ции, аппаратура связи и сопряжения с другими устройствами комплекса, тренажерные и вычислительные средства.

Перегрев СВЧ-приборов передающего устройства МФРЛС является одной из главных причин отказов. Причиной перегрева является непоступление (поступление в недостаточном количестве) или отсутствие охлаждающей жидкости по контуру охлаждения прибора. Для этих целей в передающем устройстве МФРЛС используются системы жидкостного и воздушного охлаждения.

Система жидкостного охлаждения (СЖО) представляет собой самостоятельное изделие и предназначена для снятия тепловыделений и обеспечения термостабилизированного теплового режима работы СВЧ-приборов и выходного волноводного тракта, размещенных в передающем устройстве МФРЛС [1].

Проверка уровня охлаждающей жидкости СЖО осуществляется по смотровому окошку ресивера. Уровень охлаждающей жидкости должен находиться между рисками контрольного стекла ресивера. При снижении уровня охлаждающей жидкости ниже допустимого включать передающее устройство (даже кратковременно) запрещается [2].

Ресивер СЖО расположен на внешней стенке антенного поста. Поэтому при установке антенного поста на вышку 40В6М контроль уровня охлаждающей жидкости является затруднительным, так как для выполнения данной проверки необходимо перевести вышку 40В6М в горизонтальное положение. Данная операция занимает до 90 % (37 минут) времени на контроль уровня охлаждающей жидкости СЖО.

Следовательно, одним из путей сокращения времени контроля уровня охлаждающей жидкости СЖО антенного поста МФРЛС является разработка датчика уровня жидкости, который обеспечит индикацию допустимого уровня, а также аварийное отключение СЖО и передающего устройства МФРЛС при снижении уровня охлаждающей жидкости ниже допустимого, что в свою очередь позволит уменьшить время оценки его технического состояния (контроля уровня охлаждающей жидкости в ресивере) и, как следствие, повысить коэффициент готовности.

Литература

1. Техническое описание. Антенный пост Ф1С.
2. Инструкция по эксплуатации. Антенный пост Ф1С.

МЕТОДЫ И ПРОГРАММНОЕ СРЕДСТВО СТЕГАНОГРАФИЧЕСКОГО ПРЕОБРАЗОВАНИЯ ТЕКСТОВ-КОНТЕЙНЕРОВ НА ОСНОВЕ ЯЗЫКОВ РАЗМЕТКИ

А.А. СУЩЕНЯ

НАУЧНЫЙ РУКОВОДИТЕЛЬ – П.П. УРБАНОВИЧ, ДОКТОР ТЕХНИЧЕСКИХ НАУК, ПРОФЕССОР

Рассмотрены авторские стеганографические методы внедрения текстовой информации, основанные на свойствах электронного документа Microsoft Word формата .DOCX. Описаны особенности метода на основе модификации кавычек в XML-файле. Разработано приложение, позволяющее создавать стеганографические контейнеры из электронных документов с использованием данного подхода, что может быть использовано для скрытой передачи и хранения данных, а также подтверждения права собственности на информацию, представленную в цифровом виде

Ключевые слова: стеганография, формат .DOCX, XML, веб-приложение

Развитие информационных технологий характеризуется обострением проблем, связанных с обеспечением безопасности. Безопасность данных — одна из главных задач, решаемых в IT сфере. Причем речь идет не только о предотвращении утечки информации, снижении объемов паразитного трафика и отражении атак на ценные ресурсы, но и об оптимизации работы системы в целом. Найти универсальное решение в данном вопросе практически невозможно из-за неоднородности сфер деятельности, а также разнообразности организационных структур, которые требуют индивидуального решения для каждого отдельного случая [1].

На данный момент существует ряд средств, обеспечивающих защиту информации на основе использования различных подходов: аппаратных, физических, программных, организационных, законодательных. Одним из перспективных направлений в области разработки программных средств для решения проблемы защиты конфиденциальных данных является использование стеганографии. Основная задача стеганографии – это скрытие факта наличия информации в открытом канале передачи данных [1].

Использование стеганографического метода предусматривает наличие: контейнера, для осаждения сообщения; сообщения, содержащего конфиденциальную информацию; открытого канала передачи данных; способа кодирования информации. В качестве стеганоконтейнера можно использовать

цифровой объект, обладающий некоторой избыточностью, модификация которого не затронет его семантику. Перспективным направлением, является текстовая стеганография. При скрытии информации используются символы в тексте, не учитываемые при прочтении человеком и компьютерном анализе текстового файла. Одним из наиболее популярных контейнеров является электронный документ формата DOCX, в котором для создания визуального оформления текста используется язык разметки XML.

XML (eXtensible Markup Language, или расширяемый язык разметки) – текстовый формат, предназначенный для хранения структурированных данных, для обмена информацией между программами, а также для создания на его основе более специализированных языков разметки, иногда называемых словарями. Документ представляет собой обычный текстовый файл, в котором при помощи специальных маркеров создаются элементы данных, последовательность и вложенность которых определяет структуру документа и его содержание.

У документа формата XML есть определенные достоинства. Этот язык разметки позволяет отобразить двоичные данные в текст, читаемый человеком и анализируемый компьютером. Данный формат поддерживает Юникод. В формате XML могут быть описаны такие структуры данных, как записи, списки и деревья. XML имеет строго определённый синтаксис и требования к анализу, что позволяет ему оставаться простым, эффективным и непротиворечивым. XML представляет собой простой текст, свободный от лицензирования и каких-либо ограничений; XML не зависит от платформы, он не накладывает требований на расположение символов в строке. В отличие от бинарных форматов, XML содержит метаданные об именах, типах и классах описываемых объектов, по которым приложение может обработать документ неизвестной структуры.

Однако документам формата XML присущ ряд недостатков. Его синтаксис избыточен. Большой размер XML-документа существенно больше бинарного представления тех же данных. Размер XML-документа существенно больше также размера документа в альтернативных текстовых форматах передачи данных (например, JSON, YAML) и особенно в форматах данных, оптимизированных для конкретного случая использования. Для большого количества задач не нужна вся мощь синтаксиса XML и можно использовать значительно более простые и производительные решения.

Ввиду того, что синтаксис XML избыточен – это позволяет рассматривать документы в данном формате в качестве стеганографического контейнера (см. *рисунок* 1).

```
<person>
    <myTag id="one">value</myTag >
    < myTag id="two"> value </myTag >
    < myTag id="three"> value </myTag >
    < myTag id="four"> value </myTag >
    < myTag id="five"> value </myTag >
    < myTag id="six">value </myTag >
    < myTag id="seven"> value</myTag >
</person >
```

Рис. 1 – Пример использования XML для отображения объекта person

Зачастую XML используется скорее в качестве языка разметки, а не формата данных. При описании внешнего вида документа на языке XML, как правило, используются атрибуты, что позволяет при помощи определенного алгоритма разместить в файле XML информацию, никак не влияющую на семантику документа.

Известно, что интерпретатор XML-документа не «придает значения» тому, какой тип кавычек используется при его создании. Следовательно, если заменить какую-нибудь пару кавычек в валидном XML-документе, например, с двойной на одинарную, то при визуальном анализе документа со стороны пользователя в браузере никакой разницы видно не будет. Используя эту технику, в XML-документ можно тайно разметить бинарную последовательность.

Перед тем, как начинать осаждение информации, нужно убедиться в том, что контейнер имеет достаточную емкость. Емкость определяется как количество пар кавычек во всем документе.

При встраивании последовательности бит условимся, что единице будет соответствовать двойная кавычка, а нулю одинарная. Начиная с первой пары кавычек в документе, будем ставить ей в соответствие бит встраиваемого сообщения и, при необходимости, изменять тип кавычки на противоположный. Например, первая пара кавычек в документе двойная, а первый бит осаждаемой последовательности нулевой, следовательно, необходимо тип кавычек заменить на одинарный.

При использовании данного метода также необходимо заранее определить количество бит, отводимое под один символ сообщения. Установка количества бит позволяет эффективно использовать место в контейнере. Ведь, если необходимо передать текст, состоящий только из букв английского алфавита, то для представления одного символа в двоичном виде будет вполне достаточно семи бит, в отличие от русского алфавита, где для представления одного символа необходимо уже, как минимум, одиннадцать бит. В конец осажденного сообщения встраивается уникальная последовательность, указывающая на то, что сообщение закончилось.

Рассмотрим пример. Запишем сообщение «A» в XML-документ, представленный на рисунке 1. Для осуществления процедуры внедрения, представим сообщение «A» в виде числа. Согласно кодам ASCII, символу «A» соответствует число 65. Далее переведем число 65 в двоичный вид, чему соответствует значение «1000001». Для осаждения представленной бинарной последовательности достаточно 7 бит. Запишем первый символ бинарной последовательности. Первой парой кавычек в документе является та, которая оборачивает значение «one» атрибута «id». Так как эта кавычка двойная, а бит внедряемого сообщения – единица, то никакой замены производить не нужно. Первый бит сообщения размещен. Вторая пара кавычек – это та, которая оборачивает значение «two» атрибута «id». В соответствии с битом внедряемого сообщения данную пару кавычек необходимо заменить на одинарную, после чего процесс осаждения второго бита завершен. Далее процесс повторяется до момента пока сообщение не закончится.

Эффективность представленного метода зависит от количества атрибутов в XML-документе, позволяя при наличии *n* атрибутов записать *n* бит бинарной последовательности. Преимуществом данного метода является учет особенностей языка разметки XML при внедрении секретной информации, а также простота реализации. Алгоритм преобразования XML-документа на основе представленного метода обладает линейной сложностью.

Следует также подчеркнуть, что формат DOCX представляет собой модернизированную версию формата DOC, причем по сравнению со своим предшественником этот формат гораздо более популярен и доступен. В отличие от DOC формат DOCX не является расширенным файловым форматом. Он представляет собой файл-архив. Формат файла основан на Open XML и использует сжатие по алгоритму ZIP для уменьшения размера файла. Исходя из того, что DOCX файл является ZIP архивом с XML-документами, можно использовать этот формат для внедрения в него тайной информации, применив метод замены типа кавычки в XML-документе.

Для осаждения информации в файл с расширением DOCX можно выполнить данную последовательность шагов [2–6]:

- создать документ формата DOCX, например, при помощи текстового редактора Microsoft Office Word 2016;
- разместить в созданном документе текст, применив к нему стили, по необходимости;
- при помощи стандартных средств операционной системы Windows поменять расширение у созданного ранее документа с DOCX на ZIP;
- при помощи стандартных средств операционной системы Windows открыть полученный архив и извлечь XML-документ с именем, например, *document.xml* из папки *word*;
- записать в извлеченный XML-документ тайное сообщение, например, при помощи метода замены кавычек;
- заменить полученным в результате осаждения XML-документ тот, который изначально был в архиве;
- при помощи стандартных средств операционной системы Windows поменять расширение у измененного архива с ZIP на DOCX.

В результате выполнения данной последовательности шагов получен стеганографический контейнер, содержащий некоторую осажденную в него информацию. После преобразования контейнер может быть открыт при помощи Mircoroft Office Word.

Для демонстрации стеганографического метода внедрения информации разработано программное средство «*MarkupStego*», позволяющее на основе созданных электронных документов, формировать стеганографические контейнеры на основе предложенных методов. Для реализации приложения была выбрана платформа ASP.NET Core, которая представляет собой технологию, предназначенную для создания различного рода веб-приложений. ASP.NET Core включает в себя фреймворк MVC, объединяющий функциональность MVC, Web API и Web Pages, что позволяет разделить логику приложения и его визуальное представление.

Основными преимуществами платформы ASP.NET являются:

- легковесный и модульный конвейер HTTP-запросов;

- возможность развертывать приложение как на IIS, так и в рамках своего собственного процесса;
- использование платформы .NET Core и ее функциональности;
- единый стек web-разработки, сочетающий Web UI и Web API;
- наличие встроенных библиотек для работы с такими форматами данных как: DOCX, ZIP позволяющих модифицировать данные форматы;
- кроссплатформенность: возможность разработки и развертывания приложений ASP.NET на Windows, Mac и Linux;
- совместимость с UI-фреймворками.

Фреймворком для реализации клиентской части был выбран Angular. Angular – это фреймворк от компании Google для создания клиентских приложений. Прежде всего, он нацелен на разработку SPA-решений (Single Page Application), то есть одностраничных приложений. В этом плане Angular является наследником другого фреймворка AngularJS. В то же время Angular это не новая версия AngularJS, а принципиально новый фреймворк. Angular 5 предоставляет такую функциональность, как двустороннее связывание, позволяющее динамически изменять данные в одном месте интерфейса при изменении данных модели в другом, шаблоны, маршрутизация и так далее. Одной из ключевых особенностей Angular является то, что он использует в качестве языка программирования TypeScript.

Для осуществления процедуры осаждения в адресной строке браузера необходимо ввести адрес приложения *MarkupStego*. После загрузки приложения возможно выполнение операций внедрения и извлечения. Переключаться между этими двумя функциями можно при помощи меню, выбрав необходимые кнопки. При переходе на вкладку «Внедрение» для проведения внедрения информации необходимо загрузить файл с расширением DOCX. После чего указать язык внедряемого сообщения, ввести само сообщение и ввести название контейнера, содержащего информацию. Для проведения операции извлечения необходимо загрузить контейнер, в который было произведено осаждение предварительно выбрав язык сообщения, после чего внедренная ранее информация отобразиться в окне браузера.

Разработанные и реализованные методы характеризуются простотой, высокой скоростью выполнения операций осаждения/извлечения тайной информации при сравнительно невысокой информационной емкости осаждаемых сообщений. Характеризуются высокой эффективности при защите авторских прав, где не требуется осаждать длинных сообщений.

Литература

1. *Урбанович, П.П.* Защита информации методами криптографии, стеганографии и обфускации/ П.П. Урбанович. – Минск: БГТУ, 2016, – 220 с.
2. *Сущеня, А. А.* Стеганографическое преобразование текстов-контейнеров на основе языков разметки / *А. А. Сущеня* // 68-я научно-техническая конференция учащихся, студентов и магистрантов, 17-22 апреля, Минск: сборник научных работ: в 4 ч. Ч. 4 / Белорусский государственный технологический университет. - Минск: БГТУ, 2017. - С. 145-149.
3. *Сущеня, А.А.* Способ стеганографического осаждения информации в документ с расширением .DOCX / *А. А. Сущеня* // XXI Республиканская научная конференция студентов и аспирантов, 19–21 марта, Гомель: сборник научных работ / Гомельский государственный университет имени Ф. Скорины. – С. 303-304.
4. *Сущеня, А.А.* Идея и архитектура веб-приложения, использующего в качестве стеганографического контейнера документы формата DOCX / *А. А. Сущеня* // Международная научно-практическая конференция, 14–18 мая, Минск: сборник научных работ / Белорусский государственный университет. – С. 170.
5. *Сущеня, А.А.* Модификация стеганографического метода изменения междустрочного расстояния электронного документа/ А.А. *Сущеня, Е.А. Блинова, П.П. Урбанович*// Технические средства защиты информации: Тезисы докладов XVI Белорусско-российской научно-технической конференции, 5 июня 2018 г., Минск. Минск: БГУИР, 2018. – С 90-91.
6. *Сущеня, А. А.* Программное средство стеганографического преобразования текстов-контейнеров на основе языка разметки XML / *А. А. Сущеня* // 69-я научно-техническая конференция учащихся, студентов и магистрантов, 2-13 апреля, Минск: сборник научных работ: в 4 ч. Ч. 4 / Белорусский государственный технологический университет. - Минск: БГТУ, 2018. - С. 81-84.

ИССЛЕДОВАНИЕ РАБОТЫ ДИАГОНАЛЬНОГО ПЛАСТИНЧАТОГО РЕКУПЕРАТОРА ЦЕНТРАЛЬНОГО ПРОМЫШЛЕННОГО КОНДИЦИОНЕРА В ТЕПЛЫЙ И ХОЛОДНЫЙ ПЕРИОДЫ

В.М. СЫТЕНКО, Н.В. КУШНЕРУК

НАУЧНЫЙ РУКОВОДИТЕЛЬ – П.Ф. ЯНЧИЛИН, МАГИСТР ТЕХНИЧЕСКИХ НАУК

Проблематика. Данная работа направлена на исследование возможных проблем при работе диагонального пластинчатого рекуператора центрального промышленного кондиционера в теплый и холодный периоды года.