электронный научно-технический журнал
ИНЖЕНЕРНЫЙ ВЕСТНИК
Издатель ФГБОУ ВПО "МГТУ им. Н.Э. Баумана". Эл No. ФС77-51036. ISSN 2307-0595

Метод сокрытия данных в стереофонических аудиофайлах

 # 09, сентябрь 2015

Чичварин Н. В.[1,*], Волосатова Т. М.[1]

УДК: 004.9:66.013.512.

[1]Россия, МГТУ им. Н.Э. Баумана
[*]genrih.gertz@gmail.com

Введение

В работе принимается что САПР — это организационно-техническая система, состоящая из совокупности комплекса аппаратно – программных средств автоматизации проектирования и коллектива специалистов подразделений проектной организации, выполняющая автоматизированное проектирование изделия [1].

При этом имеется ввиду, что САПР — иерархическая система, реализующая комплексный подход к автоматизации всех уровней проектирования. Иерархия уровней проектирования является прямым следствием существования иерархии модельного представления объекта проектирования. Это создает специфические требования, предьявлямыми к САПР. Анализ доступных публикаций позволяет сделать также вывод о наметившейся в последние годы тенденции применение PLM – технологий. Так, как повышение цен на ПО САПР и усложнение дорогостоящих технических средств САПР делает средства автоматизированного проектирования недоступными для малого и среднего бизнеса, применение облачных вычислений и PLM – технологий становится все более привлекательным. Поскольку применение открытых САПР, облачных технологий и PLM – технологий предполагает возможность НСД к проектной документации, проблемы обеспечения ИБ САПР становятся весьма актуальными. Многие программные средства подлежат обязательной сертификации и нуждаются в постоянном контроле специалистами по информационной безопасности. Поэтому будет справедливо считать, что вопросы ИБ САПР обладают спецификой, заставляющей рассматривать их отдельно от общих вопросов информационной безопасности остальных автоматизированнных информационных систем. Очевидно, что защита проектной документации, продуцируемой в среде САПР возможна двумя методами:

- Криптографические.
- Стеганографические.

В работе наибольшее внимание уделено методам стеганографической защиты поектной САПР. Это обусловлено следующими прчинами:

- Криптографические методы защиты от НСД сложны, не всегда санкционируется спецслужбами. Кроме того, параметры криптографической защиты регламнтируются ГОСТ, а применение агоритмов, составляющих государственную тайну недопустимо.
- Факт применения стеганографических алгоритмов чрезвычайно затруднительно обнаружить.

Следует отметить также, что применение криптографических алгоритмов для защиты проектной документации от НСД целесообразно в проектных организациях оборонной промышленности.

1. Состояние проблемы. Специфика ИБ САПР.

1.1. Анализ доступных публикаций в области информационной безопасности САПР [1 – 5] показывает, что для обеспечения информационной безопасности технического и программного обеспечений САПР в основном используются системы информационной безопасности (СЗИ) общего назначения. САПР — открытая и развивающаяся система. Усложнение ОП, вычислительной техники и вычислительной математики приводит к появлению новых математических моделей и программ. Причем в последние десятилетия по вашеуказанным причинам ПО САЕ все чаще используется по лизингу, с примененим облачных технологий.

1.2. Анализ методов защиты проектной документации от НСД.

Задачи защиты САПР от НСД:

- Защита от НСД проектной документации внутри организации успешно обеспечивается за счет применения СЗИ.
- Защита каналов связи, применяемых в САПР.

Первая задача успешно решается путем использования вычислительных средств, оснащенных соответствующими программно-аппаратными комплексами, прошедших соответствующую аттестацию. В отдельных случаях степень защиты текстовой документации может быть повышена за счет применения методов криптографии. Для решения этой задач применимы аппаратные и аппаратно-программные средства на базе специализированного процессора АККОРД [4]. Однако использование криптографических методов значительно усложняет процесс проектирования и не всегда допустимо с точки зрения действующего законодательства.

Как показывает обзор доступных публикаций, в настоящее время нет известных удовлетворительных решений в области решения второй задачи. В работе [5] рассмотрены и предложены оригинальные методы стеганографической защиты текстовой проектной документации в среде САПР. Их достоинствами являются:

- Гибкость изменения системы паролей
- Многоуровневая система паролей, соответствующая комбинированию стеганографических методов для защиты от НСД одного и того же документа.
- Ненаблюдаемость факта сокрытия данных в том или ином контейнере.

- Возможность применения изображений чертежей для сокрытия спецификаций и другой текстовой информации.

Исследования, обобщающие результаты численных экспериментов с 15 алгоритмическими алгоритмами проведенные авторами настоящей публикации, показали, что для сокрытия проектной документации, передаваемых по открытым КПС, наиболее предпочтительно применение записи стего в аудиоконтейнер.

2. Основные результаты теоретических исследований

Суть предлагаемого метода заключается в следующем:

- на первой стадии регистрируется изображение защищаемого документа либо с использованием искусственно расфокусированным известным образом устройством ввода в ЭВМ. Решается так называемая прямая задача (конволюции);
- на второй стадии производится формирование стеганограммы с использованием какого-либо предпочтительного метода стеганографии.
- На третьей стадии формируется стегосообщение – в первом стереоканале записывается стего, а во втором записывается ключ. В частности, в предложенном методе ключ – это ядро уравнения Фредгольма, например открытой документации.

При санкционированном доступе к защищенным данным последовательность действий имеет обратный порядок:

- На первой стадии выделяются первый и второй стереоканала.
- На второй стадии по известному ключу из заполненного контейнера извлекается стего в виде «размытого» изображения.
- На третьем этапе решается так называемая обратная задача (деконволюции) – восстановление дефокусированного изображения документа.

Реализация метода

Для большинства реальных технически реализуемых фокусирующих систем и особенно в случае моделирования дефокусировки на ЭВМ, она моделируется интегральным уравнением. Это уравнение можно записать в виде интегрального уравнения Фредгольма I рода:

$$\int_a^b k(x-s_x;y-s_y)g(s_x;s_y)ds_x ds_y = f(x;y) \qquad (1)$$

В качестве математической модели дефокусированной системы используется интегральное уравнение типа свертки. Уравнение применимо для описания формирования искусственно дефокусированного изображения (конволюции) при моделировании на ЭВМ и деконволюции в случае решения обратной задачи. В случае конволюции искомой является функция f , а в случае деконволюции – функция g. Ключом в данном методе является ядро (импульсный отклик), т.е. функция $K(*\ ,*\ .)$, либо какой – либо параметр (параметры), однозначно определяющий ядро.

Основываясь на свойствах оператора свертки, данное уравнение в частотной области можно записать как

$$K(u,v)G(u,v) = F(u,v) \quad (2)$$

где: (u,v) – координаты в частотной области, K, G, F – Фурье-образы соответствующих функций. $K(u,v)$ также называют передаточной функцией.

Однако прямое алгебраическое решение уравнения простым делением невозможно – функция $K(*, *)$ имеет нули и полюса.

Для решения задачи применяется регуляризация, когда уравнение (2) записывается в виде:

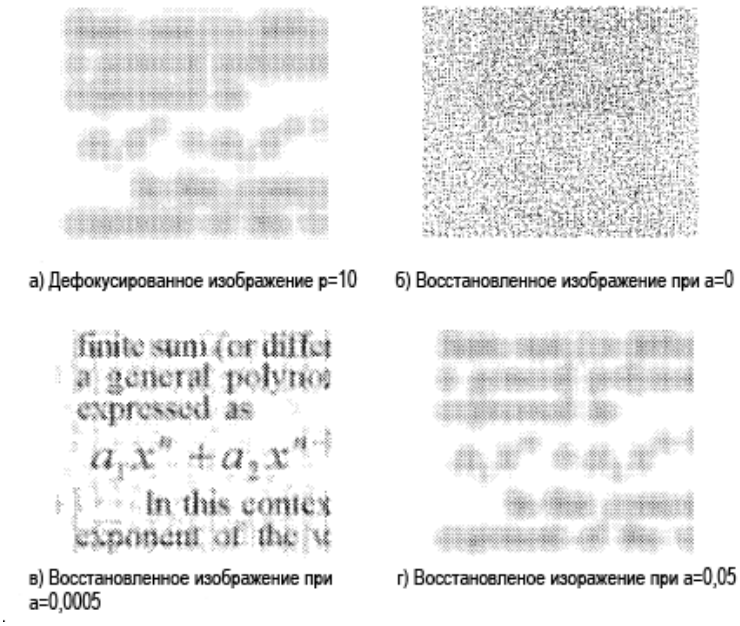
$$G'(u,v) = W(u,v)F(u,v) \quad (3)$$

В качестве функции W берется:

$$W(u,v) = \frac{K^*(u,v)}{|K(u,v)|^2 + \alpha M(u,v)} \quad (4)$$

где $M(u,v)$ –неотрицательная функция выбирается таким образом, чтобы добиться стабильности решения, но не внести слишком много искажений в решении α – параметр регуляризации, Символ «*» обозначает комплексно сопряженную величину.

Параметр регуляризации выбирается таким образом, чтобы добиться стабильности решения, но не внести слишком много искажений в решении. Для его определения используется метод Тихонова. На рис. 4,5 представлены примеры дефокусированных изображений и результаты их восстановления. В случае, когда санкционированный пользователь знает ключ в виде параметра импульсного отклика $k(. . .)$ и приближенно – параметр а регуляризации, возможно восстановление дефокусированного изображения (рис. 1). В противном случае восстановление потребует затрат больших ресурсов.



а) Дефокусированное изображение p=10 б) Восстановленное изображение при a=0

в) Восстановленное изображение при a=0,0005 г) Восстановленое изоражение при a=0,05

Рис. 1. Дефокусированное изображение и восстановленное при различных параметрах регуляризации.

3. Корреляционный метод сокрытия изображений

Поскольку вычисления корреляционной и ковариационной с применением БПФ аналогичны, далее не делается между ними.

Примеры решения задачи вычисления ковариационной функции и результат деконволюции приведены на Рис. 2, 3 ,4 и 5.

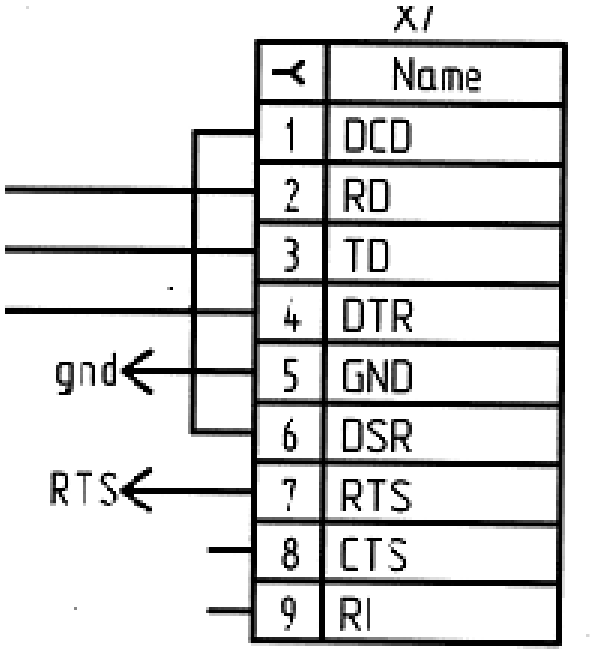


Рис. 2. Исходное (шифруемое) изображение.

Рис. 3. Зашифрованное изображение.

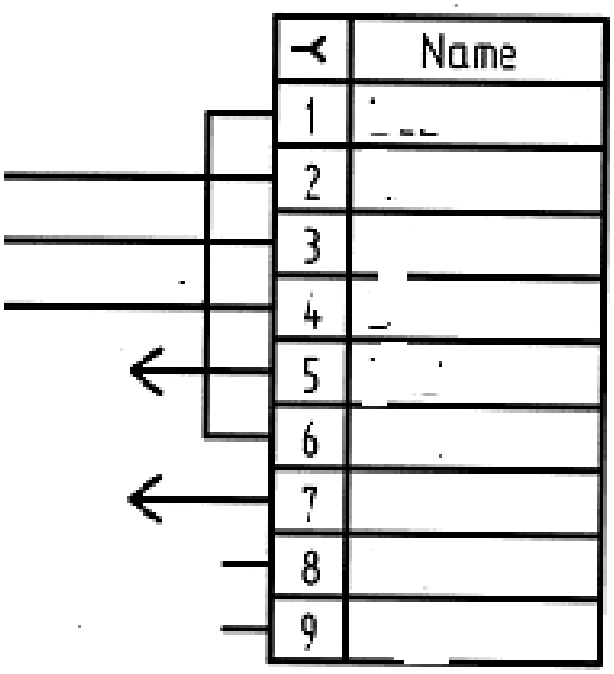


Рис. 4. Кодирующее изображение («слепая» распиновка).

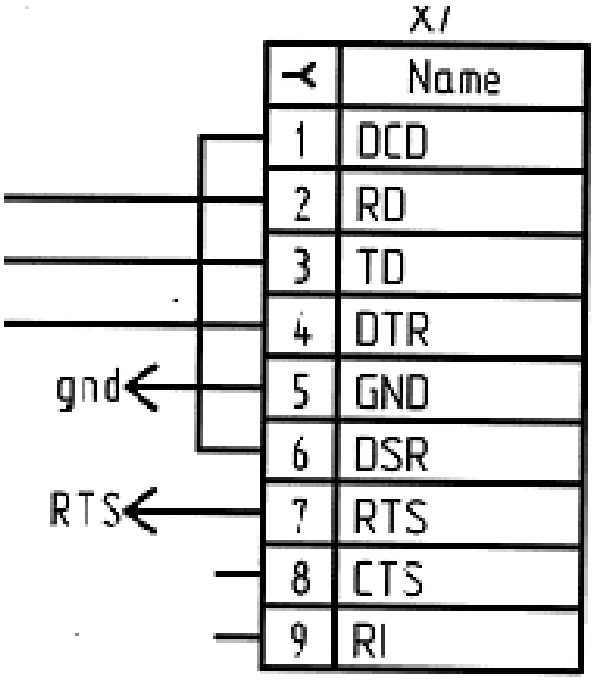


Рис. 5. Восстановленное изображение.

Численные эксперименты проводились со стего большего объема. На Рис. 6 показана схема усторойства, название которого условно обозначим №1. На Рис. 7 приведена вторая схема, условно обозначенная №2

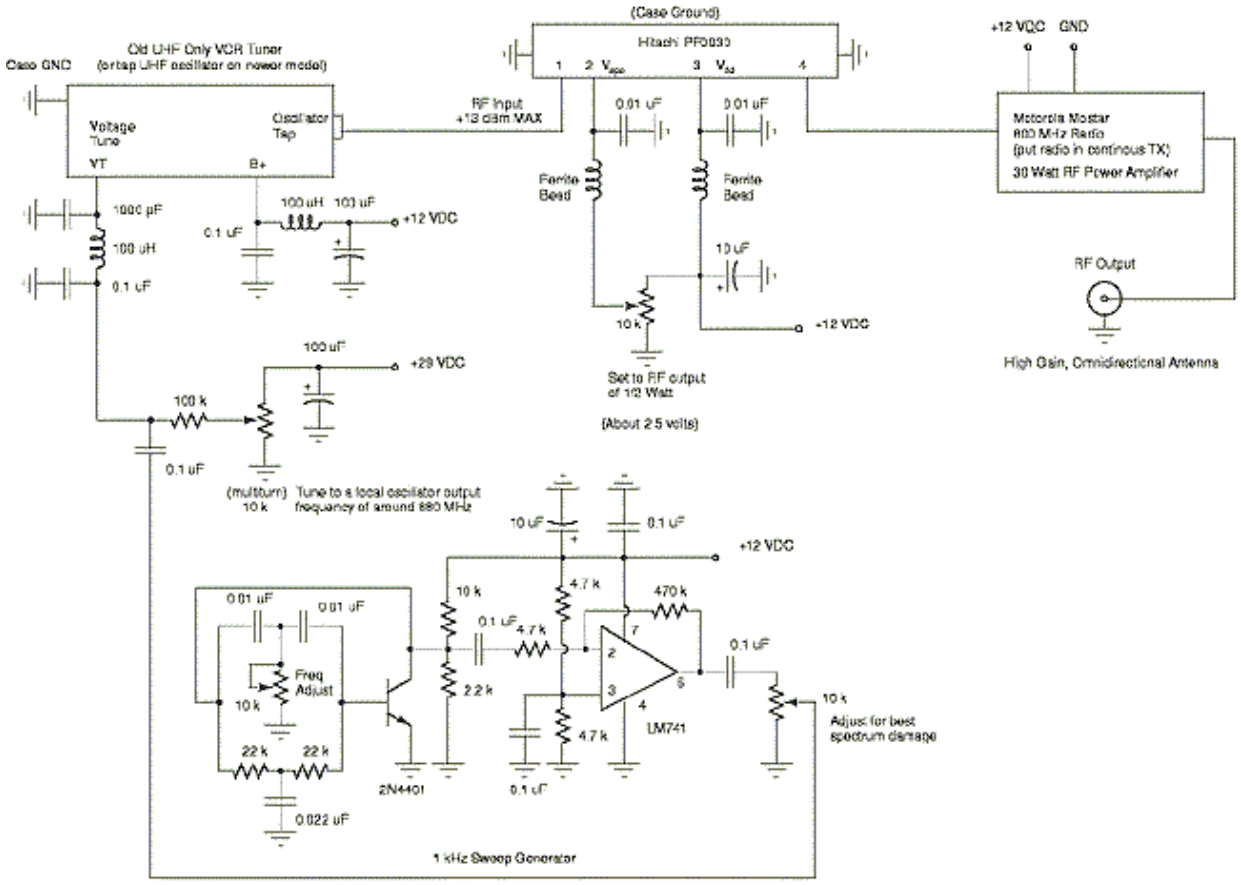


Рис. 6. Электрическая схема № 1.

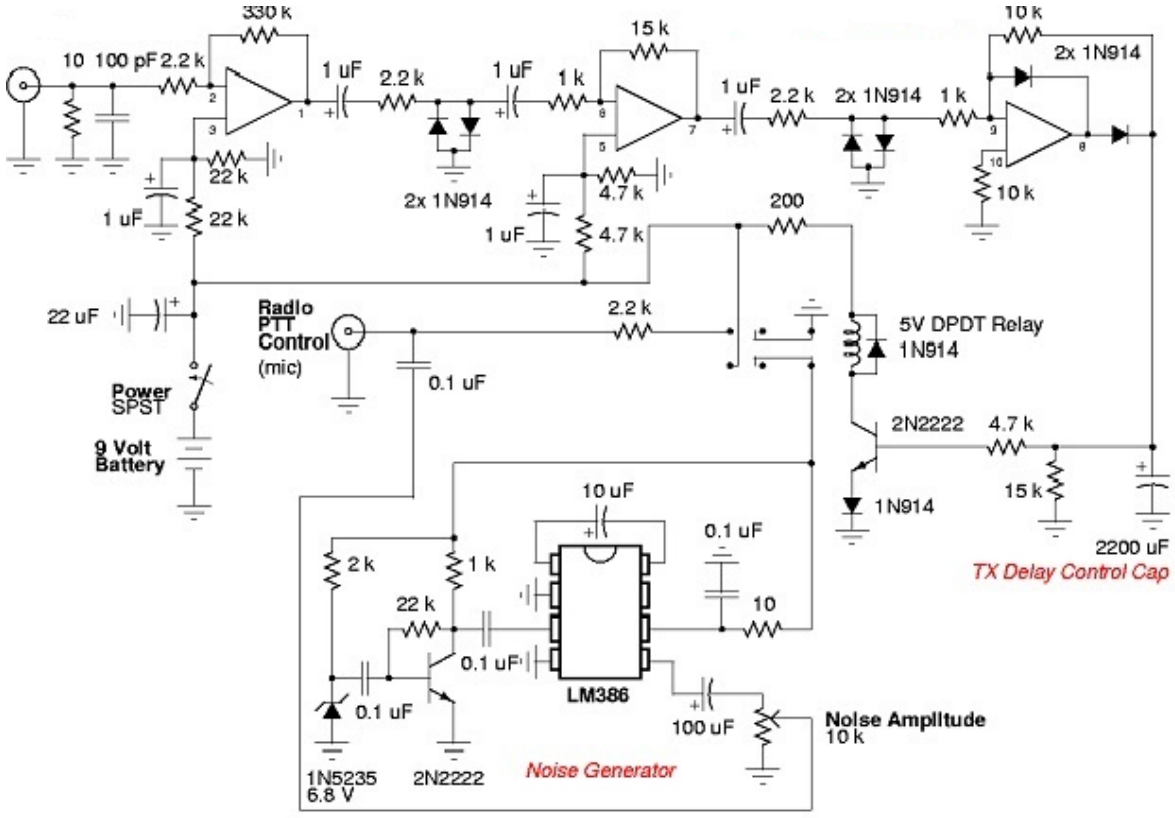


Рис. 6. Электрическая схема № 2.

На Рис. 7 приведено изображение, описываемое функцией взаимной ковариации между функцией, описывающей изображение схемы № 1 и № 2.

На выходе алгоритма кодирования получаем ключ шифрования и контейнер с зашифрованными данными. На выходе алгоритма декодирования получаем, с использованием ключа, зашифрованные данные.

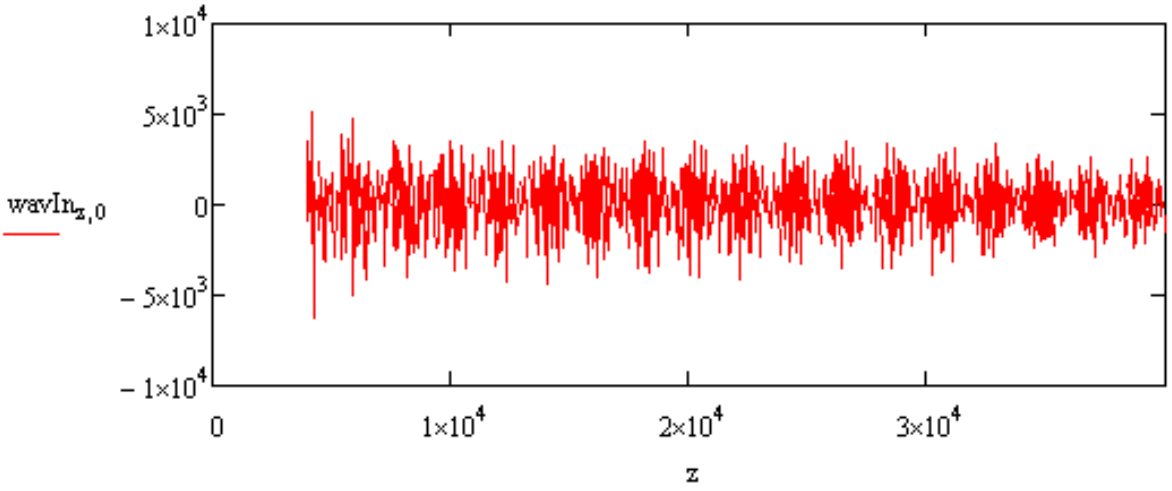


Рис. 8. Осциллограмма исходного звуковой файла (контейнера).

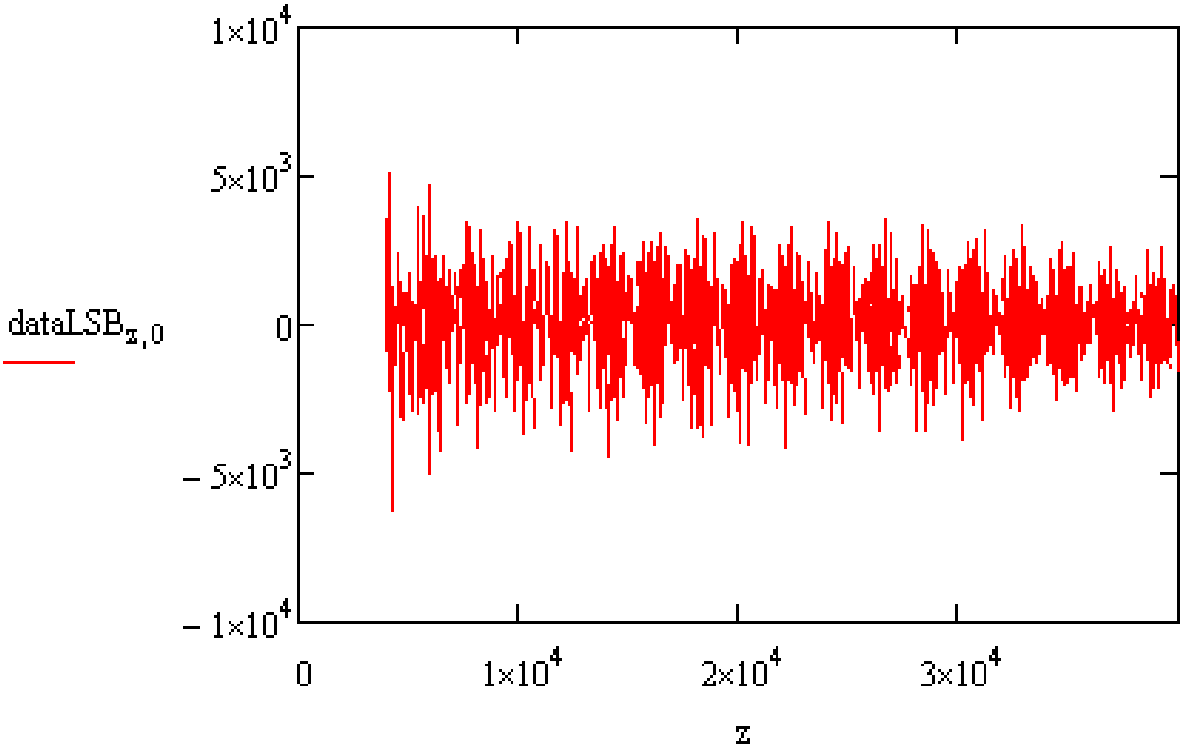


Рис. 9. Осциллограмма WAV файла со стегосообщением.

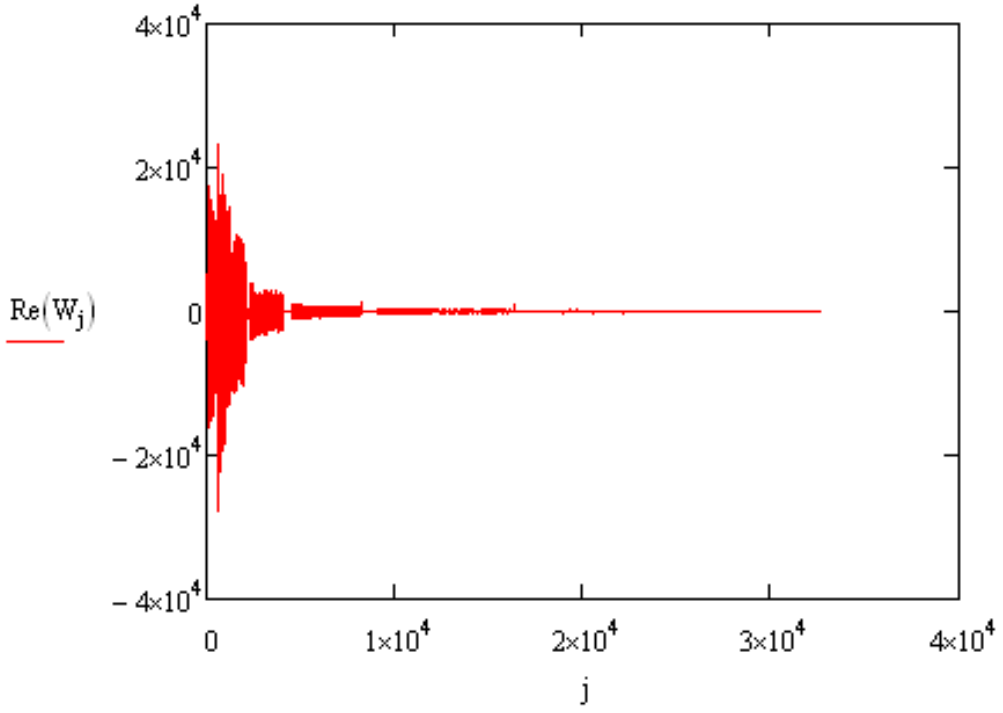


Рис. 10 Визуализация вейвлет преобразования WAV файла со стего(первого канала звукового файла)

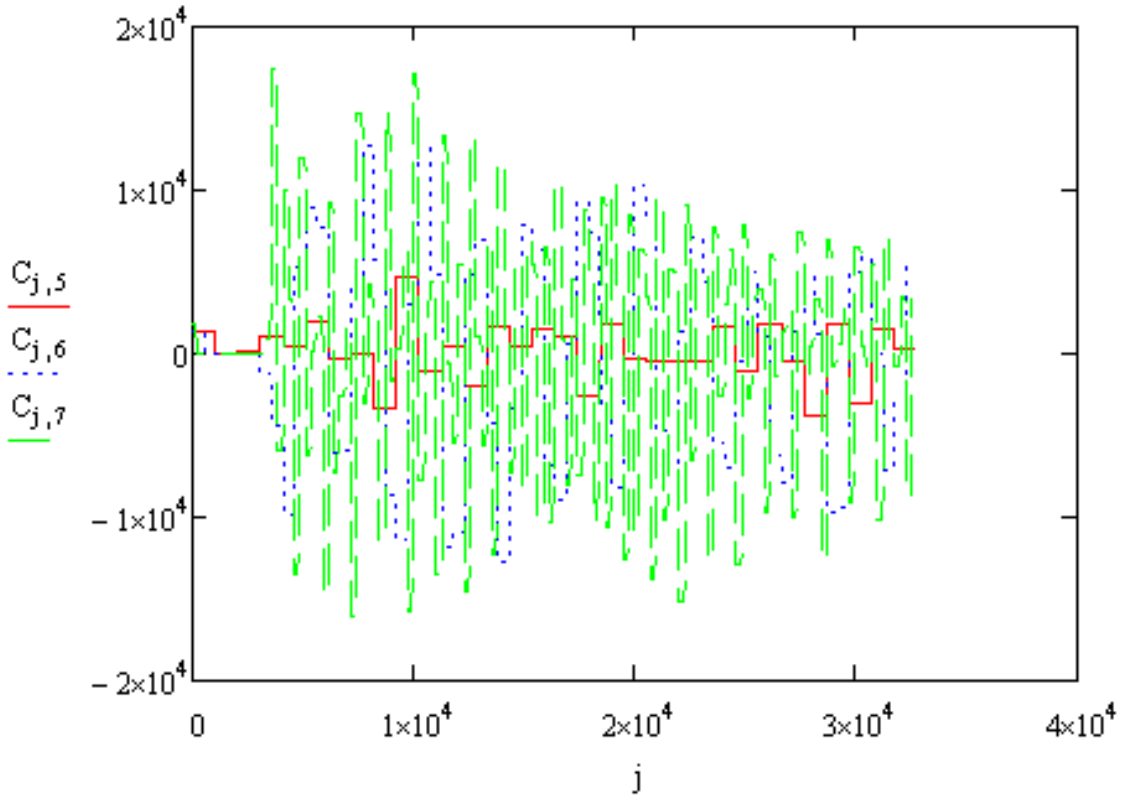


Рис. 11. Визуализация семейств коэффициентов вейвлет-спектра Добеши WAV файла со стего(первого канала звукового файла). Cj,x – коэффициенты вейвлет-преобразования, x - номер семейств коэффициентов вейвлет-спектра Добеши.

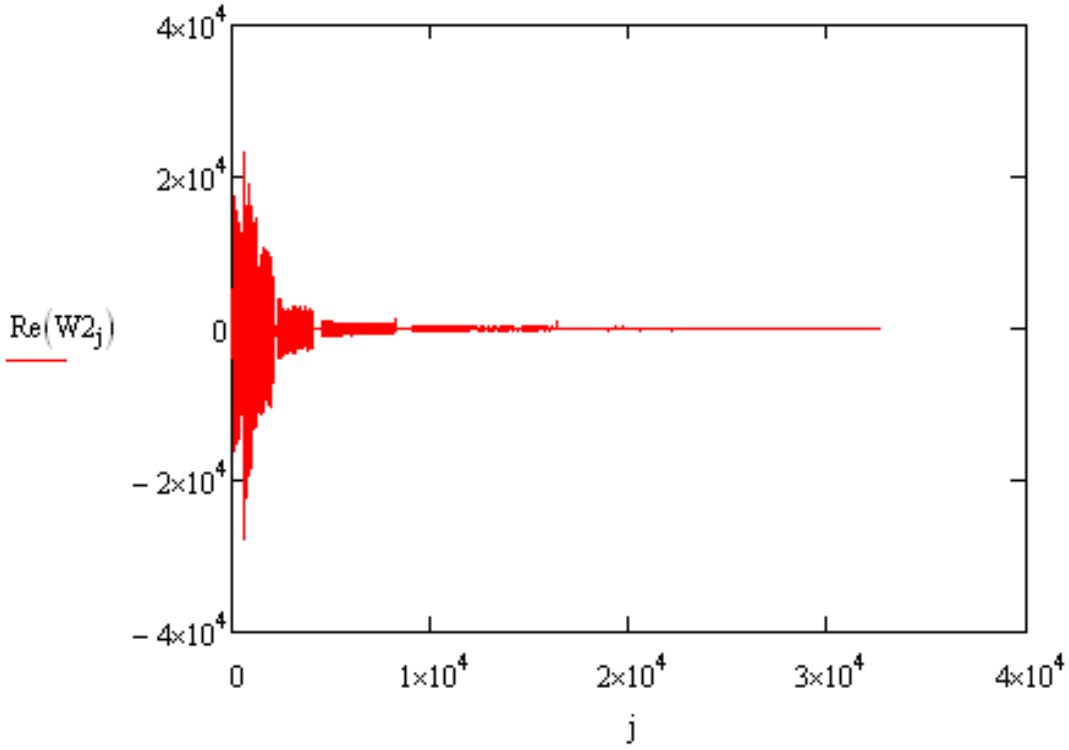


Рис. 12. Визуализация вейвлет преобразования исходного аудио файла (второго канала звукового файла)

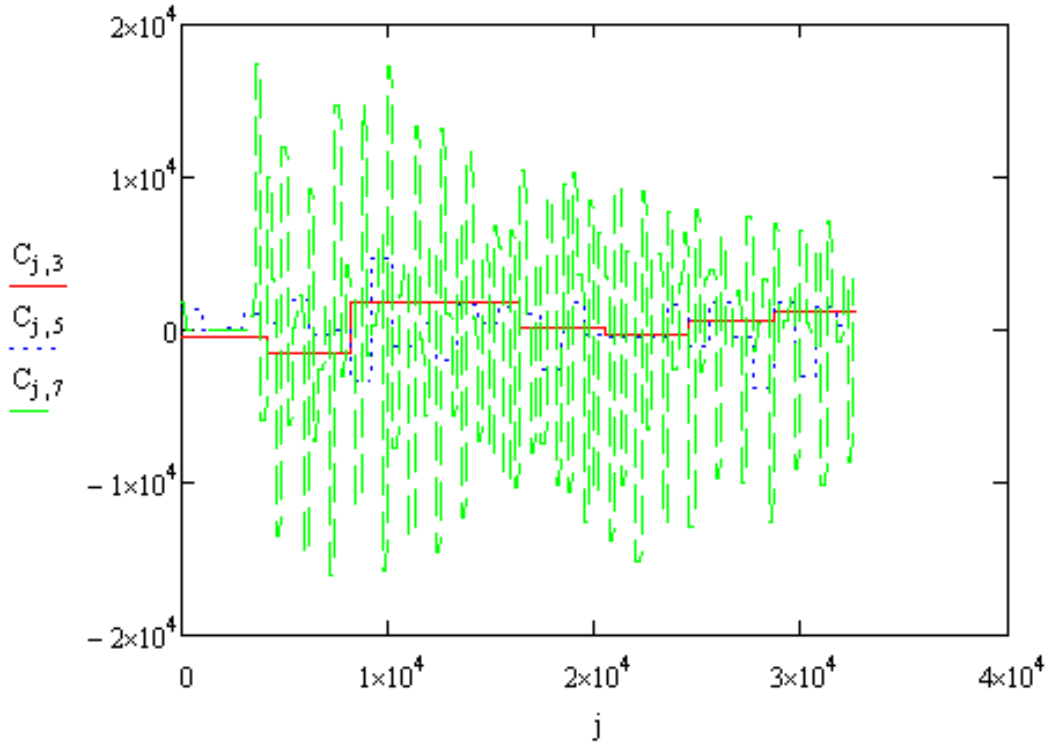


Рис. 13. Визуализация семейств коэффициентов вейвлет-спектра Добеши WAV файла БЕЗ стего (первого канала звукового файла)

Далее приведены результаты стегоанализа корреляционным методом.

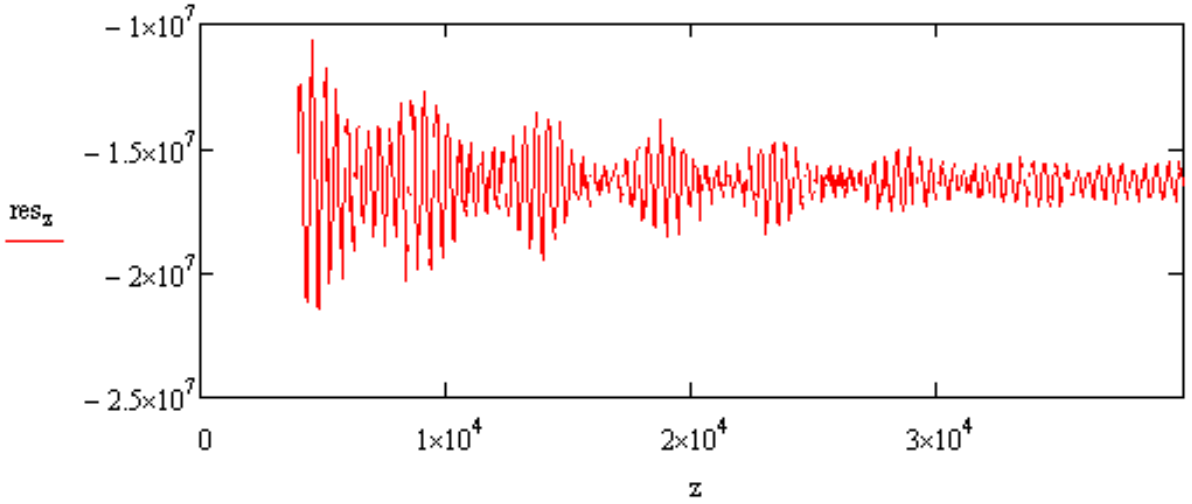


Рис. 13. Функция взаимной корреляции между сигналом – контецнером и сигналом со стего. Отдельные мксимумы позволяют предполагать наличие стего.

Как видно выше, стеганоанализ корреляционным методом приносит свои плоды по крайней мере в случаи применения стеганографического метода LSB и выявляет различия между аудио контейнером без сокрытого в нем сообщения и аудио файлом со стего сообщением внутри.

Делее приведены тексты записываемого и восстанавливаемого стего.

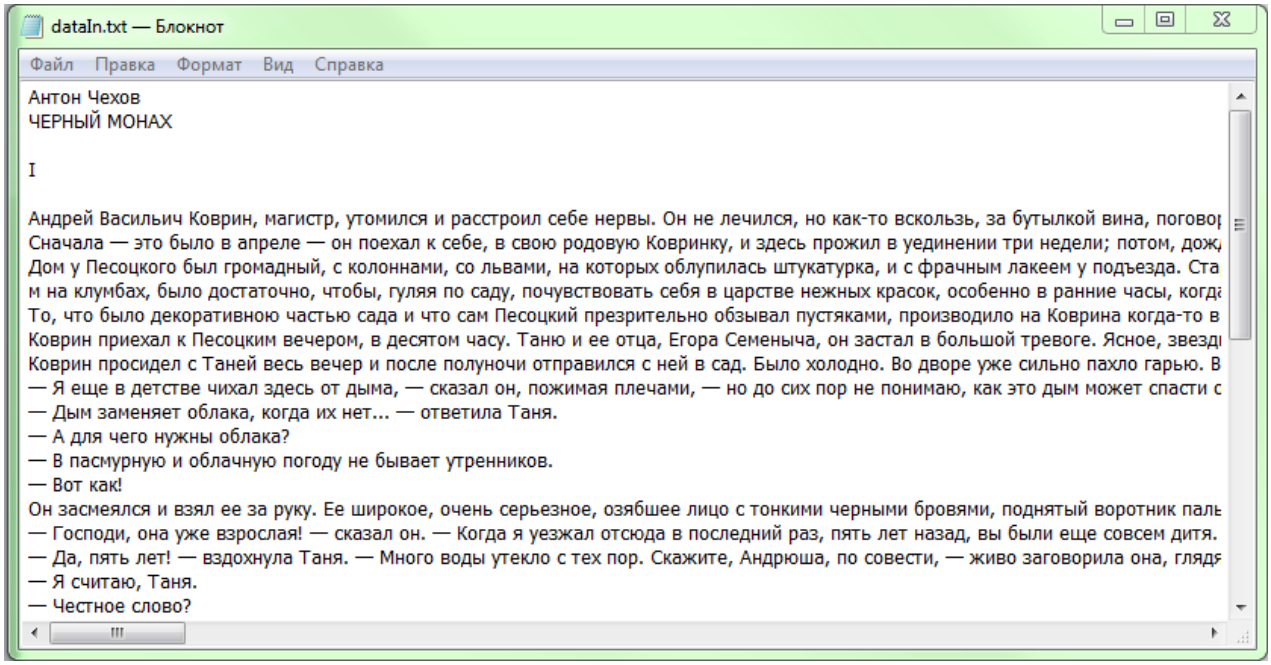


Рис.14. Исходный текст.

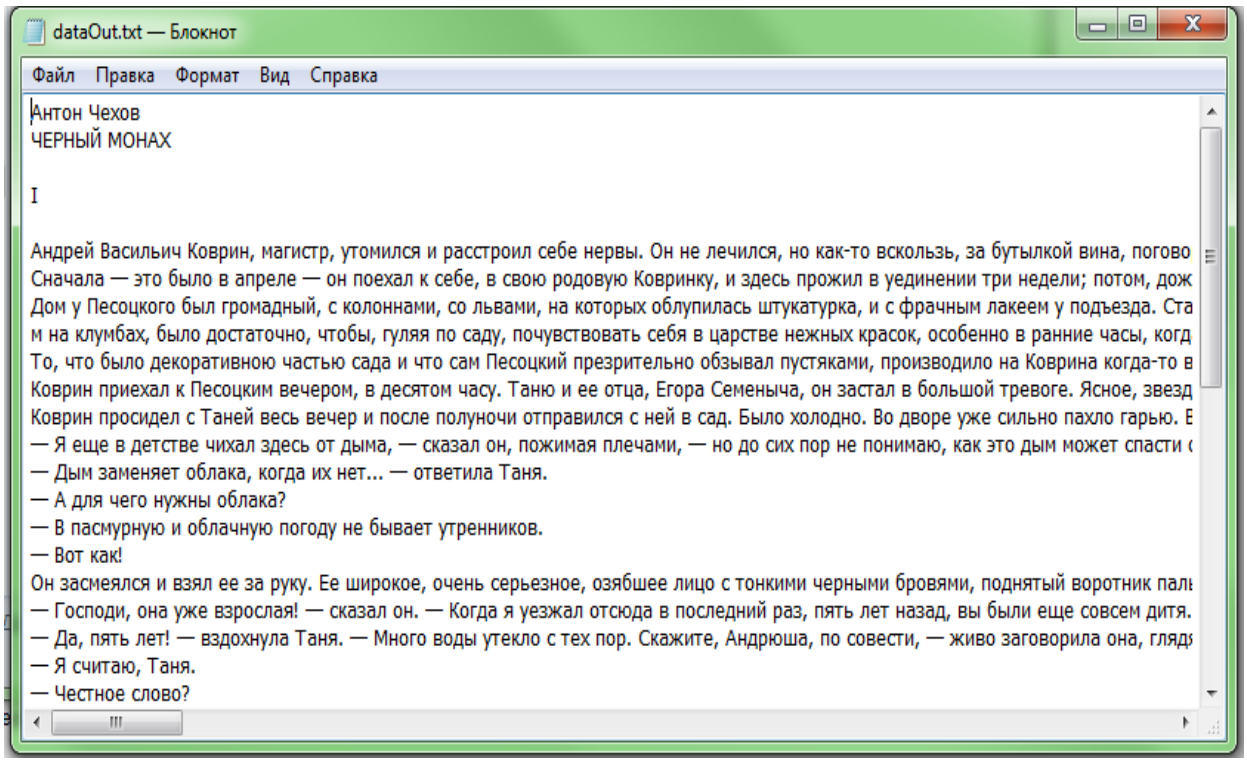


Рис.15. Восстановленное стего.

Рис. 16. Изображение, описываемое функцией взаимной ковариации между функцией, описывающей изображение схемы № 1 и № 2. Размер изображения по вполне понятным причинам значительно уменьшен.

Как видно, результаты вполне удовлетворительны. Можно считать, что предложенный алгоритм достаточно устойчив к атакам, так как для распознавания стего необходимо во – первых, установить метод сокрытия, а затем – определив что восстановить исходное по известному заранее кодирующему изображение «слепой» документации, которое не содержит ничего полезного для злоумышленника.

Все рассмотренные алгоритмы реализуются совместно со стеганографическими алгоритмами сокрытия денных. Это делает предлагаемые алгоритмы наиболее устойчивыми.

Заключение

Проведенный анализ позволяет считать, что проблема ИБ САПР требует отдельного внимания.

- важнешим специфическим фактором обеспечения ИБ САПР является проблема защиты от НСД проектно – эксплуатационной документации.
- Для защиты документации от НСД предлагается коомбинировать стеганографические методы и средства.
- Для защиты от НСД предлагается использовать аудиоконтейнер и сокрытие данных, кодируемых функцией корреляции (или ковариации) изображения шифруемого и известного документов. Предлагается также применять стеганографию для защиты коммерческой тайны особенно для производителей, берущих на себя полную ответственность за разработку, производство, текущее техническое обслуживание (включая ремонт и плановые доработки) в период всего жизненного цикла объекта проектирования.
- Предложенный метод полезен при использовании облачных вычислений, если поставщик услуг не берет на себя ответсвенности за защиту канала связи.

Список литературы

1. Нореков И.П. Разработка систем автоматизированного проектирования: учебник для вузов. М.: Изд-во МГТУ им. Н.Э. Баумана. 1994. 203 с.
2. Волосатова Т.М., Чичварин И.Н. Специфика информационной безопасности САПР // Известия высших учебных заведений. Сер. «Машиностроение». 2012. Спец. выпуск № «Фундаментальные проблемы создания». С. 89 - 94.
3. Мишин Е.Т., Оленин Ю.А., Капитонов А.А. Системы безопасности предприятия – новые акценты // Конверсия в машиностроении. 1998. № 4. С. 5-6.
4. Ефимов А.И. Информационная безопасность ОАО «Газпром»: проблемы гиганта. // Information Security / Информационная безопасность. 2006. № 5. С. 4-6.
5. Программно-аппаратные комплексы защиты информации от НСД // www.accord.ru / Официальный сайт ОКБ САПР. Режим доступа: http://www.accord.ru/documentation.html (дата обращения: 02.04.2014)
6. Волосатова Т.М., Денисов А.В., Чичварин Н.В. Комбинированные методы защиты данных в САПР // Приложение к журналу Информационные технологии. 2012. № 5. С. 1-32.
7. Чичварин Н.В. Сопоставительный анализ областей применения и граничных возможностей характерных стеганографических алгоритмов // Третья всероссийская научно-техническая конференция (Москва, 14 ноября 2012 года) «Безопасные информационные технологии – 2012»: сборник трудов конференции / Минобрнауки

РФ, ФГБОУ ВПО МГТУ им. Н.Э. Баумана; под. общ. ред. В.А. Матвеева. М.: НИИ радиоэлектроники и лазерной техники. 2012. 184 с. С. 174-179.

Сокращения:

АРМ – автоматизированное рабочее место	PLM – жизненный цикл изделия
ИБ – информационная безопасность	ПО – программное обеспечение
КПС – канал передачи сообщений	PLM – технологии сопровождения объекта проектирования в период жизненного цикла
НСД – несанкционированный доступ	ПС – программные средства
ОП – объект проектирования	СЗИ – система информационной безопасности