$R=\{r_1, r_2, r_3\}$, где r_1 — вариант реализации средств; r_2 — расположение средств; r_3 — функции средств.

Предлагается в одном из подмножеств отразить социально-психологические качества потенциального нарушителя: замкнутость или общительность, воля или нерешительность, авантюризм, прагматизм, карьеризм и др. Это позволит создать гипотетическую модель наиболее опасного нарушителя и выделить так называемую "группу риска".

Синтез моделей проводится с использованием аппарата логики высказываний.

Расширение номенклатуры классифицирующих признаков позволит детализировать модель нарушителя и получить более достоверные оценки вероятного направления, характера и риска возможного несанкционированного доступа.

ЗАДАЧА ИДЕНТИФИКАЦИИ АТАК В СРЕДСТВАХ АУДИТА БЕЗОПАСНОСТИ

Е.П. МАКСИМОВИЧ

В соответствии со стандартом СТБ 34.101.2-2001 (ИСО/МЭК 15408-2) средства аудита безопасности должны обнаруживать возможные нарушения безопасности на основе идентификации определенных правил, знаковых событий; известных сценариев проникновения; несоответствия текущей деятельности пользователя ранее применяемому профилю использования системы. Правила, знаковые события и профили стандартного поведения представляют собой некоторые шаблоны или экспертные правила, каждому из которых соответствуют нечеткое слабо формализуемое множество возможных реализаций. В таких условиях возникает нетривиальная задача идентификации наблюдаемых действий, выраженных в некоторых низкоуровневых сигналах относительно заданных эталонных описаний.

Один из возможных подходов к решению указанной задачи идентификации состоит в использовании распознавания с обучением.

Каждая атака представляется выборкой возможных реализаций, которые образуют один или несколько кластеров близких (в смысле заданной функции) ситуаций. Идентификация ситуации сводится к оценке ее возможной принадлежности одному из полученных кластеров. Если расстояние ситуации до ближайшего кластера меньше заданного порогового значения, то принимается решение о реализации соответствующей атаки. Для определения значения порога можно использовать контрольную выборку. В качестве критерия близости предлагается использовать правило типа "ближайшего соседа" либо близость к эталону кластера, заданному, например, в виде дизъюнктивной нормальной формы.

РАНДОМИЗАЦИОННЫЕ ПРЕОБРАЗОВАНИЯ С АЛФАВИТОМ БОЛЬШОЙ МОЩНОСТИ

В.В. ЗАХАРОВ

Известно, что одним из приемов, разрушающих частотные свойства исходного текста является рандомизация. В процессе рандомизации буквам алфавита исходного текста случайным образом ставятся в соответствие буквы алфавита рандомизированного текста. При этом если мощность алфавита рандомизатора незначительно превышает мощность алфавита исходного текста, то такой шифр может быть легко вскрыт.

Доклад посвящен синтезу и анализу рандомизационных преобразований с большой мощностью алфавита рандомизатора.

Показано, что такие рандомизаторы при мощности алфавита рандомизации $L \to \infty$ обеспечивают бесконечную энтропию криптограммы и, соответственно, полную статистическую независимость криптограммы от исходного текста. При этом возможно получение различной степени приближения к полной статистической независимости исходного и зашифрованного текстов путем использования рандомизатора с ограниченным, достаточно большим полем рандомизации.

Дана численная оценка мощности алфавита рандомизатора, при которой достигается практическая статистическая независимость исходного текста и криптограммы.

Приведена методика синтеза рандомизаторов с большой мощностью алфавита рандомизации на основе кусочно-линейных разрывных функций. Показаны возможные подходы к анализу стойкости таких рандомизаторов.

МЕТОД МНОГОКАНАЛЬНОГО ПРЕОБРАЗОВАНИЯ ДАННЫХ И ЕГО ПРИМЕНЕНИЕ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ

Ю.В. ВИЛАНСКИЙ

В 1999 году в заявке PCT /BY99/ 00005 был предложен метод преобразования данных, в котором исходный текст преобразуется в два или более выходных потока. Особенностью метода является циклический характер получения составляющих выходных потоков, что позволяет распределять их совокупности, каналам передачи или использовать как дополнительные степени свободы в различных системах. При этом, по крайней мере, один из выходных потоков можно сделать достаточно малым.

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 (cros-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 копьютере.

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. Абашин 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