ПРИМЕНЕНИЕ АСИНХРОННОГО МУЛЬТИПЛЕКСИРОВАНИЯ СКРЫТЫХ КАНАЛОВ ПЕРЕДАЧИ ДАННЫХ В ОДНОМ ВИДЕОПОТОКЕ СИСТЕМ СПУТНИКОВОЙ СВЯЗИ

Е.С. Абазина[1*], **А.А. Ерунов**[1]

[1]Военно-космическая академия имени А.Ф. Можайского, Санкт-Петербург, 197198, Российская Федерация
*Адрес для переписки: e.s.abazina@yandex.ru

Информация о статье
УДК 621.396
Язык статьи – русский

Ссылка для цитирования: Абазина Е.С., Ерунов А.А. Применение ассинхронного мультиплексирования скрытых каналов передачи данных в одном видеопотоке систем спутниковой связи // Труды учебных заведений связи. 2017. Т. 3. № 2. С. 5–15.

Аннотация: *Развитие методов сокрытия данных и расширение приложений цифровой стеганографии требует поиска компромисса между скрытностью и пропускной способностью скрытых каналов передачи данных. В данной статье обоснована актуальность исследований в направлении перераспределения пропускной способности группового скрытого канала передачи данных в видеопотоке системы спутниковой связи, предствлен подход, позволяющий увеличить число скрытых каналов передачи данных в одном видеопотоке за счет асинхронного мультиплексирования.*

Ключевые слова: *цифровая стеганография, скрытые каналы, стегоканалы, скрытая пропускная способность, асинхронное мультиплексирование, переменная пропускная способность скрытого канала.*

APPLICATION OF ASYNCHRONOUS MULTIPLEXING FOR HIDDEN CHANNELS IN ONE VIDEO STREAM OF SATELLITE COMMUNICATION SYSTEMS

E. Abazina[1], **A. Erunov**[1]

[1]Military Space Academy of A.F. Mozhaysky, St. Petersburg, 197198, Russian Federation

Article info
Article in Russian

For citation: Abazina E., Erunov A. Application of Asynchronous Multiplexing for Hidden Channels in One Video Stream of Satellite Communication Systems // Proceedings of Educational Institutes of Communication. 2017. Vol. 3. Iss. 2. PP. 5–15.

Abstract: *The development of data's concealment and extension of the applied scope of digital steganography demand to search the compromise between concealment and capacity of the hidden channel. In this article the relevance of redistribution in one video stream of satellite communication systems of the hidden channels capacity is justified. An approach to increasing numbers*

of the hidden channels in one video stream is submitted here. It can be achieved by the using of asynchronous multiplexing for hidden channels.

Keywords: *Digital steganography, the hidden channels, stegochannels, capacity of the hidden channel, asynchronous multiplexing, variable capacity of the hidden channel.*

В современных условиях эффективность применения сил и средств в значительной степени определяется эффективностью функционирования системы управления этими силами и средствами. Под силами и средствами авторы понимают любые абстрактные человеческие ресурсы и материальные средства, на которые возложено выполнение задач по предназначению. Независимо от решаемых задач, система управления включает в себя органы управления – лица, принимающие решения и контролирующие их исполнение, управляемые объекты – силы и средства, на которые возложено выполнение поставленной задачи, и инфокоммуникационную систему, обеспечивающую взаимодействие органов управления и управляемых объектов. При организации управления на распределенной территории, в труднодоступных районах, в регионах с отсутствующей телекоммуникационной инфраструктурой взаимодействие возможно лишь при использовании спутниковых систем связи. При этом одним из основных недостатков систем спутниковой связи является разведдоступность и низкая помехоустойчивость. Передача информации ограниченного распространения по спутниковым каналам требует применения дополнительных технологических решений, обеспечивающих защиту передаваемой информации. С этой целью целесообразно совместное применение криптографических и стеганографических методов.

Основной задачей цифровой стеганографии, в отличие от криптографии, является сокрытие предаваемых данных за счет избыточности различных видов информации, представляемой в цифровом виде и не привлекающей внимания несанкционированных наблюдателей. Информацию, в которой осуществляется скрытая передача, принято называть контейнером [1, 2]. Основным требованием, предъявляемым к стеганографическому обмену, является скрытность в смысле сохранения в тайне факта передачи информации. Скрытность, как правило, определяется искажениями, вносимыми в контейнер при встраивании скрываемой информации: чем меньшей модификации подвержен контейнер, тем более скрытно осуществлено встраивание дополнительных данных.

По целям использования методов цифровой стеганографии общепризнанными являются три направления [1–3]:

– встраивание скрытых каналов передачи информации – целью встраивания является сокрытие факта передачи информации;

– встраивание цифровых водяных знаков (ЦВЗ) – цель встраивания состоит в подтверждении подлинности предаваемых данных и в предотвращении несанкционированного доступа к ним;

– встраивание идентификационных номеров (цифровые отпечатки пальцев, ЦОП) – с целью скрытой аннотации и аутентификации передаваемой информации.

Под скрытым (стеганографическим) каналом понимают совокупность программных (или аппаратно-программных) средств, реализующих методы встраивания и извлечения информации в контейнер, и среды распространения контейнера, позволяющих сохранить в тайне факт передачи встроенной информации.

В отличие от ЦВЗ и ЦОП, скрытые каналы характеризуются максимальным количеством информации, которое возможно встроить в один контейнер при сохранении скрытности встраивания, называемым в стеганографии пропускной способностью скрытого канала или скрытой пропускной способностью. Скрытая пропускная способность тем больше, чем больше число элементов контейнера возможно исказить или заменить при встраивании скрываемой информации. Скрытность и пропускная способность скрытого канала состоят в противоречии друг с другом: увеличение одного из них приводит к снижению другого [1–3].

Дополнительные ограничения на пропускную способность скрытого канала возникают из-за необходимости обеспечения достоверности приёма скрываемых данных не хуже заданной. Зависимость скрытой пропускной способности $C_{\text{стег}}$ от скрытности U и достоверности приёма скрываемых данных $P_{\text{ош}}$ представлена на рис. 1.

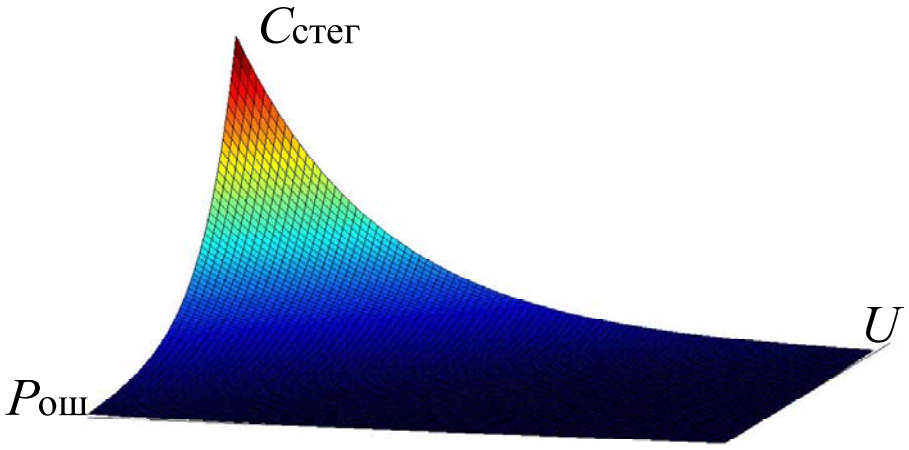


Рисунок 1. Определение пропускной способности скрытого канала

С целью организации защищенных каналов обмена информацией ограниченного распространения по спутниковым радиолиниям предлагается рассмотреть возможность построения стегосистемы, обеспечивающей скрытый информационный обмен между несколькими парами абонентов в одном контейнере. Значительная избыточность видеоданных в сравнении с остальными видами трафика определяет их приоритетное использование в качестве контейнера для скрытой передачи информации.

Потребность в числе каналов спутниковой связи для обеспечения функционирования системы управления силами и средствам, требования к пропускной способности элементарных каналов связи и степени их защищенности

определяются иерархическим уровнем органа управления, которому они предоставляются. Требования же по достоверности приема информации и времени ее передачи зависят от вида передаваемой информации. В условиях чрезвычайных ситуаций целесообразно предусмотреть первоочередную организацию низкоскоростных информационных каналов, ориентированных на передачу речи и коротких текстовых сообщений или телеграмм. Таким образом, основными видами трафика скрытых каналов, рассматриваемых в работе, следует считать:

– трафик, критичный к задержке по времени (телефонные переговоры), с ограничением на время доставки пакета не хуже, чем $t_{\text{дост}} \leq 400$ мс;

– трафик, критичный к достоверности приема (текстовые сообщения и телеграммы), с ограничением на вероятность ошибочного приема не хуже, чем $P_{\text{ош}} \leq 10^{-3}$.

Анализ ранее разработанных технологических решений организации скрытых каналов в видеоданных, подробно представленный в работах [1–3], позволил сформулировать следующие выводы. Наибольшей скрытностью обладают методы встраивания информации в частотную область видеоданных до проведения операций сжатия. Однако это приводит к искажению скрываемой информации в процессе сжатия, что обуславливает необходимость ее помехоустойчивого кодирования, а, следовательно, накладывает дополнительные ограничения на скрытую пропускную способность. Многоабонентный скрытый информационный обмен в структуре одного видеоконтейнера может быть реализован за счет кодового уплотнения скрываемых сообщений [4–6]. Существующая технология позволяет сформировать порядка 30-ти элементарных скрытых каналов с пропускной способностью в 1,2 кбит/с каждый при средней скорости передачи видеопотока 8 Мбит/с [4–6]. Пропускная способность скрытого канала в видеопотоке зависит от его динамики и, следовательно, не постоянна.

Таким образом, применение одной только технологии кодового уплотнения скрываемых данных недостаточно для организации скрытого информационного обмена достаточно крупной (порядка 100 абонентов) системы управления. Одним из способов повышения пропускной способности скрытого канала является применение асинхронного мультиплексирования скрываемых данных: телефонных и телеграфных переговоров. Возможность применения данной технологии обоснована пульсирующим характером речи, состоящей из последовательности периодов активности абонента и пауз между ними. Статистика активности речевых абонентов свидетельствует о том, что в среднем лишь 40–45 % времени переговоров приходится на долю активной речи. Наличие пауз может быть использовано для передачи иной информации одновременно с ведущимся телефонным разговором по средствам статистического мультиплексирования.

В отличие от мультиплексирования с временным разделением, предполагающего выделение фиксированного временного интервала из общей полосы пропускания для каждого из каналов, при статистическом мультиплексирова-

нии каждому информационному потоку предоставляется временной интервал в соответствии с требуемой скоростью передачи информации.

В соответствии с ранее разработанным методом организации кодово-уплотненного скрытого канала [4–6], встраивание скрываемых данных осуществляется путем замены пары бит оцифрованного спектра видеоконтейнера, полученного в базисе функций, согласованных с двумерной шумоподобной сигнальной конструкцией (ДШСК), элементами ДШСК, модулированной информацией, требующей сокрытия. При применении статистического мультиплексирования в стегосистеме, разделяемым ресурсом между активными абонентами выступают элементы видеоконтейнера, подлежащие модификации при встраивании, а также строки матрицы ДШСК.

Особенность мультиплексирования состоит в необходимости согласования выходной скорости пакетированных данных абонентов скрытого информационного обмена с переменной скоростью их встраивания в контейнер. Принцип работы такого асинхронного мультиплексора представлен на рис. 2.

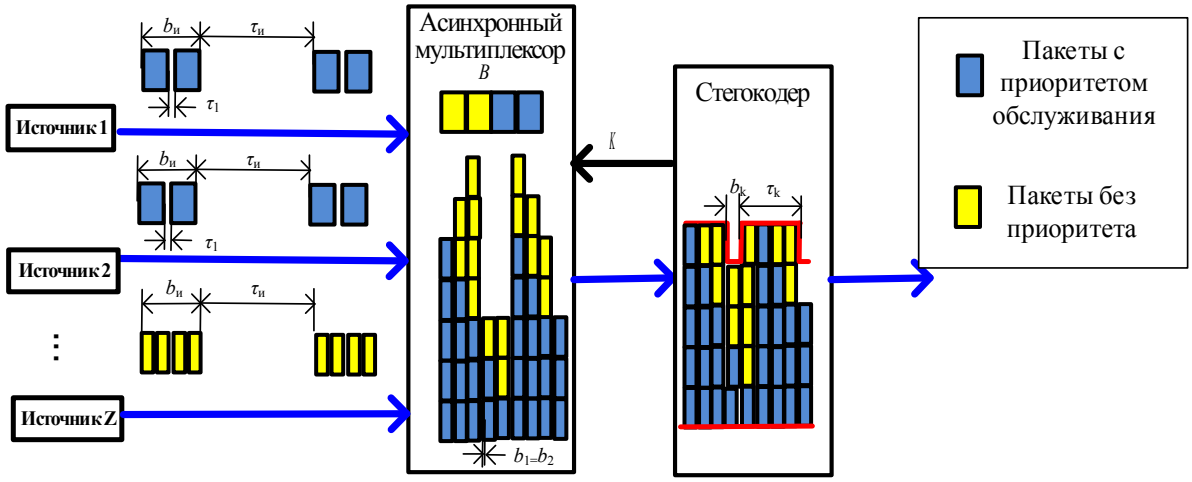


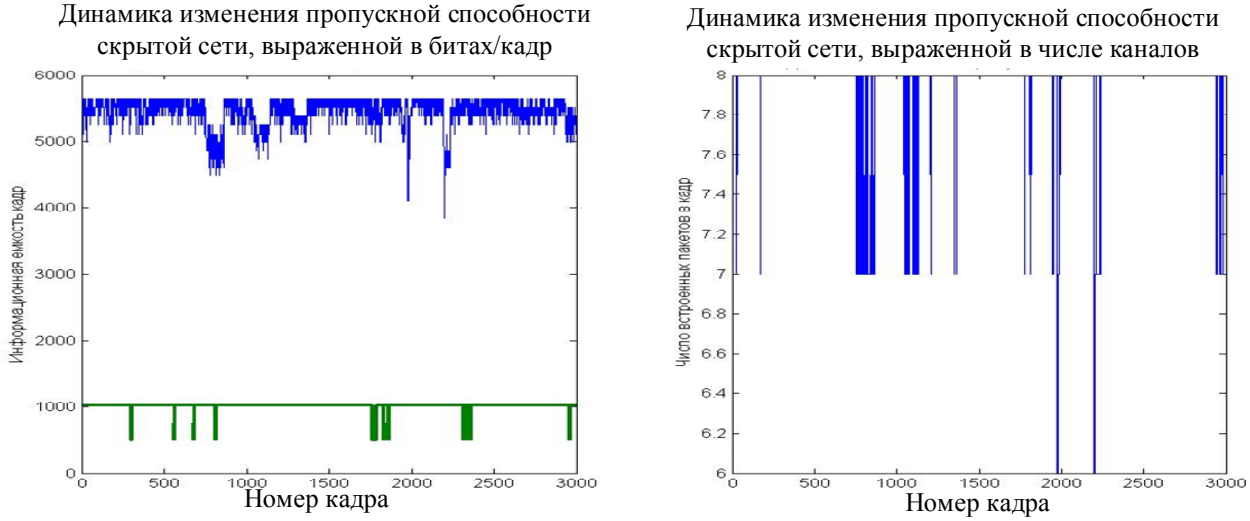
Рисунок 2. Принцип работы асинхронного мультиплексора с переменной скоростью передачи

Пакетированные данные абонентов скрытого информационного обмена поступают на вход стегокодера в соответствии с приоритетом обслуживания со скоростью передачи, согласованной с текущей скоростью встраивания. Приоритет в обслуживании потока пакетированных данных, подлежащих сокрытию, может быть назначенв соответствии со срочностью или важностью передаваемой информации. В случае переполнения входного буфера асинхронного мультиплексора происходит потеря пакетов, а с увеличением его емкости – увеличение времени задержки пакетов. Параметры вероятности потери пакетов и времени их задержки являются ключевыми при оценивании качества обслуживания трафика абонентов скрытого информационного обмена.

Для оценивания пропускной способности скрытого канала с кодовым уплотнением в работе разделены понятия емкости скрытого канала и скрытой пропускной способности. Под емкостью скрытого канала K авторы понимают

потенциальные возможности видеоконтейнера, определяемые, как максимум типовых скрытых каналов, организуемых в этом контейнере, из числа возможных. Под скрытой пропускной способностью $C_{стег}$ в статье подразумевается максимально достижимая скорость скрытой передачи данных в одном видеоконтейнере и измеряемая в бит/с.

Результаты имитационного моделирования оценивания переменной пропускной способности группового скрытого канала представлены на рис. 3: оценена скрытая пропускная способность $C_{стег}$ (рис. 3а) и емкость скрытого канала K (рис. 3б). Результаты получены для значений вероятностей ошибочного приема $P_{ош}$ не хуже 10^{-3} (соответствует синей кривой графиков) и $P_{ош}$ не хуже 10^{-5} (соответствует зеленой кривой графиков). Ось абсцисс соответствует номерам кадров в видеопотоке и характеризует динамику видеоконтейнера, ось ординат – скрытой пропускной способности $C_{стег}$ или емкости скрытого канала K (рис. 3а и рис. 3б соответственно).



а) б)

Рисунок 3. Результаты оценивания пропускной способности скрытого канала

На рис. 4 представлены накопленные статистические данные об изменении числа элементарных каналов и снижении скрытой пропускной способности (зеленая кривая), аппроксимированные кривой, изменяющейся по экспоненциальному закону распределения случайной величины (синяя кривая).

Результаты проверки соответствия выбранного закона распределения случайной величины снижения пропускной способности реальному процессу по критерию Пирсона, представлены на рис. 5.

Полученные значения критерия Пирсона $x^2_{эксп}$ соответствуют синей кривой на рис. 5. При этом зеленая линия соответствует критическому значению критерия Пирсона $x^2_{крит}$.при заданном числе степеней свободы $r = k - s = 7$ ($k = 8$ – число разрядов, $s = 1$ – число наложенных связей) для выборки. Вероятность, равная 0,7, характеризует расхождение теоретического и статистического распределения и означает, что данное расхождение, обусловленное случайными

причинами, будет не меньше, чем фактически наблюдаемое в данной серии опытов значение χ^2.

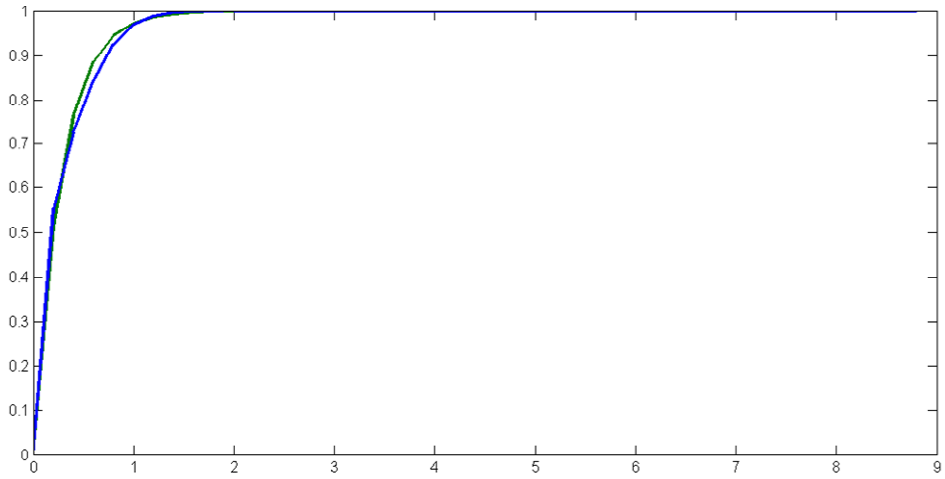


Рисунок 4. Аппроксимация закона распределения случайной величины снижения пропускной способности скрытого канала

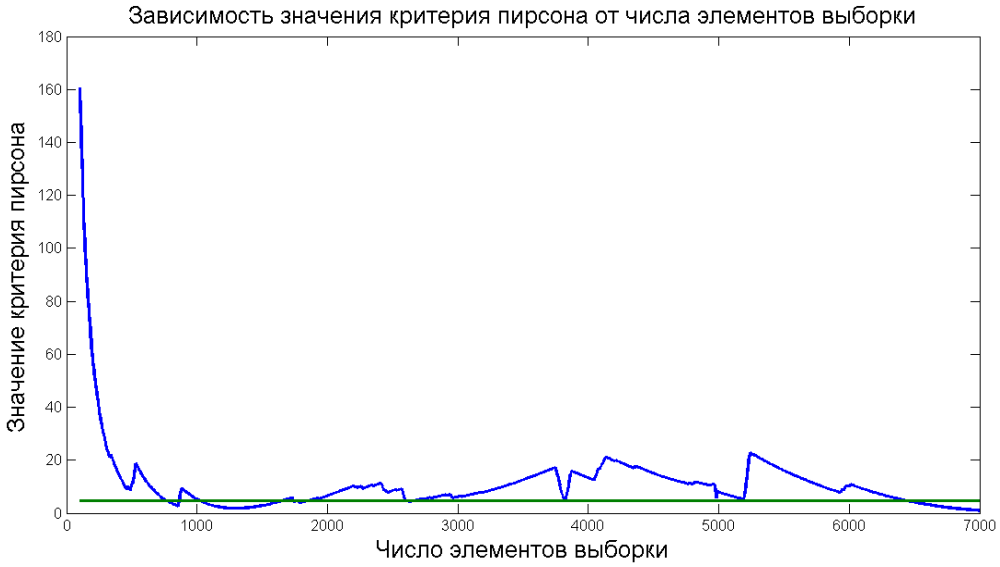


Рисунок 5. Проверка выбранного закона распределения случайной величины снижения пропускной способности по критерию Пирсона

Анализ представленных графиков позволяет заключить, что применение выбранного закона аппроксимации случайной величины снижения пропускной способности допустимо в модели асинхронного мультиплексирования скрываемых данных в видеоконтейнере.

Применение асинхронного мультиплексирования низкоскоростных информационных потоков при формировании группового скрытого канала в видеоданных позволяет достичь увеличения скрытой пропускной способности. Зависимость коэффициента уплотнения канала от активности источников трафика, подлежащего сокрытию, при изменении канальной емкости мультиплексора представлены на рис. 6.

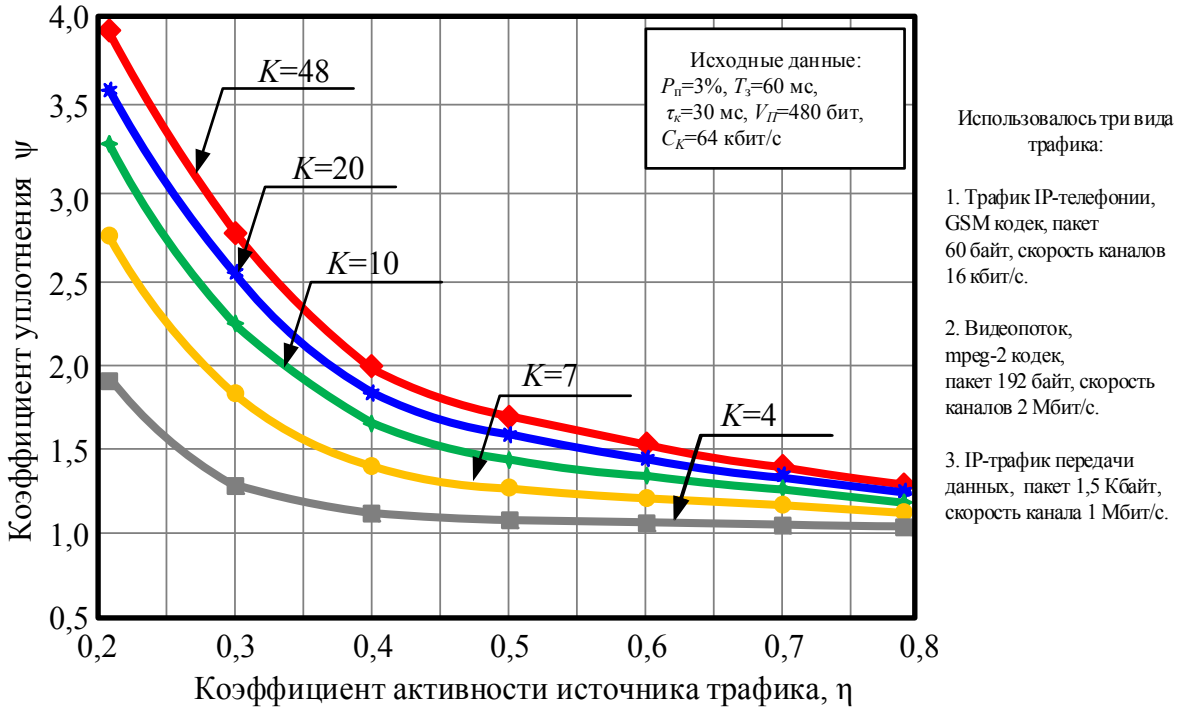
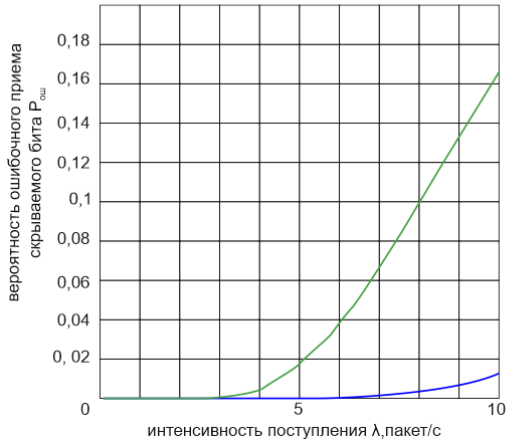


Рисунок 6. Зависимость коэффициента уплотнения от активности источников трафика при изменении канальной емкости мультиплексора

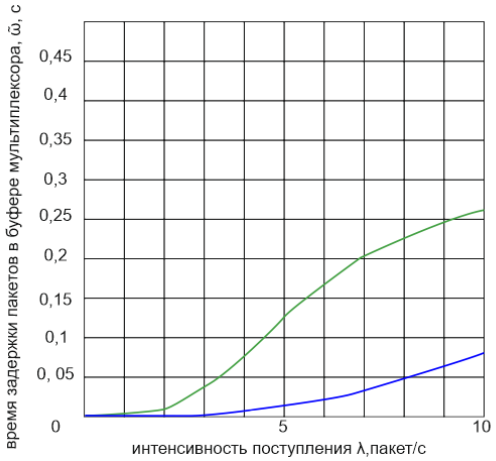
Данная технология реализована при работе мультиплексора с постоянной канальной емкостью и позволяет повысить скрытую пропускную способность на величину, обратную коэффициенту активности мультиплексированных источников.

Результаты оценивания емкости скрытого канала K, пропускной способности скрытого канала $C_{стег}$ при ограничениях на качество обслуживания мультисервисного трафика абонентов скрытого информационного обмена (вероятность потери пакетов $p_{пп}$, время задержки пакетов $t_{зад}$) при асинхронном мультиплексировании с переменной скоростью встраивания скрываемых данных приведены на рис. 7.

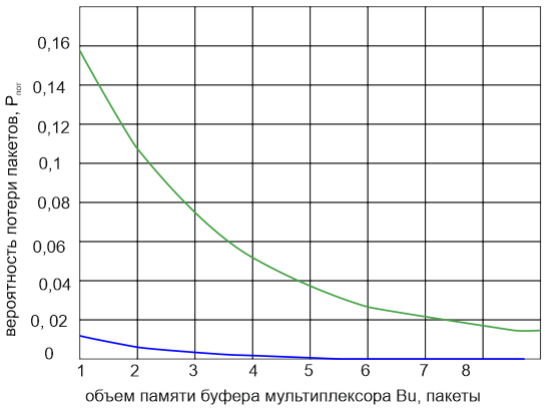
Представленные зависимости получены при следующих условиях: интенсивность активизации речевых абонентов $\alpha = 1{,}2$; интенсивность умолкания источников трафика $\beta = 1{,}8$; число источников трафика $Z = 9$; число статистически уплотняемых скрытых каналов $K = 4$; объем памяти буфера мультиплексора $Bu = 8$ пакетов; интенсивность поступления пакетов 1 приоритета $\lambda_1 = 10$ пакетов/с; интенсивность поступления пакетов 2 приоритета $\lambda_2 = 20$ пакетов/с; интенсивность обслуживания пакетов 1 и 2 приоритетов = 10 пакетов/с; среднее время снижения пропускной способности скрытого канала $t_{сниж} = 5$ с; среднее время восстановления пропускной способности скрытого канала $t_{восст} = 0{,}25$ с. Пакеты трафика первого приоритета отмечены на графиках синим, второго приоритета – зеленым.



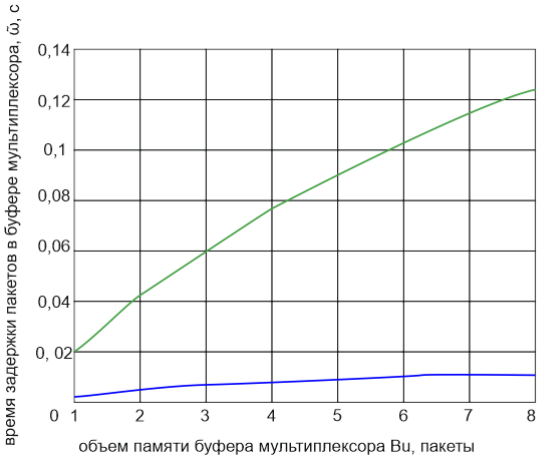
Зависимость вероятности потери пакетов от интенсивности поступления пакетов



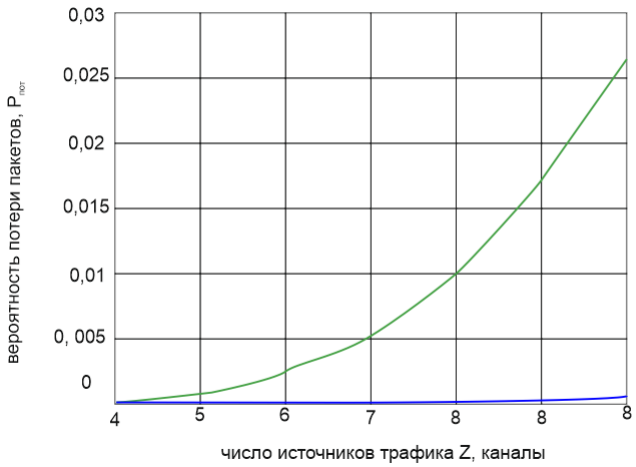
Зависимость времени задержки пакетов от интенсивности поступления пакетов



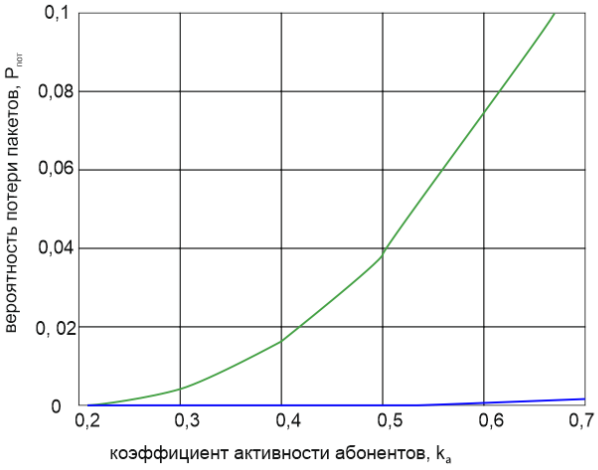
Зависимость вероятности потери пакетов от емкости буфера



Зависимость вероятности потери пакетов от числа источников трафика



Зависимость времени задержки пакетов от емкости буфера



Зависимость вероятности потери пакетов от активности абонентов

Рисунок 7. Результаты оценивания параметров мультисервисного трафика абонентов скрытого информационного обмена при асинхронном мультиплексировании

На рис. 8 представлена зависимость выигрыша, получаемого в результате асинхронного мультиплексирования, от канальной емкости группового скрытого канала при вероятности потери пакетов не более 1 % (синие кривые) и при вероятности потери пакетов не более 3 % (зеленые кривые). При времени задержки пакетов в буфере мультиплексора $\tilde{\omega}$ = 120 мс полученные зависимости отмечены на графиках сплошными кривыми, при времени задержки пакетов в буфере мультиплексора $\tilde{\omega}$ = 60 мс – пунктирными.

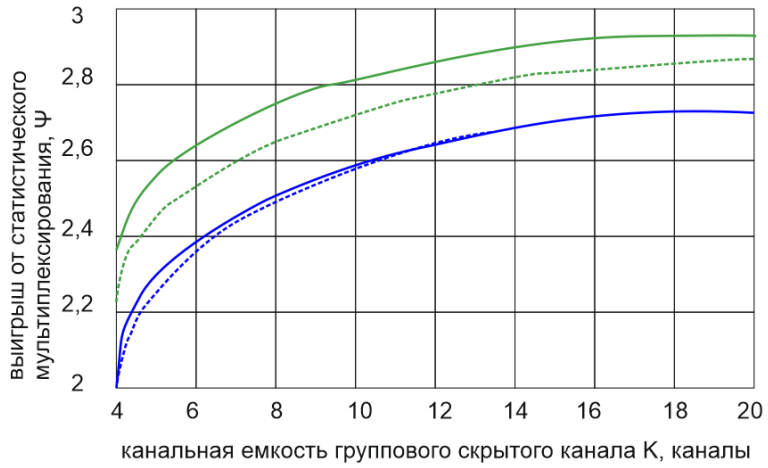


Рисунок 8. Зависимость выигрыша, получаемого в результате асинхронного мультиплексирования, от канальной емкости группового скрытого канала

При оценивании скрытности разработанной технологии организации скрытых каналов в видеопотоке был осуществлен контроль параметров контейнера до и после встраивания скрываемых данных:

– субъективное оценивание визуального качества видеоконтейнера (визуальная атака) [7];

– объективное оценивание визуального качества видеоконтейнера по показателю пикового отношения сигнал-шум (ПОСШ), для которого в [8] определено значение не ниже 30 дБ, что соответствует удовлетворительному качеству видеоданных;

– оценивание изменения гистограммы видеоконтейнера до и после встраивания (статистическая атака).

Результаты оценивания скрытности разработанной технологии организации группового скрытого канала передачи данных с применением асинхронного мультиплексирования в видеоконтейнере представлены в [9]. Выполнение требований к ПОСШ видеоданных после встраивания скрываемой информации в совокупности с изменениями визуального качества и гистограммы видеоизображения, неотличимыми от искажений, вносимых шумами канала, позволяет делать вывод о построении ρ-надежной стегосистеме с вероятностью ошибочного обнаружения несуществующего скрытого сообщения, стремящейся

к нулю, при вероятности не обнаружения скрытого сообщения, стремящегося к единице [1, 2].

Таким образом, применение в процессе формирования группового скрытого канала в видеоконтейнере технологии асинхронного мультиплексирования встраиваемых данных, предаваемого в интересах управления силами и средствами, позволяет:

– обеспечить требования, предъявляемые к качеству обслуживания мультисервисного трафика абонентов скрытого информационного обмена;

– повысить пропускную способность скрытого канала и емкость скрытого канала в видеоконтейнере при ограничениях на скрытность встраивания и качество обслуживания. Достигаемый выигрыш при этом составляет до 2,9 раз в сравнении с существующей технологией формирования скрытого канала с кодовым уплотнением в структуре видеопотока.

Список используемых источников

1. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография. М.: Солон-Пресс. 2009. 272 с.

2. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика. Киев: МК-Пресс. 2006. 283 с.

3. Абазина Е.С., Ерунов А.А. Цифровая стеганография: состояние и перспективы // Системы управления, связи и безопасности. 2016. № 2. С. 182–201. URL: http://journals.intelgr.com/sccs/20162/html.

4. Абазина Е.С., Ерунов А.А. Результаты моделирования метода скрытой передачи информации с кодовым уплотнением в видеоданных // Системы управления, связи и безопасности. 2015. № 2. С. 1–25. URL: http://journals.intelgr.com/sccs/20152/html.

5. Абазина Е.С. Метод кодового уплотнения скрытого канала при передаче видеоданных // Системы управления, связи и безопасности. 2015. № 3. С. 14–42. URL. http://journals.intelgr.com/sccs/20153/html.

6. Абазина Е.С., Коровин В.М., Федосеев В.Е., Цветков К.Ю. Имитационная модель скрытой передачи информации с кодовым уплотнением в структуре сжимаемых видеоданных // Свидетельство о государственной регистрации программы для ЭВМ № 2015615358. 15.02.2015.

7. ГОСТ 26320-84. Оборудование телевизионное студийное и внестудийное. Методы субъективной оценки качества цветных телевизионных изображений. М.: Изд-во стандартов. 1985. 8 с.

8. ГОСТ Р 52722-2007. Каналы передачи цифровых телевизионных сигналов. Основные параметры и методы измерений. М.: Стандартинформ. 2007. 18 с.

9. Абазина Е.С., Ерунов А.А., Федосеев В.Е., Цветков К.Ю. Выбор параметров стегосистемы при передаче скрытой информации в видеоданных // Сборник докладов XII научно-технической конференции по криптографии, посвященной 95-летию образования Специальной службы. Орел: Академия ФСО. 2016. С. 112–116.