ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОТКРЫТЫХ КАНАЛОВ ПЕРЕДАЧИ ПРОЕКТНОЙ ДОКУМЕНТАЦИИ, ПРОДУЦИРУЕМОЙ В САПР

Глинская Елена Вячеславовна.,
***Чичварин Николай Викторович**, кандидат технических наук, доцент*

Проведенный анализ различных публикаций показывает, что такие информационные системы как САПР, рассматриваются российскими и иностранными специалистами в области информационной безопасности без учета многих специфичных факторов. Поэтому настоящая публикация представляется актуальной. В работе приводятся результаты авторских разработок нетрадиционных методов стеганографического сокрытия проектной организации. Эти разработки представляются полезными для проектных организаций, разрабатывающих изделия двойного назначения и применяющих их поддержку и сопровождение в период всего жизненного цикла. Приведенные результаты численных экспериментов подтвердили корректность предложенных методов.

***Ключевые слова**: Волоконно – оптическая линия связи, безопасность, защита, информация, криптография, квантовая криптография, несанкционированный доступ, объект проектирования, проектная документация, стеганография.*

INFORMATION SECURITY OPEN CHANNEL DESIGN DOCUMENTATION PRODUCED IN CAD

Elena Glinskaya
***Nicolay Chichvarin**, Ph.D., Associate Professor*

The analysis of various publications shows that information systems such as CAD, considered by Russian and foreign experts in the field of information security and exclude many specific factors. This publication is therefore urgent. The paper presents the results of authoring unconventional methods of steganography conceal the project organization. These developments are useful for project organizations developing dual-use items and apply them support and assistance during the entire life cycle. The presented results of numerical experiments confirmed the correctness of the proposed methods.

***Keywords**: Fiber – optic communication line, safety, protection, information, cryptography, quantum cryptography, unauthorized access, facility design, project documentation, steganography.*

Перечень сокращений:

ВОЛС	волоконно – оптическая линия связи,
ИБ	информационная безопасность
КК	квантовая криптография
КЛС	квантовая линия связи
КПС	канал передачи сообщений
НСД	несанкционированный доступ
ОВ	оптическое волокно
САПР	система автоматизированного проектирования
CALS	сопровождение объекта проектирования в период жизненного цикла изделия
НДВ	недокументированные возможности
СЗИ	система защиты информации

Введение

В настоящее время вопросам безопасности информационных систем уделяется нарастающее внимание. Указ президента В.В. Путина «О концепции национальной безопасности РФ» от 10.01.2000 г. определяет необходимость дальнейших разработок в этом направлении. Если в области безопасности информационных систем уже накоплен большой теоретический и практический опыт, то в области информационной безопасности (ИБ) САПР специальных комплексных разработок не ведется. Проведенный анализ различных публикаций показывает, что такие инфор-

мационные системы, как САПР, рассматриваются российскими и иностранными специалистами в области информационной безопасности без учета многих специфичных факторов.

В публикации под САПР понимаются системы, обозначаемые за рубежом аббревиатурами CALS, CAD/CAM/CAE, CAD/CAM/CAPP, CAD/CAM/PDM, PLM. Большинство средств автоматизированного проектирования, применяемых в отечественных проектных организациях являются зарубежными продуктами. Несмотря на существование эффективных структур сертификации (ФСТЭК и т. п.), обеспечивающих выявление НДВ программных продуктов, защиту от программных и аппаратных закладок, а также (НСД) к корпоративной информации, специфичные особенности ИБ САПР пока учитываются не в полной мере. Как показал анализ публикаций [1-5], проблемы информационной безопасности САПР нарастают и за рубежом. Известно, что у американской аэрокосмической корпорации Lockheed Martin в 1997 году была совершена кража электронных чертежей и информации о конструкции самолета-невидимки Stealth. Еще в 2000 году был обнаружен первый вирус ACAD. Star для программного обеспечения CAD/CAM - AutoCAD. До настоящего времени ни в России, ни за рубежом не найдены методы и средства обеспечения информационной безопасности проекта и объекта проектирования в период всего жизненного цикла объекта (т. е., в условиях применения CALS – технологий). Нет и фундаментальных теоретических исследований в этой области. СЗИ от НСД (например, «Страж NT», «Secret Net», «Security Studio», «Панцирь-К» и т. п.) в полной мере специфику информационной безопасности САПР не учитывают.

Задача защиты проектной документации от несанкционированного доступа условно может быть разделена на три:

- защита документации, составляющей коммерческую тайну;
- защита документации, составляющей государственную тайну;
- защита документации при проектировании изделий двойного назначения по CALS-технологиям

Вторая задача зачастую решается путем использования вычислительных средств, оснащенных сертифицированными программно-аппаратными комплексами, прошедших аттестацию.

Принципиально возможны три метода защиты проектной документации от НСД:

- стеганографический;
- криптографический. При этом возможно использование методов как классической, так квантовой криптографии;
- аппаратный.

Последний метод основан на технической защите КПС, от НСД. По возможности применяются средства защиты как беспроводных, так и проводных КПС. В свою очередь проводные каналы можно классифицировать следующим образом:

- телефонные,
- витая пара,
- ВОЛС.

Централизация всей проектной документации, большое число как внутренних, так и внешних пользователей систем CALS, особенно на заключительном этапе цикла – эксплуатационном – требуют особого внимания к задаче обеспечения ИБ.

В условиях замедления темпов экономического роста, есть соблазн сократить расходы на ИБ в рамках общего сокращения издержек. Однако, согласно отчету KPMG [1], большинство организаций планируют увеличить бюджеты на ИБ в следующем году, что доказывает насколько возросло внимание за последние несколько лет к управлению информационными рисками.

Важная роль в решении задач ИБ отводится международному стандарту ISO17799. Российские предприятия руководствуются также «РД Гостехкомиссии России: Автоматизированные системы. Защита от НСД к информации. Классификация АС и требования по защите информации» и другими документами, рассмотренными в частности в работах [2,3].

Результат внедрения стандарта ISO17799 - система менеджмента информационной безопасности [4,5]. Её цель - сокращение потерь, связанных с нарушением ИБ. В некоторых случаях масштаб потерь может быть таким, что грозит предприятию банкротством. Примером невосполнимой потери может служить CALS-проект высокотехнологичного изделия с длительным циклом разработки и поддержки в эксплуатации.

Говоря о практическом применении стандарта ISO17799, следует иметь ввиду три обстоятельства, которые затрудняют его непосредственное использование.

Во-первых, рекомендации стандарта в ряде случаев являются весьма общими.

Во-вторых, в организации, как правило, уже существует определенная система процессов, в которую необходимо интегрировать процесс управления безопасностью.

В третьих, реализации стандарта ISO17799 характеризуются определенной статичностью, что не позволяет им достаточно оперативно следовать постоянным изменениям в информационных технологиях (ИТ).

В настоящей публикации приводятся результаты исследований возможности защиты проектной документации от НСД с применением методов квантовой криптографии.

1. Цель и задачи исследований

При подготовке материалов статьи авторы провели исследования, целью которых была разработка предложений по модификации известного протокола BB84 для повышения криптоустойчивости квантовых линий связи. Для достижения поставленной цели последовательно решены следующие задачи:

Проведение аналитического литературного обзора методов и протоколов КК.

Анализ уязвимостей КЛС.

Анализ проводных и беспроводных линий связи, используемых в КК.

Разработка собственно предложений.

2. Анализ известных методов и средств передачи сообщений, шифруемых с применением КК с учетом специфики решаемых задач. Описание принципа возможной модификации.

В дальнейшем в публикации рассматривается КПС, схема которого приведена на рисунке 1.

Различают две компоненты проектной документации:

- графическая. Причем чертежи могут быть представлены как в векторном, так и растровом формате.
- текстовая (включая программы для микропроцессоров, однокристальных ЭВМ, ПЛИС).

Во всех случаях передаче подлежит последовательность битов, поэтому далее рассматриваются протоколы и алгоритмы шифрования проектной документации, передаваемой по открытым КПС.

Рассмотрим основной криптографический протокол, применимый к КПС.

2.1 Протокол BB84 [2]**.**

Как известно, носителями кода в протоколе BB84 являются фотоны, поляризованные под углами 0, 45, 90, 135 градусов. Применяются два ортогональных состояния: если известно, что фотон поляризован либо вертикально, либо горизонтально, то путем измерения, можно установить — как именно; то же самое можно утверждать относительно поляризации под углами 45 и 135 градусов. Однако с абсолютной достоверностью отличить вертикально поляризованный фотон от фотона, поляризованного под углом 45, принципиально невозможно. В основу протокола квантового распространения ключа заложено следующие действия Индуктора и Перципиента:

- Индуктор посылает Перципиенту фотон в одном из поляризованных состояний (0, 45, 90, 135 градусов) и записывает угол поляризации. Отсчет углов ведется от направления «вертикально вверх» по часовой стрелке.
- Перципиент, располагающий двумя анализаторами - вертикально-горизонтальной поляризацию, и диагональной, для каждого фотона случайно выбирает один из анализаторов и записывает тип анализатора и результат измерений.
- По открытому каналу связи Перципиент сообщает Индуктору, какие анализаторы использовались, но не сообщает, какие результаты были получены.
- Индуктор по открытому каналу связи сообщает Перципиенту, какие анализаторы он выбрал правильно. Фотоны, для которых Перципиент неверно выбрал анализатор, отбрасываются. Если бы производился НСД при помощи оборудования, подобного оборудованию Перципиента, то примерно в 50 процентах случаев будет выбран неверный анализатор и невозможно определить состояние полученного фотона, и отправление фотона Перципиенту произойдет в состоянии, выбранном наугад. При этом в половине случаев будет выбрана неверная поляризация и примерно в 25 процентах случаев результаты измерений Перципиента могут отличаться от результатов Индуктора. Для обнаружения перехвата Индуктор и

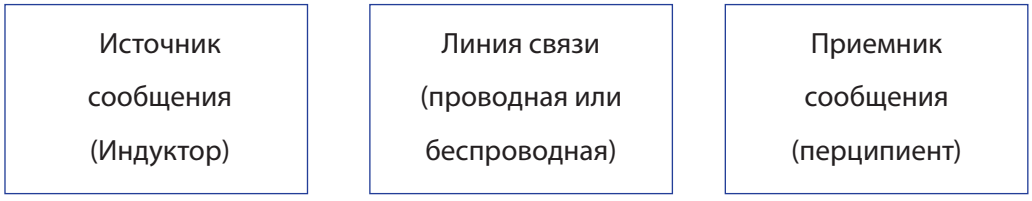


***Рис. 1**. Схема КПС*

Перципиент выбирают случайный участок ключа и сравнивают его по общедоступному каналу связи. Если процент ошибок велик, то он может быть отнесен на счет результатов НСД, и процедура повторяется сначала. Анализ результатов обзора показывает, что на практике дополнительно применяются специальные протоколы для коррекции ошибок при передаче, а также протокол усиления секретности (privacy amplification), позволяющий с высокой вероятностью устранить из ключа информацию, которая могла быть перехвачена. Однако на общность получаемых далее результатов это никак не влияет. Известен протокол Экерта, позволяющий обеспечивать скрытность распространения и хранения ключа, основанный на эффекте сцепления квантовых частиц. В нем используется следующее свойство сцепленных частицы: если произвести измерение одной из них, то другая (на каком бы расстоянии она ни находилась) обязательно «перейдет» в состояние, противоположное состоянию первой частицы. Важным свойством любого протокола, является то, что в качестве физического носителя сигнала выступает фотон. Перехват любого фотона становится известным Перципиенту.

При этом Индуктор может получить по открытому каналу сообщение о том, что произошла утечка информации. Таким образом, при передаче вначале «провокационного сообщения» можно учесть факт НСД в КПС. Сказанное позволяет считать, что квантовая криптография имеет несомненное преимущество перед криптографией классической. Кроме, того, применение протоколов КК в этом случае никак не регламентируется, и на них не распространяются ограничения спецслужб.

2.2 Сопоставление стеганографических и криптографических методов шифрования для обеспечения ИБ САПР/PLM

Очевидным преимуществом стеганографических методов сокрытия сообщений является то, что их применение позволяет сделать неизвестным сам факт сокрытия. Стеганографические алгоритмы относительно просто реализуются. Однако, поскольку число вариантов построения стеганографических алгоритмов конечно, решить задачу распознавания сокрытых данных.

Тем не менее, применение специальных методов, основанных на использовании цифровой голографии, искусственной дефокусировки, и т. д., делает число вариантов бесконечным. Это показано авторами в [6-16].

3. Описание комбинированных стеганографических методов

Далее рассмотрены описания голографического, корреляционного метода и метода, применяющего искусственную дефокусировку.

3.1 Голографический метод

Рассмотрим результаты численного эксперимента, проведенного с применением программы, реализующей алгоритм формирования и восстановления цифровой Фурье-голограммы.

На рисунке 2 приведено изображение маскируемой документации.

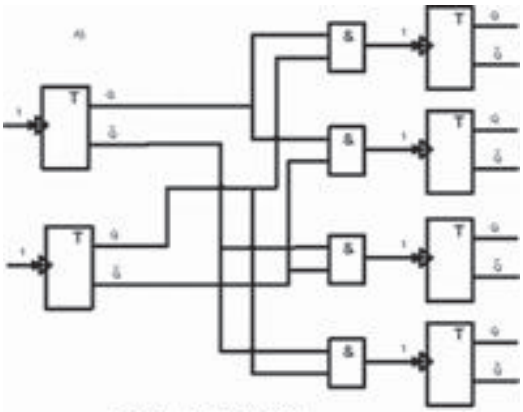


***Рис. 2**. Схема голографируемой документации*

На рисунке 3 приведено изображение соответствующей голограммы.

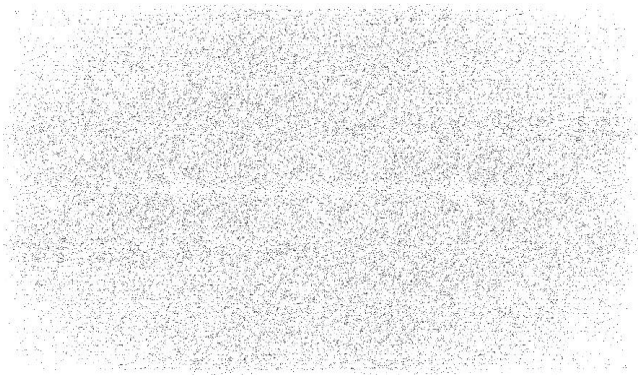


***Рис. 3.** Изображение Фурье – голограммы изображения, приведенного на Рис.2*

Второй алгоритм также реализуется двумя этапами:

- вычисление корреляционной функции, моделирующей распределение контраста в изображении шифруемой схемы с функцией, моделирующей распределение контраста в изображении кодирующей схемы («слепой» схемы). Авторы предложили применять вычисление свертки при вычислении корреляционной функции, поскольку в данном случае изображения кодируются веще-

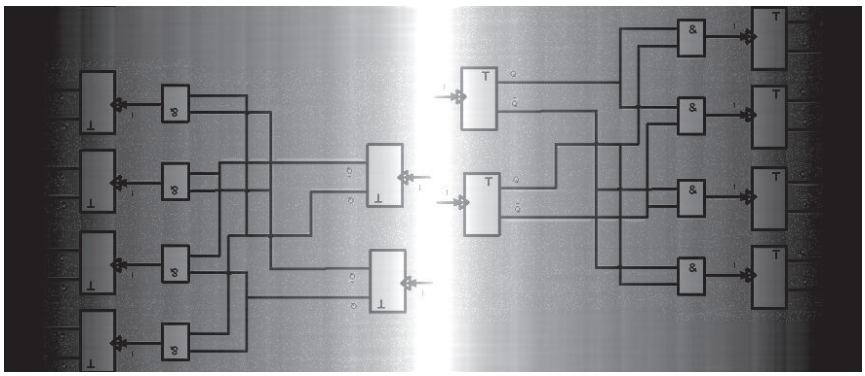


Рис. 4. Восстановленная голограмма

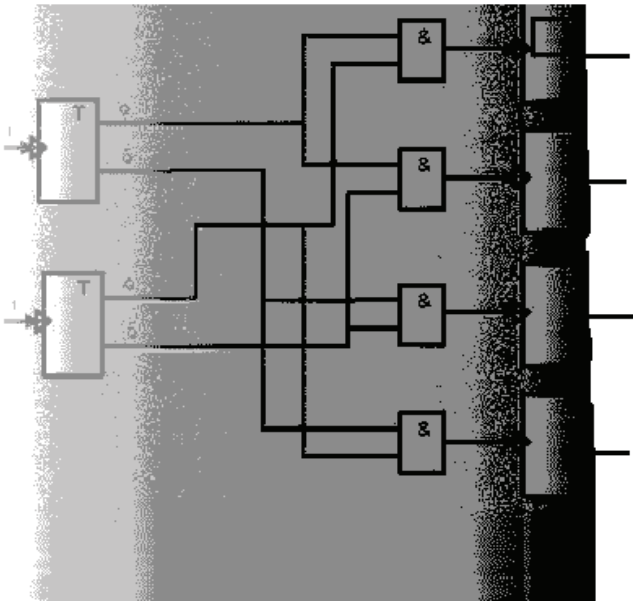


***Рис. 5**. Не полностью препарированное восстановленное изображение голограммы*

ственными функциями.

• внедрение результата первого этапа в контейнер любым из известных методов стеганографии.

Так же, как и в первом алгоритме, восстановление изображения зашифрованной документации осуществляется в порядке, обратном процессу шифровки, т. е. решается обратная задача.

***Рис. 6** Фурье-голограмма (слева – без модификаций)*

На рисунке 5 приведены результаты эксперимента по оценке стойкости предлагаемого метода. Отчетливо видно, что значительные искажения контейнера со стегофайлом не приводят к значительному ухудшению восстановленных данных. Показано, что Фурье–голограмма, обладая большей избыточностью, позволяет восстановить ЦВЗ в лучшем качестве, нежели косинусная голограмма.

На рисунке 7 показано изображение-контейнер со встроенной голограммой (Фурье и косинусной), значительная часть которого вырезана. Несмотря на это, восстанавливаемый ЦВЗ еще читаем. Особенно актуален данный аспект тем, что при встраивании голограммы в изображение-контейнер, последний может иметь области, которые не пригодны для встраивания, или области, которые при печати на аналоговые носители утрачиваются. Кроме того, применение голограмм позволяет заполнять контейнер наполовину.

Рис. 7. *Изображение-контейнер со встроенной косинусной и Фурье голограммами. Верхний ряд соответствует косинусной голограмме. Справа – удалена часть изображения контейнера*

3.2 Метод сокрытия данных с использованием искусственной дефокусировки

Формально оба метода – настоящий и рассмотренный выше объединяет то, что на первой стадии сокрытия данных используются оптические аналогии. Важнейшим элементом их сходства и отличием от известных является то, что на первой стадии сокрытия возможна аппаратная реализация как Фурье-голограммы, так и сканера с искусственной дефокусировкой.

Суть предлагаемого метода заключается в следующем: 1) на первой стадии регистрируется изображение защищаемого документа либо с использованием искусственно расфокусированным известным образом устройством ввода в ЭВМ. Решается так называемая прямая задача (конволюции); 2) на второй стадии производится формирование стеганограммы с использованием какого-либо предпочтительного метода стеганографии.

При санкционированном доступе к защищенным данным последовательность действий имеет обратный порядок: 1) на первой стадии по известному ключу из заполненного контейнера извлекается стего в виде «размытого» изображения. Решается так называемая обратная задача (деконволюции) – восстановление дефокусированного изображения документа.

Реализация метода

Для большинства реальных систем и, особенно, в случае моделирования дефокусировки на ЭВМ это уравнение можно записать в виде интегрального уравнения Фредгольма I рода типа свертки:

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

В качестве математической модели дефокусированной системы используется интегральное уравнение типа свертки. Уравнение применено для 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 $\mathrm{k}(*\ ,\ *)$, 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 оптической передаточной функцией.

Однако прямое алгебраическое решение уравнения простым делением невозможно – функция $\mathrm{K}(*\ ,\ *)$ 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, .* 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 рисунках 4 и 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.8). В противном случае восстановление потребует затрат больших ресурсов.

3.3 Корреляционный метод сокрытия изображений

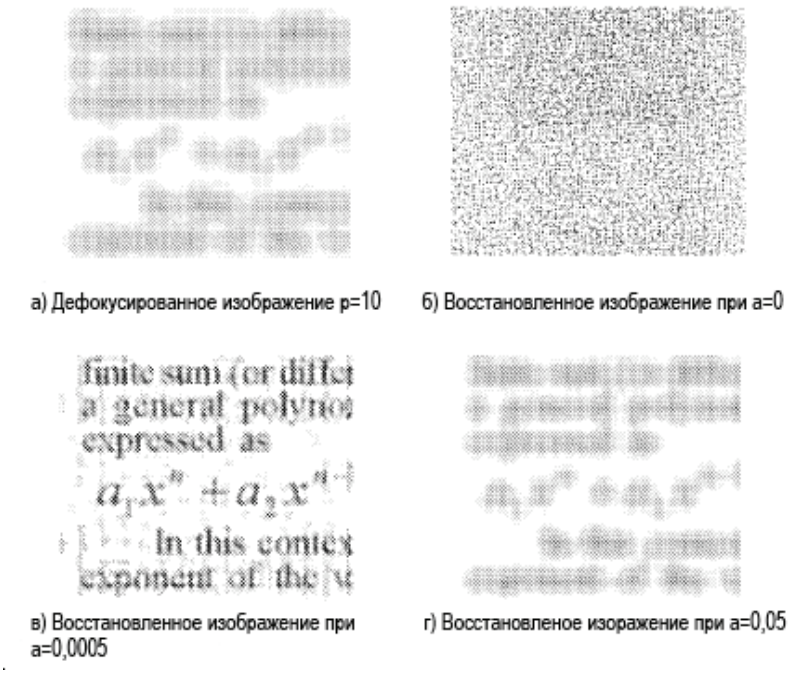
Поскольку вычисления корреляционной и ковариационной с применением БПФ аналогичны, далее не делается между ними.

Примеры решения задачи вычисления ковариационной функции и результат деконволюции приведены на рисунках 5, 6 ,7 и 8.

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. Для оценки эффективности предложенных алгоритмов авторами проведена серия численных экспериментов. Результаты приведены в таблице 1.

Анализ показал, что главным достоинством криптогафических методов является их абсолютная криптоустойчивость. Недостатком – сложность и дорговизна реализации.



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. 8.

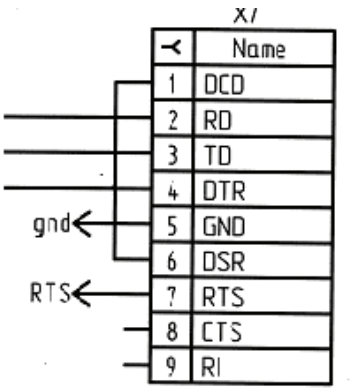


Рис. 9. *Исходное (шифруемое) изображение*

Рис. 10. *Зашифрованное изображение*

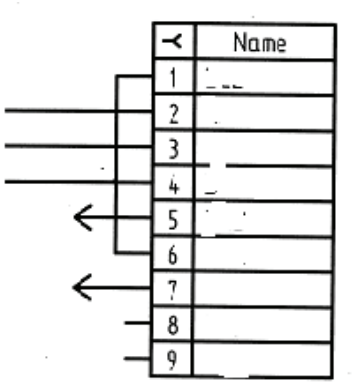


Рис. 11. *Кодирующее изображение («слепая» распиновка)*

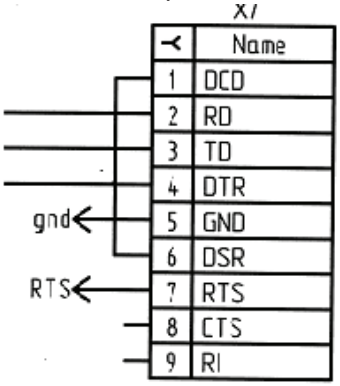


Рис12. *Восстановленное изображение*

Таким образом, можно считать, что для сохранения коммерческой тайны предпочтительнее применять стеганографические методы, а для сохранения тайны государственной – методы криптографии. Для сохранения тайны проектной документации на изделия двойного назначения целесообразно применять методы квантовой криптографии.

4. Описание предлагаемого метода защиты проектной документации от НСД

Атаки на канал тесно связаны с конкретной физической реализацией квантовой криптографической линии и теми лазейками, которые она предоставляет для перехватчика. Для перехвата информации перхватчик должен совершить квантовое измерение. Квантовое измерение может быть прямым, когда квантовая система непосредственно взаимодействует с измерительным аппаратом, или косвенным, когда квантовая система взаимодействует с пробной системой, которая впоследствии подвергается прямому измерению. Соответственно, перехватчик может незаметно отключить квантовый канал, заменив его эквивалентным генератором шума.

Одним из перспективных способов увеличения скрутности передачи сигналов в ВОЛС, как отмечалось, представляется разнесение фотонов со спинами, кодирующими нули и единицы по коаксиальным, либо параллельным линиям связи. Во втором случае представляется перспективным применение многомодового лазерного излучения с передачей сообщений в многомодовых ОВ. Представляет интерес следующий способ увеличения полосы пропускания ВОЛС, который применим для КЛС.

Формула изобретения:

«Способ увеличения полосы пропускания многомодовой волоконно-оптической линии передачи, заключающийся в том, что последовательно с основным многомодовым оптическим волокном в линии передачи включают компенсирующее многомодовое оптическое волокно, профиль которого выбирают в зависимости от профиля основного многомодового оптического волокна, отличающийся тем, что глубину, ширину и форму осевого провала профиля показателя преломления компенси-

Таблица 1. *Результаты экспериментальных исследований при сопоставительном анализе стеганографических алгоритмов.*

№ п/ п	Наименование	у/ш*	у/и*	Ск.1*	Ск.2*
1	Алгоритм LSB	-	-	+	+
2	Алгоритм Куттера	-	-	+	+
3	Алгоритм Брундокса	-	+	+	+
4	Алгоритм Ленгелаара	-	-	+	+
5	Алгоритм Питаса	-	-	+	+
6	Алгоритм Роджена	-	-	+	+
7	Алгоритм PatchWork	-	-	+	+
8	Алгоритм Бендера	-	+	+	+
9	Алгоритм Коча	-	+	+	+
10	Алгоритм Подилчука	+	+	+	+
11	Алгоритм Кокса	+	+	+	+
12	Аддитивные алгоритмы	+	+	+	+
13	Алгоритм Бенхама	+	+	+	+

Условные обозначения:
у/ш – устойчивость к шумам
у/и - устойчивость к искажениям
ск.1 – преимущество 1 комбинированного алгоритма в скорости по отношению к классическому алгоритму (LSB)

рующего многомодового оптического волокна выбирают так, чтобы дифференциальная модовая задержка между группами мод низшего порядка и группами мод высшего порядка в основном многомодовом оптическом и компенсирующем многомодовом оптическом волокнах имела противоположные знаки. Устройство, реализующее способ, содержит основное многомодовое оптическое волокно линии связи, которое последовательно соединено с компенсирующим многомодовым оптическим волокном, реализует способ следующим образом. Соотношение между скоростями распространения группы мод низшего порядка и скоростями распространения группы мод высшего порядка в многомодовом оптическом волокне с провалом профиля показателя преломления по оси зависит от параметров провала профиля, его глубины, ширины и формы (Рис. 9)».

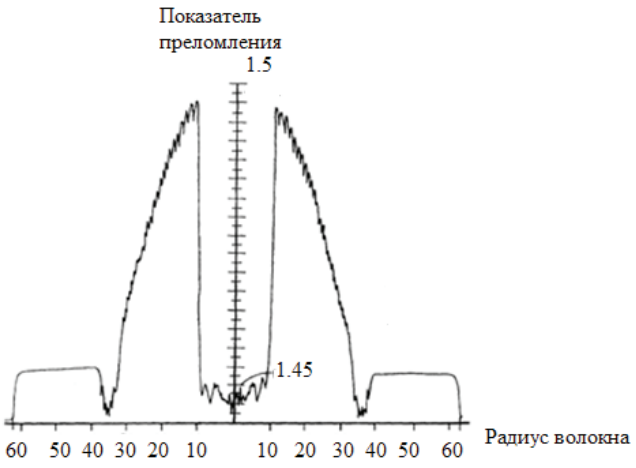


Рис.13. *Профиль показателя преломления многомодового оптического волокна*

Для одних значений параметров быстрее распространяются низшие моды, для других - высшие. Соответственно, выбирая параметры провала профиля показателя многомодового оптического волокна можно добиться заданного соотношения между скоростями распространения группы мод низшего порядка и группы мод высшего порядка. Параметры профиля показателя преломления компенсирующего волокна, а имен-

но глубину, ширину и форму осевого провала выбирают так, чтобы дифференциальная модовая задержка компенсирующего волокна была противоположна по знаку дифференциальной модовой задержке основного волокна, что обеспечивает уменьшение (компенсацию) дифференциальной модовой задержки в последовательном соединении таких волокон. Таким образом, в многомодовой волоконно-оптической линии передачи, в которой последовательно соединены основное и компенсирующее волокна и профиль компенсирующего волокна выбран согласно данному способу, за счет компенсации дифференциальной модовой задержки увеличивается полоса пропускания линии передачи.

Поскольку способ предусматривает компенсацию дифференциальной модовой задержки, он может быть использован для увеличения полосы пропускания многомодовой волоконно-оптической линии передачи с многомодовыми оптическими волокнами, профиль которых имеет провал по оси.

Заключение

Проведенные исследования, основные результаты которых изложены в публикации, позволяют сделать следующие выводы:

Проведено сопоставление принципов и областей применения комбинированных методов сокрытия данных.

Показано, что крипптостойкость КПС может быть существенно повышена путем параллельной или коаксиальной передачи единиц и нулей кода сигнала.

Показано, что разнесение кода в ВОЛС возможно с применением многомодового ОВ.

Показано, что разнесение кода в беспроводных линиях связи возможно с применением многомодового лазерного излучения.

Предлагается использовать эффект возникновения второй гармоники в лазерах и нелинейных кристаллах.

Предложена методика проектирования линии связи с предложенной модификаций криптографического протокола.

Литература:

1. Официальный сайт фирмы The Insitu Group Inc [Электронный ресурс]. Режим доступа: http://www.insitu.com/systems/launch-and-recovery/launch-systems (дата обращения 20.05.2013).
2. Точилов Л.С., Крылов Е.С. Стратегия развития инфраструктуры сервисов IT-подразделений высокотехнологичного предприятия// 2-ая международная конференция CAD/CAM/PDM: труды. (Москва, 2002). М.: Институт проблем управления РАН. С. 270-274.
3. Точилов Л.С. Информационная безопасность и корпоративные сети. М.: Корпорация «Галактика», 1999. 36 с.
4. Точилов Л.С. Управление безопасностью на примере Федеральной резервной системы США. 2003. Режим доступа: http://lstochilov.narod.ru (дата обращения 02.03.13).
5. OGC. IT Infrastructure Library. Best Practice for Security Management. London: TSO. 2002. 124 с.
6. Хузина Э.И. Экспериментальные исследования алгоритма стеганографического сокрытия данных методом катера // Сборник трудов Третьей всероссийской научно-технической конференции «Безопасные информационные технологии». (Москва, 2012). М.: МГТУ им. Н.Э. Баумана. С. 169-172.
7. Чичварин Н.В. Сопоставительный анализ областей применения и граничных возможностей характерных стеганографических алгоритмов // Сборник трудов Третьей всероссийской научно-технической конференции «Безопасные информационные технологии». (Москва, 2012). М.: МГТУ им. Н.Э. Баумана. С. 174-179
8. Ларионцева Е.Л., Стельмашук Н.Н. Экспериментальные исследования эффективности стеганографического алгоритма, реализующего метод lsb // Сборник трудов Третьей всероссийской научно-технической конференции «Безопасные информационные технологии». (Москва, 2012). М.: МГТУ им. Н.Э. Баумана. С. 94-96.
9. Логинов К.Е. Экспериментальные исследования устойчивости алгоритма стеганографического сокрытия данных методом langelaar при воздействиях на стегоконтейнер // Сборник трудов Третьей всероссийской научно-технической конференции «Безопасные информационные технологии». (Москва, 2012). М.: МГТУ им. Н.Э. Баумана. С. 99-101.
10. Сиволапов А. С. Исследование влияния контейнера на качество сокрытия сообщений методом Langelaar // Сборник трудов Третьей всероссийской научно-технической конференции «Безопасные информационные технологии». (Москва, 2012). М.: МГТУ им. Н.Э. Баумана. С. 153-155.
11. Круглая Е.И., Пилипенко А.В. Защита данных в САПР: анализ стеганографических алгоритмов коча (koch) и

бенхама (benham) // Сборник трудов Третьей всероссийской научно-технической конференции «Безопасные информационные технологии». (Москва, 2012). - М.: МГТУ им. Н.Э. Баумана. С. 87-90.
12. Максимов Р.Л. Экспериментальное исследование эффективности стеганографического алгоритма, реализующего метод брайндонкса (bruyndonckx) // Сборник трудов Третьей всероссийской научно-технической конференции «Безопасные информационные технологии». (Москва, 2012). М.: МГТУ им. Н.Э. Баумана. С. 101-105.
13. Гончаров И.О., Заикин М.А. Экспериментальные исследования стеганографического метода эхо-кодирования // Сборник трудов Третьей всероссийской научно-технической конференции «Безопасные информационные технологии». (Москва, 2012). М.: МГТУ им. Н.Э. Баумана. С. 45-48.
14. Иванова Е.Ю. Обзор атак на стегоалгоритм patchwork и методов противодействия // Сборник трудов Третьей всероссийской научно-технической конференции «Безопасные информационные технологии». (Москва, 2012). М.: МГТУ им. Н.Э. Баумана. С. 66-69.
15. Волосатова Т.М., Денисов А.В., Чичварин Н.В. Комбинированные методы защиты данных в САПР // Информационные технологии. Приложение. 2012, №5. С.1- 32.
16. Волосатова Т.М., Денисов А.В., Чичварин Н.В. Защита проектной документации от несанкционированного доступа // 9 Международная конференция «Эффективные методы автоматизации подготовки и планирования производства»: труды. (Москва, 2012). М.: МГТУ им. Н.Э. Баумана. С.141-144.
17. Real-time Watermarking Techniques for Compressed Video Data // Langelaar, Gerrit Cornelis - Thesis Delft University of Technology.(Veenendaal, 2000). V.: Universal Press. 136 c.
18. Bruyndonckx O., Quisquater J.-J., Macq B.Spatial method of copyright labeling of digital images // IEEE Workshop on Nonlinear Images/Signal Processing, Thessal. 1995, June , PP.19-27.
19. Bender B., Morimoto N., Lu, Methods of hiding data // IBM System Journal, 1996, July. PP.25-33.

References:

1. Ofitcial`ny`i` sai`t firmy` The Insitu Group Inc [E`lektronny`i` resurs]. Rezhim dostupa: http://www.insitu.com/systems/launch-and-recovery/launch-systems (data obrashcheniia 20.05.2013).
2. Tochilov L.S., Kry`lov E.S. Strategiia razvitiia infrastruktury` servisov IT-podrazdelenii` vy`sokotekhnologichnogo predpriiatiia// 2-aia mezhdunarodnaia konferentciia CAD/CAM/PDM: trudy`. (Moskva, 2002). M.: Institut problem upravleniia RAN. C. 270-274.
3. Tochilov L.S. Informatcionnaia bezopasnost` i korporativny`e seti. M.: Korporatciia «Galaktika», 1999. 36 s.
4. Tochilov L.S. Upravlenie bezopasnost`iu na primere Federal`noi` rezervnoi` sistemy` SSHA. 2003. Rezhim dostupa: http://lstochilov.narod.ru (data obrashcheniia 02.03.13).
5. OGC. IT Infrastructure Library. Best Practice for Security Management. London: TSO. 2002. 124 c.
6. Huzina E`.I. E`ksperimental`ny`e issledovaniia algoritma steganograficheskogo sokry`tiia danny`kh metodom katera // Sbornik trudov Tret`ei` vserossii`skoi` nauchno-tekhnicheskoi` konferentcii «Bezopasny`e informatcionny`e tekhnologii». (Moskva, 2012). M.: MGTU im. N.E`. Baumana. S. 169-172.
7. Chichvarin N.V. Sopostavitel`ny`i` analiz oblastei` primeneniia i granichny`kh vozmozhnostei` harakterny`kh steganograficheskikh algoritmov // Sbornik trudov Tret`ei` vserossii`skoi` nauchno-tekhnicheskoi` konferentcii «Bezopasny`e informatcionny`e tekhnologii». (Moskva, 2012). M.: MGTU im. N.E`. Baumana. S. 174-179
8. Lariontceva E.L., Stel`mashuk N.N. E`ksperimental`ny`e issledovaniia e`ffektivnosti steganograficheskogo algoritma, realizuiushchego metod lsb // Sbornik trudov Tret`ei` vserossii`skoi` nauchno-tekhnicheskoi` konferentcii «Bezopasny`e informatcionny`e tekhnologii». (Moskva, 2012). M.: MGTU im. N.E`. Baumana. S. 94-96.
9. Loginov K.E. E`ksperimental`ny`e issledovaniia ustoi`chivosti algoritma steganograficheskogo sokry`tiia danny`kh metodom langelaar pri vozdei`stviiakh na stegokontei`ner // Sbornik trudov Tret`ei` vserossii`skoi` nauchno-tekhnicheskoi` konferentcii «Bezopasny`e informatcionny`e tekhnologii». (Moskva, 2012). M.: MGTU im. N.E`. Baumana. S. 99-101.
10. Sivolapov A. S. Issledovanie vliianiia kontei`nera na kachestvo sokry`tiia soobshchenii` metodom Langelaar // Sbornik trudov Tret`ei` vserossii`skoi` nauchno-tekhnicheskoi` konferentcii «Bezopasny`e informatcionny`e tekhnologii». (Moskva, 2012). M.: MGTU im. N.E`. Baumana. S. 153-155.
11. Kruglaia E.I., Pilipenko A.V. Zashchita danny`kh v SAPR: analiz steganograficheskikh algoritmov kocha (koch) i benhama (benham) // Sbornik trudov Tret`ei` vserossii`skoi` nauchno-tekhnicheskoi` konferentcii «Bezopasny`e

informatcionny`e tekhnologii». (Moskva, 2012). - M.: MGTU im. N.E`. Baumana. S. 87-90.
12. Maksimov R.L. E`ksperimental`noe issledovanie e`ffektivnosti steganograficheskogo algoritma, realizuiushchego metod brai`ndonksa (bruyndonckx) // Sbornik trudov Tret`ei` vserossii`skoi` nauchno-tekhnicheskoi` konferentcii «Bezopasny`e informatcionny`e tekhnologii». (Moskva, 2012). M.: MGTU im. N.E`. Baumana. S. 101-105.
13. Goncharov I.O., Zaikin M.A. E`ksperimental`ny`e issledovaniia steganograficheskogo metoda e`ho-kodirovaniia // Sbornik trudov Tret`ei` vserossii`skoi` nauchno-tekhnicheskoi` konferentcii «Bezopasny`e informatcionny`e tekhnologii». (Moskva, 2012). M.: MGTU im. N.E`. Baumana. S. 45-48.
14. Ivanova E.Iu. Obzor atak na stegoalgoritm patchwork i metodov protivodei`stviia // Sbornik trudov Tret`ei` vserossii`skoi` nauchno-tekhnicheskoi` konferentcii «Bezopasny`e informatcionny`e tekhnologii». (Moskva, 2012). M.: MGTU im. N.E`. Baumana. S. 66-69.
15. Volosatova T.M., Denisov A.V., Chichvarin N.V. Kombinirovanny`e metody` zashchity` danny`kh v SAPR // Informatcionny`e tekhnologii. Prilozhenie. 2012, №5. S.1- 32.
16. Volosatova T.M., Denisov A.V., Chichvarin N.V. Zashchita proektnoi` dokumentatcii ot nesanktcionirovannogo dostupa // 9 Mezhdunarodnaia konferentciia «E`ffektivny`e metody` avtomatizatcii podgotovki i planirovaniia proizvodstva»: trudy`. (Moskva, 2012). M.: MGTU im. N.E`. Baumana. S.141-144.
17. Real-time Watermarking Techniques for Compressed Video Data // Langelaar, Gerrit Cornelis - Thesis Delft University of Technology.(Veenendaal, 2000). V.: Universal Press. 136 c.
18. Bruyndonckx O., Quisquater J.-J., Macq B.Spatial method of copyright labeling of digital images // IEEE Workshop on Nonlinear Images/Signal Processing, Thessal. 1995, June , PP.19-27.
19. Bender B., Morimoto N., Lu, Methods of hiding data // IBM System Journal, 1996, July. PP.25-33.