УДК 665.64.097.3

СИСТЕМА ЗАЩИЩЕННОГО ОБМЕНА ДОКУМЕНТАМИ МЕЖДУ ОРГАНИЗАЦИЯМИ

Гапонова О.В.

THE SYSTEM SECURE EXCHANGE OF DOCUMENTS BETWEEN INSTITUTIONS

Gaponova O.V

В статье рассмотрена система для защиты электронного документооборота "ДЕЛО" - Подсистема "ЭЦП и шифрование". Электронная цифровая подпись (ЭЦП) поможет проверить целостность электронного письма (e-Mail) и убедиться в надёжности отправителя. Однозначно определит автора статьи, опубликованной в Интернете, и укажет дату публикации.
***Ключевые слова**: электронный документ, шифрование данных, защита информации.*

1. Введение. Современный этап развития общества характеризуется возрастающей ролью информационной сферы, представляющей собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации.

Под информацией обычно понимаются сведения (сообщения, данные) независимо от формы их представления. К защищаемой информации относится информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации. Это, как правило, информация ограниченного доступа, содержащая сведения, отнесенные к государственной тайне, а также сведения конфиденциального характера.

Эффективная работа любого предприятия в настоящее время немыслима без организации электронного документооборота. Работа с документами в электронной форме позволяет быстро и удобно хранить, обрабатывать и передавать документы в информационной системе предприятия. Однако системы электронного документооборота могут быть подвержены следующим воздействиям:

- нарушение конфиденциальности передаваемых документов;
- несанкционированное искажение электронных документов;
- отправка ложного электронного документа от имени легального пользователя системы.

Целью работы является комплексное решение по организации защищённого электронного документооборота системой "ДЕЛО" - Подсистемой "ЭЦП и шифрование".

2. Изложение материала. Электронная цифровая подпись (ЭЦП) является необходимым условием для полноценной реализации защищенного электронного документооборота. Она представляет собой аналог традиционного заверения бумажного документа при помощи подписи и печати. Помимо этого ЭЦП позволяет подтвердить личность автора или отправителя корреспонденции, а также является гарантией того, что в документ после его подписания не были внесены изменения.

Возможности применения ЭЦП и шифрования данных обеспечиваются благодаря интегрированным в систему «ДЕЛО» сертифицированным средствам криптографической защиты информации – Крипто АРМ, Крипто Про CSP, Сигнал Ком CSP, Верба OW, Домен-К, Авест, Генкей, решения Microsoft. Параметры подписи и выбор сертификата представлены на рис. 1, 2.

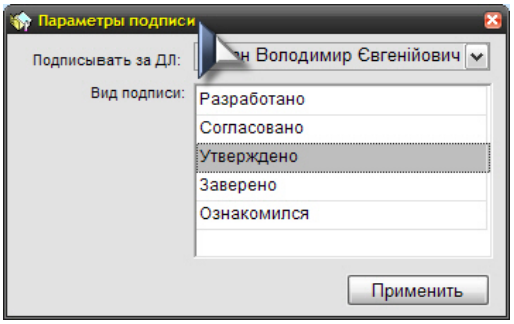

Рис. 1. Параметры подписи

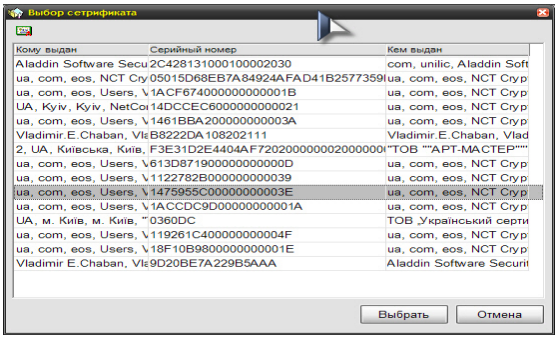

Рис. 2. Выбор сертификата

Применение электронной цифровой подписи (рис. 3.):

- регистрируя входящие документы, сотрудник может ставить свою ЭЦП на прикрепляемый к карточке файл, удостоверяя его подлинность. При работе с проектами документов, исходящими и внутренними документами организации, ЭЦП может применяться при согласовании, визировании, утверждении, регистрации и отправке документа адресату;

- система предоставляет возможность подписывать ЭЦП файлы, хранящиеся в базе данных и отправляемые по электронной почте. При необходимости, документ может быть подписан несколькими сотрудниками, что очень удобно для автоматизации процедур согласования и утверждения документов. В случае, если система «ДЕЛО» установлена у всех участников обмена информацией, пользователи получают возможность распространять подписанные документы по всей территориально-распределенной организации;

- любой сотрудник, имеющий доступ к документу, получает достоверную информацию о подписях и подписавших лицах, а также может проверить подлинность каждой подписи «одним нажатием кнопки».

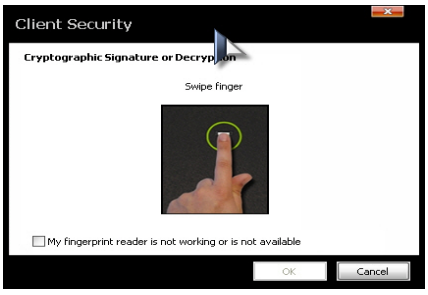

Рис. 3. Применение электронной цифровой подписи

Технология применения ЭЦП:

Для каждого пользователя, обладающего правом подписи, формируется ключ, состоящий из двух частей:

1. Секретный ключ – используется для подписания документов и для дешифрации сообщений, отправляемых пользователем по электронной почте. Он записывается на носитель информации, передаваемый лично пользователю (и может быть дополнительно защищен паролем на случай потери носителя). Подписание происходит путем ввода носителя в считывающее устройство компьютера и нажатия кнопки «Подписать».

2. Открытый ключ – используется для проверки подлинности ЭЦП. Проверка производится на основании сертификата открытого ключа.

Использование технологии ЭЦП позволяет применить один из двух возможных подходов к организации защищенного электронного документооборота, которым соответствуют два варианта поставки опции «ЭЦП и шифрование»:

1 вариант: «корпоративный электронный документооборот»;

2 вариант: «юридически значимый электронный документооборот».

Организация корпоративного электронного документооборота. Электронная цифровая подпись может быть использована для подписания электронных документов в рамках внутрикорпоративных или межкорпоративных соглашений по использованию ЭЦП.

В этом случае электронные документы, подписанные ЭЦП, могут иметь хождение внутри одной организации, а также может быть организован обмен с территориально удаленными подразделениями, филиалами, дочерними компаниями. Возможна также реализация обмена электронными документами с ЭЦП между различными организациями в рамках двухсторонних или многосторонних соглашений.

Данный подход не решает вопросов обеспечения юридической значимости электронного документооборота, но позволяет существенно сократить затраты временных и человеческих ресурсов на передачу документов и их оперативное исполнение.

Криптографический комплекс «Корпоративный документооборот» включает: СКЗИ Крипто Про CSP 3.0 или Сигнал-Ком 3.0, система «ДЕЛО», начиная с версии 8.8.0 (для системы «ДЕЛО» версии 8.6.0 — СКЗИ Крипто Про CSP 2.0).

Организация юридически значимого электронного документооборота. Данный подход является более полным решением и позволяет придать юридическую значимость создаваемым в системе «ДЕЛО» электронным документам благодаря обеспечению ряда условий (установленных законодательно):

- удостоверение точного времени создания электронных документов с помощью штампов времени;

- получение в реальном времени информации о статусе сертификатов цифровых подписей (всей цепочки сертификатов – от личного до сертификата головного удостоверяющего центра);

- поддержка усовершенствованного формата подписи «Крипто Про ЭЦП», обеспечивающего

возможность длительного хранения документов в электронном виде с ЭЦП (до 30 лет).

Документ, подписанный такой ЭЦП, приобретает ряд существенных преимуществ, например:

1. электронные документы, подписанные ЭЦП, имеют одинаковую юридическую силу с бумажными;
2. документы, подписанные ЭЦП, принимаются в ходе судебных разбирательств;
3. ЭЦП может использоваться для подписания первичных бухгалтерских документов для Налоговой инспекции и пр.

Данное решение создает предпосылки для реального перехода к безбумажным технологиям документооборота.

Кроме того, следует отметить, что организация корпоративного и юридически значимого электронного документооборота требует создания регламентов использования ЭЦП в рамках организации.

Криптографический комплекс «Юридически значимый документооборот» включает: СКЗИ Крипто Про CSP 3.0 или Сигнал Ком 3.0, Крипто Арм Стандарт ПРО 4.2, система «ДЕЛО» (рис.4), начиная с версии 8.8.0.

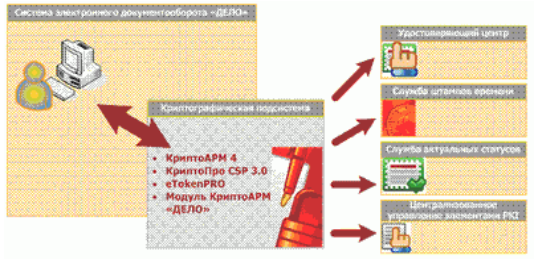

Рис. 4. Система «ДЕЛО»

Шифрование документов, передаваемых по электронной почте. Помимо поддержки ЭЦП средства криптографической защиты информации, входящие в состав данной опции, обеспечивают надежное шифрование данных.

Шифрование сообщений, передаваемых по открытым каналам, позволяет гарантированно защитить конфиденциальную информацию от несанкционированного доступа – прочтения, искажения либо подмены.

Для использования дополнительной опции «ЭЦП и шифрование» необходимо установить на рабочей станции СКЗИ, поддерживающую стандарт Microsoft CryptoAPI.

Для использования данной подсистемы понадобится:

- eToken PRO/32K (CERT) в форм-факторе USB-ключа, СКЗИ разработчика;
- система «КАРМА»

3. Выводы. Возможность защищенного обмена документами по внешним каналам связи является наиболее актуальной для территориально распределенных организаций, т.е. имеющих сеть филиалов или дочерние организации. Гарантий конфиденциальности передаваемых сведений часто требует также переписка с клиентами или партнерами.

Література

1. Бузов Г. А., Калинин С. В., Кондратьев А. В. Защита от утечки информации по техническим каналам: Учебное пособие. - М.: Горячая линия - Телеком, 2005. - 416 с.
2. Программный комплекс «Навигатор». Описание применения. - М.: НПЦ «Нелк», 2002. -104 с.
3. Терминология в области защиты информации: Справочник. - М.: ВНИИ Стандарт, 1993.- 110 с.
4. Хореев А. А. Защита информации от утечки по техническим каналам. Часть 1. Технические каналы утечки информации. - М.: Гостехкомиссия РФ, 1998. – 320с.
5. Рошер С. Основы анализа спектра. - Германия.: Роде и Шварц, 2002. - 215 с.

References

1. Buzov G.A., Kalinin S.V., Kondratyev A.V. Protection against leakage of information on technical channels: Textbook. - M: Hot line - Telecom, 2005. - 416 p.
2. The software package "Navigator". Description application. M .: SPC "NELK", 2002. -104 p.
3. Terminology in the field of information: Handbook. - M .: Institute Standard, 1993.- 110c.
4. Horites A.A. Protection leakage information from technical channels. Part 1 Technical channels of information leakage. -M .: State Technical Commission of the Russian Federation, 1998. - 320 p.
5. Rauscher C. Fundamentals of spectrum analysis. - Germany.: Rohde & Schwarz, 2002. - 215 с.

Гапонова О.В. Система захисту обміну документами між організаціями

В статті розглянуто систему для захисту електронного документообігу "Дело" - Підсистему "ЕЦП і шифрування".

Електронний цифровий підпис (ЕЦП) допоможе перевірити цілісність електронного листа (e-Mail) і переконатися в надійності відправника. Однозначно визначить автора статті, опублікованій в Інтернеті, і вкаже дату публікації.

Ключові слова: *електронний документ, шифрування даних, захист інформації.*

Gaponova O.V. The system secure exchange of documents between institutions

The article describes a system for the protection of electronic document "affair" - Subsystem "electronic signature and encryption."

Electronic digital signature (EDS) will check the integrity of e-mail (e-Mail), and ensure the reliability of the sender. Clearly identify the author of an article published on the Internet, and will indicate the date of publication.

Will write your own opinion about to read a document in Microsoft Word and attach it as a "sticker" to the file, not "spoil" your file itself notes, with a securely tied "sticker" to the current contents of the document (when you change the text of the document "sticker" immediately detects that the document changed). Leaving the "business card" of the

actions committed in the electronic world, confirm the credentials, etc.

Electronic digital signature (EDS) - a powerful tool for the control of authenticity of electronic information, ensure the integrity of electronic data confirm their authorship and relevance. Digital signature - is a data object that is created for signing data, allowing to verify the integrity and authenticity of the data.

EDS can be used as a responsible signature to an electronic document - that is, as an analogue of a handwritten signature or seal on a paper document. In particular, in this incarnation digital signature is used in electronic document for different purposes. EDS is widely used to sign programs or individual modules to computer users by downloading the program from the Internet, and using them in their work, I could be convinced of the reliability and accuracy of their work and the reliability of the source of these programs. When conducting business correspondence secretaries from different companies digital signature can serve as an "envelope" - at one end of a letter sealed with the help of electronic signature, and at the finish of the recipient "opens" the envelope, making sure the full integrity and authenticity of data. With EDS you can agree on how electronic versions of documents between different services within an organization and between different organizations. In this case, the text of the agreement will be protected from uncoordinated changes, and every responsible authority would have to agree on the document using their own electronic signature, thus confirming their attitude towards him. This signature unmistakably tell not only about who signed the document, but also indicate the date and time of signing. If the employee chooses to give up responsibility for the sight of a document or sending the information in the letter, sealed by his electronic signature, the digital signature is easy to convict him. For example, often requires a contract to agree to the legal department, the accounting department and other departments of the company, and only after that it will sign the leaders of both sides. This agreement, and the sight of all responsible agencies may be carried out now in electronic form using digital signature.

Key words: *electronic document, data encryption, data protection.*

Гапонова Оксана Володимирівна – спеціаліст кафедри електронних апаратів, Технологічний інститут східноукраїнського національного університету ім. В.Даля (м. Сєвєродонецьк). mobulochka@rambler.ru

Рецензент: **Смолій В.М.** – д.т.н., професор.

Стаття подана 6.01.2015