

БЕЗОПАСНОСТЬ ИСПОЛЬЗОВАНИЯ ПОЛЬЗОВАТЕЛЬСКИХ СКРИПТОВ ПРИ РАБОТЕ С ВЕБ-САЙТАМИ

М.А. Николенко, И.А. Адуцкевич

Пользовательские скрипты представляют собой написанный на языке JavaScript исполняемый код, подключаемый браузером на страницы веб-сайтов, предназначенный для расширения стандартного функционала браузера. Примечательной особенностью пользовательских скриптов является возможность работать на разных сайтах, несмотря на правило ограничения домена, что способствует возможности нежелательной утечки и распространению информации. В данной работе была исследована безопасность использования пользовательских скриптов на примере разработанного модуля голосового управления веб-сайтами. Модуль представляет собой пользовательский скрипт, позволяющий управлять веб-сайтом при помощи голосовых команд. Его работа заключается в считывании и анализе данных с веб-сайта, определении основных функциональных элементов для работы с веб-сайтом, и организацию голосового управления. Для реализации голосового интерфейса были использованы Web Speech API и JavaScript библиотека Pocketsphinx.js.

В ходе исследования работы модуля было обнаружено, что при анализе данных с некоторых веб-сайтов могут возникать утечки информации и личных данных, считывание вредоносного кода и его распространение. Исследование показало, что этот факт находится в прямой взаимосвязи с низким уровнем защиты ряда веб-сайтов в сети Интернет. Чтобы предотвратить утечку и распространение информации был реализован комплекс мер по исправлению критических уязвимостей в пользовательских скриптах, которые включают в себя: валидацию и анализ полученных данных на предмет вредоносного кода, защиту от XSS и CSRF атак. Последующий анализ показал, что шанс утечки пользовательских данных при работе со скриптами существенно снизился.

Литература

1. Microsoft, Developer Network: [Электронный ресурс]. Режим доступа: [https://msdn.microsoft.com/ru-ru/library/zdh19h94\(v=vs.100\).aspx](https://msdn.microsoft.com/ru-ru/library/zdh19h94(v=vs.100).aspx). – Дата доступа: 15.05.2017.
2. Molily.de [Электронный ресурс]. Режим доступа: <https://molily.de/xss/>. – Дата доступа: 17.05.2017.

КОМПЬЮТЕРНО-ИЗМЕРИТЕЛЬНАЯ СИСТЕМА ДЛЯ ИЗМЕРЕНИЯ ПАРАМЕТРОВ АФАР

В.Т. Ревин, Н.М. Наумович, А.А. Гавриченко

Исследование амплитудно-фазового распределения активных фазированных антенных решеток (АФАР) представляет собой достаточно трудоемкую задачу, решить которую без автоматизации процессов выделения, сбора, обработки и регистрации измерительной информации практически невозможно. Современные средства измерений – компьютерно-измерительные системы – позволяют решить данную задачу путем реализации голографического метода, который считается одним из наиболее перспективных направлений для исследования характеристик антенн. Суть данного метода заключается в исследовании амплитудно-фазового распределения (АФР) электромагнитного поля вблизи раскрыва тестируемой антенны посредством прецизионного сканирующего зонда.

Механическая часть разработанной компьютерно-измерительной системы представляет собой двух координатное сканирующее устройство в азимутальной (ось X) и угломестной (ось Y) плоскостях. Диапазон сканирования в азимутальной плоскости до 1200 мм, а в угломестной – до 700 мм, Погрешность определения координат по осям не превышает 0,1 мм. Скорость сканирования регулируется программно-временным способом и может достигать 50 мм/с.

Измерение амплитудных и фазовых параметров СВЧ сигнала, задаваемого компьютерно-управляемым синтезатором частоты, обеспечивается векторным анализатором цепей в диапазоне частот от 8 до 12 ГГц, динамическом диапазоне от 0 до 70 дБ и диапазоне изменения фазовых сдвигов от 0 до 360° ($\pm 180^\circ$). При тщательной настройке средств измерений и хорошем качестве радиопоглощающего покрытия погрешность измерения коэффициента усиления амплитудных параметров $\pm 0,2 \dots 0,5$ дБ; фазовых параметров $\pm 2^\circ$.

Литература

1. Сверхширокополосные измерительные системы [Электронный ресурс]. – Режим доступа: www.trimcom.ru. –Дата доступа: 19.05.2017.
2. Синани А.И. Антенный полигон для измерения.

ПОМЕХОЗАЩИТА РАДИОЛИНИЙ

В.В. Симончик

Основная цель системы радиоэлектронного подавления РЭС - при имеющейся мощности станции помех как можно больше увеличить вероятность ошибки за счет снижения отношения энергии бита к суммарной спектральной плотности мощности помех и собственных шумов. С другой стороны система РЭС старается обеспечить энергетическую и пространственную скрытность работы за счет применения широкополосных сигналов и антенн с малым уровнем боковых лепестков диаграммы направленности антенны. Если известно местоположение станции помех и ее эффективная изотропно излучаемая мощность (ЭИИМ), то для обеспечения помехозащиты РЭС надо воспользоваться уравнением помехозащиты, которое выводится при следующих предположениях [1, 2].

Уравнение помехозащиты в логарифмическом виде будет иметь следующий вид [3]:

$$P_{c\text{ пд}} \cdot G_{c\text{ пд}} = P_{\text{ пд}} \cdot G_{\text{ пд}} + h_{\text{пор}}^2 - B + \left(\frac{r_c}{r_a}\right)^2 + \frac{G(\Theta)_{\text{пм}}}{G_{c\text{ пм}}}, \text{ дБВт, где } N_0 - \text{ спектральная плотность шумов}$$

в нашей системе связи; $G(\Theta)_{\text{пм}}$ – коэффициент усиления антенны приемника СРС в направлении на станцию помех; B – база сигнала; P_n/P_c – отношение мощности помехи к мощности сигнала; $h_{\text{пор}}^2$ – пороговое значение, при котором обеспечивается работа радиолинии

с заданным качеством; $\frac{G(\Theta)_{\text{пм}}}{G_{c\text{ пм}}}$ – уровень бокового лепестка диаграммы направленности

антенны нашей приемной станции; $\left(\frac{r_c}{r_a}\right)^2$ – расстояние между приемником и передатчиком нашей системы связи.

Из уравнения помехозащиты следует, чтобы было легче противостоять помехе надо увеличивать базу сигнала и уменьшать уровень бокового лепестка диаграммы направленности антенны нашей приемной станции, уменьшать расстояние между приемником и передатчиком нашей системы связи $\left(\frac{r_c}{r_a}\right)^2$, а также за счет применения помехоустойчивого кодирования уменьшать.

Уменьшение расстояния между станциями систем связи приводит к уменьшению мощности передатчика и тем самым понижает перехватывающую мощность разведывательного приемника. Основной стратегией постановщика помех положено как при имеющейся мощности передатчика помех вызвать, или увеличивать вероятность ошибки на бит в нашей системе связи.

Литература

1. Помехозащищенность систем радиосвязи / В.И. Борисов [и др.]. – Москва : Радио и связь, 2003. – 640 с.
2. Помехозащищенность с расширением спектра сигналов методом ППРЧ / В.И. Борисов [и др.]. – Москва: Радио и связь, 2000. – 384 с.
3. Тепляков, И.М. Телекоммуникационные системы / И.М. Тепляков. – Москва: ИП РадиоСофт, 2008.