2. *Нортон Д., Каплан Р.* Организация, ориентированная на стратегию. Как в новой бизнес-среде преуспевают организации, применяющие сбалансированную систему показателей / Пер. с англ. – М.: Изд-во «Олимп-Бизнес», 2009. – 416 с.
3. *Харари Ф.* Теория графов / Пер. с англ. – М.: Изд-во «Либроком», 2009. – 302 с.

Статью рекомендовал к опубликованию д.т.н., профессор С.Л. Беляков.

Граецкая Оксана Владимировна – Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Южный федеральный университет»; e-mail: kaf_sau@mail.ru; 344090, г. Ростов-на-Дону, Мильчакова, 10; тел.: 88632696991; кафедра системного анализа и управления; к.т.н.; доцент.

Пономарева Наталья Сергеевна – кафедра системного анализа и управления; преподаватель; аспирантка.

Graetskaya Oksana Vladimirovna – Federal State-Owned Autonomy Educational Establishment of Higher Vocational Education «Southern Federal University»; e-mail: kaf_sau@mail.ru; 10, Mil'chakova, Rostov-on-Don, 344090, Russia; phone: +78632696991; the department of systems analysis and control; cand. of eng. sc.; associate professor.

Ponomareva Natalia Sergeevna – the department of systems analysis and control; master of science; postgraduate student.

УДК 025.4.03

А.С. Родионов, С.Л. Сухарев

ИСПОЛЬЗОВАНИЕ ХЕШ-ФУНКЦИИ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ В ЛОКАЛЬНЫХ ВЫЧИСЛИТЕЛЬНЫХ СЕТЯХ ВОЕННОГО НАЗНАЧЕНИЯ

На основании проведенного анализа применения методов хеширования информации (симметричное, асимметричное), которые в настоящее время используются в инфокоммуникационных системах военного и гражданского назначения и электронном документообороте, разработаны оригинальные алгоритмы, реализующие кодирование текстовой информации в виде комбинации криптоалгоритмов. При симметричном кодировании основным является алгоритм MD5 (Message Digest 5) с использованными при реализации вариантами: постоянная длина ключа, рекурсивный ключ, циклический ключ со сдвигом, циклический ключ со сдвигом кода. Асимметричное кодирование для хеширования текстового документа с одновременным созданием электронной цифровой подписи реализовано в соответствии с ГОСТ 34.10-2001. Разработанное программное обеспечение может оказаться полезным системному администратору.

Симметричное; асимметричное кодирование; хеширование; электронный документооборот; электронная цифровая подпись.

A.S. Rodionov, S.L. Sukharev

HASH-FUNCTION USING FOR INFORMATION PROTECTION IN LAN MILITARY APPOINTMENTS

Based on the analysis of hashing methods information (symmetric, asymmetric), which are currently used in information and communication systems for military and civilian use and electronic workflow, developed original algorithms that implement the coding of textual information in the form of a combination of cryptographic algorithms. With symmetric encryption algorithm is the basic MD5 (Message Digest 5) used in the implementation of options: a constant length of the key, the key recursive, cyclical shift key, the key cyclic shift code. Asymmetric encryption to hash a text document with the simultaneous creation of digital signature is implemented in accordance with GOST 34.10-2001. The developed software can be useful to system administrator.

Symmetrical; asymmetrical coding; hashing; electronic workflow; digital signature.

В настоящее время в Вооруженных Силах (ВС) РФ происходит реформирование, старая техника связи с использованием аналоговых сигналов не удовлетворяет требованиям современного общевойскового боя. Информация должна проходить с большей скоростью, достоверностью и точностью. Проводимые реформы предполагают введение в ВС РФ новых, удовлетворяющих современным требованиям, образцов техники связи, работающих с цифровыми сигналами. При работе с цифровыми сигналами скорость обмена данными будет существенно повышаться, вследствие чего, требуются новые, точные, недорогие и удовлетворяющие современным условиям и требованиям методы и способы шифрования передаваемой информации.

Высокие темпы развития научно-технического процесса приводят к уязвимости информации в современных системах обмена данными, которые должны передаваться своевременно, достоверно и конфиденциально. Основу обеспечения информационной безопасности в информационно-телекоммуникационных системах составляют криптографические методы и средства защиты информации. Следует учесть, что наиболее надежную защиту можно обеспечить только с помощью комплексного подхода, то есть решение задачи должно представлять собой совокупность организационно-технических и криптографических мероприятий.

В основе криптографических методов лежит понятие криптографического преобразования информации, производимого по определенным математическим алгоритмам, с целью исключить доступ к данной информации посторонних пользователей, а также с целью обеспечения невозможности бесконтрольного изменения информации со стороны тех же лиц.

Применение криптографических методов защиты обеспечивает решение основных задач информационной безопасности.

Эти цели могут быть достигнуты после реализации следующих криптографических методов защиты как пользовательской и служебной информации, так и информационных ресурсов в целом:

- шифрование всего информационного трафика, передающегося через открытые сети передачи данных и отдельных сообщений;
- криптографическая аутентификация устанавливающих связь разноуровневых объектов (имеются в виду уровни модели взаимодействия открытых систем – OSI);
- защита несущего данные трафика средствами имитозащиты (защиты от навязывания ложных сообщений) и электронно-цифровой подписи с целью обеспечения целостности и достоверности передаваемой информации;
- шифрование данных, представленных в виде файлов либо хранящихся в базе данных;
- контроль целостности программного обеспечения путем применения криптографически стойких контрольных сумм.

При реализации большинства из приведенных методов криптографической защиты возникает необходимость обмена некоторой информацией (например, аутентификация сопровождается обменом как идентифицирующей, так и аутентифицирующей информации) [1, 2].

Данные обстоятельства предъявляют высокие требования к алгоритмам шифрования. Одним из наиболее перспективных направлений решения данной проблемы в системах автоматизации и локальных вычислительных сетях (ЛВС) военного назначения является применение криптографической хеш-функции.

Основные задачами работы:

- обзор и сравнение существующих алгоритмов шифрования;
- сравнение симметричного и ассиметричного алгоритмов.

Исходными данными для решения данной проблемы являются:

- основы концепции реформирования системы и войск связи ВС РФ и способы ее реализации;
- архитектура построения современных телекоммуникационных сетей военного назначения;
- общая характеристика систем связи ВС РФ;
- проблемные вопросы и направления развития системы связи ВС РФ в современных условиях;
- нормативные документы по обеспечению безопасности служебной и секретной информации в подразделениях, в частях связи.

Основные алгоритмы симметричного шифрования: DES, TDEA, Blowfish, RC5, ГОСТ 28147-89.

В симметричных криптоалгоритмах для шифрования и расшифрования информации используется один и тот же секретный ключ.

Достоинствами таких алгоритмов являются:

- простота программной и аппаратной реализации;
- высокая скорость работы в прямом и обратном направлениях;
- обеспечение необходимого уровня защиты информации при использовании коротких ключей.

К основным недостаткам этих криптоалгоритмов следует отнести увеличение затрат по обеспечению дополнительных мер секретности при распространении ключей, а также то, что алгоритм с секретным ключом выполняет свою задачу только в условиях полного доверия корреспондентов друг другу.

Алгоритм MD5 (Message Digest 5) – алгоритм хеширования текста в 32- символьную строку. Используется для создания «отпечатка» (дайджеста) текста, такого как, например, личный пароль или любых других данных, которые необходимо передавать в зашифрованном виде в режиме «онлайн». Расшифровка md5-хеша практически невозможна, так как кодирование не предусмотратривает обратной расшифровки, а также одному md5-образу (хешу) могут соответствовать разные исходные данные. Несмотря на это, существует вероятность определения исходного текста методом перебора.

Разработанный вариант программного обеспечения, реализующий хеширование с помощью *комбинации симметричных алгоритмов*, имеет основное окно, представленное на рис. 1. На рис. 2 представлен зашифрованный документ, значение хеша в шестнадцатеричной и ASCII кодировках с выбором основного алгоритма (задается пользователем, реализация комбинации алгоритмов выполняется программно). Дешифрование, естественно, позволяет получить исходный текст документа.

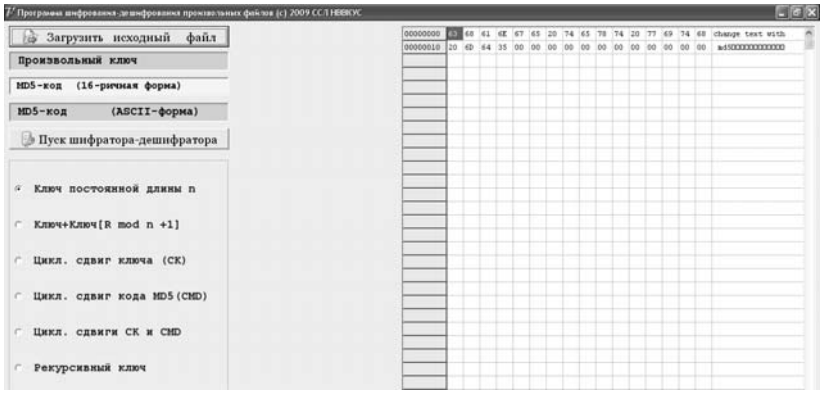

Рис. 1. Хеширование с помощью комбинации симметричных алгоритмов, исходный документ

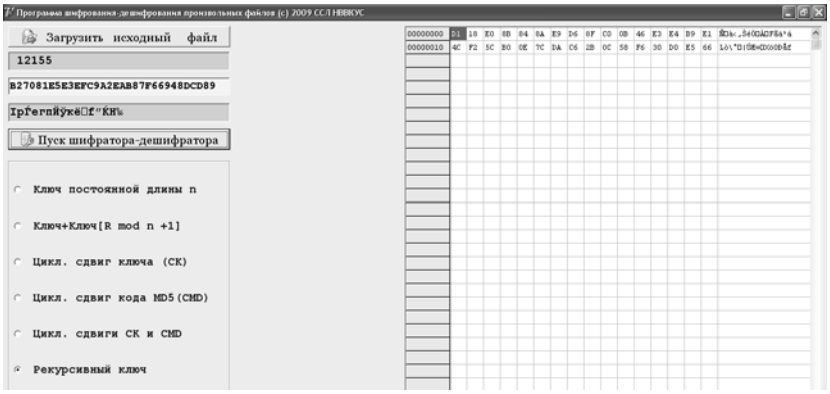

Рис. 2. Хеширование с помощью комбинации симметричных алгоритмов, зашифрованный документ

Алгоритмами асимметричного шифрования являются:

– RSA; DSA; Elgamal; ГОСТ 34.10-2001.

Разработанный вариант программного обеспечения, реализующий требования ГОСТ 34.10-2001 при хешировании с помощью *асимметричного алгоритма с одновременным созданием электронной цифровой подписи (ЭЦП)*, имеет основное окно, представленное на рис. 3, где представлен исходный документ, значение хеша в шестнадцатеричной кодировке. Дешифрование, естественно, позволяет получить исходный текст документа только после проверки правильности *ЭЦП*.

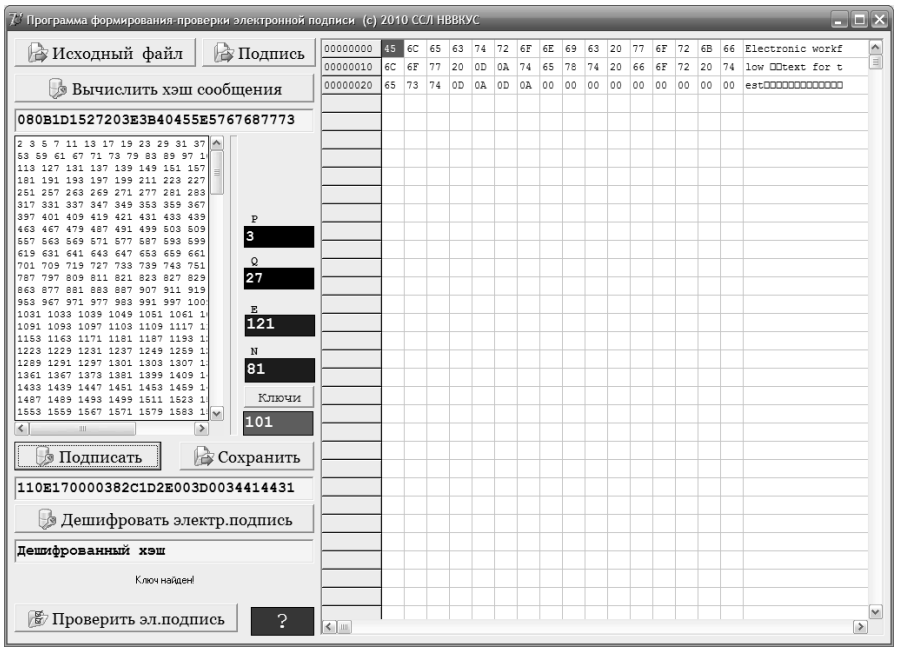

Рис. 3. Хеширование с использованием ЭЦП, исходный документ

Целесообразность использования хеш-функции в криптографическом преобразовании документа (приказа) командира при передаче сообщений в вычислительных сетях военного назначения не вызывает сомнений. Разработанные про-

граммные продукты, легко реализуемые с помощью современных аппаратных средств, позволяют значительно экономить время при передачи документа, контролировать целостность и внедрение ложных данных как в полевых, так и в стационарных условиях.

В современных системах электронного документооборота в ЛВС «среднего уровня» (до 10 тыс. абонентов) хеширование представляется необходимым встроенным средством для распределения и защиты информации абонентов сети. Разработанное программное обеспечение может оказаться полезным системному администратору ЛВС.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Олифер В.Г.* Компьютерные сети. Принципы, технологии, протоколы. – 3-е изд. – СПБ.: Питер, 2006. – 958 с.
2. *Рябко Б.Я.* Криптографические методы защиты информации: Учебное пособие для вузов. – М.: Горячая линия-Телеком, 2005. – 229 с.

Статью рекомендовал к опубликованию д.т.н., профессор А.А. Зори.

Родионов Александр Сергеевич – Военная академия связи (филиал, г. Новочеркасск); e-mail: ras001m@mail.ru; 346418, г. Новочеркасск, ул. Атаманская 36; тел.: +79085118349; кафедра автоматизированных систем управления войсками и связи; к.т.н.; доцент.

Сухарев Сергей Леонидович – e-mail: ssl@mail.ru; тел.: +79185362043; кафедра автоматизированных систем управления войсками и связи; к.т.н.; доцент.

Rodionov Alexander Sergeevich – Military Academy of Communication (Branch office, Novocherkassk); e-mail: ras001m@mail.ru; 36, Atamanskaya street, Novocherkassk, 346418; phone: +79085118349; the department of automated systems of troop control and communication; cand. of technical sciences; associate professor.

Sukharev Sergey Leonidovich – e-mail: ssl@mail.ru, phone: +7 918 536 2043; the department of automated systems of troop control and communication; cand. of eng. sc.; associate professor.

УДК 519.2: 681.51

Е.С. Филева

СИСТЕМА АДАПТИВНОГО УПРАВЛЕНИЯ ДОКУМЕНТООБОРОТОМ

Рассматриваются системы адаптивного управления документооборотом (САУД) на производственном предприятии. Структура САУД основывалась на анализе информационной модели состояния предприятия. Проектирование САУД осуществлялось в результате решения двух основных задач: определение состава модулей (структура) прямых и обратных связей между ними. На основе анализа технической информационной модели предприятия разрабатывались требования к САУД. В целях выявления движений документов, их информационной емкости и повторяемости вплоть до закрытия вопроса были разработаны диаграммы информационной эволюции документов. Сформирован общий адаптивный алгоритм построения САУД. Предложенный подход позволяет сформировать специализированную систему документооборота на производственном предприятии.

САУД; проектирование документооборота; схема документооборота; адаптивная модель управления; информационная эволюция документа; диаграмма движения документа; алгоритм построения САУД.