

personal information such as birthdates and mothers' maiden names. In this field the number of legal acts is growing but there is still much to improve.

3. Summary

To summarise, there is none legal environment which fully protects information, which can assure the owner of particular data that it is safe and absolutely nobody can get access to check it. In case of information security is never ending process that requires constant monitoring, updates, research, investment and implementation of new technologies. But before everything the secret lies within the law system which is able to control all abuses. The perfect model simply can not be done. The role of each legislator is to try to gain such a level that will increase, as much as possible, probability of safety.

On the other side the punishment must be also quite severe. But here emerges another problem. To punish with pecuniary penalty or with insulating penalties. Conscientiousness of concrete society is crucial in this case.

Nevertheless, does every modern country has that kind of muscle to enforce the implementation of its own legal regulations, basis, in relation to informational security. For many reasons, some of them were mentioned above, it raises concerns.

Information security is becoming more demanding, as the skills involved become more complex and managerial. Experts who create protection models or systems must be aware of the enormity of obstacles which have to be surmount. Obviously it is not easy but also can't be left unsolved.

Bibliography

1. Claudel, *Journal 1904-1955*, PAX, Warsaw 1977
2. Abeles, Bartol, Batdorff, Hash, Rollins, Robinson, *Integrating IT Security into the Capital Planning and Investment Control Process*, NIST, Gaithersburg 2005
3. Namieśnik, Wesołowski, *Security and protection of data*, Gdańsk 2007
4. Kifner, *Security policy and the protection of information*, Helion Publishers, Warsaw 1999

О ТЕХНОЛОГИЧЕСКИХ АСПЕКТАХ ЕДИНОГО ГОСУДАРСТВЕННОГО ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

Андрей САУЛЯК,

*ЦГИР "REGISTRU" Министерства информационных
технологий и связи Республики Молдова*

Aspects of security at creation uniform system of paper and electronic state document circulation. Protection methods of electronic documents. Electrodigit Technology of Protection of the paper documents.

Построение единого государственного документооборота (ЕГД) кажется задачей невыполнимой или требующей несоизмеримых усилий. Но даже если она будет жестко-вертикально внедрена не факт, что она сможет существовать и поддержи-

ваться пользователями (государственными служащими) и/или ее не парализуют внутренние противоречия и коллизии.

Функциональные (типовые) требования – необходимое базовое условие существования АСЭД, а не-функциональные (специальные) требования – условие *эффективной* работы системы государственного документооборота. Как видится авторам, специальные требования к АСЭД могут быть сформированы Единым электронным административным регламентом государства (ЕЭАРГ).

Со способами обмена электронными документами и методами обеспечения их долговременного хранения тесно связаны проблемы обеспечения их *аутентичности и безопасности*.

С появлением и развитием технологии “цифровой подписи” проблема аутентичности и целостности электронных документов была успешно решена. Более того, “электронные” документы теперь защищены гораздо надёжнее “бумажных”, а широкий арсенал вариантов реализации “цифровой подписи” [8] – классическая подпись, коллективная подпись, слепая подпись, подпись с забыванием и др. – позволяет в любых конкретных ситуациях получать гибкие и эффективные решения с недостижимыми ранее возможностями.

“Бумажные” документы защищены хуже. Полиграфические методы защиты “не вписываются” в рамки концепции современного автоматизированного документооборота. Поэтому если некая система документооборота предполагает работу как с “электронными”, так и с “бумажными” документами, то возникают определённые сложности. В частности, возникает потребность в универсальных автоматизированных методах и средствах, которые позволяли бы одинаковым образом обрабатывать документы обоих видов при их идентификации и проверке подлинности. Очевидно, что при этом уровень автоматизации и уровень надёжности защиты должны соответствовать более высоким критериям, присущим обороту именно “электронных”, а не “бумажных” документов.

Автором статьи предлагается новый метод идентификации и защиты “бумажных” документов, который полностью совместим с аналогичными процедурами для “электронных” документов, что позволяет организовать единый документооборот для документов обоих видов.

Основу метода [5] составляет специальная физическая метка, которая наносится на защищаемый документ с помощью неуправляемого стохастического электрического разряда (пробоя). В результате пробоя на бумажном носителе создаётся множество отверстий, общее количество которых, а также размеры и взаимное расположение имеют случайный характер.

Теперь задача идентификации может быть решена следующим образом. На начальном этапе жизненного цикла документа – перед выпуском документа в оборот – на “чистый” бланк документа наносится уникальная метка, затем на бланке печатаются порядковый номер документа, информация о его происхождении и собственно содержание (текст) документа.

Метка проставляется в специально отведенной для этого зоне, удобной для автоматизированного нанесения (записи) и считывания. С помощью специального

мобильного сканера производится считывание изображения метки и его преобразование в компактный двоичный код – т.н. цифровой образ метки.

Далее возможны варианты. Например, в простейшем случае, который приводится здесь только для иллюстрации общих положений, пара ”порядковый номер документа – цифровой образ метки” помещается в базу данных системы документооборота и используется в дальнейшем для идентификации и проверки подлинности документа, находящегося в обороте.

Более реалистичным представляется другой подход, который не предполагает постоянных обращений к удаленной базе данных. На этапе подготовки документа цифровой образ метки, полученный при сканировании, а также другие данные о документе – порядковый номер и информация о происхождении – “подписываются” цифровой подписью (закрытым ключом) официального лица, выпускающего документ. Подписанная информация печатается на документе в виде штрихового кода. После этого информация о документе регистрируется в базе данных, а сам документ выпускается в оборот. Обращение к базе данных происходит в исключительных случаях.

Объединив технологию ЭЦП и электроразрядных меток можно получить достаточно защищенную систему государственного документооборота, в котором бумажный и электронный документ будут иметь соизмеримую юридическую силу. Один и тот же документ в бумажной и виртуальной форме может быть однозначно идентифицирован и защищен, и может быть осуществлен переход из электронной версии документа в бумажную и обратно с сохранением юридической силы такого изменения.

Литература

1. Тихонов В.И., к.и.н., директор Центрального архива документов на электронных носителях Москвы (ЦАДЭНМ) Архивное хранение электронных документов: проблемы и решения. Журнал «Делопроизводство и документооборот на предприятии». М., (№2)2006.
3. Г. Ретер. Электронные лавины и пробой в газах. Перевод с английского под редакцией В.С. Комелькова, Издательство «Мир». Москва, 1968, -390 с.
4. Шкилев В.Д., Адамчук А.Н., Недиогло В.Г. Электроразрядная технология защиты документов особой важности (строгой отчетности) Электронная обработка материалов, №2, 2008, с. 4-10.
5. Шкилев В.Д., Мартынюк Н.П. Патент Российской Федерации .RU 2 399 496 С2 «Электроразрядный способ изготовления бумажных документов строгой отчетности и бумажных денежных знаков».
6. Шкилев В.Д., Патент Российской Федерации .RU 2 397 845 С2 «Электроразрядный способ изготовления бумажных документов строгой отчетности и бумажных денежных знаков».
7. W. Diffie, M. Hellman, New Directions in Cryptography, IEEE Transactions on Information Theory, 22(6): 644-654, November 1976.
8. В. Мао. Современная криптография. Теория и практика. – М.: Изд-во ”Вильямс”, 2005 г., 768 с.