которые посредством своего трансграничного распространения способны вызвать вредные последствия для окружающей среды и человека.

При разработке национальных нормативных правовых актов по вопросам трансграничного загрязнения представляется обоснованным предусмотреть в них добровольное привлечение к борьбе с загрязнением субъектов хозяйствования, производящих вредные выбросы. Реализация этого возможна посредством заключения соглашений с такими субъектами. Принцип добровольности в целом должен стать основным в борьбе с загрязнением воздуха, поскольку только административные методы зачастую оказываются неэффективными.

Принимая во внимание тот факт, что многие государства не справляются с поставленными перед ними международными нормативными правовыми актами задачами, полагаем возможным введение субсидирования международными организациями некоторых программ, разрабатываемых государствами.

Также полагаем, что дифференцированный подход к установлению обязательств в международных соглашениях является более предпочтительным в построении взаимоотношений государств, поскольку все государства обладают разными экономическими и административными возможностями и производят различное количество выбросов загрязняющих веществ в атмосферный воздух.

В.Н. Загурский
Витебский государственный технологический университет,
Н.В. Савельева
Витебский государственный университет им. П.М. Машерова

МАТЕМАТИЧЕСКИЕ АСПЕКТЫ ИСПОЛЬЗОВАНИЯ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ В ЭКОНОМИКЕ И УПРАВЛЕНИИ ПРОИЗВОДСТВОМ

Потребность реализовать аналог собственноручной подписи человека в электронном виде возникла как результат проникновения компьютерных технологий во все сферы человеческой деятельности. Широкое применение электронный способ подписи бумаг нашел в документационном обеспечении управления (ДОУ), платежных системах, электронной торговле и бухгалтерии. Из перечисленных направлений наиболее востребованной и сложной является задача автоматизации ДОУ организаций — главная цель создания систем электронного документооборота (СЭД).

Следует заметить, что электронно-цифровая подпись (ЭЦП) — это не оцифрованный образ рукописной подписи, а результат математических преобразований, выполненных в соответствии с конкретным алгоритмом, свойства и результаты исполнения которого заранее определены и доказаны. В 1976 г. Диффи и Хеллманом было предложено решение такой задачи, которое предполагало использование криптографи-

ческих алгоритмов с открытым ключом. Особенностью такой криптографической системы является наличие у каждой стороны пары ключей — открытого (известного всем) и закрытого (секретного). Открытый ключ есть пара чисел n и e, где $n = pq$ (p и q — простые числа, длина n превышает 512 бит, e — число, взаимно простое со значением функции Эйлера $\varphi(n)$. Секретный ключ – число $d = e^{-1} \ mod \ (p - 1)(q - 1)$.

Стойкость ЭЦП основана на невозможности разложить на простые множители числа p и q. Специальные односторонние функции f (так называемые цифровые дайджесты) выступают в роли «контрольных сумм» сообщений: при изменении в исходном сообщении даже 1 бита дайджест измененной информации отличается от исходного.

Заметим, что функционирование систем ЭЦП основано на фактах, законах и алгоритмах современной теории чисел. В стандарте цифровой подписи DSS (Digital signature standard) при подписи нешифрованных сообщений используется следующая схема организации многосторонней связи с ЭЦП. Каждый участник, имея свою пару ключей, сообщает всем партнерам собственный открытый ключ. Отправитель X получает дайджест $f(S)$ своего исходного сообщения S (например, f возвращает хэш-код md5), зашифровывает дайджест с помощью своего секретного ключа K (подписывает дайджест), получает ЭЦП $K(f(S))$ и посылает получателю Y пару $<S, K(f(S))>$ — «подписанное» сообщение. Получатель Y, получив такую пару, дешифрует подписанный дайджест с помощью открытого ключа O отправителя X, вычисляет дайджест полученного сообщения (S=$O(K(f(S)))$) и сравнивает эти два дайджеста. Совпадение означает, что исходное сообщение не изменено и получено именно от того лица, чей публичный ключ используется для дешифрования. Так подтверждается подлинность отправителя информации. Если дайджесты не совпадают, то сообщение при передаче было искажено или фальсифицировано.

Таким образом, ЭЦП представляет собой некоторое число, структура которого зависит от передаваемого электронного сообщения, причем создать число с такой структурой может только владелец закрытого ключа.

Заметим, что в подобного рода схемах возможны различные проблемы как математического, так и социального характера. К математическим относят проблемы стойкости дайджеста, определения срока действия и длины ключа, которая ввиду роста вычислительных возможностей компьютеров может со временем увеличиваться. Проблема социального происхождения сводится к нападениям на криптографическую систему, которые могут осуществляться как внешними субъектами, так и подписывающей стороной (отказ от подписи) или стороной, проверяющей подпись (навязывание ложной подписи). Для обеспечения устойчивости криптографической системы к нападениям существуют рекомендации по выбору параметров алгоритма.

При этом ЭЦП обеспечила электронному документу необходимые характеристики: подлинность, целостность и неотрекаемость, устранив большинство проблем, свойственных подписи на бумажном документе.

В настоящий период технический прогресс опережает развитие правовой базы стран СНГ. К примеру, ни один суд в Беларуси не признает документ с ЭЦП, а любая виртуальная сделка будет считаться заключенной вне закона. Однако в Российской Федерации некоторые крупные компании (например, «Газпром») создали собственные, действующие внутри этих компаний, корпоративные стандарты ЭЦП и начали заключать виртуальные сделки по ним. К такому шагу готов белорусский концерн «Белнефтехим».

Ожидается, что в 2009 г. в Беларуси будет сформирована нормативная и аппаратно-программная база для широкого внедрения ЭЦП в электронном документообороте. Эти задачи планируется выполнить в рамках реализации программы «Электронная Беларусь». Принятие закона об ЭЦП даст стимул развитию IT-бизнеса, так как электронные документы, подписанные ЭЦП, будут иметь юридическую и доказательную силу в суде наряду с бумажными документами. Налогоплательщики смогут декларировать свои доходы в налоговых органах с использованием сети Интернет и электронной почты, предприниматели заключать виртуальные сделки, признаваемые судом. Законы об ЭЦП приняты в США, Китае, странах ЕС, некоторых странах СНГ.

Н.П. Карасева
Белорусский государственный экономический университет (Минск)

ПОЗИЦИИ РАЗВИВАЮЩИХСЯ СТРАН В ТОРГОВЛЕ ВЫСОКОТЕХНОЛОГИЧНОЙ ПРОДУКЦИЕЙ

До недавнего времени высокотехнологичный экспорт осуществляли развитые страны — США, Германия, Япония, Франция. Однако данные международной статистики указывают на то, что развивающиеся страны активно стали включаться в конкуренцию на рынке высокотехнологичной продукции. Расчет на основе классификации экспортных товаров по степени технологичности показал, что за 1980—2005 гг. позиции развитых стран в мировом экспорте высокотехнологичных товаров значительно ослабли.

Развитие высокотехнологичного экспорта позволяет развивающимся странам предупредить негативные последствия, связанные с нестабильностью цен и доходов от экспорта сырьевой и ресурсоемкой продукции, диверсифицировать структуру экспорта, модернизировать технологическую базу промышленности, снизить экологическую нагрузку на экономику и т.д.

О развитии высокотехнологичного экспорта развивающихся стран свидетельствует увеличение высокотехнологичной продукции в структуре их промышленного экспорта.

С помощью показателей экспорта и импорта высокотехнологичных отраслей промышленности проанализировано развитие высокотехнологичного экспорта 21-й развивающейся страны за 1985—2005 гг. В вы-