УДК 681.3.06

АНАЛИЗ ЭФФЕКТИВНОСТИ ПЕРЕДАЧИ ДАННЫХ В КОМПЬЮТЕРНЫХ СИСТЕМАХ С ИСПОЛЬЗОВАНИЕМ ИНТЕГРИРОВАННЫХ МЕХАНИЗМОВ ОБЕСПЕЧЕНИЯ НАДЕЖНОСТИ И БЕЗОПАСНОСТИ

С.П. Евсеев
Кандидат технических наук, доцент*
E-mail: Evseev_Serg@hneu.edu.ua
Д.В. Сумцов
Кандидат технических наук, доцент
Кафедра математического обеспечения АСУ
Харьковский университет воздушных сил Украины им. Ивана Кожедуба
ул. Сумская, 77/79, г. Харьков, 61123
Контактный тел.: (057) 702-01-47
E-mail: sumtsow@gmail.com
О.Г. Король
Преподаватель*
E-mail: Korol_o@mail.ru
*Кафедра информационных систем
Харьковский национальный экономический университет
пр-т Ленина, 9-а, г. Харьков, 61001
Контактный телефон: (057) 702-18-31
Б.П. Томашевский
Научный сотрудник научного центра
Львовский институт Сухопутных войск имени гетьмана Петра Сагайдачного
ул. Гвардейская, 32, г. Львов, 79012
Контактный тел.: (0322) 34-01-18
E-mail:oficer2007@ucr.net

Розглядаються умови функціонування та вимоги, які пред'являються до сучасних локальних і глобальних обчислювальних систем (ЛОС, ГОС), механізми комплексного забезпечення безпеки та вірогідності передачі даних у комп'ютерних системах і мережах. Досліджується ефективність передачі данних у ЛОС (ГОС) з використанням розроблених крипто-кодових засобів захисту інформації на основі теоретико-кодової схеми Нідерайтера

Ключові слова: ЛОМ, ГОМ, безпека, вірогідність, теоретико-кодова схема

Рассматриваются условия функционирования и требования, предъявляемые к современным локальным и глобальным вычислительным системам (ЛВС, ГВС), механизмы комплексного обеспечения безопасности и достоверности передачи данных в компьютерных системах и сетях. Исследуется эффективность передачи данных в ЛВС (ГВС) с использованием разработанных крипто-кодовых средств защиты информации на основе теоретико-кодовой схемы Нидерайтера

Ключевые слова: ЛВС, ГВС, безпасность, достоверность, теоретико-кодовая схема

The article shows modalities and requirements for modern local and global computing systems (LAN, WAN), comprehensive security and reliability mechanisms of data transmission in computer systems and networks. We investigate the efficiency of data transmission in logal area networks (WAN) using crypto-code information based on the Niderayter's theoretical coding scheme

Key words: LAN, WAN, security, validity, theoretical coding scheme

1. Постановка проблемы и анализ литературы

Вычислительные возможности в последние десятилетия позволяют человечеству выйти на совершенно новый уровень обработки информации, что, в свою очередь, позволяет пользователям локальных и глобальных систем вычислений увеличить на два-три порядка (каждые пять-десять лет) объемы поступаю-

щих данных, а также новые услуги, представляемые пользователям компьютерных сетей [1 – 6]. Вместе с техническим прогрессом растет и компьютерная преступность, появляются новые виды атак и новые виды кибертерроризма. Увеличение обрабатываемых объемов данных в критических системах ЛВС (ГВС) выдвигает новые требования к обеспечению надежности и производительности компьютерных систем, безопасности и достоверности передаваемых и обрабатываемых данных.

Проведенный анализ показывает [1 – 6], что в последнее время не все современные криптографические средства защиты информации обеспечивают своевременную обработку огромных объемов данных (десятки-сотни Мбит/с) и удовлетворяют жестким требованиям по достоверности и безопасности информации.

Целью статьи является обоснование требований, предъявляемых к функциональным возможностям современных компьютерных систем и сетей, исследование интегрированного обеспечения надежности (отказоустойчивости) и безопасности разработанных крипто-кодовых схем защиты информации на основе ТКС Нидерайтера.

2. Анализ условий функционирования и обоснование требований, предъявляемых к современным компьютерным системам и сетям

Анализ условий функционирования локальных и глобальных вычислительных сетей (ЛВС, ГВС) показал, что главным требованием, предъявляемым к ним, является обеспечение пользователям потенциальной возможности доступа к разделяемым ресурсам всех компьютеров, объединенных в сеть [2, 6].

К основным требованиям функционирования ГВС относятся: производительность, надежность, совместимость, управляемость, защищенность, расширяемость и масштабируемость.

Основные требования и их составляющие представлены на рис. 1.

В настоящее время для оценки функционирования ЛВС и ГВС введено понятие “качество обслуживания” (Quality of Service, QoS) компьютерной сети, включающее только две самые важные характеристики сети – производительность и надежность [2, 6]. Проведенный анализ показателя качества обслуживания сети определяет два подхода к его обеспечению [2, 6]. Первый подход состоит в гарантированном обеспечении пользователю соблюдения некоторой числовой величины показателя качества обслуживания (обеспечения установленного показателя средней пропускной способности, показателя времени задержки передачи и т.д.). Так, технологии Frame Relay и ATM позволяют строить сети, гарантирующие качество обслуживания по производительности (показатели средней пропускной способности, времени реакции, времени задержки и т.д).

Второй подход состоит в приоритетном обслуживании пользователей в соответствии с установленной иерархией сети. Таким образом, качество обслуживания зависит от степени привилегированности пользователя или группы пользователей, к которой он принадлежит. Для уполномоченных пользователей ГВС качество обслуживания не гарантируется, а гарантируется только уровень их привилегий. Такое обслуживание называется обслуживанием best effort – с наибольшим старанием.

Проведенный анализ функционирования локальных сетей показывает, что по такому принципу работают ЛВС, построенные на коммутаторах с приоритезацией кадров.

Для обеспечения требуемого показателя качества обслуживания ГВС необходимо обеспечить производительность и надежность. Основными характеристиками производительности являются: время реакции, пропускная способность, задержка передачи и ее вариация.

Время реакции [6] является интегральной характеристикой производительности сети и определяется как интервал времени между возникновением запроса пользователя к какой-либо сетевой службе и получением ответа на этот запрос.

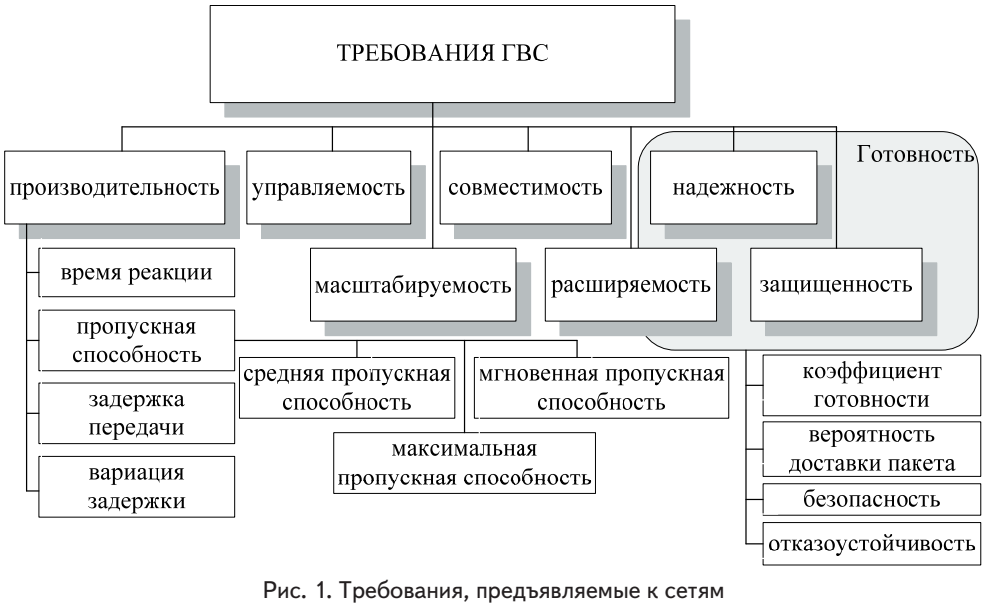

Рис. 1. Требования, предъявляемые к сетям

Проведенный анализ данного показателя показывает, что его значение зависит только от типа службы, к которой обращается пользователь, статуса пользователя в сети, типа сервера, а также от текущего состояния элементов ГВС – загруженности сегментов, коммутаторов и маршрутизаторов, через которые проходит запрос, загруженности сервера и т. п.

Время реакции сети подразделяется на время подготовки запросов на клиентском компьютере, время передачи запросов между клиентом

и сервером через коммуникационное оборудование, время обработки запросов на сервере, время передачи ответов от сервера клиенту и время обработки получаемых от сервера ответов на клиентском компьютере.

Для определения объема передаваемых данных за единицу времени используется пропускная способность и ее производные (мгновенная, максимальная и средняя пропускные способности).

Анализ функционирования ГВС показывает, что для проектирования, настройки и оптимизации используются такие показатели, как средняя и максимальная пропускные способности. Для определения качества сети в целом, не дифференцируя его по отдельным сегментам или устройствам, используется общая пропускная способность сети, которая определяется как среднее количество информации, переданной между всеми узлами сети в единицу времени. Для определения качества сети также используют количественный показатель максимальной задержки передачи и ее вариации. Задержка передачи определяется как время нахождения пакета в каком-либо сетевом устройстве или части сети. Этот параметр производительности по смыслу близок ко времени реакции сети, но отличается тем, что всегда характеризует только сетевые этапы обработки данных, без задержек обработки компьютерами ЛВС.

Анализ создания распределенных систем и эксплуатации ЛВС и ГВС показывает, что для обеспечения их надежности применяются характеристики сложных систем: готовность или коэффициент готовности, означающий долю времени, в течение которого система может быть использована; сохранность данных, т.е. защиту их от искажений; согласованность (непротиворечивость) и их идентичность.

Для описания передачи пакетов между конечными узлами используются вероятностные характеристики канала связи: вероятность доставки пакета узлу назначения без искажений, вероятность потери пакета (по любой из причин – переполнения буфера маршрутизатора, из-за несовпадения контрольной суммы, из-за отсутствия работоспособного пути к узлу назначения и т. д.), вероятность искажения отдельного бита передаваемых данных.

В показатель общей надежности включается безопасность – способность системы защитить данные от несанкционированного доступа и отказоустойчивость – способность системы скрыть от пользователя отказ отдельных ее элементов.

При проектировании и модернизации ЛВС учитываются дополнительные требования к вычислительным сетям:

Расширяемость (extensibility) – возможность сравнительно легкого добавления отдельных элементов сети (пользователей, компьютеров, приложений, служб), наращивания длины сегментов сети и замены существующей аппаратуры более мощной.

Масштабируемость (scalability) – возможность сети наращивать количество узлов и протяженность связей в очень широких пределах, при сохранении показателя производительности сети.

Прозрачность (transparency) – возможность работы с удаленными ресурсами с использованием тех же команд и процедур, что и для работы с локальными ресурсами. Компьютерные сети изначально предназначены для совместного доступа пользователя к ресурсам компьютеров: файлам, принтерам и т. п.

Анализ работоспособности ЛВС (ГВС) показывает, что особую сложность представляет совмещение в одной сети традиционного компьютерного и мультимедийного трафика. Для учета составного трафика используются следующие дополнительные параметры сети:

Управляемость – возможность централизованно контролировать состояние основных элементов сети, выявлять и разрешать проблемы, возникающие при работе сети, выполнять анализ производительности и планировать развитие сети.

Планирование – возможность прогнозирования изменений требований пользователей к сети, применения новых приложений и сетевых технологий.

Совместимость или интегрируемость – возможность включения в ЛВС (ГВС) самого разнообразного программного и аппаратного обеспечения (различные операционные системы, поддерживающие разные стеки коммуникационных протоколов, аппаратные средства и приложения от разных производителей).

Таким образом, анализ основных требований предъявляемых к ЛВС и ГВС показывает, что для выполнения главной задачи обеспечения пользователям потенциальной возможности доступа к разделяемым ресурсам всех компьютеров, объединенных в сеть необходимо выполнить требования двух основных характеристик показателя “качества обслуживания” – производительности и надежности. Для оценки надежности сети используются основные характеристики сложных систем: коэффициент готовности – доля времени, в течение которого система может быть использована; безопасность – способность системы защитить данные от несанкционированного доступа и отказоустойчивость – способность системы работать в условиях отказа некоторых ее элементов.

Проблема защиты компьютерных сетей от несанкционированного доступа приобрела особую остроту. Развитие коммуникационных технологий позволяет строить сети распределенной архитектуры, объединяющие большое количество сегментов, расположенных на значительном удалении друг от друга. Все это вызывает увеличение числа узлов сетей и количества различных линий связи между ними, что, в свою очередь, повышает риск несанкционированного подключения к сети и доступа к важной информации.

Кроме того, современное развитие информационных технологий, высокий уровень компьютеризации и информатизации современного общества обусловили возникновение новых угроз безопасности информации [2, 6].

Для обеспечения аутентификации, целостности и конфиденциальности передачи данных в компьютерных сетях используются криптографические методы, основанные на использовании симметричных и несимметричных алгоритмов преобразования информации.

Вместе с тем, дальнейшее усиление угроз указывает на необходимость интегрированного подхода для обеспечения защиты передаваемой информации. Общая классификация методов криптографической обработки информации в телекоммуникационных системах представлена на рис. 2.

Рис. 2. Общая классификация криптографических методов защиты

Методы симметричной криптографии основаны на простых и легко реализующихся блоках подстановок и перестановок. Методы криптографии с открытым ключом основаны на использовании соответствующей теоретико-сложностной задачи (факторизации, дискретного логарифмирования и т.д.).

Перспективным направлением в развитии криптографических средств защиты информации доказуемой стойкости являются крипто-кодовые механизмы, построение которых основано на сведении задачи взлома ключевых данных к решению теоретико-числовой задачи декодирования случайного кода [1 – 11]. Их применение позволит [7 – 11]:

реализовать быстрые криптографические преобразования больших объемов данных с использованием открытых ключей в компьютерных системах и сетях;

обеспечить высокий уровень стойкости к современным методам криптоанализа, за счет сведения задачи бесключевого чтения к решению теоретико-сложностной задачи декодирования случайного кода обеспечить доказуемую стойкость криптографических средств защиты информации;

строить на канальном уровне ВОС интегрированные механизмы криптографической защиты информации и достоверности данных в компьютерных системах и сетях.

3. Исследование эффективности передачи данных в компьютерных системах и сетях с использованием разработанных крипто-кодовых средств защиты информации

Оценим показатель эффективности компьютерной сети (Wi) при использовании в протоколах обмена симметричных схем шифрования, схем шифрования с открытым ключом и разработанной крипто-кодовой системы на основе теоретико-кодовой схемы Нидерайтера с алгоритмом недвоичного равновесного кодирования. На рис. 3 представлены результаты исследований эффективности передачи данных в компьютерных системах и сетях с использованием разработанных крипто-кодовых средств защиты информации, симметричных и несимметричных криптосистем в каналах без памяти.

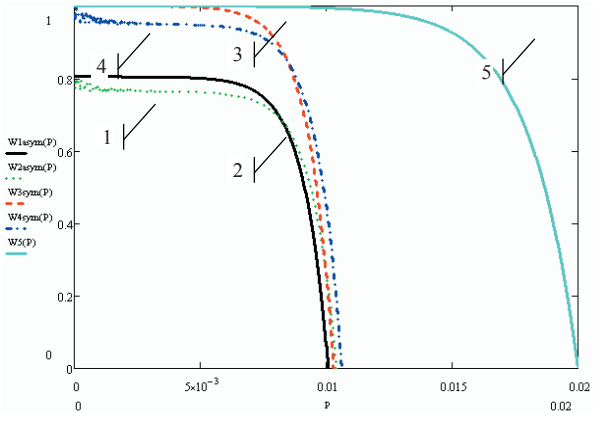

Рис. 3. Зависимость показателя эффективности обмена данными в компьютерной сети W от вероятности битовых ошибок P_0

Примечание. При расчетах принимались следующие исходные данные: C = 56000 бит/с; L = 1000 км; Vp = $3 \cdot 10^8$ м/с; r = 16; t = 8; n = 1024 и n разр. метод =512 бит; s = 32; Z = 2; РЗ = 0,95; $t_{ш\_сим} = t_{расш\_сим}$ = 0,01 с; $t_{ш\_асим} = t_{расш\_асим}$ = 100 с; $t_{ш\_разр.\ метод} = t_{рш\_разр.\ метод}$ = 0,01 с; B = 10^{24} и B разр. метод =10^{30}; $\Psi = 10^{15}$.

Обозначения графиков:

1 – Возвращение-на-N (протокол с асимметричной криптосистемой).

2 – Састри (с решающей обратной связью и положительной квитанцией, протокол с асимметричной криптосистемой).

3 – Возвращение-на-N (протокол с симметричной криптосистемой).

4 – Састри (с решающей обратной связью и положительной квитанцией, протокол с симметричной криптосистемой).

5 – Разработанная крипто-кодовая система защиты информации на основе теоретико-кодовой схемы Нидерайтера с алгоритмом равновесного кодирования недвоичных кодов.

Проведенные исследования обобщенного показателя эффективности в работе [12] показали, что несимметричные криптосистемы обеспечивают требуемый показатель безопасности (надежности) при использовании стратегии (протоколе обмена) с решаю-

щей обратной связью и непрерывной передачей кадров (РОСнп) “Возвращение-на-N” (с решающей обратной связью и положительной квитанцией (РОСпк)). Однако показатель оперативности (время реакции сети) при этом увеличивается на 20% за счет сложности реализации алгоритмов шифрования с открытым ключом.

Симметричные криптосистемы обеспечивают требуемый показатель времени реакции сети (показатель производительности), однако значительно уступают в показателе безопасности. Разработанные крипто-кодовые системы позволяют интегрировано обеспечить основные показатели “качества обслуживания сети” – производительность и надежность – по времени реакции сети (показатель производительности) соответствуют симметричным криптосистемам, а показатель безопасности – криптосистемам с открытым ключом. Кроме этих показателей данные системы позволяют обеспечить и показатель отказоустойчивости за счет применения помехоустойчивых кодов, позволяющих исправлять установленное количество ошибок.

Анализ рис. 3 показывает, использование протоколов с асимметричными криптосистемами обеспечивает требуемый показатель эффективности обмена данными в компьютерной сети W только при использовании цифровых каналов связи с $P_{ош} = =10^{-6} – 10^{-12}$. В проводных каналах связи применение данных криптосистем значительно снижает показатель эффективности (W> 0,8) из-за значительного (на 3 – 5 порядков) увеличения времени формирования криптограммы по сравнению с симметричными криптосистемами. Применение в протоколах обмена с обратной связью между пользователями сети традиционных криптоалгоритмов позволяет обеспечить требуемый показатель эффективности обмена данными в каналах связи с $P_{ош} = 10^{-4} – 10^{-12}$, что позволяет применять данные криптосистемы в каналах связи на основе коаксиальных кабелей и неэкранированной витой пары (категории 3, 5). Однако применение их в проводных линиях связи не обеспечивает требуемый показатель эффективности.

Применение разработанных крипто-кодовых систем позволяет обеспечить требуемый показатель эффективности обмена данными в компьютерной сети W = 0,95 при использовании всех видов каналов связи (от проводных линий с $P_{ош} = 10^{-2} – 10^{-3}$ до оптоволоконных линий с $P_{ош} = 10^{-9} – 10^{-12}$).

Таким образом, разработанные крипто-кодовые системы позволяют интегрировано обеспечить показатели безопасности и надежности сети и, следовательно, выполнить главное требование, предъявляемое к сетям – обеспечение пользователям потенциальной возможности доступа к разделяемым ресурсам всех компьютеров, объединенных в сеть.

4. Выводы

Проведенные исследования показали, что применение разработанных крипто-кодовых средств защиты информации позволяет эффективно обеспечить безопасность больших объемов передаваемых данных с использованием быстрых (10 – 100 Мбит/с) криптографических преобразований с возможностью частой смены ключевых данных, что удовлетворяет требованиям по производительности компьютерных систем и сетей.

Проведенные исследования обобщенного показателя эффективности компьютерных сетей с использованием разработанных крипто-кодовых систем показали, что их применение в протоколах с решающей обратной связью обеспечивают требования по надежности и безопасности, и, следовательно, выполняют главное требование к сетям – обеспечение пользователям потенциальной возможности доступа к разделяемым ресурсам всех компьютеров, объединенных в сеть. *Перспективным направлением дальнейших исследований* является оценка эффективности передачи данных в компьютерных системах и сетях, с использованием разработанных крипто-кодовых средств защиты информации в каналах передачи данных с памятью. Дальнейшая разработка и дальнейшее совершенствование комплексных (интегрированных) средств защиты передаваемой информации на основе крипто-кодовых схем, формирование протоколов обмена секретными сообщениями в различных режимах функционирования компьютерных систем и сетей.

Литература

1. Захист інформації в комп’ютерних системах від несанкціонованого доступу. / За ред. С.Г. Лаптєва. – К., 2001. – 321 с.
2. Мамаев Е. Технологии защиты информации в Интернете. – СПб.: ИД Питер, 2001. – 848 с.
3. Харин Ю.С. Математические и компьютерные основы криптологии / Ю.С. Харин, В.И. Берник, Г.В. Матвеев, С.В. Агиевич – Мн.: Новое знание, 2003. – 382 с.
4. Мао В. Современная криптография. Теория и практика. М.: «Вильямс», 2005. – 768 с.
5. Шнайер Б. Прикладная криптография. –М.: «ТРИУМФ», 2003. – 816 с.
6. Молдавян Н.А. Криптография: от примитивов к синтезу алгоритмов / Н.А. Молдавян, А.А. Молдавян, М.А. Еремееев– СПб.: БХВ, 2004. – 448 с.
7. R.J. McEliece. A Public-Key Criptosystem Based on Algebraic Theory. // DGN Progres Report 42-44, Jet Propulsi on Lab. Pasadena, CA. January – February, 1978. – P. 114-116.
8. H. Niederreiter. Knapsack-Type Cryptosystems and Algebraic Coding Theory. // Probl. Control and Inform. Theory. – 1986. –V.15. – P. 19-34.
9. Стасев Ю.В. Несимметричные теоретико-кодовые схемы с использованием алгеброгеометрических кодов / Ю.В. Стасев, А.А. Кузнецов // Кибернетика и системный анализ: Международный научно-теоретический журнал. – Киев: НАНУ. – 2005. – №3. – С. 47–57.
10. Кузнецов А.А. Несимметричные криптосистемы доказуемой стойкости на алгебраических блоковых кодах // Радіоелектронні і комп’ютерні системи. Науково-технічний журнал – Х.: ХАИ. – 2007.– №8(27) – С.130–144.
11. Науменко Н. І.. Теоретичні основи та методи побудови алгебраїчних блокових кодів / Н. І. Науменко, Ю. В. Стасев, О.О. Кузнецов. – Х.:ХУ ПС, 2005р. – 267 с.
12. Евсеев С.П. Эфективность обмена данными в компьютерной сети при различных способах управления обменом / С.П. Евсеев, Д.В. Сумцов, О.Г. Король, Б.П. Томашевский // Збірник наукових праць. Донецький інститут залізничного транспорту. Випуск 17. – 2009. – С. 33 – 45.