Исходя из потребностей организаций номенклатура ПТСЗИ, используемых в ИС, может включать: средства криптографической защиты информации; средства идентификации и аутентификации пользователей; средства управления доступом и т.д. Ввиду этого матрица безопасности ПТСЗИ каждой конкретной организации будет представлять собой соответственно таблицу, отображающую выполняемые функции, критические параметры и характеристики, правила и условия безопасной эксплуатации (использования), количество единиц используемых средств защиты информации определенного наименования.

Построение такой матрицы необходимо для последующей формализации связей между целями/объектами/условиями нерегламентированного воздействия и соответствующим ущербом ИС организации при решении задачи количественной оценки негативных последствий от атак на ПТСЗИ [2].

Список литературы

1. ТР 2013/027/BY. Информационные технологии. Средства защиты информации. Информационная безопасность.

2. Федорцов А.В. Последствия инсайдерских атак на программно-технические средства защиты информации в контексте оценки рисков для информационной сети // Наука и воен. безопасность. 2018. № 4 (58). С. 25–30.

ЗАЩИТА ВЕБ-ПРИЛОЖЕНИЙ ОТ XSS АТАК

Н.В. Харитонов, М.П. Хоронеко, М.А. Медунецкий, В.В. Шиманский

Сегодня мир веб-разработки развивается с огромной скоростью. Наблюдается тенденция перехода от десктопных приложений в сторону веба. Возможности веб-приложений впечатляют, ведь они позволяют связаться с людьми из разных стран; поиграть в игры; посмотреть новости; заказать билеты и т. д. за несколько минут и на любом устройстве, будь то ПК, смартфон или умные часы. Но наряду с данными функциями образуется ряд проблем, одной из которых является проблема защиты информации и безопасности. В данной публикации рассматриваются XSS атаки, являющиеся наиболее распространенными.

XSS атаки заставляют пользователя выполнять нежелаемые задачи на веб-сайтах (например, отправлять письма, деньги, секретные токены для авторизации на сайте), причем пользователь даже не подозревает об этом.

Сущность XSS (cross site scripting) атаки заключается во внедрении вредоносного кода в возвращаемую сервером веб-страницу, который при последующем открытии страницы будет выполнен в браузере пользователя. Такой код может быть внедрен в страницу, например, при отправке вместо привычного нам комментария, комментария вида:

```
<script>
  var img = document.createElement("img");
  img.setAttribute('src', 'http://hackers.site/?token=' + localStorage.getItem('token'));
  document.body.appendChild(img);
</script>
```
(1)

если при отображении страницы такой комментарий добавляется в html, то злоумышленники получат секретный токен приложения в качестве параметра запроса и смогут работать от имени приложения. Для защиты от такого вида атак следует фильтровать пользовательский ввод, то есть заменять все спецсимволы на escape-последовательности(например, < на &lt, & на &amp) прежде чем вставить такой комментарий в html. Современные фронтенд фреймфорки (React.js, Angular, Vue.js и т.д.) имеют встроенную защиту от XSS атак, ни один из них не позволит просто вставить код вида (1) в веб-страницу. Однако у каждого из них все же остается довольно много уязвимостей, которые позволяют обойти фильтры сайта и внедрить вредоносный код.

Таким образом, XSS атаки являются инструментом для хищения данных из cookies, sessionStorage, localStorage и т. д. Разработчики веб-сайтов не должны пренебрегать созданием защиты от атак данного типа, дабы не ставить своих пользователей под угрозу.

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 ДЛЯ 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 ДЛЯ 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.O-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.