Самостоятельный раздел представляют Положения. Это Положение о порядке разработки, производства, реализации и использования средств криптографической защиты информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, Положение о коммерческой тайне, Положение о порядке хранения сведений, составляющих налоговую тайну, доступа к ним и их разглашения, Положение о Государственном центре безопасности информации при Президенте Республики Беларусь.

Документы Национального банка Республики Беларусь - пример правового обеспечения передовой корпоративной информационной системы, влияют на регламент нормативно-правовой деятельности всех предприятий республики и включают концепции, руководящие документы, методики испытаний. Концепции представлены двумя документами: Концепция ИБ Национального банка РБ, Концепция ИБ платёжной системы.

ЦИФРОВАЯ ПОДПИСЬ НА БУМАЖНОМ ДОКУМЕНТЕ

Юрий ПУШНЯК, Владимир ШКИЛЁВ, Аркадий АДАМЧУК
Государственное предприятие ЦГИР "REGISTRU"

The new technology of cryptographic protection of paper documents from a fake is offered. The technology bases on the general approach to protection of the material objects, formulated earlier. The technology borrows the effective mechanism of the digital signature used up for protection of electronic documents only.

Предложена новая технология криптографической защиты бумажных документов от подделки. Технология опирается на общий подход к защите материальных объектов, сформулированный ранее. Технология заимствует эффективный механизм цифровой подписи, применявшийся до этого для защиты только электронных документов.

Многовековая проблема защиты от подделки разнообразных бумажных документов – официальных текстовых документов, финансовых документов строгой отчётности, паспортов и удостоверений личности, дипломов, аттестатов, сертификатов, ценных бумаг, денежных банкнот, бюллетеней для голосования, виз, акцизных марок, этикеток для упаковки товара и др. – остаётся весьма актуальной и в наши дни.

Особенность нынешней ситуации заключается в том, что теперь в обращении наряду с бумажными документами участвуют и электронные документы, причём последние защищены гораздо надёжнее. Этому способствовало интенсивное развитие современной криптографии, предложившей эффективные альтернативы для традиционной печати и подписи.

Очевидно, что в будущем доля бумажных документов в общем обороте будет постепенно снижаться, но они ещё достаточно долго будут оставаться востребованными.

Этими обстоятельствами продиктован интерес к новым технологиям, которые обеспечивали бы безопасное и эффективное **совместное** обращение как электронных, так и бумажных документов в составе единой автоматизированной системы документооборота.

Использовавшиеся ранее технологии полиграфической защиты бумажных документов, основанные на применении специальной бумаги, особой краски, "водяных знаков", рельефных рисунков, специальных вкраплений, микротекста и т.п., в сочетании с традиционной печатью и подписью, никак не соответствуют этому требованию.

Технологии нового поколения - голограмма, RFID – представляются перспективными, но пока достаточно затратными. Поэтому интенсивный поиск новых подходов и технологий продолжается.

Авторами доклада предлагается новая технология криптографической защиты бумажных документов от подделки. Технология опирается на ранее предложенный авторами общий подход к защите материальных объектов произвольной природы, а также заимствует общеизвестный механизм цифровой подписи, который до этого применялся только по отношению к электронным документам.

Общий подход заключается в следующем. В состав объекта искусственно вводится специальная физическая метка, по своей природе адекватная защищаемому объекту, но не нарушающая его потребительских свойств и других важных качеств.

Применительно к бумажному документу это может быть совокупность отверстий произвольной конфигурации, полученная на бумажном носителе документа с помощью неуправляемого электрического разряда [1].

Метка наносится на бумажный носитель документа с помощью специальной электроразрядной установки на этапе подготовки документа к выпуску в обращение.

В докладе показано, что полученная в результате стохастического физического процесса метка обладает следующими интересными качествами:

(a) Она физически неотделима от защищаемого объекта (бумажного документа).
(b) Она уникальна, неповторима.
(c) Она характеризуется набором случайных параметров.
(d) Она невоспроизводима.

Указанные качества делают метку ценнейшим элементом механизма криптографической защиты бумажного документа на основе традиционной цифровой подписи [2].

Процедура подписания документа выглядит так. Сначала на бумажный документ наносится физическая метка. Затем метка сканируется. Полученное цифровое изображение метки подписывается цифровой подписью (закрытый ключ) авторитетного лица. Далее подписанное изображение преобразуется в штриховой код, который печатается на бумажном документе рядом с меткой.

Поскольку метка физически неотделима от документа, то, "подписав" изображение метки, авторитетное лицо фактически подписывает соответствующий бумажный документ, т.е. удостоверяет его подлинность.

Процедура проверки подлинности документа выглядит так. Любой проверяющий читает штриховой код, напечатанный на документе, раскрывает цифровую подпись с помощью открытого ключа авторитетного лица и узнаёт "правильное" изображение метки. Затем он сканирует реальную физическую метку, нанесенную на документ, и сравнивает оба изображения. Если они совпадают, то документ признаётся подлинным.

В докладе показано, что предложенная технология надежно защищает бумажный документ от любых потенциальных атак злоумышленника. Запускать в обращение подделку собственного изготовления или нелегальную копию (дубликат) уже имеющегося подлинника бессмысленно – первая же проверка выявит факт подделки.

Литература:

1. Шкилёв В., Недиогло В., Адамчук А. Электроразрядная защита от подделки бумажных документов. – Securitatea informațională 2010: Conf. intern. (ed. a 7-a) – Ch.: ASEM, 2010. – p. 24-26.
2. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – Издательство "Триумф", 2002 г. – 816 стр.

НАДЕЖНОСТЬ АНАЛИТИЧЕСКОЙ ИНФОРМАЦИИ ПРИ УПРАВЛЕНИИ ПРЕДПРИЯТИЕМ

Росица Н. ИВАНОВА
Университет национального
и мирового хозяйства (София, Болгария)

The Financial-Economic (business) analysis is an information system. In the process of generation of result-oriented analytical information regarding the company management should be provided and secured objective conditions for its protection against the multiple and various threats and risks. Therefore, an information security system for analytical information should be developed and should effectively operate by observing the security principles. This is an objective prerequisite for the formation of competitive advantages for the company.

Финансово-хозяйственный (бизнес) анализ представляет собой специализированную функцию управления предприятием. Он обеспечивает информацию всем уровням управления. Административное управление отвечает за достижение ключевых целей предприятия, а оперативное – за достижение специфических целей отдельных структурных звеньев. Таким образом достигается объективная синхронизация целей предприятия с целями по функциональным центрам ответственности.

Финансово-хозяйственный (бизнес) анализ представляет собой информационную систему. Информация определяется как совокупность определенных