Уважаемый председатель, члены специализированного ученого совета, приглашенные. Вашему вниманию предлагается доклад, содержащий основные положения диссертационной работы на тему**: «структурно-стеганографическое кодирования с плавающим базисом встраивания для повышения безопасности информационных ресурсов».**

«после того как озвучена тема, сразу идет показ слайда 2»

Развитие информационно-телекомунникационных технологий для систем критического назначения сопровождается необходимостью повышения безопасности информационных ресурсов.

Актуальность такого подхода обосновывается развитием существующих прикладных сфер, а также диктуется необходимостью поддержки информационного обеспечения в условиях кризисных ситуаций на рис. 1 слайда 3.

В тоже время повышаются угрозы со стороны злоумышленника относительно нарушения категорий конфиденциальности и целостности информационного ресурса, что обусловлено факторами, приведенными на рис. 2 слайда 4.

Поэтому повышение безопасности специальных информационных ресурсов в инфокоммуникационных системах является актуальной ***научно-прикладной задачей***.

Неудовлетворительный уровень безопасности специальных информационных ресурсов имеет негативные информационно-пропагандистские последствия, и наносит ущерб политическому и экономическому имиджу государства.

Поэтому наряду с криптогафическими методами защиты специальной информации требуется использовать методы стеганографии на основе использования цифрового изображения в качестве контейнера. Функциональная схема реализации скрытой передачи данных на основе использования компьютерной стеганографии представлены на рис 3 слайда 4.

Классификация существующих методов стеганографии представлена на рис. 4 слайда 5. Соответственно показатели для оценки эффективности методов стеганографического преобразования представлены на слайде 6 формулами 1-3, а именно: относительная стеганографическая емкость стеганографической системы, вероятность безошибочного изъятия встроенных данных авторизированным пользователем, пиковое отношение сигнал-шум изображения со встроенными данными. По этим показателям предпочтительными являются методы непосредственного встраивания ***специальной***информации.

Среди таких методов наиболее широко используемыми на практике являются методы встраивания в наименее значимый бит и методы на основе расширения спектра. При анализе эффективности стеганографических методов необходимо учитывать возможность применения злоумышленником активных и пассивных атак в условиях кризисных ситуаций.

Оценка методов стеганографических преобразований по относительной стеганографической емкости системы представлена в таблице 1 слайда 7. Откуда видно, что значение относительной стеганографической емкости принимает значение от 0,78 до 6,25 %. Оценка по вероятности безошибочного изъятия встроенных данных в условиях отсутствия атак приведена на рис. 5 слайда 8. Откуда замечаем, что значение вероятности безошибочного изъятия встроенных данных в условиях отсутствия атак принимает значение от 0,5 до 0,6. Оценка по количеству безошибочно изъятых бит встроенных данных в условиях применения противником атак рассматривается на рис.6 слайда 7. Это позволяет сделать вывод, что количество безошибочно изъятых бит принимает значение 50 %.

Значит, существующие технологии стеганографических преобразований не обеспечивают в полной мере системных требований в критических условиях с активным противостоянием противнику.

Отсюда, ***цель исследований*** заключается в разработке метода повышения безопасности специальной информации для инфокоммуникационных систем на основе стеганографических преобразований.

***Рассмотрим решение первой задачи***

***Предлагается*** использовать кодообразующую функцию для неравновесного позиционного числа. Структурная схема такого похода задана на рис 7. слайда 9.

Имплантации элемента скрываемого сообщения проводится в неравновесное позиционное число выражение 4 слайда 9, что задается формулой 5. Второй этап включает формирование значения стеганокода с учетом ключевой информации по формуле 6. На третьем этапе строится результирующее кодовое представление для числа с имплантированным элементом формула 7.

Схема описывающая подход для стеганографического преобразования на основе неравновесного позиционного кодирования представлена на рис 8. слайд 10.

***Рассмотрим решение второй задачи***

В процессе неравновесного позиционного кодирования выявляется структурная избыточность обусловленная ограничением на динамический диапазон. В связи с чем предлагается использовать выявленное количество структурной избыточности для встраивания информации. Такое встраивание будем называть структурным стеганографическим кодированием, что задано определением 1 слайда 12. Структурная схема кодирования отображена на рис. 9 слайда 12, и задаются следующими этапами;

1. Имплантация элемента скрываемого сообщения в неравновесное позиционное число формула 8 слайда 13.

2. Формирование значения стеганокода, что задается формулой 9.

3. Формирование кодограммы стеганокода описывается выражением 12.

Однако для такого подхода существует стеганографическая избыточность. Схематично процесс образования стеганографической избыточности задается на рис 10. Наличие такой избыточности приводит к неоднозначной обработке значения стеганокода и как следствие снижается устойчивость относительно визуальных атак на факт встроенных сообщений.

Для локализации стеганографической избыточности ***предлагается*** проводить маскирование путем коррекции кодограммы стеганокода рис. 10 с. Такую локализацию будем называть структурным стеганографическим маскированием, что задается определением 2. Процесс маскирования предусматривает приведение длины кодограммы стеганокода к значению длины кода-контейнера путем отбрасывания младших бит.

Схема стеганографической системы с маскированием структурной стеганографической избыточности представлены на рис 11 слайда 15.

Этап стеганографического декодирования осуществляется по биполярному принципу для авторизированного и неавторизированного пользователя. Условия для неавторизированного доступа представлены на рис. 12 слайда 16. В случае неавторизированного доступа декодирование включает следующие этапы:

1. Извлечение из кодограммы скорректированного стеганокода при помощи системы оснований.

2. Восстановление элементов исходной видеопоследовательности по формуле 13 слайда 16.

3. Оценка качества визуального восприятия реконструированного изображения, т.е. проведение атаки относительно факта наличия встроенной информации.

Наоборот, в случае авторизованного доступа пользователю доступна следующая информация рис 13 слайда 17.

В этом случае стеганографическое декодирование будет содержать следующие этапы:

1. Извлечение из кодограммы скорректированного стеганокода на основе системы оснований.

2. Устранение эффекта маскирование. Проведение демаскирования стеганокода выполняется по формуле 14 слайда 17.

3. Восстановление встроенного элемента. Данный этап реализуется на основе выражения 15 слайда 17 при наличии информации о позиции встроенного элемента и его основания.

4. Восстановление остальных элементов исходной видеопоследовательности осуществляется по формуле 16 слайда 17.

***Рассмотрим решение третьей задачи***

На слайде 19 представлены изображения, над которыми выполнялись преобразования согласно разработанному алгоритм, а также результат последующего декодирования.

Сравнительная оценка величины относительной стеганографической емкости и ПОСШ различных классов изображений, декодированных при неавторизированном доступе, для разработанного и существующих стеганографических методов приведены в табл. 2. слайда 20. Исследование таблицы 2, позволяет заключить следующее: 1)  при одинаковых значениях относительной стеганографической емкости выигрыш для разработанного метода относительно существующих методов по величине ПОСШ для различных классов изображений составляет от 5 до 80%.

Сравнительная оценка значений вероятности безошибочного изъятия встроенных данных при авторизированном доступе для методов НЗБ, РС и разработанного метода в условиях отсутствия атак на встроенное сообщение рассматривается на рис. 20. слайда 20.

Исследование результатов на рис. 20 позволяет заключить, что: 1) выигрыш для разработанного метода относительно методов НЗБ и РС по значению вероятности безошибочного изъятия в условиях применения противником атак на встроенное сообщение составляет в среднем 40 %.

Научная новизна результатов исследований представлена на слайде 21.

Практическая значимость исследований представлена на слайде 22.

На 23 перечислены публикации по теме работы

Благодарю за внимание