УДК 004.032.24 **doi: 10.20998/2522-9052.2017.2.11**

Г. Г. Швачич, Е. В. Иващенко, В. В. Бусыгин

Национальная металлургическая академия Украины, Днепр, Украина

НЕКОТОРЫЕ АСПЕКТЫ ОРГАНИЗАЦИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ФУНКЦИОНИРОВАНИЯ МНОГОПРОЦЕССОРНЫХ ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ

Предметом исследования является усовершенствование особенностей организации информационной безопасности функционирования многопроцессорных вычислительных систем. **Цель** работы заключается в определении и реализации мероприятий по защите информации, которые могут быть эффективны при использовании многопроцессорных модульных вычислительных систем или при параллельных расчетах на многопоточных системах. Решаются следующие **задачи**: сравнение методов защиты данных в многопроцессорных и последовательных системах, а также рассмотрение особенностей применения различных криптографических методов на методы реализации защиты; рассмотрение и выявление ключевых элементов, которые требуют особенного внимания при разработке системы безопасности. Используемыми **методами** являются: основные положения теорий вычислительных систем, параллельных вычислений, построения операционных систем, методы и алгоритмы защиты данных. Получены следующие **результаты**. Выявлены основные аспекты в определении и использовании мероприятий по защите информации, которые могут быть эффективны при использовании многопроцессорных модульных вычислительных систем или при параллельных расчетах на многопоточных системах. Проведено сравнение методов защиты данных с последовательными системами, а также рассмотрено влияние применения различных криптографических методов на методы реализации защиты данных. Показано, что основной выбор методов защиты данных в многопроцессорных системах определяется отличиями от последовательных систем в теоретической и аппаратной реализации. **Выводы.** Показано, что для параллельной системы требуется больше аппаратных и программных средств и с каждым дополнительным модулем вычисления система усложняется. А это, в свою очередь, еще больше усложняет систему защиты в целом, что может повлечь некоторое замедление при выполнении прикладных программ при помощи многопроцессорных вычислительных систем. Однако в перспективе предложенный подход позволяет обеспечить повышенную безопасность функционирования многопроцессорных систем. Для защиты данных в таких системах рассматривается и анализируется ряд методов.

Ключевые слова: многопроцессорная вычислительная система; вычислительные узлы; криптографические алгоритмы; защита данных; ядро; сети; ключи; операционная система.

Введение

На современном этапе все большую роль в дальнейшем развитии информационных ресурсов играют параллельные вычислительные системы и вычисления [1 − 6]. Подобные системы находят применение в сфере военных, экономических, технологических и других процессов. В связи с их развитием, внедрением и совершенствованием широкое распространение получили методы нанесения ущерба таким ресурсам. Наибольший интерес вызывают проблемы исследования методов и средств защиты информации в параллельных вычислительных процессах. В настоящее время подобные исследования не приобрели надлежащего развития. Изучение и разработка подобной проблематики предоставит возможность для дальнейшего развития новых и уже существующих методов защиты информации. Таким образом, одной из основных проблем использования многопроцессорной и параллельной вычислительной системы является реализация методов защиты информации.

Проблема реализации методов защиты информации имеет два аспекта:

− разработка средств, реализующих криптографические алгоритмы,

− методика использования этих средств.

Предложенные далее криптографические методы могут быть реализованы либо программным, либо аппаратным способом. Возможность программной реализации обуславливается тем, что все методы криптографического преобразования формальны и могут быть представлены в виде конечной алгоритмической процедуры.

При аппаратной реализации все процедуры шифрования и дешифрования выполняются специальными электронными схемами. Наибольшее распространение получили модули, реализующие комбинированные методы. Анализируя некоторые аспекты информационной безопасности модульных вычислительных систем можно отметить следующее:

1. Вычислительную сеть многопроцессорной системы можно считать безопасной с точки зрения обработки информации, если в ней предусмотрена централизованная система управляемых и взаимоувязанных препятствий, которая перекрывает с гарантированной надежностью (в соответствии с моделью потенциального нарушителя) количество возможных каналов несанкционированного доступа и угроз, направленных на потерю или модификацию информации, а также несанкционированное ознакомление с ней посторонних лиц.

2. При проектировании мероприятий защиты данных в параллельных вычислительных системах необходимо провести анализ мест хранения информации, интерфейса управления данными и каналами их передачи (локальными сетями или другими подобными средствами обмена данными). При этом основной аспект защиты данных должен быть направлен, в первую очередь, на защиту интерфейса управления дан-

ными, во вторую очередь, на защиту интерфейса обмена данными, и далее на места хранения информации, поскольку они наиболее уязвимы для несанкционированного доступа в параллельных моделирующих средах. Своевременная защита позволит обеспечить надежность функционирования таких систем.

Анализ проблемы и постановка задачи

В наше время круг задач, требующих для своего решения мощных вычислительных ресурсов, еще более расширился. Это связано с тем, что произошли фундаментальные изменения в самой организации научных исследований. Вследствие широкого внедрения вычислительной техники значительно усилилось направление численного моделирования и численного эксперимента. Численное моделирование, заполняя промежуток между физическими экспериментами и аналитическими подходами, позволило изучать явления, которые являются либо слишком сложными для исследования аналитическими методами, либо слишком дорогостоящими или опасными для экспериментального изучения. При этом численный эксперимент позволил значительно удешевить процесс научного и технологического поиска. Стало возможным моделировать в реальном времени процессы интенсивных физико-химических и ядерных реакций, глобальные атмосферные процессы, процессы экономического и промышленного развития регионов и т.д. Очевидно, что решение таких масштабных задач требует значительных вычислительных ресурсов.

Подавляющее большинство функционирующих супервычислительных установок являются фактически многопроцессорными параллельными вычислительными системами MPP архитектуры (Massively Parallel Processing) [1 – 5]. Многопроцессорные вычислительные системы, сконструированные на локальных сетях, стали называться «кластерными системами» или просто «кластерами». Это объясняется тем, что логически MPP – система мало отличается от обычной локальной сети. Анализ путей развития высокопроизводительных установок показывает, что реального перелома в овладении технологиями параллельных вычислений можно достичь развитием дополнительного (фактически базового) уровня в иерархии мощностей аппаратных средств многопроцессорных вычислительных систем MPP-архитектуры – персональных вычислительных кластеров [3, 5]. Область применения таких систем – овладение технологиями параллельных вычислений, создание и отладка параллельных программ, в т.ч. проблемно-ориентированных пакетов и библиотек, а также модельная прогонка разработанного ПО.

Однако проблемы, возникающие при организации информационной безопасности функционирования многопроцессорных вычислительных систем, как правило, являются первостепенными и требуют глубокого изучения и исследования. При чем такого рода исследования в настоящее время не получили своего развития. В тоже время, тенденции роста киберпреступности требуют особого внимания к проблеме защиты данных таких систем и их программного обеспечения. В этой связи, поставленная в данной работе задача является актуальной и первоочередной.

Решение проблемы

1. Анализ информационной безопасности функционирования многопроцессорных вычислительных систем

На первом этапе рассмотрим существующие виды информационных угроз. Такие угрозы можно разделить на две больших группы:

− отказы и нарушения работоспособности программных и технических средств;

− преднамеренные угрозы, которые загодя планируются злоумышленниками для задания вреда.

Выделяют следующие основные группы причин сбоев и отказов в работе компьютерных систем:

− нарушение физической и логической целостности структур данных, которые хранятся в оперативной и внешней памяти, что возникает вследствие старения или преждевременного износа их носителей;

− нарушения, которые возникают в работе аппаратных средств из-за их старения или преждевременного износа;

− нарушение физической и логической целостности структур данных, которые хранятся в оперативной и внешней памяти, что возникает вследствие некорректного использования компьютерных ресурсов;

− нарушения, которые возникают в работе аппаратных средств из-за неправильного использования или повреждения, в том числе из-за неправильного использования программных средств;

− не устраненные ошибки в программных средствах, не выявленные в процессе отладки и испытаний, а также те, что остались в аппаратных средствах после их разработки.

Рассмотрим некоторые аспекты теории последовательного и параллельного программирования.

Параллельная программа – это огромное количество параллельных процессов, которые взаимодействуют (синхронизируют свою работу и обмениваются данными) при помощи передачи сообщений. Идея распараллеливания вычислений основана на том, что большинство заданий представляются в виде совокупности меньших заданий, которые могут быть решены одновременно. Обычно параллельные вычисления требуют координации действий. Параллельное программирование включает все черты традиционного, последовательного программирования, но в нем есть три дополнительных, четко определенных этапа. Это:

− *определение параллелизма*: анализ задания с целью выделить подзадачи, которые могут выполняться одновременно;

− *выявление параллелизма*: изменение структуры задания так, чтобы можно было эффективно выполнять подзадачи. Для этого часто требуется найти зависимости между подзадачами и организовать начальный код так, чтобы ими можно было эффективно управлять;

− *выражение параллелизма*: реализация параллельного алгоритма в начальном коде при помощи

системы обозначений параллельного программирования.

На основании изложенного можно отметить, что основное отличие параллельной системы - это увеличение количества подзадач, которые пересылаются и могут выполняться одновременно, а также наличие отдельной системы управления этими подзадачами. Заметим, что с точки зрения ядра операционной системы поддержка кластеров и распределенных систем заключается в эффективной работе с сетью. С некоторым упрощением любую современную высокопроизводительную вычислительную систему можно представить как огромное количество многопроцессорных вычислительных узлов, связанных одной или несколькими коммуникационными сетями [7].

2. Организация информационной безопасности ресурсов многопроцессорных вычислительных систем

Вычислительную сеть можно считать безопасной в смысле обработки информации, если в ней предусмотрена централизованная система управляемых и взаимосвязанных препятствий, которые перекрывают с гарантированной прочностью количество возможных каналов несанкционированного доступа и угроз, направленных на потерю или модификацию информации, а также несанкционированное ознакомление с ней посторонних лиц.

При проектировании защиты параллельных систем, необходимо провести анализ мест хранения информации, интерфейса управления данными и каналами передачи (локальными сетями или другими подобными средствами обмена). При этом основной аспект защиты должен быть, в первую очередь, направлен на защиту интерфейса управления данными, во вторую очередь, на защиту интерфейса обмена данными и в дальнейшем на места хранения информации, поскольку они определяются как наиболее уязвимые для несанкционированного доступа. В свою очередь, своевременная защита позволит обеспечить надежность и отказоустойчивость системы в целом.

Упрощенная система защиты информационных ресурсов многопроцессорных вычислительных систем в общем виде представлена на рис. 1.

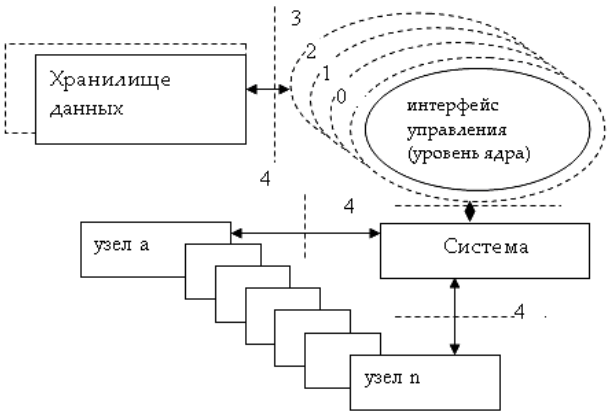

Рис. 1. Упрощенная система защиты информационных ресурсов многопроцессорных вычислительных систем

При определении защиты интерфейса управления, возможно, использовать рекомендации корпорации Intel, которая предлагает следующие уровни привилегий: 0 – ядро операционной системы; 1 – операционная система; 2 – системы программирования и базы данных; 3 – прикладные программы (предназначены для пользователя); 4 – на уровне коммутации целесообразно использовать как криптографические, так и аппаратные методы защиты; 5 – на уровне хранения желательно использовать криптографические и аппаратные методы в системе распределенного хранения информации. Подобные системы предусматривают внешний доступ и управление соответственно. При этом должны использоваться и методы защиты удаленных подключений.

Основными параметрами транспортной среды с коммутацией пакетов являются количество коммутаторов (r) и длина заглавия (h), от которых непосредственно зависит время доставки массива информации. Именно величины r и h предопределяют возможность адаптации времени доставки массива данных D к конкретным узлам системы.

Поэтому процесс выбора необходимого времени доставки массива данных объемом D байтов, выходя из заданных значений величин r и h, будет определяться на основании соотношения:

$$T_{A\to B}^{D} = D(r+1) + \sum_{i=1}^{r+1} h_i .$$

Величина D будет меняться для систем многоканальной доставки данных с одинаковым и разным количеством транзита. Эта величина будет непосредственно зависеть от времени обработки информации (например, методы шифровки, архивации и т.д.). Наиболее полная транспортная среда описана Н.И. Алишовим [8].

3. Организации безопасности информационных ресурсов в корпоративных сетях

Рассмотрим подсистему организации безопасности информационных ресурсов в корпоративных сетях, в частности распределенных вычислительных сетях. Подсистема включает: данные, средства обработки (аппаратные и программные), активные компоненты (процессы и действия пользователей). Представим подсистему организации безопасности в виде схемы (рис. 2).

На схеме цифрами отмечены:

– аппаратные и программные средства обработки в системе коммутации;

– процессы и действия пользователей.

Для параллельной системы требуется больше аппаратных и программных средств и с каждым дополнительным модулем вычисления система усложняется. А это, в свою очередь, еще больше усложняет систему защиты в целом, снижая в некоторой степени общую вычислительную мощность.

Для защиты данных в таких системах используются указанные ниже методы и алгоритмы:

алгоритмы запутывания – используются хаотические переходы в разные части кода, внедрения

ошибочных процедур - "пустышек", холостые циклы, искажение количества реальных параметров процедур ПО, разброс участков кода по разным областям ОЗУ и тому подобное;

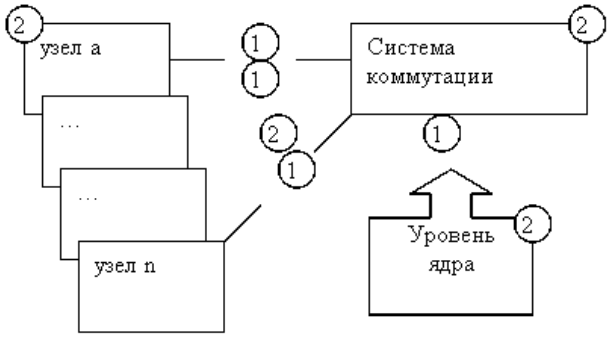

Рис. 2. Подсистема организации безопасности информационных ресурсов в корпоративных сетях

алгоритмы мутации – создаются таблицы соответствия операндов – синонимов и замена их друг на друга при каждом запуске программы по определенной схеме или случайному образу, случайные изменения структуры программы;

алгоритмы компрессии данных – программа упаковывается, а потом распаковывается по мере выполнения;

алгоритмы шифровки данных – программа шифруется, а потом расшифровывается по мере выполнения.

Вычисление сложных математических выражений в процессе отработки механизма защиты - элементы логики защиты зависят от результата вычисления значения какой-либо формулы или группы формул. Методы затруднения дизассемблирования - используются разные приемы, направленные на предотвращение дизассемблирования в пакетном режиме. Методы затруднения отладки - используются разные приемы, направленные на осложнение отладки программы.

Эмуляция процессоров и операционных систем - создается виртуальный процессор и операционная система (не обязательно реально существующие) и программа-переводчик из системы команд IBM в систему команд созданного процессора или ОС; после такого перевода ПО может выполняться только с помощью эмулятора, который резко затрудняет исследование алгоритма ПО.

Нестандартные методы работы с аппаратным обеспечением - модули системы защиты обращаются к аппаратуре ЭВМ, минуя процедуры операционной системы, и используют малоизвестные или недокументируемые ее возможности.

Из рассмотренного выше можно заключить, что основным отличительным звеном уязвимости параллельных систем, являются апаратно-программные средства системы коммутации (так как увеличивается их число) в соответствии с требованиями решаемых задач. Поэтому для средств коммутации актуальным является применение методов шифрования данных.

Существует симметричное (традиционное) и асимметричное шифрование данных. Они известны и применяются во многих последовательных системах. Однако наиболее перспективным для исследования и дальнейших модификаций в параллельных системах является метод блуждающих ключей.

4. Защита данных при помощи метода блуждающих ключей

Проблема распределения ключей является наиболее острой в больших информационных системах, к которым можно отнести большую часть параллельных систем. Частично эта проблема решается (а точнее снимается) за счет использования открытых ключей. Но наиболее надежные криптосистемы с открытым ключом типа RSA достаточно трудоемки, а для шифрования мультимедийных данных и вовсе не приспособлены. Оригинальные решения проблемы "блуждающих ключей" активно разрабатываются специалистами [9 – 11]. Эти системы являются некотором компромисом между системами с открытыми ключами и обычными алгоритмами, для которых требуется наличие одного и того же ключа и у отправителя и у получателя.

Рассмотрим суть идеи метода. После того, как ключ использован в одном сеансе, по некоторому правилу он изменяется в другом. Это правило должно быть известно и отправителю, и получателю. Зная такое правило, при получении очередного сообщения получатель тоже меняет ключ. Если правила изменения ключей придерживается и отправитель, и получатель, то в каждый момент времени они имеют одинаковый ключ. Постоянное изменение ключа затрудняет раскрытие информации злоумышленником.

Основное задание в реализации этого метода – выбор эффективного правила изменения ключей. Наиболее простой путь - генерация случайного списка ключей. Изменение ключей осуществляется в порядке списка. Однако очевидно, список придется каким-то образом передавать.

Другой вариант - использование математических алгоритмов, основанных на так называемых перебирающих последовательностях. На огромном количестве ключей путем одной и той же операции над элементом выходит другой элемент. Последовательность этих операций позволяет переходить от одного элемента к другому, пока не будет перебрано все множество.

5. Реализация криптографических методов

Проблема реализации методов защиты информации имеет два аспекта (рис. 3):

− разработку средств, реализующих криптографические алгоритмы;

− методику использования этих средств.

Каждый из рассмотренных криптографических методов может быть реализован или программным, или аппаратным способом. Возможность программной реализации обусловливается тем, что все методы криптографического превращения формальны и могут быть представлены в виде конечной алгоритмической процедуры. При апаратной реализации все процедуры шифрования и дешифрования выполняются специальными электронными средствами.

Наибольшее распространение получили модули, реализующие комбинированные методы.

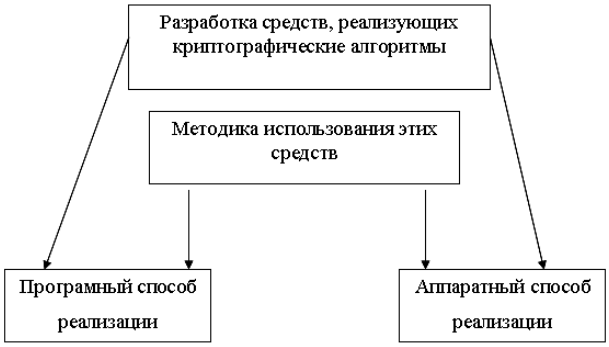

Рис. 3. Схема реализации криптографических методов защиты данных

Рассмотрим практическую реализацию данных методов. Осветим при этом несколько базовых алгоритмов шифрования.

5.1. Алгоритм DES

DES (Data Encryption Standart) – это симметричный алгоритм шифрования, т. е. один ключ используется как для зашифровки, так и для расшифровки сообщений. Разработан фирмой IBM и утвержден правительством США в 1977 как официальный стандарт. DES имеет блоки по 64 бит и основан на 16-ти кратной перестановке данных, для зашифровки использует также ключ в 56 бит. Существует несколько режимов DES, например Electronic Code Book (ECB) и Cipher Block Chaining (CBC). 56 бит - это 8 семибитовых ASCII символов, т. е. пароль не может быть длиннее 8 букв. Если вдобавок использовать только буквы и цифры, то количество возможных вариантов будет гораздо меньше максимально возможных 256.

Рассмотрим один из шагов алгоритма DES. Входной блок данных делится пополам на левую (L') и правую (R') части. После этого формируется выходной массив так, что его левая часть L" представлена правой частью R' входного; из 32-битового слова R' с помощью битовых перестановок формируется 48-битовое слово. К полученному 48-битовому слову и 48-битовому раундовому ключу применяется операция XOR. Результирующее 48-битовое слово разбивается на 8 6-битовых групп; каждая 6-битовая группа с помощью соответствующего S-box'a заменяется на 4-битовую группу, и из полученных восьми 4-битовых групп составляется 32-битовое слово. К полученному слову и L' применяется XOR, в результате получается R". Можно убедиться, что все проведенные операции могут быть обратимы, и расшифровка может осуществляться за число операций, линейно зависящее от размера блока. После нескольких таких проходов можно считать, что каждый бит выходного блока шифровки может зависеть от каждого бита сообщения.

5.2. Алгоритм “тройной DES”

Так как текст, зашифрованный двойным DES (встреча на середине (meet in the middle)), оказывается хрупким при криптографической атаке, то текст шифруется 3 раза DES. Таким образом, длина ключа возрастает до 168-бит (56x3). Не всегда применение тройного DES означает увеличение уровня безопасности сообщения. Типы тройного шифрования DES:

– DES-EEE3: шифруется 3 раза с 3 различными ключами;

– DES-EDE3: 3 DES операции шифрование - дешифрование - шифрование с 3 разыми ключами;

– DES-EEE2 и DES-EDE2: как и предыдущие, за исключением того, что первая и третья операции используют одинаковый ключ.

В табл. 1 приведено сравнение различных видов DES шифрования.

5.3. Алгоритм ГОСТ

ГОСТ предусматривает 3 режима шифрования (простая замена, гаммирование, гаммирование с обратной связью) и один режим выработки имитовставки. Первый из режимов шифрования предназначен для шифрования ключевой информации и не может использоваться для шифрования других данных, для этого предусмотрены два других режима шифрования. Режим выработки имитовставки (криптографической контрольной комбинации) предназначен для имитозащиты шифруемых данных, то есть для их защиты от случайных или преднамеренных несанкционированных изменений.

Алгоритм построен по тому же принципу, что и DES – это классический блочный шифр с секретным ключом – однако отличается от DES'a большей длиной ключа, большим количеством раундов, и более простой схемой построения самих раундов.

Таблица 1. **Сравнение видов DES шифрования**

Тип шифрования	*Колич. ключей*	*Вычисление (Computation)*	*Хранение (Storage)*	*Тип атаки*
Одиночный	1	256	-	known plaintext
Одиночный	1	238	238	chosen plaintext
Одиночный	1	-	256	chosen plaintext
Двойной	2	2112	-	known plaintext
Двойной	2	256	256	known plaintext
Двойной	2	-	2112	chosen plaintext
Тройной	2	2112	-	known plaintext
Тройной	2	256	256	256 chosen plaintext
Тройной	2	2(120- t)	-	2t known plaintext
Тройной	2	-	256	chosen plaintext
Тройной	3	2112	256	known plaintext
Тройной	3	256	2112	chosen plaintext

Из-за намного большей длины ключа ГОСТ гораздо устойчивей DES'a к вскрытию "грубой силой" – путем полного перебора по множеству возможных значений ключа.

Функция шифрования ГОСТа гораздо проще функции шифрования DES'a, она не содержит операций битовых перестановок, коими изобилует DES и которые крайне неэффективно реализуются на современных универсальных процессорах (хотя очень просто аппаратно - путем разводки проводников в кристалле или на плате). В силу сказанного, при вдвое большем количестве раундов (32 против 16) программная реализация ГОСТа на процессорах Intel x86 более чем в 2 раза превосходит по быстродействию реализацию DES'a. Естественно, сравнивались близкие к оптимуму по быстродействию реализации.

Из других отличий ГОСТа от DES'a надо отметить следующие: На каждом раунде шифрования используется "раундовый ключ", в DES'е он 48-битовый и вырабатывается по относительно сложному алгоритму, включающему битовые перестановки и замены по таблице, в ГОСТе он берется как фрагмент ключа шифрования. Длина ключа шифрования в ГОСТе равна 256 битам, длина раундового ключа - 32 битам, итого получаем, что ключ шифрования ГОСТа содержит 256/32=8 раундовых ключей. В ГОСТе 32 раунда, следовательно, каждый раундовый ключ используется 4 раза, порядок использования раундовых ключей установлен в ГОСТе и различен для различных режимов. Таблица замен в ГОСТе - аналог S-блоков DES'a - представляет собой таблицу (матрицу) размером 8x16, содержащую число от 0 до 15. В каждой строке каждое из 16-ти чисел должно встретиться ровно 1 раз. В отличие от DES'a, таблица замен в ГОСТе одна и та же для всех раундов и не зафиксирована в стандарте, а является сменяемым секретным ключевым элементом. От качества этой таблицы зависит качество шифра. При "сильной" таблице замен стойкость шифра не опускается ниже некоторого допустимого предела даже в случае ее разглашения. И наоборот, использование "слабой" таблицы может уменьшить стойкость шифра до недопустимо низкого предела.

5.4. Шифр Blowfish

Blowfish – это 64-битный блочный шифр разработанный Шнайером (Schneier) в 1993 году. Это шифр Файстела (Feistel) [12], и каждый проход состоит из зависимой от ключа перестановки и зависимой от ключа с данными замены. Все операции основаны на операциях XOR и прибавлениях к 32-битным словам (XORs and additions on 32-bit words). Ключ имеет переменную длину (максимально 448 бит) и используется для генерации нескольких подключевых массивов (subkey arrays). Шифр был создан специально для 32-битных машин и существенно быстрее DES.

5.5. Шифр RC5

RC5 – это довольно быстрый блочный шифр, разработанный Ривестом для RSA Data Security. Этот алгоритм параметричный, т.е. с переменным размером блока, длиной ключа и переменным числом проходов. Размер блока может быть 32, 64, или 128 битов. Количество проходов в промежутке от 0 до 2048 бит. Параметричность такого рода дает гибкость и эффективность шифрования. RC5 состоит из ввода ключа (key expansion), шифрования и дешифровки. При вводе ключа вводятся также количество проходов, размер блока и т.д. Шифрование состоит из 3 примитивных операций: сложения, побитового XOR и чередования (rotation). Исключительная простота RC5 делает его простым в использовании. RC5 текст, также как и RSA, может быть дописан в конец письма в зашифрованном виде. Безопасность RC5 основывается на зависящих от данных чередования и смешивания результатах различных операций. RC5 с размером блока 64 бита и 12 или более проходов обеспечивает хорошую стойкость к дифференциальному и линейному криптоанализу.

5.6. Шифр IDEA

IDEA (International Data Encryption Algorithm) - это вторая версия блочного шифра, разработанная К. Лейем (Lai) [13] и Д. Месси (Massey) в конце 80-х. Это шифр, состоящий из 64-битных повторяющихся блоков со 128-битным ключом и восемью проходами (rounds). Хотя этот шифр не является шифром Файстела, дешифровка выполняется по тому же принципу, что и шифрование. Структура шифра была разработана для легкого воплощения как программно, так и аппаратно, и безопасность IDEA основывается на использовании трех несовместимых типов арифметических операций над 16-битными словами. Скорость программного IDEA сравнима со скоростью DES. Один из принципов создания IDEA – затруднить дифференциальный криптоанализ. Ни одна линейная криптоаналитическая атака не закончилась успешно, как и не было выявлено алгебраически слабых мест. Самый полный анализ провел Daemen. Он открыл большой класс 251 слабых ключей, при использовании которых в процессе шифрования ключ может быть обнаружен и восстановлен. Однако, в IDEA существует 2128 возможных вариантов ключей, поэтому это открытие не влияет на практическую безопасность шифра.

5.7. Шифр RSA

RSA (авторами являются Rivest, Shamir и Alderman) – это система с открытым ключом (public-key), предназначенная как для шифрования, так и для аутентификации. Она основана на трудности разложения очень больших целых чисел на простые сомножители. RSA – очень медленный алгоритм. Для сравнения: на программном уровне DES по меньшей мере в 100 раз быстрее RSA, на аппаратном – в 1000-10000 раз, в зависимости от выполнения. Алгоритм RSA состоит в следующем:

– для двух очень больших целых чисел P и Q определяются N=PQ и M=(P - 1)(Q - 1);

– выбирается случайное целое число D, взаимно простое с M, и вычисляется E = (1 mod M)/D;

– D и N публикуются как открытый ключ, а E сохраняется в тайне;

– пусть S – сообщение. Его длина определяется значением выражаемого им целого числа и находит-

ся в интервале (1, N). S превращается в шифровку возведением в степень D по модулю N и отправляется получателю S ' = (SD mod N);

– получатель сообщения расшифровывает его, возведя в степень E (число E ему уже известно) по модулю N, т. к. S = ((S ')D mod N) = (SDE mod N).

5.8. Шифрование PGP

Pretty Good Privacy(PGP) - это программный пакет, разработанный Филипом Циммерманом (Philip Zimmerman), который обеспечивает шифровку почты и файлов. Циммерман взял существующие криптосистемы и криптографические протоколы и разработал бесплатную (freeware) программу для различных платформ. Она обеспечивает шифрование сообщений, цифровые подписи и совместимую почту (email compatibility).

Алгоритмы, используемые для шифрования сообщений - это RSA для передачи ключа и IDEA для самого шифрования сообщений. Цифровые подписи достигаются при использовании RSA для подписи и MD5 для вычисления дайджеста сообщения (message digest). PGP использует ZIP компрессию, а также маскирует координаты и данные отправителя, что немного осложняет процесс анализа трафика. Совместимость почты достигается путем использования Radix-64 конвертации (conversion).

Выводы

В работе показано, что в настоящее время наибольший интерес вызывают проблемы исследования методов и средств защиты информации в параллельных вычислительных процессах. Это объясняется тем, что подобные исследования не приобрели надлежащего развития. Изучение и разработка подобной проблематики позволяет создать новые и развить уже существующие методов защиты информации.

В работе показано, что для параллельной системы требуется больше аппаратных и программных средств и с каждым дополнительным модулем вычисления система усложняется. А это, в свою очередь, еще больше усложняет систему защиты в целом, что может повлечь некоторое замедление при выполнении прикладных программ. Однако в перспективе предложенный подход позволяет обеспечить повышенную безопасность функционирования многопроцессорных систем. Для защиты данных в таких системах рассматривается и анализируется ряд методов. В соответствии с некоторыми аспектами построения многопроцессорных систем рассмотрены и выявлены ключевые элементы, которые требуют особенного внимания при разработке системы безопасности. Показано, что основной выбор методов защиты данных в многопроцессорных системах определяется отличиями от последовательных систем в теоретической и аппаратной реализации.

Показано, что на современном этапе комбинированные средства шифрования, включающие программно-аппаратные средства являются наиболее актуальными как в плане использования так и в плане разработок. При этом выявлено, что выбор метода реализации криптозащиты для параллельной вычислительной системы зависит от ее направленности и конструктивных особенностей, а использование блуждающих ключей предоставляет возможность повысить универсальность системы, при невысоких потерях производительности.

СПИСОК ЛИТЕРАТУРЫ

1. Rajkumar B. High Performance Cluster Computing. New Jersey: Prentice-Hall, 1999. 453 p.
2. Xu Z. Scalable Parallel Computing Technology, Architecture, Programming . Boston: McGraw-Hill, 1998. 557 p.
3. Shvachych G.G., Tkach M.A., Shcherbyna P.A. About problems of designing of the high-efficiency integrated environment on the basis of computing clusters. Nauka i inowacja – 2008: Przemysl : Nauka i stadia, 2008. S. 41 – 46.
4. Beowulf Introduction & Overview [Електронний ресурс]. Режим доступа: http://www.beowulf.org (24.05.2017).
5. Shvachych G.G. Prospects of construction highly productive computers systems on the base of standard technologies. Strategy of Quality in Industry and Education: IV Int. Conf.; May 30 – June 6, 2008; Varna; Bulgaria, 2008. V. 2. P. 815 – 819.
6. Buyya R. High Performance Cluster Computing. USA, 1999.
7. Лацис А.О. Как построить и использовать суперкомпьютер. М.: Бестселлер, 2003. 240 с.
8. Алишов Н.И. Развитые методы взаимодействия ресурсов в распределенных системах. К.: Сталь, 2009. 448 с.
9. Brassard J. Modern Cryptology. Springer – Verlag, Berlin – Heidelberg,1988. 107 p.
10. Capocelli R.M., De Santis A., Gargano L., Vaccaro U. On the Size of Shares for Secret Sharing Schemes. J. Cryptology. 1993. V.6. P. 157–167.
11. Goldreich O. On the Foundations of Modern Gryptography. Proc. of CRYPTO'97, LNCS. 1997. V.1294. P. 46–74.
12. Feistel Horst. Cryptography and Computer Privacy. Scientific American. Vol. 228, No. 5. 1973.
13. Zheng Gong, Xuejia Lai, Kefei Chen. A Synthetic Indifferentiability Analysis of Some Block-Cipher-Based Hash Functions, 2009. P. 293-385.

REFERENCES

1. Rajkumar, B. (1999), *High Performance Cluster Computing*, New Jersey, Prentice-Hall, 453 p.
2. Xu, Z. (1998), *Scalable Parallel Computing Technology, Architecture, Programming*, McGraw-Hill, Boston, 557 p.
3. Shvachych, G.G., Tkach, M.A. and Shcherbyna, P.A. (2008), “About problems of designing of the high-efficiency integrated environment on the basis of computing clusters”, *Nauka i inowacja*, Materiály IV Midznarodnej naukowi-praktyznej konferencji,T. 11. Nowoczesne informacyine technologie, Nauka i stadia, Przemysl, pp. 41–46.
4. *Beowulf Introduction & Overview*, available at: http://www.beowulf.org (last accessed May 24, 2017).
5. Shvachych, G.G. (2008), “Prospects of construction highly productive computers systems on the base of standard technologies”, *Strategy of Quality in Industry and Education*, IV Int. Conf.; May 30 – June 6; Varna; Bulgaria, Vol. 2. pp. 815–819.

6. Buyya, R. (1999), *High Performance Cluster Computing*, USA.
7. Latsis, A.O. (2003), *How to build and use a supercomputer*, Bestseller, Moscow, 240 p.
8. Alishov, N.I. (2009), *Developed methods for interaction of resources in distributed systems*, Stal, Kyiv, 448 p.
9. Brassard, J. (1988), *Modern Cryptology, Springer* – Verlag, Berlin – Heidelberg, 107 p.
10. Capocelli, R.M., De Santis, A., Gargano, L. and Vaccaro, U. (1993), "On the Size of Shares for Secret Sharing Schemes", *J. Cryptology*, V.6, pp. 157–167.
11. Goldreich, O. (1997), On the Foundations of Modern Gryptography, Proc. of *CRYPTO'97*, LNCS, Vol. 1294, pp. 46–74.
12. Horst, Feistel (1973), "Cryptography and Computer Privacy"*, Scientific American*, Vol. 228, No. 5.
13. Zheng, Gong, Xuejia, Lai and Kefei, Chen (2009), *A Synthetic Indifferentiability Analysis of Some Block-Cipher-Based Hash Functions,* pp. 293-385.

Надійшла (received) 25.06.2017
Прийнята до друку (accepted for publication) 18.10.2017

Деякі аспекти організації інформаційної безпеки функціонування багатопроцесорних обчислювальних систем

Г. Г. Швачич, О. В. Іващенко, В. В. Бусигін

Предметом дослідження є удосконалення особливостей організації інформаційної безпеки функціонування багатопроцесорних обчислювальних систем. **Мета** роботи полягає у визначенні та реалізації заходів щодо захисту інформації, які можуть бути ефективними при використанні багатопроцесорних модульних обчислювальних систем. Для досягнення поставленої мети вирішуються наступні **задачі**: порівняння методів захисту даних у багатопроцесорних і послідовних системах, а також розгляд особливостей застосування різних криптографічних методів на методи реалізації захисту; відповідно до деяких аспектів побудови багатопроцесорних систем розгляд і виявлення ключових елементів, які вимагають особливої уваги при розробці системи безпеки; показати, що основний вибір методів захисту даних у багатопроцесорних системах визначається відмінностями від послідовних систем в теоретичній і апаратній реалізації. Використовуваними **методами** є: основні положення теорії обчислювальних систем, теорії паралельних обчислень, теорії побудови операційних систем, методи та алгоритми захисту даних. Отримано наступні **результати**. Виявлено основні аспекти у визначенні та використанні заходів щодо захисту інформації, які можуть бути ефективними при використанні багатопроцесорних модульних обчислювальних систем, або при паралельних розрахунках на багатопотокових системах. Проведено порівняння методів захисту даних з послідовними системами, а також розглянуто вплив застосування різних криптографічних методів на методи реалізації захисту даних. Показано, що основний вибір методів захисту даних у багатопроцесорних системах визначається відмінностями від послідовних систем в теоретичній і апаратній реалізації. **Висновки.** Відповідно до деяких аспектів побудови багатопроцесорних систем розглянуто та виявлено ключові елементи, які вимагають особливої уваги при розробці системи безпеки. У роботі показано, що для паралельної системи потрібно більше апаратних та програмних засобів і з кожним додатковим модулем обчислення система ускладнюється. А це, в свою чергу, ще більше ускладнює систему захисту в цілому, що може спричинити деяке уповільнення виконання прикладних програм за допомогою багатопроцесорних обчислювальних систем. Для захисту даних в таких системах розглядається та аналізується ряд методів. Проте в перспективі запропонований підхід дозволяє забезпечити підвищену безпеку функціонування багатопроцесорних систем.

Ключові слова: багатопроцесорна обчислювальна система; обчислювальні вузли; криптографічні алгоритми; захист даних; ядро; мережі; ключі; операційна система.

Some aspects of the organization of information security of functioning of multiprocessor computing systems

G. Shvachich, O. Ivaschenko, V. Busygin

The subject of the research is to improve the features of the organization of information security of multiprocessor computing systems. **The goal** of this work is to identify and implement measures to secure information that can be effective when using multiprocessor modular computing systems or in parallel calculations on multithreaded systems. To achieve this goal, the following **tasks** are solved: comparison of data protection methods in multiprocessor and sequential systems, as well as study of the specifics of applying various cryptographic methods to the methods of implementing protection; in accordance with some aspects of constructing multiprocessor systems, consideration and identification of key elements that require special attention in the development of a security system; to show that the main choice of data protection methods in multiprocessor systems is determined by differences from sequential systems in the theoretical and hardware implementation. **The methods** used are: main provisions of the theory of computing systems, theory of parallel computing, theory of the construction of operating systems, methods and algorithms for data protection. The following **results** were obtained. The main aspects in definition and use of information protection measures that can be effective when using multiprocessor modular computing systems or in parallel calculations on multithreaded systems are identified. Comparison of methods of data protection with sequential systems is carried out, and also the influence of application of various cryptographic methods on methods of data protection implementation is considered. It is shown that the main choice of data protection methods in multiprocessor systems is determined by differences from sequential systems in theoretical and hardware implementation. **The conclusions**. In accordance with some aspects of the construction of multiprocessor systems, the key elements that require special attention in the development of a security system are examined and identified. The paper shows that a parallel system requires both more hardware and software, and with each additional calculation module the system becomes more complex. And this, in turn, further complicates the protection system as a whole, which may entail some slowdown in the execution of application programs with the help of multiprocessor computing systems. However, in the long term, the proposed approach makes it possible to provide increased security for the operation of multiprocessor systems. To protect data in such systems, a number of methods are considered and analyzed.

Keywords: multiprocessor computing system; computational nodes; cryptographic algorithms; data protection; core, networks; keys; operating system.