ЛАНИТ

LanDocs: ПОДСИСТЕМА БЕЗОПАСНОСТИ

Руководство пользователя (LD3)

Система автоматизации делопроизводства и ведения архива электронных документов LanDocs 3

105066, Москва, ул. Доброслободская, д. 5, стр. 1

Тел. (495) 967-66-50, факс (499) 261-57-81

E-mail: lanit@lanit.ru, http://www.lanit.ru

Аннотация

Данный документ является руководством пользователя подсистемы безопасности системы LanDocs. Документ предназначен для пользователей, использующих механизмы электронной подписи и шифрования конфиденциальных документов.

Программа, описанная в данном документе, поставляется в соответствии с лицензионным договором и может использоваться лишь в строгом соответствии с условиями лицензионного договора.

В документе содержатся:

- руководство по генерации личных ключей пользователей;
- руководство пользователя по использованию ЭП при работе с документами LanDocs;
- руководство по шифрованию конфиденциальных документов.

СОДЕРЖАНИЕ

1. НАЗНАЧЕНИЕ И УСЛОВИЯ ПРИМЕНЕНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

1.1. Назначение программного обеспечения

Подсистема безопасности системы LanDocs предназначена для защиты целостности и подтверждения авторства документов посредством использования механизма электронной подписи, а также защиты конфиденциальной информации методом ее шифрования.

Часть подсистемы, функционирующая на клиенте, позволяет пользователю подписывать своим личным ключом документы, сообщения и другие информационные объекты LanDocs, производить проверку подписей других пользователей, а также зашифровывать и расшифровывать конфиденциальные документы.

Используя клиентское программное обеспечение системы LanDocs, пользователь производит генерацию личных ключей и создает запросы на сертификаты.

1.2. Требования к квалификации пользователей

Для работы с подсистемой безопасности LanDocs пользователи должны:

- уметь работать с используемым клиентским программным обеспечением LanDocs в объеме, определенном в соответствующем руководстве пользователя LanDocs;
- обладать навыками работы в графическом интерфейсе Windows;
- знать положения настоящего руководства.

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Администратор безопасности (администратор) – ответственный сотрудник организации, осуществляющий настройку и администрирование подсистемы безопасности. Администратор безопасности также осуществляет выпуск и отзыв сертификатов пользователей.

Администратор сервера безопасности (удаленная консоль СБ) – приложение, позволяющее осуществлять удаленное администрирование СБ, производить выпуск и отзыв сертификатов, просматривать журнал безопасности.

База данных сертификатов – централизованное хранилище сертификатов открытых ключей пользователей и списка отозванных сертификатов в базе данных LanDocs. База данных сертификатов используется для доступа к открытым ключам локальных клиентов.

Выпуск сертификата – изготовление сертификата открытого ключа Центром сертификации на основе запроса. Выпущенные сертификаты сохраняются в базе данных сертификатов.

Заверка электронной подписи (timestamp) – подписание электронной подписи пользователя секретным ключом Сервера безопасности. Заверка ЭП Сервером безопасности позволяет контролировать время подписания документа и гарантировать действительность ключа пользователя на момент подписания документа.

Запрос на сертификат – сообщение, формируемое пользователем и содержащее открытый ключ, и всю информацию о нем. Запрос подписывается секретным ключом, соответствующим открытому ключу запроса, и направляется в Центр сертификации.

Клиент LanDocs – включается в состав клиентского и серверного ПО системы LanDocs, требующего в ходе своей работы исполнения криптографических операций.

Ключ – ключевой элемент криптографических преобразований, используемый при простановке и проверке ЭП, шифровании и дешифровке информации. Ключ состоит из двух частей: личного (секретного) ключа и открытого ключа. Личные ключи используются при простановке ЭП, а также расшифровывании зашифрованной информации. Личный ключ защищается средствами криптопровайдера, владелец личного ключа отвечает за его хранение. Открытый ключ используется при шифровании документов, и проверке ЭП. Сертификаты открытых ключей, подписанные Центром сертификации, доступны всем пользователям системы LanDocs.

Контейнер личных (секретных) ключей – средство хранения личных ключей. Структура, размещение контейнеров личных ключей, а так же максимальное количество личных ключей в одном контейнере зависят от используемого криптопровайдера. В подсистеме безопасности ведется учет всех созданных контейнеров личных ключей пользователей.

Криптопровайдер (или **CSP** – Cryptographic Service Provider) — независимый программный модуль, интегрированный в MS Windows и содержащий библиотеку криптографических функций со стандартизованным интерфейсом. CSP выполняет следующие криптографические функции:

- формирование/проверка электронной подписи (ЭП),
- шифрование/дешифрование информации,
- хранение ключей всех типов.

Локальный клиент LanDocs – клиент LanDocs: УПРАВЛЕНИЕ ДОКУМЕНТАМИ. Пользователи, работающие на локальном клиенте, имеют доступ к серверу баз данных и Серверу безопасности по локальной сети (on-line доступ) и получают сертификаты открытых ключей непосредственно от Сервера безопасности.

Отзыв сертификата – прекращение действия сертификата открытого ключа. ЭП. Действия, произведенные секретным ключом после отзыва сертификата соответствующего открытого ключа, недействительны. ЭП считается действительной, если она была сделана и заверена до момента отзыва соответствующего сертификата.

Проверка ЭП – криптографическая процедура, позволяющая определить подлинность и авторство документа на основе текста документа и сертификата открытого ключа пользователя, его подписавшего.

Сервер безопасности, СБ – серверная компонента системы LanDocs. СБ функционирует в качестве сервиса Windows. К основным функция СБ относятся: Центр сертификации, предоставление локальным пользователям on-line доступа к базе данных сертификатов открытых ключей, заверка ЭП пользователей, ведение журнала безопасности.

Сертификат – блок данных, содержащий открытый ключ пользователя, дату и время начала и окончания действия ключа, информацию о пользователе, криптографических алгоритмах, Центре сертификации, другую информацию. Данные, содержащиеся в сертификате, подписываются Центром сертификации. Сертификат ЦС имеется у всех клиентов системы LanDocs, каждый пользователь имеет возможность проверить подлинность сертификатов других пользователей.

Сертификат ЦС – содержит открытый ключ Центра сертификации, предназначен для проверки подлинности сертификатов пользователей. Сертификат ЦС подписывается секретным ключом, который соответствует открытому ключу, на который выпущен сертификат.

Справочник сертификатов – Файл, содержащий сертификаты открытых ключей пользователей системы LanDocs, а также списки отозванных сертификатов. Справочник сертификатов используется при работе удаленных клиентов.

Удаленный клиент LanDocs – LanDocs: ПОЧТОВЫЙ КЛИЕНТ. Удаленные клиенты участвуют в делопроизводственном процессе, используя электронную почту. Пользователи, работающие на удаленном клиенте, используют сертификаты открытых ключей из справочника сертификатов, хранящегося на компьютере пользователя.

Центр сертификации, ЦС – третья сторона, удостоверяющая аутентичность открытых ключей пользователей или других центров сертификации. В обязанности Центров сертификации входит связывание открытых ключей с уникальными именами посредством подписанных сертификатов, управление порядковыми номерами сертификатов и отзыв сертификатов. Подсистема безопасности LanDocs может использовать как собственный ЦС, так и ЦС сторонних производителей.

Электронная подпись, ЭП – блок данных, содержащий информацию о лице, подписавшем документ, о времени подписания, сертификате открытого ключа, а также бинарную последовательность, получаемую в результате криптографических преобразований на основании текста документа и секретного ключа пользователя. ЭП позволяет контролировать целостность документа и однозначно определять его автора.

3. АКТИВИЗАЦИЯ ФУНКЦИЙ БЕЗОПАСНОСТИ

Подсистему безопасности можно отключать и активизировать, в файле конфигурации LanDocs3.exe.config устанавливая соответствующее значение параметра

<add key="SecurityEnabled" value="false"/>

При отключенной подсистеме безопасности простановка и проверка ЭП и шифрование не производятся. По умолчанию, после инсталляции подсистема безопасности отключена.

4. РАБОТА ПОЛЬЗОВАТЕЛЯ С ПОДСИСТЕМОЙ БЕЗОПАСНОСТИ LANDOCS

4.1. Настройка параметров подсистемы безопасности клиентского программного обеспечения

Перед началом использования подсистемы безопасности необходимо произвести настройку параметров безопасности клиента:

- задать имя контейнера личных ключей пользователя;
- задать файл шаблона запроса на сертификат;
- указать каталог, где будут сохраняться запросы на сертификаты;
- установить режим работы (локальный / удаленный);
- задать имя сервера безопасности или указать имя файла справочника сертификатов;
- установить сертификаты Центра сертификации.

4.1.1. Окно настройки безопасности клиента LanDocs

Окно настройки безопасности служит для задания параметров безопасности клиента, установки сертификатов ЦС, генерации личных ключей пользователя и создания запросов на сертификаты открытых ключей, для просмотра сертификатов пользователей.

Вызов из клиента LanDocs: УПРАВЛЕНИЕ ДОКУМЕНТАМИ

➢ В Главном окне на закладке **LanDocs** в меню общих операций выберите пункт **Учетная запись ► Конфигурация безопасности.**

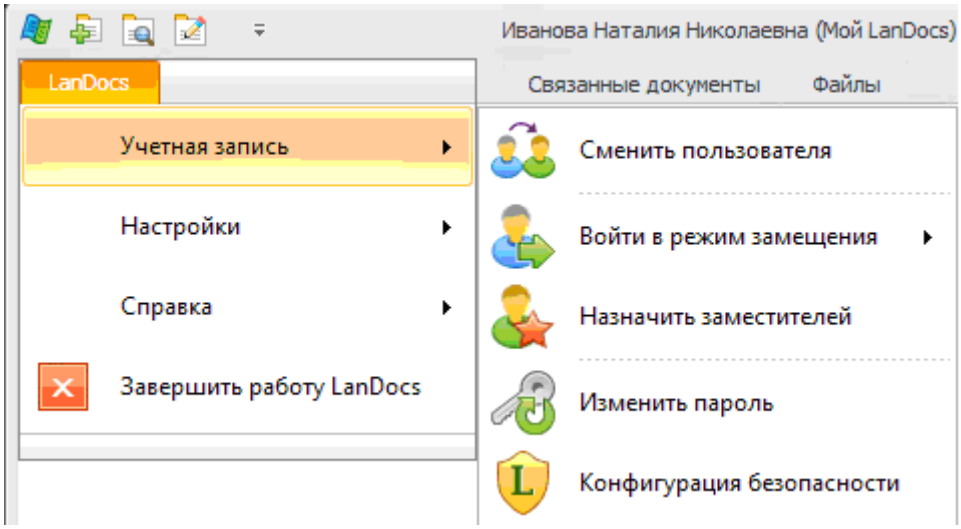

Рис. 1 – Настройка безопасности

- Задайте пароль доступа к контейнеру личных ключей и нажмите кнопку **OK** или нажмите кнопку **Отмена**. При первом входе в конфигурацию, когда еще отсутствуют настройки на контейнер личных ключей, в окне ввода пароля нужно выбрать кнопку **Отмена**. Окно настроек в этом случае будет содержать только вкладки **Общие настройки** и **Сертификаты ЦС** (см. примечание).

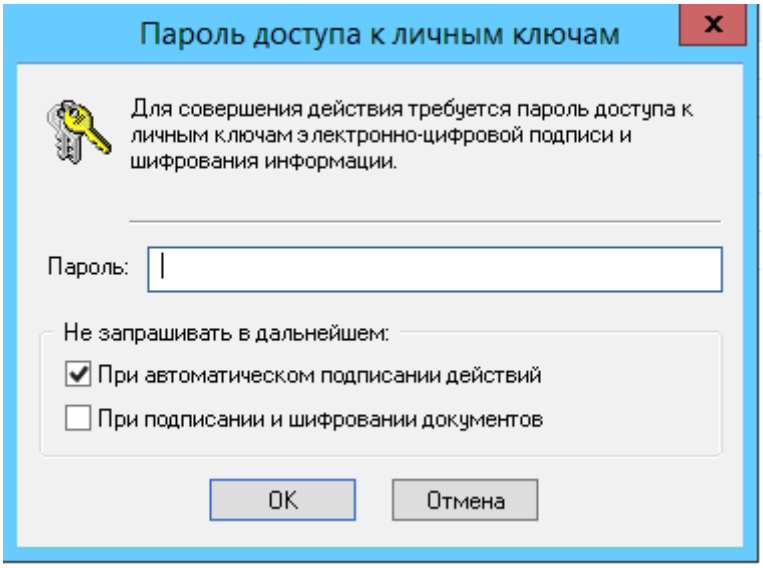

Рис. 2 – Окно ввода пароля доступа к контейнеру личных ключей

Пользователю предоставляется, по умолчанию, только три попытки ввода правильного пароля. Если за три попытки, пароль не будет введен правильно, система в информационном окне выдаст сообщение: "Исчерпано допустимое количество попыток ввода пароля". После закрытия информационного окна, откроется окно настроек, которое будет содержать только вкладки **Общие настройки** и **Сертификаты ЦС.**

В дальнейшем, когда путь к контейнеру личных ключей уже задан, и пароль указан правильно, окно настроек будет открываться со всеми вкладками, включая вкладки личных ключей и сертификатов.

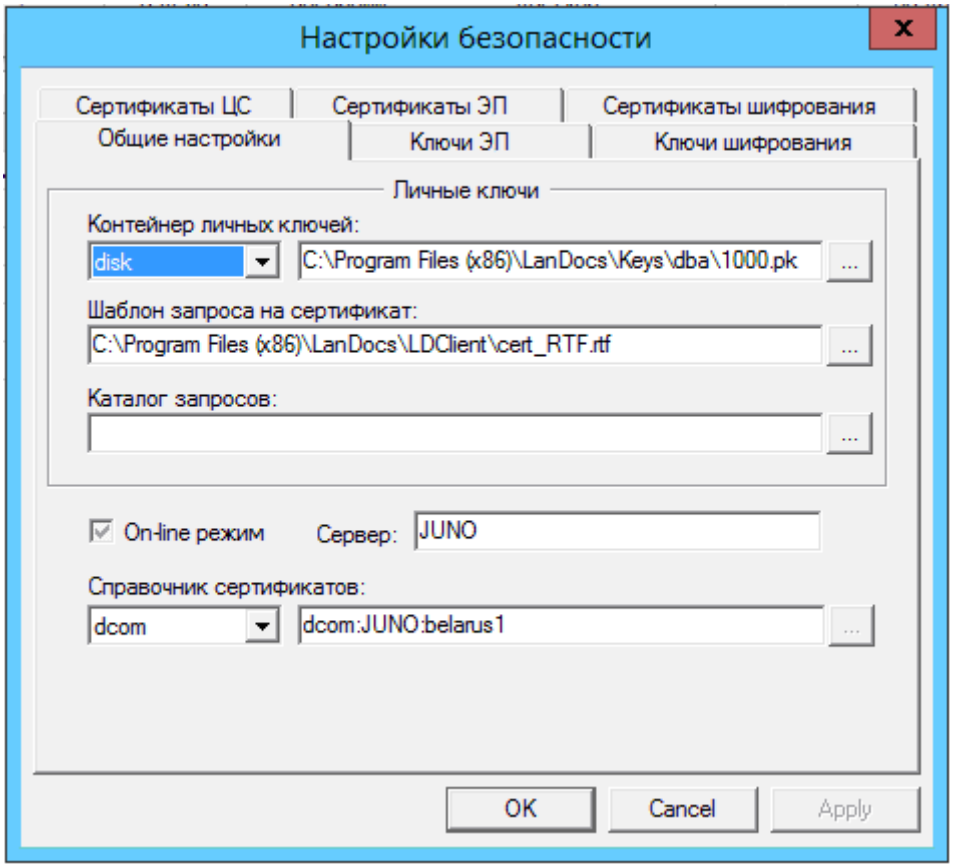

Рис. 3 – Окно настроек безопасности

Первоначальная настройка параметров безопасности клиента LanDocs производится на вкладке **Общие настройки**. Настраиваются следующие параметры:

- **Контейнер личных ключей** – тип носителя, на котором расположен контейнер, и название контейнера личных ключей пользователей, работающих с системой LanDocs на данном компьютере;
- **Шаблон запроса на сертификат** – полное имя файла шаблона бумажного экземпляра запроса на сертификат;
- **Каталог запросов** – каталог, в котором сохраняются файлы запросов на сертификаты открытых ключей;
- **On-line режим** – устанавливает режим работы клиента (локальный / удаленный);
- **Сервер** – имя сервера безопасности, указывается при установленном флажке **On-line режим**;
- **Справочник сертификатов** – полное имя файла справочника сертификатов открытых ключей пользователей и способ доступа к нему. Указывается, если флаг **On-line режим** не установлен.

4.1.2. Контейнер личных ключей пользователей

Личные ключи пользователей, используемые при простановке ЭП и расшифровании документов, хранятся в специальных хранилищах – контейнерах личных ключей.

Контейнеры ключей передаются администратором пользователю. В настройках необходимо задать имя контейнера.

Контейнер защищается паролем, который задается при его создании.

При работе с системой LanDocs на разных компьютерах пользователь должен при переходе с компьютера на компьютер также переносить свой контейнер личных ключей. Размножение файла контейнера личных ключей не допускается (кроме создания резервной копии).

- Для настройки на контейнер с личными ключами на вкладке **Общие настройки** выберите из списка тип контейнера:
  - для значения ***disk*** укажите имя контейнера (с полным путем к нему) вводя значение в поле **Контейнер личных ключей** или выберите его, используя кнопку  , справа от поля.
  - для значения ***native*** нажмите кнопку  , справа от поля и выберите контейнер, соответствующий данному пользователю;
  - для значения ***Smartcard*** настройка не производится.

4.1.3. Шаблон запроса на сертификат

Шаблон запроса на сертификат – это файл формата RTF, содержащий форму бумажного экземпляра запроса на сертификат открытого ключа.

Этот файл устанавливается в главный каталог клиента LanDocs при инсталляции подсистемы безопасности. В случае изменения формы запроса, шаблон может рассылаться администратором системы.

Использование шаблона на запрос сертификата зависит от регламента работы системы безопасности организации.

Имя файла шаблона задается в поле **Шаблон запроса на сертификат**.

4.1.4. Каталог запросов

Файлы запросов на сертификаты открытых ключей пользователя сохраняются в специальном каталоге. Администратор системы может устанавливать разделяемые сетевые каталоги для передачи файлов запросов от пользователей на Центр сертификации. При выборе имени каталога запросов пользователь должен руководствоваться действующими в организации инструкциями или указаниями администратора системы.

Имя каталога запросов задается в поле **Каталог запросов** или выбирается посредством кнопки  , справа от поля.

4.1.5. Режим работы клиента (локальный / удаленный)

Режим работы клиента устанавливается переключателем **On-line режим**. При включенном переключателе (локальный клиент) сертификаты открытых ключей пользователей, используемые при проверке ЭП, а также при шифровании конфиденциальных документов,

автоматически запрашиваются с Сервера безопасности, имя которого задается в поле **Сервер**. При выключенном переключателе, (удаленный клиент), сертификаты открытых ключей считываются из файла справочника сертификатов, имя которого задается в поле **Справочник сертификатов**.

4.1.5.1. Ввод данных о Сервере безопасности

Для локальных клиентов в поле **Сервер** указывается имя или IP адрес компьютера, на котором функционирует сервер безопасности. Имя или IP адрес пользователь получает у администратора системы. Первоначально, этот параметр устанавливается при инсталляции компонента.

4.1.5.2. Ввод данных о Справочнике сертификатов

Это поле задается для удаленных клиентов, не имеющих соединения с сервером безопасности по локальной сети. В поле **Справочник сертификатов** указывается путь и имя файла справочника.

Справочник содержит сертификаты открытых ключей пользователей и списки отозванных сертификатов. Справочник сертификатов создается и распространяется администратором системы. Установка справочника производится простым копированием файла справочника на жесткий диск компьютера или сетевой диск и задания на вкладке **Общие настройки** полного пути к этому файлу.

4.2. Работа с сертификатами Центра сертификации

Сертификаты Центра сертификации используются для проверки целостности и подлинности сертификатов открытых ключей пользователей. Все действующие сертификаты ЦС должны быть заранее установлены на компьютере пользователя, на котором функционирует клиент LanDocs, способом, исключающим их подмену.

Установка, просмотр, и удаление сертификатов ЦС производится на вкладке **Сертификаты ЦС**.

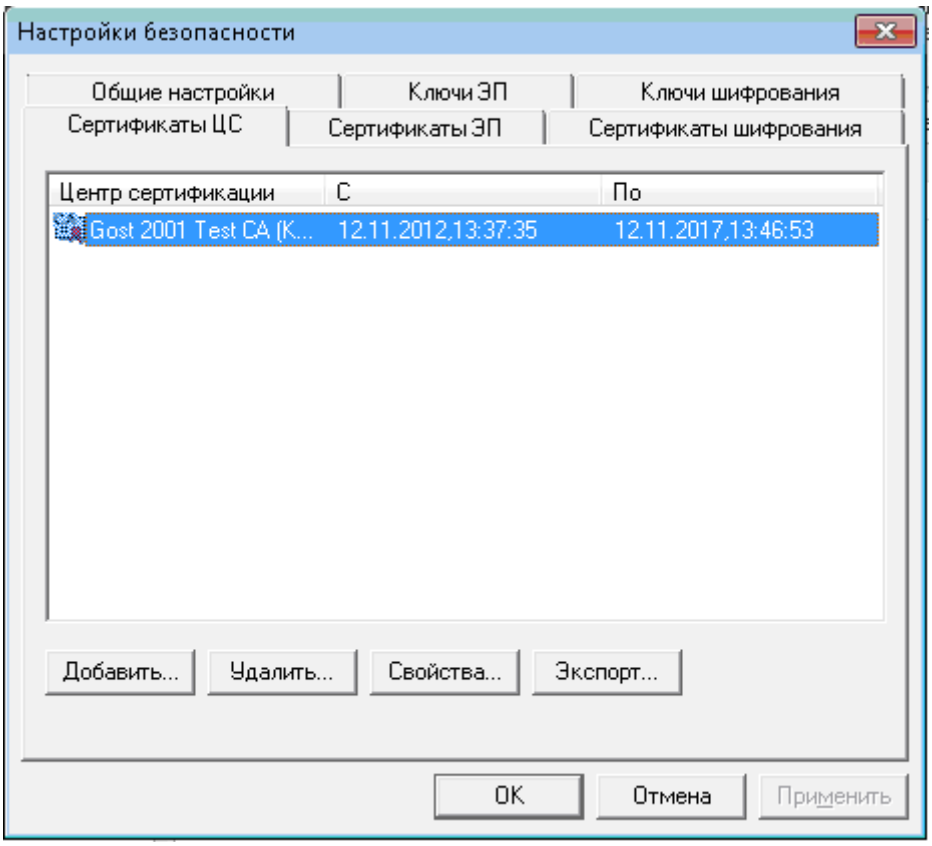

Рис. 4 – Окно настроек Центра сертификации

4.2.1. Установка сертификата ЦС

Для того чтобы установить сертификат ЦС на компьютер пользователя он должен быть предварительно экспортирован из базы данных сертификатов в файл специального формата (DER encoded binary X.509), имеющий расширение DER. Экспорт сертификатов ЦС из базы данных и их рассылку производит администратор системы. Пользователь получает сертификаты ЦС в виде файлов с расширением DER от администратора. Пользователь также может экспортировать сертификат ЦС с другого клиентского компьютера, на котором сертификат уже установлен.

Для установки сертификата:

- На вкладке **Сертификаты ЦС** нажмите кнопку **Добавить**.
- В поле **File name** (**Имя файла**) окна **Open** (**Открыть**) задайте имя файла сертификата, выберите копку **Open (Открыть**).

4.2.2. Удаление сертификата ЦС

Установленные на компьютер пользователя сертификаты можно удалить, используя функцию удаления на вкладке **Сертификаты ЦС**.

Для удаления сертификата:

- Выделите сертификат, который собираетесь удалить в списке сертификатов ЦС на вкладке **Сертификаты ЦС**.
- Нажмите кнопку **Удалить**.

4.2.3. Просмотр сертификата ЦС

В списке сертификатов на вкладке **Сертификаты ЦС** отображаются только название Центра сертификации и сроки действия ключа. Информацию об идентификаторе ключа, серийном номере сертификата, применяемых алгоритмах, собственно открытый ключ и другую информацию пользователь может посмотреть в окне просмотра сертификата.

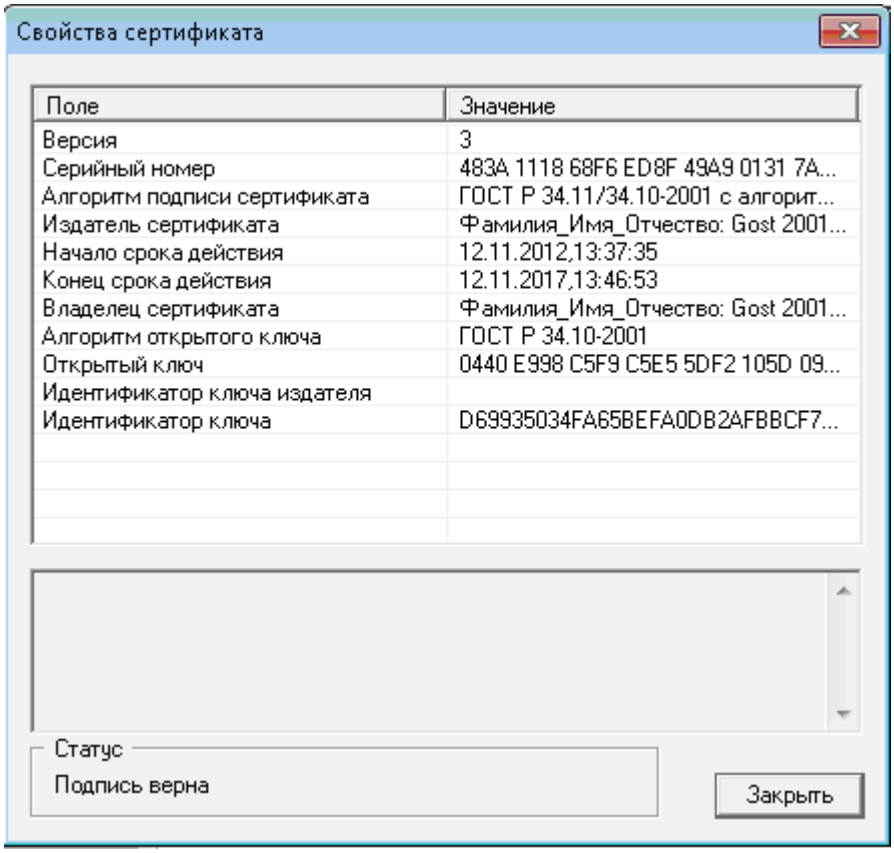

Рис. 5 – Просмотр сертификата ключа

Для просмотра содержимого сертификата:

- Выделите сертификат, содержимое которого хотите просмотреть, в списке сертификатов ЦС на вкладке **Сертификаты ЦС**.
- Нажмите кнопку **Свойства**.

Откроется окно просмотра содержимого сертификата. В верхней части окна выводится список полей, а в нижней части – значение выделенного поля.

4.2.4. Экспорт сертификата ЦС

Сертификаты могут быть экспортированы в файл специального формата с расширением DER, для последующей установки на другом компьютере.

Для экспорта сертификата в файл:

- Выделите сертификат в списке сертификатов ЦС на вкладке **Сертификаты ЦС**.
- Нажмите кнопку **Экспорт**.
- В поле **File name** (**Имя файла**) окна **Save as** (**Сохранить как**) задайте имя файла и нажмите кнопку **Save (Сохранить**).

4.3. Работа с ключами пользователей

Ключи используются при простановке и проверке ЭП, шифровании и дешифровке документов и сообщений. У каждого пользователя имеется два вида ключей: ключи шифрования и ключи электронной подписи. Каждый ключ имеет две составляющие: личный ключ и открытый ключ.

Личный ключ подписи применяется при подписании документов и сообщений, личный ключ шифрования необходим для дешифрования информации, шифрованной для пользователя-владельца ключа. Личные ключи пользователя хранятся в специальном файле – контейнере личных ключей на компьютере пользователя или на сменном носителе. Все ключи в контейнере шифруются на пароле пользователя, для совершения каких-либо операций, требующих применения личных ключей пользователь должен задать пароль.

Открытые ключи подписи применяются при проверке ЭП, открытые ключи шифрования используются для шифрования информации. Открытые ключи хранятся и используются в виде сертификатов - специальных сообщений, подписанных ключом Центра сертификации. Сертификаты, используемые в подсистеме безопасности LanDocs, соответствуют рекомендациям ITU-T X.509. Сертификаты хранятся и передаются по каналам связи в открытом виде.

4.3.1. Личные ключи пользователей

Для просмотра содержимого контейнера личных ключей пользователя служат вкладки **Ключи ЭП** и **Ключи шифрования** окна **Настройки безопасности**, эти вкладки одинаковы по своей структуре и функциональности и отображают соответственно информацию о личных ключах ЭП и шифрования.

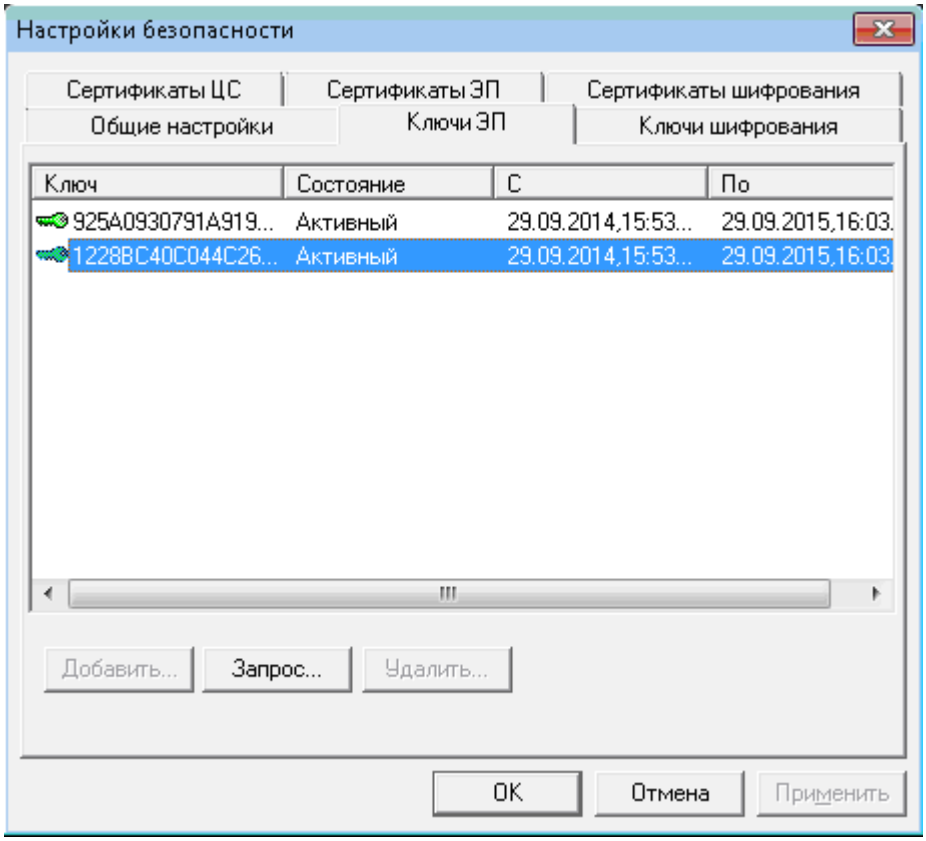

Рис. 6 – Информация о ключах пользователя

4.3.2. Список ключей

В списке ключей отображается следующая информация: индикатор состояния, идентификатор ключа, состояние, сроки действия.

4.3.2.1. Состояние ключа

Состояние ключа определяется наличием сертификата соответствующего открытого ключа, а также соотношением сроков действия ключа с текущей датой. Состояние ключа выводится в поле **Состояние** а также отображается графическим значком.

Таблица 1.
Состояния ключей и их обозначения в перечне

Значок	Состояние	Описание состояния
(желтый)	Неактивный	сертификат есть, но срок действия ключа не настал
(зеленый)	Активный	сертификат есть, ключ действует
(фиолетовый)	Действие закончилось	сертификат есть, срок действия ключа истек

Значок	Состояние	Описание состояния
(красный)	Отозван	сертификат ключа отозван досрочно

4.3.2.2. Идентификатор ключа

При создании ключа ему присваивается уникальный идентификатор. Идентификатор заносится в сертификат открытого ключа, по нему можно определить соответствие личного ключа и сертификата. Идентификатор служит для определения ключа, которым совершалось подписание или проводилось шифрование документа.

4.3.2.3. Сроки действия ключа

Срок начала и окончания действия ключа определяется сертификатом открытого ключа и отображается в списке ключей.

Для ключей, сертификаты, которых были отозваны досрочно, отображаются дата и время отзыва сертификата (т.е. действительный срок действия).

4.3.3. Пароль доступа к контейнеру ключей

Все ключи, содержащиеся в контейнере личных ключей, защищены паролем. Для выполнения всех операций, требующих обращения к контейнеру ключей, необходимо задание пароля. Пользователь должен помнить свой пароль доступа к ключам, в случае утраты пароля восстановить доступ к контейнеру ключей **невозможно**.

Пароль задается при генерации контейнера ключей и сообщается пользователю при передаче ему контейнера.

4.3.4. Генерация и ввод в обращение нового ключа пользователя

Процедура генерации и ввода в обращение нового ключа пользователя производится в соответствии с регламентом предприятия. Запрос на выдачу нового ключа пользователя, запрос на смену по истечении срока действия сертификата передается администратору безопасности согласно правилам, принятым на предприятии (через стороннее ПО).

После выпуска личный ключ должен быть передан пользователю администратором безопасности, также должен быть сообщен пароль доступа к контейнеру ключей.

- Выполните настройку безопасности, указав контейнер личных ключей пользователя (см. п 4.1.2). Нажмите кнопку **Применить**.

- Обновите список сертификатов (см. п. 4.4.2) или добавьте сертификаты ЭП и шифрования.

- Для этого перейдите на вкладку **Сертификаты ЭП** (**Сертификаты шифрования**) и нажмите кнопку **Добавить.** В окне **Open** (**Открыть**) задайте имя файла формата DER, сертификат будет добавлен.

4.3.4.1. Активизация ключа

Активизация ключа производится автоматически при нахождении системой сертификата соответствующего открытого ключа в базе данных сертификатов (для локальных клиентов) или в справочнике сертификатов пользователей (для удаленных клиентов). После активизации ключ имеет состояние "***Активен***", если срок действия ключа уже наступил или "***Неактивен***", если срок действия ключа еще не настал.

В системе существует возможность сформировать запрос на выпуск открытого сертификата и сохранить его в преднастроенной директории.

4.3.4.2. Создание запроса на сертификат открытого ключа

Процедура создания запроса включает генерацию файла запроса (электронный экземпляр запроса) и вывода на печать бумажного экземпляра запроса. Оба экземпляра запроса содержат открытый ключ, его тип, идентификатор, имя пользователя и сроки действия ключа. Электронный запрос представляет собой файл сообщения в специальном формате (PKCS#10), подписанного личным ключом пользователя. Бумажный экземпляр запроса оформляется в соответствии с действующими в организации правилами.

Для создания запроса на сертификат:

- Перейдите на вкладку **Ключи ЭП** или **Ключи шифрования** в зависимости от типа ключа.

- Выделите в списке ключ, для которого создается запрос. Нажмите кнопку **Запрос**.

- Выберите каталог, для сохранения запроса и нажмите кнопку **Save** (**Сохранить**). По умолчанию открывается каталог, указанный в поле **Каталог запросов** окна **Настройки безопасности.**

- Появится окно свойств запроса на сертификат. В открывшемся окне (кнопка **Печать**) можно просмотреть документ, внести в него изменения, вывести его на печать или сохранить в файле формата RTF. Сохраненный RTF файл запроса можно распечатать позднее вне системы LanDocs.

Файл запроса может быть направлен в Центр сертификации, для этого может быть использована передача файла через файл-сервер, электронную почту или внешний магнитный носитель.

4.4. Работа с сертификатами открытых ключей пользователей

Сертификаты открытых ключей выпускаются Центром сертификации на основе запросов пользователей. Сертификаты открытых ключей подразделяются на сертификаты ЭП и сертификаты шифрования. Сертификаты доступны всем пользователям системы, использующим механизмы ЭП и шифрования. В процессе работы, в зависимости от типа клиента, сертификаты либо запрашиваются у Сервера безопасности по локальной сети, либо считываются из справочника сертификатов, установленного на компьютере.

4.4.1. Настройка на источник получения сертификатов

Для того чтобы сертификаты запрашивались у Сервера безопасности при выполнении процедур проверки ЭП и шифрования, необходимо на вкладке **Общие настройки** установить режим **On-line** и задать имя или IP адрес компьютера, на котором установлен Сервер безопасности. В этом режиме вся информация о выпущенных и отозванных сертификатах автоматически становится доступной пользователям.

Для удаленных клиентов, у которых нет связи через локальную сеть с Сервером безопасности, нужно установить убрать флаг **On-line** и задать в поле **Справочник сертификатов** полный путь к файлу справочника. При работе в подобном режиме необходимо обновлять справочник сертификатов каждый раз после выпуска новых или отзыва действующих сертификатов (см. п. 4.4.3).

4.4.2. Просмотр списка сертификатов

Для просмотра списков сертификатов открытых ключей ЭП и сертификатов открытых ключей шифрования служат соответственно вкладки **Сертификаты ЭП** и **Сертификаты шифрования** окна **Настройки безопасности**.

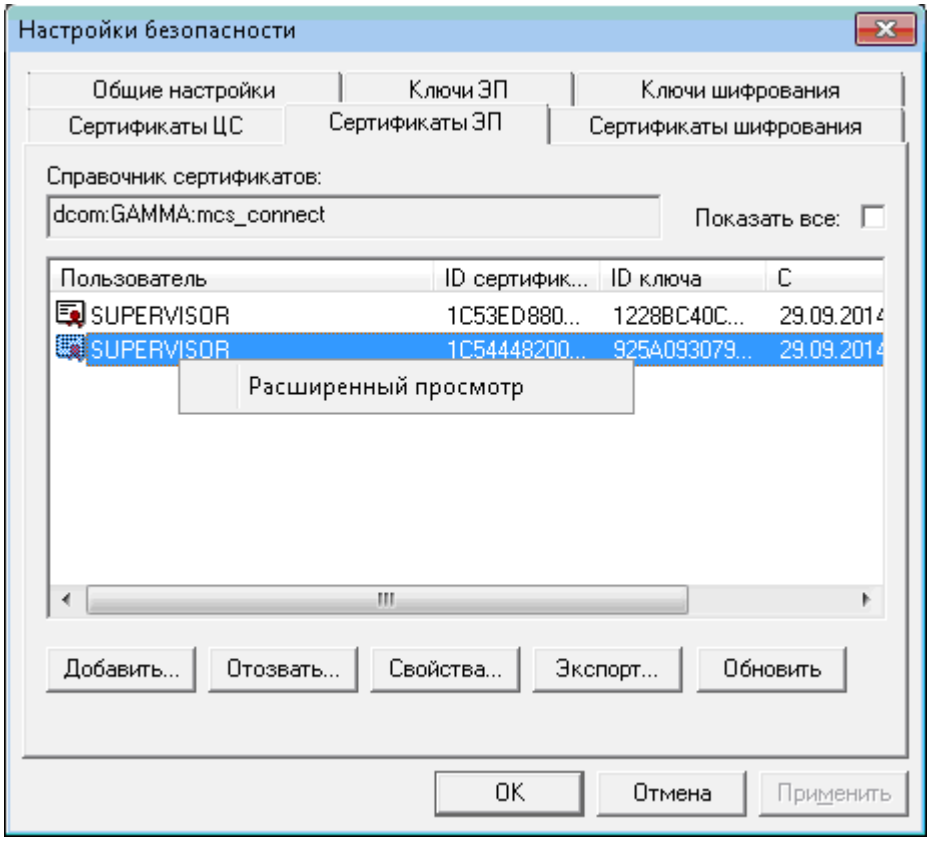

Рис. 7 – Список сертификатов шифрования

В поле **Справочник**, в зависимости от установленного режима, отображается полный путь и имя файла справочника сертификатов, либо имя компьютера, на котором функционирует Сервер безопасности.

Независимо от того, установлен ли режим **On-line**, по умолчанию флаг **Показать все** не установлен и отображаются только сертификаты текущего пользователя. Для просмотра всех сертификатов нужно установить флаг **Показать все**.

Список сертификатов не обновляется динамически при изменении содержимого базы данных.

Для обновления списка:

- Нажмите кнопку **Обновить**.

Сертификат пользователя содержит открытый ключ, а также информацию о применяемых алгоритмах, сроках действия ключа, его идентификаторе, а также сведения об издателе сертификата (Центре сертификации).

Для просмотра содержимого сертификата:

- Выделите сертификат в списке, используя мышь или клавиатуру.
- Нажмите кнопку **Свойства...**.

Откроется окно просмотра содержимого сертификата. В верхней части окна выводится список полей, а в нижней части – значение выделенного поля.

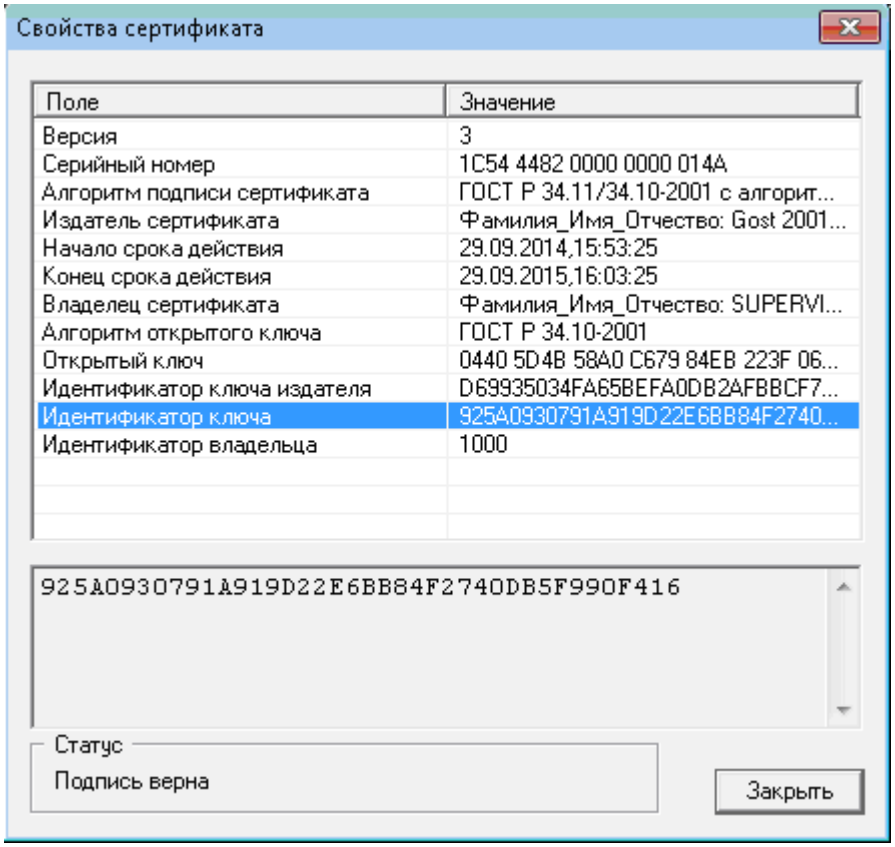

Рис. 8 – Информация о сертификате

- Кроме того, информацию о сертификате можно получить и в стандартном окне просмотра Windows. Для этого выберите сертификат в списке и воспользуйтесь командой контекстного меню **Расширенный просмотр** (см. Рис. 7).

В разделе **Статус** отображается текущее состояние и результат проверки целостности сертификата (результат проверки подписи Центра сертификации).

4.4.3. Добавление сертификатов в справочник

Для удаленных пользователей (не установлен режим **On-line**) необходимо поддерживать справочник сертификатов в актуальном состоянии, обновляя его после выпуска новых или отзыва действующих сертификатов пользователей. Обновление справочника можно производить заменой файла справочника на новый. Имеется также возможность обновления справочника, добавлением в него отдельных сертификатов.

Клиентское программное обеспечение позволяет экспортировать сертификат из справочника на клиентском компьютере в режиме **Off-line** или из базы данных в режиме **On-line**.

Для добавления сертификата в справочник:

- Нажмите кнопку **Добавить....**
- В окне **Open** (**Открыть**) задайте имя файла формата DER.

Сертификат будет добавлен в справочник.

Для экспорта сертификата из справочника:

- Выделите сертификат в списке, используя мышь или клавиатуру.
- Нажмите кнопку **Экспорт...**.
- В окне **Save as** (**Сохранить как**) задайте имя файла, в который будет экспортирован сертификат.

4.4.4. Отзыв сертификатов по инициативе пользователя

Отзыв сертификата – это процедура досрочного прекращения действия ключа. Отзыв сертификата производится в случае компрометации ключа или ограничения сроков его действия по другим причинам.

Информация об отзыве сертификата открытого ключа пользователя должна быть передана администратору безопасности согласно регламенту работы с безопасностью на предприятии (вне системы LanDocs).

После отзыва сертификата открытого ключа необходимо обновить справочник сертификатов на компьютерах удаленных пользователей. После обнаружения системой сертификата в списке отозванных сертификатов соответствующий личный ключ меняет состояние на "**Отозван**". Время окончания действия личного ключа совпадает со временем отзыва сертификата.

В системе есть возможность создать и сохранить в преднастроенной директории запрос на отзыв сертификата (см. п. 4.4.4.1).

4.4.4.1. Создание запроса на отзыв сертификата

Создание запроса на отзыв сертификатов ЭП и шифрования производится на вкладках **Сертификаты ЭП** и **Сертификаты шифрования** соответственно. Пользователь может создать запрос только на отзыв собственного сертификата.

Для создания запроса на отзыв сертификата:

- Перейдите на вкладку **Сертификаты ЭП** или **Сертификаты шифрования**.
- Выделите сертификат, подлежащий отзыву.
- Нажмите кнопку **Отозвать**.
- В окне **Запрос на отзыв сертификата ключа** в поле **Дата и время отзыва** задайте дату и время, с которого отзывается сертификат, в поле **Причина отзыва** укажите причину отзыва, выбрав из выпадающего списка.
- Нажмите кнопку **Отзыв**.

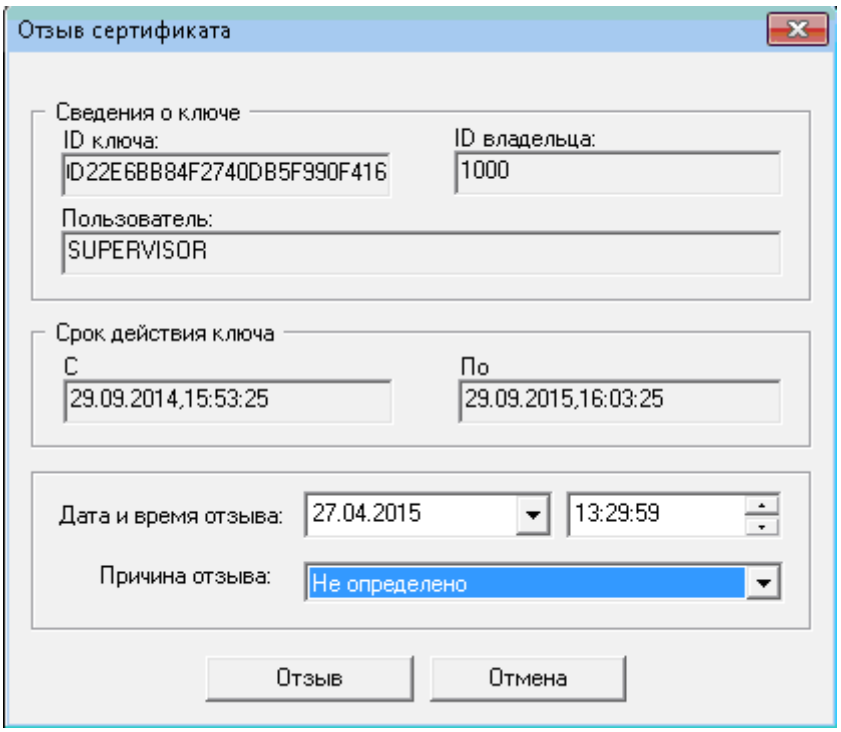

Рис. 9 – Запрос на отзыв сертификата

Запрос на отзыв сохраняется в файле с расширением REV в каталоге запросов, заданном на вкладке **Общие настройки**.

4.5. Простановка и проверка ЭП при работе в LanDocs

Действия, которые производит система LanDocs в ответ на команды пользователя, называются операциями. Результат выполнения операций сохраняется в виде записей в базе данных. Регистрация документов, создание сообщений, создание и редактирование версий документов – все это операции. Полный список операций и их свойств можно просмотреть, используя программу LanDocs: АДМИНИСТРАТОР, а подробное описание содержится в документе "LanDocs: АДМИНИСТРАТОР. Руководство администратора". С каждой операцией может быть связан объект. Объектами LanDocs являются карточки документов, сообщения, версии файлов документов, справочники. Ряд операций создают новые объекты, например операция создания нового сообщения, создает объект "сообщение", другие операции изменяют существующие объекты, так операция редактирования версии документа изменяет объект "версия документа".

Механизм применения ЭП связан с механизмом операций LanDocs. Любая операция может быть подписана ЭП пользователя, при этом подписываются данные, содержащие информацию о совершенной операции, а также связанный с операцией объект. Таким образом, при совершении операции могут создаваться две электронные подписи: подпись операции и подпись объекта.

Например, при визировании документа, создаются две подписи: ЭП операции визирования (подтверждает целостность данных, описывающих операцию) и ЭП файла версии, (подтверждает целостность файла версии документа). А при редактировании карточки

подписывается операция редактирования (данные о том кто, когда производил редактирование карточки), а также регистрационные данные, содержащиеся в карточке.

Ряд операций в LanDocs отражают выполнение делопроизводственных действий, связанных с подписанием документа. К таким операциям относятся "Подписание", "Визирование", "Согласование" и т.п. При выполнении этих операций электронная подпись является аналогом собственноручной подписи пользователя, которую он проставляет на документе при обычном (неэлектронном) делопроизводстве, такие операции называются операциями **подписания документа**.

Другие операции, такие как создание и редактирование карточки документа, редактирование справочника и т.п., не требуют обязательной подписи пользователя. Однако такие операции также могут быть настроены таким образом, что они и связанные с ними объекты будут заверяться ЭП пользователя.

Нажимая соответствующую кнопку отправки сообщения, сохраняя изменения в документе или вызывая команду выполнения операции, пользователь тем самым подтверждает подписание данных, содержащих информацию о совершенной операции, а также если есть, то и подписание связанного с операцией объекта. При этом если при выполнении операции, в ходе которой создается ЭП, не появилось сообщений об ошибках, то считается что подпись создана успешна, в противном случае выводится окно с информацией об ошибке.

Криптографическая операция подписания происходит по инициативе пользователя, когда подписывается любой документ, который доступен пользователю, автоматическое подписание происходит при отправке отчета по заданию и автоматически подписываются операции, определенные администратором.

Операция проверки ЭП операции и/или объекта выполняется по инициативе пользователя при открытии окна «Свойств…» на вкладке ЭП.

Администратор задает перечень операций, которые будут автоматически подписываться электронной подписью пользователя при их совершении. К таким операциям могут быть отнесены операции создания и редактирования карточки документа, создания и редактирования версий, редактирование справочников и другие. Подписание операций производится автоматически и не требует от пользователя дополнительных команд, кроме задания пароля доступа к своим личным ключам. Если пользователь задал режим запоминания пароля на время текущей сессии, то пароль к ключам запрашивается один раз.

При создании/проверке ЭП для отображения содержания информации в ППО «LanDocs» 3 используются следующие приложения:

В качестве средств просмотра графических изображений:

- Программа просмотра изображений и факсов для операционных систем Windows XP, Windows Vista, Windows 7, Windows 8.
  - Поддерживаемые форматы: bmp, tiff, jpeg, gif, png.
- Графический редактор Paint 5.1 (Windows XP, Windows Server 2003), 6.1 (Windows 7).
  - Поддерживаемые форматы: bmp, tiff, jpeg, gif.
- Microsoft Office Visio viewer 2010.
  - Поддерживаемые форматы: vsd.

В качестве средства просмотра (распаковки) архивов:

- Используется 7-Zip версии 9.20.
  - Поддерживаемые форматы упаковки и распаковки: 7z, zip, rar, arj.

В качестве средства просмотра документов:

- Microsoft Word 2007 (или выше).
  - Поддерживаемые форматы: odf (odt).
- Microsoft Office Excel Viewer 12.0.6424.1000;
- Microsoft Excel 2007 (или выше);
  - Поддерживаемые форматы: xlsx, xls.
- Microsoft Office Word Viewer 11.8169.8172;
- Microsoft Word 2007 (или выше);
  - Поддерживаемые форматы: doc, docx, txt, xml.
- Adobe Reader XI.
  - Поддерживаемые форматы: pdf.

Для обеспечения однозначности отображения информации в ППО «LanDocs» 3 в Приложение 1 приведен перечень дополнительных настроек данных приложений.

4.5.1. Подписание и проверка подписи документов

При совершении делопроизводственных действий, связанных с подписанием документов (подписание, визирование и т.п.), подписание выполняется по команде пользователя. При выполнении подписания пользователь задает операцию, которая определяет значение подписи (или операция уже определена в задании).

Если документ имеет несколько файлов, и каждый файл имеет несколько версий, то при подписании документа пользователь выбирает операцию и файл, который он желает подписать. При этом подписывается всегда актуальная (т. е. последняя) версия файла. После простановки ЭП версия файла документа получает атрибут **Только для чтения**.

Пользователь может проверить ЭП любой версии файла.

4.5.1.1. Подписание документа в LanDocs: УПРАВЛЕНИЕ ДОКУМЕНТАМИ

При работе в LanDocs: УПРАВЛЕНИЕ ДОКУМЕНТАМИ подписание документов производится:

- при просмотре списка документов в журнале;
- при подготовке отчета по заданию.

Пользователь имеет возможность подписать любой документ, который доступен для него при просмотре журналов.

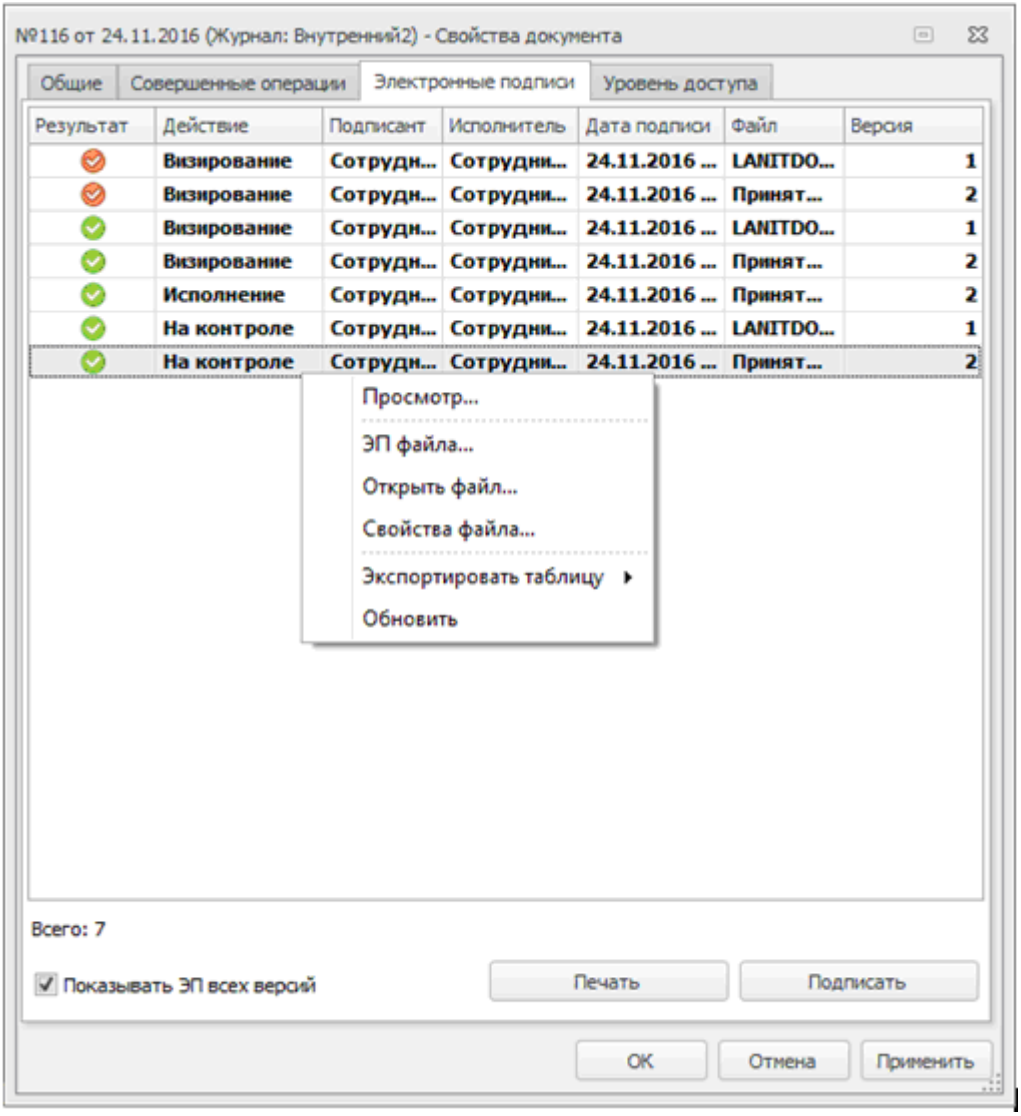

Рис. 10 – Окно операции подписания документа

Подписание документа при просмотре документов в журнале регистрации:

- Выберите журнал регистрации в левой части главного окна.
- Выделите документ в списке журнала в правой части главного окна.
- На ленточном меню нажмите кнопку **ЭП**. Откроется окно просмотра свойств документа на закладке **ЭП**.
- Нажмите кнопку **Подписать**.
- В окне **Подписание документа** (Рис. 11) в поле **Действие** выберите делопроизводственную операцию:
  - Ознакомление;
  - Подготовка;

- Визирование;
- Подписание;
- И т.п.

➢ И установите флаг у файла или нескольких файлов, для которых будут подписываться действия.

➢ Нажмите кнопку **Выполнить**. Нажимая данную кнопку, пользователь подтверждает, что подписывает данные (проставляет ЭП) – выбранную операцию и файлы документа.

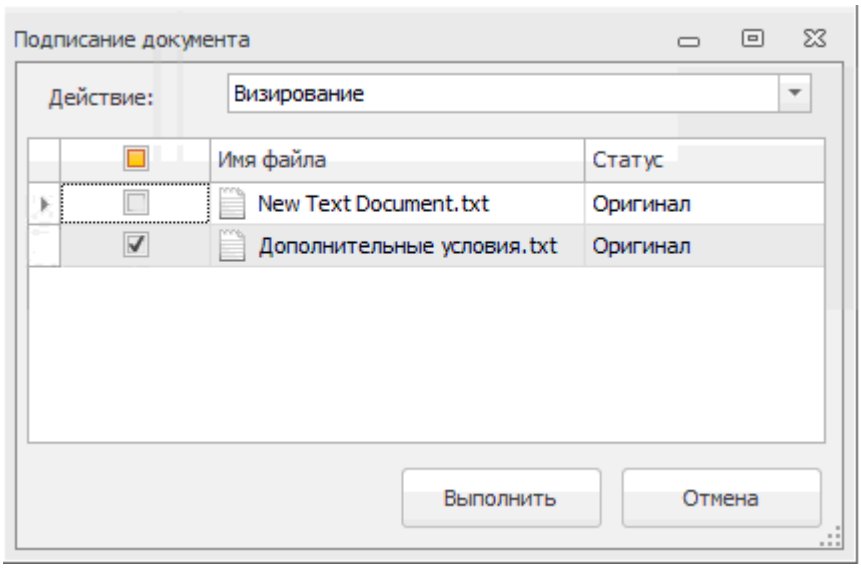

Рис. 11 – Окно подписания документа

➢ Откроется окно **Пароль доступа к личным ключам**. Введите пароль. Если ранее в этом окне была выбрана опция "Не запрашивать в дальнейшем при подписании и шифровании документов", то это окно не открывается, а сразу производится процесс подписания.

Если при подписании возникли какие–либо ситуации, например, попытка заново подписать уже подписанный файл, система выдаст соответствующее сообщение и запросит решение пользователя. При новом подписании, прежняя подпись становится недействительной, что обозначается в списке подписей специальным значком.

Если, по каким–либо причинам, при подписании возникла ошибка, откроется информационное окно с сообщением об этом.

Пользователь может также произвести выполнение делопроизводственного действия и связанного с ним подписания документа при подготовке отчета по заданию. Действие (операция), которое выполняет пользователь, определяется в задании.

В качестве примера рассмотрим отчет по заданию на визирование документа.

Визирование документа при подготовке отчета:

➢ Откройте полученное сообщение, выбрав его, в списке сообщений **Сообщения ► Входящие.**

- Нажмите кнопку ленты меню **Создать отчет**. Заполните текст отчета. При необходимости, проделайте другие операции, описаны в документации по работе с сообщениями.

- Нажмите кнопку ленточного меню **Завизировать**. Нажимая кнопку выполнения делопроизводственной операции (в данном случае одновременно и отправки отчета по заданию), пользователь подтверждает подписание данных (создание ЭП), которые отправляются в сообщении (отчете).

Наименование кнопки меню будет зависеть от типа сообщения и определенной для него делопроизводственной операции.

- Откроется (если не задействована опция "Не запрашивать в дальнейшем при подписании и шифровании документов") окно **Пароль доступа к личным ключам**. Задайте пароль.

- Окно работы с сообщением будет закрыто, а операция визирования файла (файлов) документа, прикрепленного к сообщению, будет подписана. Если при закрытии окна работы с сообщением не появилось сообщений об ошибках, то подпись создана успешна.

4.5.1.2. Проверка ЭП документа в LanDocs: УПРАВЛЕНИЕ ДОКУМЕНТАМИ

Проверка ЭП документов производится при просмотре списка документов в журнале.

Для проверки ЭП документа:

- Выберите журнал и выделите документ в списке.

- На ленточном меню нажмите кнопку **ЭП**. Откроется окно просмотра свойств документа на закладке **Электронные подписи**. В этом окне отображаются учетные реквизиты подписей (действие, файл, кто и когда подписал), а также результат проверки уже имеющихся подписей.

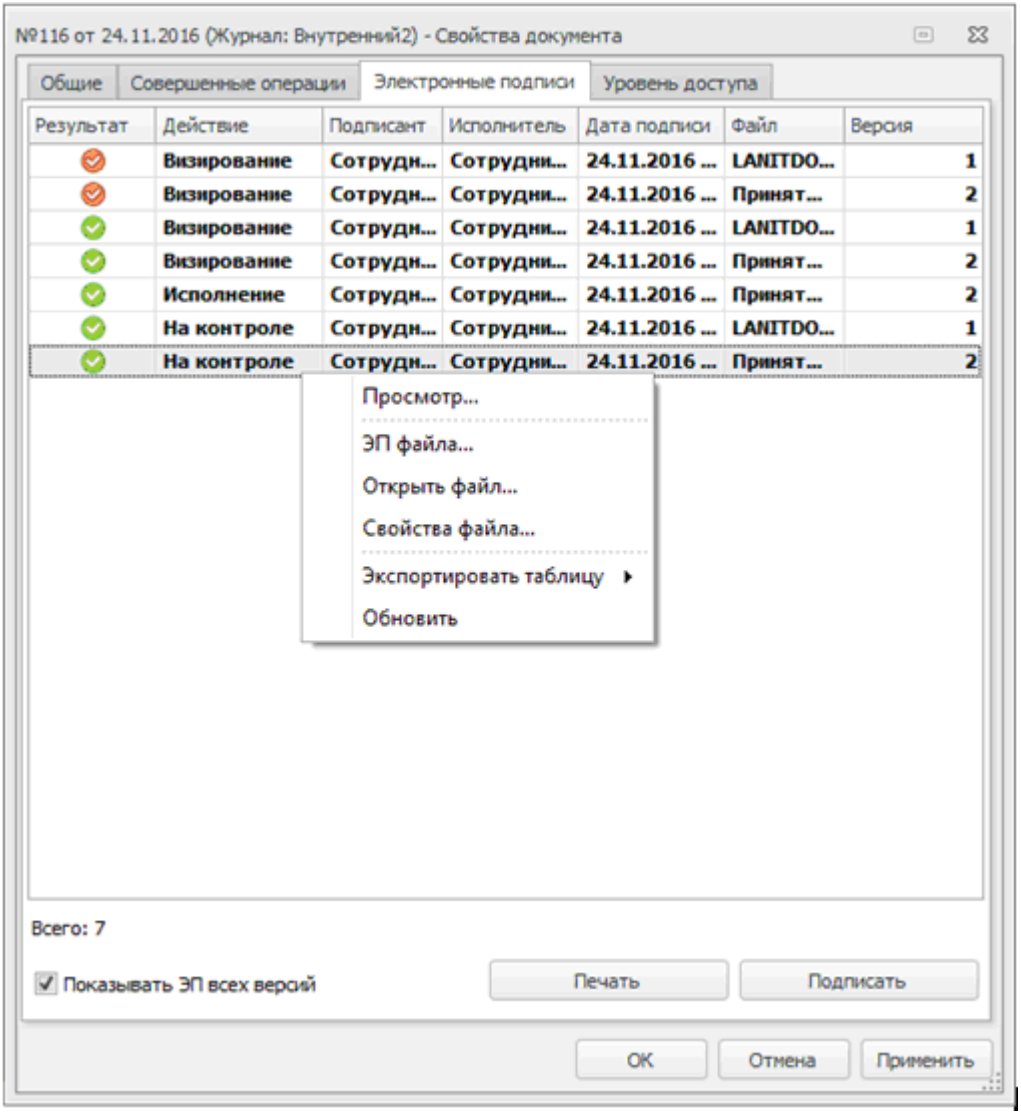

Рис. 12 – Окно отображения результатов проверки ЭП документа

Пользователю предоставляется возможность вывести ЭП всех версий, для этого выставляется флаг **Показывать ЭП всех версий**.

Для просмотра ЭП файла:

- В окне просмотра и редактирования документа перейдите на закладку **Файлы**.
- Укажите интересующий вас файл и нажмите кнопку **ЭП** на ленте меню или выберите одноименный пункт из контекстного меню.
- Откроется окно просмотра свойств файла на закладке **Электронные подписи** (Рис. 13), где представлена информация о подписании файла (актуальной версии). Установка флажка **Показывать ЭП всех версий** позволяет отобразить ЭП предыдущих версий файла.

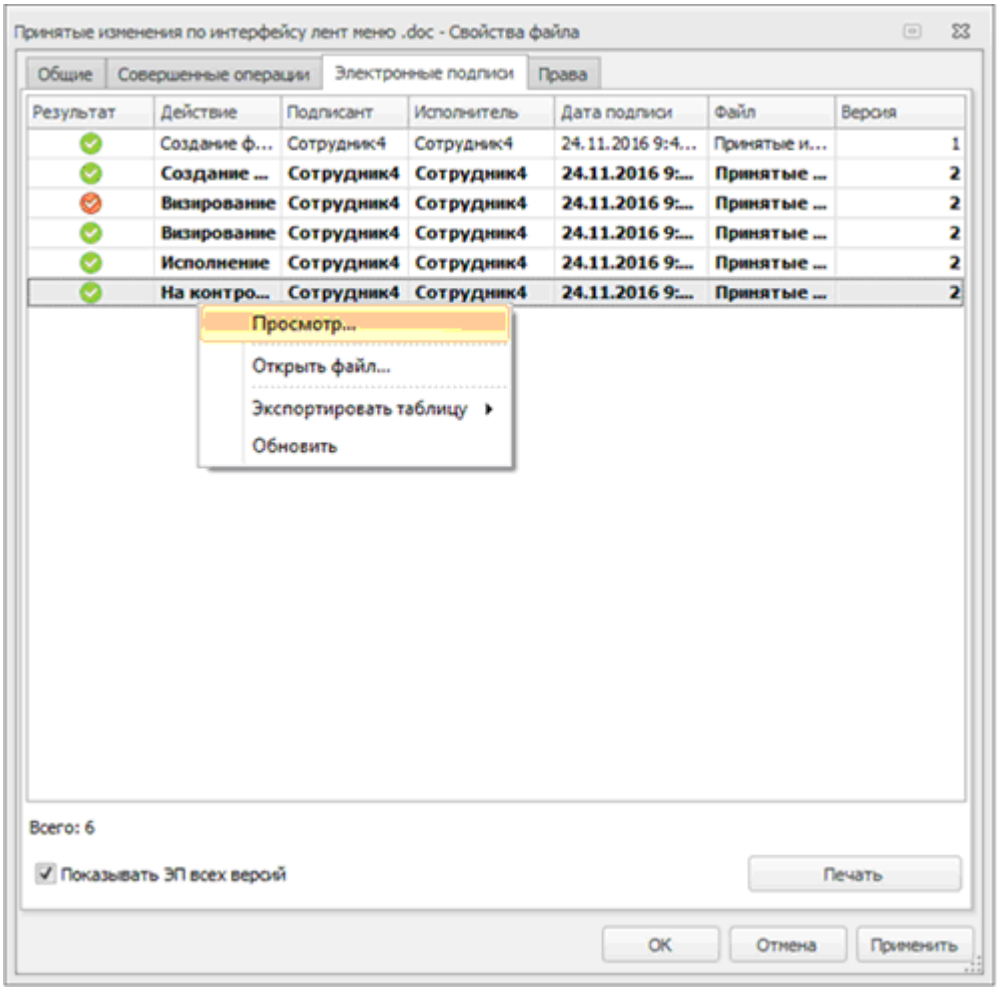

Рис. 13 – Информация об электронных подписях файла

При выборе пункта контекстного меню **Открыть файл…** открывается в режиме просмотра указанная версия файла.

Вывод на печать текста файла с проставленными подписями осуществляется по нажатию кнопки **Печать**. На печать выводятся только подписи в состоянии «***Верна***».

Для экспорта таблицы выберите одноименный пункт контекстного меню, а для получения подробной информации о подписи файла (Рис. 14) – пункт **Просмотр…**

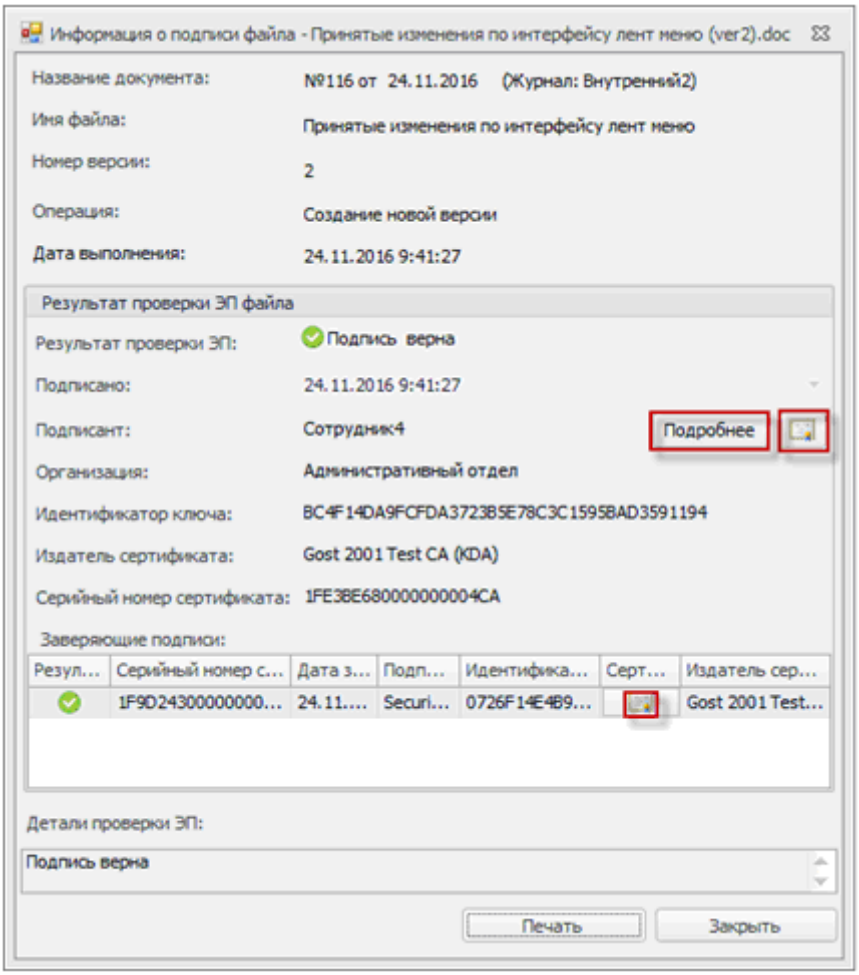

Рис. 14 – Подробная информация об ЭП файла

В окне информации об ЭП файла помимо общей информации о файле выведен результат проверки ЭП и таблица заверяющих подписей. При нажатии на иконку «Сертификат» (Рис. 14) отображается окно сертификата пользователя, а по нажатию кнопки **Подробнее** выводится краткая информация о сотруднике.

Вывести в MS Word детальную информацию о подписи файла можно, нажав кнопку **Печать**.

Окно с информацией о заверяющих подписях вызывается по команде контекстного меню **Просмотр** (курсор мыши для вызова контекстного меню должен находиться в области таблицы заверяющих подписей).

4.5.2. ЭП сообщений LanDocs

Система LanDocs может быть сконфигурирована таким образом, что все сообщения системы (извещения, задания, отчеты и т.д.) будут подписываться ЭП пользователя. Настройку режима подписания сообщений производит администратор системы. Подписание сообщений производится автоматически и не требует от пользователя дополнительных команд, кроме задания пароля доступа к своим личным ключам. Нажимая соответствующую кнопку отправки сообщения, пользователь подтверждает подписание данных, которые отправляются в сообщении. Если пользователь задал режим запоминания пароля на время

текущей сессии, то пароль запрашивается только один раз. Электронной подписью пользователя заверяется операция создания сообщения, а также его содержание.

4.5.2.1. Проверка ЭП сообщений в LanDocs: УПРАВЛЕНИЕ ДОКУМЕНТАМИ

Для проверки ЭП сообщения:

- В списке сообщений укажите интересующее вас сообщение и на ленте меню нажмите кнопку **ЭП**

или

- в окне просмотра сообщения нажмите на ленте меню кнопку **ЭП…**

Откроется окно, содержащее информацию об ЭП сообщения (Рис. 15).

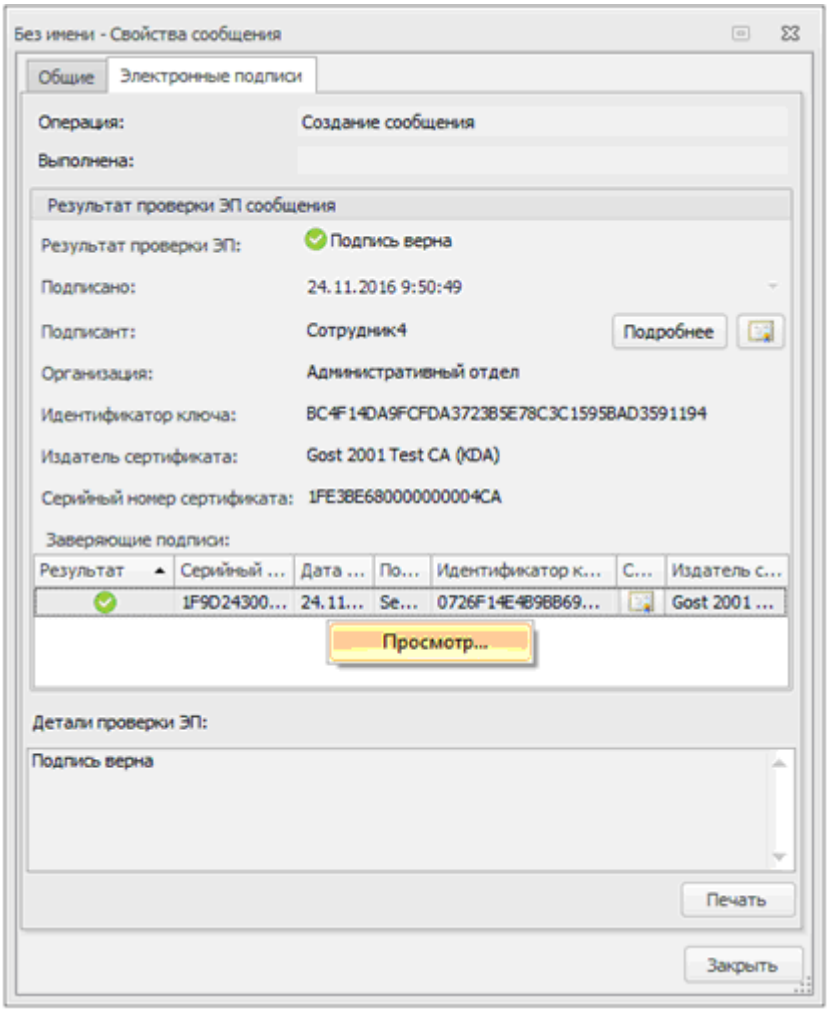

Рис. 15 – Информация об ЭП сообщения

Пиктограммы результатов проверки ЭП сообщения аналогично ЭП документа.

При нажатии на иконку «Сертификат» в таблице заверяющих подписей или у поля **Подписант** выводится окно сертификата пользователя. По нажатию кнопки **Подробнее** выводится краткая информация о сотруднике.

Если сообщение было подписано, то по кнопке **Печать** выводится информация об ЭП сообщения.

Выберите пункт контекстного меню **Просмотр** (курсор мыши для вызова контекстного меню должен находиться в области таблицы заверяющих подписей) откроется окно заверяющей подписи, где выводится подробная информация о заверяющей электронной подписи и результат проверки. При нажатии кнопки **Печать** результат проверки заверяющей ЭП выводится в MS Word для дальнейшей печати.

4.5.3. ЭП операции и совершенные операции по документу

Информация о действиях, совершенных с документом, представлена на закладке **Совершенные операции** окна просмотра свойств документа.

В таблице **События по документу** отображаются следующие сведения:

- **Результат** – пиктограмма, соответствующая результату завершения операции (успешно/неуспешно/выполняется и т.д.);
- **Операция** – название операции;
- **Начало выполнения** – дата и время начала выполнения операции;
- **Окончание выполнения** – дата и время окончания выполнения операции.
- **Имя исполнителя** – ФИО пользователя, выполнявшего операцию;
- **Физический пользователь** – ФИО фактического пользователя;

Нажатие кнопки **Проверить подпись** на закладке **Совершенные операции** позволяет произвести проверку ЭП операции, выделенной в списке.

Результат проверки ЭП операции выводится в отдельном окне (Рис. 16) и представлен следующими атрибутами:

- **Операция** – наименование (физическое название в базе данных) операции, которая была выполнена с документом;
- **Дата выполнения** – дата совершения операции;
- **Результат проверки ЭП** – результат проверки подписи (пиктограммы результатов проверки ЭП операции аналогично ЭП документа);
- **Подписана** – дата и время проставления ЭП;
- **Подписант** – имя пользователя, совершившего операцию или ФИО подписанта/ название организации, от имени которой создана подпись.

- **Организация** – название организации сотрудника или физического лица, создавшего подпись.
- **Идентификатор ключа** – идентификатор ключа пользователя, проставившего ЭП.
- **Издатель сертификата, Серийный номер сертификата** – информация по издателю сертификата подписанта и серийный номер сертификата подписанта.
- **Заверяющие подписи** – таблица с информацией о заверяющих подписях;
- **Результат проверки ЭП связанных объектов** – информация о связанных объектах и результатах проверки ЭП;
- **Детали проверки ЭП** – подробная информация об операции проверки подписи

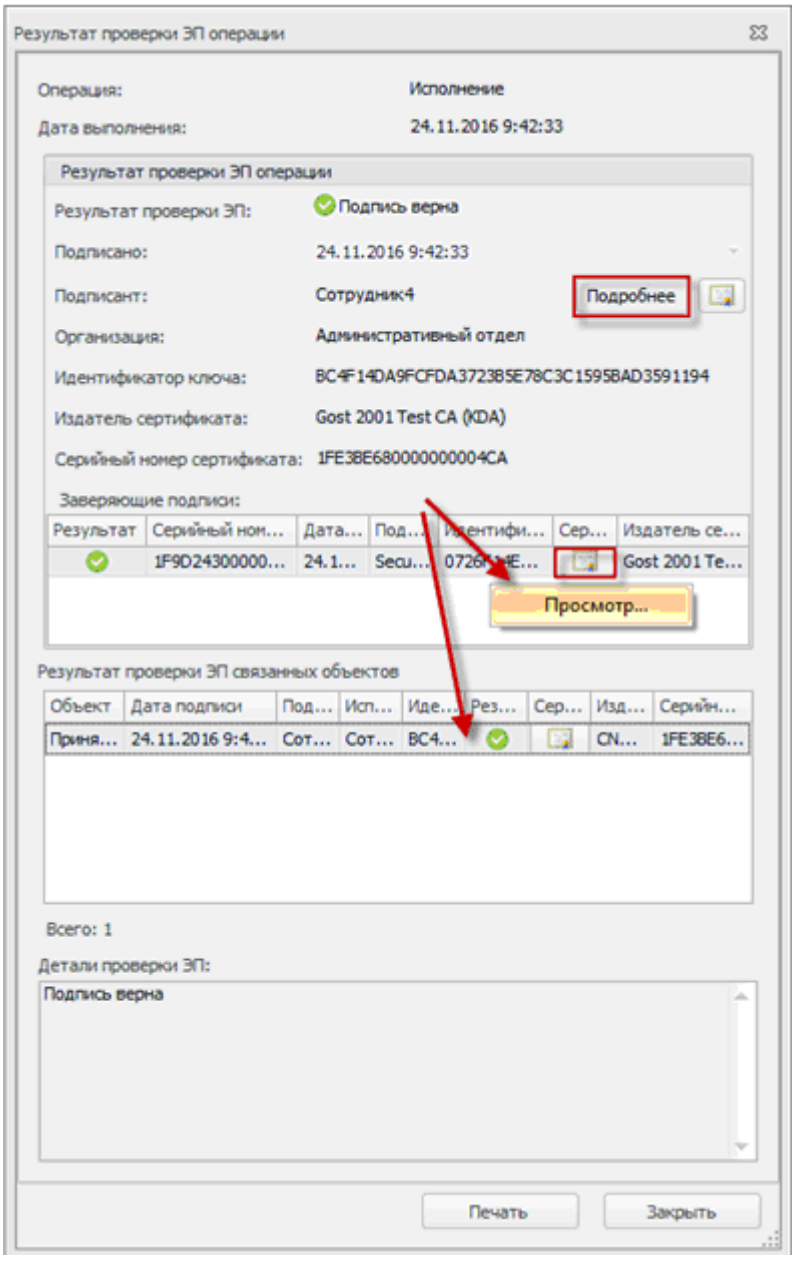

Рис. 16 – Результат проверки ЭП операции

При нажатии на иконку «Сертификат» в таблицах заверяющих подписей, связанных объектов или у поля **Подписант** выводится окно сертификата пользователя. Сертификаты могут иметь следующие статусы: сертификат действует, сертификат отозван, истек срок действия сертификата. При нажатии кнопки **Подробнее**, при внутренней подписи выводится краткая информации о сотруднике[1], а при внешней подписи – краткая информация о внешнем подписанте.

Для вывода MS Word информации об ЭП события нажмите кнопку **Печать**.

Выберите пункт контекстного меню **Просмотр** (курсор мыши для вызова контекстного меню должен находиться в области таблицы заверяющих подписей) откроется окно заверяющей подписи (Рис. 17).

При выполнении аналогичного действия, но из области связанных объектов откроется окно информации о подписи объекта (например, о подписи файла).

В окне заверяющей подписи выводится подробная информация о заверяющей электронной подписи и результат проверки. При нажатии кнопки **Печать** результат проверки заверяющей ЭП выводится в MS Word для дальнейшей печати.

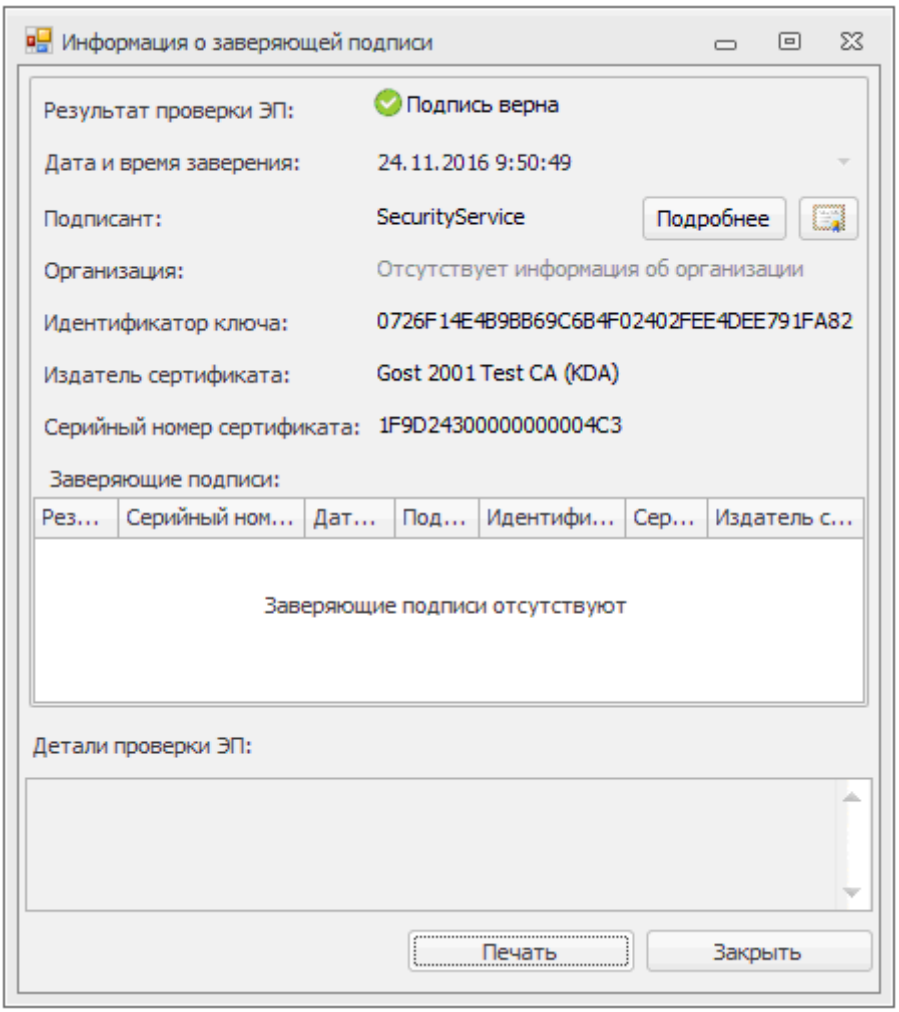

Рис. 17 – Окно заверяющей подписи

[1] Из справочника «Сотрудники»

4.6. Шифрование конфиденциальных документов

Шифрование файлов версий производится автоматически для всех документов с категорией доступа "Конфиденциальный". Шифрование производится прозрачно для пользователя, без задания дополнительных команд. Все версии конфиденциальных документов передаются по каналам связи и хранятся на сервере в шифрованном виде.

Шифрование файла производится индивидуально для каждого пользователя, имеющего доступ к документу. Для того чтобы пользователь мог быть включен в список лиц, имеющих доступ к конфиденциальному документу, он должен иметь действующий сертификат шифрования.

Дешифрование конфиденциального документа производится с использованием личного ключа шифрования пользователя, для которого документ был шифрован. Для доступа к конфиденциальному документу пользователь должен задать пароль контейнера личных ключей. По умолчанию пароль задается каждый раз при открытии шифрованного документа. Пользователь может установить режим запоминания пароля на время текущей сессии LanDocs.

Установка для документа категории доступа "Конфиденциальный" производится при регистрации документа или редактировании карточки существующего документа до присоединения файла документа.

Криптографическая операция шифрования происходит при добавлении файла в конфиденциальный документ, а при внесении изменений в конфиденциальный документ происходит перезашифрование. Подробнее о добавлении и редактировании файла см. "LD3 Работа с документами".

Операция расшифрования производится при открытии документа для просмотра и редактирования. Расшифровать конфиденциальный документ могут только пользователи, которым определен доступ к документу.

Информация, связанная с уровнем доступа, отражается на закладке **Уровень доступа** (Рис. 18) окна просмотра свойств документа.

Для задания конфиденциального уровня доступа

- В поле **Уровень доступа** выберите из раскрывающегося списка требуемое значение.

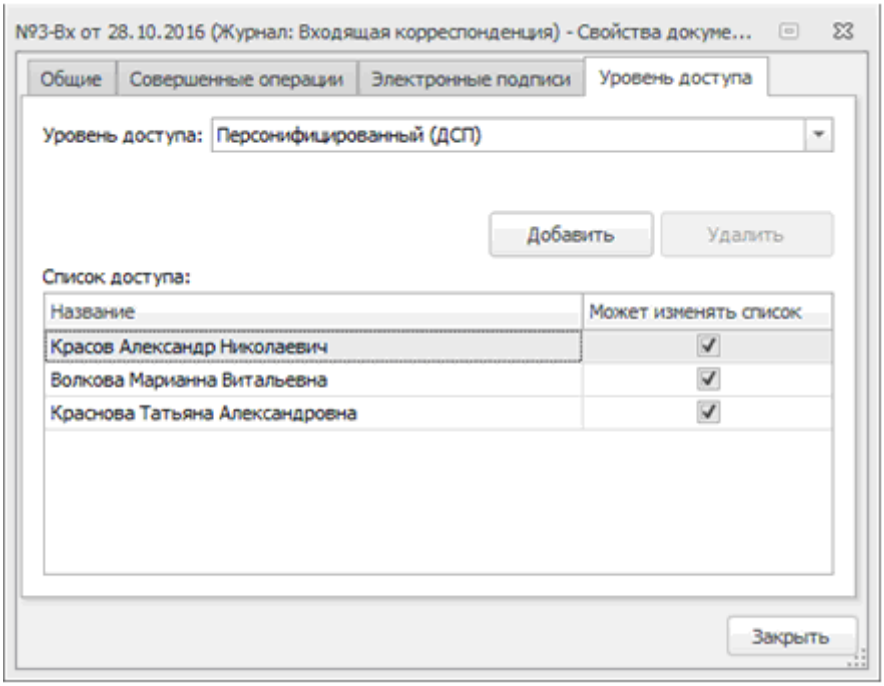

Рис. 18 – Окно просмотра свойств документа. Закладка Уровень доступа

При выборе значения ***Конфиденциальный*** необходимо указать, кому из сотрудников будет доступен данный документ, т.е. сформировать список доступа.

Для формирования списка конфиденциального доступа:

- Нажмите кнопку **Добавить**. Откроется окно **Назначение доступа**.
- Задайте пользователей, имеющих доступ к документу и их права на редактирование списка доступа.
- Нажмите кнопку **Выбрать**.

Подробнее о регистрации документов см. "LanDocs: УПРАВЛЕНИЕ ДОКУМЕНТАМИ. Часть II. Работа с документами".

Приложение 1. Дополнительные настройки приложений

Для Microsoft Word 2007 (и выше):

- Нажмите кнопку главного меню  , затем кнопку **Параметры Word** (Рис. 19).

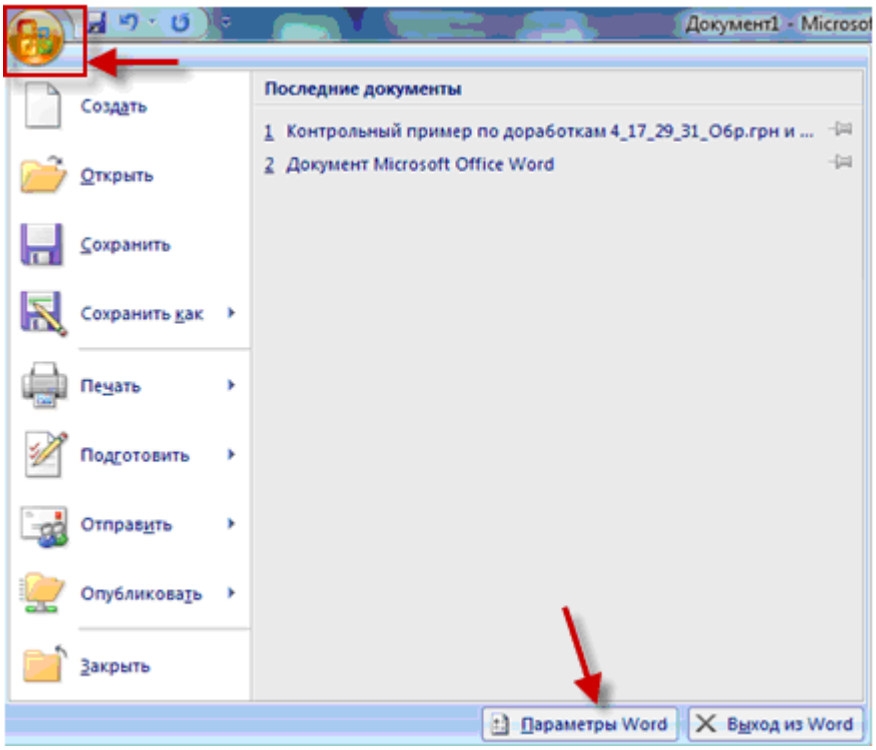

Рис. 19 – Выбор настроек Word

- На вкладке **Экран** и **Дополнительно** установите параметры, выделенные красными рамками, в соответствии с Рис. 20 и Рис. 21 и нажмите **ОК**.

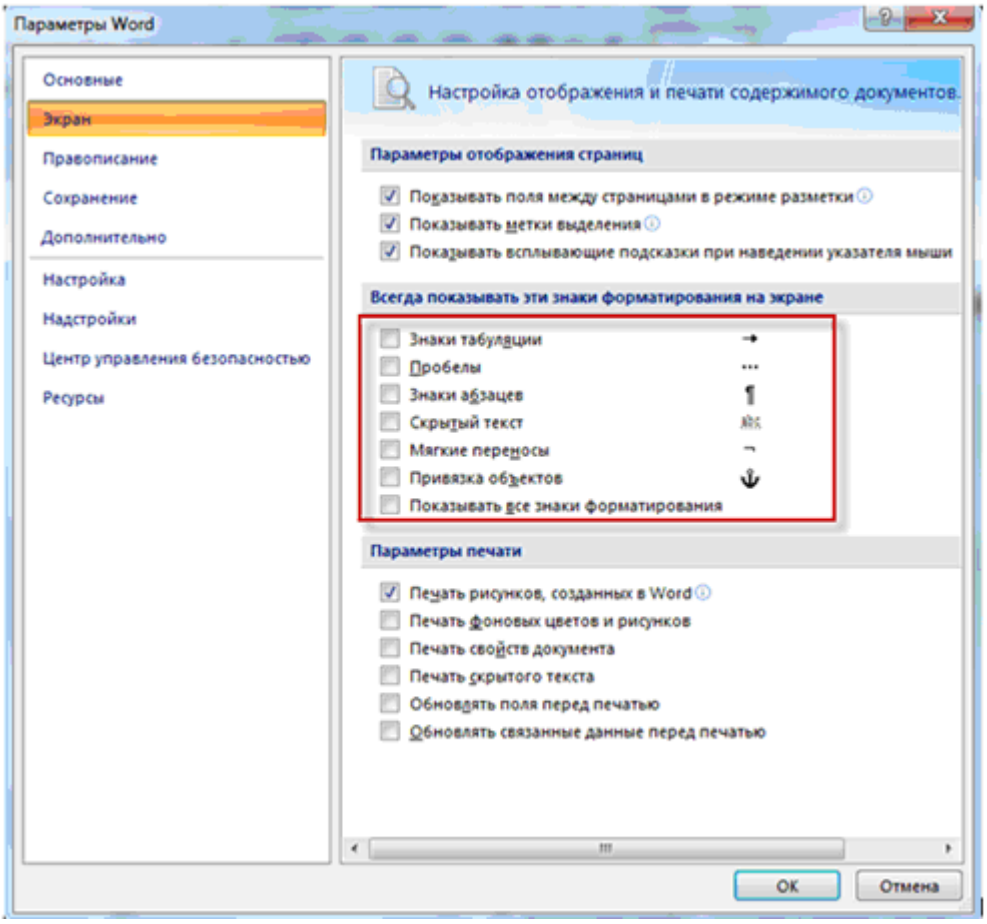

Рис. 20 – Вкладка Экран

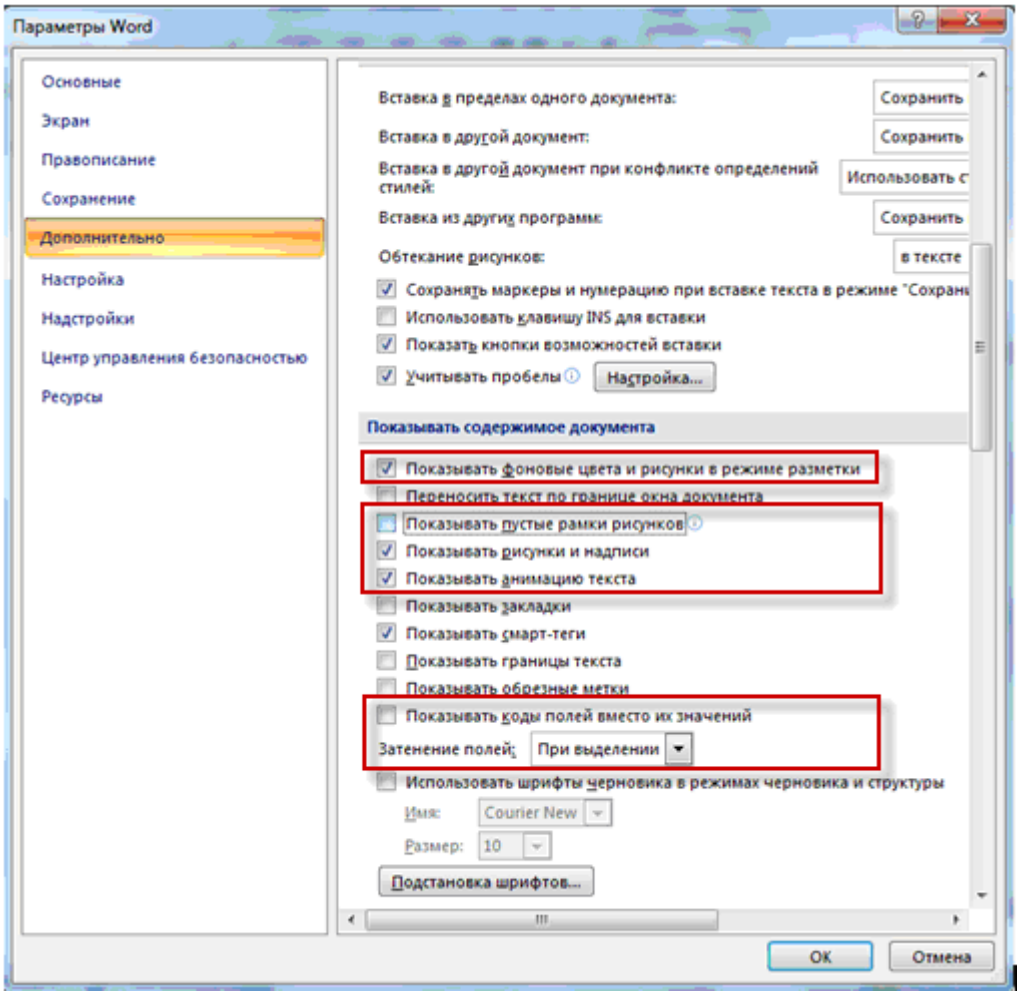

Рис. 21 – Вкладка Дополнительно

Microsoft Office Word Viewer 11.8169.8172:

- В главном меню программы выберите команду **Сервис**, затем **Параметры** (Рис. 22).

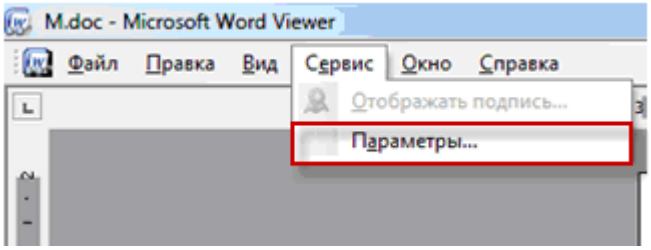

Рис. 22 – Выбор настроек Word Viewer

- В окне Параметры перейдите на вкладку **Вид** и установите параметры, выделенные красными рамками, в соответствии с Рис. 23 .

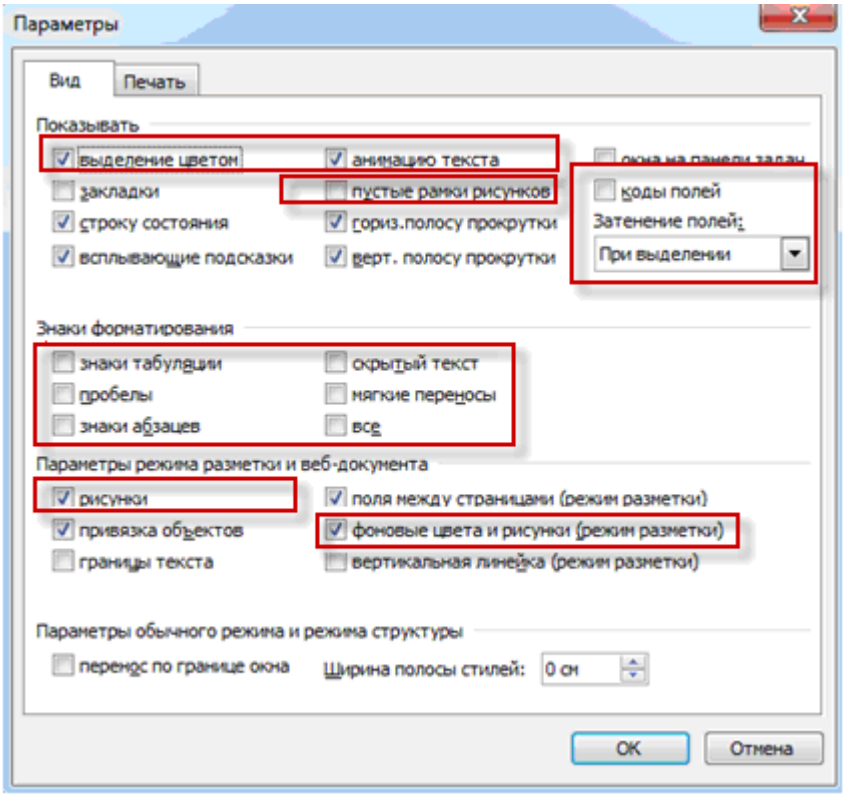

Рис. 23 – Вкладка Вид

Microsoft Microsoft Excel 2007 (или выше) и Microsoft Office Excel Viewer 12.0.6424.1000:

- Нажмите кнопку главного меню  , затем кнопку **Параметры Excel**

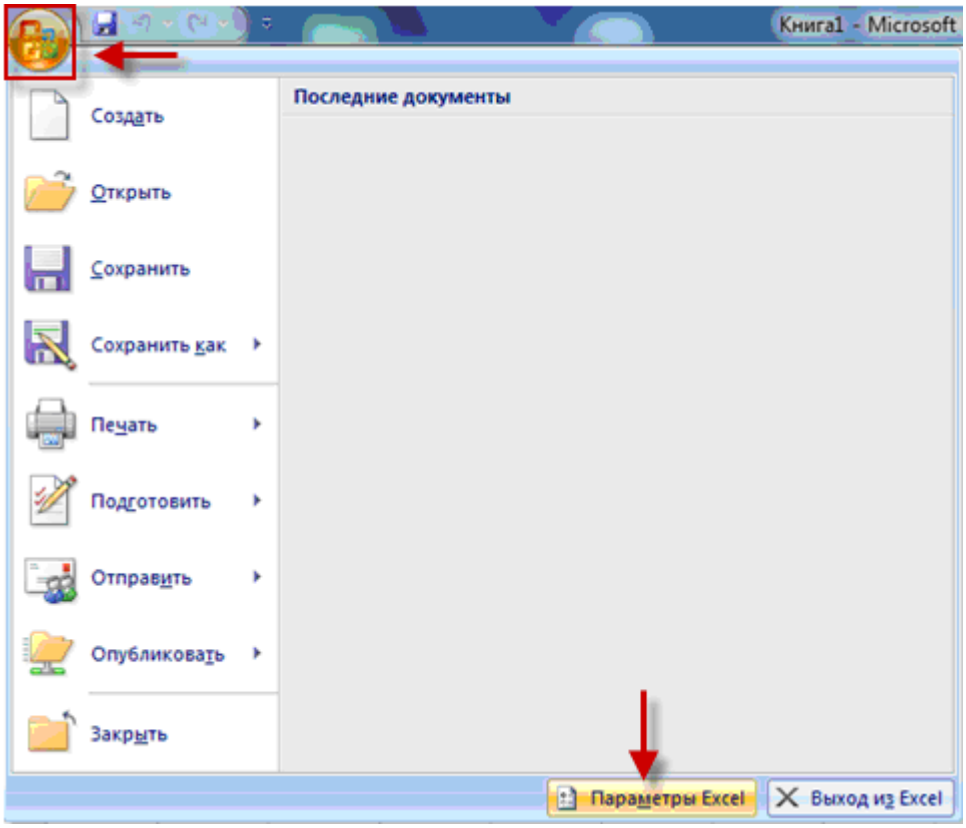

Рис. 24 – Выбор настроек Excel

- На вкладке **Дополнительно** установите параметры, выделенные красными рамками, в соответствии с Рис. 25 и нажмите **ОК**.

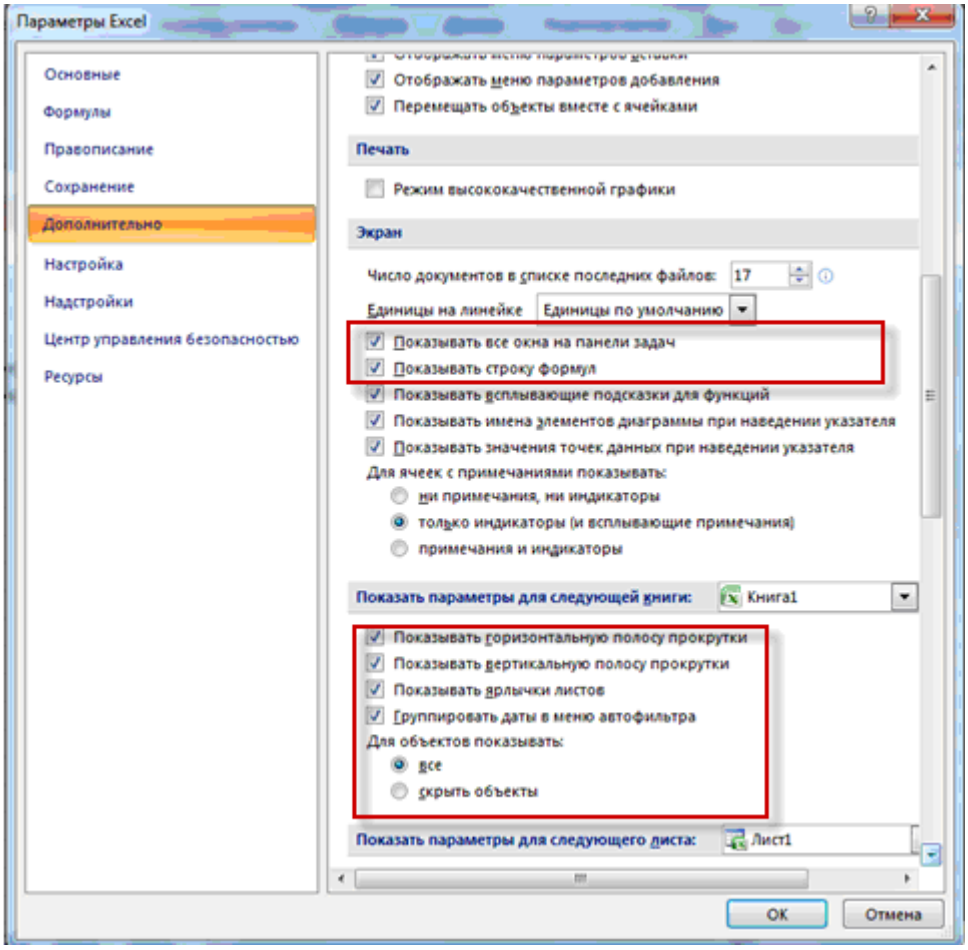

Рис. 25 – Вкладка Дополнительно (Excel)

Adobe Reader XI:

- В главном меню программы выберите команду **Редактирование**, затем **Установки…**

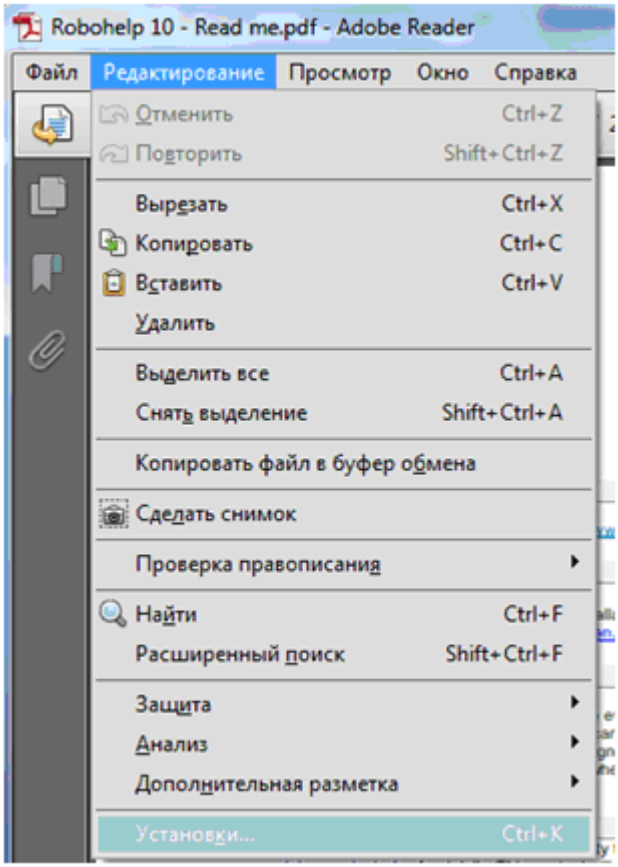

Рис. 26 – Выбор настроек Adobe Reader

- В окне Установки выберите категорию **Вид страницы** и установите параметры, выделенные красными рамками, в соответствии с Рис. 27.

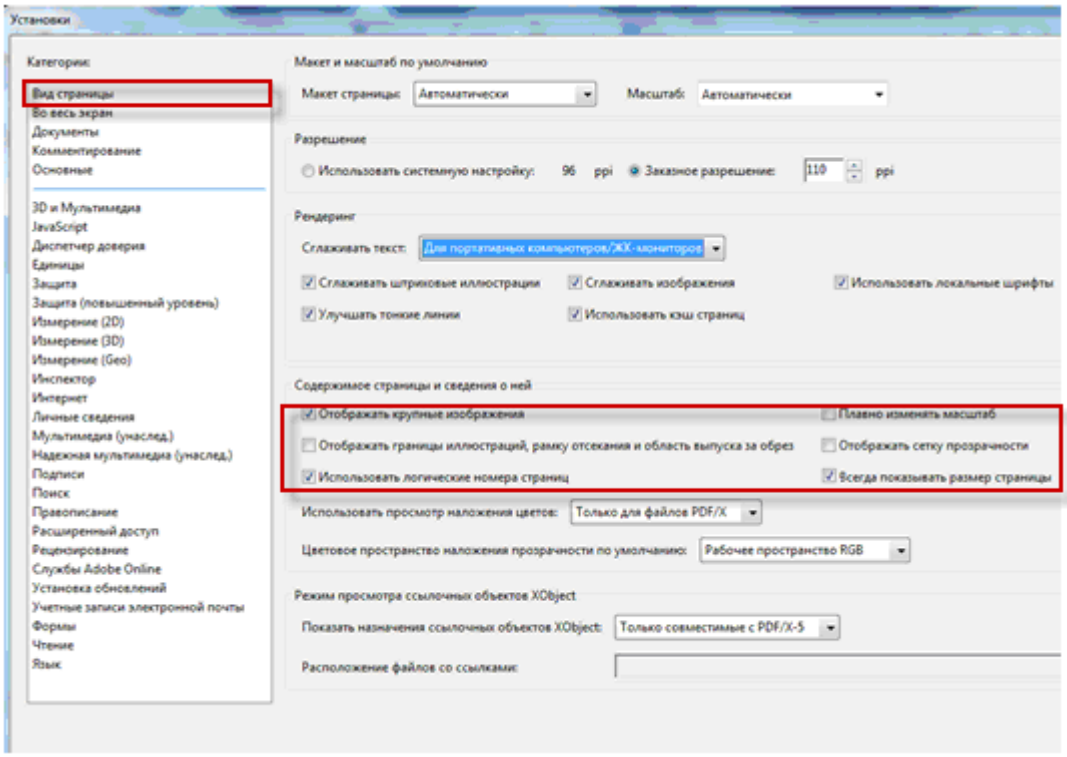

Рис. 27 – Окно «Установки»