тегией развития информационного общества на период до 2015 года, утвержденной постановлением Совета Министров Республики Беларусь от 9 августа 2010 г. № 1074, и Законом Республики Беларусь «Об информации, информатизации и защите информации». Данные правовые акты определяют основные требования по защите информации: обеспечение целостности и сохранности информации, содержащейся в государственных информационных системах, путем установления и соблюдения единых требований по защите информации от неправомерного доступа, уничтожения, модификации (изменения) и блокирования правомерного доступа к ней, в том числе при осуществлении доступа к информационным сетям. Любой государственный орган, получающий ресурсы, в том числе и информационные, перерабатывает их в продукты своей деятельности, порождая специфическую внутреннюю среду, которая формируется совокупностью структурных подразделений, персоналом, техническими средствами и технологическими процессами, экономическими и социальными отношениями как внутри органа, так и во взаимодействии с внешней средой.

Внутри государственного органа информационные потоки поступают в соответствующие модули корпоративной системы для структурирования, систематизации, обработки, анализа и практического использования. Большая часть этой информации является свободно используемой в процессе реализации деятельности государственного органа, однако в зависимости от особенностей внутренней деятельности и взаимодействия с внешним миром часть информации может быть предназначенной для служебного пользования, строго конфиденциальной или секретной. Такая информация является, как правило, закрытой и требует соответствующих мер защиты.

Программно-аппаратные средства для работы с охраняемой информацией либо встраиваются в соответствующие модули корпоративной информационной системы, либо используются локально в системах, указанных в политике информационной базы. Средства противодействия угрозам информационной базы и утечкам данных и информации являются, по сути, программно-аппаратным слоем в существующей ИТ-инфраструктуре государственного органа, в которой не только обрабатываются конфиденциальные данные, но и работают сотрудники с этими данными. Защитный комплекс состоит как из технических устройств и программного обеспечения, так и из совокупности организационных мер по реализации политики внутренней безопасности – целостное решение связывает воедино инфраструктуру, информацию и персонал.

К мерам по защите информации относится обеспечение особого режима допуска на территорию (в помещения), на которой может быть осуществлен доступ к информации (материальным носителям информации), а также разграничение доступа к информации по кругу лиц и характеру информации.

К техническим мерам по защите информации относятся меры по использованию средств технической и криптографической защиты информации, а также меры по контролю защищенности информации.

Государственные органы и юридические лица, осуществляющие обработку информации, распространение и (или) предоставление которой ограничено, определяют соответствующие подразделения или должностных лиц, ответственных за обеспечение защиты информации.

Целостные программные продукты осуществляют контроль и управление рисками внутренней безопасности и минимизируют утечки конфиденциальной информации за счет соответствующих технологических составляющих, глубоко интегрированных в информационную структуру органа. К ним относятся программно-аппаратные устройства:

отслеживания перемещения конфиденциальной информации по информационной системе;

управления контролем утечки данных через сетевой трафик по сетевым протоколам;

шлюза, через который идет трафик из внутренней сети во внешнюю сеть;

сервера, обрабатывающего определенный тип трафика;

рабочей станции;

внутренних каналов почты и др.;

управления контролем утечки охраняемой информации с рабочих станций, периферийных и мобильных устройств посредством контроля действий авторизованных пользователей с конфиденциальными данными: с файлами, внешними устройствами, сетью (локальной, беспроводной), буфером обмена, приложениями, устройств печати (локальные, сетевые);

теневого копирования информационных объектов в единую базу контентной фильтрации по единым правилам для всех каналов.

УДК 004.315.5

Н.С. Уваров

ВВЕДЕНИЕ В КОМБИНИРОВАННУЮ АРИФМЕТИКУ НА ОСНОВЕ АЛГЕБРЫ КВАТЕРНИОНОВ И ЛОГАРИФМИЧЕСКОЙ СИСТЕМЫ СЧИСЛЕНИЯ

Известно обобщение из действительной и комплексной арифметики (два вещественных числа), которое распространяется далее на более неясную арифметику кватернионов (четыре вещественных числа),

применяемой в обработке сигналов, аэрокосмических приложениях, графике и виртуальной реальности. Умножение кватернионов реализуется 3D-вращением, но оно затратное (обычно 16 умножений с плавающей запятой и 12 сложений). В работе предполагается альтернативное представление кватернионов с использовании логарифмов в целях уменьшения затрат умножения.

Как логарифмы, так и кватернионы – почтенные математические понятия. После открытия каждый из них произвел революцию и правил вековой наукой и техникой и с теоретической, и с практической точки зрения (ручное вычисление). В этой работе рассматривается возможность объединения кватернионов с логарифмической системой счисления. Потребность такого подхода имеет место в различных приложениях, таких как анимационная графика, виртуальная реальность, робототехника и системы управления.

Альтернативный способ, известный как конструкция Кэли – Диксона, заключается в том, что, чтобы определить кватернион, необходимо начать с пары комплексных значений: $\overline{Q}_0 = Q_{00} + Q_{01}i$ и $\overline{Q_1} = Q_{10} + \zeta$, каждое из которых содержит половину информации кватерниона. Такое представление Кэли – Диксона было использовано для построения умножителя кватернионов в прямоугольной форме и использовалось, чтобы предложить альтернативное полярное представление одного угла (с помощью комплексного угла, а не действительных углов, используемых в нашей работе): $Q = \overline{Q}_0 + \overline{Q}_1 j = (Q_{00} + Q_{01}i) + (Q_{10} + Q_{11}i) = Q_{00} + Q_{01}i + Q_{10}j + Q_{11}k.$ Как известно, $ij = k$ дает четвертый элемент прямоугольного представления кватернионов. Для формирования сопряженного кватерниона Q в этом представлении требуется комплексное сопряженное число $\overline{Q}_0^*$ и комплексное отрицательное $-\overline{Q}_1^*$. Для формирования отрицательного требуется отрицание обеих частей: $-\overline{Q}_0$ и $-\overline{Q}_1$. Если два кватерниона представлены парой комплексных значений Q и аналогично $P = \overline{P}_0 + \overline{P}_1 j,$ то результат умножения P на Q может быть описан в виде набора комплексных операций: $\overline{R}_0 = \overline{P}_0\overline{Q}_0 - \overline{P}_1\overline{Q}_1^*;$ $\overline{R}_1 = \overline{P}_0\overline{Q}_1 + \overline{P}_1\overline{Q}_0^*$ За исключением присутствия сопряженных операций, этот алгоритм похож на прямоугольный алгоритм умножения.

Новая концепция, которую называют кватернионная комплексная ЛСЧ (ККЛСЧ), заключается в замене прямоугольного представления для комплексных переменных: $\overline{Q}_0 = Q_{00} + Q_{01}i,$ $\overline{Q}_1 = Q_{10} + Q_{11}i,$

$\overline{P}_0 = P_{00} + P_{01}i,$ $\overline{P}_1 = P_{10} + P_{11}i,$ с представлением КЛСЧ при тех же значениях: $\overline{Q}_0 = \beta^{q_{00}} cis(q_{01}),$ $\overline{Q}_1 = \beta^{q_{10}} cis(q_{11}),$ $\overline{P}_0 = \beta^{p_{00}} cis(p_{01}),$ $\overline{P}_1 = \beta^{p_{10}} cis(p_{11}).$ Другими словами, $P_i = \beta^{p_{00}} cis(p_{01}) + \beta^{p_{10}} cis(p_{11}) j,$ $Q_0 = \beta^{q_{00}} cis(q_{01}) + \beta^{q_{10}} cis(q_{11}) j.$

Было доказано, что два самых естественных способа, которые можно было бы попытаться использовать в ЛСЧ для умножения кватернионов, не эффективны: во-первых, функция кватернионного логарифма не поможет упростить умножения, потому что умножение кватернионов не коммутативно, хотя сложение кватернионов коммутативно; во-вторых, с помощью ЛСЧ для двенадцати сложений/вычитаний, участвующих в прямоугольном определении умножения кватернионов, гораздо дороже, чем при использовании плавающей запятой. Чтобы преодолеть это, было предложено новое представление ККЛСЧ. Для кватерниона Q используется пара комплексных чисел в конструкции Кэли – Диксона, в котором каждое комплексное число представляется в КЛСЧ в логарифмическо-полярной форме. Для простой реализации с этим представлением нужны четыре КЛСЧ умножителя и два КЛСЧ сумматора, а так как ККЛСЧ сумматоры имеют общие подвыражения, оборудование может быть оптимизировано до эквивалента около по 5,5 ЛСЧ сумматоров и один ЛСЧ сумматор/вычитатель. Эти особенности могут извлечь выгоду во встраиваемых системах, которые интенсивно используют кватернионы в различных приложениях.

УДК 004.056:061.68

А.В. Федорцов

ПОРЯДОК ФОРМАЛИЗАЦИИ МОДЕЛИ ПОЛЬЗОВАТЕЛЯ ПРОГРАММНО-ТЕХНИЧЕСКИМИ СРЕДСТВАМИ ДЛЯ ОБЕСПЕЧЕНИЯ УПРАВЛЕНИЯ ЗАЩИТОЙ ИНФОРМАЦИИ НА ОСНОВЕ АППАРАТА НЕЧЕТКОЙ ЛОГИКИ

Влияние человеческого фактора на процессы, протекающие в информационных системах различных организаций, нельзя недооценивать. Вместе с тем отсутствие четкого представления об источнике угроз (внутреннем нарушителе), ассоциируемом с указанным фактором, а также о последовательности и результатах его злоумышленных и незлоумышленных действий не позволяет осуществлять адекватное руководство защитой информации и приводит, в свою очередь, к ощутимым для организации негативным последствиям. По этой же причине