

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 сложных 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 высоким 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 высокомарганцевистой 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 стали 110Г13Л рассмотрим следующую зависимость:

$$D = (2 + K_d) \frac{\Delta h}{N},$$

где D – число двойников; K_d – 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_d	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-