УДК 338.2:681.3

Г. Л. Матюшкова[1], Л. П. Матюшков[2]
[1]Беларусь, Минск, ОИПИ НАН Беларуси
[2]Беларусь, Брест, БрГУ имени А. С. Пушкина

ОБЕСПЕЧЕНИЕ ЗАЩИТЫ И ДОСТОВЕРНОСТИ ИНФОРМАЦИИ В СЕТЕЦЕНТРИЧЕСКИХ СИСТЕМАХ

Сетецентризм является одним из современных подходов к созданию сложных информационных систем для различных органов управления государственного уровня (электронное правительство, оборона страны, экономическая безопасность и т.п.). Реализация таких задач немыслима без обеспечения надежного взаимодействия типовых элементов по сбору, обработке и хранению информации.

В первую очередь это направлено на развитие новых форм управления, опирающихся на быстрый сбор информации в зоне ответственности различных подсистем и информационно-управляющие средства, реализующие функции анализа и управления с одновременным информированием вышестоящих и взаимодействующих подсистем.

Достоверность, полнота и своевременность поступающей информации во многом определяют эффективность всей системы, так как в конечном итоге лица, принимающие решение (ЛПР), часто страдают от недостоверности и недостатка поступающей информации. Например, даже в разрекламированных военных системах, применяемых США в уличных боях в Ираке и горах Афганистана против талибов сказывалась нехватка и недостоверность информации с места боевой операции из-за невозможности ее получения самыми современными техническими средствами (беспилотные самолеты, спутники, фиксаторы звуков и излучений и т.п.) [1].

Поэтому в системах гражданского применения желательно избегать подобных недостатков, так как в них легче влиять на процессы подготовки своевременной и качественной информации.

Для этих целей нами предлагается широко использовать стандартные подходы представления информации в табличных форматах. Это позволяет облегчить ее контроль на стадии подготовки табличного материала с проверкой его корректности на основе специальных контрольных сумм или закономерностей, присущих данному типу таблиц (например, равенство сумм чисел в столбцах и строках, а также использование других видов функциональных зависимостей: сумма весов элементов равна 1 и т.п.). В случаях умышленных искажений информации можно вырабатывать сигналы о проверке ее достоверности на базе сравнений с аналогичной информацией в других узлах сети, например, затраты на содержание типовых объектов на душу населения и т.д. Одновременно такой анализ может подтолкнуть и к выработке специальных решений о распространении хорошего опыта или наказания за подтасовку данных. Этот подход полезен к данным, порождаемым внутри сети. Иной подход нужен при использовании

данных, поступающих из других сетей, так как могут быть специальные поступления искаженной информации и сами ее владельцы могут также пользоваться искаженными данными ничего не подозревая. Поэтому предлагается пользоваться внешними данными очень осторожно, избегая их использования в вычислениях различных показателей, а также иметь перечень источников и документов, которые готовятся для специальных целей и применяются авторитетными международными организациями.

Вторым важным организационным шагом является подбор системы протоколов при обмене информации между узлами собственной сети, чтобы разграничить права доступа к различной информации собственной сети и права выхода в другие сети (особенно с платной информацией).

Для управленческих государственных сетей эта задача облегчается тем, что существует иерархическая система подчиненности (район, область, центральный орган) и можно построить распределенную подсистему доступа к информации и использованию уровня защиты по узловому принципу. Тогда права на операцию с информацией определяются типом узла и возможными полномочиями доступа к элементам информации в нем в зависимости от функций специалистов в системе управления. Особо разрабатываются протоколы для связи с населением, так как при реализации принципа одного окна необходимо решить задачи конфиденциальности доступа к некоторым видам информации (состояния здоровья человека, справки о его страховках, вкладах и т.п.).

Одним из главных для всех типов информационного обмена и накопления данных становится задача отыскания простого и надежного способа аутентификации любого ранга пользователя сети, то есть первая часть задачи состоит в обеспечении достоверности данных и созданием механизма доступа к ним, исключающего вход в систему нарушителей.

Вторая часть задачи включает организацию механизма ответственности за подготовленные данные и решения. Она может опираться на использование электронной цифровой подписи (ЭЦП) так, чтобы было легко обнаружить исполнителя данного фрагмента информации. Эта часть задачи тесно переплетается с аутентификацией пользователей и для ее решения полезно использовать аппарат двух ключевых систем для шифрования информации – хэш-функции и процедуру гаммирования [2].

Аналогичные идеи высказываются [3] при описании механизмов алгоритма и протоколов для аутентификации информации в автоматизированных системах управления. Довольно убедительно такой подход иллюстрируется [2]. В частности, его эффективность легко наблюдается при применении любой двухключевой системы с закрытым и открытым ключами типа RSA.

Для этой цели необходимо при подписывании фрагмента текста вычислять значения $m = H(T)$ по функции хеширования H для текста T и вместе с зашифрованным текстом секретным ключом E передавать число $S = (m^E) \bmod N$ (N – первая часть открытого ключа, D – вторая часть открытого ключа), которое может читаться на приемном конце с помощью первой и второй частей открытого ключа, то есть должно получаться $m = S^D \bmod N$,

одновременно вычисляется $H(T)=m'$ по расшифрованному тексту T. При совпадении m и m' цифровая подпись считается подлинной и ее владелец может нести ответственность за текст или допускается к входу в названный узел сети.

При использовании операции гаммирования передающая и принимающая информацию стороны могут иметь идентичную таблицу случайных чисел. Секретность гаммирования может обеспечиваться путем зашифрованного начального случайного числа в таблице, либо оно может вычисляться по известной пользователям функции, содержащей среди переменных время передачи текста.

Учитывая, что при шифровании работа ведется с двоичными кодами и основой для операции гаммирования является последовательность из нулей и единиц, отметим как результаты чтения таблицы случайных чисел перевести в удобную для приложений форму. Для этой цели можно читать таблицу случайных чисел по строкам, преобразуя каждую десятичную цифру в двоично-десятичный код. При порождении последовательности из нужного количества двоичных знаков она складывается с полученным текстом Т поразрядно по модулю 2 (1 + 1 = 0, 0 + 1 = 1) и получаем зашифрованный текст который подготовлен в точке отправления. Так как он вычислен по одним и тем же законам в пункте оправления и получения текста Т на одинаковом отрезке случайной последовательности благодаря общей исходной таблице, распространяемой операции пользователей сети.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Конышев, В. Н. Военная стратегия США после холодной войны / В. Н. Конышев. – СПб. : Наука, 2009. – С. 85–86.

2. Головко, В. А. Основы компьютерных технологий : учеб.-метод. пособие / В. А. Головко, А. А. Дудкин, Л. П. Матюшков. – Брест : БрГТУ, 2015. – 180 с.

3. Молдовян, А. А. Новые алгоритмы и протоколы для аутентификации информации в АСУ / А. А. Молдовян, Н. А. Молдовян // Автоматика и телемеханика. – 2008. – Вып. 7. – С. 157–169.

УДК 519.24

Е. И. Мирская
Беларусь, Брест, БрГУ имени А. С. Пушкина

ИССЛЕДОВАНИЕ ОЦЕНКИ СПЕКТРАЛЬНОЙ ПЛОТНОСТИ МНОГОМЕРНОГО ВРЕМЕННОГО РЯДА

Исследование статистических оценок спектральных плотностей является одной из классических задач анализа временных рядов. В данной работе в качестве оценки неизвестной спектральной плотности многомерного временного ряда исследована статистика, построенная по методу Уэлча.

Предположим, что число наблюдений T за процессом $X(t)$, $t \in Z$ представимо в виде: $T = L\,[r(N-1)+1]$, где $r \in \{1,2,...\}$, $N \in \{1,2,...\}$, L – число непересе-