КОРРЕКЦИЯ МОДУЛЬНЫХ ОШИБОК БЛОКОВЫМИ КОДАМИ, ПОСТРОЕННЫМИ НА ОСНОВЕ СОСТАВНЫХ САМООРТОГОНАЛЬНЫХ СВЕРТОЧНЫХ КОДОВ

Е.Г. Макейчик, А.И. Королёв, В.К. Конопелько, М.Д. Исакович,
А.С. Ковалевский, Ю.Е. Яворко

Предложен метод построения канального кодека блокового кода на основе составного самортогонального сверточного кода (СССК) с пороговым алгоритмом декодирования со скоростью $R \geq 2/3$. Определены параметры канального кодека, реализующего блоковый способ кодирования и декодирования информации, построенного на основе составного самоортогонального сверточного кода с пороговым алгоритмом декодирования. Установлено, что метод построения канальных кодеков на основе составных самоортогональных сверточных кодов с пороговым алгоритмом декодирования и реализующий блоковый способ кодирования и декодирования информации, обеспечивает увеличение в $\alpha(\alpha \geq 2)$ раз корректирующую способность базового СССК. Для практического применения предложенного метода построения канальных кодеков для коррекции модульных (зависимых) ошибок достаточно использование коэффициента внутреннего перемежения информационных символов $\alpha = 2$.

Литература

1. Радченко А.Н., Мирончиков Е.Г. // Радиотехника и электроника. 1961. № 11. С. 18–33.
2. Дмитриев О.Ф. // Радиотехника. 1964. Т. 19, № 4. С. 68–75.

КОРРЕКЦИЯ ЗАВИСИМЫХ ОШИБОК НА ОСНОВЕ РАВНОМЕРНЫХ СВЕРТОЧНЫХ КОДОВ

Е.Г. Макейчик, А.И. Королёв, В.К. Конопелько

Рассматриваются методы $(n_0 = k_0 + 2)$-канального кодирования и декодирования зависимых ошибок на основе систематических равномерных сверточных кодов (СРСК), обеспечивающие повышение скорости передачи кода и корректирующую способность исходных СРСК. Оценивается эффективность предложенных методов кодирования. Разработан метод $(n_0 - 1,\ n_0 \geq 3)$-канального кодирования/декодирования зависимых ошибок на основе двух систематических равномерных сверточных кодов, обеспечивающий повышение в 2 и более раза скорость передачи кода и увеличение в 1,33 раза корректирующую способность канального кодека. Разработан метод $(n_0 - 1,\ n_0 = k_0 + 2,\ k_0 = 1)$-канального кодирования/декодирования зависимых ошибок на основе систематического равномерного сверточного кода, обеспечивающий коррекцию ошибок заданной кратности при увеличении в 1,34 раза скорости передачи СРСК канального кодера. Установлено, что предложенные методы кодирования и декодирования обеспечивают увеличение скорости передачи исходных (базовых) СРСК и уменьшают вероятность ошибочного декодирования.

Литература

1. Конопелько В.К., Липницкий В.А., Дворников В.Д. и др. Теория прикладного кодирования. Минск, 2004.
2. Кудряшов Б.Д. // Пробл. передачи информ. 1990. Т. 26, вып. 2. С. 18–26.

ИССЛЕДОВАНИЕ СТЕГАНОГРАФИЧЕСКИХ ТЕХНОЛОГИЙ МОДИФИКАЦИИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

В.В. Маликов, М.А. Бабич, А.В. Макатерчик

Использование стеганографических технологий модификации конфиденциальной информации позволяет преодолеть защиту традиционных средств и систем информационной безопасности применяемых в организациях. В рамках исследования проведено тестирование эффективности DLP-системы на стеганографические технологии модификации файлов. Для оценки эффективности перехвата модифицированной информации была выбрана DLP-система

«SecureTower» российской компании Falcongaze [1]. В качестве эксперимента 2 тестовых файла (формат: doc, rar; объем: до 50 КБ) с конфиденциальной информацией с использованием стенографического ПО «OpenPuff» (v.4.00 /настройки качества: по умолчанию/, LSB-метод) [2] встраивались в файл-контейнер (формат: png, jpg, pdf). Эффективность перехвата оценивалась в процентах от детекции сформированной тестовой базы из 6 файлов. Моделирование проводилось на физических и виртуальных вычислительных машинах (ПО «VMware Workstation Pro» [3]).

На основании проведенного исследования можно сделать вывод, что использование DLP-системы в настоящее время не позволяет детектировать стеганографические технологии модификации файлов. Эффективность перехвата данных DLP-системой по заданному перечню стеганографических модификаций файлов составила 0 % («цифровой отпечаток» (Digital Fingerprints) / контрольная сумма (хэш)).

Литература

1. Falcongaze «SecureTower» // falcongaze.ru [Электрон. ресурс]. – 2010-2017. – Режим доступа: https://falcongaze.ru/. – Дата доступа: 22.04.2017.

2. OpenPuff team // download.cnet.com [Электрон. ресурс]. – 2017. – Режим доступа: http://download.cnet.com/windows/openpuff-team/3260-20_4-10146585-1.html. – Дата доступа: 23.04.2017.

3. VMware Workstation Pro // vmware.com [Электрон. ресурс]. – 2017. – Режим доступа: http://www.vmware.com/ru/products/workstation.html. – Дата доступа: 22.04.2017.

ТЕСТИРОВАНИЕ ТЕХНОЛОГИЙ ПЕРЕХВАТА ДАННЫХ DLP-СИСТЕМЫ

В.В. Маликов, Е.О. Перхальский, И.И. Лившиц

Внедрение и использование DLP-систем позволяет эффективно автоматизировать ряд задач по защите конфиденциальной информации от утечки по технических каналам. Для оценки эффективности была выбрана DLP-система «SecureTower» российской компании Falcongaze [1], которая представляет собой программный продукт, позволяющий решать задачи по защите конфиденциальной информации от утечки по технических каналам.

В рамках исследования эффективности проведено:

Тестирование программной среды функционирования DLP-системы на предмет поддерживаемых операционных систем (ОС). Моделирование проводилось на физических и виртуальных вычислительных машинах (ПО «VMware Workstation Pro» [2]).

Тестирование эффективности перехвата данных DLP-системой в приложениях, использующих протоколы: POP3, SMTP, HTTP и др.). Назначение портов приложений использовались по умолчанию. Эффективность перехвата оценивалась в процентах от детекции сформированных тестовых баз из 20 файлов / сообщений в 2-х режимах DLP-системы (настройки по умолчанию / специальная настройка параметров). Моделирование проводилось на физических и виртуальных вычислительных машинах (ПО «VMware Workstation Pro»).

На основании проведенного исследования эффективности работы DLP-системы по защите конфиденциальной информации от утечки по технических каналам можно сделать следующие выводы:

1. Программная среда функционирования DLP-системы Falcongaze «SecureTower» в настоящее время поддерживает все основные ОС семейства Microsoft «Windows».

2. Внедрение и использование DLP-системы позволяет эффективно автоматизировать задачи по защите конфиденциальной информации от утечки по технических каналам. Эффективность перехвата данных DLP-системой по заданному перечню протоколов / портов составила от 90 % до 100 %.

Литература

1. Falcongaze «SecureTower» // falcongaze.ru [Электрон. ресурс]. – 2010-2017. – Режим доступа: https://falcongaze.ru/. – Дата доступа: 22.04.2017.

2. VMware Workstation Pro // vmware.com [Электрон. ресурс]. – 2017. – Режим доступа: http://www.vmware.com/ru/products/workstation.html. – Дата доступа: 22.04.2017.