b61 & b62 & b63 & b46 & b65 & b66 & b67 & b68 & b69 & b70 & b71 & b72 \\ b73 & b74 & b75 & b76 & b77 & b78 & b79 & b80 & b81 & b82 & b83 & b84 \\ b85 & b86 & b87 & b88 & b89 & b90 & b91 & b92 & b93 & b94 & b95 & b96 \end{bmatrix},$$

где $\text{stack}(A1, A2)$ – матричная функция, в результате которой происходит слияние матриц-аргументов A1 и A2 сверху вниз.

Таким образом, образуется битовая матрица $\overline{\overline{T}}_{\varphi}^{(\xi,\gamma)}$ компонент трансформанты $T_{\varphi}^{(\xi,\gamma)}$ ДКП из 8 строк. Каждая строка матрицы $\overline{\overline{T}}_{\varphi}^{(\xi,\gamma)}$ состоит из 12 элементов по 8 бит.

5. Преобразование битовой матрицы $\overline{\overline{T}}_{\varphi}^{(\xi,\gamma)}$ в матрицу значений компонент трансформанты $T_{\varphi}^{(\xi,\gamma)}$ ДКП. Это происходит следующим образом:

- Каждая строка битовой матрицы $\overline{\overline{T}}_{\varphi}^{(\xi,\gamma)}$ длиной в 12 байт (96 бит) делится на 8 элементов по 12 бит. Таким образом, формируются битовые представления компонент трансформанты $T_{\varphi}^{(\xi,\gamma)}$ ДКП.

- первые 11 бит двоичного представления значения компоненты трансформанты $T_{\varphi}^{(\xi,\gamma)}$ ДКП переводятся в десятичную систему исчисления, а 12-ый бит определяет знак компоненты.

6. Далее сформированная трансформанта $T_{\varphi}^{(\xi,\gamma)}$ ДКП блока $B_{\varphi}^{(\xi,\gamma)}$ изображения (ξ,γ)-ой структурной единицы базового видеокадра обрабатывается по стандартному методу декодирования.

Выводы

Впервые разработан метод совместимости кодовой конструкции энергетически значимой структурной единицы с требованием метода блочного симметричного шифрования для закрытия потоковых видеоданных на основе технологии внутрикадровой селекции базового видеокадра. Отличительные особенности данного метода от других методов совместимости заключаются в:

- формирование четной длины двоичного кода компонент трансформанты ДКП для блока изображения за счет использования максимального (фиксированного) значения компоненты трансформанты ДКП и ее знака;

- формирование матриц из двоичного кода значимой структурной единицы такого же размера, что и матрица ключа шифрования для их полной совместимости.

В результате применения данного метода интенсивность двоичного кода зашифрованного видеоизображения уменьшается на 25% по сравнению с интенсивностью исходного видеокадра. Это происходит за счет использования формата цветового представления 4:2:0 и формирования матриц из двоичного кода значимой структурной единицы такого же размера, что и матрица ключа шифрования без внесения дополнительной избыточности. За счет шифрования только наиболее значимых структурных единиц, а не всего битового потока базового видеокадра, повышается помехоустойчивость передаваемых видеоданных. В результате применения данного метода повышается качество восстановленных видеоданных.

Впервые разработан метод повышения пропускной способности закрытого видеоканала на основе технологии совмещения кодовой конструкции компрессионного представления видеоданных с технологией гарантированного шифрования. Отличительной особенностью данного метода является то, что закрытию подлежат энергетически значимые структурные единицы базового видеокадра, выявленные на основе двухуровневого сравнения в спектральной области трансформанты ДКП блока яркостной составляющей. Это позволяет повысить пропускную способность закрытого видеоканала в условиях заданного уровня по обеспечению конфиденциальности, достоверности и оперативности.

Получил дальнейшее развитие метод реконструкции закрытого видеопотока на основе технологии дифференцированной обработки кадров. Отличительными характеристиками данного метода являются дифференцированный процесс декодирования базового кадра в зависимости от значимости его структурных составляющих с последующим обратным криптографическим преобразованием информативных структурных единиц. Это позволяет обеспечить требуемый уровень конфиденциальности видеопотока для несанкционированного пользователя и наоборот, обеспечивать достоверное восстановление видеоинформации для авторизированного пользователя.

РАЗДЕЛ 4
ОЦЕНКА ЭФФЕКТИВНОСТИ РАЗРАБОТАННОГО МЕТОДА ПОВЫШЕНИЯ ПРОПУСКНОЙ СПОСОБНОСТИ ЗАКРЫТОГО ВИДЕОКАНАЛА НА ОСНОВЕ ВНУТРИКАДРОВОЙ СЕЛЕКЦИИ БАЗОВЫХ ВИДЕОКАДРОВ

Проведена сравнительная оценка пропускной способности закрытого видеоканала в случае применения существующих методов закрытия видеоданных и в результате применения метода закрытия на основе селекции значимых структурных единиц, который базируется на анализе значений по низкочастотной составляющей блоков яркостной составляющей базового видеокадра.

Представлены результаты экспериментов по скрытию базового кадра и его влиянию на степень закрытия группы видеокадров.

Показано, что созданный метод повышения пропускной способности закрытого видеоканала обладает способностью повышения качества предоставления видеоинформационных сервисов и снижению интенсивности переданного скрытого видеопотока по равнению с существующими методами, за счет того, что закрытию подлежат только значимые фрагменты базового кадра..

4.1. Обоснование выбора показателей, которые определяют значимые структурные единицы для достижения требуемого уровня закрытия оперативной видеоинформации.

Разработан метод селективного закрытия видеоданных, основанный на шифровании наиболее значимых структурных единиц базового видеокадра. Его эфективность зависит от достоверного выявления семантически значимых областей видеодокумента. Выявление таких областей осуществляется на основе

проведения анализа структурных единиц по степени структурной и семантической информативности.

Оценка структурной и семантической информативности структурной единицы базового видеокадра осуществляется по ее спектральным характеристикам. Степень структурной и семантической информативности обрабатываемого блока видеокадра будет меньше если площадь однородной яркостной области видеоизображения будет больше. Степень информативности блока также будет уменьшаться, если площадь, заполненная мелкими деталями, будет меньше. Наоборот, чем чаще встречаются яркостные и контурные перепады, и чем больше площадь, отводимая под мелкие детали, тем выше структурная и семантическая информативность. [115] В связи с чем, для оценки значимости структурных единиц используется информация, содержащаяся в спектральном представлении изображения.

Значимые структурные единицы базового видеокадра определяются по степени семантической и структурной насыщенности входящих в них блоков яркостной составляющей. [37] Для этого осуществляется оценка информации по совокупности низкочастотных значений компонент трансформанты ДКП. [75]

Для оценки информации о семантической и структурной насыщенности блока $B(Y)_{\varphi}^{(\xi,\gamma)}$ яркостной составляющей применяется технология сравнения показателя $Z(B_{н})_{\varphi}^{(\xi,\gamma)}$ по совокупности низкочастотных значений компонент трансформанты ДКП с пороговыми значениями $\delta_{\min_{н}}$ и $\delta_{\max_{н}}$. Пороговое значение $\delta_{\max_{н}}$ – верхний предел для оценки показателя $Z(B_{н})_{\varphi}^{(\xi,\gamma)}$ совокупности значений низкочастотных компонент блока $B(Y)_{\varphi}^{(\xi,\gamma)}$ яркостной составляющей. $\delta_{\min_{н}}$ – нижний предел для оценки показателя $Z(B_{н})_{\varphi}^{(\xi,\gamma)}$ совокупности значений низкочастотных компонент блока $B(Y)_{\varphi}^{(\xi,\gamma)}$ яркостной составляющей.

Расчет показателя $Z(B_н)_{\varphi}^{(\xi,\gamma)}$ по совокупности низкочастотных значений компонент трансформанты ДКП в блоках $B(Y)_{\varphi}^{(\xi,\gamma)}$ яркостной составляющей осуществляется по следующей формуле:

$$Z(B_н)_{\varphi}^{(\xi,\gamma)} = \frac{\log_2 \sum_{\alpha_н=1}^{\lambda_н} \sum_{\upsilon=1}^{\ell(\alpha_н)} y_{\alpha_н,\upsilon}^2}{\sum_{\alpha_н=1}^{\lambda_н} \ell(\alpha_н)},$$

где $Z(B_н)_{\varphi}^{(\xi,\gamma)}$ – показатель, который определяет суммарное значение низкочастотных компонент ДКП блока $B(Y)_{\varphi}^{(\xi,\gamma)}$ яркости;

$y_{\alpha_н,\upsilon}$ – значение компоненты трансформанты;

$\lambda_н$ – количество диагоналей с низкочастотными компонентами в трансформанте;

υ – индекс элемента внутри $\alpha_н$-ой диагонали;

$\alpha_н$ – индекс низкочастотной $\lambda_н$-ой диагонали;

$\ell(\alpha_н)$ – длина низкочастотной $\alpha_н$-ой диагонали.

Принятие решения по определению энергетической значимости структурной единицы и ее дальнейшему закрытию проводится на основе оценки энергетической значимости макроблока $M(Y)^{(\xi,\gamma)}$ яркостной составляющей базового видеокадра K_I. Макроблок $M(Y)^{(\xi,\gamma)}$ яркостной составляющей считается энергетически значимым в двух случаях:

1. Если в состав макроблока $M(Y)^{(\xi,\gamma)}$ яркостной составляющей входит один и больше блоков $B(Y)_{\varphi}^{(\xi,\gamma)}$ с высокой степенью семантической и структурной насыщенности. Это можно описать следующим выражением:

$$M(Y)^{(\xi,\gamma)} = M(Y)_{зн}^{(\xi,\gamma)} \text{ и } M=1, \text{ если } Z(B_н)_{\varphi}^{(\xi,\gamma)} > \delta_{max_н}.$$

2. Если в состав макроблока $M(Y)^{(\xi,\gamma)}$ яркостной составляющей входят два $N_{sr}=2$ и больше $N_{sr}>2$ блоков $B(Y)_{\varphi}^{(\xi,\gamma)}$ со средней степенью семантической и структурной насыщенности, то есть выполняется неравенство:

$$(\delta_{\min_н} \le Z(B_н)_{\varphi}^{(\xi,\gamma)} \le \delta_{\max_н}),$$

тогда:

$$M(Y)^{(\xi,\gamma)} = M(Y)_{зн}^{(\xi,\gamma)} \text{ и } M=1 \text{ если } N_{sr} \ge 2,$$

$$N_{sr} = N_{sr} + 1, \text{ если } (\delta_{\min_н} \le Z(B_н)_{\varphi}^{(\xi,\gamma)} \le \delta_{\max_н})$$

где N_{sr} – количество блоков со средней структурной и семантической насыщенности.

Остальные структурные единицы обрабатываются по стандартному алгоритму видеокомпрессии.

Рассмотрим пример работы метода закрытия базового видеокадра на основе селекции значимых $S_{зн}^{(\xi,\gamma)}$ структурных единиц. Для этого были выбраны два видеокадра (рис. 4.1 – «Селекторное видеосовещание», рис. 4.2 – «Видеодокументирование задержания»).

Рис. 4.1. Исходный видеокадр «Селекторное видеосовещание».

Рис. 4.2. Исходный видеокадр «Видеодокументирование задержания».

В этих видеодокументах ведомственного характера (рис. 4.1, рис. 4.2) экспертом были отмечены участки, в которых необходимо проводить оценку правильности выбора значимых $S_{зн}^{(\xi,\gamma)}$ структурных единиц для шифрования (рис. 4.3, рис. 4.4).

Рис. 4.3. Видеокадр «Селекторное видеосовещание» с экспертной обработкой участков, в которых необходимо проводить оценку правильности выбора значимых $S_{зн}^{(\xi,\gamma)}$ структурных единиц для шифрования.

Рис. 4.4. Видеокадр «Видеодокументирование задержания» с экспертной обработкой участков, в которых необходимо проводить оценку правильности выбора значимых $S_{зн}^{(\xi,\gamma)}$ структурных единиц для шифрования.

В результате закрытия видеокадров с применением метода селекции значимых $S_{зн}^{(\xi,\gamma)}$ структурных единиц на основе анализа значений по низкочастотной составляющей получены результаты, представленные на рис. 4.5, рис. 4.6.

Рис. 4.5. Результат автоматического закрытия видеокадра «Селекторное видеосовещание» с применением метода селекции значимых $S_{зн}^{(\xi,\gamma)}$ структурных единиц на основе анализа значений только по низкочастотной составляющей, где пороговые значения $\delta_{\min_{н}} = 12$, $\delta_{\max_{н}} = 14$.

Рис. 4.6. Результат автоматического закрытия видеокадра «Видеодокументирование задержания» с применением метода селекции значимых $S_{зн}^{(\xi,\gamma)}$ структурных единиц на основе анализа значений по низкочастотной составляющей, где пороговые значения $\delta_{\min_н} = 12$, $\delta_{\max_н} = 14$.

На рис. 4.5, рис. 4.6. представлены результаты автоматического закрытия видеокадров «Селекторное видеосовещание» и «Видеодокументирование задержания» с применением метода селекции значимых $S_{зн}^{(\xi,\gamma)}$ структурных единиц, где пороговые значения $\delta_{\min_н}$ и $\delta_{\max_н}$ для сравнения с показателями $Z(B_н)_{\varphi}^{(\xi,\gamma)}$ по совокупности низкочастотных значений компонент трансформанты ДКП в блоках $B(Y)_{\varphi}^{(\xi,\gamma)}$ яркостной составляющей уставлены таким образом:

$$\delta_{\min_н} = 12,\ \delta_{\max_н} = 14.$$

В таблице 4.1. представлены значения показателя $Z(B_н)_{\varphi}^{(\xi,\gamma)}$ по совокупности низкочастотных значений компонент трансформанты ДКП в

блоках $B(Y)_{\varphi}^{(\xi,\gamma)}$ яркостной составляющей для разных участков изображения в базовом видеокадре. [88]

Таблица 4.1.

Значения показателя $Z(B_н)_{\varphi}^{(\xi,\gamma)}$ по совокупности низкочастотных значений компонент трансформанты ДКП в блоках $B(Y)_{\varphi}^{(\xi,\gamma)}$ яркостной составляющей для разных участков изображения в базовом видеокадре.

Название участка изображения базового видеокадра	Показатель $Z(B_н)_{\varphi}^{(\xi,\gamma)}$ по совокупности низкочастотных значений компонент трансформанты ДКП
camouflage1	13,23
camouflage2	14,238
face1	13,374
face2	13,456
face3	13,4
gerb1	13,69
image1	14,38
table1	13,74
wall1	8,258

Данный метод позволяет закрывать значимые структурные единицы $S_{зн}$ базового видеокадра K_I на основе оценки показателя $Z(B_н)_{\varphi}^{(\xi,\gamma)}$ по совокупности значений низкочастотных компонент блока $B(Y)_{\varphi}^{(\xi,\gamma)}$ яркостной составляющей с пороговыми значениями $\delta_{min_н}$ и $\delta_{max_н}$. [81] В результате работы такого метода происходит закрытие участков изображения базового видеокадра, которые обладают:

1. Выраженными текстурными перепадами. Такими фрагментами изображения могут быть текстурные перепады.

2. Высокой насыщенностью, имеют однородные области, в которых присутствуют контрастные незначимые мелкие детали.

Это подтверждает правильность работы метода закрытия базового видеокадра на основе селекции значимых $S_{зн}^{(\xi,\gamma)}$ структурных единиц.

В результате закрытия видеокадров «Селекторное видеосовещание» (рис. 4.5) и «Видеодокументирование задержания» (рис. 4.6) с применением метода селекции значимых $S_{зн}^{(\xi,\gamma)}$ структурных единиц на основе анализа значений по низкочастотной составляющей достигнуты следующие результаты:

1. Корректно выполняется оценка блоков и макроблоков яркостной составляющей видеокадра по низкочастотным компонентам трансформанты ДКП для выявления участков изображения, которые обладают выраженными структурными переходами, текстурными и яркостными перепадами.

По вышеизложенному можно заключить, что:

1. Разработан метод селекции значимых структурных единиц базового видеокадра на основе анализа значений по низкочастотной составляющей трансформанты ДКП. Данный метод осуществляет автоматический выбор энергетически значимых структурных единиц и обеспечивает их скрытие, которое соответствует требованиям ведомственной организации по обеспечению конфиденциальности.

2. Созданный метод на основе анализа значений по низкочастотной составляющей трансформанты ДКП позволяет автоматически определять области видеодокумента, обладающие выраженными контрастными, структурными и яркостными перепадами. В зависимости от установленных пороговых значений, определяющих уровень семантической сложности, происходит более точное выделение значимых областей видеоизображения. Это позволяет уменьшить площадь закрываемых объектов, которые представляют оперативную важность в ведомственных видеоинформационных системах.

В результате скрытия базовых ведомственных видеокадров «Селекторное видеосовещание» (рис. 4.1) и «Видеодокументирование задержания» (рис. 4.2) с применением метода селекции значимых структурных единиц при установленных пороговых значениях $\delta_{\min_н} = 12$, $\delta_{\max_н} = 14$ по низкочастотной составляющей для определения энергетической насыщенности блока яркостной составляющей были получены следующие практические результаты:

- происходит скрытие важных областей видеодокумента и мелких деталей, представляющих ведомственный оперативный интерес.

- количество значимых структурных единиц составляет от 40% до 80% от всего количества структурных единиц базового видеокадра в зависимости от семантической насыщенности видеоизображения.

Достоверность полученных результатов обеспечивается тем, что автоматический выбор фрагментов, которые представляют ведомственный оперативный интерес, совпадает с результатами, полученными на основе экспертных оценок. [86] Это подтверждает корректность функционирования разработанного метода селективного закрытия видеоданных, основанного на шифровании наиболее значимых структурных единиц базового видеокадра.

Пример обработки характерных видеоизображений «Селекторное видеосовещание» и «Видеодокументирование задержания» с применением метода селекции значимых структурных единиц базового видеокадра показал, что при оценке значений показателей по совокупности низкочастотных компонент трансформанты ДКП блока яркостной составляющей обеспечивается ведомственные требования по конфиденциальности. [63]

4.2. Оценка степени закрытия видеокадра с позиции семантического анализа с учетом ведомственных требований Министерства внутренних дел.

Для систем передачи видеоданных, используемых в Министерстве внутренних дел Украины, необходимо обеспечивать требуемый уровень конфиденциальности.

Если классифицировать изображения по степени оперативной важности, то наиболее значимыми являются фрагменты, которые позволяют:

- идентифицировать объекты;
- осуществить логическую привязку к объектам;
- привязать объекты к местности или времени;
- провести общую оценку оперативной ситуации.

К таким фрагментам изображения относятся:

- лица людей;
- различные изображения в виде надписей, чисел, знаков;
- мелкие детали (шевроны, погоны, автомобильные номера, эмблемы на одежде или автомобилях и т.д.).

Количество структурных единиц, подлежащих шифрованию, зависит от пороговых значений $\delta_{\min_н}$, $\delta_{\max_н}$ по низкочастотной составляющей, определяющих энергетическую значимость структурных единиц. [78]

Определение пороговых значений $\delta_{\min_н}$ и $\delta_{\max_н}$ проводилось на основе визуальной экспертной оценки выбранных фрагментов изображения в базовых видеокадрах (рис. 4.3, рис. 4.4) с полученными значениями показателей $Z(B_н)_\varphi^{(\xi,\gamma)}$ по совокупности низкочастотных значений компонент трансформанты ДКП в блоках $B(Y)_\varphi^{(\xi,\gamma)}$ яркостной составляющей. [87]

Таким образом, значения верхнего и нижнего пределов $\delta_{\max_н}$ и $\delta_{\min_н}$ для оценки показателя $Z(B_н)_\varphi^{(\xi,\gamma)}$ совокупности значений низкочастотных

компонент блока $B(Y)_{\varphi}^{(\xi,\gamma)}$ яркостной составляющей установлены на уровне $\delta_{\max_{н}} = 14$ и $\delta_{\min_{н}} = 12$.

Если пороговые значения установлены $\delta_{\max_{н}} > 14$ и $\delta_{\min_{н}} > 12$, то будут скрываться только максимально семантически насыщенные структурные единицы, наполненные множеством мелких графических элементов и насыщенных резкими структурными переходами. Это представлено на рис. 4.9, рис. 4.10.

Рис. 4.9. Результат автоматического закрытия видеокадра «Селекторное видеосовещание» с применением метода селекции значимых $S_{зн}^{(\xi,\gamma)}$ структурных единиц на основе анализа значений по низкочастотной составляющей, где пороговые значения $\delta_{\min_{н}} > 12$, $\delta_{\max_{н}} > 14$.

Рис. 4.10. Результат автоматического закрытия видеокадра «Видеодокументирование задержания» с применением метода селекции значимых $S_{зн}^{(\xi,\gamma)}$ структурных единиц на основе анализа значений по низкочастотной составляющей, где пороговые значения $\delta_{\min_н} > 12$, $\delta_{\max_н} > 14$.

В процессе скрытия характерных ведомственных видеодокументов «Селекторное видеосовещание» и «Видеодокументирование задержания» на основе разработанного метода селекции значимых структурных единиц с использованием показателей по низкочастотной составляющей показал, что:

1. При установленных пороговых значениях по низкочастотной составляющей на уровне $\delta_{\max_н} > 14$, $\delta_{\min_н} > 12$ выполняется автоматическое выявление от 10% до 25% значимых структурных единиц от общего их количества в зависимости от семантической сложности. В результате чего скрываются не все важные объекты ведомственной видеосъемки, представляющие оперативный интерес. Открытыми остаются важные мелкие элементы, которые создают условия для дальнейшего оперативного анализа объектов и логической привязки к ним. Такими элементами являются: особые приметы людей (шрамы, родинки, увечья), автомобильные номера, текст и эмблемы на одежде или автомобилях (повреждения в результате ДТП,

царапины, сколы, наклейки), элементы местности и т.д. Это позволяет частично идентифицировать объекты видеосъемки и сократить круг их поиска.

2. При установленных пороговых значениях по низкочастотной составляющей на уровне $\delta_{\max_н} < 14$, $\delta_{\min_н} < 12$ выполняется скрытие до 90% базового видеокадра. В результате чего полностью скрываются семантически значимые характерные области видеодокумента, представляющие оперативный интерес: лица объектов, элементы местности, которые позволяют определить местоположение объекта оперативной видеосъемки. С одной стороны это обеспечивает выполнение ведомственных требований по конфиденциальности. Но с другой стороны происходит увеличение интенсивности передаваемых скрытых видеоданных. В результате чего происходит снижение пропускной способности закрытого канала передачи данных в 2-4 раза.

Таким образом, при установке пороговых значений $\delta_{\min_н} = 14$, $\delta_{\max_н} = 12$ по низкочастотной составляющей при функционировании метода закрытия базового видеокадра на основе селекции значимых структурных единиц происходит скрытие до 90% семантически значимых характерных областей видеодокумента, представляющих оперативный интерес. Также выполняется полное скрытие мелких деталей, наличие которых позволяет получить достоверную информацию об объектах оперативной видеосъемки. Это обеспечивает выполнение ведомственных требований по конфиденциальности для закрытого видеоинформационного ресурса. При этом скрытию подлежит от 40% до 80% структурных единиц базового видеокадра в зависимости от семантической сложности.

4.3. Оценка степени закрытия видеоинформационного потока по базовому кадру.

Технология закрытия видеопотока с применением метода селекции значимых структурных единиц на основе анализа значений по низкочастотной составляющей базируется на закрытии только базового кадра. Остальные кадры обрабатываются по стандартному алгоритму кодирования. [69] Поэтому необходимо оценить, как скрытый базовый видеокадр влияет на степень закрытия всей группы видеокадров.

Рассмотрим влияние закрытого базового кадра на степень закрытия группы видеокадров. Для этого взята исходная группа из 8 характерных ведомственных видеокадров. На рис. 4.11 изображена восстановленная группа видеокадров «Движение наряда патрульной полиции на служебном автомобиле» после применения стандартного алгоритма кодирования. На рис. 4.12 изображена восстановленная неавторизованным пользователем без учета обратной селективной обработки группа видеокадров «Движение наряда патрульной полиции на служебном автомобиле» при условии режима обработки когда обеспечивается степень снижения интенсивности для I-кадра $\kappa_I = 1{,}3$, для B-кадров $\kappa_B = 2{,}9$, для P-кадров $\kappa_P = 6{,}8$. На рис. 4.13 изображена восстановленная неавторизованным пользователем без учета обратной селективной обработки группа видеокадров «Движение наряда патрульной полиции на служебном автомобиле» при условии режима обработки когда обеспечивается степень снижения интенсивности для I-кадра $\kappa_I = 2{,}1$, для B-кадров $\kappa_B = 5$, для P-кадров $\kappa_P = 16$. На рис. 4.14 изображена восстановленная неавторизованным пользователем без учета обратной селективной обработки группа видеокадров «Движение наряда патрульной полиции на служебном автомобиле» при условии режима обработки когда обеспечивается степень снижения интенсивности для I-кадра $\kappa_I = 2{,}9$, для B-кадров $\kappa_B = 6{,}8$, для P-кадров $\kappa_P = 28$.

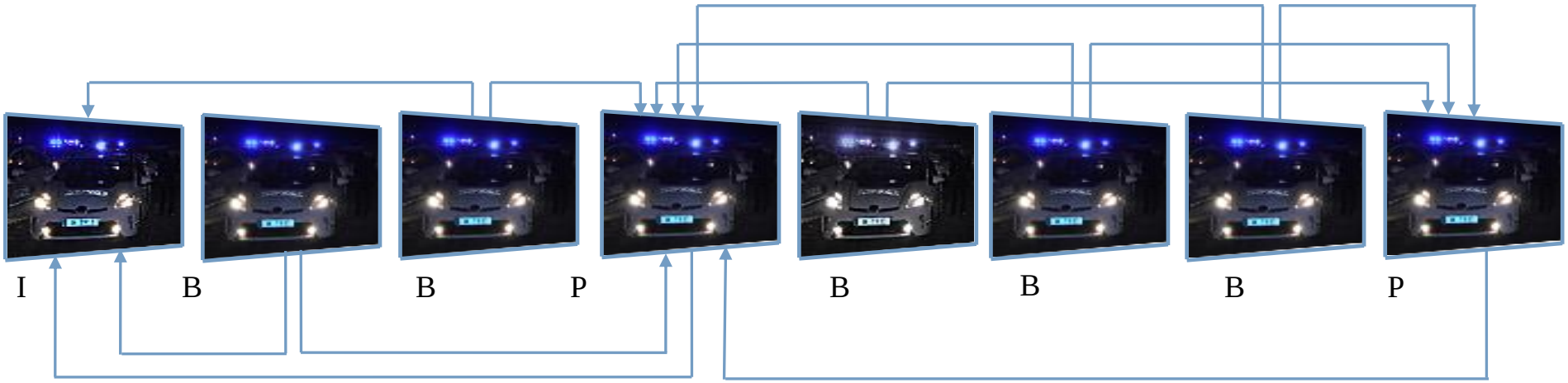


Рис. 4.11. Восстановленная группа из 8 видеокадров «Движение наряда патрульной полиции на служебном автомобиле» после применения стандартного алгоритма компрессии.

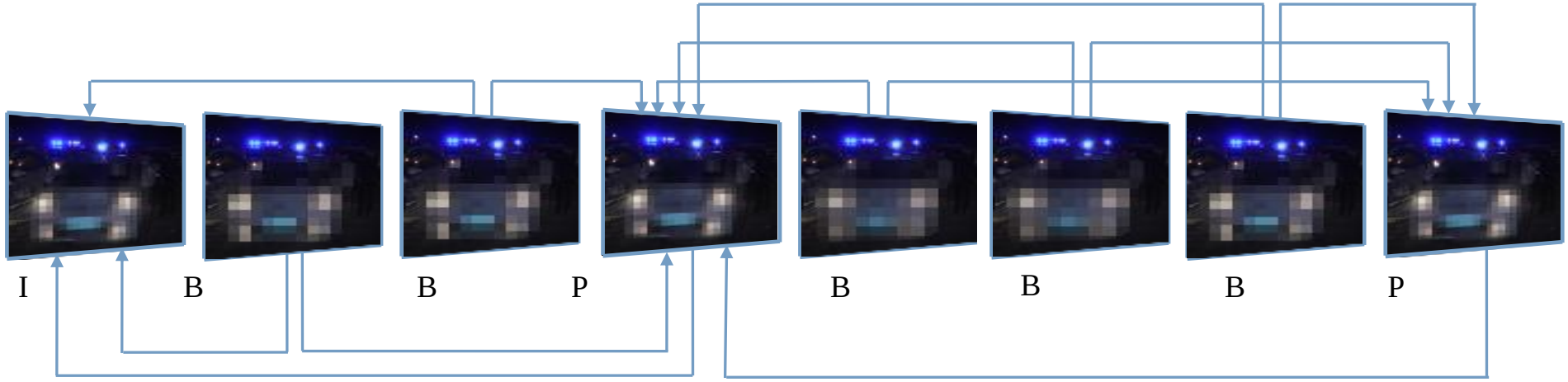


Рис. 4.12. Восстановленная неавторизованным пользователем без учета обратной селективной обработки группа из 8 видеокадров «Движение наряда патрульной полиции на служебном автомобиле» высокого качества.

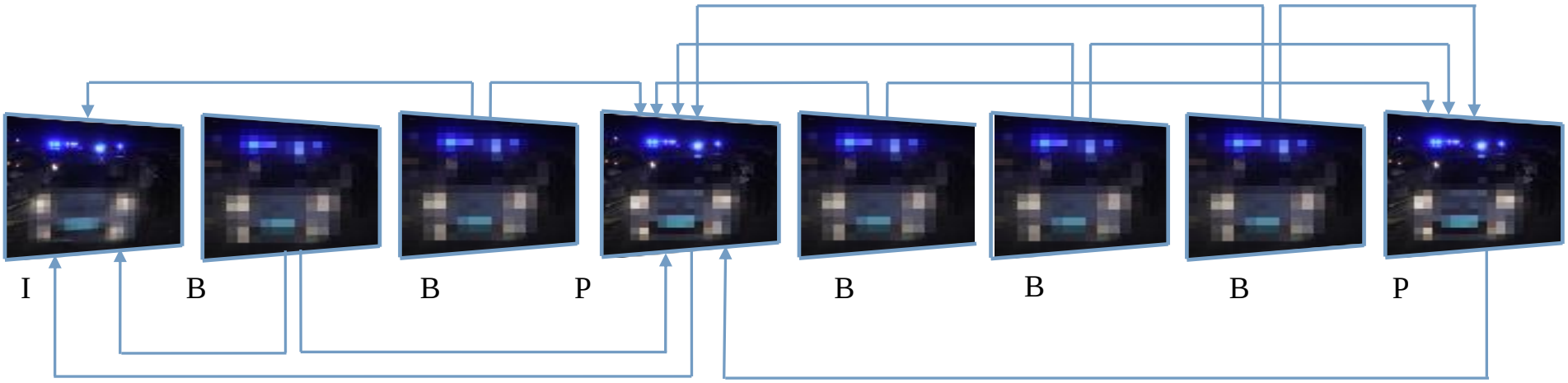


Рис. 4.13. Восстановленная неавторизованным пользователем без учета обратной селективной обработки группа из 8 видеокадров «Движение наряда патрульной полиции на служебном автомобиле» среднего качества.

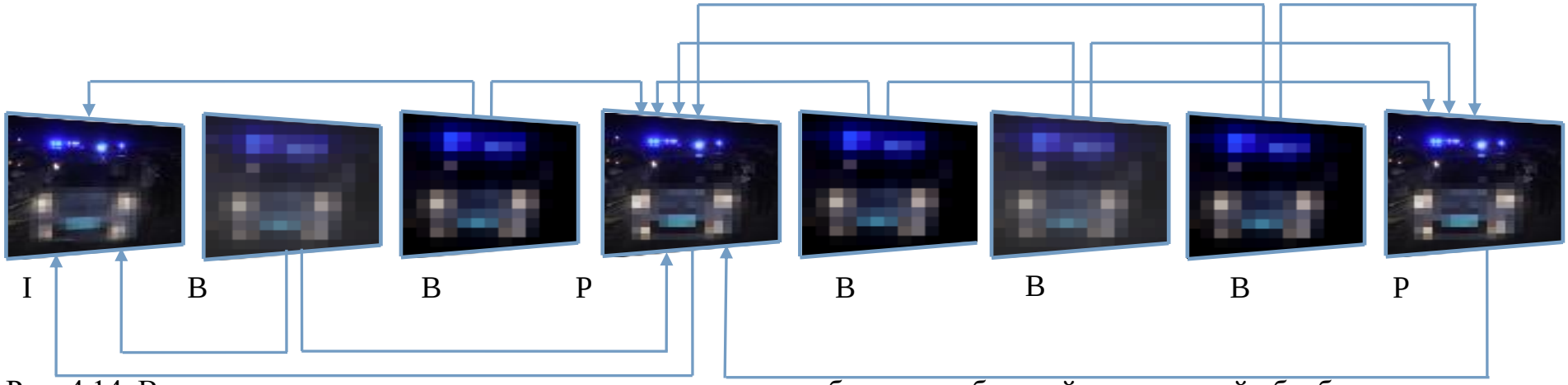


Рис. 4.14. Восстановленная неавторизованным пользователем без учета обратной селективной обработки группа из 8 видеокадров «Движение наряда патрульной полиции на служебном автомобиле» низкого качества.

Анализ восстановленной неавторизованным пользователем без учета обратной селективной обработки группы видеокадров «Движение наряда патрульной полиции на служебном автомобиле» (рис. 4.12, 4.13, 4.14) позволяет заключить, что при слабой компрессии видеоданных выполняется автоматическое выявление до 80% значимых структурных единиц от общего их количества за счет множества контрастных и яркостных перепадов. В результате чего выполняется обеспечение необходимого уровня конфиденциальности для ведомственных видеоинформационных ресурсов. При сильной компрессии видеоданных выполняется автоматическое выявление до 40% значимых структурных единиц от общего их количества. В этом случае уменьшение количества значимых структурных единиц происходит ухудшения качества видеоданных (за счет сглаживания контрастных и яркостных перепадов) в результате применения алгоритмов компрессии. [70] При этом также выполняется обеспечение необходимого уровня конфиденциальности для ведомственных видеоинформационных ресурсов за счет размытия важных областей и полного скрытия мелких деталей, представляющих оперативный интерес.

В результате применения метода закрытия базового видеокадра на основе селекции значимых $S_{зн}^{(\xi,\gamma)}$ структурных единиц происходит частичное скрытие важных областей и полное скрытие мелких деталей всех видеокадрах группы, представляющих оперативный интерес. В данном видеодокументе значимыми областями изображений являются:

– символы на государственном номерном знаке автомобиля;

– марка автомобиля;

– лица людей в автомобиле;

– элементы символики на автомобиле;

– фрагменты фона вокруг автомобиля.

При этом выполняется автоматическое скрытие от 40% до 80% значимых структурных единиц от общего их количества в зависимости от семантической сложности в каждом видеокадре группы, и их отбор осуществляется корректно.

Следовательно, в результате кодирования группы видеокадров при разных коэффициентах снижения интенсивности с применением метода закрытия базового видеокадра на основе селекции значимых $S_{зн}^{(\xi,\gamma)}$ структурных единиц выполняется скрытие семантически значимых характерных областей во всех видеокадрах группы, представляющих оперативный интерес. [64] Это обеспечивает выполнение ведомственных требований по конфиденциальности для закрытого видеоинформационного ресурса.

Следует отметить тот факт, что с увеличением коэффициента снижения интенсивности κ обеспечивается размытие контуров, сглаживание яркостных и контрастных переходов. [113] Поэтому качество видеодокумента ухудшается, соответственно происходит уменьшение количества значимых структурных единиц. Это влияет на интенсивность передаваемых скрытых видеоданных. Поэтому необходимо оценить изменения интенсивности скрытой группы видеокадров при различном качестве видео.

Оценку предлагается проводить с помощью различных значений PSNR пикового отношения сигнал/шум, которые определяют коэффициент снижения интенсивности κ для различных типов видеокадров в группе. [94]

На рис. 4.15 представлена диаграмма зависимости значений интенсивности компрессионного представления I-кадра и значений интенсивности скрытого I-кадра относительно интенсивности группы кадров в процентном соотношении.

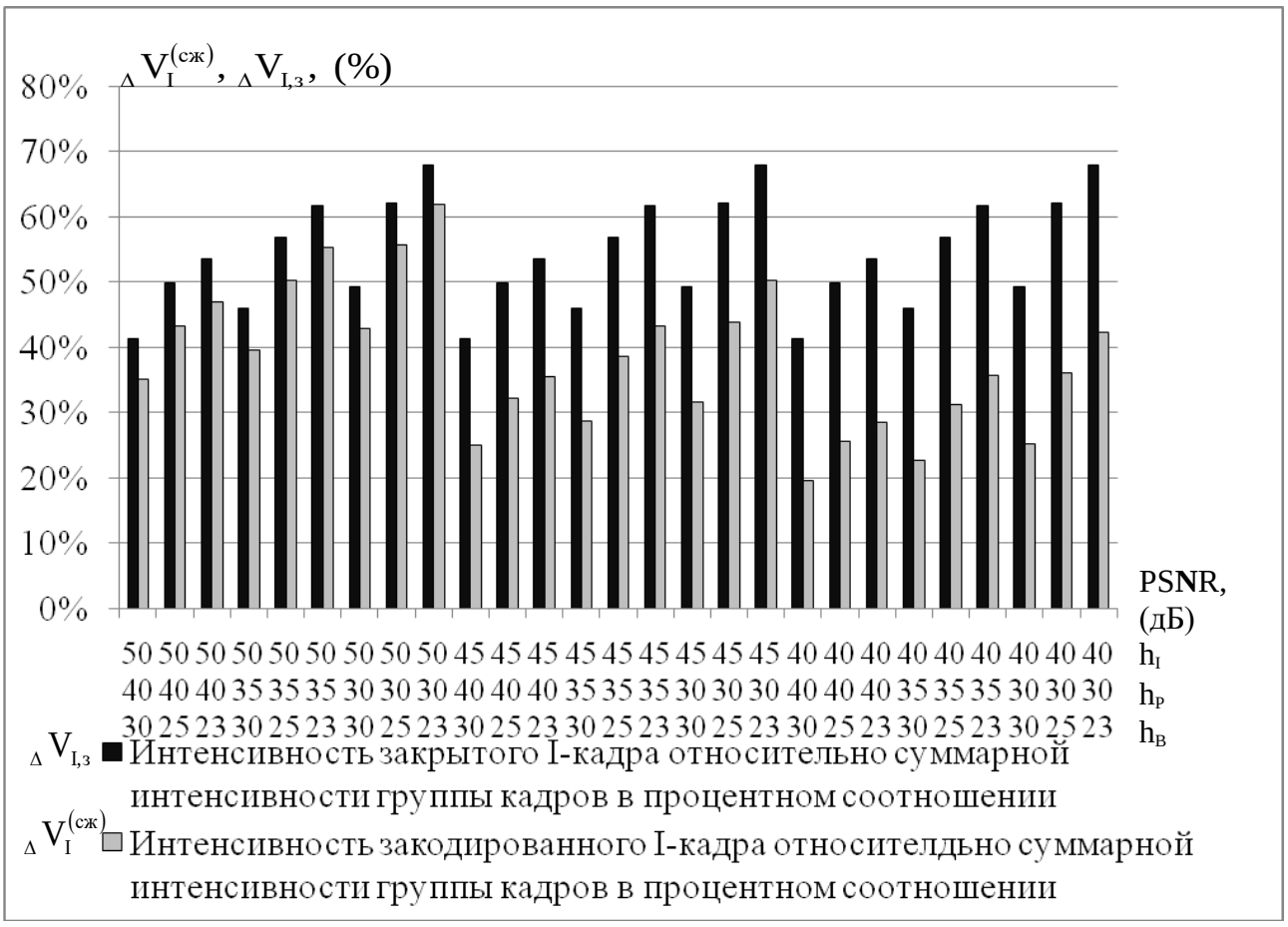


Рис. 4.1.5 Диаграмма значений величин интенсивности $_{\Delta}V_{I,з}$ компрессионного представления I-кадра и интенсивности $_{\Delta}V_{I}^{(сж)}$ скрытого I-кадра в зависимости от пикового отношения сигнал/шум в группе кадров в процентном соотношении.

Из диаграммы (рис. 4.15) видно, что с понижением значений пикового отношения сигнал/шум интенсивность (в процентах) скрытого I-кадра в группе кадров увеличивается. Это связано с тем, что при низких значениях PSNR для P и B-кадров степень компрессии увеличивается, а для скрытого I-кадра – степень компрессии будет постоянной ($\kappa_I = 1$). Расчеты показали, что при высоких значениях PSNR интенсивность закодированного I-кадра составляет 35% от всей интенсивности группы кадров, а интенсивность скрытого I-кадра в группе кадров составил 42%. При низких значениях PSNR интенсивность закодированного I-кадра относительно интенсивности группы кадров равна 43%, а скрытого I-кадра – 68%. Поэтому разработанный метод скрытия

базового видеокадра на основе селекции значимых структурных единиц будет обеспечивать высокую эффективность работы при обработке видео как высокого та и низкого качества. [87]

На рис. 4.16 представлена диаграмма значений величины прироста $D(h_I; h_B; h_P)$ интенсивности $V_{гк,з}^{(сж)}$ группы кадров со скрытым I-кадром по отношению к интенсивности $V_{гк,з}^{(сж)}$ группы кадров без скрытия в процентном соотношении с учетом пикового отношения сигнал/шум для средненасыщенных изображений. Значения величины прироста $D(h_I; h_B; h_P)$ рассчитывается по формуле:

$$D(h_I; h_P; h_B) = \left(1 - \frac{V_{гк,з}^{(сж)}}{V_{гк}^{(сж)}}\right) \cdot 100\% .$$

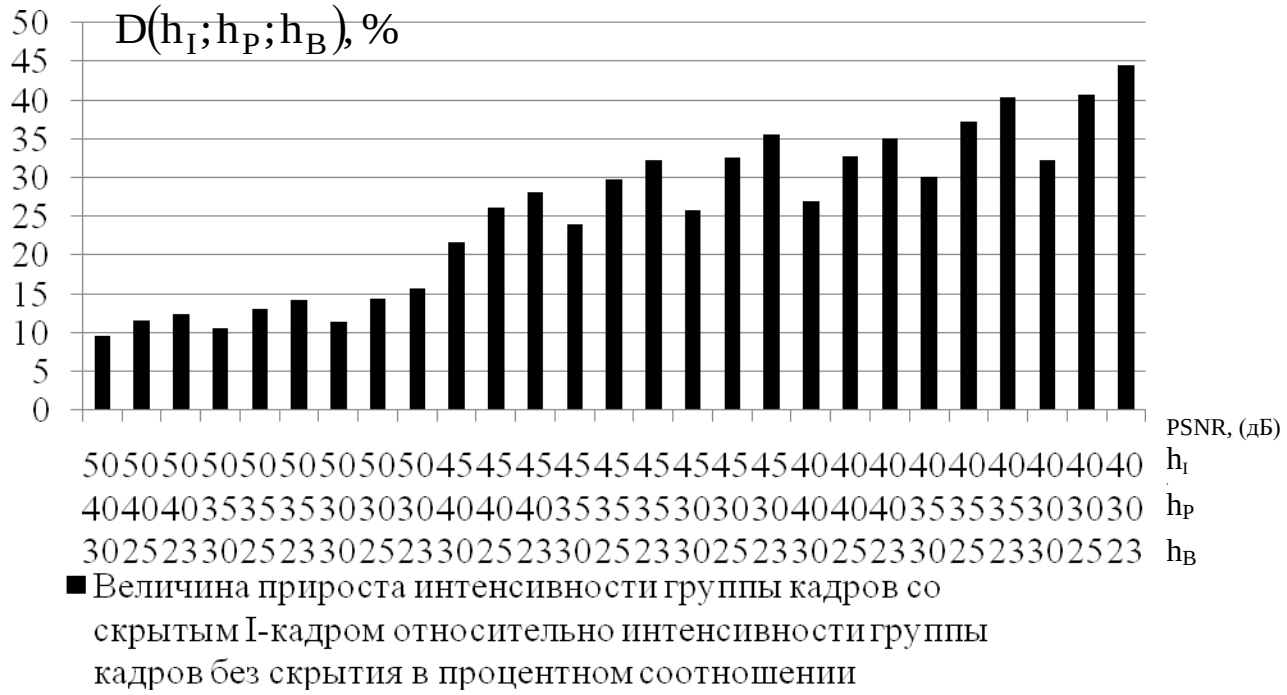


Рис. 4.16. Диаграмма значений величины прироста $D(h_I; h_P; h_B)$ интенсивности $V_{гк,з}^{(скр)}$ группы кадров со скрытым I-кадром по отношению к интенсивности $V_{гк,з}^{(сж)}$ группы кадров без скрытия в процентном соотношении с учетом пикового отношения сигнал/шум для средненасыщенных изображений.

Анализ диаграммы на рис. 4.16 показывает:

- увеличение интенсивности компрессионного представления группы кадров со скрытым I-кадром напрямую зависит от пикового отношения сигнал/шум. При понижении пикового отношения сигнал/шум для I-кадра на 5дБ происходит увеличение процентного соотношения интенсивности компрессионного представления группы кадров со скрытым I-кадром в зависимости от компрессионного представления группы кадров без скрытия I-кадра в среднем на 12%;

- при наибольших пиковых отношениях сигнал/шум для средненасыщенных изображений (высокое качество изображений) величина прироста $D(h_I; h_P; h_B)$ компрессионного представления $V_{гк,з}^{(сж)}$ группы кадров со скрытым I-кадром по отношению к компрессионному представлению $V_{гк,з}^{(сж)}$ группы кадров без скрытия в процентном соотношении составляет около 10%-15%, а при минимальных значениях PSNR величина прироста увеличивается до 40%-44%. Поэтому использование разработанного метода скрытия видеоданных в ведомственных инфокоммуникационных системах на основе селекции значимых структурных единиц базового видеокадра является актуальным для передачи видео высокого качества.

Для определения степени защищенности скрытой группы видеокадров проведем оценку значений пикового отношения сигнал/шум для восстановленных кадров в группе видеокадров авторизированным пользователем относительно восстановленных кадров неавторизированным пользователем при разных коэффициентах снижения интенсивности. [82] Это рассчитывается следующим образом:

$$PSNR(K)_{несанкц} = 20\lg\left(\frac{I_{max}}{\frac{1}{mn}\sum_{i=1}^{m}\sum_{j=1}^{n}(A_{i,j} - A'_{i,j})^2}\right),$$

где $I_{max} = 255$ – максимальное значение 8-битного сигнала;

$PSNR(K)_{несанкц}$ – значений пикового отношения сигнал/шум для К-го кадра группы при несанкционированной попытке его восстановления;

$A_{i,j}$ – $(i; j)$-й исходный элемент видеокадра;

$A'_{i,j}$ – $(i; j)$-й восстановленный элемент видеокадр неавторизированным пользователем.

Ниже представлены диаграммы значений пикового отношения сигнал/шум при несанкционированной попытке восстановления кадров в группе при условии режима обработки:

1) когда обеспечивается степень снижения интенсивности для I-кадра $\kappa_I = 1{,}3$, для B-кадров $\kappa_B = 2{,}9$, для P-кадров $\kappa_P = 6{,}8$ (рис. 4.17) – режим обработки видео высокого качества;

2) когда обеспечивается степень снижения интенсивности для I-кадра $\kappa_I = 2{,}1$, для B-кадров $\kappa_B = 5$, для P-кадров $\kappa_P = 16$ (рис. 4.18) – режим обработки видео среднего качества;

3) когда обеспечивается степень снижения интенсивности для I-кадра $\kappa_I = 2{,}9$, для B-кадров $\kappa_B = 6{,}8$, для P-кадров $\kappa_P = 28$ (рис. 4.19) – режим обработки видео низкого качества.

Из анализа диаграмм на рис. 4.17, 4.18, 4.19 видно, что средние значения пикового отношения сигнал/шум для P-кадров в группе при попытке несанкционированного восстановления находятся в пределах от 7 до 10 дБ при разных режимах обработки. Это связано с тем, что P-кадры несут меньше визуальной нагрузки, чем базовый кадр. При их кодировании применяются алгоритмы компенсации движения и межкадрового предсказания вперед по предшествующим I- или P-кадрам. Средние значения пикового отношения сигнал/шум для B-кадров в группе при попытке несанкционированного восстановления находятся в пределах от 5 до 9 дБ. Средние значения пикового отношения сигнал/шум для B-кадров меньше чем для I- или P-кадров, так как в процессе их формирования применяются алгоритмы компенсации движения и

двунаправленного предсказания по предшествующим и последующим I- или P-кадрам. [114]

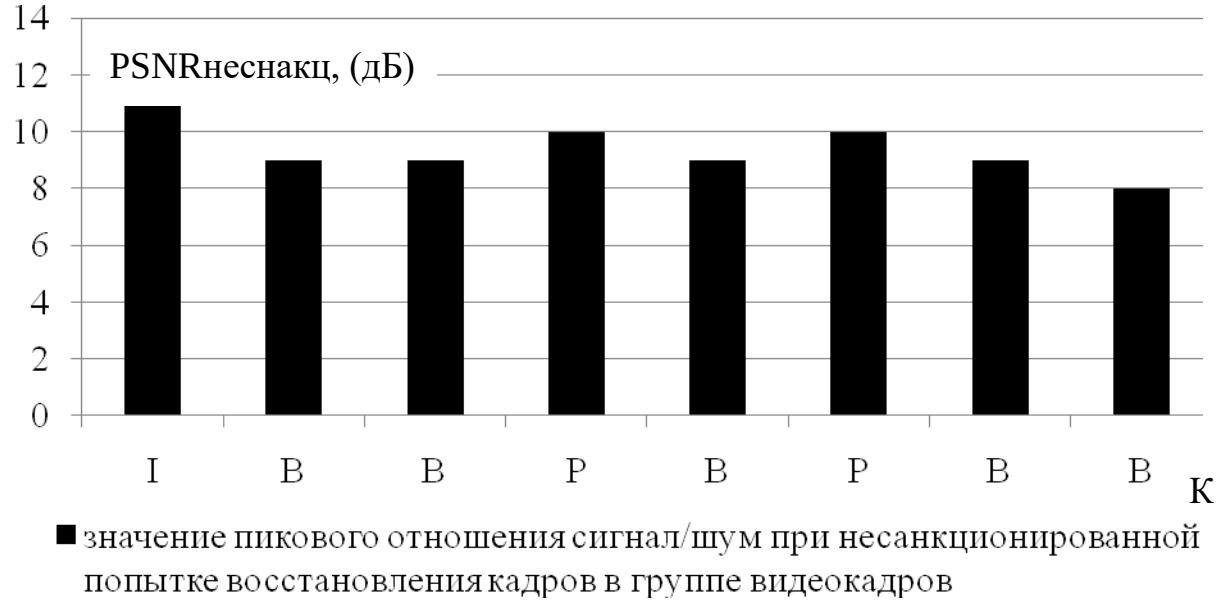


Рис. 4.17. Диаграмма значений пикового отношения сигнал/шум при несанкционированной попытке восстановления кадров в группе при условии режима обработки 1.

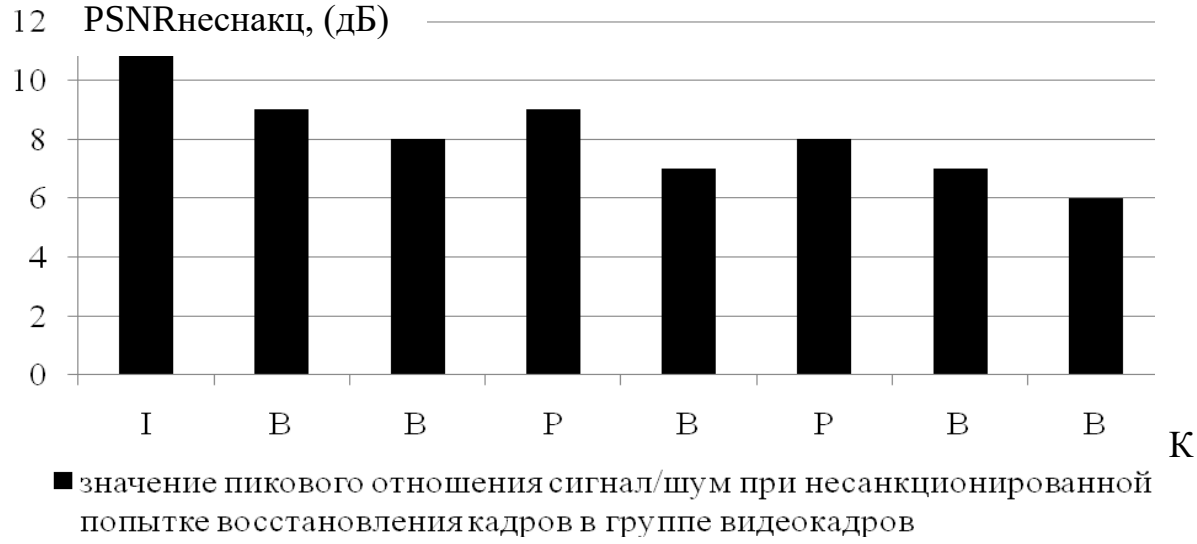


Рис. 4.18. Диаграмма значений пикового отношения сигнал/шум при несанкционированной попытке восстановления кадров в группе при условии режима обработки 2.

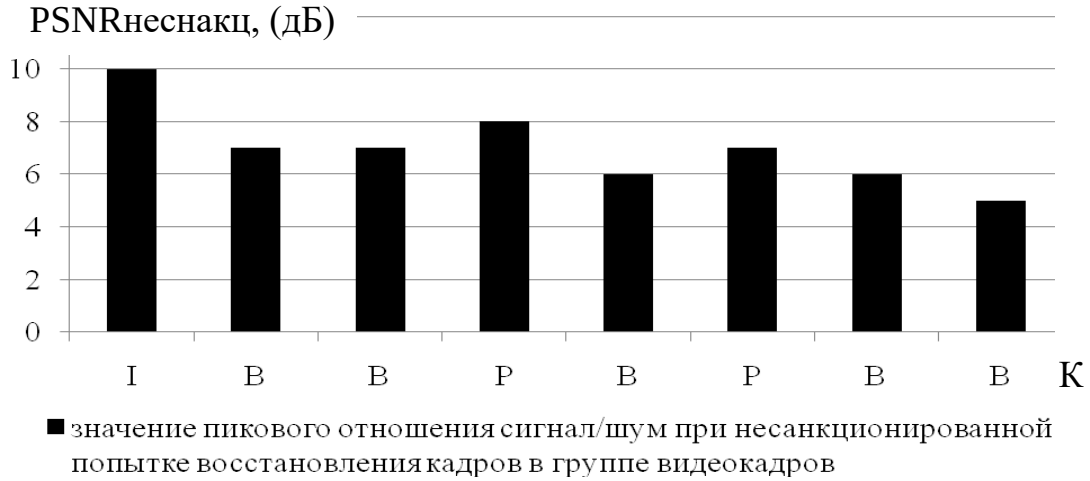


Рис. 4.19. Диаграмма значений пикового отношения сигнал/шум при несанкционированной попытке восстановления кадров в группе при условии режима обработки 3.

Результаты обработки группы из 8 видеокадров «Движение наряда патрульной полиции на служебном автомобиле» (рис. 4.12, 4.13, 4.14) и диаграмм (рис. 4.15, 4.16, 4.17, 4.18, 4.19) с использованием метода селекции значимых структурных единиц показали, что с уменьшением значений пикового отношения сигнал/шум происходит увеличение компрессионного представления группы кадров со скрытым I-кадром по отношению к компрессионному представлению группы кадров без скрытия с 10% до 44%. При закрытии группы видеокадров с использованием метода селекции значимых структурных единиц на основе анализа значений по низкочастотной составляющей базового кадра значения пикового отношения сигнал/шум для P и B-кадров при несанкционированной попытке восстановления не превышают 10 дБ в зависимости от режима обработки, что свидетельствует об их полном разрушении. Это обеспечивает необходимый уровень конфиденциальности для ведомственного видеоинформационного ресурса. Поэтому разработанный метод скрытия видеоданных будет обеспечивать высокую эффективность работы в ведомственных видеоинформационных системах при обработке видео как высокого та и низкого качества.

4.4. Оценка пропускной способности закрытого видеоканала для разработанного метода на основе селекции значимых структурных единиц.

Для определения эффективности технологии закрытия видеоинформационного ресурса с использованием метода селекции значимых $S_{зн}^{(\xi,\gamma)}$ структурных единиц базового видеокадра предлагается сравнить пропускную способность исходного видеопотока с пропускной способностью закрытого видеоканала в случае применения:

1) метода обработки видеоданных на основе стандартизированных технологий MPEG (рис. 4.20);

2) метода закрытия видеоданных на основе последовательной схемы (компрессия с последующим шифрованием) (рис. 4.21);

3) метода скрытия всех видеоданных после дискретного косинусного преобразования блоков базового видеокадра (рис. 4.22);

4) разработанного метода на основе селекции значимых структурных единиц базового видеокадра (рис. 4.23).

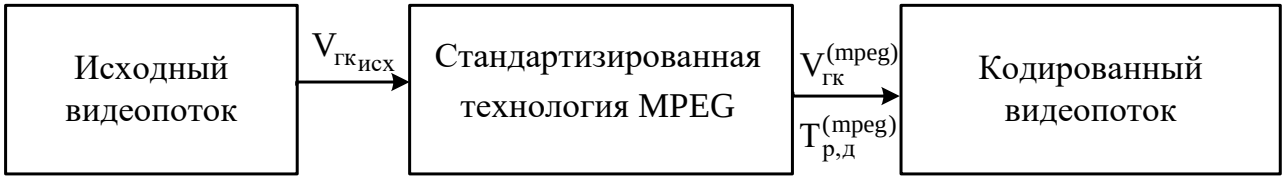


Рис. 4.20. Метод обработки группы видеокадров на основе стандартизированной технологии MPEG.

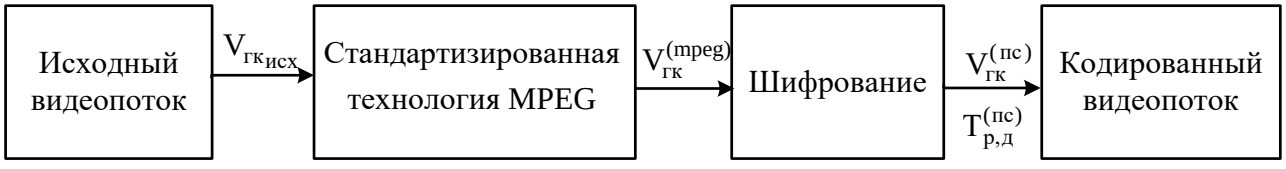


Рис. 4.21. Метода закрытия группы видеокадров на основе последовательной схемы.

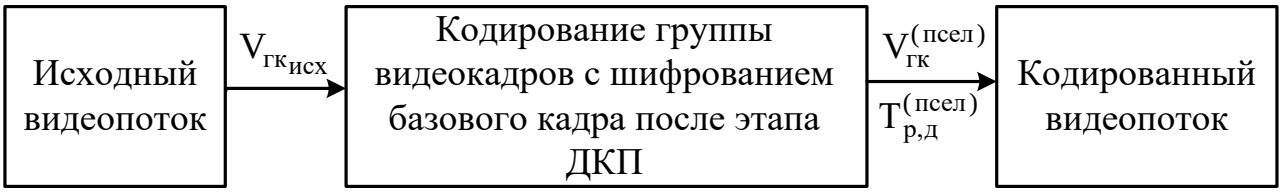


Рис. 4.22. Метод скрытия всех структурных единиц базового видеокадра после ДКП.

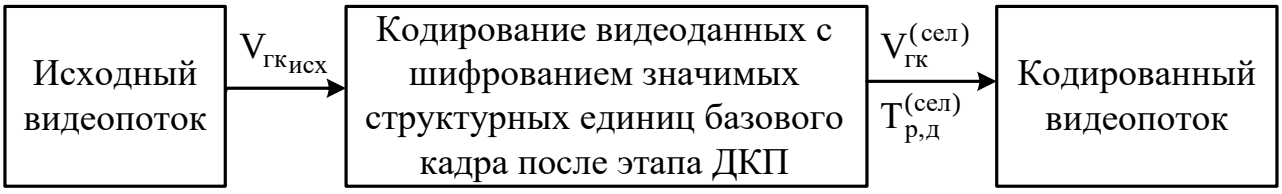


Рис. 4.23. Разработанная технология на основе селекции значимых структурных единиц базового видеокадра.

В таблице 4.2 представлены основные показатели эффективности доставки и закрытия для разных методов обработки видеоданных в ведомственных инфокоммуникационных системах.

Таблица 4.2.

Основные показатели эффективности доставки и закрытия для разных методов обработки видеоданных в ведомственных инфокоммуникационных системах.

Метод обработки видеоданных	Пропускная способность $H_{ок}$ открытого видеоканала, Мбит/с	Пиковое отношение сигнал/шум $PSNR_{с}$ для санкционированного доступа, дБ	Пропускная способность $H_{зк}$ закрытого видеоканала, Мбит/с	Пиковое отношение сигнал/шум $PSNR_{нск}$ для несанкционированного доступа, дБ	Время $T_{обр}$ обработки, с	Время $T_{п}$ передачи, с
Исходный видеопоток (без обработки)	$L_{сети}$	$PSNR_{исх} \to \infty$	0	$PSNR_{исх}$	–	$T_{р,п}^{исх}$
Метод на основе технологии MPEG	$V_{гк_{исх}} = N_K \cdot V_{K_{исх}}$	$PSNR^{(mpeg)}$	0	$PSNR^{(mpeg)}$	$T_{р,обр}^{(mpeg)}$	$T_{р,п}^{(mpeg)}$
Метода скрытия на основе последовательной схемы	–	$PSNR_{с}^{(пс)}$	$V_{гк}^{(пс)}$	$PSNR_{нск}^{(пс)}$	$T_{р,обр}^{(пс)}$	$T_{р,п}^{(пс)}$
Метод скрытия группы видеокадров после ДКП блоков базового кадра	–	$PSNR_{с}^{(псел)}$	$V_{гк}^{(псел)}$	$PSNR_{нск}^{(псел)}$	$T_{р,обр}^{(псел)}$	$T_{р,п}^{(псел)}$
Разработанная технология на основе селекции значимых структурных единиц базового видеокадра	–	$PSNR_{с}^{(сел)}$	$V_{гк}^{(сел)}$	$PSNR_{нск}^{(сел)}$	$T_{р,обр}^{(сел)}$	$T_{р,п}^{(сел)}$

Для ведомственных видеоинформационных ресурсов, используемых в МВД Украины характерны особенности, применяемые для оперативной съемки. К таким особенностям относятся: использование одной видеокамеры без динамических сцен, неизменяемый режим оптического увеличения. Поэтому для оценки разработанного метода скрытия видеоинформационного ресурса и пропускной способности закрытого видеоканала использовались характерные видеоизображения (рис. 4.1 – «Селекторное видеосовещание», рис. 4.2 – «Видеодокументирование задержания», рис. 4.11. – «Движение наряда патрульной полиции на служебном автомобиле»).

Поскольку единицей MPEG-потока является группа видеокадров, то для оценки пропускной способности закрытого видеоканала в ведомственной видеоинформационной системе необходимо определить интенсивность $V_{гк_{код}}$ скрытой группы из 8 видеокадров. [50]

Рассмотрим расчет интенсивности скрытой группы видеокадров для разных методов обработки видеоданных. [83]

Интенсивность $\tilde{V}_{гк}^{(пс)}$ скрытой группы при последовательном шифровании (компрессия с последующим скрытием всего видеопотока) без учета ограничения на время доставки $T_{тр,д}$ определяется следующим выражением:

$$\tilde{V}_{гк}^{(пс)} = \frac{V_I}{\kappa_I} + \frac{N_P \cdot V_P}{\kappa_P} + \frac{N_B \cdot V_B}{\kappa_B},$$

где κ_I – средний коэффициент снижения интенсивности базового видеокадра;

V_I – интенсивность исходного базового видеокадра;

κ_P – средний коэффициент снижения интенсивности для Р-кадров;

V_P – интенсивность исходного Р-кадра; N_P – количество Р-кадров;

κ_B – средний коэффициент снижения интенсивности для B-кадров;

V_B – интенсивность исходного B-кадра;

N_B – количество B-кадров.

Формула для оценки пропускной способности закрытого видеоканала в ведомственной видеоинформационной системе при последовательном шифровании с учетом ограничения на время доставки $T_{тр,д}$ будет иметь следующий вид:

$$V_{гк}^{(пс)} = f(T_{тр,д}, \tilde{V}_{гк}^{(пс)}).$$

Здесь $f(T_{тр,д}, \tilde{V}_{гк}^{(пс)})$ – функционал, позволяющий определить ту часть интенсивности $\tilde{V}_{гк}^{(пс)}$ скрытых кодированных видеоданных при последовательном шифровании, которые удовлетворяют ведомственным требованиям по обработке $T_{р,обр}^{(пс)}$ и передаче $T_{р,п}^{(пс)}$. [50]

Интенсивность $\tilde{V}_{гк}^{(псел)}$ группы, скрытой на основе метода селекции всех структурных единиц без учета ограничения на время доставки $T_{тр,д}$ вычисляется так:

$$\tilde{V}_{гк}^{(псел)} = \sum_{s=1}^{|\Psi_{стр}|} V_I(S_{стр}^{(s)}) + \frac{N_P \cdot V_P}{\kappa_P} + \frac{N_B \cdot V_B}{\kappa_B},$$

где $V_I(S^{(s)})$ – количество бит на представление s-ой структурной единицы базового видеокадра K_I;

$|\Psi_{стр}|$ – количество всех структурных единиц S в базовом видеокадре.

Оценка пропускной способности закрытого видеоканала в ведомственной видеоинформационной системе на основе метода селекции всех структурных единиц после этапа ДКП с учетом ограничения на время доставки $T_{тр,д}$ рассчитывается так:

$$V_{гк}^{(псел)} = f(T_{тр,д}, \tilde{V}_{гк}^{(псел)}).$$

Здесь $f(T_{тр,д}, \tilde{V}_{гк}^{(псел)})$ – функционал, позволяющий определить ту часть интенсивности $\tilde{V}_{гк}^{(псел)}$ скрытых кодированных видеоданных при использовании метода на основе селекции всех структурных единиц, которые удовлетворяют ведомственным требованиям по обработке $T_{р,обр}^{(псел)}$ и передаче $T_{р,п}^{(псел)}$.

Оценка интенсивности $\tilde{V}_{гк}^{(сел)}$ скрытой группы на основе разработанного метода селекции значимых структурных единиц без учета ограничения на время доставки $T_{тр,д}$ происходит следующим образом:

$$\tilde{V}_{гк}^{(сел)} = \sum_{s=1}^{|\Psi_{зн}|} V_I(S_{зн}^{(s)}) + \sum_{s=1}^{|\Psi_{незн}|} V_I(S_{незн}^{(s)}) + \frac{N_Р \cdot V_Р}{\kappa_Р} + \frac{N_В \cdot V_В}{\kappa_В},$$

где $V_I(S_{зн}^{(s)})$ – количество бит на представление значимой s-ой структурной единицы $S_{зн}$ видеокадра K_I;

$|\Psi_{зн}|$ – количество значимых структурных единиц $S_{зн}$ в базовом видеокадре;

$V_I(S_{незн}^{(s)})$ – количество бит на представление s-ой незначимой структурной единицы $S_{незн}$ видеокадра K_I;

$|\Psi_{\text{незн}}|$ – количество незначимых структурных единиц $S_{\text{незн}}$ в базовом видеокадре.

Формула для оценки пропускной способности закрытого видеоканала в ведомственной видеоинформационной системе на основе разработанного метода селекции значимых структурных единиц с учетом ограничения на время доставки $T_{\text{тр,д}}$ имеет следующий вид:

$$V_{\text{гк}}^{(\text{сел})} = f(T_{\text{тр,д}}, \tilde{V}_{\text{гк}}^{(\text{сел})}).$$

Здесь $f(T_{\text{тр,д}}, \tilde{V}_{\text{гк}}^{(\text{сел})})$ – функционал, позволяющий определить ту часть интенсивности $\tilde{V}_{\text{гк}}^{(\text{сел})}$ скрытых кодированных видеоданных для разработанного метода на основе селекции значимых структурных единиц, которые удовлетворяют ведомственным требованиям по обработке $T_{\text{р,обр}}^{(\text{сел})}$ и передаче $T_{\text{р,п}}^{(\text{сел})}$.

Поскольку во всех расчетах используется группа видеокадров как структурная составляющая видеопотока, то необходимо определить требуемое время $T(8)_{\text{тр,д}}$ доставки, приходящееся на группу из 8 видеокадров, которое вычисляется следующим образом:

$$T(8)_{\text{тр,д}} = \frac{8(\text{кадров})}{25(\text{кадров}/\text{с})} = 0{,}32\ \text{с}.$$

В таблице 4.3. представлены основные показатели эффективности доставки и закрытия, полученные в результате экспериментов по скрытию видеоданных в ведомственных инфокоммуникационных системах для разных методов обработки в следующих условиях:

1) ограничения по времени доставки составляют $T_{\text{тр,д}} = T_{\text{обр}} + T_{\text{п}} \le 1\text{с}$;

2) допустимых усредненных значений пикового отношения сигнал/шум по всем типам кадров при санкционированном доступе на уровне $PSNR_c > 21$ дБ;

3) максимальных значений пикового отношения сигнал/шум по всем типам кадров при несанкционированном доступе, не превышающих $PSNR_{нсд} < 10$ дБ;

4) использования видеоформата Full HD (1920×1080);

5) использования пропускной способности единой ведомственной цифровой телекоммуникационной сети $L_{сети} = 20$ Мбит (оптические межобластные каналы связи, предоставляемые компаниями ЧАО «Датагруп» и СП «Инфоком»);

6) использования пропускной способности полевого узла (комплекта спутниковой связи) единой ведомственной цифровой телекоммуникационной сети $L_{сети} = 5$ Мбит (спутникового и оптического каналов связи, предоставляемых компанией ЧАО «Датагруп»);

7) использования оборудования видеоконференцсвязи на базе персонального компьютера Intel Pentium Core2Duo 3 Ггц, ОЗУ – 3 Гб, IP-камера – 2 Мрх.

Таблица 4.3

Основные показатели, полученные в результаты экспериментов по скрытию видеоданных при разных методах обработки в формате Full HD (1920×1080).

Метод обработки видеоданных	Пропускная способность $H_{ок}$ открытого видеоканала, Мбит/с	Пиковое отношение сигнал/шум $PSNR_{с}$ для санкционированного доступа, дБ	Пропускная способность $H_{зк}$ закрытого видеоканала, Мбит/с	Пиковое отношение сигнал/шум $PSNR_{нск}$ для несанкционированного доступа, дБ	Время $T_{обр}$ обработки, %	Время $T_{п}$ передачи, %
Исходный видеопоток (без обработки)	20	$PSNR_{исх} \to \infty$	0	$PSNR_{исх}$	–	100 – 1с
Метод на основе технологии MPEG	398	22 – 30	0	22 – 30	60	40
Метода скрытия на основе последовательной схемы	–	22 – 30	176	до 3	86	14
Метод скрытия группы видеокадров после ДКП блоков базового кадра	–	28	243	до 7	71	29
		32	217			
Разработанная технология на основе селекции значимых структурных единиц базового видеокадра	–	28	407	7-9	63	37
		31	397,5			

Из анализа данных, представленных в таблице 4.3 видно, что:

1. В результате экспериментов по скрытию видеоданных на основе разработанного метода селекции значимых структурных единиц для значений пикового отношения сигнал/шум в 31 дБ пропускная способность закрытого видеоканала достигает 397,5 Мбит/с. Это обеспечивает выполнение ведомственных требований по оперативной доставке скрытых видеоданных для значений пикового отношения сигнал/шум 28-30 дБ при санкционированном доступе. Пропускная способность закрытого видеоканала на основе разработанного метода для значений пикового отношения сигнал/шум в 28 дБ достигает 407 Мбит/с.

2. Для разработанного метода селекции значимых структурных единиц базового видеокадра при выполнении ведомственных требований по оперативности, достоверности и конфиденциальности обеспечивается выигрыш по пропускной способности закрытого видеоканала на 56% по сравнению с пропускной способностью закрытого видеоканала в случае применения последовательного метода, и на 39% по сравнению с пропускной способностью закрытого видеоканала в случае применения метода на основе метода селекции всех структурных единиц базового видеокадра.

3. Результаты сравнения методов закрытия видеоданных показали, что значения пикового отношения сигнал/шум при несанкционированном доступе для разработанного метода селекции значимых структурных единиц базового видеокадра находятся на уровне 7-9 дБ, что обеспечивает выполнение ведомственных требований по конфиденциальности. При этом достигается выигрыш по пропускной способности закрытого видеоканала по сравнению с другими методами скрытия. Другие методы скрытия обеспечивают закрытие видеоданных на уровне 3-7 дБ. При этом они уступают по времени обработки видеоданных на 8-23%.

Рассмотрим зависимость пропускной способности закрытого видеоканала в зависимости от размера $m \times n$ видеокадров. В диаграмме, представленной на рис. 4.24, отображены результаты расчетов зависимости пропускной

способности закрытого видеоканала от методов обработки видеоданных, проводимые в следующих условиях:

1) использования размеров видеокадров:

– низкое разрешение SD – Standard Definition (640×480);

– среднее разрешение HD – High Definition (1024×768);

– высокое разрешение Full HD – High Definition (1920×1080);

2) допустимых усредненных значений пикового отношения сигнал/шум по всем типам кадров при санкционированном доступе на уровне $PSNR_c > 21$ дБ;

3) максимальных значений пикового отношения сигнал/шум по всем типам кадров при несанкционированном доступе, не превышающих $PSNR_{нсд} < 10$ дБ;

4) использования следующих методов обработки видеоданных:

– технология обработки 1 – метод закрытия видеоданных на основе последовательной схемы;

– технология обработки 2 – метод скрытия всех видеоданных после дискретного косинусного преобразования блоков базового видеокадра;

– технология обработки 3 – разработанный метод на основе селекции значимых структурных единиц базового видеокадра.

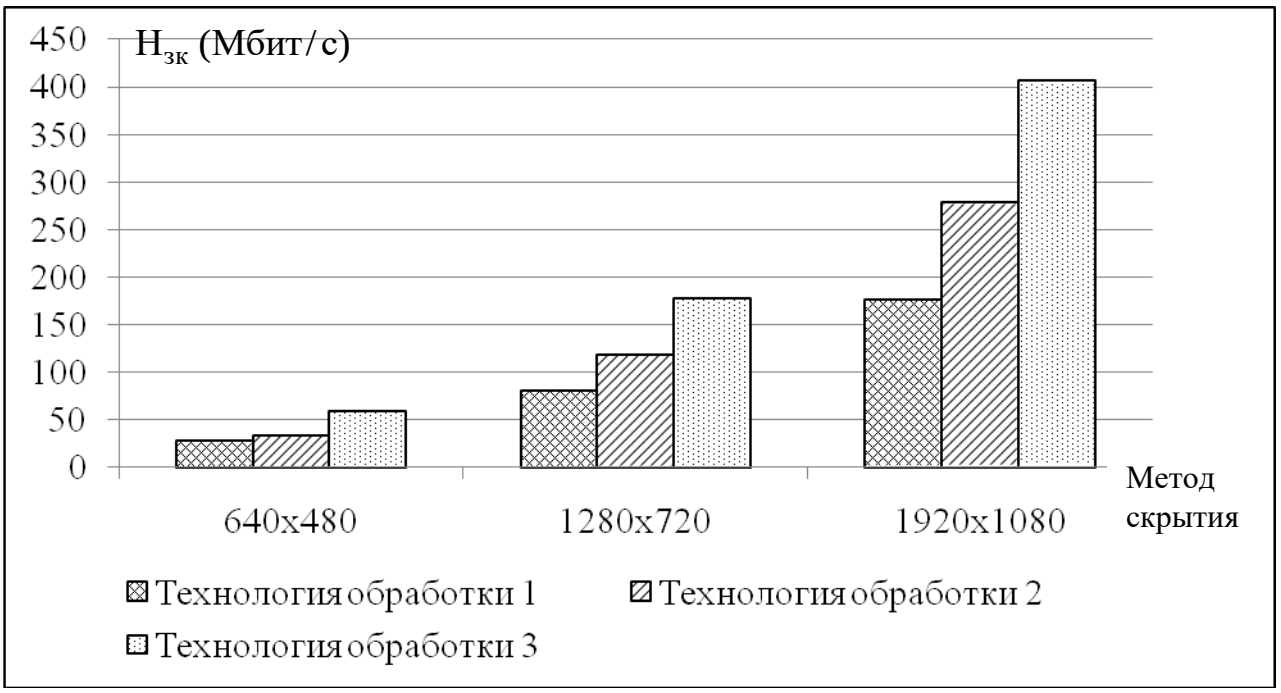


Рис. 4.24. Диаграмма зависимости пропускной способности закрытого видеоканала от размера $m \times n$ видеокадров для разных методов обработки видеоданных при санкционированном доступе.

Из анализа диаграммы на рис. 4.24 видно, что:

1. Для разработанного метода обеспечивается наибольшая пропускная способность закрытого видеоканала в случае использования единой ведомственной цифровой телекоммуникационной сети (пропускная способность сети $L_{сети} = 20$ Мбит) в видеоформате Full HD (1920×1080) и достигает 407 Мбит/с. Это обусловлено тем, что обеспечивается баланс между интенсивностью кодированных видеоданных и пропускной способностью закрытого видеоканала. Баланс обеспечивается за счет того, что выполняется стандартное кодирование P, B-кадров и частично I-кадров, а шифрование значимых фрагментов базового видеокадра выполняется перед этапом квантования. Следовательно, отсутствуют временные затраты на кодирование значимых фрагментов базового видеокадра. А в случае применения других методов скрытия из-за увеличения времени обработки и передачи кодированных видеоданных повышается интенсивность, следовательно, уменьшается пропускная способность закрытого видеоканала.

2. Для разработанного метода на основе селекции значимых структурных единиц базового видеокадра пропускная способность закрытого видеоканала повышается в среднем на 53% по сравнению с пропускной способностью закрытого видеоканала в случае кодирование видеоданных с последующим их шифрованием, и повышается на 40% по сравнению с пропускной способностью закрытого видеоканала в случае применения метода на основе метода селекции всех структурных единиц базового видеокадра.

3. Разработанный метод обеспечивает пропускную способность закрытого видеоканала на уровне 59 Мбит/с (24 кадра/с в пересчете на исходный видеопоток) в условиях использования полевых узлов (спутниковых комплектов связи с пропускной способностью сети $L_{\text{сети}} = 5$ Мбит) для проведения сеансов ведомственной видеоконференцсвязи в видоформате SD (640×480) при выполнении ведомственных требований по оперативности, достоверности $PSNR_{\text{с}} > 21$ дБ и конфиденциальности $PSNR_{\text{нсд}} < 10$ дБ.

Рассмотрим зависимость пропускной способности закрытого видеоканала от значений пикового отношения сигнал/шум для разных методов обработки видеоданных. В диаграмме, представленной на рис. 4.25, отображены результаты расчетов пропускной способности закрытого видеоканала для разных методов обработки видеоданных в зависимости от значений пикового отношения сигнал/шум, которые выбираются в соответствии с типом кадра, проводимые в следующих условиях:

1) использования размера видеокадров 1920×1080;

2) при допустимых усредненных значениях пикового отношения сигнал/шум по всем типам кадров при санкционированном доступе на уровне $PSNR_{\text{с}} > 21$ дБ;

3) при максимальных значениях пикового отношения сигнал/шум по всем типам кадров при несанкционированном доступе, не превышающих $PSNR_{\text{нсд}} < 10$ дБ;

4) использования следующих методов обработки видеоданных:

– технология обработки 1 – метод закрытия видеоданных на основе последовательной схемы;

– технология обработки 2 – метод скрытия всех видеоданных после дискретного косинусного преобразования блоков базового видеокадра;

– технология обработки 3 – разработанный метод на основе селекции значимых структурных единиц базового видеокадра.

5) выделения таких характерных режимов:

– режим 1 – высокое качество видеоданных, для которого значения пикового отношения сигнал/шум для каждого типа кадров соответствуют $\mathrm{PSNR}_{\mathrm{I}} = 50\,\text{дБ}$, $\mathrm{PSNR}_{\mathrm{P}} = 40\,\text{дБ}$, $\mathrm{PSNR}_{\mathrm{B}} = 30\,\text{дБ}$;

– режим 2 – среднее качество видеоданных, для которого значения пикового отношения сигнал/шум для каждого типа кадров соответствуют $\mathrm{PSNR}_{\mathrm{I}} = 45\,\text{дБ}$, $\mathrm{PSNR}_{\mathrm{P}} = 35\,\text{дБ}$, $\mathrm{PSNR}_{\mathrm{B}} = 25\,\text{дБ}$;

– режим 3 – низкое качество видеоданных, для которого значения пикового отношения сигнал/шум для каждого типа кадров соответствуют $\mathrm{PSNR}_{\mathrm{I}} = 40\,\text{дБ}$, $\mathrm{PSNR}_{\mathrm{P}} = 30\,\text{дБ}$, $\mathrm{PSNR}_{\mathrm{B}} = 23\,\text{дБ}$.

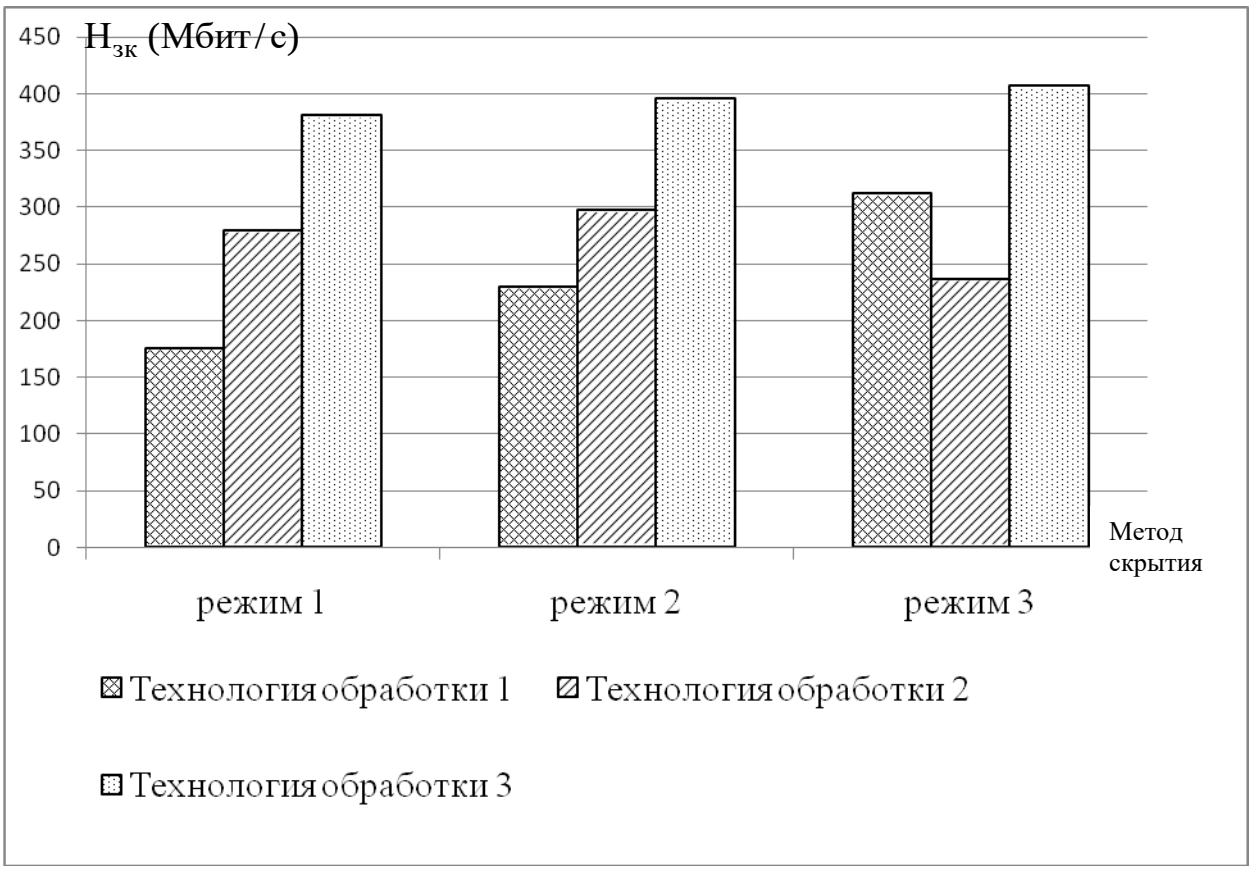


Рис. 4.25. Диаграмма зависимости пропускной способности закрытого видеоканала от значений пикового отношения сигнал/шум для размера видеокадров 1920×1080 для разных методов обработки видеоданных.

Из диаграммы на рис. 4.25 видно, что:

1. Для разработанного метода закрытия видеопотока формата Full HD (1920×1080) в случае, когда обеспечивается нижний уровень пикового отношения сигнал/шум, достигается значение пропускной способности закрытого видеоканала 381 Мбит/с. Здесь обеспечивается выполнение требований по оперативной передаче видеоинформационного ресурса в единой ведомственной цифровой телекоммуникационной сети для низкоскоростных каналов связи.

2. Для разработанного метода закрытия видеопотока формата Full HD (1920×1080) в случае, когда обеспечивается верхний уровень пикового отношения сигнал/шум, пропускная способность закрытого видеоканала составляет 407 Мбит/с (25,6 кадров/с в пересчете на исходный видеопоток) и 397,5 Мбит/с (24,9 кадров/с в пересчете на исходный видеопоток) для видео

допустимого качества. Это позволяет выполнить ведомственные требования по оперативности передачи в условиях повышенной частоты кадров. При этом качество восстановленных видеоданных выше, чем при использовании других методов скрытия. Это происходит за счет того, что в процессе кодирования учитывается обработка значимых структурных единиц базового видеокадра.

3. В случае использования разработанного метода селекции значимых структурных единиц базового видеокадра для видеоформата Full HD (1920×1080) обеспечивается выигрыш по пропускной способности закрытого видеоканала от 23% до 51% по сравнению с методом последовательного шифрования (кодирование видеоданных с последующим их шифрованием) и от 26% до 42% по сравнению с методом селекции всех структурных единиц базового видеокадра в зависимости качества передаваемых видеоданных. Это позволяет повысить качество предоставления видеоинформационных услуг для инфокоммуникационных систем с высокой разрешающей способностью при выполнении ведомственных условий по конфиденциальности, оперативной доставке и достоверности.

Таким образом, в результате обработки характерных ведомственных исходных видеоданных получены следующие практические результаты:

1. Разработан метод оценки пропускной способности закрытого видеоканала на основе определения интенсивности передаваемых скрытых видеоданных в условиях ограничения по степени закрытия, уровню достоверности и времени доставки, которое включает в себя время кодирования, время шифрования и время передачи. Отличительной особенностью данного метода является то, что в процессе оценки эффективности учитывается влияние количества закрываемых значимых структурных единиц на основные показатели передаваемых скрытых видеоданных. Это позволяет оценить пропускную способность закрытого видеоканала в условиях выполнения ведомственных требований по доставке видеоданных, конфиденциальности и достоверности.

2. Для разработанного метода селекции значимых структурных единиц базового видеокадра пропускная способность закрытого видеоканала зависит от

пикового отношения сигнал/шум, и достигает 397 Мбит/с для нижнего уровня пикового отношения сигнал/шум и 407 Мбит/с для высоких значениях пикового отношения сигнал/шум, что составляет 24-25 кадров/с в пересчете на исходный видеопоток. Это обеспечивает выполнение ведомственных требований по оперативной доставке скрытых видеоданных в инфокоммуникационных системах.

3. Для разработанного метода достигается выигрыш по пропускной способности закрытого видеоканала в результате уменьшения значений пикового отношения сигнал/шум для P и B-кадров. Это приводит к уменьшению интенсивности закрытых видеоданных без заметного ухудшения визуального качества доставленного видеоконтента. Визуальное качество сохраняется за счет того, что не применяется обработка, связанная с потерей качества и достоверности при кодировании значимых структурных единиц базового видеокадра. При этом информация о базовом видеокадре определяет качество восстановления P и B-кадров. За счет этого можно регулировать пиковое отношение сигнал/шум для P и B-кадров для увеличение пропускной способности закрытого видеоканала.

4. Для разработанного метода селекции значимых структурных единиц базового видеокадра пропускная способность закрытого видеоканала повышается в среднем на 53% по сравнению с пропускной способностью закрытого видеоканала в случае кодирования видеоданных с последующим их шифрованием, и повышается на 40% по сравнению с пропускной способностью закрытого видеоканала в случае применения метода на основе метода селекции всех структурных единиц базового видеокадра. Это обеспечивает качество предоставления видеоинформационных услуг в режиме закрытия видеопотока.

На основе полученных результатов можно заключить, что по сравнению с существующими методами шифрования видеоданных разработанный метод скрытия на основе селекции значимых структурных единиц базового видеокадра будет обеспечивать выполнение ведомственных требований по конфиденциальности, оперативности и достоверности.

Выводы

В результате экспериментов по обработке характерных ведомственных видеоизображений с применением разработанного метода скрытия видеоданных на основе селекции значимых структурных единиц базового видеокадра получены следующие результаты:

1. Обоснованы показатели структурной насыщенности структурных единиц для достижения требуемого уровня закрытия оперативной видеоинформации и получены следующие практические результаты:

– при установленных пороговых значениях $\delta_{\min_{\text{н}}} = 12$, $\delta_{\max_{\text{н}}} = 14$ энергетической насыщенности блока яркости по низкочастотной составляющей блока яркости происходит скрытие важных областей видеодокумента и мелких деталей, представляющих ведомственный оперативный интерес. При этом количество значимых структурных единиц составляет от 40% до 80% от всего количества структурных единиц базового видеокадра в зависимости от семантической насыщенности видеоизображения. В этом случае достигается соответствие между выявленным автоматически количеством информативно важных областей с тем количеством, которое выявил эксперт в процессе визуальной оценки. Это обеспечивает выполнение ведомственных требований по конфиденциальности и избыточности;

– достоверность полученных результатов обеспечивается тем, что автоматический выбор фрагментов, которые представляют ведомственный оперативный интерес, совпадает с результатами, полученными на основе экспертных оценок. Это подтверждает корректность функционирования разработанного метода селективного закрытия видеоданных, основанного на шифровании наиболее значимых структурных единиц базового видеокадра;

– проведенная экспериментальная оценка характерных видеоизображений «Селекторное видеосовещание» и «Видеодокументирование задержания» с применением метода селекции значимых структурных единиц базового видеокадра показала, что ведомственные требования по конфиденциальности

обеспечивается только при оценке значений показателей по совокупности низкочастотных компонент трансформанты ДКП блока яркостной составляющей.

2. Оценка степени закрытия видеокадра с позиции семантического анализа с учетом ведомственных требований Министерства внутренних дел показала, что при установке пороговых значений $\delta_{\min_{н}} = 14$, $\delta_{\max_{н}} = 12$ уровня энергетической насыщенности блока яркости по низкочастотной составляющей при функционировании метода закрытия базового видеокадра на основе селекции значимых структурных единиц происходит скрытие до 90% семантически значимых характерных областей видеодокумента, представляющих оперативный интерес. При этом выполняется полное скрытие мелких деталей, наличие которых позволяет злоумышленнику получить достоверную информацию об объектах оперативной видеосъемки. Это обеспечивает выполнение ведомственных требований по конфиденциальности для закрытого видеоинформационного ресурса.

3. Оценка степени закрытия видеоинформационного потока по базовому кадру показала, что:

– средние значения пикового отношения сигнал/шум для P-кадров в группе при попытке несанкционированного восстановления находятся в пределах от 7 до 10 дБ при разных режимах обработки. Это связано с тем, что P-кадры несут меньше визуальной нагрузки, чем базовый кадр. При их кодировании применяются алгоритмы компенсации движения и межкадрового предсказания вперед по предшествующим I- или P-кадрам;

– средние значения пикового отношения сигнал/шум для B-кадров в группе при попытке несанкционированного восстановления находятся в пределах от 5 до 9 дБ. Средние значения пикового отношения сигнал/шум для B-кадров меньше чем для I- или P-кадров, так как в процессе их формирования применяются алгоритмы компенсации движения и двунаправленного предсказания по предшествующим и последующим I- или P-кадрам;

– с уменьшением значений пикового отношения сигнал/шум происходит увеличение интенсивности группы кадров со скрытым I-кадром по отношению к интенсивности группы кадров без скрытия с 10% до 44%. При закрытии группы видеокадров с использованием метода селекции значимых структурных единиц на основе анализа значений по низкочастотной составляющей базового кадра значения пикового отношения сигнал/шум для P и B-кадров при несанкционированной попытке восстановления не превышают 10 дБ в зависимости от режима обработки, что свидетельствует об их полном разрушении. Это обеспечивает необходимый уровень конфиденциальности для ведомственного видеоинформационного ресурса.

4. Разработан метод оценки пропускной способности закрытого видеоканала. Он позволяет проводить оценку эффективности метода скрытия, коррекцию интенсивности скрытого видеопотока с учетом ведомственных требований по оперативности, достоверности и конфиденциальности. Данный метод оценки пропускной способности закрытого видеоканала разработан на основе определения интенсивности передаваемых скрытых видеоданных в условиях ограничения по степени закрытия, уровню достоверности и времени доставки, которое включает в себя время кодирования, время шифрования и время передачи. Отличительной особенностью данного метода является то, что в процессе оценки эффективности учитывается влияние количества закрываемых значимых структурных единиц на основные показатели передаваемых скрытых видеоданных. Это позволяет оценить пропускную способность закрытого видеоканала в условиях выполнения ведомственных требований по доставке видеоданных, конфиденциальности и достоверности.

На основе метода оценки пропускной способности закрытого видеоканала получены следующие практические результаты:

– для разработанного метода обеспечивается наибольшая пропускная способность закрытого видеоканала в случае использования единой ведомственной цифровой телекоммуникационной сети (пропускная способность сети $L_{\text{сети}} = 20$ Мбит) в видеоформате Full HD (1920×1080) и

достигает 407 Мбит/с. Это обусловлено тем, что обеспечивается баланс между интенсивностью кодированных видеоданных и пропускной способностью закрытого видеоканала. Баланс обеспечивается за счет того, что выполняется стандартное кодирование P, B-кадров и частично I-кадров, а шифрование значимых фрагментов базового видеокадра выполняется перед этапом квантования. Следовательно, отсутствуют временные затраты на кодирование значимых фрагментов базового видеокадра. А в случае применения других методов скрытия из-за увеличения времени обработки и передачи кодированных видеоданных повышается интенсивность, следовательно, уменьшается пропускная способность закрытого видеоканала;

– для разработанного метода на основе селекции значимых структурных единиц базового видеокадра пропускная способность закрытого видеоканала повышается в среднем на 53% по сравнению с пропускной способностью закрытого видеоканала в случае кодирование видеоданных с последующим их шифрованием, и повышается на 40% по сравнению с пропускной способностью закрытого видеоканала в случае применения метода на основе метода селекции всех структурных единиц базового видеокадра.

– разработанный метод обеспечивает пропускную способность закрытого видеоканала на уровне 59 Мбит/с (24 кадра/с в пересчете на исходный видеопоток) в условиях использования полевых узлов (спутниковых комплектов связи с пропускной способностью сети $L_{\text{сети}} = 5$ Мбит) для проведения сеансов ведомственной видеоконференцсвязи в видоформате SD (640×480) при выполнении ведомственных требований по оперативности, достоверности $PSNR_{\text{с}} > 21$ дБ и конфиденциальности $PSNR_{\text{нсд}} < 10$ дБ.

– для разработанного метода закрытия видеопотока формата Full HD (1920×1080) в случае, когда обеспечивается нижний уровень пикового отношения сигнал/шум, достигается значение пропускной способности закрытого видеоканала 381 Мбит/с. Здесь обеспечивается выполнение требований по оперативной передаче видеоинформационного ресурса в единой

ведомственной цифровой телекоммуникационной сети для низкоскоростных каналов связи.

– для разработанного метода закрытия видеопотока формата Full HD (1920×1080) в случае, когда обеспечивается верхний уровень пикового отношения сигнал/шум, пропускная способность закрытого видеоканала составляет 407 Мбит/с (25,6 кадров/с в пересчете на исходный видеопоток) и 397,5 Мбит/с (24,9 кадров/с в пересчете на исходный видеопоток) для видео допустимого качества. Это позволяет выполнить ведомственные требования по оперативности передачи в условиях повышенной частоты кадров. При этом качество восстановленных видеоданных выше, чем при использовании других методов скрытия. Это происходит за счет того, что в процессе кодирования учитывается обработка значимых структурных единиц базового видеокадра.

– в случае использования разработанного метода селекции значимых структурных единиц базового видеокадра для видеоформата Full HD (1920×1080) обеспечивается выигрыш по пропускной способности закрытого видеоканала от 23% до 51% по сравнению с методом последовательного шифрования (кодирование видеоданных с последующим их шифрованием) и от 26% до 42% по сравнению с методом селекции всех структурных единиц базового видеокадра в зависимости качества передаваемых видеоданных. Это позволяет повысить качество предоставления видеоинформационных услуг для инфокоммуникационных систем с высокой разрешающей способностью при выполнении ведомственных условий по конфиденциальности, оперативной доставке и достоверности.

ЗАКЛЮЧНИЕ

В диссертационной работе решена актуальная научно-прикладная задача повышения качества видеоинформационного сервиса для ведомственных инфокоммуникационных сетей в условиях обеспечения заданной конфиденциальности.

Развитие инфокоммуникационных технологий, и, в частности, ведомственных систем видеоконференцсвязи в МВД Украины, которые определяются постоянным возрастанием объемов передаваемых данных и потребностью в создании новых сервисов, приводит к необходимости создания новых и модернизации существующих ведомственных телекоммуникационных систем. При этом разработаны ведомственные требования по обеспечению оперативности, достоверности и конфиденциальности для таких систем видеоконференцсвязи. Выполнение этих требований с помощью импортного оборудования, которое обеспечивает необходимый уровень конфиденциальности при проведении сеансов видеоконференцсвязи, и использование на разных участках трансляции видеоданных низкоскоростных каналов связи приводит к существенному увеличению времени обработки и передачи закрытых видеоданных.

Проведенный анализ использующихся в МВД Украины каналов связи и различных методов обеспечения конфиденциальности показал, что они не обеспечивают выполнение ведомственных требований по достоверности и оперативной доставке скрытых видеоинформационных потоков.

Поэтому для обеспечения качества видеоинформационных сервисов в системе органов внутренних дел Украины требуется разработать метод повышения пропускной способности закрытого видеоканала для ведомственных телекоммуникационных систем.

В процессе проведения исследований получены следующие **основные научные результаты**:

1. Создан метод выявления значимых фрагментов видеокадра на основе анализа информации в трансформантах двумерного дискретного косинусного преобразования. Метод базируется на: определении энергетической значимости для структурных единиц базового кадра, состоящих из макроблоков полноцветовой модели; решающем правиле относительно установления значимости макроблоков яркостной составляющей. Здесь количество автоматически выявляемых значимых структурных единиц достигает 90% от суммарного их количества в базовых кадрах в зависимости от семантической насыщенности.

2. Построен метод оценки информационной интенсивности закрытого видеопотока. Данный метод базируется на следующих механизмах в процессе оцени интенсивности, а именно на том, что: криптографической защите всего видеопотока подлежат только значимые структурные единицы базового кадра, отсюда прирост по интенсивности не превышает 7 %; учитывается ключевое влияние структурных единиц базового кадра на процесс формирования предсказываемых кадров видеопотока. Здесь средние значения пикового отношения сигнал/шум для предсказываемых кадров в группе в случае несанкционированного доступа находятся в пределах от 5 до 9 дБ, что соответствует полному семантическому разрушению их содержания.

3. Разработан метод повышения пропускной способности закрытого видеоканала. Созданный метод строится на таких базовых составляющих: автоматической селекции значимых фрагментов видеопотока на основе каскадных решающих правил с использованием интегрированных оценок значимости макроблоков структурных единиц базовых кадров в трансформированном представлении; согласовании особенностей формирования кодовых конструкций соответственно для значимых структурных единиц кадра и блочного симметричного шифрования без внесения дополнительной избыточности. Это обеспечивает пропускную

способность закрытого видеоканала на уровне 59 Мбит/с (25 кадра/с в пересчете на исходный видеопоток) в условиях использования полевых узлов (спутниковых комплектов связи с пропускной способностью сети $L_{сети} = 5$ Мбит) для проведения сеансов ведомственной видеоконференцсвязи в видеоформате SD (640×480) при выполнении ведомственных требований по оперативности, достоверности $PSNR_c > 21$ дБ и конфиденциальности $PSNR_{нсд} < 10$ дБ.

4. Создан метод реконструкции закрытого видеоинформационного потока на основе селективной обработки и закрытия ключевых фрагментов, представляющих ведомственный интерес. Данный метод базируется на следующих особенностях: проводится идентификация закрытых структурных единиц базового кадра в общем кодовом потоке на основе использования установленных меток и взаимной согласованности требований относительно формирования кодовых конструкций; дифференцированной обработки структурных единиц в процессе восстановления базовых кадров с учетом наличия механизма криптографического шифрования значимых фрагментов.

Основные практические результаты:

1. Для разработанного метода достигается скрытие до 90% семантически значимых областей видеодокументов, представляющих оперативный интерес, что обеспечивает выполнение ведомственных требований по конфиденциальности видеоинформационного потока. При этом скрытию подлежит от 40% до 80% структурных единиц базового видеокадра в зависимости от его семантической сложности.

2. Для разработанного метода закрытия видеопотока формата Full HD (1920×1080) в случае, когда обеспечивается нижний уровень пикового отношения сигнал/шум, достигается значение пропускной способности закрытого видеоканала 381 Мбит/с. Здесь обеспечивается выполнение требований по оперативной передаче видеоинформационного ресурса в единой

ведомственной цифровой телекоммуникационной сети для низкоскоростных каналов связи.

3. Для разработанного метода закрытия видеопотока формата Full HD (1920×1080) в случае, когда обеспечивается верхний уровень пикового отношения сигнал/шум, пропускная способность закрытого видеоканала составляет 407 Мбит/с (25,6 кадров/с в пересчете на исходный видеопоток) и 397,5 Мбит/с (24,9 кадров/с в пересчете на исходный видеопоток) для видео допустимого качества. Это позволяет выполнить ведомственные требования по оперативности передачи в условиях повышенной частоты кадров. При этом качество восстановленных видеоданных выше, чем при использовании других методов скрытия.

4. Для разработанного метода на основе селекции значимых структурных единиц базового видеокадра пропускная способность закрытого видеоканала повышается в среднем на 53%, по сравнению с пропускной способностью закрытого видеоканала в случае использования известных методов кодирования видеоданных с последующим их шифрованием, и повышается на 40%, по сравнению с пропускной способностью закрытого видеоканала в случае применения существующих методов на основе селекции всех структурных единиц базового видеокадра.

Достоверность полученных результатов подтверждается адекватностью результатов относительно повышения пропускной способности закрытого видеоканала и обеспечения требуемого уровня конфиденциальности и достоверности ведомственной видеоинформации, полученных, соответственно, в процессе экспериментальной эксплуатации ведомственных технологий видеоинформационного обеспечения теоретическим данным на основе моделирования; экспертными оценками относительно анализа видеодокументов на предмет наличия незакрытой информации, представляющей ведомственный интерес и возможности ее несанкционированного изъятия.

Результаты диссертационной работы целесообразно использовать:

– при разработке систем обеспечения конфиденциальности и повышения пропускной способности закрытого видеоканала для ведомственных инфокоммуникационных сетей;

– при проведении научно-исследовательских работ по созданию новых технических средств и программных изделий по обработке видеоинформации;

– при изучении учебных дисциплин по кодированию и обработке видеотрафика для подготовки специалистов в ВУЗах Украины.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Айфичер Э. Цифровая обработка сигналов: практический подход, 2-е издание: Пер. с англ. / Э. Айфичер, Б. Джервис. – М.: Издательский дом "Вильямс", 2004. – 992 с.

2. Анисимов Б.В. Распознавание и цифровая обработка изображений: учебное пособие для студентов вузов / Б.В. Анисимов, В.Д. Курганов, В.К. Злобин. – М. : Высшая школа, 1983. – 295 с.

3. Ансон Л., Барнсли М. Фрактальное сжатие изображений // Мир ПК. – 1992. – №4. – С. 23-27.

4. Аудиовизуальные системы связи и вещания: новые технологии третьего тысячелетия, задачи и проблемы внедрения в Украине / [О.В. Гофайзен, А.И. Ляхов, Н.К. Михалов и др.] // Праці УНДІРТ. – 2000. – № 3. – С. 3-40.

5. Ахмед Н. Ортогональные преобразования при обработке цифровых сигналов / Н. Ахмед, К.Р. Рао; пер. с англ. под ред. И.Б. Фоменко. – М. : Связь, 1980. – 248 с.

6. Баранник В.В. Кодирование трансформированных изображений в инфокоммуникационных системах / В.В. Баранник, В.П. Поляков – Х.: ХУПС, 2010. – 234 с.

7. Баранник В.В. Кодирование трехмерных моделей видеокадров в инфотелекоммуникационных системах / В.В. Баранник, В.П. Поляков, А.В. Слободянюк // Каменец-Подольский-Харьков: Вид-во Каліграф, 2011. – 210 с.

8. Баранник В.В. Метод защиты видеоинформации в энергоэффективных телекоммуникационных системах / В.В. Баранник, Д.И. Комолов, Р.В. Тарнополов // Открытые компьютерные информационные интегрированные технологии. – 2015. - №70. – С. 131-141.

9. Баранник В.В. Метод селективной обработки базового кадра для повышения пропускной способности закрытого видеоканала в ведомственных системах / В.В. Баранник, Д.И. Комолов // Системи обробки інформації. – 2016. - №5(142). – С. 105 – 114.

10. Баранник В.В. Метод суміщення кодової конструкції енергетично значимої структурної одиниці з вимогою методу блокового симетричного

шифрування для закриття потокових відеоданих на основі технології внутрікадрової селекції / В.В. Баранник, Д.І. Комолов // Наукоємні технології. – 2016. – № 1. - С. 39-47.

11. Баранник В.В. Методология селективной защиты видеопотока по базовым кадрам / В.В. Баранник, Ю.Н. Рябуха, Д.И. Комолов // Информационно-управляющие системы на железнодорожном транспорте. - 2014. - № 6. - С. 69-57.

12. Баранник В.В. Методология селективной защиты видеопотока по базовым кадрам для ведомственных систем / Баранник В.В., Комолов Д.И., Тарнополов Р.В., Отман Шади О.Ю. // Науково-технічна конференція ["Інформаційна безпека України″] / Київський національний університет імені Тараса Шевченка, 12-13 березня 2015 р. - С. 25.

13. Баранник В.В. Модель представления усеченной трансформанты для обработки в инфокоммуникационных системах / В.В. Баранник, С.В. Туренко, Д.И. Комолов // XXII Міжнародна науково-практична конференція [″Інформаційні технології: наука, техніка, технологія, освіта, здоров'я ″], (Харків, 21 - 23 травня 2014 р.) / Національный технічний університет «ХПІ», Харків, 2014. – С. 41-42.

14. Баранник В.В. Селективний метод шифрування видеопотіку в телекомуникаційних системах на основі приховування базового І-кадру / В.В. Баранник, Д.І. Комолов, Ю.М. Рябуха // Наукоємні технології. – 2015. – № 2. - С. 69-77.

15. Баранник В.В. Структурно-комбинаторное представление данных в АСУ / В.В. Баранник, Ю.В. Стасев, Н.А. Королева – Х.: ХУПС, 2009. – 252 с.

16. Баранник В.В. Технология селекции значимых объектов кадра для защиты видеопотока в системах управления критическими ситуациями / В.В. Баранник, Д.И. Комолов, А.В. Тарасенко, А.П. Мусиенко // АСУ и приборы автоматики. – 2015. - №170.

17. Бекіров А.Е. Спосіб компресії зображень в інфокомунікаціях на основі кодування кортежів / А.Е. Бекіров, В.В. Бараннік, С.В. Туренко, Д.І. Комолов // VI Международной научно-практической конференции [″Проблеми і перспективи розвитку ІТ-індустрії ″], (Харків, 17 - 18 квітня

2014 р.) / Харьковский национальный экономический университет, Харьков, 2014. – С. 233.

18. Бекиров А.Э. Способ обработки потока кадров с предсказанием для систем телекоммуникаций / А.Э. Бекиров, Н.А. Харченко, Д.И. Комолов // Науково-методична конференція ["Сучасні проблеми телекомунікації і підготовка фахівців в галузі телекомунікацій - 2014″] / Національний університет "Львівська політехніка", - 1-4 листопада 2014р. - С. - 117-118.

19. Блаттер К. Вейвлет-анализ. Основы теории / К. Блаттер. – М. : Техно сфера, 2006. – 279 с.

20. Блейхут Р. Быстрые алгоритмы цифровой обработки сигналов: Пер. с англ. – М.: Мир, – 1989. – 448 с.

21. Бондарев В.Н., Трестер Г., Чернега В.С. Цифровая обработка сигналов: методы и средства. Учебное пособие для вузов. 2-е изд. – Х.: Конус, 2001. – 398с.

22. Буров Є. Комп'ютерні мережі. – Львів: Бак, 1999. – 468 с.

23. Быков Р.Е. Цифровое преобразование изображений / Р.Е. Быков. – М. : Горячая линия – Телеком. – 2003. – 228 с.

24. Быстрые алгоритмы в цифровой обработке изображений / [Т.С. Хуанг, Дж.О. Эклунд, Г.Дж. Нуссбаумер и др.]; под ред. Т.С. Хуанга; пер. с англ. – М. : Радио и связь, 1984. – 224 с.

25. Васильев В.Н. Компьютерная обработка сигналов / В.Н. Васильев, И.П. Гуров. – СПб: БХВ Санкт-Петербург, 1998. – 240 с.

26. Ватолин Д. Методы сжатия данных. Устройство архиваторов, сжатие изображений и видео / Д. Ватолин, А. Ратушняк, М. Смирнов, В. Юкин – М.: ДИАЛОГ – МИФИ, 2003. – 384с.

27. Введение в контурный анализ: приложения к обработке изображений и сигналов / [Я.А. Фурман, А.В. Кревецкий, А.К. Передреев и др.]; под ред. Я.А. Фурмана. – [2-е изд.]. – М. : ФИЗМАТЛИТ, 2003. – 592 с.

28. Вентцель Е.С. Теория вероятностей и ее инженерные приложения. – М.: Наука. Гл. ред. физ.-мат.лит. – 1988. – 480с.

29. Власов А.В. Кодирование информационных ресурсов систем видеоконференцсвязи для повышения их безопасности. / А.В. Власов,

В.В. Лукин, Д.И. Комолов // Радиоэлектроника и информатика. – 2013. – № 2. – С. 44 – 48.

30. Воробьев В.И. Теория и практика вейвлет – преобразования / В.И. Воробьев, В.Г. Грибунин. – СПб.: ВУС, 1999. – 203 с.

31. Голубов Б.И. Ряды и преобразования Уолша: теория и применения / Б.И. Голубов, А.В. Ефимов, В.А. Скворцов. – М. : Наука, 1987. – 344 с.

32. Гонсалес Р. Цифровая обработка изображений / Р. Гонсалес, Р. Вудс. – М. : Техносфера, 2005. – 1073 с.

33. Господарський процесуальний кодекс України // Відомості Верховної Ради України. – 1992. – № 6 – 56 с. – ч. 1 ст. 81.

34. Гургенидзе А.Т., Корше В.И. Мультисервисные сети и услуги широкополосного доступа. – С.-П.,2003. – 434с.

35. Гуржий П.Н. Декодирование сжатых видеоданных в инфокоммуникационных системах объективного контроля // Сучасна спеціальна техніка. – 2014. – 1. – С. 22-30.

36. Дмитриев В.И. Прикладная теория информации. – М.: Высш. шк., 1989. – 320 с.

37. Залманзон Л.А. Преобразования Фурье, Уолша, Хаара и их применение в управлении, связи и других областях / Л.А. Залманзон. – М. : Наука, 1989. – 496 с.

38. Засядько А.А. и др. К анализу эффективности алгоритмов и программ быстрых ортогональных дискретных преобразований // Электрон. моделирование. – 1998. – №6. – С. 109-111.

39. Золотарев В.В. Реальный энергетический выигрыш кодирования для спутниковых каналов / В.В. Золотарев // Спутниковая связь – ICSC-2000: IV междунар. конф.: труды конф. – М. : МЦНТИ, 2000. – Т. 2. – С. 20-25.

40. Зубков С.В. Assembler. Для DOS, Windows и Linux. – М.: ДМК, 1999. – 640 с.

41. Иванов В.Г. Формальное описание дискретных преобразований Хаара // Проблемы управления и информатики. – 2003. – №5. – С. 68-75.

42. Кашкин В.Б. Цифровая обработка аэрокосмических изображений: Конспект лекций.- Красноярск : ИПК СФУ, 2008. – 121 с.

43. Климов А.С. Форматы графических файлов. – С.-Пб.: ДиаСофт, 1995. – 385 с.

44. Коган Б.М. Основы проектирования микропроцессорных устройств автоматики / Б.М. Коган, В.Б. Сташин . – М.: Энергия, 1989. – 376 с.

45. Кодекс адміністративного судочинства України // Офіційний вісник України. – 2005. – № 32. – 11 с. – Ст. 12.

46. Комолов Д.И. Анализ состояния видеоинформационного обеспечения органов и подразделений Министерства внутренних дел Украины / Д.И. Комолов, С.А. Сидченко // Сучасна спеціальна техніка. – 2014. – № 2. – С. 36 – 44.

47. Комолов Д.И. Кодирование информационных ресурсов систем видеоконференцсвязи для повышения их безопасности. / А.В. Власов, В.В. Лукин, А. В. Власов // Радиоэлектроника и информатика. – 2013. – № 2. – С. 44 – 48.

48. Комолов Д.І. Метод захисту низькочастотних складових в алгоритмі кодування JPEG / Д.І. Комолов, В.В. Ларін, Д.С. Гаврилов, К. Ялівець // Системи обробки інформації. – 2015. – №9. – С. 121 – 123.

49. Комолов Д.И. Технология формирования кодовой конструкции для селективного метода обработки видеоданных // Радиоэлектроника и информатика. – 2015. – №4.

50. Корнеев В.В. Современные микропроцессоры / В.В. Корнеев, А.В. Киселев. – СПб.: БВХ-Петербург, 2003. – 448 с.

51. Королев А.В. Метод восстановления трансформант дискретного косинусного преобразования / А.В. Королев, В.В. Баранник // Системи обробки інформації.-Харків: НАНУ, ПАНМ, ХВУ. – 2000. – Вип. 3(9). – С. 83-86.

52. Королева Н.А. Обоснование двухкомпонентного подхода сжатия видеоданных в информационно-телекоммуникационных системах / Н.А. Королева, А.К. Юдин, А.Ю. Школьник // Информационные управляющие системы на ЖД транспорте. – 2012. – №1. – С. 22-28.

53. Кравченко В.Ф. ″Wavelet″– системы и их применение в обработке сигналов / В.Ф. Кравченко, В.А. Рвачев // Зарубежная радиоэлектроника. – №4. – 1996. – С. 3-20.

54. Красильников Н.Н. Теория передачи и восприятия изображений. Теория передачи изображений и ее приложения / Н.Н. Красильников. – М. : Радио и связь, 1986. – 248 с.

55. Красильников Н.Н. Цифровая обработка изображений. – М.: Вузовская книга, 2011. – 320 с.

56. Красноруцкий А.А. Метод арифметического классификационного кодирования трансформант Уолша / А.А. Красноруцкий, С.Я. Яценко // Открытые информационные и компьютерные интегрированные технологии. – Харьков: НАКУ «ХАИ», 2006. – Вып. 31. – С. 138-141.

57. Кривуца В. Г. Інфокомунікаційні мережі нового покоління: монографія / В.Г. Кривуца, Л.Н. Беркман, С. В. Толюпа; ред.: В. Г. Кривуца; Держ. ун-т інформ.-комунікац. технологій. - К. : ДУІКТ, 2012. - 286 с.

58. Кримінально-процесуальний кодекс України // Відомості Верховної Ради УРСР. – 1961. – № 2 – Ст. 15.

59. Крук Б.И. Телекоммуникационные системы и сети. Том 1, 2, 3 / Б.И. Крук, В.Н. Попантонопуло, В.П. Шувалов. – М.: Горячая линия-Телеком, 2003. – 647 с.

60. Лидовский В.В. Теория информации / В.В. Лидовский. – М.: Компания Спутник+, 2004. – 111 с.

61. Малла С. Вейвлеты в обработке сигналов: Пер. с англ. – М.: Мир, 2005. – 671 с.

62. Мастрюков Д. Алгоритмы сжатия информации. Часть 4. Алгоритм LZW // Монитор. – 1994. – №2. – С. 8-11.

63. Мастрюков Д. Алгоритмы сжатия информации. Часть 2. Арифметическое кодирование // Монитор. – 1994. – №1. – С. 20-23.

64. Миано Дж. Форматы и алгоритмы сжатия изображений в действии: учебное пособие / Дж. Миано; пер. с англ. – М. : Триумф, 2003. – 336 с.

65. Нетравали А.М. Кодирование изображений / А.М. Нетравали, Дж.О. Лимб // ТИИЭР. – 1980. – №3. – С. 76-124.

66. Николаев Ф.А. Проблемы повышения достоверности в информационных системах / Ф.А. Николаев, В.И. Фолин, Л.М. Хохлачев . -Л.: Энергоатомиздат, 1982. – 138с.

67. Обработка изображений и цифровая фильтрация / [под ред. Т.С. Хуанга]. – М. : Мир, 1979. – 318 с.

68. Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 3-е изд. / В.Г. Олифер, Н.А. Олифер. – СПб.: Питер, 2006. – 958 с.

69. Осипов Л.А. Обработка сигналов на цифровых процессорах / Л.А. Осипов. – М.: Горячая линия – Телеком, 2001. – 112 с.

70. Павлидис Т. Алгоритмы машинной графики и обработка изображений, М.: Радио и связь, 1986, 400 с.

71. Поляков П.Ф. Метод восстановления изображений с контролируемой погрешностью / П.Ф. Поляков,В.В. Баранник, А.В. Яковенко // Системи управління, навігації та зв'язку.–ЦНДІ НіЗ. – 2008. – № 4. – С. 44 – 47.

72. Про Національну поліцію: Закон України від 02.07.2015. // Офіційний вісник України. – 2015. – № 63. – 33 с.

73. Про оперативно-розшукову діяльність: Закон України від 18.02.1992.// Відомості Верховної Ради України. – 1992. – № 22. – С. 303.

74. Про особливості забезпечення відкритості, прозорості та демократичності виборів народних депутатів України 28 жовтня 2012 року: Закон України від 05.07.2012.// Офіційний вісник України.–2012.–№ 60. – С.51.

75. Прокис Дж. Цифровая связь. Пер. с англ. / Под ред, Д.Д Кловского. – М.: Радио и связь. 2000. – 800 с.

76. Прэтт У. Цифровая обработка изображений: в 2 т. / У. Прэтт; пер. с англ. – М. : Мир, 1985. – 736 с.

77. Рябуха Ю.Н. Анализ эффективности технологий шифрования в процессе формирования видеопотока / Ю.Н. Рябуха, Д. И. Комолов, Р.В. Тарнополов // The 4th International Scientific Conference ″ITSEC″ (Київ, 20 – 23 травня 2014 р.) / Національний авіаційний університет, Київ, 2014. – С. 60.

78. Рябуха Ю.Н. Метод обработки потока кадров для повышения безопасности видеоинформации / Ю.Н. Рябуха, В.В. Баранник, Д.И. Комолов // V Міжнародна науково-практична конференція ["Інформаційні технології та комп'ютерна інженерія " (ІТКІ-2015)] (Івано-Франківськ – Ворохта – Винниця, 27 – 29 травня 2015 р.) / Прикарпатський національний університет імені Василя Стефаника, Івано-Франківськ, 2015. – С. 47-48.

79. Рябуха Ю.Н. Пути повышения информационной безопасности ресурсов в системах специального назначения / Ю.Н. Рябуха, В.В. Баранник, А.Е. Бекиров, Д.И. Комолов // Четверта міжнародна науково-практична конференція [″Інформаційні технології та комп'ютерна інженерія″], (Вінниця, 28 – 30 травня 2014 р.) / Вінницький національний технічний університет, Вінниця, 2014. – С. 151.

80. Свириденко В.А. Анализ систем со сжатием данных. – М.: Связь 1978.- 183с.

81. Семко В. В. Модель управління захистом інформації в інформаційно-телекомунікаційній системі / В.В. Семко, В.Л. Бурячок, С.В. Толюпа, П.М. Складанний // Радіоелектроніка та телекомунікації : [збірник наукових праць] / відповідальний редактор Б. А. Мандзій. – Львів : Видавництво Львівської політехніки, 2015. – С. 151–155.

82. Синепол В.С. Системы компьютерной видеоконференцсвязи / В.С. Синепол, И.А. Цикин. – М.: ООО "Мобильные коммуникации", 1999. – 166 с.

83. Сэломон Д. Сжатие данных, изображений и звука / Д. Сэломон. – М: Техносфера, 2004. – 368 с.

84. Стрихалюк Б.М. Дослідження статистичних параметрів та характеристик інформаційних потоків в гетерогенних мережах / Б.М.Стрихалюк, І.В.Демидов, В.І. Романчук, М.І. Бешлей // Наукові записки УНДІЗ. – 2014. – №6(34). – С. 82-92.

85. Толюпа С.В. Методи та алгоритми обробки та захисту радіолокаційної інформації у багатопозиційних системах зі змінною просторовою конфігурацією : монографія / С.В. Толюпа, В. А. Дружинін, В.С.Наконечний, Н. В. Цьопа, Є. О. Батрак; Держ. ун-т телекомунікацій. - Київ : Логос, 2014. - 251 с.

86. Тропченко А.Ю. Методы сжатия изображений, аудтосигналов и видео / А.Ю. Тропченко, А.А. Тропченко // Учебное пособие – СПб: СПбГУ ИТМО, 2009. – 108 с.

87. Туренко С.В. Спосіб компресії зображень в інфокомунікаціях на основі кодування кортежів / С.В. Туренко, В.В. Бараннік, А.Є. Бекіров, Д.І. Комолов // VI Международной научно-практической конференции [″Проблеми і перспективи розвитку ІТ-індустрії ″], (Харьков, 17 - 18 апреля

2014 р.) / Харьковский национальный экономический университет, Харьков, 2014. – С. 233.

88. Фисенко В. Т.. Компьютерная обработка и распознавание изображений: учебн. пособие / В. Т. Фисенко, Т. Ю. Фисенко. – СПб. : СПбГУ ИТМО, 2008. – 192 с.

89. Цивільний кодекс України // Офіційний вісник України. – 2003. – № 11, 7 с. – ч. 3 ст. 307.

90. Цифровая обработка изображений в информационных системах / И.С. Грузман, В.С. Киричук и др. – Новосибирск: Изд-во НГТУ, 2002. – 352 с.

91. Чернега В.С. Сжатие информации в компьютерных сетях / В.С. Чернега. – Севастополь: Изд-во СевГТУ, 1997. – 214 с.

92. Шеннон К. Работы по теории информации и кибернетике. – М.: Изд – во иностр. лит – ры, 1963. – 793 с.

93. Шлихт Г.Ю. Цифровая обработка цветных изображений / Г.Ю. Шлихт // М.: ЭКОМ, 1997. – 336 с.

94. Яковенко А.В. Методологічні основи комплексного представлення зображень з контрольованою погрішністю / А.В. Яковенко // Системи озброєння і військова техніка – Х.: ХУПС. – 2008. – Вип. 2(14). – С. 128-131.

95. Akimov D. Occlusion Refinement for Stereo Video Using Optical Flo / D. Akimov, A. Shestov, A. Voronov, D. Vatolin // In: International Conference on 3D Imaging. – 2012. – P. 115-138.

96. Andrews H.C., Hunt B.R. Digital Image Restoration.- Englewood Cliffs (NJ): Prentice Hall, 1977. – XVIII, 238 p.

97. Bai X. Towards temporally-coherent video matting / X. Bai, J. Wang, D. Simons // Proceedings of the 5th international conference on Computer vision/computer graphics collaboration techniques. MIRAGE'11, Springer-Verlag. – 2011 – P. 63-74.

98. Barannik V. A Methodology of video stream selective protection by reference frames / V. Barannik, Dmitry Komolov, Yu. Ryabukha, R. Tarnopolov // // The XIIIth International Conference The Experience of Designing and Application of CAD Systems in Microelectronics CADSM’2015 (24-27 February 2015 Polyana-Svalyava (Zakarpattya), Ukraine). – P. 29-31.

99. Barannik V.V. Encoding of Approximating Making Images for their Transmission in Telecommunication System / V.V. Barannik, A.N. Dodukh, R.I. Akimov // International Conference [“The Experience of Designing and Application of CAD Systems in Microelectronics”], (Lviv – Polyana, Ukraine, February 19 – 23, 2013) / Lviv – Polyana: 2013. – P. 21.

100. Barannik V. Method Of Encoding Transformant Uolsha Is In Systems Air Monitoring Of Earth / V. Barannik, A. Yakovenko, A. Krasnorutkiy // Lviv-Slavsko, Ukraine, Lviv Polytechnic National University, International Conference TCSET’2009, Modern problems of radio engineering, telecommunications and computer science, February 19 – 23, 2009. – P. 381-383.

101. Barannik V. V. Methodological Basis For Determining The Energy Significance Of The Structural Unit Of A Video Frame Based On The Estimation Of Low-Frequency Components Of The Matrices Of The DCT Blocks Of The Luminance Component / V. V. Barannik, Dmitry Komolov, A.P. Musienko, R.V. Tarnopolov // XIVth International Conference [″Modern Problems of Radio Engineering, Telecommunications and Computer Science, TCSET’2016 ″], (Lviv-Slavske, Ukraine, February 22 – 26, 2016) / Lviv-Slavske: 2016. – P. 572 – 574.

102. Barannik V. Technology of the Data Processing on the Basis of Adaptive Spectral-Frequency Transformation of Multiadical Presentation of Images / Barannik V., Sidchenko S., Vasiliev D. // International Symposium [″IEEE East-West Design & Test″], (Moscow, Russia, September 18 – 21, 2009) / Moscow: 2009. – P. 495-498.

103. Barannik V. The Positional Structural-Weight Coding of the Binary View of Transformants / Barannik V., Hahanova A. // International Symposium [″IEEE East-West Design & Test″], (Kharkov, Ukraine, September 18 – 21, 2012) / Kharkov: 2012. – P. 490-494.

104. Barinova O, On detection of multiple object instances using hough transforms / O. Barinova, V. Lempitsky, P. Kholi // Pattern Analysis and Machine Intelligence, IEEE Transactions. 2012. – P. 177-184.

105. Barlaud M. Pyramidal lattice victor quantization for multiscale image coding / M. Barlaud // IEEE Trans. image Proc. – 1994. – V. 3. – № 4. – P. 367-381.

106. Chigorin A, A method for traffic sign detection in an image with learning from synthetic dat / A. Chigorin, G. Krivovyaz, A. Velizhev, A. Konushin //

14th International Conference Digital Signal Processing and its Applications. Vol 2. 2012. – P. 316-335.

107. Ding Z. GPU accelerated interactive space-time video matting / Z. Ding, H. Chen, Y. Gua, Q. Peng // In Computer Graphics International. – 2010. – P. 163-168.

108. Gonzales R.C. Digital image processing / R.C. Gonzales, R.E. Woods. – Prentice Inc. Upper Saddle River, New Jersey 2002. – 779 p.

109. Gopinath R.A. On cosine-modulated wavelet orthogonal bases / R.A. Gopinath, C.S. Burrus // IEEE Trans. Image Proc. – 1995. – V. 4. – № 2. – P. 162-177.

110. Grundmann M. Efficient hierarchical graph based video segmentation / M. Grundmann, V. Kwatra, M. Han, I. Essa / IEEE CVPR. // 2010. – P. 85-91.

111. Habibi A.,Wintz P.F. Image coding by linear transformation and block quantization // IEEE Trans. Commun. Tech. – 1971. V. COM – 19. – №1. P.50-63.

112. Kaarna A. Blockwise Distortion Measure for Lossy Compression of Multispectral Image / A. Kaarna, J. Parkkinen // Proceeding of the 10-th European Signal Processing Conference, 5-8 September 2000. – Tampere, Finland, 2000. – P. 2197-2200.

113. Kang H. R. Color Technology for Electronic Imaging Devices, Vol. PM28, SPIE Press, Bellingham, WA, 1997.

114. Komolov Dm. Assessment of Video Information Resource Security of Videoconferencing in Public Administration/ Dm. Komolov, T. Saprykina, A. Vlasov, S. Sidchenko , // International Symposium «IEEE East-West Design & Test», (Kiev, Ukraine, September 26–29, 2014) / Kiev: 2014. – P. - 329 – 331.

115. Komolov D. Selective Method For Hiding Of Video Information Resource In Telecommunication Systems Based On Encryption Of Energy-Significant Blocks Of Reference I-Frame / D. Komolov, D. Zhurbynskyy, O. Kulitsa // 1st International Conference «Advanced Information and Communication Technologies-2015, AICT'2015», (Lviv, Ukraine, October 29 – November 1) / Lviv: 2015. – P. 80 – 83.

116. Kossentini F., Chung W.C., Smith M. Subband image coding using entropy-constrained residual vector quantization // Information Processing and Management. – 1994. – V.30. – №6. – P. 887 – 896.

117. Lee S.Y. Temporally coherent video matting / S.Y. Lee, J.C. Yoon, I.K. Lee // Graphical Models 72. – 2010. – P. 25 – 33.

118. Lezama J. Track to the future: Spatio-temporal video segmentation with long-range motion cues / J. Lezama, K. Alahari, J. Sivic, I. Laptev // In: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition. – 2011. – P.256-289.

119. MATLAB 6.0. Финансовые, инженерные и научные расчеты в среде Windows. – М.: Информационно-издательский дом «Филинъ», 1997. – 712 с.

120. Milyaev S. Image binarization for end-to-end text understanding in natural images / S. Milyaev, O. Barinova, T. Novikova, V. Lempitsky, P. Kohli // ICDAR. – 2013. – P. 35-42.

121. Ponomarenko N., Lukin V., Egiazarian K., Astola J., Partition Schemes in DCT Based Image Compression, // Technical Report 3-2002, ISBN 952-15-0811-6, Tampere University of Technology, Finland, 2002, 100 p.

122. Pratt K. Digital Image Processing: PIKS Inside, Third Edition. John Wiley & Sons, Inc., 2001, 738 p.

123. Sindeev M. Alpha-flow for video matting / M. Sindeev, A. Konushin, C. Rother // Technical Report. – 2012. P. – 41 – 46.

124. Strykhalyuk B. Implementation of wireless heterogeneous network based on LTE core virtualization for military communication systems / B. Strykhalyuk, I. Kahalo, M. Brych, M. Beshley, M. Seliuchenko // Системи озброєння і військова техніка: наук. журнал / Х: Харк. ун-т Повітр. Сил ім. Івана Кожедуба. – 2014. - №4(40). - С. 125-132.

125. Voronov A. Methodology of stereoscopic motion picture quality assessment / A. Voronov, D. Vatolin, D. Sumin, V. Napadovsky, A. Borisov // Stereoscopic Displays and Applications XXIV, Proc. of SPIE-IS&T Electronic Imaging, SPIE. – 2013. – P. 67 – 69.

126. Wallace G.K. The JPEG Still Picture Compression Standard // Communication in ACM. – 1991. – V34 – №4. – P.31-34.

127. Wallace G.K. Overview of the JPEG (ISO/CCITT) Still image compression: image processing algorithms and techniques / G.K. Wallace // Processing of the SPIE. – 1990. – Vol. 1244. – P. – 220-233.

ПРИЛОЖЕНИЕ

ЗАТВЕРДЖУЮ

Проректор ХНУРЕ
з наукової роботи
_____ М.І. Сліпченко
«15» 09 2015р.

АКТ
впровадження результатів дисертаційної роботи Комолова Д.І. в держбюджетну НДР № 276-4 «Технології створення інтегрованих інформаційних систем на основі мереж цифрового мобільного зв'язку»

Комісія у складі: завідуючого кафедрою «Мережі зв'язку» д.т.н. Безрука В.М., доцента кафедри «Мережі зв'язку» к.т.н. Колтуна Ю.М., відповідального виконавця НДР № 276-4 к.т.н. Кочкіна М.І., підтверджує, що ряд наукових та практичних результатів дисертаційної роботи Комолова Д.І. використані при виконанні держбюджетної НДР № 276-4 «Технології створення інтегрованих інформаційних систем на основі мереж цифрового мобільного зв'язку», що виконувалась згідно тематичного плану НДР ХНУРЕ. Зокрема, були використані наступні результати:

- розроблена методологічна база селективного приховування відеопотоку в умовах обмежень на бітову швидкість стиснутого представлення відеокадру та групи кадрів. Тут враховуються залежності бітової швидкості прихованого відеопотоку в умовах доставки в реальному часі від коефіцієнтів стиснення і пікового відношення сигнал/шум;
- розроблено селективний метод приховування потоку відеоданих із закриттям базового І-кадру. У результаті закриття базового І-кадру його обсяг збільшується на 6-30% залежно від пікового відношення сигнал/шум. Таким чином, у разі закриття від 20% до 60% відеоданих, досягається приховування всієї переданої відеоінформації. При цьому спостерігається значна економія часу на обробку та передачу відеоданих.

Вказані результати використані при підготовці заключного звіту по НДР № 276-4, зокрема підрозділу 4.5 «Методологія селективного захисту відеопотоку з базових кадрів в інфокомунікаціях».

В.М. Безрук
Ю.М. Колтун
М.І. Кочкін

ЗАТВЕРДЖУЮ
Начальник ГУМВС України
в Харківській області
генерал-майор міліції
Дмитрієв А.А.

07 10 2015

А К Т

впровадження результатів науково-прикладних досліджень Комолова Дмитра Івановича

Комісія у складі:
голови комісії: заступник начальника ГУМВС України в Харківській області полковник міліції Пахомов В.А.;
членів комісії: заступник начальника Управління матеріального забезпечення – начальник відділу зв'язку ГУМВС України в Харківській області Маслій В.В.;
заступник начальника відділу зв'язку Управління матеріального забезпечення ГУМВС України в Харківській області підполковник міліції Єрмаков Д.С.;
старший інженер відділу зв'язку Управління матеріального забезпечення ГУМВС України в Харківській області підполковник міліції Лосьєв В.А.;
склала дійсний акт, який полягає в тому, що при виконанні дослідно-конструкторських робіт використані наступні результати науково-прикладних досліджень Комолова Дмитра Івановича:

1. Метод закриття відеопотоку на основі внутрікадрової селекції структурних одиниць базового відеокадру, який базується на:

1) розділенні зображення на структурні одиниці та розподіленні їх за рівнем семантичної та структурної інформативності;

2) технології закриття найбільш інформативних структурних одиниць базового відекадру, яка включає наступні процедури: обчислення сумарного значення низькочастотних компонент матриці дискретного косинусного перетворення блоків яскравої складової структурної одиниці кадру; визначення найбільш інформативних блоків яскравої складової структурної одиниці кадру за рівнем енергетичного значення у відношенні з пороговими значеннями;

приховування структурних одиниць базового відеокадру, до складу яких входять найбільш інформативні блоки яскравої складової.

2. Метод реконструкції прихованих відеоданих в системі диференційованої обробки кадрів. Метод відновлення базується на диференційованому процесі декодування базового кадру в залежності від значимості його структурних складових з наступним зворотнім криптографічним перетворенням інформативних структурних одиниць.

Впровадження результатів досліджень Комолова Д.І. в відомчій системі відеоконференцзв'язку на основі програмно-апаратних реалізацій дозволило забезпечити:

1) виграш по інтенсивності закритого базового кадру при шифруванні тільки найбільш значущих структурних одиниць на 40-60% залежно від пікового відношення сигнал/шум у порівнянні з закриттям всього базового кадру;

2) значення пікового відношення сигнал/шум у разі несанкціонованого доступу на рівні 10дБ. Таким чином, за рахунок закриття тільки найбільш значущих структурних одиниць пікове відношення сигнал/шуму знаходиться в допустимих межах;

3) скорочення часу кодування і передачі закритого відеопотоку за рахунок зменшення кількості операцій з кодування кадру на 25-40%;

4) підвищення пропускної спроможності закритого відео каналу при шифруванні тільки найбільш значущих структурних одиниць базового кадру на 40-50% залежно від пікового відношення сигнал/шум.

голови комісії: заступник начальника ГУМВС України в Харківській області полковник міліції _____ В.А. Пахомов

членів комісії: заступник начальника Управління матеріального забезпечення – начальник відділу зв'язку ГУМВС України в Харківській області _____ В.В. Маслій

заступник начальника відділу зв'язку Управління матеріального забезпечення ГУМВС України в Харківській області підполковника міліції _____ Д.С. Єрмаков

старший інженер відділу зв'язку Управління матеріального забезпечення ГУМВС України в Харківській області підполковник міліції _____ В.А. Лосьєв