

Список литературы

1. Shema M. Seven Deadliest Web Application Attacks (Syngrass Seven Deadlest Attacks).— Syngress Publishing, Inc. Elsevier, Inc. 30 Corporate Drive Burlington, 2010.
2. XSS Attacks – Cross Site Scripting Exploits and Defense / S. Fogie [et al.]. Syngress Publishing, Inc. Elsevier, Inc. 30 Corporate Drive Burlington, 2011. 28 p.

ГИБКИЕ МНОГОСЛОЙНЫЕ ЭЛЕКТРОМАГНИТНЫЕ ЭКРАНЫ ДЛ Я СНИЖЕНИЯ УРОВНЯ ПОМЕХ СРЕДСТВ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ

У.М. Харма, Н.Н. Гринчик

Разработана и апробирована методика изготовления гибких многослойных электромагнитных экранов, характеризующихся значениями коэффициента передачи электромагнитного излучения в диапазоне частот 0,7...17 ГГц, изменяющимися в пределах от –30 до –40 дБ и значениями коэффициента отражения электромагнитного излучения, изменяющимися в пределах от –5 до –15 дБ. Эти экраны состоят из пяти слоев. Их первый, третий и пятый слои (относительно фронта распространения электромагнитных волн) выполнены на основе влагосодержащей плотной целлюлозы. Влагосодержание каждого следующего из указанных слоев превышает влагосодержание предыдущего. Второй и четвертый слои электромагнитных экранов, изготовленных в соответствии с предложенной методикой, выполнены на основе углеродосодержащего материала. Такие экраны могут быть использованы для изготовления изделий, предназначенных для снижения уровня побочного электромагнитного излучения средств вычислительной техники.

LDPC-КОДЫ ДЛ Я ЗАЩИТЫ ИНФОРМАЦИИ

А.В. Хмелевский

Корректирующие коды получили широкое применение в задачах защиты информации. В настоящее время такие коды представлены в многочисленных технических приложениях, например, в стандартах CCSDS 101.0-B (Consultative Committee for Space Data Systems), ITU-T G.975.1 (International Telecommunication Union) и IEEE 802.16 (The Institute of Electrical and Electronics Engineers).

Одними из таких кодов являются коды с малой плотностью проверок на четность (LDPC-коды).

Целью исследования является разработка новой методики комплексной оценки помехоустойчивых кодов, применяемой на предварительном этапе построения систем, реализующих защиту информации в высокоскоростных каналах передачи данных.

В работе были получены следующие результаты.

1. Разработана новая, научно обоснованная методика комплексной оценки помехоустойчивых кодов, которая может применяться на начальном этапе разработки систем помехоустойчивого кодирования, позволяющих с заданной достоверностью гарантировать защищенность целостности данных от разрушающих воздействий в высокоскоростных каналах передачи данных, реализуя механизмы защиты информационных символов. Отличительной особенностью данной методики является то, что она оперирует комплексным набором показателей для оценки кода, учитывает различные аспекты использования данного типа кодов и предназначена для оценки возможности и способов построения систем декодирования с применением рассматриваемого типа кодов. Методика приведена на примере LDPC-кода.

2. Выявлена взаимосвязь алгоритмов декодирования LDPC-кода, которая позволяет раскрыть иерархическую вложенность данных алгоритмов и сделать вывод о том, какой алгоритм является наиболее релевантным для определенной системы передачи данных с заданными параметрами.

Список литературы

1. Gallager R.G. Low Density Parity-Check Codes. MIT Press, Cambridge, MA, 1963.
2. Jian-Bing H.A.N., Chen H.E., He Yun H.E. Research on regular LDPC codes with better performance than turbo codes // Materials of International Conference on Information Engineering ICIE '09.

ИНВАРИАНТНОСТЬ ЦИФРОВОГО ОТПЕЧАТКА УСТРОЙСТВА ПОЛЬЗОВАТЕЛЯ, ИСПОЛЬЗУЕМОГО ДЛЯ ЕГО ДОСТУПА К ИНФОРМАЦИОННЫМ РЕСУРСАМ

О.А. Хожевец, Т.В. Борботько

Идентификация пользователя информационных ресурсов предполагает использование некоторой уникальной информации, которая известна непосредственно пользователю, а также хранится в информационной системе для выполнения процедуры его аутентификации. В качестве такой информации выступает, как правило, некоторые сведения (логин, пароль и т.д.) вводимые пользователем для проверки его подлинности.

Учитывая особенности программных средств, применяемых пользователями сети интернет для доступа к информационным ресурсам, можно выделить следующие признаки таких средств, позволяющих выполнить процедуру идентификации его устройства: javascript, user agent, IP, flash, ActiveX, содержание кэша браузера, cookie, supercookie, настройки используемого программного обеспечения. Формирование из вышеперечисленных признаков массива данных и вычисление его хэш суммы позволяет получить цифровой отпечаток (фингерпринт) устройства пользователя, который будет неизменным в течение достаточно длительного времени.

Необходимо отметить, что во всех существующих браузерах есть широкий спектр переменных с большой инвариантностью, которые позволяют, даже не подготовленному пользователю, изменять цифровой отпечаток своего устройства перед подключением к информационному ресурсу. Наиболее простыми способами, являются: использование нового браузера или новой версии, изменение масштаба окна браузера, изменение часового пояса устройства, изменение языка браузера. Экспериментально установлено, что варьируя значениями указанных переменных можно получить от 1000 до 230000 уникальных цифровых отпечатков устройства, в зависимости от используемого браузера. Таким образом, для снижения ошибок первого и второго рода необходимо формировать базу цифровых отпечатков устройства пользователя, которая, в дальнейшем, может быть использована для его идентификации.

БЕЗОПАСНОСТЬ REACT-ПРИЛОЖЕНИЙ

М.П. Хоронек, Н.В. Харитонов, М.А. Медунецкий, В.Я. Анисимов

ReactJS – самая популярная JavaScript библиотека для построения пользовательских интерфейсов по данным Google Trends на 2019 год [1]. Приложения на ее основе используют большое количество js-кода, поэтому справедливо предположить что атаки типа XSS могут принести злоумышленникам определенный результат.

Практика использования ReactJS в мире показывает, что библиотека содержит большое число компонентов поддержания безопасности приложения. Например, спецсимволы, без которых невозможно осуществить XSS атаку, автоматически заменяются управляющей последовательностью при их использовании в строчных значениях в JSX (синтаксис, подобный HTML, в основе которого лежат теги, позволяющий использовать JS-код непосредственно при построении разметки) [2]. Тем не менее, проблемы, связанные с внедрением скриптов, могут быть результатом использования неподходящих практик программирования и не всегда являются очевидными. Среди них:

- создание React-компонентов из объектов, поставляемых пользователем;
- отображение ссылок с href-атрибутом, определяемым пользователем;
- явное задание свойства dangerouslySetInnerHTML у элемента;