устройство уплотнения. Поскольку в каждом из каналов возможно появление как «0», так и «1», то, очевидно, в любой фиксированный момент времени на устройство уплотнения от всех каналов поступает одна из $2^{L_У}$ возможных комбинаций «0» и «1». В общем случае при представлении сообщения в каждом из каналов с помощью кода с основанием b (шестиричного кода, где $b \geq 2$) в любой фиксированный момент времени на устройство уплотнения от всех $L_{т}$ каналов будет поступать одна из возможных комбинаций символов 0, 1, ... , $b-1$. Устройство уплотнения каждой из поступивших комбинаций ставит в соответствие свой номер (однозначно соответствующее этой комбинации число), который и является групповым сигналом. Таким образом, при данном методе уплотнения групповой сигнал не является линейной комбинацией канальных сигналов, а представляет собой однозначное отображение возможных комбинаций канальных символов, чем и объясняется название данного метода уплотнения. Групповой сигнал может кодироваться различными способами. На приемной стороне по принятому групповому сигналу восстанавливаются символы кодов сообщений в каждом из каналов, т. е. осуществляется разделение каналов. Данное разделение возможно, потому что любая комбинация символов кода сообщения однозначно соответствует групповому сигналу. В общем случае разделение каналов осуществляется нелинейными устройствами, хотя возможны модификации комбинационного уплотнения, при которых разделение осуществляется линейными устройствами.

На выбор того или иного типа кода группового сигнала существенное влияние оказывает сложность реализации соответствующей операции нелинейного преобразования (операции уплотнения) и обратной операции (операции разделения каналов). В этой связи большой интерес представляет один из частных случаев комбинационного уплотнения – логическое, или мажоритарное, уплотнение каналов. В результате данного уплотнения каждой комбинации двоичного кода с блоковой длиной $П_С$ в параллельной форме поступившей от уплотняемых источников, в устройстве уплотнения ставится в однозначное соответствие комбинация двоичного кода группового сигнала с блоковой длиной $П$, представленного в последовательной форме. При этом значение каждого двоичного символа кодовой комбинации группового сигнала определяется в соответствии с логической функцией абсолютного большинства, т. е. мажоритарно, что и определяет название данного метода уплотнения.

Двоичный код группового сигнала, получаемый при мажоритарном уплотнении, удобен для дальнейших преобразований на передающей стороне и обработки на приемной стороне и имеет минимально возможный пикфактор, что позволяет полностью использовать потенциальные возможности радиопередающего устройства. При этом нелинейность группового тракта не приводит к появлению междуканальных помех. Кроме того, при данном методе уплотнения оказывается возможным линейное разделение каналов, реализуемое полностью цифровым устройством разделения.

На сегодняшний день важнейшими достоинствами кодового уплотнения являются эффективное использование выделенной полосы частот (все каналы занимают одну и ту же полосу частот в одном временном интервале), обеспечение высокой потенциальной помехоустойчивости (за счет ортогональных функций) и высокая помехозащищенность, возможность обеспечить энергетическую и структурную скрытность передаваемой информации.

УДК 004.42

В.А. Тарасенко, Р.В. Кислинский

ЗАЩИТА ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ГОСУДАРСТВЕННЫХ ОРГАНОВ

«Кто владеет информацией – тот владеет миром» – это, наверно, одно из самых известных высказываний, выражающее суть самой острой проблемы в мире. Актуальность данной работы связана с необходимостью защиты конфиденциальных данных, информации и сведений, утеря, разглашение или искажение которых может повлечь за собой негативные последствия для организации, предприятия и государства, а также необходимость соответствия информационной системы требованиям нормативно-правовых документов. Создание технологий и индустрии сбора, переработки, анализа информации и ее доставки конечному пользователю порождает ряд сложных проблем. Одной из таких проблем является надежное обеспечение сохранности и установленного статуса информации, циркулирующей и обрабатываемой в информационно-вычислительных системах и сетях, а также безопасность самих систем и технологий.

Безопасность информационных систем является одной из важнейших составляющих проблем обеспечения безопасности государственного органа. Переход к новым формам государственного и хозяйственного управления в республике в условиях дефицита и противоречивости правовой базы породил целый комплекс проблем в области защиты данных, информации, знаний и самих информационно-коммуникационных технологий. Развитие информатизации в Республике Беларусь в течение 2011–2015 гг. осуществлялось в соответствии со Стра-

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),