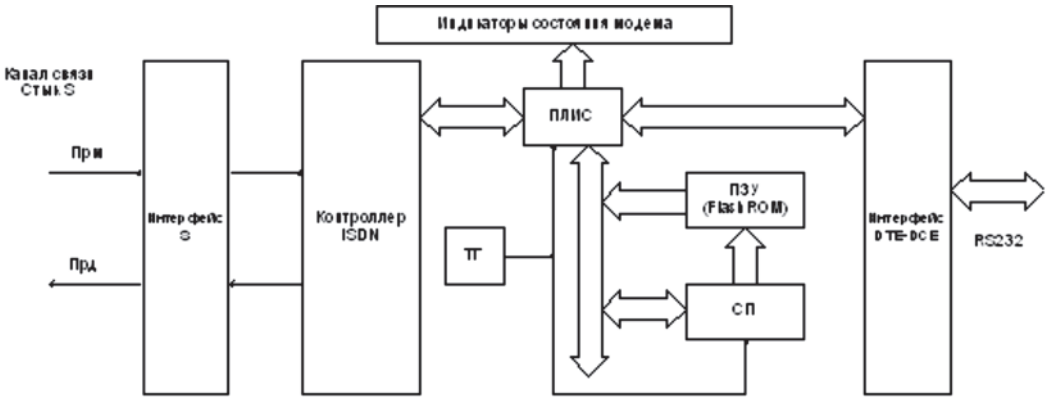
удаленного и терминального доступа на предприятиях с использованием внутренней цифровой сети *ISDN*, универсальность не является непременным атрибутом оборудования. Поэтому при проектировании цифрового модема были установлены параметры устройства с жестко заданными характеристиками, благодаря чему общая схема устройства значительно упрощается и, как следствие, уменьшится и его стоимость.

Структурная схема цифрового модема приведена на рисунке. Модем представляет собой устройство, имеющее цифровой интерфейс с компьютером (последовательный порт *RS*-232) и интерфейс с каналом связи – разъем для телефонного кабеля (*RJ*-45). В цифровых модемах не используется модуляция и демодуляция сигнала, поэтому его структура проще аналогового. Модем состоит из следующих основных блоков: интерфейс DTE-DCE; интерфейс S; сигнальный процессор (СП); флэш-ПЗУ; программируемая логическая интегральная схема (ПЛИС); тактовый генератор (ТГ); индикаторы состояния модема; узел питания.



Структурная схема модема

Реализация модема в соответствии с приведённой структурной схемой позволяет снизить габариты и стоимость устройства.

КРИПТОСИСТЕМЫ И ВИДЫ АТАК

Секретова Л. В., Борисова С.Н.

ГОУ ВПО «Пензенская государственная технологическая академия», Пенза, e-mail: iis@pgta.ru

Теоретически, приложив достаточно усилий, можно взломать любую криптографическую систему. Вопрос заключается в том, сколько работы необходимо проделать, чтобы информация была расшифрована. Существует множество типов атак, каждый из которых обладает той или иной степенью сложности. Рассмотрим некоторые из них.

Только шифрованный текст. Говоря о взломе системы шифрования, многие имеют в виду атаку с использованием только шифрованного текста. В этом случае пользователи А и Б зашифровывают свои данные, а злоумышленник видит только шифрованный текст. Попытка расшифровать сообщения только при наличии шифрованного текста и называется атакой с использованием только шифрованного текста. Это наиболее трудный тип атаки, поскольку злоумышленник обладает наименьшим объемом информации.

Известный открытый текст. При атаке с известным открытым текстом известен и открытый и шифрованный текст. Цель такой атаки состоит в том, чтобы найти ключ.

На практике существует множество ситуаций, откуда можно узнать открытый текст сообщения. Иногда содержимое сообщения легко отгадать.

При наличии известного открытого текста у злоумышленника оказывается больше информации, чем при наличии только шифрованного текста, а вся дополнительная информация только увеличивает шанс расшифрования.

Существует два вида атак с избранным открытым текстом:

Автономный (offline). Открытый текст, который должен подвергнуться шифрованию, подготавливается заранее, еще до получения шифрованного текста.

*Оперативный (online).*Набор каждого последующего открытого текста осуществляется, исходя из уже полученных шифрованных текстов. Данный вид является более результативным.

Криптосистемы и виды атак на них. Рассмотренные выше виды атак применимы ко всем видам криптосистем. Но каждая из них имеет свои индивидуальные особенности, в результате чего имеются и специфические атаки характерные только для определенных видов криптосистем.

Атаки на блочные шифры. *Блочный шифр* – это функция шифрования, которая применяется к блокам текста фиксированной длины. Текущее поколение блочных шифров работает с блоками текста длиной 128 бит.

Функции шифрования построены на основе многократного применения 32-битовых операций. Применяя такие операции, довольно сложно получить нечетную перестановку. В результате практически все известные блочные шифры генерируют только четную перестановку. Упомянутый факт позволяет злоумышленнику построить простой *различитель* (на основе *различающей атаки*). Так называемый *атака с проверкой четности*. Для заданного значения ключа строится перестановку, зашифровав по порядку все возможные варианты открытого текста. Если перестановка является нечетной, значит, перед нами идеальный блочный шифр, так как реальный блочный шифр никогда не генерирует нечетную перестановку.

Атака с помощью решения уравнений. Основная идея этого метода заключается в том, чтобы представить блочное шифрование в виде системы линейных и квадратных уравнений над некоторым конечным полем, а затем решить эти уравнения, используя новые методы наподобие *XL*, *FXL* и *XSL*.

Атаки на асимметричные шифры. Алгоритм *RSA* обеспечивает как цифровое подписывание, так и шифрование, что делает его весьма универсальным средством.

Алгоритм *RSA* основан на использовании односторонней функции с лазейкой. N – это открытый ключ, который формируется как $n = p \cdot q$. Разложение числа n на множители и есть та самая «лазейка». Значения p и q – это два разных больших простых числа,

длина каждого из которых составляет порядка тысячи бит или более.

Возникает проблема, когда пользователь Б зашифровывает с помощью открытого ключа пользователя А сообщение небольшого размера. Если $e = 5$ и $m < \sqrt[5]{n}$, тогда $m^e = m^5 < n$, поэтому взятие числа по модулю не требуется. Злоумышленник сможет восстановить m, просто извлекая корень пятой степени из m^5.

Структура алгоритма *RSA* допускает осуществление сразу нескольких типов атак. Но существуют и более изощренные атаки, основанные на методах решения полиномиальных уравнений по модулю n . Все сводятся к одному: подчинение чисел, которыми оперирует алгоритм *RSA*, *какой бы то ни было* структуре крайне нежелательно.

Таким образом, применение алгоритма *RSA* должно ограничиваться шифрованием коротких последовательностей, а именно секретных ключей шифрования для симметричных криптосистем. Для шифрования нужно использовать более стойкие к атакам шифры с длиной ключа 256 бит. К таким шифрам относят шифр *AES* и ГОСТ 28147-89.

ПОВЫШЕНИЕ ИЗНОСОСТОЙКОСТИ УПОРНЫХ ПОДШИПНИКОВ СКОЛЬЖЕНИЯ ПУТЕМ НАНЕСЕНИЯ ПОЛИМЕРНОГО ПОКРЫТИЯ

Селивоненко О.Н., Шиков А.В.

Муромский институт Владимирского государственного университета, Муром, e-mail: mivlgu@mail.ru

Упорные подшипники скольжения в основном работают в условиях высоких потерь на трение и невозможности обеспечения смазывающего клина. При работе в таких условиях происходит изнашивание подшипника, что является основной причиной выхода из строя машины.

В основном подшипники скольжения выполняют из антифрикционного материала (бронза, сплавы на основе алюминия и др.) [1]. Но все эти материалы подвержены абразивному изнашиванию и недолговечны. В последние годы основным материалом для изготовления подшипников является карбид кремния. Но такие опоры скольжения растрескиваются из-за высокой хрупкости материала. Поэтому применяют материалы, которые имеют более высокие прочностные характеристики при работе в усложненных условиях (высокие температуры, абразивное изнашивание).

При таких условиях целесообразно применять упорные подшипники, представляющие собой стальную подложку с нанесенным на нее полимерным покрытием. Сталь придает материалу более высокую прочность, а полимерное покрытие создает приработку трущихся поверхностей.

Основным трибоматериалом в условиях повышенных температур являются композиты на основе полиэфирэфиркетона (ПЭЭК), ,благодаря их высоких термо- и износостойкости. На основе испытаний установили, что композиты с содержанием ПЭЭК обладают высокой ударной прочностью.

Для увеличения износостойкости в ПЭЭК вводят упрочняющие добавки. Хорошей способностью уменьшать износ полимеров обладает политетрафторэтилен (ПТФЭ). ПТФЭ очень хорошо снижает коэффициент трения. Такое же хорошее влияние оказывает и другой наполнитель – карбид кремния[1].

Нанесение такого полимерного материала на стальное основание позволяет получить упорный подшипник скольжения с более высокими показателями износостойкости и долговечности.

Список литературы

1. Алексеева Е.В. Применение полимерного покрытия для повышения износостойкости упорных подшипников скольжения // Новые материалы и технологии в машиностроении: сборник материалов по итогам Международной научно-технологической конференции / под ред. Е.А. Панфилова. – Брянск, БГИТА. 2006. – С. 41-45.

МЕХАНИЗМ МИКРОСТРУКТУРНЫХ ИЗМЕНЕНИЙ ПРОЦЕССА УПРОЧНЕНИЯ ВЫСОКОМАРГАНЦОВИСТОЙ СТАЛИ ПРИ СТАТИКО–ИМПУЛЬСНОЙ ОБРАБОТКЕ

Селина Д.В., Кокорева О.Г.

Муромский институт Владимирского государственного университета, Муром, e-mail: mivlgu@mail.ru

Упрочнение поверхностно-пластичной деформацией (ППД) обусловлено разнообразными по физической природе явлениями, которые определяются условиями нагружения детали и оцениваются следующими параметрами: степенью и глубиной упрочнения, микроструктурой, твердостью, пределом усталости и временным сопротивлением, ударной вязкостью и т.д. Увеличение прочности металла связано с формируемой дислокационной структурой. Характер этой структуры зависит от типа кристаллической решетки, степени упрочнения (пластической деформации) и температуры деформирования.

Энергия при статико-импульсном взаимодействии поглощается металлом, часть которой проявляется в форме деформационного упрочнения. Последнее представляет собой сопротивление металла его дальнейшему деформированию. Количественно его определяем измерением твердости при внедрении. Наиболее интенсивное упрочнение достигается на ранних стадиях деформации. Как и можно было ожидать, максимальное возрастание твердости достигается там, где деформация была наибольшей. Распределение твердости от поверхности по глубине для упрочненных СИО образцов из высокомарганцовистой стали (ВМС) характеризуется достаточно равномерным убыванием. Это связано с течением зерен, которое сочетается с двойникованием, весьма интенсивным у поверхности и затухающим на некотором расстоянии от поверхности. Для характеристики зависимости числа двойников от твердости при распределении по глубине упрочненного образца из стали110Г13Л рассмотрим следующую зависимость:

$$D = \left(2 + K_{д}\right)\frac{\Delta h}{N},$$

где D – число двойников; $K_{д}$ – коэффициент характеризующий количественную однородность двойников (определяется по таблице); Δh – расстояние по глубине образца; N – номер площадки твердости.

Номер площадки твердости, N	1	2	3	4	5	6	7	8
Коэффициент однородности двойников, $K_{д}$	0	1	1	0	1	1	0	1

МЕТАЛЛОГРАФИЧЕСКИЕ ИССЛЕДОВАНИЯ ОБРАЗЦОВ,УПРОЧНЕННЫХ СТАТИКО-ИМПУЛЬСНОЙ ОБРАБОТКОЙ

Селина Д.В., Кокорева О.Г.

Муромский институт Владимирского государственного университета, Муром, e-mail: mivlgu@mail.ru

Металлографические исследования образцов, упрочненных статико-импульсной обработкой, показали наличие площадок постоянной твердости, которые связаны определенным образом с распределением ударных двойников (рисунок).

Обнаружена зависимость между максимальным числом направлений двойников в отдельном зерне и положением площадки твердости. Число направлений уменьшается при переходе на каждую следующую площадку. Так, металлографические исследования показали, что наибольшее число направлений двойников в отдельном зерне в области первой площадки оказалось равным четырем. Во второй площадке наибольшее число направлений двойников равно трем; для третьей и четвертой число направле-