Программный модуль «Применение ЭП в АС «Бюджет» и АС «УРМ»

НПО «Криста» 2016

Содержание

1. Общая информация о подсистеме криптографии в АС «Бюджет» и АС «УРМ» ... 3
1.1. Назначение ... 3
1.2. Цели внедрения ... 3
1.3. Функциональные возможности ... 3
1.4. Отличительные особенности ... 4
1.5. Требования к программным и аппаратным средствам ... 4
2. Принципы реализации ЭП в АС «Бюджет» и АС «УРМ» ... 5
2.1. Что такое ЭП? ... 5
2.2. Основные термины и понятия, связанные с ЭП ... 7
2.3. Использование СКЗИ «КриптоПро CSP» для защиты информации ... 9
2.4. Взаимосвязь системы состояний и ЭП ... 11
2.5. Организация хранения документов с ЭП ... 12
2.6. Процедура наложения ЭП на электронный документ ... 14
2.7. Процедура проверки подлинности ЭП электронного документа ... 14
2.8. Выгрузка информации из хранилища подписанных документов в файловую систему ... 16
3. Архитектура подсистемы криптографии АС «Бюджет» и АС «УРМ» ... 16
3.1. Режимы работы подсистемы криптографии ... 16
3.2. Crypto API СКЗИ «КриптоПро CSP» ... 17
3.3. Открытие, закрытие и типы криптопровайдеров «КриптоПро CSP» ... 17
3.4. Установка и связывание сертификатов с ключевым носителем ... 17
3.5. Корневые сертификаты ... 20
3.6. Ограничения на структуру используемых удостоверяющих центров ... 20
3.7. Схема хранения сертификатов и списков отзыва ... 20
4. Установка и настройка СКЗИ «КриптоПро CSP» ... 21
5. Установка и настройка модулей АС «Бюджет», обеспечивающих работу с ЭП ... 21
5.1. Состав модулей ... 21
5.2. Общий алгоритм установки и настройки ... 21
5.3. Настройка диспетчера подсистемы криптографии (файл DSign.ini) ... 22
5.4. Настройки подключения к хранилищу данных ЭП ... 23
5.5. Настройка АС «Бюджет» для работы с ЭП ... 24
6. Установка и настройка модулей АС «УРМ», обеспечивающих работу с ЭП ... 30
6.1. Состав модулей ... 30
6.2. Общий алгоритм установки и настройки ... 30
6.3. Настройка сервера обмена данными для работы с ЭП ... 30
6.4. Настройка клиента АС «УРМ» для работы с ЭП ... 32
6.5. Настройка механизма штампов времени ... 33
6.6. Настройка OCSP ... 34
6.7. Настройка клиента АС «УРМ» для работы с множественной ЭП ... 36
7. Работа с ЭП при передаче электронных документов из АС «УРМ» в АС «Бюджет» ... 37
7.1. Наложение ЭП в АС «УРМ» ... 37
7.2. Проверка корректности ЭП при передаче электронных документов из АС «УРМ» в АС «Бюджет» ... 38
7.3. Особенности передачи документов с ЭП при наличии ПМ «Конвейерная обработка и множественное визирование документов» ... 39
7.4. Возможные ошибки при работе с ЭП в АС «УРМ» ... 39
8. Работа пользователя с ЭП в АС «Бюджет» при совместном использовании с ПМ «Конвейерная обработка и множественное визирование документов» ... 40
8.1. Инструменты для работы с ЭП в АС «Бюджет» ... 40
8.2. Наложение электронной подписи в АС «Бюджет» ... 40
8.3. Просмотр истории изменения состояний документа и наложения ЭП в АС «Бюджет» ... 41
8.4. Проверка корректности электронной подписи в АС «Бюджет» ... 43
9. Возможности совместного использования с ПМ «Прикрепление к документам произвольных файлов с ЭП» ... 45
10. Возможности совместного использования с ПМ «Передача выписок с ЭП из АС «Бюджет» в АС «УРМ» 50
11. Утилита для работы администратора с хранилищем документов с ЭП (AdminSign.exe) ... 52
11.1. Запуск утилиты AdminSign.exe ... 53
11.2. Вид окна утилиты ... 53
11.3. Функциональные возможности ... 56

12. Список сокращений 61

1. Общая информация о подсистеме криптографии в АС «Бюджет» и АС «УРМ»

1.1. Назначение

ПМ «Применение ЭП в АС «Бюджет» и АС «УРМ» дает возможность использования средств ЭП при передаче электронных документов от ТПФО, ГРБС, РБС и ПБС в финансовый орган посредством АС «УРМ», а также предоставляет базовый функционал для внедрения ЭП на различных участках системы электронного документооборота, реализуемых дополнительными программными модулями.

1.2. Цели внедрения

- Интеграция системы электронного документооборота с финансово-учетной системой исполнения бюджета путем обеспечения юридической значимости электронных документов, передаваемых от удаленных клиентов и во внутреннем документообороте ФО, в том числе виз и других отметок на электронных документах.
- Защита передаваемой информации от подмены и искажения.
- Сокращение расходов на формирование, доставку и обработку бумажных документов.
- Значительное снижение временных затрат на доставку документов от удаленных клиентов, а также при согласовании и утверждении документов специалистами ФО, что ускоряет процессы исполнения бюджета в целом.

1.3. Функциональные возможности

- Наложение ЭП на электронные документы при передаче из АС «УРМ» в АС «Бюджет».
- Наложение ЭП при прохождении электронными документами определенных этапов обработки, которые могут быть заданы на различных участках маршрута документов: как между пользователями АС «Бюджет», так и между АС «УРМ» и АС «Бюджет»[*].
- Невозможность отправки документов из АС «УРМ» или передачи по маршруту в АС «Бюджет», если прохождение этапа требует наложение ЭП, но она не установлена или не верна[*].
- Проверка корректности ЭП электронных документов и автоматическое отклонение документа, в случае несанкционированного изменения его атрибутов или некорректности ЭП при передаче документов из АС «УРМ».
- Автоматическая проверка документов и блокировка от дальнейшей передачи по маршруту в АС «Бюджет» при несанкционированном изменении его атрибутов или некорректности ЭП[*].
- Возможность просмотра и выгрузки в файл подписанных электронных документов.

[*] При совместном использовании с ПМ «Конвейерная обработка и множественное визирование документов»

1.4. Отличительные особенности

- Интегрируется в систему электронного документооборота между ФО и удаленными клиентами, дополняя ее средством передачи заверенных ЭП документов из АС «УРМ» в АС «Бюджет».
- Является фундаментом для построения системы защищенного документооборота между финансовым органом и удаленными клиентами и обеспечивает внедрение средств ЭП:
  - на этапе согласования документов – при совместном использовании с ПМ «Конвейерная обработка и множественное визирование документов»;
  - на этапе представления подтверждающих документов в финансовый орган – при совместном использовании с ПМ «Прикрепление к документам произвольных файлов с ЭП»;
  - на этапе выдачи выписок и проведенных первичных документов – при совместном использовании с ПМ «Передача выписок с ЭП из АС «Бюджет» в АС «УРМ».
- Электронные документы в xml-формате, ЭП и служебные данные подписанного документа сохраняются в специальном хранилище подписанных документов финансового органа, которое представляет собой отдельную базу данных.
- На один документ в процессе его обработки может быть наложено несколько ЭП, при этом сохраняются все подписи, наложенные на документ.
- Используется только сертифицированное ФСБ СКЗИ.
- Полностью совместим с российским криптопровайдером «КриптоПро CSP», возможно использование СКЗИ других производителей.
- НПО «Криста» имеет все необходимые лицензии Центра по лицензированию, сертификации и защите государственной тайны ФСБ России.
- Возможность использования различных ключевых носителей: дискеты 3,5” (1,44 MB), смарт-карты, USB-ключи.

1.5. Требования к программным и аппаратным средствам

❖ **База данных для хранения документов с ЭП**

- СУБД: Oracle – версия 11.2.0.3 и выше, FireBird 2.1.x, 2.5.x и выше;
- Программное обеспечение СКЗИ «КриптоПро CSP» версии 3.6 и старше.

❖ **СКЗИ «КриптоПро CSP» функционирует в следующих операционных системах (ОС):**

- Windows XP;
- Windows Vista;
- Windows 7;
- Windows 8.

2. Принципы реализации ЭП в АС «Бюджет» и АС «УРМ»

2.1. Что такое ЭП?

При электронной передаче данных как от внешней организации в финансовый орган и обратно, так и внутри ФО, необходимо обеспечить защиту передаваемых данных от искажения. Для такой защиты производится дополнительная обработка данных – наложение и проверка электронной подписи.

Электронная подпись (ЭП/ЭЦП) – реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки и полученный в результате криптографического преобразования информации с использованием закрытого (секретного) ключа ЭП. ЭП позволяет идентифицировать владельца подписи, а также установить отсутствие искажений информации в электронном документе.

Практическая невозможность подделки электронной подписи опирается на очень большой объем определенных математических вычислений, необходимых для раскрытия закрытого ключа на основе открытой информации.

Наложение подписи на документ не изменяет самого документа, но дает возможность проверить его подлинность и авторство. ЭП обладает свойствами неотрекаемости, благодаря чему лицо, наложившее ЭП, не может от нее отказаться при разрешении спорных вопросов.

Проверка электронной подписи блока открытой информации производится с помощью криптографического преобразования и открытого ключа, соответствующего закрытому ключу, участвовавшему в процессе наложения ЭП.

Закрытый ключ подписи используется для выработки электронной подписи. Для проверки подписи проверяющий должен располагать открытым ключом (сертификатом) пользователя, поставившего подпись. Проверяющий должен быть полностью уверен в подлинности открытого ключа, в частности в том, что имеющийся у него открытый ключ соответствует открытому ключу конкретного пользователя. Для этой цели используется сертификат открытого ключа, подписанный третьей доверенной стороной. Каждому пользователю, обладающему правом подписи, необходимо иметь:

- для наложения подписи – закрытый ключ подписи; выдается индивидуально и является секретным;
- для проверки подписей – открытые ключи подписей (сертификаты открытых ключей) других пользователей, доступные публично.

При использовании открытого ключа должна быть обеспечена его целостность и неизменность. Это может быть реализовано:

- путем заверения открытого ключа ЭП доверенной стороной (например, в случае использования сертификатов открытых ключей);
- путем доверенного распространения и хранения открытых ключей в виде справочников.

При использовании сертификатов открытых ключей, заверенных подписью доверенной стороны, должна быть обеспечена безопасная доставка и хранение корневого сертификата – открытого ключа доверенной стороны, с использованием которого проверяются остальные сертификаты открытых ключей пользователей.

Иногда возникает необходимость в отзыве ключей (прекращении использования ключей по причинам ухода сотрудника из организации, компрометации ключа, изменения атрибутов владельца ключа и тому подобное). При этом, если ключ используется для обмена информацией между двумя сторонами, то достаточно информировать вторую сторону о

прекращении использования ключа. Если ключ зарегистрирован в инфраструктуре открытых ключей (PKI), то необходимо информировать об отзыве ключа инфраструктуру, которая далее будет рассылать уведомления, указывая на невозможность использования отозванного ключа.

Электронная подпись вырабатывается на основе электронного документа, требующего заверения, и закрытого ключа (рисунок 1).

Рисунок 1 – Схема использования электронной подписи

Сначала производится «сжатие» документа с помощью функции хэширования. Однонаправленная хэш-функция получает на вход исходное сообщение произвольной длины и преобразует его в хэш-значение фиксированной длины (256 бит). Значение хэш-функции сложным образом зависит от содержания документа и не позволяет восстановить сам документ. Хэш-функция чувствительна к всевозможным изменениям в документе. Для хэш-функции практически нельзя подобрать два исходных сообщения, которые будут иметь одно и то же хэш-значение или одну и ту же электронную подпись (что то же самое). Далее, к полученному хэш-значению применяется определенное математическое преобразование, в результате которого и получается собственно ЭП электронного документа.

В настоящий момент в России действует стандарт ГОСТ Р 34.11–94, который определяет обязательную для использования хэш-функцию и регламентирует ее использование. Для формирования и проверки ЭП используется ГОСТ Р 34.10–2001.

Для проверки подписи проверяющий должен располагать открытым ключом конкретного пользователя, наложившего подпись. Проверяющий должен быть полностью

уверен в подлинности открытого ключа (в том, что имеющийся у него открытый ключ соответствует открытому ключу конкретного пользователя). Процедура проверки электронной подписи состоит в вычислении хэш-значения документа и проверке некоторых математических соотношений, связывающих хэш-значение документа, ЭП и открытый ключ пользователя, накладывающего ЭП. Документ считается подлинным, а электронная подпись – правильной, если эти соотношения выполняются. Недействительной ЭП будет в случае, когда сертификат открытого ключа отозван по каким-либо причинам, либо соотношения электронной подписи не выполняются.

Для разрешения спорных ситуаций между отправителем и получателем документа, связанных с возможностью искажения пересылаемого документа или открытого ключа электронной подписи, достоверная копия этого ключа может выдаваться третьей стороне (арбитру), которая должна быть способна справедливо разрешить дело без запроса доступа к закрытому ключу подписи отправителя.

2.2. Основные термины и понятия, связанные с ЭП

Администратор безопасности – субъект доступа, основной обязанностью которого является обеспечение безопасности конфиденциальной связи на том участке сети, которую он курирует.

Возобновление действия сертификата – процесс возвращения в пользование ранее приостановленного сертификата. Сертификат считается возобновленным, если он исключен из вновь опубликованного удостоверяющим центром списка отзыва сертификатов.

Закрытый ключ – уникальная последовательность символов, известная владельцу сертификата ключа подписи и предназначенная для создания в электронных документах электронной подписи с использованием средств электронной подписи.

Источник сертификатов – файл или системное хранилище, из которого выбирается сертификат.

Ключевая пара – пара соответствующих друг другу ключей: открытого и закрытого.

Ключевой контейнер – логическая совокупность данных, содержащая закрытый ключ (возможно зашифрованный), открытый ключ, а также некоторые необязательные атрибуты.

Ключевой носитель – внешний физический носитель, на который записан один или несколько ключевых контейнеров.

Код отзыва – код ситуации, послужившей причиной отзыва сертификата.

Корневой сертификат – сертификат удостоверяющего центра, используемый для проверки подписи сертификатов и списков отзыва, издаваемых этим центром.

Криптопровайдер (Cryptographic Service Provider – CSP) – программный модуль, встраиваемый в операционную систему, реализующий основные криптографические преобразования.

Личный сертификат – сертификат, для которого имеется соответствующий ему закрытый ключ на ключевом носителе.

Обратный переход – особый тип перехода, который применяется, чтобы указать на то, что переход используется для возврата в предыдущее состояние в цепочке (возврат документа на предыдущий этап обработки).

Отзыв сертификата – процесс исключения сертификата (и соответствующего ключа) из использования в связи с компрометацией ключа, сменой реквизитов владельца ключа,

прекращением операций и т.д. Сертификат считается отозванным, когда он опубликован удостоверяющим центром в списке отзыва. Процесс отзыва является необратимым.

Открытый ключ – уникальная последовательность символов, соответствующая закрытому ключу электронной подписи, доступная любому пользователю информационной системы и предназначенная для подтверждения с использованием средств электронной подписи подлинности электронной подписи в электронном документе.

Переход – связь между двумя состояниями документа: начальным (из которого переходят) и конечным (в которое переходят). Совокупность переходов и состояний определяет цепочку прохождения документа.

PKI (Public Key Infrastructure) – инфраструктура открытых ключей, предназначенная для облегчения использования криптографии с открытым ключом.

Приостановка действия сертификата – процесс временного исключения сертификата (и соответствующего ключа) из использования. Сертификат считается приостановленным, когда он опубликован удостоверяющим центром в списке отзыва с соответствующим кодом отзыва. Действие сертификата, позже, может быть возобновлено.

Проверка подписи – процесс установления подлинности электронного документа на основе его подписи и сертификата (открытого ключа) пользователя.

Связывание сертификатов – процесс установления однозначного соответствия между сертификатом, содержащим открытый ключ ключевой пары, и ключевым контейнером, содержащим закрытый ключ этой ключевой пары.

Сеанс работы с ЭП – логически связная последовательность операций формирования ЭП (возможно для нескольких документов), объединяемая использованием одного и того же закрытого ключа.

Сертификат открытого ключа пользователя – электронный документ, содержащий информацию об открытом ключе пользователя, идентификационную информацию пользователя, а также период действия самого сертификата. Сертификат подписывается сторонним лицом (арбитром), в роли которого, согласно PKI выступает удостоверяющий центр.

Системное хранилище сертификатов (списков отзыва) – механизм операционной системы, предназначенный для структурированного хранения цифровых сертификатов (списков отзыва), и работы с ними.

Средство криптографической защиты информации (СКЗИ) «КриптоПро CSP» – программное средство, осуществляющее криптографическое преобразование информации для обеспечения ее безопасности, работающее на основе принципа открытого распределения ключей.

Состояние – определенный этап в обработке электронного документа. Текущее состояние определяет возможные пути дальнейшего изменения электронного документа (возможные следующие состояния, возможные изменения атрибутов).

Crypto API (Cryptographic Application Programming Interface) – совокупность функций библиотек операционной системы, предоставляющих возможность работы с криптографическими алгоритмами и данными для этих алгоритмов.

Удостоверяющий центр – согласно PKI стороннее юридическое лицо, оказывающее услуги управления ключевой информацией.

Установка сертификата – процесс помещения сертификата в системное хранилище.

Формирование электронной подписи (подписание электронного документа) – процесс формирования ЭП для указанного электронного документа с использованием закрытого ключа пользователя.

Хранилище данных ЭП (хранилище подписанных документов) – база данных для хранения описаний документов в xml-формате, электронных подписей и служебных данных подписанных документов.

Шаблон выборки – аналогичен шаблону макро-отчетов, но не имеет части, описывающей визуализацию выбранных данных. Шаблоны выборки используются для получения данных в системе обработки состояний и наложения ЭП. Хранятся шаблоны выборки в специальной структуре каталогов в файловой системе. Наборы атрибутов колонок, а также функциональность шаблонов выборок расширены по сравнению с шаблонами макро-отчетов, чтобы удовлетворять дополнительным требованиям таких задач как организация работы с применением ЭП.

Электронная подпись (ЭП/ЭЦП) – реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажений информации в электронном документе.

Электронный документ – документ, в котором информация представлена в электронно-цифровой форме.

2.3. Использование СКЗИ «КриптоПро CSP» для защиты информации

СКЗИ «КриптоПро CSP» представляет собой набор модулей, которые должны быть использованы в составе программного обеспечения для реализации криптографической защиты на основе протокола подписи. Программные библиотеки СКЗИ «КриптоПро CSP» предоставляют унифицированный COM-интерфейс, используемый разработчиками АС «Бюджет» и АС «УРМ» при формировании и проверке подписи, скрывающий детали реализации криптографических преобразований.

СКЗИ «КриптоПро CSP» предназначено для:

- авторизации и обеспечения юридической значимости электронных документов при обмене ими между пользователями посредством использования процедур формирования и проверки электронной подписи (ЭП);
- контроля целостности системного и прикладного программного обеспечения для его защиты от несанкционированного изменения или от нарушения правильности функционирования;
- управления ключевыми элементами системы в соответствии с регламентом средств защиты.

Основные функции, реализуемые СКЗИ «КриптоПро CSP»:

- генерация закрытых и открытых ключей ЭП и шифрования;
- запись закрытых ключей на различные типы ключевых носителей;
- возможность генерации ключей с различными параметрами в соответствии с ГОСТ Р 34.10-2001 «Информационная технология. Криптографическая защита информации. Система электронной подписи на базе асимметричного криптографического алгоритма»;

- хеширование данных в соответствии с ГОСТ Р 34.11-94 «Информационная технология. Криптографическая защита информации. Функция хэширования»;
- шифрование данных во всех режимах, определенных ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая»;
- формирование электронной подписи в соответствии с ГОСТ Р 34.10-2001 «Информационная технология. Криптографическая защита информации. Система электронной подписи на базе асимметричного криптографического алгоритма»;
- опциональное использование пароля (пин-кода) для дополнительной защиты ключевой информации;
- реализация мер защиты от несанкционированного доступа к ключевой информации пользователя.

СКЗИ «КриптоПро CSP» является системой с открытым распределением ключей. Открытые ключи подписи представлены в виде сертификатов открытых ключей. Для формирования ЭП используется закрытый ключ подписи.

При работе со СКЗИ каждый пользователь, обладающий правом подписи, вырабатывает на своем компьютере или получает от администратора безопасности (в зависимости от политики безопасности) личные закрытый и открытый ключи. На основе каждого открытого ключа третьей стороной (удостоверяющим центром) формируется сертификат открытого ключа.

При формировании закрытые ключи СКЗИ «КриптоПро CSP» записываются в ключевой контейнер. Ключевой контейнер содержит ключевую пару, а также служебную информацию, необходимую для обеспечения криптографической защиты ключей, их целостности и т.п.

Длина ключей электронной подписи определяется ГОСТ Р 34.10-2001 «Информационная технология. Криптографическая защита информации. Система электронной подписи на базе асимметричного криптографического алгоритма»:

- закрытый ключ - 256 бит;
- открытый ключ - 512 бит.

Каждый ключевой контейнер (независимо от типа носителя) является полностью самостоятельным и содержит всю необходимую информацию для работы, как с самим контейнером, так и с закрытыми (и соответствующими им открытыми) ключами.

Для хранения ключевой контейнер размещают на внешнем физическом носителе, который может быть одного из следующих видов:

- дискета 3.5”;
- электронный идентификатор eToken;
- электронный идентификатор ruToken;
- электронный идентификатор JaCarta;
- таблетки Touch-Memory DS1993 – DS1996 с использованием устройств Аккорд-АМДЗ, электронный замок «Соболь» или устройство чтения таблеток Touch-Memory DALLAS;
- процессорные карты MPCOS-EMV и российские интеллектуальные карты (РИК) с использованием считывателя smart card GemPlus GCR-410.

Личные ключевые носители пользователей рекомендуется хранить в сейфе. Пользователь несет персональную ответственность за хранение личных ключевых носителей.

2.4. Взаимосвязь системы состояний и ЭП

Данная возможность появляется при совместном использовании с ПМ «Конвейерная обработка и множественное визирование документов».

Принцип обработки электронных документов подразумевает переход документов из одного состояния в другое, и от одного участника к другому. На каждом этапе движения электронный документ находится в определенном состоянии, которое подлежит закреплению. Для каждого электронного документа составляется перечень состояний, а также схема разрешенных состояний и переходов. Допускаются сложные схемы согласования электронных документов, когда в процессе участвуют главные распорядители, распорядители и получатели бюджетных средств, территориальные подразделения финансового органа, а также структурные подразделения внутри финансового органа.

При переводе электронного документа в некоторое состояние может быть установлено требование наложения ЭП. АС «Бюджет» и АС «УРМ» позволяют использовать ЭП во внутреннем документообороте финансового органа и при электронном обмене документами между финансовым органом и клиентами АС «УРМ». Моменты наложения ЭП определяются в соответствии с заданными схемами движения документов между участниками бюджетного процесса (внутри ФО, при взаимодействии ФО с удаленными клиентами). Число электронных подписей (далее – подписей) на одном документе, в общем случае, не ограничено. Все подписи, наложенные на электронный документ, сохраняются в системе.

В АС «Бюджет» при первом переводе документа из состояния в состояние автоматически контролируются все подписи удаленных клиентов, сформированные ранее для этого документа.

Подписи, наложенные на электронный документ, могут иметь различные логические типы.

- Обычная подпись – подпись, заверяющая корректность электронного документа на определенном этапе. Обычная подпись накладывается при прямом переходе.
- Отмененная подпись – в ходе работы подпись может быть отменена (стать неактивной).
- Подпись отката – подпись, заверяющая отмену подписи (данная подпись может впоследствии использоваться для выяснения причин отмены подписания документа). Подпись отката (иначе говоря, подпись обратного перехода) накладывается при обратном переходе.
- Активная подпись – последняя (по порядку) обычная подпись, наложенная на документ.

Нужно отметить, что предполагается отсутствие циклов при использовании прямых переходов. То есть, вернуться в состояние, в котором документ уже находился ранее, можно только с помощью обратного перехода. При выполнении обратного перехода все электронные подписи, наложенные после выхода из данного состояния, будут помечены как отмененные.

Общая последовательность действий при переходе в новое состояние:

1. Проверяются права пользователя на данный переход.
2. Выбираются электронные документы, которые необходимо перевести в новое состояние.
3. Если для нового состояния нужна подпись, то выполняется проверка активной подписи: ее наличие, корректность, а также неизменность значимых атрибутов документа.
4. В электронные документы вносятся изменения (например, указывается дата принятия, документ включается в реестр и так далее). В частности указывается номер состояния, в которое переводится документ.

5. Если для нового состояния нужна подпись, то выбранные электронные документы подписываются с помощью закрытого ключа сотрудника.

На время выполнения перечисленных действий выбранные электронные документы блокируются для редактирования другими сотрудниками. Кроме того, вся перечисленная совокупность действий рассматривается как одна транзакция, то есть, либо все эти действия будут успешно выполнены, либо не выполнится ни одно из них.

Более подробно о системе состояний можно узнать в документации к ПМ «Конвейерная обработка и множественное визирование документов».

2.5. Организация хранения документов с ЭП

❖ **Структура хранилища данных ЭП**

Исходные электронные документы, на которые накладывается ЭП, хранятся в основной базе данных АС «Бюджет». Для наложения ЭП создается их представление в виде xml-документа определенного формата. Различают понятия ***документ***, хранимый в базе данных, и ***xml-документ*** – описание состояния документа в xml-формате на момент наложения ЭП. Описание документа в xml-формате, электронная подпись и служебные данные подписанного документа сохраняются в специальном хранилище данных ЭП АС «Бюджет», которое представляет собой отдельную базу данных (криптобазу). Доступ к нему со стороны пользователей ограничен. Реализована выгрузка данных из хранилища данных ЭП АС «Бюджет» в файловую систему. Вся информация о подписании документов, как в рамках АС «УРМ», так и в рамках АС «Бюджет» хранится в одном хранилище данных ЭП в финансовом органе. На стороне АС «УРМ» хранилище данных с ЭП не предусмотрено. Ниже приведен формат таблицы, в которой хранится информация о подписании документов.

Таблица 1 – Таблица SignDocRecords

Имя поля	Тип	Описание
ID	ID	Первичный ключ
DocumentData	Blob	xml-документ
SignData	Blob	Подпись
FUID	Integer	Идентификатор документа в БД АС «Бюджет»
DocumentType	Integer	Тип документа в АС «Бюджет»
UniqueNumber	Integer	Порядковый номер подписи (уникален для записей с одинаковым FUID)
BeginState/ State	Integer	Номера начального и конечного состояний, определяющих переход. По этим полям в истории изменений состояний будет производиться сопоставление подписи с конкретным этапом обработки
Flag	Integer	Логический тип подписи (обычная, активная, отмененная, подпись отката)
SenderId	Integer	Идентификатор клиента (для документов, пришедших из АС «УРМ»)
UserName	string(15)	Имя пользователя, который записал информацию в базу данных
CreateDate	OldDate	Дата и время подписания
UUID	Integer	Уникальный идентификатор подписи

ID – это суррогатный (идентифицирующий) ключ, реальным ключом является комбинация FUID и UniqueNumber. Подпись соответствует некоторому состоянию, в котором находился документ на момент подписания. Информация о состоянии хранится в полях BeginState, State и DocumentType.

❖ Формат xml-документа

В таблице «SignDocRecords» электронные документы хранятся в xml-форме в поле DocumentData. Ниже схематично описана структура xml-документа. В xml-документе должен присутствовать заголовок внутри тэга <Caption> (всегда ровно одна запись) и может присутствовать несколько детализаций внутри тэгов <Detail00>, <Detail01> и т.д. (несколько записей в каждой).

```
<?xml version="1.0" encoding="windows-1251"?>
<Document>
  <Caption>
    <!-- Мастер запись (заголовок) в специальном формате -->
  </Caption>
  <Detail00>
    <!-- Подчиненные записи первой детали в специальном формате -->
  </Detail00>
  ...
</Document>
```

Формат сохранения записей заголовка и детализаций приводится ниже.

```
<FDL>
  <FD>
    <N>имя поля</N>
    <CN>класс поля (класс компонента)</CN>
    <FDT>тип поля (тип данных)</FDT>
    <S>размер поля</Size>
    <DL>заголовок, выводимый при отображении</DL>
  </FD>
  .....
</FDL>

<RL>
  <R>
    <V N="имя поля">значение поля</V>
    .....
  </R>
  .....
</RL>
```

Внутри тэга <FDL> выполняется описание типов полей электронного документа. Каждый тип поля описывается внутри отдельного тэга <FD>. Данные сохранятся в тэге <RL>. Каждая запись хранится в отдельном тэге <R> в виде набора вложенных тэгов <V>, каждый из которых хранит данные в формате «имя поля – значение». Запись соответствует либо заголовку, либо одной строке детализации.

❖ Шаблон выборки

Отображение сравниваемых электронных документов выполняется на основании информации из шаблона выборки, с помощью которого документы выбираются из базы данных. Информация о структуре электронного документа, хранимая внутри тэга <FDL>,

при операции сравнения использоваться не будет. Предполагается, что эта информация может быть использована в дальнейшем для просмотра информации о подписанных документах в тех случаях, когда в силу тех или иных причин формат соответствующих документов и, следовательно, их шаблоны будут изменены.

В шаблоне выборки хранится информация:

- о способе выборки документов;
- о первичном ключе заголовка и детализаций, и о полях детализации, которые ссылаются на первичный ключ заголовка (для сравнения документов и для задания отношения мастер-деталь);
- о том, как отображать выбранные данные: подписи для закладок с детализациями (если их несколько), заголовки колонок, их ширина и т.д.;
- о том, какие поля следует сохранять в xml-документе (часть полей может выбираться в служебных целях);
- о том, допускаются ли изменения данного поля (используется при переводе документа из одного состояния в другое).

2.6. Процедура наложения ЭП на электронный документ

Ниже описан алгоритм наложения подписи на один электронный документ. Если подписывается более одного документа, то указанные действия выполняются последовательно для каждого отдельного документа.

1. Преобразование документа в xml-формат.
2. Подписание документа.
3. Сохранение информации о подписании документа в хранилище данных ЭП (имя пользователя, подписывающего документ; состояние, в котором документ подписывается). В качестве имени пользователя берется имя текущего пользователя АС «Бюджет» (для АС «УРМ» указывается пользователь, от имени которого работает сервер обмена данными). Информация о состоянии, к которому относится подпись, берется из поля подписываемого документа с именем СостояниеДокумента. Если такого поля нет, то документ не имеет состояний (при сохранении данных значение поля будет NULL).

При сохранении информации о подписанных документах в хранилище данных ЭП выполняется сжатие xml-документов для уменьшения дискового пространства, занимаемого хранилищем данных ЭП. Такой xml-документ нельзя просмотреть без предварительной распаковки, которая выполняется специальными средствами системы. Выгрузка данных в файловую систему производится в распакованном виде. При сравнении и наложении подписи данные выбираются из БД при помощи макро-отчетов. Внешний вид их может отличаться от того, что видит пользователь на интерфейсе.

2.7. Процедура проверки подлинности ЭП электронного документа

Исходные данные для проверки ЭП на документах передаются в виде коллекции параметров, в которой содержатся проверяемые документы и шаблон выборки, соответствующий данному типу документа. При проверке атрибуты документа, находящегося в базе данных, сравниваются с соответствующими атрибутами того же документа, подписанного ЭП и содержащегося в xml-структуре.

Ниже описан алгоритм действий при проверке подписи одного документа. Если проверяется более одного документа, то указанные действия выполняются последовательно для каждого отдельного документа:

1. Извлечение xml-документа для проверки из хранилища данных ЭП. Если xml-документ не найден, то результат проверки отрицательный;
2. Если xml-документ найден, тогда проводится проверка подписи;
3. Преобразование xml-документа для выполнения сравнения с версией документа, хранимой в базе данных;
4. Сравнение полей документа, на который была наложена ЭП, с текущей версией этого документа, хранящейся в базе данных АС «Бюджет». При обнаружении несоответствия полей выдается предупреждение.

Процесс проверки электронной подписи (2-е действие алгоритма) разделен на два этапа. На первом этапе проверяется корректность самой подписи на основе приложенного к подписи сертификата. Если процесс проверки корректности подписи завершается ошибкой, то выдается сообщение об ошибке и второй этап не начинается. Если первый этап проверки завершается успешно, то на втором этапе производится извлечение параметров подписи (из приложенного сертификата) и проверка присоединенного сертификата по списку отзывов (CRL) и хранилищу сертификатов. Формируется промежуток времени, в течение которого данный сертификат (а, следовательно, и данная подпись) был действителен. Кроме того, извлекаются следующие данные из сертификата (приложенного) открытого ключа пользователя, осуществившего подписание:

- серийный номер сертификата;
- ФИО владельца сертификата;
- дата и время начала действия сертификата;
- дата и время окончания действия сертификата;
- OID алгоритма открытого ключа;
- название алгоритма открытого ключа;
- организация-владелец ключа;
- местонахождение организации;
- область;
- адрес;
- подразделение;
- должность подписавшего;
- издатель сертификата.

Если сертификат корректен, то проверка завершается успешно. Если сертификат оказывается некорректным, то возвращается признак ошибки, а к параметрам подписи добавляется расшифровка ошибки.

В проверку сертификата также входит проверка на наличие его в хранилище сертификатов (системном хранилище). В случае отсутствия копии приложенного к подписи сертификата в хранилище считается, что проверка завершилась ошибкой (параметры подписи при этом также доступны). Таким образом, перед проверкой электронной подписи сертификат соответствующего открытого ключа должен быть установлен в хранилище. Такое ужесточение правил проверки ЭП введено в связи с необходимостью разделения сертификатов одного Удостоверяющего центра на некоторые группы (например, по административному или географическому признаку). Строгое требование установки

сертификатов приводит к полному контролю над списком ключей, которые могут использоваться для наложения ЭП в процессе работы системы.

При проведении сравнения (4-е действие в процессе проверки подписи) документ считается неизмененным, если его заголовок и детализация одинаковы в xml-документе и в БД. Если обнаружены различия, то происходит вызов специальной формы для показа различий и принятия пользователем решения об их значимости. При просмотре различий пользователь может указать документы, изменения в которых он считает приемлемыми, и которые он хочет перевести в другое состояние.

Перед процедурой сравнения полей выполняется запрос к СОУС (служебный объект управления состояниями), который на основании состояния подписанного документа и нового состояния документа выдает список полей, изменения которых учитывать не требуется. Это сделано для того, чтобы не учитывать изменения полей, которые пользователи имели право редактировать в процессе обработки документа.

Как уже отмечалось выше, в шаблоне выборки хранится список полей, изменения которых могут быть проигнорированы (изменения остальных полей не могут быть проигнорированы пользователями, не имеющими администраторских прав). Этот список полей определяется для каждого типа документов и не зависит от состояния документа. Если между подписанным xml-документом и документом в текущем состоянии есть различия, то перевести документ в следующее состояние может только оператор, обладающий администраторскими правами.

Еще один вариант перевода документа в новое состояние, при наличии администраторских прав, предусмотрен на случай изменения свойств существующего состояния, при этом корректные документы, созданные до изменения состояния, могут не иметь подписи, так как ранее она не требовалась для данного состояния.

2.8. Выгрузка информации из хранилища подписанных документов в файловую систему

При выгрузке данных из хранилища данных ЭП в файловую систему документ и электронная подпись сохраняются в отдельных файлах. При выгрузке используется следующая структура каталогов: «год\месяц\день\час» (год – 4 цифры, месяц – номер месяца). В качестве имен файлов используется первичный ключ таблицы SignDocRecords. Файлы могут иметь различные расширения: *.nfo (файл, содержащий значения дополнительных атрибутов для связи с документом в основной базе и связи с этапом обработки, когда ЭП была наложена), *.eds (файл, содержащий саму электронную подпись), *.dat (файл, содержащий подписанный xml-документ).

3. Архитектура подсистемы криптографии АС «Бюджет» и АС «УРМ»

3.1. Режимы работы подсистемы криптографии

Модули подсистемы криптографии АС «Бюджет» и АС «УРМ» рассчитаны на работу в режиме клиентского приложения. Сервер обмена данными при использовании функций криптографии (шифрование, ЭП) должен быть запущен в режиме приложения.

3.2. Crypto API СКЗИ «КриптоПро CSP»

Модули подсистемы криптографии АС «Бюджет» и АС «УРМ» в процессе работы обращаются к функциям «КриптоПро CSP» посредством функций Crypto API.

3.3. Открытие, закрытие и типы криптопровайдеров «КриптоПро CSP»

Криптопровайдер – программный модуль, встраиваемый в операционную систему, реализующий основные криптографические преобразования.

Открытие сессии работы с криптопровайдером начинается с вызова функции инициализации криптопровайдера. Так как задается имя криптопровайдера, то никакие системные или пользовательские настройки криптопровайдера по умолчанию не действуют.

При подписании криптопровайдер открывается (с соответствующим ключевым контейнером) на сессию подписания при первом обращении. При открытии устанавливается имя ключевого контейнера, содержащего закрытый ключ, и при первом обращении к ключу запрашивается ПИН-код. По окончанию сессии подписания криптопровайдер закрывается.

При проверке ЭП имя ключевого контейнера не задается, и его наличие не требуется – достаточно наличия сертификата соответствующего открытого ключа в источнике сертификатов. Запрос ПИН-кода при проверке ЭП не осуществляется. Криптопровайдер открывается без указания имени ключевого контейнера. Криптопровайдер закрывается по окончании процесса проверки электронной подписи.

При функционировании модулей в режиме сервера открытие ключевого контейнера осуществляется с использованием флага CRYPT_MACHINE_KEYSET, что приводит к тому, что рассматриваются только контейнеры, видимые локальной машине, без учета текущего пользователя (это касается ключей, хранимых в реестре).

❖ **Автоматическое определение типа установленного криптопровайдера**

В различных версиях «КриптоПро CSP» регистрируется в системе с разными типами криптопровайдеров – CSP. Модули криптографии автоматически осуществляют распознавание криптопровайдеров, установленных на данной машине.

Система автоматически перебирает криптопровайдеры в заданной последовательности и выбирает первый из них, который будет обнаружен в системе.

Если на компьютере установлены 2 криптопровайдера, то при связывании сертификата с ключевым носителем необходимо использовать тот же тип криптопровайдера, который использовался для генерации ключевой пары.

3.4. Установка и связывание сертификатов с ключевым носителем

Выбор используемого ключевого носителя осуществляется путем связывания соответствующего сертификата с ключевым носителем. Связывание сертификата осуществляется с помощью установки свойства сертификата CERT_KEY_PROV_INFO_PROP_ID. В соответствующей структуре обязательно указываются тип используемого криптопровайдера и имя ключевого контейнера. Установка и связывание могут быть осуществлены как штатными средствами СКЗИ «КриптоПро CSP», так и непосредственно модулями криптографии.

Сертификат, используемый для нахождения соответствующего ключевого контейнера, может быть:

- задан явно своим серийным номером (режим Serial) или списком номеров, разделенных запятой;
- найден автоматически в источнике сертификатов, исходя из имеющегося ключевого контейнера (режим Link);
- искаться автоматически в источнике сертификатов, исходя из имеющегося ключевого контейнера, и, если процесс поиска завершается неудачей, автоматически извлечен из ключевого контейнера (режим Auto).

Наличие сертификата в процессе выбора ключевого контейнера для подписания обязательно, так как он является обязательной составной частью контейнера подписи.

❖ Жесткая привязка ключа (Режим Serial)

Жесткая привязка сводится к установке однозначного соответствия между сертификатом открытого ключа (задается серийным номером) и ключевым контейнером.

При жесткой привязке (по серийному номеру) системе в явном виде указывается сертификат открытого ключа пользователя, связанный с ключевым контейнером. Таким образом, система будет жестко привязана к конкретному ключевому носителю. Механизм требует явной установки сертификата и его связывания с ключевым контейнером, а также указания серийного номера установленного сертификата в настройках системы.

Поскольку сертификат задается явно, то при отсутствии соответствующего ключевого носителя выдается ошибка и подписание не производится. Ошибка также выдается в случае, если заданный сертификат отсутствует в источнике сертификатов, либо не связан с ключевым носителем.

❖ Автоматическое связывание (Режим Link)

Механизм автоматического связывания предполагает отсутствие жесткой привязки к ключевому носителю, но требует явной установки сертификатов для всех пользователей системы (сертификаты могут быть как связанными, так и несвязанными).

Механизм базируется на поиске среди всех сертификатов источника одного, который либо привязан к имеющемуся в наличии ключевому контейнеру, либо содержит открытый ключ, аналогичный открытому ключу из ключевого контейнера.

Если сертификат не будет найден, то система выдаст ошибку.

Режим требует, чтобы предварительно источник сертификатов был заполнен сертификатами, и в этом смысле, данный режим является более жестким, чем рассматриваемый далее режим автоматической установки.

Режим Link является единственно возможным из автоматических режимов, если при формировании ключей сертификат не помещается в ключевой контейнер.

В случае если настройки разрешают процесс поиска сертификата по имеющимся в наличии ключевым контейнерам (но не автоматическое извлечение из ключевого контейнера), то производится двухэтапный поиск. На первом этапе источник сертификатов просматривается на предмет наличия сертификата, уже связанного с данным ключевым контейнером. Если такой сертификат обнаруживается, то второй этап пропускается. На втором этапе из контейнера извлекается открытый ключ и ищется соответствующий сертификат, затем производится связывание этого сертификата во временном хранилище. В случае, если соответствующий сертификат (сертификат с таким же открытым ключом) отсутствует в источнике сертификатов, то выдается ошибка.

❖ **Автоматическая установка сертификата (Режим Auto)**

При разрешении автоматического извлечения сертификата из ключевого контейнера производятся те же шаги, что и при автоматическом поиске сертификатов. В случае отсутствия сертификата с таким же открытым ключом в источнике, производится попытка извлечь этот сертификат из ключевого контейнера. Если соответствующее свойство ключевого контейнера не задано, то генерируется ошибка.

Режим Auto может быть использован в случае, если ключевой контейнер не содержит сертификата – в этом случае режим будет аналогичен автоматическому связыванию (будет только отличаться сообщение об ошибке в случае неудачи).

❖ **Работа с ключевыми контейнерами в различных режимах**

В зависимости от режимов выбора ключевых контейнеров, различается и функционирование модулей подсистемы криптографии. Так как ключевой контейнер требуется только для формирования электронной подписи, то здесь рассматривается только этот процесс.

Автоматические режимы (Link, Auto) отличаются правилами работы. В таблице 2 приводятся основные различия между режимами, в зависимости от различных внешних условий.

Таблица 2 – Правила обработки ключевых контейнеров в зависимости от режимов выбора

Внешние условия	Serial	Link	Auto
Не найден сертификат с заданным серийным номером	Ошибка	*	*
В сертификате не определен ключевой контейнер	Ошибка		
Не обнаружен ключевой контейнер, определенный в сертификате	Ошибка	*	*
Не найден сертификат с открытым ключом совпадающим с открытым ключом в контейнере	*	Ошибка	
В ключевом контейнере не содержится сертификат			Ошибка

Звездочками «*» обозначены ситуации, возникновение которых невозможно. Пустые ячейки соответствуют штатной работе (без выдачи ошибок).

Наличие автоматических режимов требует более жестких правил использования модулей. Для недопущения ситуаций ошибочного формирования подписи налагаются следующие ограничения на процесс подписания:

1. В момент подписания не должно быть доступно более одного ключевого носителя. Данный запрет позволяет избежать ситуации, связанной с неправильным выбором ключевого носителя из списка доступных. Исключением из данного правила является ситуация, когда используется режим Serial. В этом случае допустимо наличие нескольких ключевых носителей при условии, что в списке серийных номеров, указанных в поле serial имеется только один из них.
2. Не допускается установка ключевого контейнера в реестр. Ситуация установки ключевого контейнера с ключом для формирования подписи в реестр является абсолютно недопустимой, так как резко повышает вероятность разглашения ключа.
3. В момент подписания множества документов не допускается извлечение ключевого носителя (или его замена).
4. Ключевой носитель не должен содержать более одного ключевого контейнера, за исключением случая, описанного в п.1.

Все эти проверки осуществляются модулями автоматически.

3.5. Корневые сертификаты

Корневой сертификат – сертификат удостоверяющего центра, используемый для проверки электронной подписи сертификатов и списков отзыва, издаваемых этим центром.

Как уже указывалось выше, корневой сертификат не включается в контейнер с электронной подписью. Корневой сертификат соответствующего удостоверяющего центра должен быть предварительно установлен на компьютере, где производится подписание документов или проверка электронной подписи.

Корневые сертификаты, в зависимости от режима функционирования, устанавливаются в системные хранилища «ROOT». Если модули функционируют в режиме сервера, то в качестве корневого хранилища используется хранилище «ROOT» локального компьютера, если в режиме клиента – хранилище «ROOT» текущего пользователя.

Корректность ЭП корневого сертификата проверяется в процессе формирования цепочки сертификатов, путем вызова функции CertGetCertificateChain.

Корневой сертификат является важным и критичным звеном подсистемы криптографии. Необходимо тщательно отслеживать установленные на машине корневые сертификаты.

3.6. Ограничения на структуру используемых удостоверяющих центров

Модули подсистемы криптографии рассчитаны только на работу с одноуровневой моделью удостоверяющих центров, т.е. путь сертификации не может включать более двух звеньев: 1 – используемый сертификат, 2 – корневой сертификат удостоверяющего центра, заверившего используемый сертификат.

Удостоверяющие центры должны использовать российские алгоритмы, как для формирования открытых ключей сертификата, так и для формирования самого сертификата открытого ключа. Использование устанавливаемых по умолчанию Microsoft Certification Authority алгоритмов SHA1 и RSA недопустимо.

3.7. Схема хранения сертификатов и списков отзыва

Сертификаты и списки отзыва сохраняются системой в хранилищах сертификатов операционной системы (системных хранилищах) или внешних файлах. В настройках могут задаваться как имена используемых системных хранилищ, так и имена внешних файлов. В случае, если имена в настройках не задаются, то используются значения по умолчанию.

Система поддерживает один источник сертификатов (либо файл, либо системное хранилище), и один источник списков отзыва (либо файл, либо системное хранилище).

В момент начала сеанса работы с электронной подписью все содержимое источников сертификатов копируется во временное хранилище (InMemory), и в процессе обработки используется именно оно.

4. Установка и настройка СКЗИ «КриптоПро CSP»

До установки и настройки модулей подсистемы криптографии АС «Бюджет» и АС «УРМ» на сервере обмена данными, станциях клиентов АС «Бюджет» и АС «УРМ» необходимо установить СКЗИ «КриптоПро CSP», корневой и личные сертификаты в соответствии с инструкцией «Установка и конфигурирование СКЗИ «КриптоПро CSP».

5. Установка и настройка модулей АС «Бюджет», обеспечивающих работу с ЭП

5.1. Состав модулей

Работу подсистемы криптографии АС «Бюджет» обеспечивают следующие основные модули:

- **AdminSign.exe** – утилита для администратора безопасности, позволяет просматривать хранилище подписанных документов, осуществлять поиск и выгрузку подписанных электронных документов из хранилища в файл для решения спорных вопросов, делать выгрузку подписей и документов на диск;
- **SignAdm.ocx** – модуль, отвечающий за работу редакторов схем подписания и справочника ролей;
- **EDSign.ocx** – модуль, отвечающий за работу функций ЭП;
- **DSign.ocx** – программная библиотека, реализующая InProcess COM-сервер. Выполняет функции диспетчера;
- **DSign.ini** – файл настроек, в котором хранятся параметры работы диспетчера подсистемы криптографии: флаг-галочка, определяющий использование ЭП при отправке документа с удаленного рабочего места, код сертификата (ключ), тип используемого криптопровайдера;

Необходимо заметить, что файлы настроек являются критичными в том смысле, что их изменение может радикально изменить алгоритмы использования криптографических методов. В связи с этим целесообразным и необходимым является защита этих файлов от изменения теми же методами, что и исполняемых файлов системы.

5.2. Общий алгоритм установки и настройки

1. Создайте на диске вспомогательный каталог, например **BudgetAx\Updates\EDS**, скопируйте в него и разархивируйте файлы архива.
2. Обязательно создайте резервную копию рабочего каталога **BudgetAx**, содержащую базу, на которую устанавливается ПМ.
3. Скопируйте в каталог текущего года **BudgetAx\Ocx** файлы из папки **EDS\OCX**.
4. Зарегистрируйте все файлы, находящиеся в рабочем каталоге **OCX** установленной АС «Бюджет» в операционной системе. Для этого воспользуйтесь утилитой Register.exe.

При использовании системного файла workplace.exe.manifest необходимо заново сформировать файл workplace.exe.manifest, запустив Register.exe из командной строки с ключом /L.

5. Выполните настройку диспетчера в файле рабочей станции DSign.ini в соответствии с пунктом 5.3 «Настройки диспетчера подсистемы криптографии (файл DSign.ini)».
6. Выполните настройки, связанные с подключением к хранилищу данных ЭП в соответствии с пунктом 5.4 «Настройки подключения к хранилищу данных ЭП».
7. Запустите АС «Бюджет» и наложите все необходимые условия и ограничения, связанные с системой состояний и ЭП, на РМ Администратор состояний и РМ Администрирование УРМ для каждого типа документов в соответствии с пунктом 5.5 «Настройка АС «Бюджет» для работы с ЭП».

5.3. Настройка диспетчера подсистемы криптографии (файл DSign.ini)

Для настройки диспетчера подсистемы криптографии АС «Бюджет», в том числе для регистрации ключевого носителя, отредактируйте файл **DSign.ini**.

Метод загрузки настроек из **DSign.ini** определяется значением параметра Provider секции [DIGITAL_SIGN]:

- CryptoPro – параметры настройки берутся из секции [CRYPTOPRO];
- Universal – параметры настройки берутся из секции [UNIVERSAL];
- EDS – параметры настройки берутся из секции [EDS].

Секция [CRYPTOPRO] содержит параметры:

- Serial – значение серийного номера сертификата, соответствующего информации на ключевом носителе. Серийный номер сертификата можно посмотреть в параметрах сертификата, открыв оснастку и выбрав нужный сертификат. Допускается указание нескольких серийных номеров, разделенных запятой. Параметр используется только в АС «УРМ». Способ задания серийных номеров сертификатов в АС «Бюджет» описан в пункте 5.5 «Настройка АС «Бюджет» для работы с ЭП».
- CertStoreType – тип используемого хранилища сертификатов, параметр может иметь следующие значения:
  - system – для поиска выпущенных сертификатов криптопровайдер будет обращаться к хранилищу сертификатов «Личные» («Private») операционной системы;
  - file – для поиска выпущенных сертификатов криптопровайдер будет обращаться к хранилищу сертификатов в файле, или к так называемому сериализованому хранилищу – «Serialized Store» (файл хранилища должен иметь расширение *.sst).
- CertStorePath – путь к хранилищу сертификатов (при CertStoreType = system – значение данного параметра игнорируется);
- CRLType – тип используемого списка отозванных сертификатов (СОС), параметр может иметь следующие значения:
  - system – для поиска СОС криптопровайдер будет обращаться к хранилищу сертификатов операционной системы;
  - file – для поиска СОС криптопровайдер будет обращаться к файлу с экспортированным списком отозванных сертификатов (файл с экспортированным СОС должен иметь расширение *.crl).

- CRLPath – путь к СОС (при CertStoreType = system – значение данного параметра игнорируется).

Для обычного режима работы с ЭП примите следующие параметры равными: CertStoreType= system, CRLType= system. Другие значения этих параметров предназначены для особых ситуаций (при использовании старых модулей, сопоставления с ними и т.п.).

Секция [EDS] содержит параметры:

- System – определяет является ли запуск системным. Если значение этого параметра TRUE, YES или ON, то считается, что запуск произошел в режиме сервиса.
- ProviderList – список имен провайдеров, которые можно использовать при подписании или проверке подписи. Допускается совместное использование разных провайдеров вперемешку.
- CertList – список серийных номеров сертификатов, перечисленных через запятую (серийные номера не должны содержать пробелов, кавычки не допустимы).
- ContainerCheck – определяет нужно ли проверять наличие контейнера перед каждым подписанием. По умолчанию TRUE, настоятельно рекомендуется не отключать, в связи с особенностями кэширования провайдеров под Win7.
- CertSourceName – имя источника (имя системного хранилища или файла).
- CertSourceType – тип источника. Допустимы два значения:
  - file – в этом случае CertSourceName – имя файла в формате *.p7b.
  - system – в этом случаем CertSourceName – имя системного хранилища.
- AutoSearch – определяет где выполнять поиск. Если TRUE, то конечные сертификаты берутся прямо с носителей, иначе из источника.
- SilentList – список провайдеров, которые поддерживают «тихий» режим (без диалоговых окон). Провайдеры из этого списка, в системном режиме будут создаваться с флагом «Silent». Так как некоторые провайдеры реагируют на такой режим ошибкой, то это поле необходимо. По умолчанию инициализировано списком провайдеров.
- Proxy – имя прокси-сервера, если он есть (по умолчанию – пусто). Если пусто, то идет обращение напрямую.
- ProxyPort – порт прокси-сервера (по умолчанию 8080).
- ProxyUserName – имя пользователя для подключения к прокси-серверу.
- ProxyPass – пароль, для подключения к прокси-серверу.
- Параметры настройки механизма штампов времени (TSAHost, TSAPort, TSAPolicy, TSAHash, TSAAlgList) рассмотрены в пункте 6.5.
- Параметры настройки OCSP (OCSPHost, OCSPPort, OCSPProxy, OCSPProxyPort, OCSPProxyUser, OCSPProxyPass, OCSPHashAlgo, OCSPServerCert, OCSPUseOnSign) рассмотрены в пункте 6.6.

5.4. Настройки подключения к хранилищу данных ЭП

Для настройки подключения к криптографической базе необходимо определить значения группы констант Системные настройки\Криптографическая схема на интерфейсе Константы системы РМ Администратор:

- Путь к базе – путь к хранилищу данных ЭП (криптографической базе данных). Следует обратить внимание на формат записи пути до файла в зависимости от выбранного сетевого протокола:
  - для сетевого протокола TCP\IP: Server\D:\BudgetAx\Database\CRYPTO.gdb;

- для сетевого протокола NetBEUI: \\Server\D:\BudgetAx\Database\CRYPTO.gdb;
- для сетевого протокола IPX/SPX: Server@D:\BudgetAx\Database\CRYPTO.gdb.

- Пользователь – имя пользователя, которое будет использоваться при подключении к хранилищу данных ЭП;
- Пароль – пароль, который будет использоваться при подключении к хранилищу данных ЭП.

5.5. Настройка АС «Бюджет» для работы с ЭП

Настройка АС «Бюджет» для работы с ЭП производится:

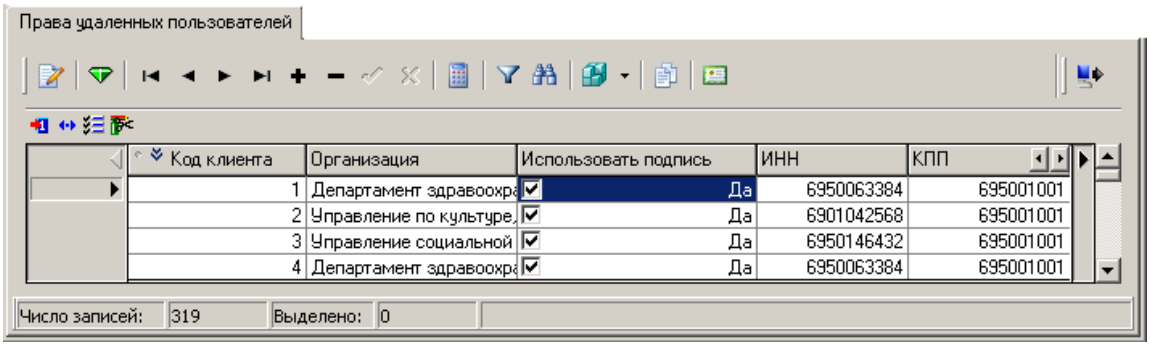
- на интерфейсе Права удаленных клиентов РМ Администрирование УРМ;
- на РМ Администратор состояний.

❖ Настройка прав удаленных пользователей на использование ЭП

В интерфейсе Права удаленных клиентов РМ Администрирование УРМ (рисунок 2) ведется реестр удаленных клиентов АС «УРМ».

Для каждого удаленного клиента необходимо указать, обязан ли он использовать ЭП (флаг-галочка в поле Использовать подпись).

Рисунок 2 – Пример настройки обязательного использования ЭП удаленным клиентом на интерфейсе «Права удаленных клиентов» РМ «Администрирование УРМ»



Если в записи об удаленном клиенте установлен флаг-галочка Использовать подпись, то он не имеет права отсылать документы без наложенной ЭП. В этом случае, если от этого клиента АС «УРМ» все-таки приходит пакет документов без ЭП, то такие документы отклоняются сервером обмена данными автоматически.

Если флаг-галочка Использовать подпись не установлен, то удаленный клиент имеет право присылать документы как с ЭП, так и без нее. При этом, если ЭП присутствует, то она проверяется и обязана быть корректной, а если ее нет, то документ добавляется в базу АС «Бюджета» без подписи.

На закладке детализации Сертификаты осуществляется ввод данных по сертификатам удаленных пользователей.

Система считает, что удаленный клиент имеет право подписывать документы только ключами, серийные номера сертификатов которых указаны на данной закладке детализации (если документ будет подписан ключом, для которого не указан серийный номер сертификата, то при проверке ЭП сервером обмена документ будет отклонен).

При проверке документа с ЭП, представленного удаленным клиентом, будет производиться контроль действительности сертификата и контроль подлинности подписи на документе.

Таблица 3 – Перечень полей таблицы детализации на закладке «Сертификаты» интерфейса «Права удаленных клиентов» РМ «Администрирование УРМ»

Название поля	Значение поля	Способ ввода значения
Номер сертификата	Серийный номер сертификата ключа	Ввод с клавиатуры
Можно подписывать	Признак доступности ключа для подписания	Установка/снятие флага-галочки в логическом поле
Начало действия	Дополнительная информация о сертификате	Поле с календарем, доступно для ввода с клавиатуры
Окончание действия		Поле с календарем, доступно для ввода с клавиатуры
Владелец		Ввод с клавиатуры
Организация владелец		Ввод с клавиатуры
Примечание		Ввод с клавиатуры
Авторизация		
Автор, Дата создания, Изменил, Дата изменения	Поля содержат информацию о создании записи и ее последней редакции	Служебные нередактируемые поля, заполняются автоматически при создании или редактировании документа

Для удобства ввода данных на панели инструментов присутствует кнопка импорта атрибутов сертификата  **Импортировать данные из сертификата**.

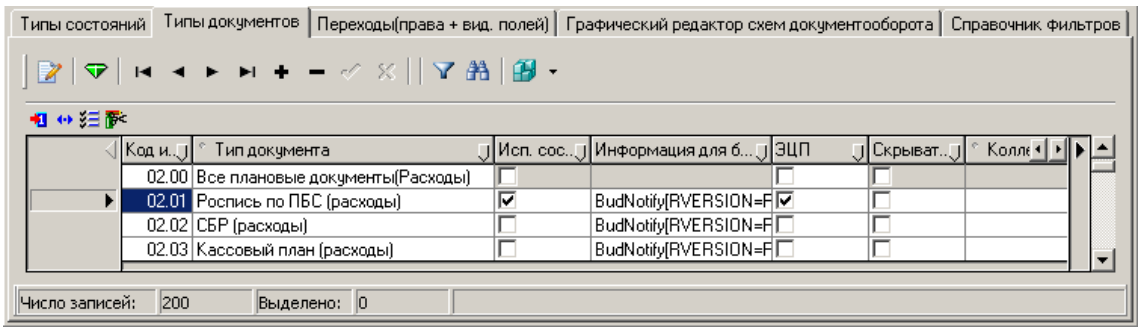
Обмен документами между ФО, ГРБС, РБС, ПБС, ТПФО с использованием ЭП через АС «УРМ» может осуществляться без подсистемы состояний. В этом случае в АС «Бюджет» документ будет проверяться только на корректность ЭП, наложенной при отправке документа из АС «УРМ».

❖ Настройка подсистемы состояний для использования ЭП

РМ Администратор состояний предназначено для настройки подсистемы состояний в случае поставки дополнительных ПМ АС «Бюджет» (ПМ «Конвейерная обработка и множественное визирование документов» и т.д.).

Все основные настройки, позволяющие работать с ЭП, осуществляются на интерфейсе Типы документов РМ Администратор состояний (рисунок 3), причем настройки должны быть произведены для каждого типа документа, предполагающего наложение ЭП.

Рисунок 3 – Настройка подсистемы состояний и возможности использования ЭП на интерфейсе «Типы документов» РМ «Администратор состояний»



В случае необходимости наложения ЭП на документ выбранного типа (значение поля Код интерфейса) установите флаг-галочку в поле Исп. состояния и в поле ЭЦП. Если требуется проверить ЭП без использования системы состояний, установите флаг-галочку только в поле ЭЦП.

Установленный флаг-галочка в поле Скрывать форму простановки подписи позволяет скрыть форму проверки ЭП, в которой отображается подписываемый документ в момент проверки или подписания (подробнее смотрите раздел 8 «Работа пользователя с ЭП в АС «Бюджет» при совместном использовании с ПМ «Конвейерная обработка и множественное визирование документов»). Если флаг-галочка не установлен, то форма проверки ЭП будет показываться всегда.

Для того, чтобы определить, на каких этапах обработки документа требуется накладывать или проверять ЭП, перейдите в детализацию Переходы интерфейса Графический редактор схем документооборота РМ Администратор состояний:

- если при переводе документа из состояния 1 в состояние 2 требуется проверка ЭП, то установите флаг-галочку в поле Проверять ЭЦП;
- если при переводе документа из состояния 1 в состояние 2 требуется наложение в момент перехода новой ЭП, то установите флаг-галочку в поле Требуется ЭЦП, при этом не забудьте проверить активность (корректность) предыдущей ЭП.

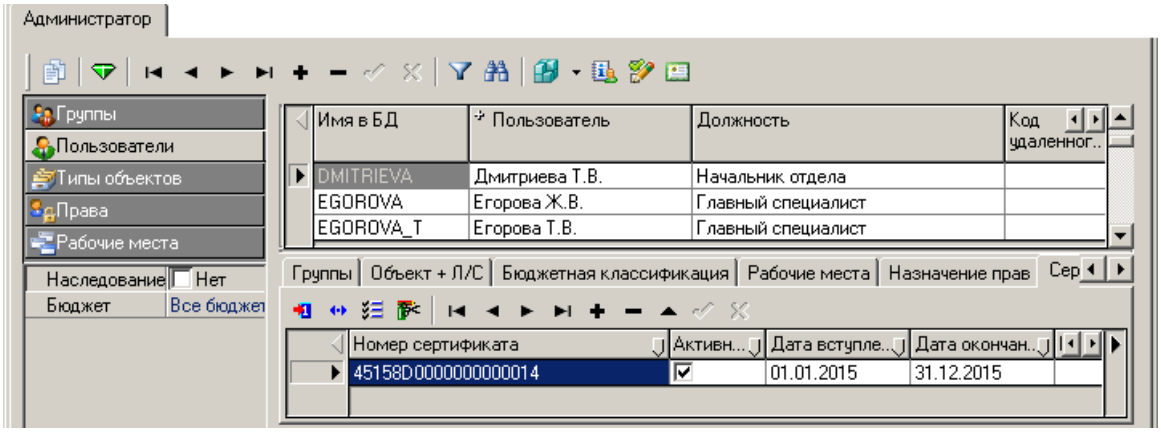
Как правило, при переходе документа из состояния в состояние меняются некоторые его атрибуты. Для указания атрибутов, которые можно изменять в процессе конкретного перехода служит страница Редактирование закладки детализации Переходы интерфейса Графический редактор схем документооборота РМ Администратор состояний. Для каждого изменяемого атрибута нужно установить флаг-галочку в поле Открыт для редактирования. Если изменения допускаются только при исполнении макроса (пользователь не может изменять атрибут вручную), то флаг-галочка ставится в двух полях Открыт для редактирования и Только для макроса.

Более подробно о работе на РМ Администратор состояний читайте в руководстве пользователя ПМ «Конвейерная обработка и множественное визирование документов» (при наличии этого ПМ).

❖ Настройки пользователей АС «Бюджет» для работы с ЭП

Установки параметров криптопровайдера для каждого пользователя осуществляется на закладке Сертификаты раздела Пользователи интерфейса Администратор РМ Администратор. Определенные в данных полях параметры будут перекрывать настройки из файла **DSign.ini**. Поле Номер сертификата служит для хранения серийного номера сертификата пользователя АС «Бюджет», участвующего в подписании документа.

Рисунок 4 – Закладка «Сертификаты» раздела «Пользователи» интерфейса «Администратор»



❖ Настройка констант

В интерфейсе Константы казначейства РМ Настройки системы константа Код причины отклонения для неверной ЭЦП определяет код причины отклонения, который будет устанавливаться у документов с некорректной ЭП.

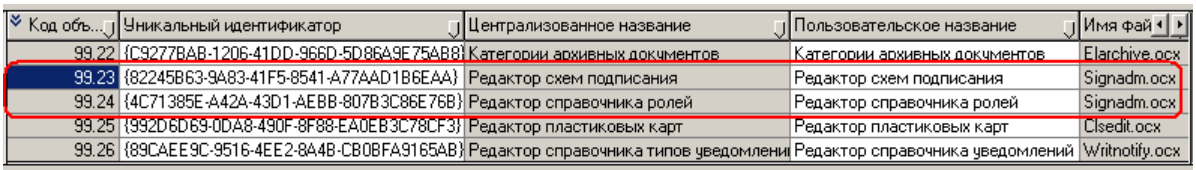
Документы, в поле Код причины отклонения которых указан код константы Код причины отклонения для неверной ЭЦП, отмечаются значком **ЭЦП не признана верной** в поле статуса записи. По умолчанию константа имеет значение «01.05.00».

❖ Настройки АС «Бюджет» для возможности наложения нескольких ЭП на клиенте УРМ

Начиная с версий АС «Бюджет» 9.0 и АС «УРМ» 09.00.00 реализована возможность наложения нескольких ЭП на документы с кодами 03.XX и 02.XX на клиенте УРМ без промежуточной отправки документов на сервер ФО. Для настройки мультиподписания в АС «УРМ» необходимо выполнить соответствующие настройки в АС «Бюджет».

В интерфейсе Объекты РМ Администратор проверьте наличие записей с кодом объекта 99.23 и 99.24.

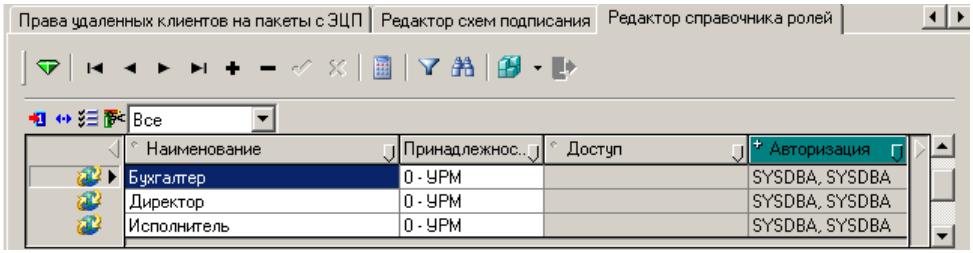
Рисунок 5 – Вид интерфейса «Объекты» РМ «Администратор»



Если данные объекты отсутствуют, необходимо добавить их с помощью кнопки **Объекты ОСХ**, выбрав модуль **SignAdm.ocx**. Добавившиеся интерфейсы необходимо назначить на любое РМ, доступное администраторам системы.

Для подписания выделяются группы пользователей (роли), например, «руководитель», «бухгалтер» и т.п., которые в дальнейшем будут использоваться для определения порядка подписания документов. Роли добавляются в интерфейсе Редактор справочника ролей.

Рисунок 6 – Вид интерфейса «Редактор справочника ролей»



При добавлении ролей необходимо обязательно указывать принадлежность «УРМ», т.к. данный механизм используется только для работы АС «УРМ» и не применим в АС «Бюджет».

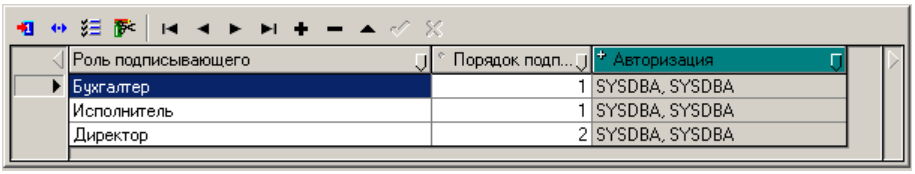
В интерфейсе Редактор схем подписания добавляются схемы подписания документов, определяющие порядок наложения подписей на документ. В заголовке указывается общая информация о схеме подписания (при указании схем не забывайте указывать принадлежность – УРМ).

Схема является общей для всех удаленных клиентов и задает какие роли в каком порядке могут подписывать данную группу документов.

Если в базе уже есть подписанные документы с использованием схемы, то данная схема становится недоступной для редактирования.

При заполнении детализации обязательным является указание значения в поле Порядок подписания - именно это поле в дальнейшем определяет в какой последовательности должны будут накладываться подписи на стороне клиента УРМ. Допустимо указание одинакового порядка, например:

Рисунок 7 – Пример указания порядка подписания



В данной ситуации сначала документ должен быть подписан ЭП бухгалтера и исполнителя (при этом порядок подписи любой – сначала бухгалтер, потом исполнитель или сначала исполнитель, потом бухгалтер), а затем (при наличии двух подписей) документ сможет подписать директор.

Далее необходимо выполнять привязку групп документов, подлежащим подписанию и привязку сертификатов пользователя УРМ к конкретным ролям. На РМ Администрирование УРМ в интерфейсе Права удаленных клиентов на закладке детализации Группы подписания документов необходимо выполнить соответствующие настройки.

Таблица 4 – Перечень полей таблицы детализации на закладке «Группы подписания документов» интерфейса «Права удаленных клиентов»

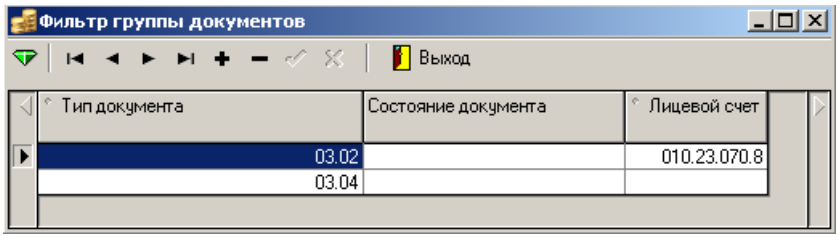
Название поля	Значение поля	Способ ввода значения
Наименование группы	Текстовое поле для ввода обозначения группы подписания документов	Ввод с клавиатуры

Название поля	Значение поля	Способ ввода значения
Примечание	Доп. информация по настроенной группе	Ввод с клавиатуры
Схема	Используемая схема подписания	Выбор из справочника «Схемы подписания»
Фильтр	Множество документов, подлежащих подписанию	Заполнение с помощью модальной формы «Фильтр группы документов»
Сертификаты	Привязка сертификатов пользователя к ролям текущей схемы подписания	Ввод с клавиатуры

После заполнения справочной информации (наименование группы, примечание) необходимо указать схему подписания, при этом для каждой группы может быть определена только одна схема подписания.

Далее необходимо задать параметры документа для определения к какой группе подписания относится тот или иной документ. В фильтре присутствуют следующие поля: Тип документа (является обязательным для заполнения), Состояние документа и Лицевой счет. Разные строки в фильтре (т.е. записи фильтра) объединяются по ИЛИ. Например, под группу подписания указанного ниже фильтра попадают документы с типом платежные поручения и лицевым счетом 010.23.070.8 или документы с типом чеки и с любым лицевым счетом:

Рисунок 8 – Вид модальной формы «Фильтр группы документов»



Настройки фильтра должны позволять отнести подписываемый документ только к одной группе подписания. Если в момент подписания документа будет определено, что документ попадает под условия нескольких групп, то наложение ЭП будет невозможным.

Последним этапом настройки со стороны ФО является привязка сертификатов к ролям. Данная информация заносится в колонке Сертификаты на закладке Группы подписания. В верхней части модального окна, вызываемого в колонке Сертификаты указываются роли выбранной схемы подписания, в нижней части окна производится привязка сертификатов к конкретной роли. В справочнике сертификатов доступны только те сертификаты, которые у данного пользователя помечены флагом-галочкой Можно подписывать. При выборе сертификата в группе подписания галка Можно подписывать на закладке Сертификаты блокируется от изменений.

Для упрощения настройки групп подписания на панель инструментов детализации интерфейса добавлена кнопка копирования выделенных групп другим клиентам **Скопировать группы подписания документов**. Для выбранных удаленных клиентов копируются поля группы подписания, фильтр и назначенные роли, при этом сертификаты не копируются.

Все выполненные настройки отразятся в АС «УРМ» после проведения синхронизации и перезапуска клиента УРМ.

6. Установка и настройка модулей АС «УРМ», обеспечивающих работу с ЭП

6.1. Состав модулей

В работе подсистемы криптографии АС «УРМ» используются следующие основные модули:

- **DSign.ocx** – программная библиотека, реализующая InProcess COM-сервер. Выполняет функции диспетчера подсистемы криптографии. Модуль необходимо устанавливать на каждом компьютере, с которого требуется подписывать документы;
- **EDSign.ocx** – модуль, отвечающий за работу функций ЭП;
- **DSign.ini** – файл настроек, в котором хранятся параметры настроек криптографии: флаг-галочка, определяющий использование ЭП при отправке документа с удаленного рабочего места, код сертификата (ключ), тип используемого криптопровайдера. Модуль должен быть установлен и зарегистрирован на каждой рабочей станции в той же папке, где и **DSign.ocx**;
- **AdminUtil.exe** – служит для указания пути к хранилищу данных ЭП, где хранятся все подписи (для того, чтобы при отсылке документа с подписью, производилась проверка на активность, корректность, регистрацию и т.п.).

6.2. Общий алгоритм установки и настройки

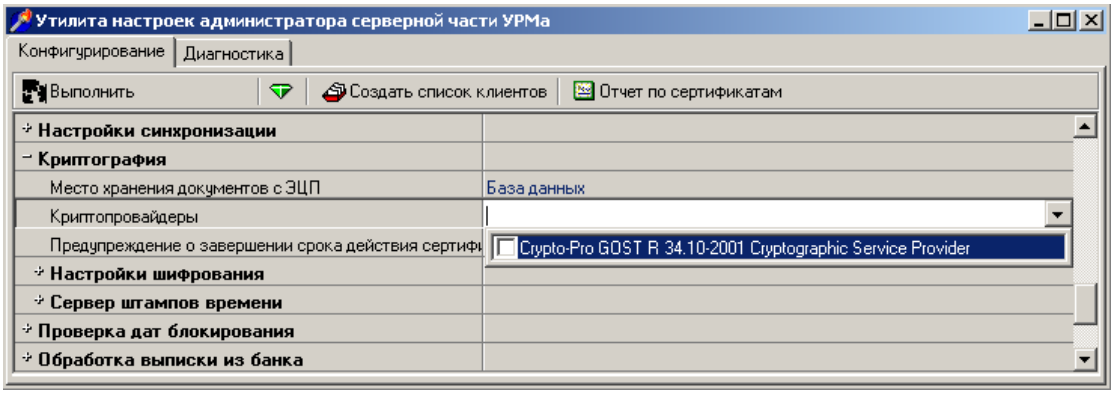
Для введения ЭП в работу на АС «УРМ» сделайте следующее:

1. Проверьте, чтобы на сервере обмена данными (сервере АС «УРМ») были выложены и зарегистрированы модули **DSign.ocx**, **EDSign.ocx**, **DSign.ini**. Для регистрации модулей «Системы удаленного документооборота» используется утилита **Creg.exe**, которая регистрирует все модули *.ocx, находящиеся с ней в одном каталоге.
2. Произведите настройки сервера обмена данными с помощью утилиты **AdminUtil.exe**, расположенной в папке **...\URMServer**, в соответствии с пунктом 6.3 «Настройка сервера обмена данными для работы с ЭП».
3. Проверьте, чтобы в папке с OCX на каждой рабочей станции клиента АС «УРМ» были выложены и зарегистрированы модули **DSign.ocx**, **DSign.ini**.
4. Произведите настройки клиентов АС «УРМ» на рабочем месте Редактор настроек.

6.3. Настройка сервера обмена данными для работы с ЭП

Настройки сервера обмена данными для работы с криптографией производятся с помощью утилиты настроек администратора серверной части АС «УРМ» **AdminUtil.exe** на закладке Конфигурирование в секции Криптография (рисунок 9).

Рисунок 9 – Вид утилиты настроек администратора серверной части АС «УРМ»



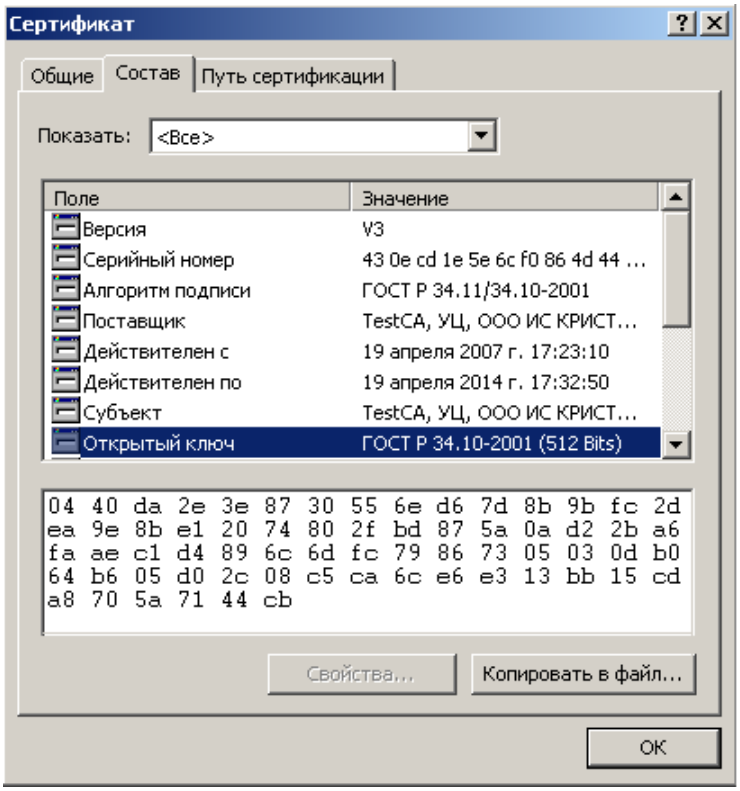
Необходимо задать следующие параметры:

- Место хранения документов с ЭЦП. В качестве доступных вариантов хранения в настоящий момент доступно только хранилище данных ЭП (хранилище является общим для АС «Бюджет» и АС «УРМ»);
- Криптопровайдеры – поле с выпадающим списком, из которого выберите значение CryptoPRO, которое говорит об использовании СКЗИ «КриптоПро CSP»;

Посмотреть криптографический алгоритм (ГОСТ), использованный при генерации ключа, можно в свойствах сертификата (Property Page Select Cert) на закладке Состав в параметре Открытый ключ (рисунок 10).

Если установка сертификата будет произведена с неверным ГОСТ (неверным типом криптопровайдера), тогда при попытке подписания пользователю будет выдано сообщение «Сертификат не найден».

Рисунок 10 – Окно свойств сертификата

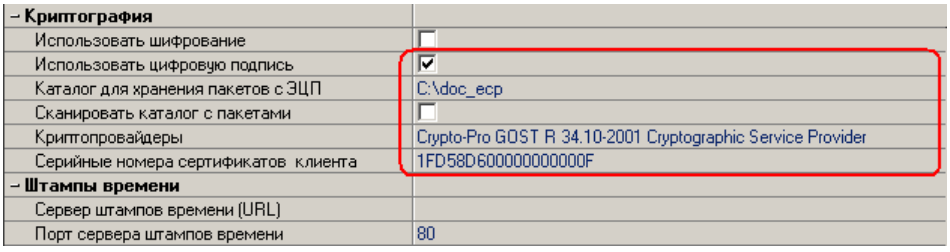


6.4. Настройка клиента АС «УРМ» для работы с ЭП

Настройка работы ЭП у клиента АС «УРМ» производится непосредственно на рабочем месте Редактор настроек (рисунок 11):

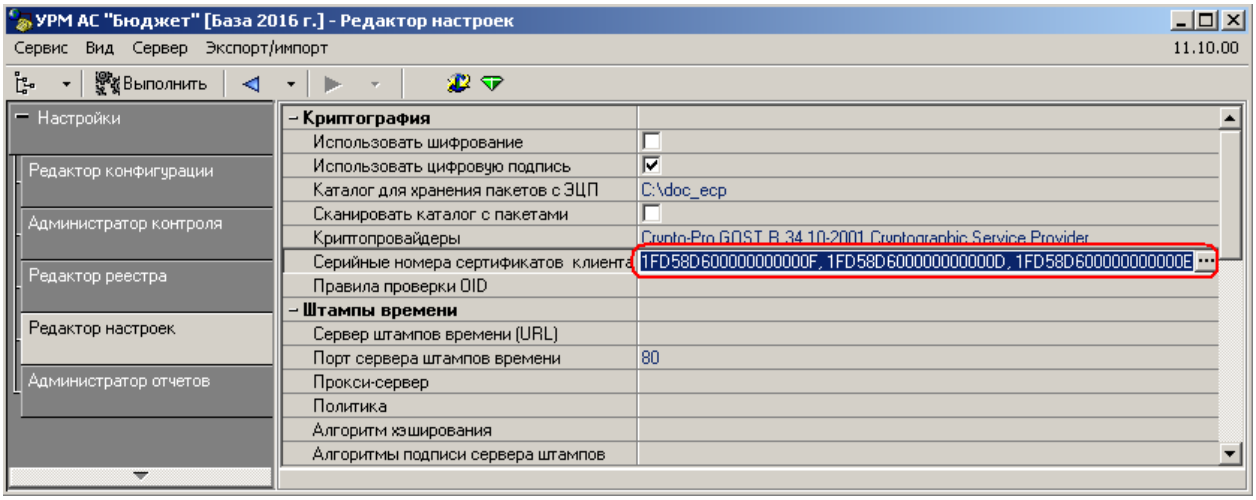
1. Установите флаг-галочку у параметра Криптопрография\Использовать цифровую подпись, которая подтвердит использование ЭП.
2. Установите значение CryptoPro для параметра Криптопрография\Криптопровайдеры.
3. Пропишите серийный номер сертификата клиента без пробелов у параметра Серийные номера сертификатов клиента. Если будет использован ключ, серийный номер которого не прописан в этой настройке, система скажет, что не нашла ключ (неверный ключ будет проигнорирован).
4. Перезапустите клиента АС «УРМ».

Рисунок 11 – Настройка параметров криптографии на РМ «Редактор настроек» клиента АС «УРМ»



В случае использования нескольких ЭП одним удаленным клиентом в поле Криптография\ Серийные номера сертификатов клиента должен быть через запятую указан перечень сертификатов, которыми может подписывать данный удаленный клиент (рисунок 12).

Рисунок 12 – Пример настройки использования нескольких ЭП одним удаленным клиентом



Обратите внимание, что все сертификаты, используемые удаленным клиентом для наложения ЭП, должны быть установлены как на клиенте АС «УРМ», так и на сервере обмена данными.

6.5. Настройка механизма штампов времени

Штампы времени – это механизм, который используется для подтверждения времени подписания.

Основой механизма штампов времени является *сервер штампов времени* или TSA (Time Stamp Authority). Это отдельная структура, которая занимается выдачей штампов и подтверждает их наличие и целостность их в случае юридических разбирательств.

Для получения штампа времени, клиент берет цифровую подпись и хэширует ее с помощью хэш-функции. Полученный хэш кодируется, и пересылается серверу. Сервер, добавляет к принятой информации свое текущее время, ряд вспомогательных атрибутов, и подписывает все это своей цифровой подписью. Полученный пакет сохраняется на сервере и отправляется клиенту.

Настройка TSA на клиенте УРМ производится на интерфейсе Редактор настроек в группе параметров Штампы времени (либо путем задания соответствующих параметров в секции [EDS] файла DSign.ini). На сервере настройка производится с помощью утилиты AdminUtil (пункты настроек аналогичны).

Таблица X – Параметры настройки сервера штампов времени

Название параметра	Параметр секции [EDS] DSign.ini	Значение поля
Сервер штампов времени (URL)	TSAHost	URL страницы, с которой ассоциирован сервер штампов времени. Например: http://ca.krista.ru/tsp/tsp.srf. Если данное поле не заполнено, то штампы времени считаются отключенными

Название параметра	Параметр секции [EDS] DSign.ini	Значение поля
Порт сервера штампов времени	TSAPort	Порт, через который идет подключение к серверу штампов времени (по умолчанию 80)
Прокси-сервер	Proxy	Используется только в том случае, если доступ к серверу штампов времени происходит с использованием Proxy-сервера, отвечающего за доступ в Интернет. Если сервер штампов стоит в локальной сети или у компьютера есть прямое подключение к Интернет, то данное поле должно оставаться пустым
Порт	ProxyPort	
Имя пользователя (proxy)	ProxyUserName	
Пароль пользователя (proxy)	ProxyPass	
Политика	TSAPolicy	OID-идентификатор, которому приписаны (в административном порядке) некоторые параметры (точность времени, принадлежность и т.д.). Предоставляется TSA. Например: 1.2.643.3.41.1.1.5
Алгоритм хэширования	TSAHash	Идентификатор алгоритма хэширования. В интерфейсах представляется в виде названия алгоритма, в ini-файле в виде OID. На данный момент допустимым значением является ГОСТ Р 34.11-94 (или OID 1.2.643.2.2.9)
Алгоритмы подписи сервера штампов	TSAAlgList	Список алгоритмов, которые могут использоваться при наложении подписи сервером штампов времени. Таких алгоритмов может быть несколько. На данный момент допустим алгоритм ГОСТ Р 34.10-2001

Возможны три схемы работы: без наложения штампов, с наложением штампов в момент подписания, с наложением штампов при промежуточной проверке, а также комбинация двух последних режимов:

- Без наложения штампов – в этом случае, штампы времени не накладываются. Для настройки такого режима необходимо указать пустые строки в параметре Сервер штампов времени на клиенте и на сервере УРМ.
- Наложение штампов в момент подписания – для наложения штампов в момент подписания, необходимо наличие доступа с подписывающей машины к серверу TSA (через Интернет или локальную сеть). Для работы в таком режиме необходимо настроить все конечные машины, указав настройки соединения и протокола. На сервере нужно указать пустой Сервер штампов времени.
- Наложение в момент проверки – в данном режиме, наложение штампа времени производится сервером УРМ в момент проверки подписи. Режим сделан для районов, в которых сложно или невозможно обеспечить выходом в Интернет всех конечных пользователей. В данном режиме, на клиенте штампы должны быть отключены (параметр Сервер штампов времени на клиенте должен быть пустым), а на сервере указаны необходимые настройки.
- Гибридный режим – в этом режиме необходима настройка сервера штампов на сервере и допустима на клиенте. В таком режиме, сервер будет проверять наличие штампа времени и накладывать свой штамп только при отсутствии штампа, наложенного пользователем.

6.6. Настройка OCSP

Протокол OCSP (Online Certificate Status Protocol) – протокол получения статуса сертификата в реальном времени, применяющийся для предоставления пользователям УЦ актуальной информации о статусах сертификатов ключей подписи.

Настройка OCSP на клиенте УРМ производится на интерфейсе Редактор настроек в группе параметров Сервер OCSP (либо путем задания соответствующих параметров в секции [EDS] файла DSign.ini). На сервере настройка производится с помощью утилиты AdminUtil (пункты настроек аналогичны).

Таблица X – Параметры настройки сервера OCSP

Название параметра	Параметр секции [EDS] DSign.ini	Значение поля
Сервер OCSP	OCSPHost	URL-адрес сервера OCSP (без префикса http://). Например: www.test.ru/ocsp.asp. Предоставляется владельцем используемого OCSP
Порт сервера OCSP	OCSPPort	Порт, через который идет подключение к серверу OCSP (по умолчанию 80). Без необходимости не менять. Если URL OCSP имеет вид www.test.ru:7878/ocsp.asp, то в поле Сервер OCSP прописывается URL без порта (www.test.ru/ocsp.asp), а в поле Порт сервера OCSP – номер этого порта (7878)
Прокси-сервер	OCSPProxy	Используется только в том случае, если доступ к серверу OCSP происходит с использованием прокси-сервера, отвечающего за доступ в Интернет
Порт	OCSPProxyPort	
Имя пользователя (proxy)	OCSPProxyUser	
Пароль (proxy)	OCSPProxyPass	
Алгоритм хэширования	OCSPHashAlgo	Используемый алгоритм хэширования (на данный момент – ГОСТ 34.11)
Сертификат сервера OCSP	OCSPServerCert	Серийный номер сертификата, которым сервер OCSP подписывает ответы. Номер вписывается без пробелов. Предоставляется владельцем используемого OCSP
Использовать OCSP при подписании	OCSPUseOnSign	Определяет необходимость проверки сертификата с помощью OCSP перед наложением подписи

Объектные идентификаторы (OID) определяют отношения, при осуществлении которых электронный документ, подписанный ЭЦП, будет иметь юридическое значение. Задание привил проверки OID в АС «УРМ» осуществляется на интерфейса Редактор настроек с помощью параметра Криптография\Правила проверки OID (либо с помощью параметра OIDCheck секции [EDS] файла DSign.ini.

Список OID задаётся в фигурных скобках, через запятую (OID в списке указываются в одинарных кавычках, через запятую). Каждый список может содержать несколько требующихся OID и несколько, которых не должно быть (знак ~ перед OID указывает на то, что данного OID не должно быть в списке OID в сертификате). Например, *OIDCheck={~'1.3.6.1.5.5.7.3.2'},{'1.2.643.3.41.1.3.4'}* – первого OID не должно быть в сертификате, второй должен быть.

Списку может быть задано (не обязательно) имя (только английскими буквами и цифрами, первым символом должна быть буква): *OIDCheck=GRBS1{'1.2.643.2.23.4',~'1.2.643.2.2.34.6'}Pbs{'1.3.6.1.5.5.7.3.4'}.*

Пример заданных настроек OCSP в файле DSign.ini:

[DIGITAL_SIGN]

Provider=EDS

[EDS]

…

OCSPHost=server.ocsp.ru

OCSPURL=/

OCSPPort=80

OCSPProxy=proxy.test.ru

OCSPProxyPort=8080

OCSPProxyUser=testuser

OCSPProxyPass=<5F5C5D5A5C5D>

OCSPHashAlgo=1.2.643.2.2.9

OCSPServerCert=610e0a8b000000012374

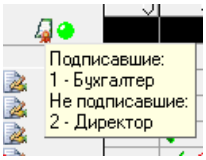
OCSPUseOnSign=ON

OIDCheck={'1.1.23.532.2.21.1'},{~'1234.123.4.2.1.234.'}

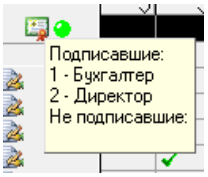
6.7. Настройка клиента АС «УРМ» для работы с множественной ЭП

Единственным отличием в настройках клиента УРМ для подписания документов несколькими ЭП является необходимость указать каталог для хранения пакетов с ЭЦП в редакторе настроек. Данный каталог должен быть доступен всем пользователям на запись. Если используется сетевая версия УРМ, то путь необходимо задать сетевой в формате ***\\ГоловнаяМашина\КаталогДляХраненияДокументовЭП***. В остальном настройки остаются прежние (указание криптопровайдера, установка флага-галочки Использовать ЭЦП, указание номеров открытых ключей).

При использовании схем подписания на интерфейсах ввода должна появиться кнопка **Подписать документы**. Чтобы подписать документы с помощью данной кнопки, необходимо их выделить, при этом среди выделенных документов должны быть записи, относящиеся к одной схеме подписания. Если среди выделенных есть документ(ы), неподлежащие подписанию, то процесс подписания будет отменен на всем пакете документов. Документы в интерфейсе ввода после первого подписания блокируются от изменений и отмечаются значком с соответствующим всплывающим сообщением:



После завершения схемы подписания сообщение будет выглядеть следующим образом:



Данные обозначения используются только для отображения процесса подписания и не сохраняются после проведения полной синхронизации.

Последнюю подпись по схеме можно наложить не только кнопкой, но и во время отсылки документов.

Перед каждым подписанием на клиенте УРМ автоматически производится проверка предыдущей подписи и проверка на возможность подписания данного документа в

соответствии со схемой. Например, если при наложении подписи вставлен ключ, не соответствующий сертификату, которым должны подписываться документы на данном этапе, то будет выведено соответствующее сообщение об ошибке.

При каждом подписании автоматически запускается бюджетный контроль (контроли на отправку), документы подписываются в случае успешного прохождения контроля.

В случае возникновения проблем (когда при наложении второй подписи первая подпись не будет признана подлинной, обнаружения ошибок в документах до отправки подписанных данных и т.п.) предусмотрена возможность откатить локальные подписи с помощью кнопки **Отменить локальные подписи**. Данная кнопка позволяет пользователю для выделенных документов откатывать любые локально наложенные (т.е. до отсылки) подписи.

Откат локальных подписей может потребоваться, если при использовании системы состояний после подписания документов, пришедших из АС Бюджет, выполнялась синхронизация.

При отправке документов на сервере УРМ проверяется корректность подписи и соответствие наложенных подписей схеме подписания в АС «Бюджет». Т.е., если в АС «Бюджет» была изменена схема подписания (например, в ней была изменена очередность подписания), и если на клиенте не была выполнена синхронизация, то при попытке отправить документы, они будут помечены красным восклицательным знаком с заполненной причиной сбоя.

При использовании ПМ «Прикрепление произвольных файлов» при наложении каждой подписи на документ, подписываются и все прикрепленные файлы. При этом в прикрепленном файле при проверке подписи в поле результат проверки ЭП указывается последняя подпись.

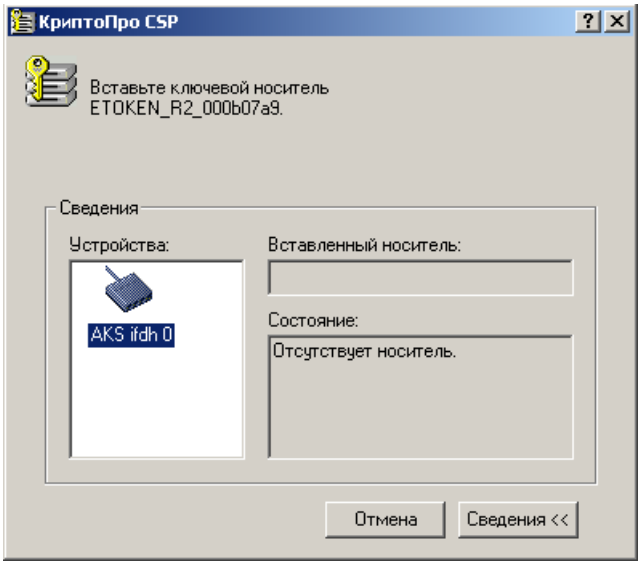
7. Работа с ЭП при передаче электронных документов из АС «УРМ» в АС «Бюджет»

7.1. Наложение ЭП в АС «УРМ»

Наложение ЭП на электронные документы при передаче из АС «УРМ» в АС «Бюджет» происходит автоматически при формировании блока данных для передачи в финансовый орган.

Ключевой носитель при этом должен быть подключен к станции. В случае отсутствия ключевого носителя при открытии ключевого контейнера система отобразит окно, сообщающее об отсутствии носителя (рисунок 13).

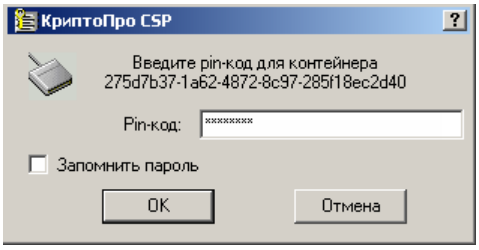
Рисунок 13 – Отсутствие необходимого носителя



В случае, когда необходимый ключевой носитель подключен, окно, сообщающее об отсутствии ключевого носителя, отображаться не будет.

После того, как необходимый носитель установлен, система потребует подтверждения пароля на доступ к закрытому ключу открываемого контейнера (рисунок 14).

Рисунок 14 – Окно ввода пароля на доступ к закрытому ключу



7.2. Проверка корректности ЭП при передаче электронных документов из АС «УРМ» в АС «Бюджет»

Первым звеном, выполняющим проверку корректности подписи документов, является сервер обмена данными. При получении документа, заверенного подписью, сервер всегда производит проверку подписи, которая производится в два этапа:

1. Проверяется корректность подписи на документе, пришедшем от удаленного клиента.
2. Проверяется, что документ подписан одним из тех ключей, которыми имеет право подписывать соответствующий удаленный клиент.

В случае, если сервер обмена не признает подпись подлинной, это ведет к ошибке обработки документа на сервере с простановкой у документа на клиенте соответствующей причины системного сбоя и, при использовании системы состояний, переводом в состояние «Отклонен». При этом документ не попадает в АС «Бюджет».

Если для удаленного клиента задан признак обязательности подписания документов, т.е. установлен флаг-галочка в поле Использовать подпись в интерфейсе Права удаленных клиентов РМ Администрирование УРМ (см. пункт 5.6 «Настройка АС «Бюджет» для работы с ЭП»), сервер

контролирует наличие подписи, и при отсутствии подписи автоматически отклоняет документ.

Таким образом, при соответствующей настройке, можно гарантировать, что документ, который пришел из АС «УРМ» не отклоненным, обязательно имеет подпись, которая принадлежит сотруднику данной организации и прошла проверку сервером обмена с положительным результатом.

Результаты автоматической проверки корректности ЭП на предметных интерфейсах АС «Бюджет» отражаются значками статуса документа (слева от таблицы заголовков):

-  **Документ имеет активную цифровую подпись** – означает, что на документ наложена ЭП, и она признана корректной. При этом ограничений по подписанным/ неподписанным документам на панели параметров интерфейса не предусматривается;
-  **Документ подписан, подпись признана недействительной** – означает, что на документ наложена ЭП, признанная некорректной, поэтому подписанный документ отклонен.

7.3. Особенности передачи документов с ЭП при наличии ПМ «Конвейерная обработка и множественное визирование документов»

При совместном использовании с ПМ «Конвейерная обработка и множественное визирование документов» возможна настройка схемы обработки с визированием главными распорядителями документов подведомственных получателей. В этом случае документ последовательно подписывается при отправке из АС «УРМ» сначала подведомственным получателем, а затем его главным распорядителем при установке соответствующей визы. Проверка подписи в АС «Бюджет» при использовании системы состояний производится автоматически при переводе документа в разрешенное состояние сотрудником финансового органа. Система извлекает все подписи удаленных клиентов для данного документа и проверяет их. Только в случае успешной проверки всех подписей удаленных клиентов производится подписание документа сотрудником финансового органа и перевод документа в следующее разрешенное состояние.

При реализации работы главных распорядителей бюджетных средств с использованием АС «УРМ» на распорядителя не возлагается функция проверки ЭП подведомственных. Эта функция возлагается на финансовый орган. При проверке ЭП финансовый орган требует наличия двух подписей для признания документа корректным и утвержденным главным распорядителем. Главный распорядитель в данном случае не видит подписи подведомственного, т.к. она доступна только сотрудникам финансового органа. Главный распорядитель имеет лишь косвенную информацию о наличии подписи подведомственного получателя: если сервер обмена корректно настроен и не отклонил документ, это означает, что подпись есть, и она корректна.

7.4. Возможные ошибки при работе с ЭП в АС «УРМ»

1. Сообщение «Данный сертификат не содержится в заданном хранилище» означает, что на станции АС «УРМ» не установлен личный сертификат с ключевого носителя.
2. Сообщение «Вставлен другой носитель» означает, что при настройке АС «УРМ» в поле Серийный номер сертификата клиента был неверно указан серийный номер сертификата клиента.

3. Сообщение «Сертификат не связан с ключевым контейнером» означает, что во время настройки и установки ЭП был неверно определен алгоритм подписания в СКЗИ «КриптоПро CSP» и АС «УРМ». Проверьте правильность значений: для СКЗИ «КриптоПро CSP» – «Crypto-Pro GOST R 34.10-2001 Cryptographic Service Provider», для АС «УРМ» – «ГОСТ Р 34.10-2001».

8. Работа пользователя с ЭП в АС «Бюджет» при совместном использовании с ПМ «Конвейерная обработка и множественное визирование документов»

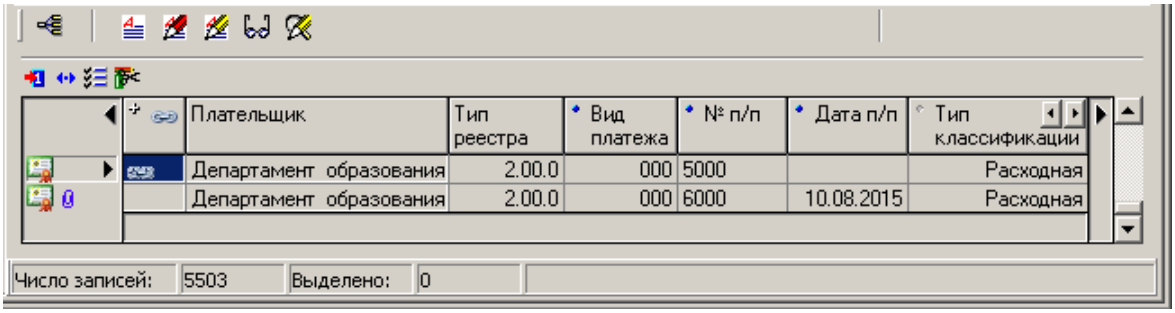
8.1. Инструменты для работы с ЭП в АС «Бюджет»

При наличии ПМ «Конвейерная обработка и множественное визирование документов» для работы с ЭП на предметных интерфейсах действуют следующие кнопки управления (рисунок 15):

- **Простановка цифровой подписи (принудительно)** – служит для принудительного наложения на документ электронной подписи;
- **Простановка цифровой подписи** – служит для наложения на документ электронной подписи, если последний совершенный переход над документом требовал подписания;
- **История изменений состояний** – вызывает окно «История изменения состояний у документов», в котором отображается информация о переходах, состояниях и клиентах, которые осуществляют эти переходы и подписывают документ (накладывают ЭП) на разных стадиях его обработки;
- **Проверка цифровой подписи** – проводит проверку наложенной электронной подписи.

Для предметного интерфейса активными кнопки становятся только после установки флагов-галочек в полях Исп. состояния и ЭЦП для документа соответствующего типа на интерфейсе Типы документов РМ Администратор состояний.

Рисунок 15 – Вид интерфейса, на котором используется система состояний и ЭП

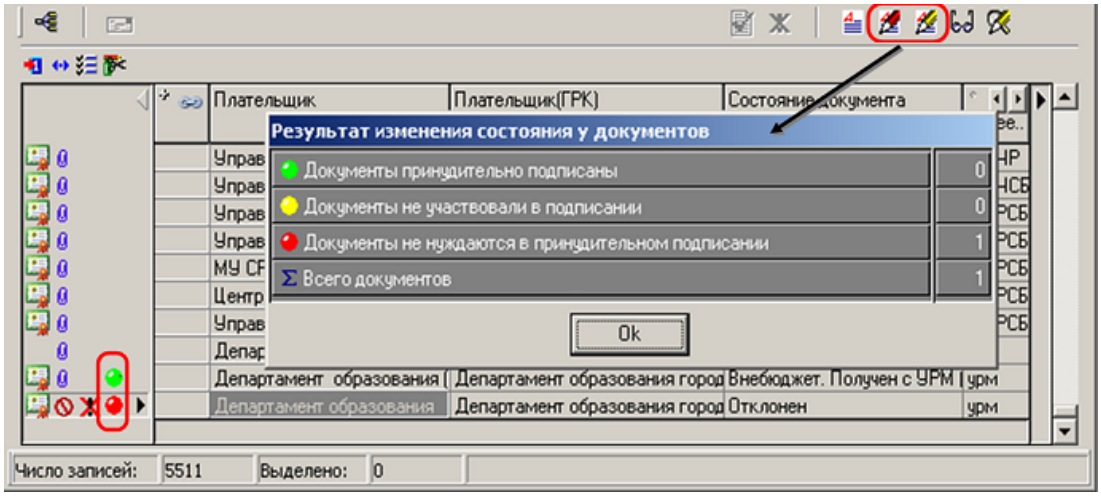


8.2. Наложение электронной подписи в АС «Бюджет»

Моменты наложения электронной подписи задаются при настройке схемы обработки документов. Для наложения на документ электронной подписи при переводе в соответствующее состояние служит кнопка управления **Простановка цифровой подписи** (рисунок 16). При нажатии на эту кнопку будет производиться предварительная проверка корректности ЭП и запрос PIN-кода к секретному ключу для наложения подписи. После

успешного наложения электронной подписи документ примет состояние Принят. Если необходимо подписать одновременно несколько документов, сначала выделите все необходимые к подписанию документы и только затем нажмите кнопку **Простановка цифровой подписи**.

Рисунок 16 – Вид информационного окна с результатами изменения состояния у документов в АС «Бюджет»



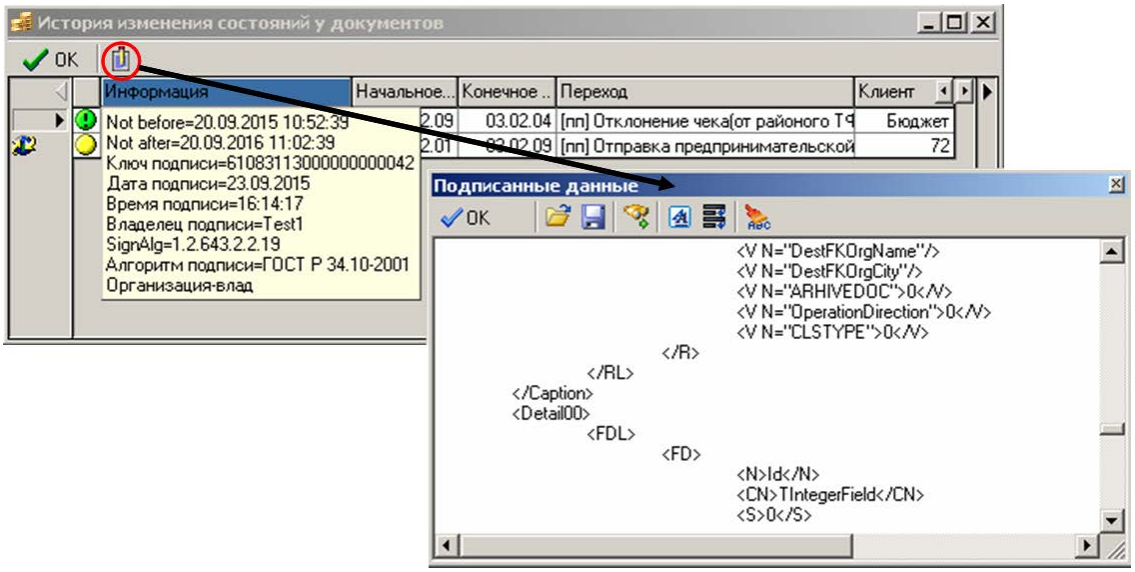
Перед подписанием документа автоматически проверяется предыдущая ЭП, наложенная на этот документ, или все ранее наложенные ЭП, если документ получен от удаленного клиента.

Кнопка **Простановка цифровой подписи (принудительно)** служит для наложения на документ электронной подписи в ходе последнего активного перехода. Такая необходимость возникает в случае наложения ЭП на документ, находящийся уже на стадиях переходов, при неавтоматизированном введении в работу системы ЭП. Подписание должно осуществляться после проверки переходов документа в окне «История изменений состояний у документов».

8.3. Просмотр истории изменения состояний документа и наложения ЭП в АС «Бюджет»

На каждом предметном интерфейсе с установленной системой состояний имеется дополнительная кнопка управления **История изменений состояний**, при нажатии на которую появляется окно «История изменений состояний у документов» с информацией о переходах, начальном и конечном состояниях, ЭП и пользователях, которые осуществляли эти переходы и подписание документа (рисунок 17).

Рисунок 17 – Окно просмотра истории изменений состояний у документов



В поле Информация для каждого перехода может быть указано одно из следующих значений:

- – ЭП не активная;
- – ЭП активная (т.е. та, с которой сравниваем текущее состояние);
- – ЭП отменена при обратном переходе;
- – ЭП обратного перехода;
- – ЭП не найдена;
- – все прочие ошибки.

В случае, когда на текущий интерфейс АС «Бюджет» из АС «УРМ» приходит документ, заверенный электронной подписью, слева от записи о состоянии ЭП появляется значок **Документ получен от удаленного клиента**, а также в полях Клиент и Пользователь указываются код удаленного клиента и логин пользователя, под которым сервер обмена данными подключается к базе АС «Бюджет».

Поле Информация не будет заполнено для тех переходов, в ходе которых ЭП на документ не накладывается.

Кнопка **Показать данные документа** окна «История изменений состояний у документов» позволяет просмотреть XML-документ в текстовом виде для каждой из стадий обработки.

На электронный документ может быть последовательно наложено несколько ЭП (одна ЭП на каждый переход). Из всего количества подписей, наложенных на электронный документ, активной является только одна – последняя. При дальнейшей обработке документа и наложении ЭП осуществляется проверка только последней (активной) подписи. После наложения новая ЭП становится активной, а предыдущая ЭП – неактивной.

В случае, когда документ подписан несколько раз, проверяется активная (последняя неотмененная) подпись, подписание документа может быть отменено руководителем или администратором системы. Исключением является ситуация, когда активной подписью является подпись АС «УРМ». Работа с ЭП в АС «УРМ» отличается от работы с ЭП в АС «Бюджет» тем, что в АС «УРМ» нет хранилища данных ЭП, а значит и сравнение с предыдущей электронной подписью не производится. Несколько пользователей АС «УРМ»

последовательно подписывают документ (распорядители, получатели), не видя, при этом, подписей друг друга. Макросы обработки АС «УРМ» существенно отличаются от тех, которые используются у АС «Бюджет». Основная их задача – формирование пакета документов и подписей, их отсылка и получение ответа, отображение изменений на интерфейсе клиента АС «УРМ». Поэтому в случае, когда активной подписью является подпись АС «УРМ», выполняется проверка всех подписей АС «УРМ».

Если в ходе работы электронная подпись оказывается неверна, ее отменяют (делают неактивной). Исходными данными при отмене подписания документов является коллекция параметров, в которой содержатся: список первичных ключей и состояние, в которое переходит документ.

Подпись обратного перехода требуется при доработке документа в случае возврата документа на предыдущий этап работы. Это означает, что последняя активная ЭП перестает действовать (становится неактивной), а активной становится подпись, которая была активна на момент совершения прямого перехода в состояние, объявленное как конечное для обратного перехода. Наложение подписи обратного перехода будет уместно в случае проставленного у перехода флага-галочки Обратный на интерфейсе Типы документов РМ Администратор состояний.

Признак подписи, пришедшей из АС «УРМ», необходим, потому что при наложении ЭП в АС «УРМ» проверка подписей не осуществляется (при переходе документа от ПБС к ГРБС и ТПФО). При наложении первой ЭП в АС «Бюджет» (после получения подписанного документа из АС «УРМ») надо проверить всю цепочку ранее произведенных подписей.

8.4. Проверка корректности электронной подписи в АС «Бюджет»

Помимо автоматического, предусмотрен ручной режим проверки корректности наложенной на документ ЭП с помощью кнопки управления **Проверка цифровой подписи** в предметных интерфейсах. Если необходимо проверить сразу несколько документов, то нужно выделить все необходимые документы и нажать кнопку управления **Проверка цифровой подписи**.

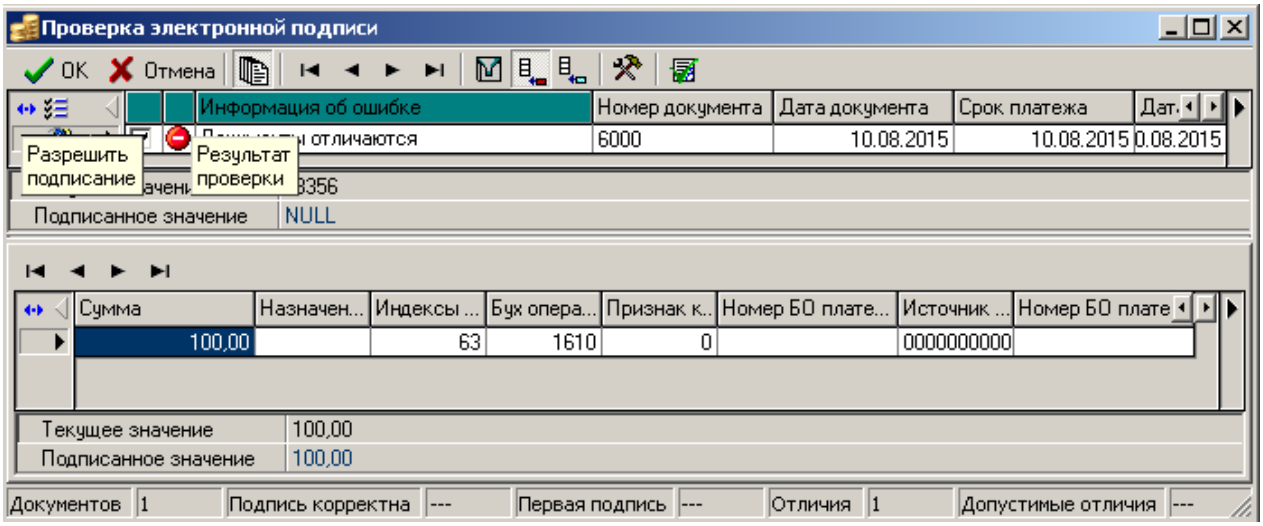
При проверке корректности ЭП производится проверка ЭП подписанного документа и сравнение текущей и подписанной версий документов (текущая версия документа хранится в базе данных АС «Бюджет», подписанная версия – в хранилище данных ЭП).

Результат проверки выводится в окне «Проверка электронной подписи» (рисунок 18). Окно разделено на две части: в верхней части выводятся заголовки документов, в нижней – записи детализации. Кнопки **ОК** и **Отмена** закрывают окно. При проверке корректности ЭП они работают одинаково. При подписании нажатие на них соответственно либо подтверждает наложение ЭП, либо отменяет его. На главной панели кнопок управления расположены кнопки, помогающие работать с документами при проверке корректности ЭП:

- Стандартный навигатор с кнопками перемещения по таблице данных;
- **Просмотр детализаций/Просмотр заголовков** – для включения и отключения режима просмотра таблицы;
- **Показывать только документы не прошедшие проверку/Показывать все документы** – фильтр по результату проверки;
- **Скрывать системные поля/Показывать все поля** – фильтр по полям;
- **Не показывать одинаковые поля/Показывать все поля** – фильтр по значениям;
- **Настройки показа отличий** – настройка условий фильтрации записей по степени допустимости отличий;

- **Отметить все документы, для которых возможно подписание** – для автоматической установки флагов-галочек в поле Разрешить подписание для документов, на которые можно наложить ЭП (доступна только в режиме подписания).

Рисунок 18 – Окно «Проверка электронной подписи»



В таблицах данных, расположенных в рабочей области, отображаются данные о выбранных документах, а также некоторая служебная информация. К служебной информации относятся следующие поля:

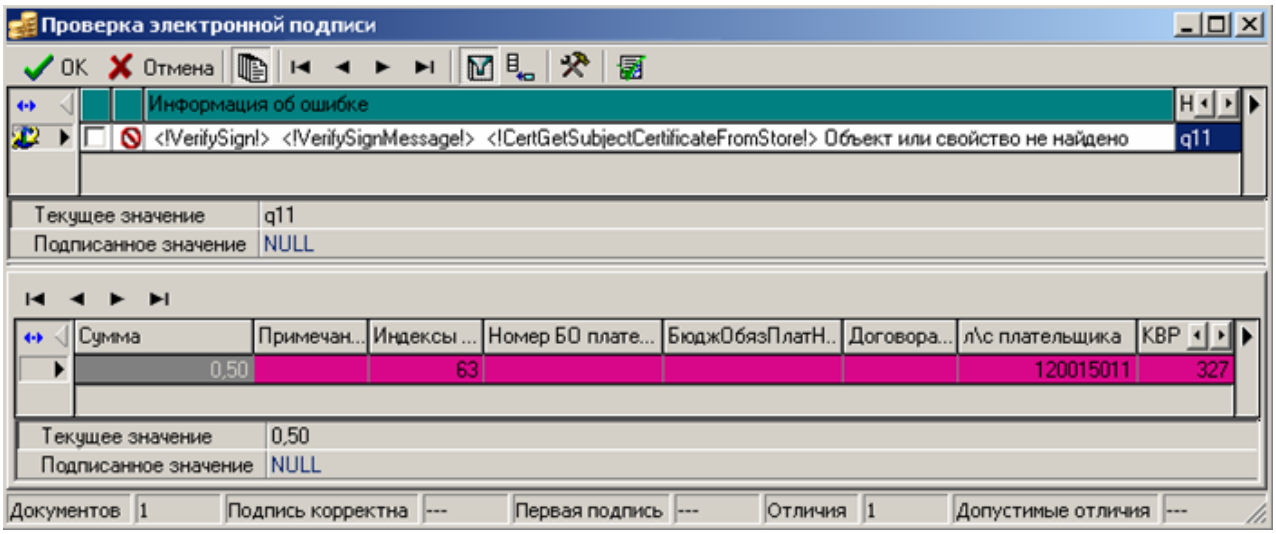
- Результат проверки, в котором, в виде значка, указан результат проверки подписи и сравнения данных. Для значков использована следующая цветовая индикация: красный – есть ошибки и подписание невозможно, желтый – есть ошибки, но возможно подписание, зеленый – проверка прошла успешно, подписание возможно;
- Разрешить подписание, в котором можно отметить документ для его перевода в последующее состояние. Все корректные документы автоматически помечаются при показе формы путем установки флага-галочки. Данное поле будет отображаться только для второго режима работы модальной формы и только для таблицы данных заголовков;
- Поля с дополнительной информацией о пользователе, подписавшем документ, и о дате подписания (только для таблицы данных заголовков).

Ниже таблиц с данными располагаются две строки с информацией соответствующей текущему полю: значение, выбранное из базы данных (Текущее значение), и значение из хранилища данных ЭП (Подписанное значение).

При просмотре таблиц данных допускается просмотр данных в «развернутом виде», то есть в режиме отображения только одной, текущей записи. Переключение между режимами отображения осуществляется с помощью кнопки-переключателя **Вид**, расположенной рядом с соответствующей таблицей данных. В «развернутом виде» вместо двух колонок (как это принято на стандартных интерфейсах АС «Бюджет»: название и значение), выводится 3 колонки – название поля, значение поля в базе данных и значение поля в хранилище данных ЭП, что предоставляет удобство визуального сравнения значений полей. При переключении в режим просмотра заголовок-детализация таблица заголовка будет отображаться только в «развернутом виде».

На рисунке 19 представлен результат проверки, который выводится, если сертификат, соответствующий подписи документа, не найден.

Рисунок 19 – Результаты проверки, отраженные в форме проверки электронной подписи



Возможны следующие значения результата проверки:

- – ЭП корректна;
- – предыдущая ЭП не найдена, но она и не требуется;
- – предыдущая ЭП не найдена, хотя должна быть;
- – ЭП неверна или не удается прочитать данные подписанного документа;
- – есть различия в подписанном и текущем документе, но они не критичны;
- – есть различия в подписанном и текущем документе, и они критичны; может быть ошибка при проведении проверки бюджетного контроля;
- – неверна предыдущая ЭП при проверке корректности подписи АС «УРМ».

9. Возможности совместного использования с ПМ «Прикрепление к документам произвольных файлов с ЭП»

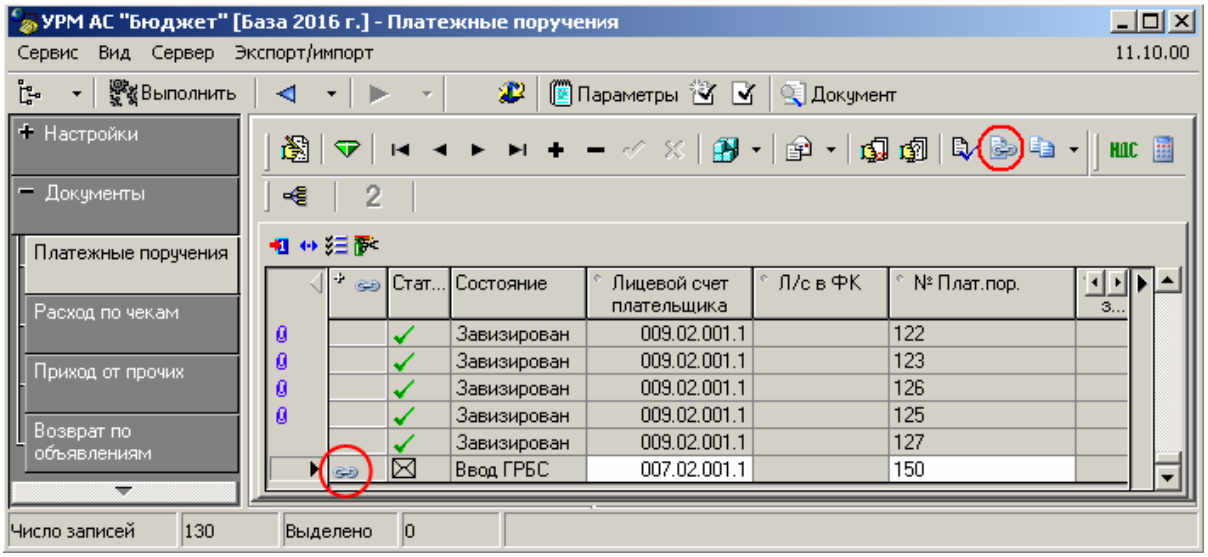
Наличие ПМ «Применение ЭП в АС «Бюджет» и АС «УРМ» и настроенной системы криптографии является необходимым условием функционирования дополнительного ПМ «Прикрепление к документам произвольных файлов с ЭП». Совместное использование указанных ПМ обеспечивает возможность доставки подтверждающих и других документов от главных распорядителей и получателей бюджетных средств в финансовый орган в электронном виде с использованием ЭП, с привязкой к конкретному электронному документу.

Подтверждающие возникновение и правомерность денежного обязательства документы преобразуются в электронный вид путем сканирования изображений либо берутся из файла на диске, после чего прикрепляются к платежным документам АС «УРМ», заверяются ЭП и отсылаются в финансовый орган в АС «Бюджет». Применение ПМ «Прикрепление к документам произвольных файлов с ЭП» позволяет прикреплять к одному первичному документу произвольное число файлов любого формата с диска (документы Microsoft Office, Open Office, pdf-документы и др.) и файлы изображения, получаемые со сканера непосредственно из АС «УРМ».

Передача прикрепленных файлов из АС «УРМ» удаленного клиента в АС «Бюджет» финансового органа производится автоматически при отсылке соответствующих первичных документов.

В АС «УРМ» прикрепление произвольных файлов к первичным документам производится в предметном интерфейсе при вводе соответствующего электронного документа. На каждом интерфейсе, для которого поддерживается механизм прикрепления файлов (РМ Документы, Работа с ФК, Санкционирование, др.), находится кнопка управления **Привязать файл к документу** для вызова модальной формы, предназначенной для работы с прикрепленными файлами.

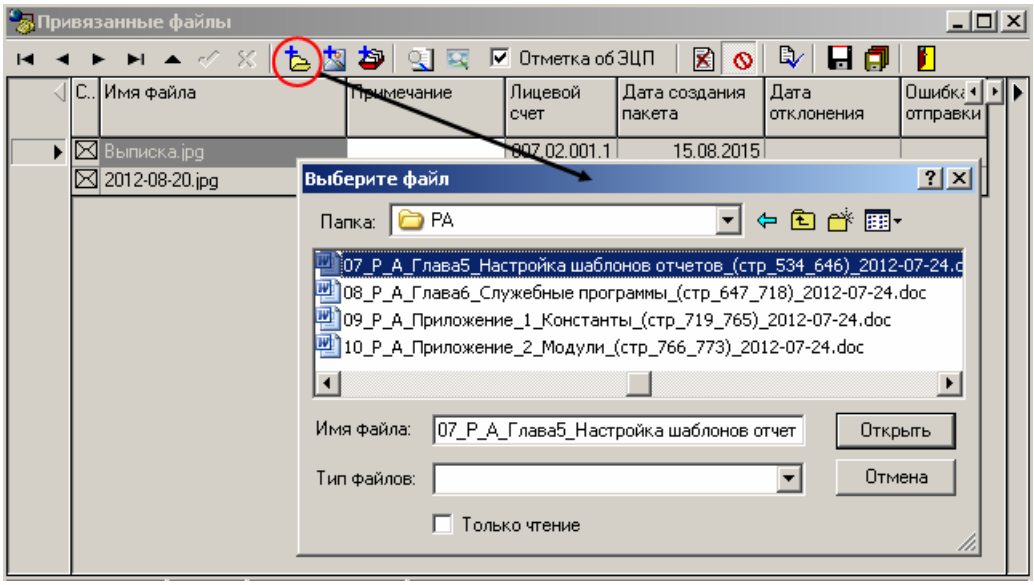
Рисунок 20 – Вид рабочей области интерфейса «Платежные поручения» АС «УРМ» с документом, содержащим прикрепленные файлы, и кнопкой «Привязать файл к документу»



Каждый документ АС «УРМ», для которого имеются прикрепленные файлы, помечается иконкой в поле статуса записи. Все операции с прикрепленными файлами (прикрепление произвольного файла, получение файла изображения со сканера и прикрепление к документу, просмотр прикрепленного файла, просмотр файла изображения, проверка корректности ЭП, др.) выполняются с помощью функциональных кнопок управления модальной формы.

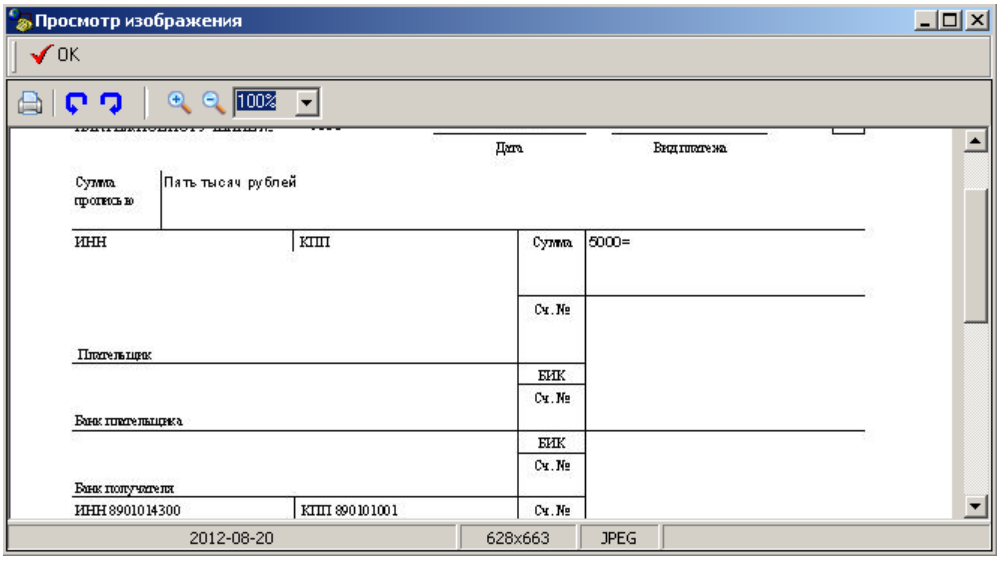
Выбор файла для прикрепления, сохраненного на диске, производится в ходе стандартного диалога выбора файла, вызванного нажатием кнопки.

Рисунок 21 – Вид модальной формы «Привязанные файлы» и стандартного диалога выбора файла для прикрепления



Получение файла изображения с бумажного оригинала с помощью сканера и прикрепление его к документу производится после нажатия на кнопку модальной формы и запуска процедуры сканирования непосредственно из интерфейса АС «УРМ». Сама операция сканирования очень проста и не требует от пользователя никаких специальных навыков. При ее выполнении согласно заданным настройкам производится автоматическое преобразование глубины цвета и разрешения отсканированного изображения с целью получения минимального объема файла данных при сохранении удовлетворительного качества изображения.

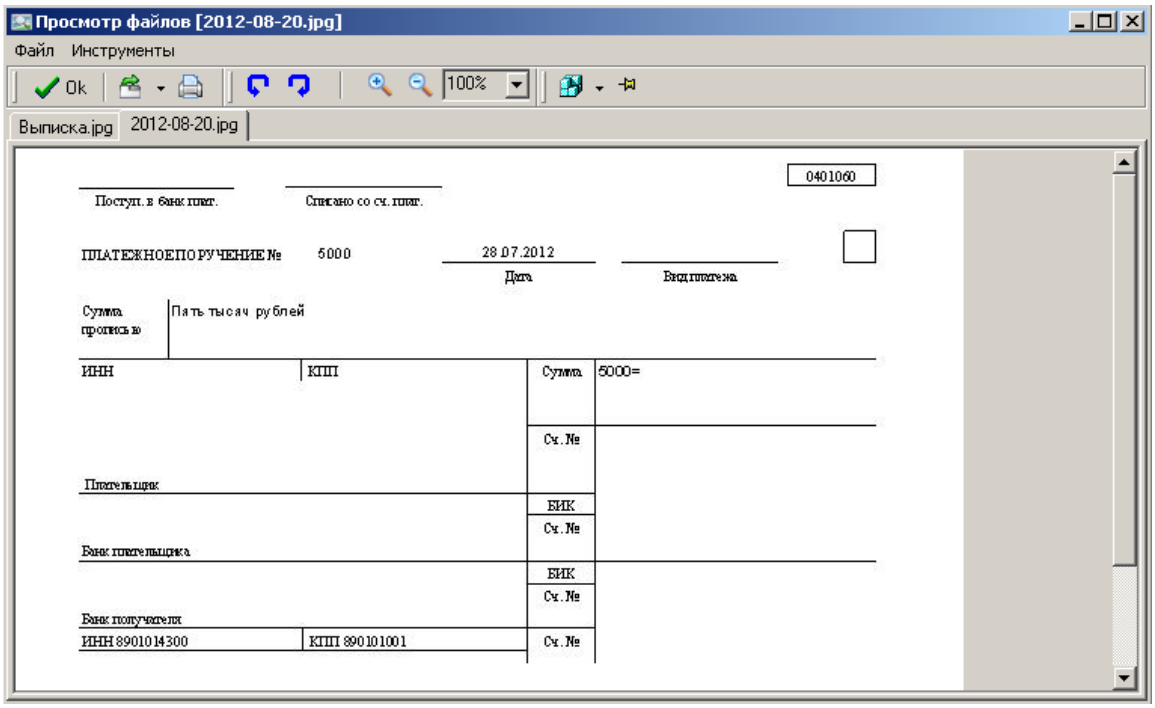
Рисунок 22 – Вид встроенной формы просмотра отсканированного изображения



Обеспечивается возможность просмотра одного прикрепленного файла с вызовом формы просмотра изображения или соответствующего файлу приложения. Также возможен одновременный просмотр файлов изображений в отдельной форме просмотра с

необходимым количеством закладок, где можно отредактировать масштаб изображения, развернуть его нужным образом, настроить параметры печати и распечатать.

Рисунок 23 – Вид специализированной формы просмотра файлов изображений, вызываемой с помощью кнопки управления из модальной формы с прикрепленными файлами

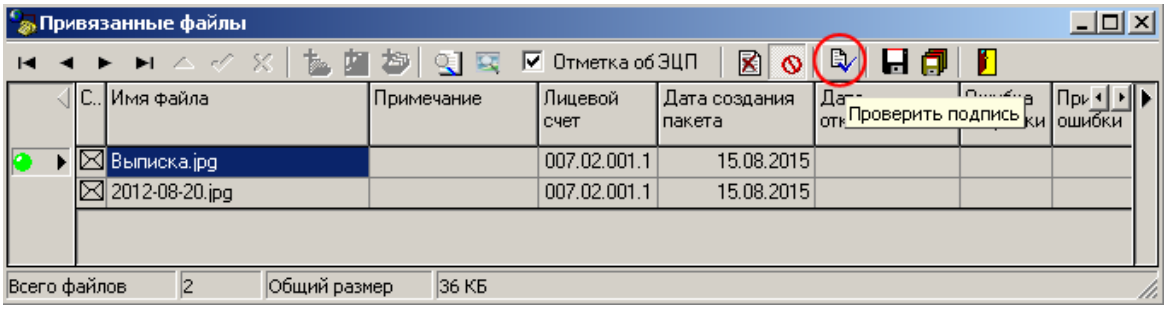


Удаление файла из списка прикрепленных к документу файлов с помощью кнопки модальной формы возможно только в том случае, если первичный документ еще не был передан в финансовый орган.

Автоматическая проверка подлинности ЭП производится сервером обмена данными на стороне финансового органа при передаче документов с прикрепленными файлами из АС «УРМ» в АС «Бюджет». Документы с некорректной ЭП не попадают в АС «Бюджет» и возвращаются в АС «УРМ» с указанием ошибки обработки.

Проверка корректности ЭП на прикрепленных файлах в ручном режиме производится в модальной форме с помощью кнопки управления. Результаты проверки ЭП отображаются в модальной форме в виде цветных шаров индивидуально для каждого прикрепленного файла.

Рисунок 24 – Вид формы просмотра и прикрепления файлов с результатами проверки корректности ЭП на прикрепленных файлах

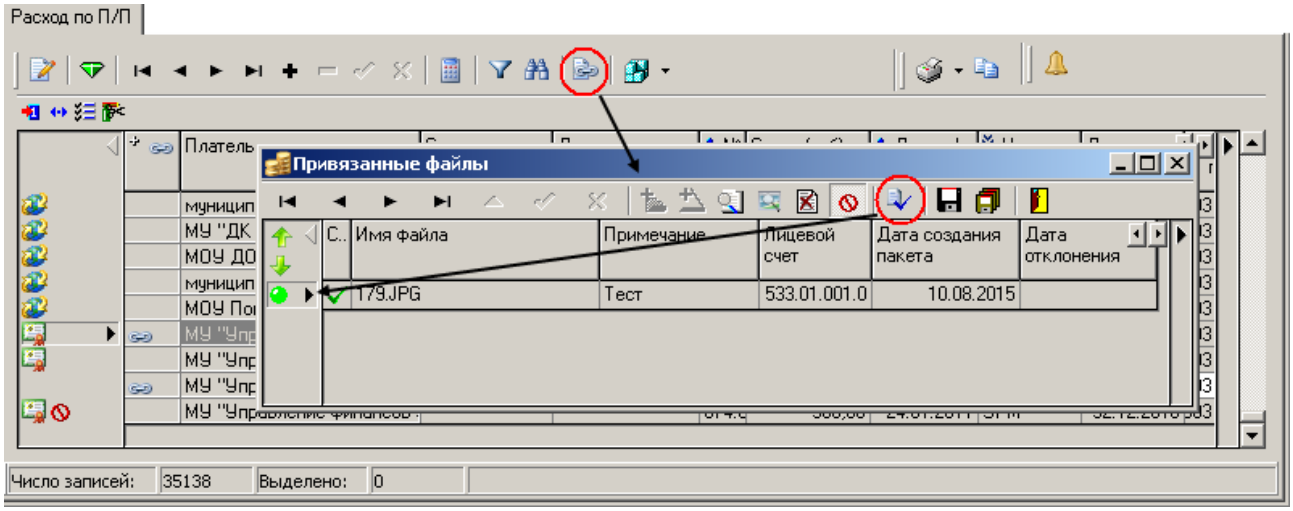


Сохранение любого прикрепленного файла из базы данных в файл соответствующего формата по указанному пути производится при помощи кнопки управления формы. Также возможно сохранение всех прикрепленных файлов в выбранный каталог на диске.

Пользователь АС «УРМ» в любой момент может посмотреть файлы, прикрепленные к документу (при наличии прав). Прикрепление файлов к электронным документам может производиться и на последующих стадиях обработки документов (при обработке по схеме состояний, при наличии ПМ «Конвейерная обработка и множественное визирование документов»). Для этого электронный документ должен быть возвращен на обработку соответствующему удаленному клиенту (ГРБС, ПБС). В тот момент, когда пользователь имеет право редактировать электронный документ, он также имеет право прикреплять к нему файлы.

В АС «Бюджет» полученные из АС «УРМ» платежные документы с ЭП, имеющие прикрепленные файлы, отражаются на соответствующих предметных интерфейсах и отмечаются иконкой в поле статуса записи. Специалист ФО может просмотреть перечень и содержание прикрепленных к документу с ЭП приложенных изображений подтверждающих документов и других электронных файлов в модальной форме просмотра, аналогичной по виду и возможностям форме из АС «УРМ, а также выполнить необходимые операции над прикрепленными файлами: сохранить на диск в файлы соответствующего им формата, проверить корректность ЭП и др. При положительных результатах проверки специалист ФО переводит документ в соответствующее состояние, при необходимости накладывая свою ЭП, тем самым отправляя документ на следующий этап маршрута обработки.

Рисунок 25 – Вид интерфейса АС «Бюджет» с кнопкой «Прикрепить файлы» после проверки наложенной ЭП на прикрепленный к документу файл



В отдельных предметных интерфейсах АС «Бюджет» (при наличии прав) также возможно прикрепление файлов к документам, которое осуществляется в модальной форме, вызываемой нажатием на кнопку управления **Прикрепить файлы** и аналогичной форме АС «УРМ». В ней можно расширить перечень файлов, прикрепленных к документу, полученному из АС «УРМ», добавив файлы с диска или получив файл изображения с помощью сканера и прикрепив его к документу, далее выполнить над ними все операции, аналогичные операциям формы АС «УРМ», а также отфильтровать перечень отображаемых файлов, исключив отклоненные.

Кроме того, в этой модальной форме можно аналогичным образом прикрепить файлы к документу, созданному в АС «Бюджет», и выполнить над ними весь перечень доступных операций. Пользуясь настройками системы прав АС «Бюджет», можно разграничить полномочия по работе с прикрепленными к документу с ЭП файлами: различные специалисты ФО могут прикреплять, откреплять файлы и отклонять первичный документ с прикрепленными файлами.

10. Возможности совместного использования с ПМ «Передача выписок с ЭП из АС «Бюджет» в АС «УРМ»

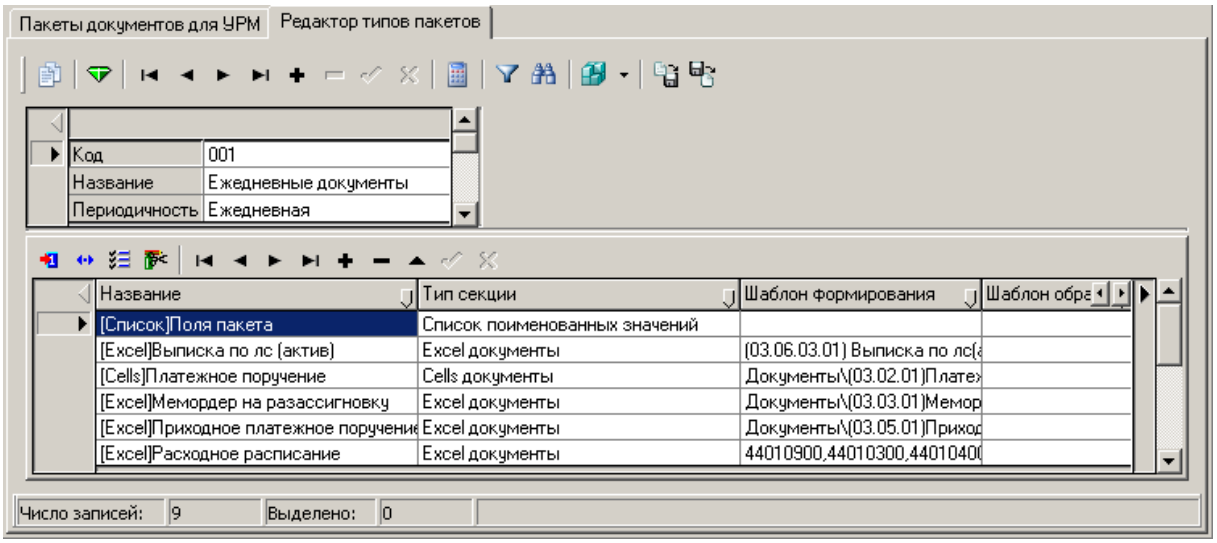
Наличие ПМ «Применение ЭП в АС «Бюджет» и АС «УРМ» и настроенной системы криптографии является необходимым условием функционирования дополнительного ПМ «Передача выписок с ЭП из АС «Бюджет» в АС «УРМ». Совместное использование указанных ПМ обеспечивает финансовому органу возможность предоставления главным распорядителям и получателям информации о проведенных по их лицевым счетам операциях, заверенной ЭП, путем формирования и передачи в АС «УРМ» электронных пакетов документов с ЭП.

В состав формируемого в АС «Бюджет» электронного пакета с ЭП могут входить:

- сводные документы, формируемые на основании первичных документов, в формате XLS (Microsoft Excel) или CLL (Krista Cells). Как правило, это выписка по лицевому счету, содержащая все остатки и обороты по лицевому счету за операционный день;
- проведенные первичные документы по лицевому счету за операционный день в формате XLS или CLL;
- файлы произвольного формата, используемые для доведения различной организационно-распорядительной документации.

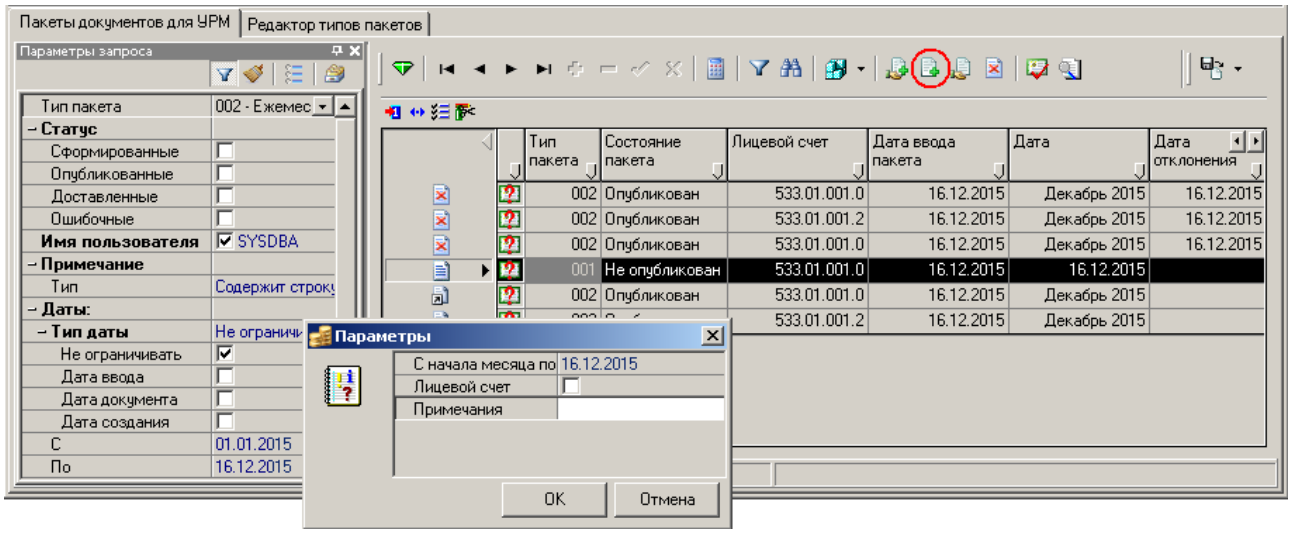
В АС «Бюджет» выполняется предварительная настройка различных типов пакетов с нужными атрибутами (периодичностью формирования, типом обработки, др.) и перечнем включаемых в них документов для передачи в АС «УРМ», а также назначаются права удаленным клиентам на получение пакетов с ЭП определенных типов по доступным им согласно иерархии лицевым счетам.

Рисунок 26 – Вид интерфейса «Редактор типов пакетов» АС «Бюджет»



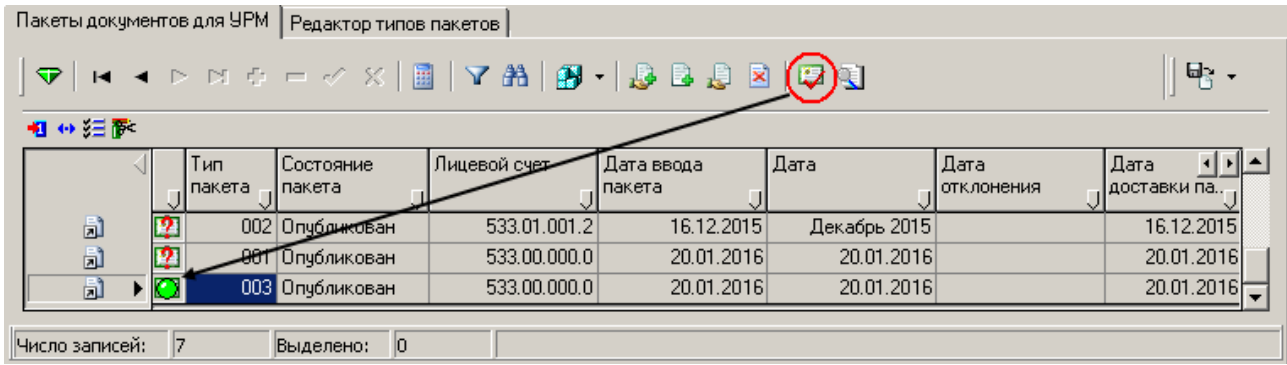
В АС «Бюджет» работа с пакетами с ЭП различных типов производится на интерфейсе Пакеты документов для УРМ дополнительного РМ Обмен пакетами с УРМ. В зависимости от требований, могут быть сформированы пакеты на заданную дату или период по одному лицевому счету, группе лицевых счетов, либо по всем лицевым счетам удаленных клиентов. На стороне финансового органа (АС «Бюджет») электронные документы в xml-формате, ЭП и служебные данные подписанного документа сохраняются в специальном хранилище подписанных документов, которое представляет собой отдельную базу данных.

Рисунок 27 – Вид интерфейса «Пакеты документов для УРМ» АС «Бюджет» с вызванным окном диалога для выбора параметров формирования пакета



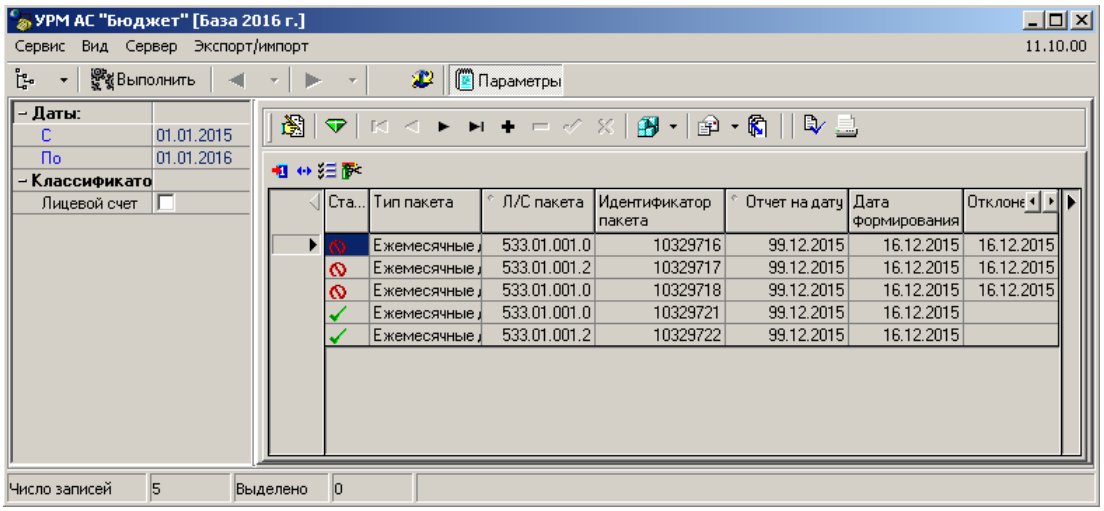
Подписание пакета ЭП производится автоматически при его формировании, при этом имеется возможность просмотреть содержимое пакета и включенных в него отчетных форм, первичных документов, других файлов перед наложением ЭП. Также можно проверить подлинность ЭП на пакете электронных документов, изменить состояние пакета, отклонить его, включить в пакет с ЭП файлы произвольного формата для лицевого счета удаленного клиента или выполнить массовую рассылку файлов. Обеспечивается возможность переформирования ошибочных пакетов и отправки нескольких подписанных ЭП пакетов по одному лицевому счету в течение дня, при этом в целях сохранения достоверности информации изменение и удаление ошибочных пакетов не допускается, действительным будет считаться только последний сформированный пакет.

Рисунок 28 – Вид интерфейса «Пакеты документов для УРМ» АС «Бюджет» с результатом проверки ЭП на пакете документов



В АС «УРМ» работа с пакетами документов с ЭП производится на интерфейсе Пакеты с ЭЦП. Получение электронных пакетов клиентами финансового органа производится в процессе синхронизации с АС «Бюджет» согласно назначенным правам. При доставке в АС «УРМ» пакет документов с ЭП не изменяется и содержит те же секции, что и в АС «Бюджет». Пакет электронных документов, наложенная на него ЭП, служебные данные подписанного документа сохраняются в виде единого файла в специальном каталоге, имеющем иерархическую структуру подкаталогов (по месяцам, по датам месяца).

Рисунок 29 – Вид интерфейса «Пакеты с ЭЦП» АС «УРМ»



Специалисты ТПФО, ГРБС и ПБС на своем удаленном рабочем месте могут проверить подлинность ЭП на полученном пакете, просмотреть его содержимое и распечатать выбранные документы с проставлением специальной пометки, означающей, что документ заверен ЭП, и она признана подлинной. Кроме того, можно произвести выгрузку доставленного пакета и его ЭП в выбранный системный каталог в виде отдельных файлов.

Таким образом, главные распорядители и получатели в электронном виде получают выписки из лицевых счетов и проведенные первичные документы, на основании которых они могут отражать операции в бюджетном учете.

11. Утилита для работы администратора с хранилищем документов с ЭП (AdminSign.exe)

AdminSign.exe – утилита для работы администратора безопасности с хранилищем документов с ЭП, использование которой позволяет:

- просматривать хранилище подписанных документов;
- производить поиск нужных записей;
- осуществлять выгрузку подписанных электронных документов и ЭП из хранилища в файловую систему для решения спорных вопросов;
- удалять данные из криптобазы;
- производить проверку корректности ЭП;
- сравнивать атрибуты электронных документов;
- производить синхронизацию данных криптобазы и базы данных АС «Бюджет».

11.1. Запуск утилиты AdminSign.exe

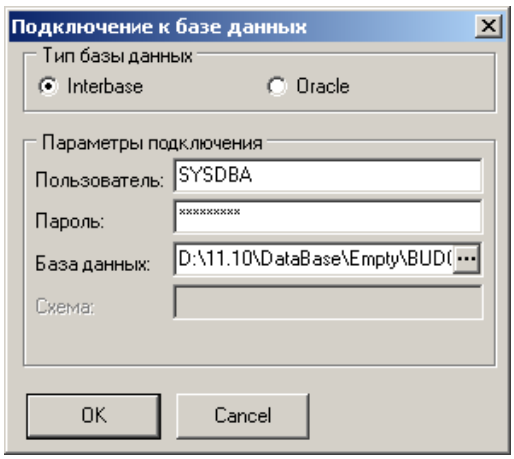
Запуск утилиты AdminSign.exe производится со стороны финансового органа, в котором установлена АС «Бюджет», и может быть осуществлен 2 способами: из каталога OCX или напрямую из первичного интерфейса АС «Бюджет» для просмотра/проверки ЭП платежных поручений.

❖ **Запуск из каталога OCX**

Запуск утилиты может производиться путем вызова программы **AdminSign.exe**, которая обычно размещается в папке **\\SERVER\BudgetAx\Ocx**. В этом случае, прежде чем пользователь войдет в программу и получит доступ к криптобазе, он должен пройти регистрацию. Для этого служит окно «Подключение к базе данных» со следующими полями:

- Тип базы данных – тип базы криптографических данных (Interbase или Oracle);
- Пользователь – имя пользователя для работы в АС «Бюджет»;
- Пароль – пароль пользователя, установленный администратором системы при регистрации в СУБД (Firebird, Oracle);
- База данных – строка подключения к криптобазе, соответствующая используемой СУБД;
- Схема – схема БД (при работе с БД Oracle).

Рисунок 30 – Вид окна «Подключение к базе данных»



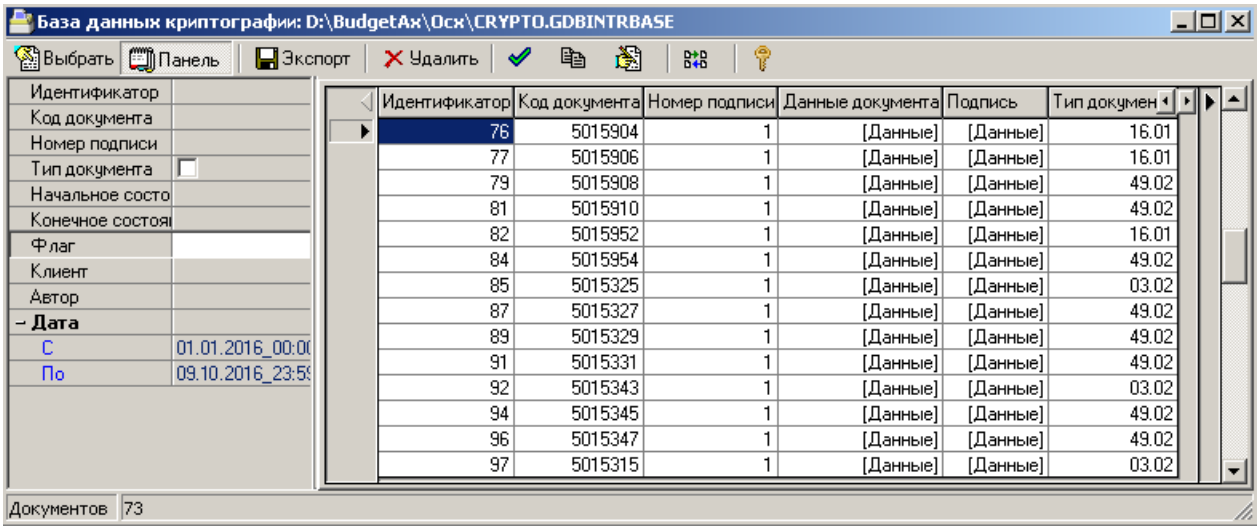
❖ **Запуск из интерфейса АС «Бюджет»**

В интерфейсе Расход по п\п РМ Казначейство обеспечивается возможность проверки ЭП у текущей версии платежного документа и сравнения ее с версией, подписанной ЭП и сохраненной в хранилище данных ЭП, путем вызова утилиты AdminSign.exe непосредственно из самого интерфейса с помощью специальной кнопки управления **Показать подписи документа**.

11.2. Вид окна утилиты

В верхней части окна утилиты расположена строка заголовка, в которой указывается путь до файла базы данных. Ниже заголовка расположена панель кнопок управления. Основную часть окна занимают панель параметров (слева) и рабочая область утилиты.

Рисунок 31 – Вид окна утилиты AdminSign.exe



❖ Панель кнопок управления

Панель кнопок управления содержит следующие кнопки:

- Выбрать **Выбрать данные подписей** – служит для выбора из базы данных и отображения в рабочей области утилиты записей, удовлетворяющих условиям, заданным на панели параметров запроса;
- Панель – позволяет отобразить/скрыть в рабочей области панель параметров запроса, где задаются условия выборки информации;
- Экспорт **Экспортировать данные** – служит для сохранения документа и ЭП из криптобазы в файловую систему на диск в указываемый каталог;
- Удалить **Удаление данных по датам** – служит для удаления данных из криптобазы;
- **Проверить корректность подписи** – производит проверку наличия и корректности ЭП выделенного документа;
- **Сравнить атрибуты** – производит сравнение атрибутов двух электронных документов;
- **Показать XML-документ** – позволяет просмотреть весь XML-документ;
- **Синхронизация основной БД и БД ЭЦП** – позволяет произвести синхронизацию базы данных АС «Бюджет» и криптобазы;
- **Изменить параметры подключения к FTP-серверу** – служит для изменения логина/пароля пользователя, которые используются при подключении к FTP-серверу.

❖ Панель параметров

Панель параметров окна утилиты позволяет представить информацию в более удобном виде для конкретного пользователя. Например, если пользователь работает с конкретным типом документа, то его значение можно установить на панели параметров, тогда данные с другими значениями типа документа (из других интерфейсов) не будут отображаться в рабочей области. Кроме того, можно ограничить выборку данных и по значениям других параметров.

Порядок действий при поиске документов требуемого вида:

1. Установите на панели параметров необходимые параметры поиска.

2. Нажмите кнопку 

Выбрать данные подписей. В рабочей области отобразится перечень документов, удовлетворяющих параметрам поиска. Примененное ограничение выделяется синим цветом.

Таблица 5 – Параметры-ограничения выборки данных утилиты AdminSign.exe

Имя параметра	Значение параметра	Способ ввода значения
Идентификатор	Ограничение выборки данных по идентификатору (первичному ключу) записи в криптобазе	Ввод с клавиатуры
Код документа	Ограничение выборки данных по значению идентификатора документа в БД АС «Бюджет»	Ввод с клавиатуры
Номер подписи	Ограничение выборки данных по порядковому номеру наложенной ЭП	Ввод с клавиатуры
Тип документа	Ограничение выборки данных по типу первичного документа системы, соответствующего интерфейсу	Ввод с клавиатуры по маске ввода
Начальное состояние	Ограничение выборки данных по наименованию начального этапа (действия) в обработке документа	Ввод с клавиатуры по маске ввода
Конечное состояние	Ограничение выборки данных по наименованию конечного этапа (действия) в обработке документа	Ввод с клавиатуры по маске ввода
Флаг	Ограничение выборки данных по типу подписи (0 – обычная, 1 – активная, 2 – отмененная, 3 – подпись отката)	Ввод с клавиатуры
Клиент	Ограничение выборки данных по коду удаленного клиента (для документов, пришедших из АС «УРМ»)	Ввод с клавиатуры
Автор	Ограничение выборки данных по автору записей	Ввод с клавиатуры
Дата:		
С, По	Ограничение выборки по дате и времени создания записи	Календарь, ввод с клавиатуры, маска ввода

❖ Перечень полей таблицы данных

Заполнение таблицы данных окна утилиты производится автоматически, не предусматривается прямого изменения или добавления данных. Все действия с данными осуществляются с помощью кнопок управления на панели инструментов окна утилиты.

Таблица 6 – Перечень полей таблицы данных утилиты AdminSign.exe

Название поля	Значение поля
Идентификатор	Идентификатор (первичный ключ) записи в криптобазе
Код документа	Идентификатор документа в БД АС «Бюджет»
Номер подписи	Порядковый номер ЭП (уникален для записей с одинаковым FUID)
Данные документа	Описание документа в xml-формате
Подпись	Подпись документа
Тип документа	Тип первичного документа системы, соответствующий интерфейсу
Начальное состояние	Наименование начального этапа (действия) в обработке документа
Конечное состояние	Наименование конечного этапа (действия) в обработке документа
Флаг	Логический тип подписи (0 – обычная, 1 – активная, 2 – отмененная,

Название поля	Значение поля
	3 – подпись отката)
Клиент	Код удаленного клиента (для документов, пришедших из АС «УРМ»)
Автор	Информация об авторе записи
Дата	Дата и время создания записи

11.3. Функциональные возможности

❖ **Просмотр данных криптобазы и поиск нужных записей**

При нажатии на кнопку управления **Показать подписи документа** интерфейса Расход по п\п РМ Казначейство в появившемся окне утилиты AdminSign.exe отобразятся записи из криптобазы, соответствующие текущей записи интерфейса АС «Бюджет». Параметр Код документа будет заполнен значением ID записи в базе АС «Бюджет».

Для возможности работы с множественной ЭП анализируется параметр Флаг, значение которого устанавливается по умолчанию равным «1» при подписании документа ЭП в АС «Бюджет», при этом у предыдущих ЭП флаг обнуляется. Поэтому при нажатии на кнопку **Показать подписи документа** из криптобазы будет выбрана запись с последней наложенной на текущий документ ЭП.

Для просмотра всех ЭП, наложенных на текущий документ в АС «Бюджет», необходимо очистить значение параметра Флаг и нажать Выбрать **Выбрать данные подписей.**

Для просмотра всех данных криптобазы необходимо очистить значение параметра запроса Код документа и нажать кнопку управления Выбрать **Выбрать данные подписей** окна утилиты. При запуске утилиты из каталога OCX и нажатии на указанную кнопку управления отобразятся все записи криптобазы.

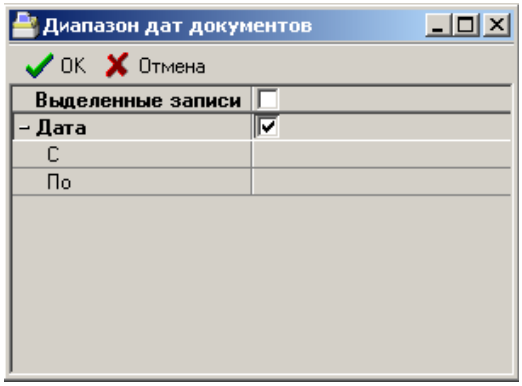
Поиск нужных записей в криптобазе производится путем установки значений соответствующих параметров на панели параметров запроса и последующего нажатия на кнопку Выбрать **Выбрать данные подписей.**

Если не требуется искать записи в криптобазе, или их поиск уже завершен, то панель параметров запроса окна утилиты можно скрыть для удобства работы с помощью кнопки управления Панель.

❖ **Экспорт данных из хранилища данных ЭП**

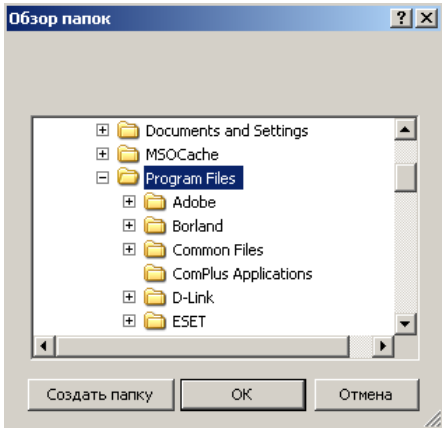
Экспорт подписанных электронных документов из хранилища в файл производится с помощью кнопки управления Экспорт **Экспортировать данные**. После нажатия на кнопку выводится окно параметров выбора документов для экспорта. При установке флага-галочки у параметра Выделенные записи будут экспортированы выделенные в данный момент записи, при установке флага-галочки у параметра Дата – все записи, отвечающие заданному диапазону дат.

Рисунок 32 – Вид окна параметров для выбора документов



При нажатии на кнопку **ОК** и выбора системного каталога (рисунок 33) происходит выгрузка подписанных электронных документов.

Рисунок 33 – Вид окна выбора каталога при экспорте документов



При выгрузке данных из хранилища данных ЭП в файловую систему документ и электронная подпись сохраняются в отдельных файлах. При выгрузке используется следующая структура каталогов: «год\месяц\день\час» (год – 4 цифры, месяц – номер месяца). В качестве имен файлов используется первичный ключ таблицы SignDocRecords.

Файлы могут иметь различные расширения:

- *.nfo – файл, содержащий значения дополнительных атрибутов для связи с документом в основной базе и связи с этапом обработки, когда ЭП была наложена;
- *.eds – файл, содержащий саму электронную подпись;
- *.dat – файл, содержащий подписанный xml-документ.

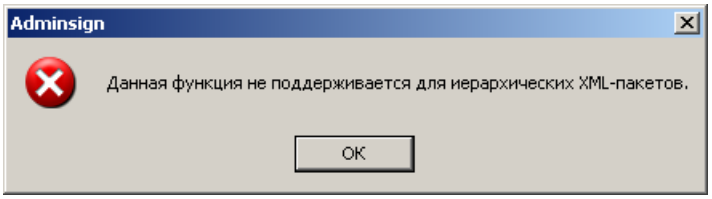
❖ Удаление данных из криптобазы

Удаление данных из хранилища данных ЭП производится при помощи кнопки управления Удалить **Удаление данных по датам**. При нажатии на кнопку выводится окно параметров (см. рисунок 32). Операция удаления данных из криптобазы не обратима. При установке флага-галочки у параметра Выделенные записи будут удалены выделенные в данный момент записи, при установке флага-галочки у параметра Дата – все записи, отвечающие заданному диапазону дат.

❖ Сравнение атрибутов двух электронных документов

Сравнение атрибутов двух электронных документов осуществляется при помощи кнопки управления **Сравнить атрибуты**. Данная операция применима лишь к документам, участвующим в электронном документообороте с использованием системы состояний. При попытке сравнения двух электронных документов, являющихся иерархическими XML-пакетами (документы, переданные с ЭП из АС «Бюджет» в АС «УРМ» (при наличии ПМ «Передача выписок с ЭП из АС «Бюджет» в АС «УРМ»), документы, полученные из АС «УРМ» с прикрепленными файлами с ЭП (при наличии ПМ «Прикрепление к документам произвольных файлов с ЭП») будет выведено соответствующее сообщение об ошибке (рисунок 34).

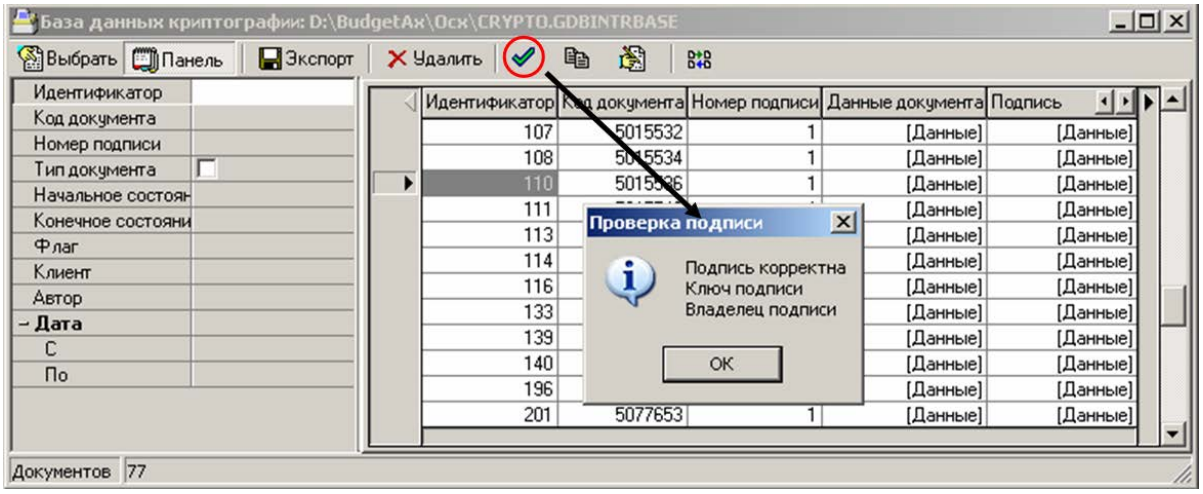
Рисунок 34 – Сообщение об ошибке «Данная функция не поддерживается для иерархических XML-пакетов»



❖ Проверка корректности ЭП

Проверить корректность ЭП у текущего документа из криптобазы можно с помощью кнопки управления **Проверить корректность подписи**. После нажатия кнопки будет выведено информационное окно (рисунок 35), содержащее результат проверки.

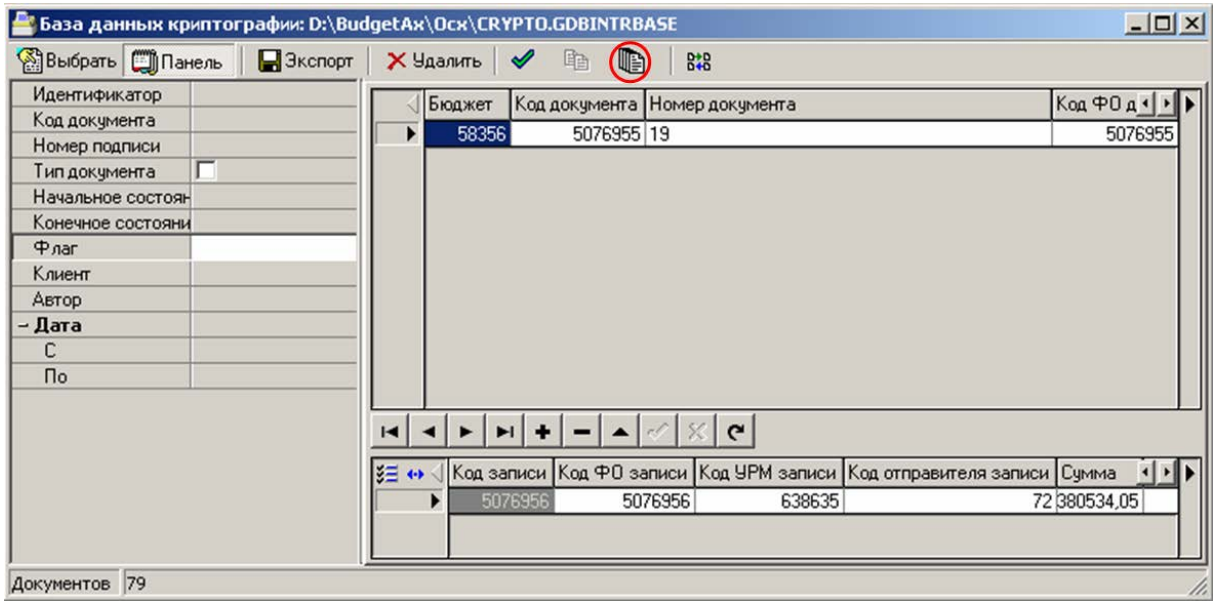
Рисунок 35 – Вид информационного окна с положительным результатом проверки



❖ Просмотр XML-документа

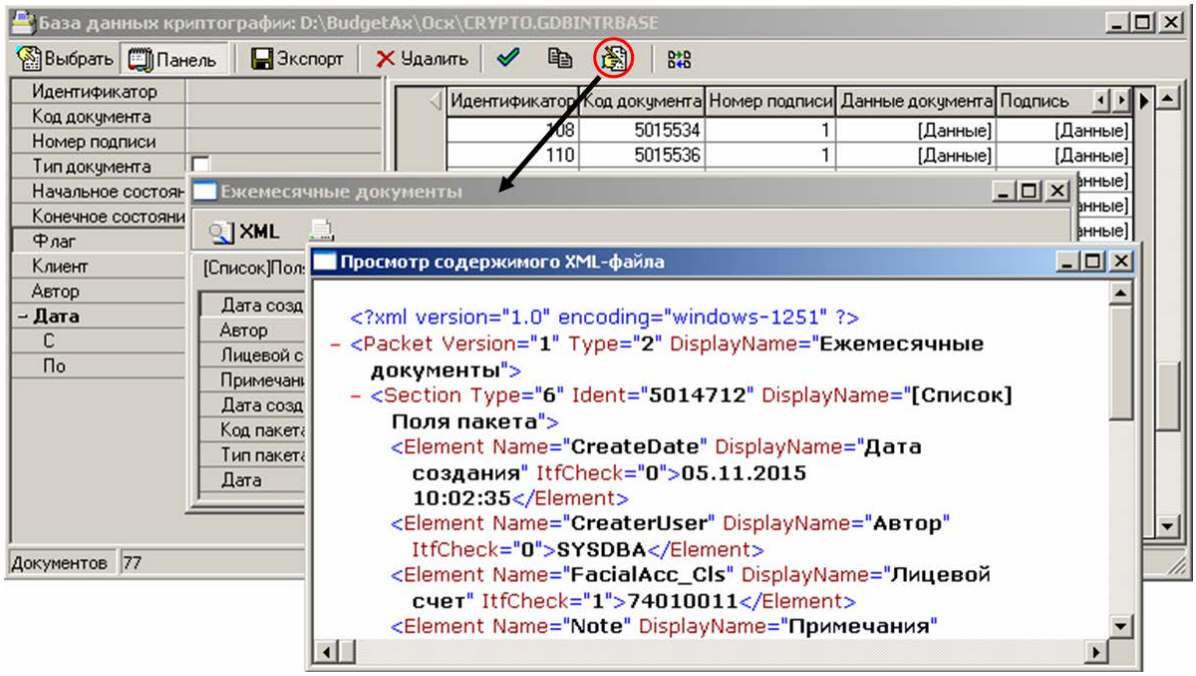
Просмотр содержимого документа осуществляется с помощью кнопки управления окна утилиты **Показать XML-документ**. В зависимости от принадлежности к определенному типу документов с ЭП, для записей БД будет открываться форма просмотра, соответствующая данному типу. Для участвующих в системе состояний документов (при наличии ПМ «Конвейерная обработка и множественное визирование документов») открывается детализация данных (рисунок 36).

Рисунок 36 – Вид окна просмотра документов (при наличии системы состояний)



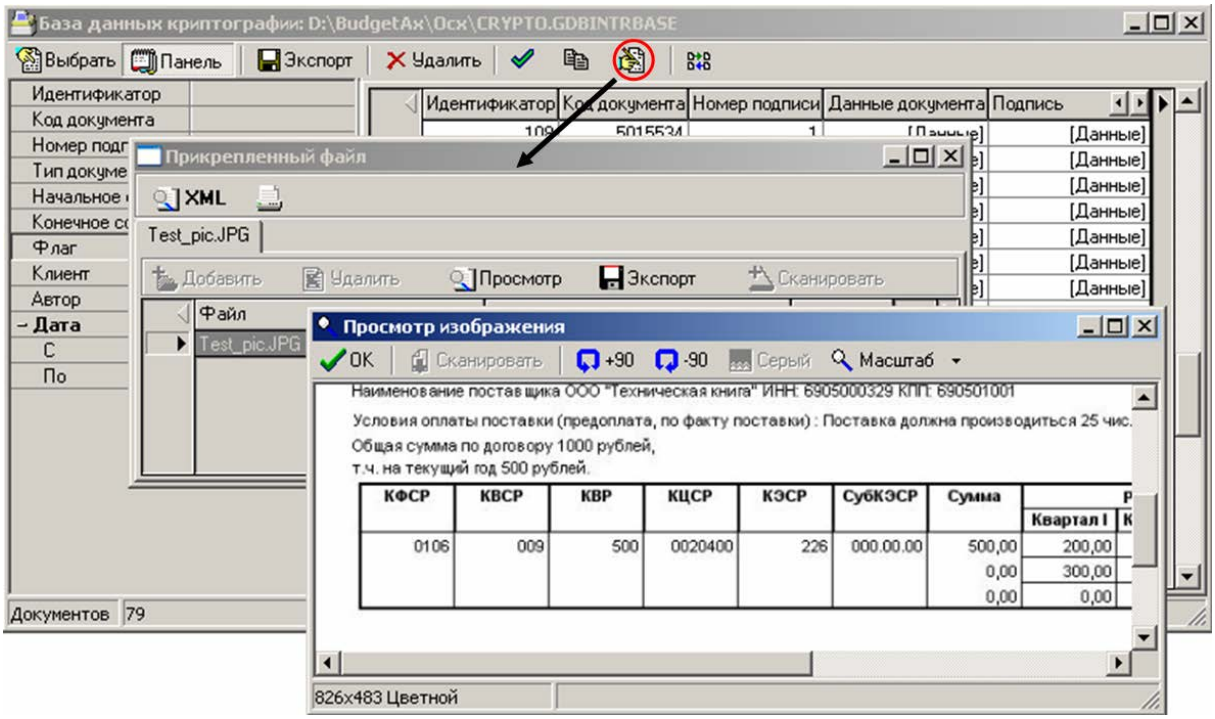
Для документов, переданных с ЭП из АС «Бюджет» в АС «УРМ» (при наличии ПМ «Передача выписок с ЭП из АС «Бюджет» в АС «УРМ»), открывается форма просмотра пакета с ЭП (рисунок 37).

Рисунок 37 – Вид окна просмотра документов (при наличии ПМ «Передача выписок с ЭП из АС «Бюджет» в АС «УРМ»)



Для документов, полученных из АС «УРМ» с прикрепленными файлами с ЭП (при наличии ПМ «Прикрепление к документам произвольных файлов с ЭП»), открывается форма «Прикрепленный файл» (рисунок 38).

Рисунок 38 – Вид окна просмотра документов (при наличии ПМ «Прикрепление к документам произвольных файлов с ЭП»)



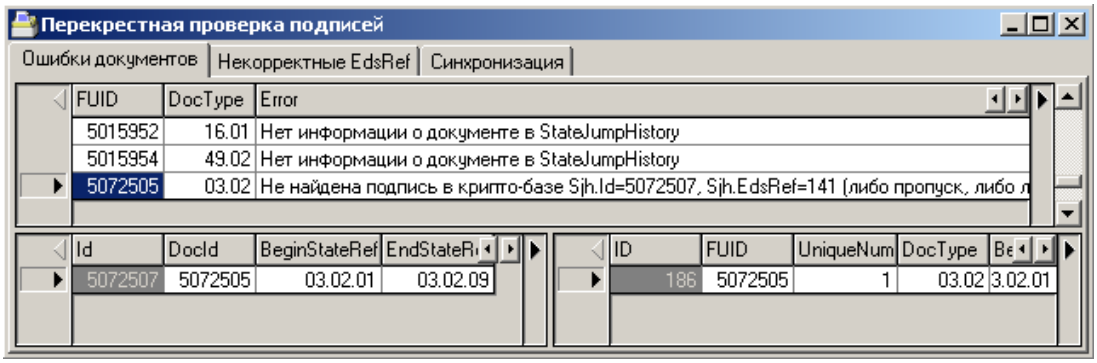
❖ Поиск отличий данных и синхронизация базы данных АС «Бюджет» и криптобазы

Синхронизация баз данных (заполнение поля EdsRef в основной схеме на основании данных крипто-схемы) осуществляется с помощью кнопки **Синхронизация основной БД и БД ЭЦП**. Это может потребоваться, когда в АС «УРМ» будет заполняться поле EdsRef, а в АС «Бюджет» будет сделан поиск по этому полю.

При нажатии кнопки сначала вызывается окно подключения к основной базе данных АС «Бюджет». После заполнения параметров и подключения к основной БД появляется форма «Перекрестная проверка подписей», заполнение данных в которой производится автоматически, ввод, редактирование и удаление данных вручную не допускается. На трех закладках формы отображается информация об осуществлении следующих процедур:

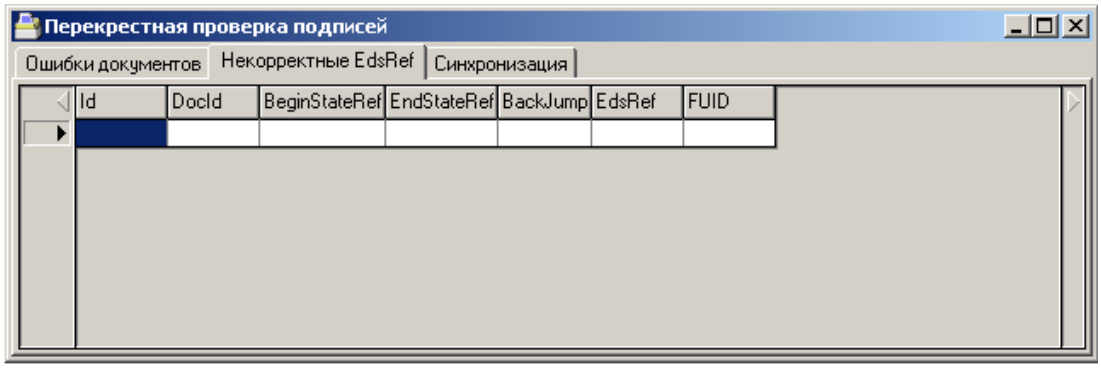
- Поиск недопустимых несоответствий между таблицами криптобазы и базы данных АС «Бюджет». Информация о найденных несоответствиях выводится на закладке Ошибки документов (рисунок 39);

Рисунок 39 – Вид закладки «Ошибки документов» окна «Перекрестная проверка подписей»



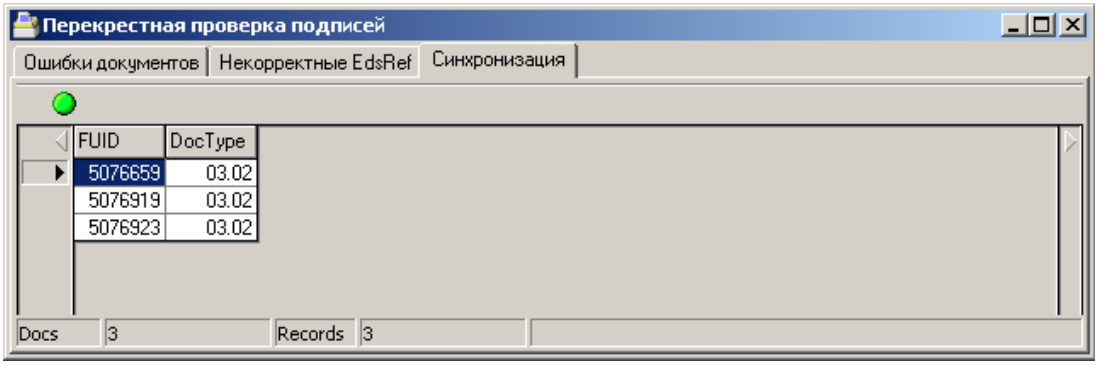
- Поиск строк таблицы StateJumpHistory с некорректными EdsRef на закладке Некорректные EdsRef (рисунок 40);

Рисунок 40 – Вид закладки «Некорректные EdsRef» окна «Перекрестная проверка подписей»



- Поиск записей, для которых возможна синхронизация на закладке Синхронизация (рисунок 41). Для каждой записи отображается код документа (идентификатор документа в БД) и тип первичного документа системы, соответствующий интерфейсу.

Рисунок 41 – Вид закладки «Синхронизация» окна «Перекрестная проверка подписей»



Для проведения синхронизации (заполнения поля EdsRef таблицы StateJumpHistory) используется кнопка  **Заполнить EdsRef (синхронизировать)** на закладке Синхронизация, которая становится активной при наличии записей в таблице.

12. Список сокращений

АС	Автоматизированная система
БД	База данных
ГОСТ	Государственный стандарт
ГРБС	Главный распорядитель бюджетных средств
ОЗУ	Оперативное запоминающее устройство
ОС	Операционная система
ПБС	Получатель бюджетных средств
ПМ	Программный модуль

ПО	Программное обеспечение
ПЭВМ	Персональная электронная вычислительная машина
РБС	Распорядитель бюджетных средств
РМ	Рабочее место
СКЗИ	Средство криптографической защиты информации
СОС	Список отозванных сертификатов
СОУС	Служебный объект управления состояниями
СУБД	Система управления базой данных
ТПФО	Территориальное подразделение финансового органа
УРМ	Удаленное рабочее место
ФО	Финансовый орган
ФСБ	Федеральная служба безопасности
ЭВМ	Электронная вычислительная машина
ЦБ РФ	Центральный банк Российской Федерации
ЭП/ЭЦП	Электронная подпись