ОСОБЕННОСТИ МЕТОДОВ ЗАЩИТЫ ИНФОРМАЦИИ

Матюшкова Г.Л., Матюшков Л.П., Муравьев Г.Л., Махнист Л.П.

На сегодня нет четких критериев выбора как параметров технических средств ЛВС конкретного назначения, так и их программного обеспечения (ПО). Решение вопросов защиты информации требует новых походов к выбору технических средств и операционной среды, в которую должна входить система управления базами данных (СУБД), содержащая средства для создания механизмов защиты информации, или соответствующие инструментальные ПО или специальные микропроцессоры.

В связи с необходимостью защиты авторских прав, конфиденциальной информации фирм, выполнением денежных операций и т.п. появилась необходимость по крайней мере ограничить доступ к некоторым видам информации, а также избежать ущерба при ее хищении. Методы защиты путем кодирования внутренней информации организации, рекомендуемые для глобальных сетей слишком дороги для ЛВС небольших фирм. В этом случае предпочтительнее методы, ведущие к снижению некоторых эксплуатационных расходов по хранению и одновременной защите информации. Прежде всего следует рассмотреть алгоритмы кодирования информации, которые ведут к ее сжатию, т.е. одновременно экономят память и уменьшают эксплуатационные расходы на хранение информации.

Учитывая, что более дешевые методы защиты информации, как правило менее надежны, то за абсолютный критерий надежности защиты информации следует принять сумму (соответствующую ценности защищаемой информации в рублях), которую необходимо затратить на преодоление защиты. Поэтому в некоторых случаях будет достаточно использовать специально разработанный алгоритм сжатия информации. В качестве следующего уровня защиты можно использовать различные криптографические методы, которые не требуют слишком больших вычислений при кодировании и декодировании текстов.

Главной особенностью этих методов должны быть такие возможности для использования, когда пользователь может из стандартных элементов и функций сам конструировать алгоритм защиты информации по ее сжатию, а также электронную подпись текста.

О ГРАНИЦАХ ДОСТОВЕРНОСТИ СИГНАТУРНЫХ АНАЛИЗАТОРОВ

Махнист Л.П.

В работе рассматривается вопрос о достоверности сигнатурных анализаторов, порождаемых образующими полиномами примитивных кодов БЧХ.

Под достоверностью понимается вероятность необнаружения ошибочной последовательности фиксированной кратности соответствующими сигнатурными анализаторами. Задача определения границ достоверности фактически сводится к оценке отношения количества кодовых слов заданного веса соответствующего кода к величине всех слов того же веса и длины.

В случае примитивного кода БЧХ с образующим полиномом степени 2m длины n=2 5m 0-1, исправляющего две ошибки с параметрами (n,n-2m,5) получены точные верхние и нижние границы этого отношения, а также величины весов, при которых они принимают эти граничные значения.

1Утверждение 0. Верхняя граница отношения числа A 5k 4n 0 кодовых слов фиксированной кратности k примитивного кода БЧХ с образующим полиномом степени 2m (m _> . 3) длины n=2 5m 0-1, исправляющего две ошибки с параметрами (n,n-2m,5) к числу C 5k 4n 5 0 слов веса k и длины n определяется следующими отношениями:

max A 5k 4n 0 / C 5k 4n 0 = (n-3)/[(n-1)(n-2)(n-4)], если m - четно, и

max A 5k 4n 0 / C 5k 4n 0 = (n-7)/[(n-2)(n-3)(n-4)], если m - нечетно,

и принимают эти значения в обоих случаях при k=5, 6, n-6, n-5.

Получены также нижние границы указанного отношения в случае когда m _> . 6, которые достигаются при k = 7, 8, n-8, n-7, если m - четно, и k = 9, 10, n-10, n-9, если m - нечетно. Тем самым определены точные верхние и нижние отклонения данного отношения от асимптотического, определяемого соотношением 1 / n 52 0. Полученные точные границы дают качественную оценку достоверности рассматриваемых сигнатурных анализаторов, которая позволяет сравнивать их с другими.

Замечание. При определении границ данного отношения не рассматривались случаи, когда A 5k 4n 0 = 0, A 5k 4n 0 = C 5k 4n 0, т.е. при k удовлетворяющем соотношению 0 _< . k _< . 4, n-4 _< . k _< . n.

Используемый метод определения границ достоверности можно распространить на случай примитивного кода БЧХ с образующим полиномом степени 3m длины n=2 5m 0-1, исправляющего три ошибки.

АВТОМАТИЗИРОВАННАЯ СИСТЕМА ПОДГОТОВКИ ТЕСТОВ

Муравьев Г.Л.

Предназначена для использования в САПР СБИС верхнего уровня в составе проектных процедур, осуществляющих моделирование проекта СБИС, для обеспечения на единой информационной основе задач моделирования всех уровней описания проекта, допустимых языком VHDL, начиная с поведенческого.

Поддерживает комплекс работ, связанных с подготовкой тестовых воздействий, имитирующих реальное окружение моделируемой СБИС, и выходных эталонных реакций проекта СБИС на входные воздей-