

Благодаря свойствам предложенного метода появляется возможность создания новых технологий защиты информации.

В докладе рассматривается один из вариантов реализации данного метода на основе функций с переменной длиной образа и некоторые возможные его применения.

Одним из таких применений, является технология для реализации безопасных телекоммуникационных связей между абонентами по открытым каналам (например, Интернет), которая обеспечивает контроль целостности передаваемой информации, идентификацию отправителя и аутентификацию сообщений.

УЯЗВИМОСТИ MICROSOFT INTERNET EXPLORER

А.Л. ГАРЦУЕВ, И.Н. ОБЕРНИХИН, А.В. БОРЗЕНКОВ

Благодаря своей популярности Microsoft Internet Explorer привлекает к себе внимание многочисленных хакеров, а также профессионалов по компьютерной безопасности.

Существует несколько типов уязвимостей, касающихся браузера Internet Explorer.

1. Уязвимости, приводящие к нестабильной работе браузера или его "зависанию".

2. Межсайтовый скриптинг (cross-site scripting). Злонамеренный сайт в интернете может узнать содержимое ваших "cookie"-файлов. Полученная информация может быть использована для выяснения таких личных данных пользователя, как адрес его электронной почты или, например, точных сведений о покупках, совершенных им на каком-либо сайте. Эти уязвимости также позволяют читать и выполнять локальные файлы на системе клиента, то есть те файлы, которые уже находятся (предустановлены) на компьютере.

Существует универсальная уязвимость, связанная с методом showHelp(). Последний патч от Microsoft (6 февраля 2003 г.), который должен был справиться с этой проблемой, все варианты использования не покрывает. Возможности: чтение cookie, чтение произвольных файлов, запуск файлов.

3. Выполнение произвольного кода, загруженного с сервера.

Используя уязвимость с showhelp(), можно запускать программы с параметрами. К примеру вставить в качестве запускаемой программы "mshta.exe" (для работы с активными web-страницами) и передать ей параметр — ссылку на активную html-страницу (name.hta). Эта страница в свою очередь может содержать код vbscript, который имеет права на чтение/запись/запуск любых файлов.

Литература

1. Абашии В.В., Бокун Н.В., Борзенков А.В. Анализ угроз информационной безопасности и путей защиты от них// Известия Белорусской инженерной академии, 2002. Т. 1(13)/2, С. 159–161.

ИСПЫТАНИЯ ПРОГРАММНЫХ ПРОДУКТОВ НА ОТСУТСТВИЕ НЕДЕКЛАРИРОВАННЫХ ВОЗМОЖНОСТЕЙ

Е.В. ШИПЕРКО, Л.И. КИРИЛЛОВА

Введение

В последние годы в Республике Беларусь значительно активизировалась работа по созданию системы сертификации в области защиты информации. Это можно объяснить тем, что происходящие в стране процессы существенно затронули организацию системы защиты информации во всех ее сферах — разработки, производства, реализации, эксплуатации средств защиты, подготовки соответствующих кадров. Исследование средств защиты информации (СЗИ), поступающих на рынок Республики Беларусь, затрагивает ряд актуальных проблем. Рынок СЗИ сегодня представлен продукцией, как зарубежных производителей, так и отечественных. Эта продукция должна быть сертифицированной. В докладе рассматриваются общие вопросы сертификации СЗИ и вопросы сертификации программных средств.

Состояние системы сертификации СЗИ

В Республике Беларусь действует Национальная система сертификации, созданная республиканским органом по стандартизации, метрологии и сертификации, и могут действовать созданные другими юридическими лицами системы сертификации продукции по показателям, по которым законодательством Республики Беларусь проведение обязательной сертификации не предусмотрено.

В Национальной системе сертификации проводится как обязательная, так и добровольная сертификация, могут быть созданы системы сертификации по видам продукции и по отдельным требованиям.

Система сертификации продукции имеют свои знаки соответствия.

Система сертификации и знаки соответствия подлежат регистрации в порядке, установленном республиканским органом по стандартизации, метрологии и сертификации.

Участниками обязательной сертификации являются республиканский орган по стандартизации, метрологии и сертификации, органы по сертификации, аккредитованные испытательные лаборатории, изготовители (продавцы) продукции.

До недавнего времени испытания СЗИ в Республике Беларусь проводились специалистами Государственного центра безопасности информации (ГЦБИ) в добровольном порядке, в связи с