Научно-производственное предприятие
“ИЖИНФОРМПРОЕКТ”

УТВЕРЖДЕН

приказом от 02.02.2006 № 1

Регламент
защищенного электронного документооборота в системе «КриптоСвязь»

Ижевск 2006

Содержание

1 Общие сведения о защищенном электронном документообороте в системе «КриптоСвязь»

Настоящий документ устанавливает общий порядок взаимодействия участников (Абонентов системы) защищенного (в т.ч. юридически значимого) электронного документооборота с использованием средств защиты информации.

НПП «Ижинформпроект» предлагает комплексный вариант создания автоматизированных рабочих мест для обеспечения обмена конфиденциальными электронными юридически значимыми документами.

В системе допускается (при обязательном использовании шифрования) обмениваться электронными документами, содержащими конфиденциальную информацию (персональные данные, служебная, банковская, коммерческая тайна и т.п.).

Абоненты системы при необходимости устанавливают особые (дополнительные) условия взаимодействия. При этом дополнительные условия в целях обеспечения защищенности электронного документооборота (конфиденциальность, целостность, аутентичность, неотказуемость и юридическая значимость) должны быть согласованы с ООО НПП «Ижинформпроект».

Регламент не устанавливает требований к форматам электронных документов, периодичности обмена, внутреннего учета и обеспечения защиты документов у Абонентов.

Защищенный электронный документооборот в системе «КриптоСвязь» реализуется с использованием базовых приложений Инфраструктуры открытых ключей (ИОК) / Public Key Infrastructure (PKI) — технологическая инфраструктура и сервисы, гарантирующие безопасность информационных и коммуникационных систем, использующих криптографические алгоритмы с открытыми ключами.

При построении защищенного электронного документооборота применяются электронная цифровая подпись (при необходимости возможно шифрование) электронных документов, представленных в виде файлов, передаваемых между Абонентами системы, и электронная цифровая подпись и шифрование почтовых сообщений Internet.

Электронная почта с цифровой подписью позволяет получателю убедиться в подлинности и целостности электронного документа/сообщения. Шифрование электронных документов/сообщений электронной почты препятствует его прочтению другими людьми в процессе доставки.

Если защищенный электронный документ/сообщение с ошибками (например, сообщение подделано или истек срок действия сертификата ключа подписи отправителя), перед тем, как можно будет просмотреть содержимое объекта будет отображаться предупреждение, в котором излагается подробное описание неполадки. На основе содержащихся в предупреждении сведений пользователь может принять решение относительно уровня доверия к нему.

Для защиты электронных документов/сообщений используются сертифицированные средства криптографической защиты информации (СКЗИ) «КриптоПро CSP» и совместимые с ним.

Применение сертифицированных СКЗИ обеспечивает использование российских криптографических алгоритмов:

— Алгоритм зашифрования/расшифрования данных и вычисление имитовставки в соответствии с ГОСТ 28147 89 «Системы обработки информации. Защита криптографическая»;

— Алгоритм формирования и проверки ЭЦП в соответствии с ГОСТ Р 34.10-2001. «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи», а также (до 01.01.2008) ГОСТ Р 34.10-94 «Информационная технология. Криптографическая защита информации. Система электронной цифровой подписи на базе асимметричного криптографического алгоритма»;

— Алгоритм выработки значения хэш-функции в соответствии с ГОСТ Р 34.11-94 «Информационная технология. Криптографическая защита информации. Функция хэширования».

Для возможности работы в Защищенный электронный документооборот в системе «КриптоСвязь» пользователь должен получить сертификат ключа подписи в Удостоверяющем центре InfoTrust ООО НПП «Ижинформпроект» в соответствии с требованиями Федерального закона от 10 января 2002 № 1-ФЗ «Об электронной цифровой подписи».

Сертификат должен содержать сведения о приложениях, системах документооборота, видах электронных документов, в которых разрешается его использовать.

После обмена абонентами их сертификатами (сертификат направляется вместе с сообщением) и помещением этих сертификатов в адресные книги/справочники сертификатов можно направлять электронные документы/сообщения в защищенном виде.

Если проверка отзыва сертификатов ключей подписи включена, статус сертификатов проверяется при открытии сообщения, если установлено подключение через Интернет к серверу Удостоверяющего центра.

2 Защита электронных документов

Для обеспечения защиты электронного документа в системе «КриптоСвязь» используется криптографический менеджер «КриптоАРМ» (разработчик — Digt, ООО «Цифровые технологии»).

Криптографический менеджер предназначен для удобного проведения операций шифрования и электронной цифровой подписи электронных документов. по российским государственным криптографическим стандартам.

«КриптоАРМ» имеет расширенные возможности использования электронной цифровой подписи (соподпись, заверяющая ЭЦП и поддержка расширенных свойств ЭЦП, например, возможность поставить комментарий к ней), а также гибкую настройку криптографических операций под индивидуальные задачи пользователя с помощью профилей.

Правила настройки и работы с криптографическим менеджером установлены эксплуатационной документацией и инструкциями ООО НПП «Ижинформпроект».

3 Защита сообщений электронной почты

Для обеспечения защищенного обмена сообщениями в системе «КриптоСвязь» используются почтовые клиенты Outlook Express (рекомендуется версия 6 и выше) и MicroSoft Outlook (рекомендуется версия MicroSoft Outlook 2003 из пакета MicroSoft Office 2003 и выше).

Указанные программы совместимы со спецификациями протокола защищенной электронной почты S/MIME (Secure/Multipurpose Internet Mail Extensions) версии 2 и 3.

Почтовые клиенты Outlook Express и MicroSoft Outlook реализуют контроль доставки сообщений до адресата (безопасные уведомления с ЭЦП получателя). В случае отсутствия у Абонентов системы требований по контролю доставки

возможно применение почтового клиента The Bat! (с поддержкой S/MIME и реализации криптографических функций с использованием CryptoAPI).

Для пользования защищенной электронной почтой пользователь должен иметь сертификат ключа подписи, поддерживающий стандартное приложение ИОК «защита электронной почты» и предназначенный для защиты почтового обмена по соответствующему адресу электронной почты пользователя.

Правила настройки и работы с почтовым клиентом установлены эксплуатационной документацией и инструкциями ООО НПП «Ижинформпроект».

4 Порядок создания защищенного электронного документа

Электронные документы и их приложения создаются в установленном (согласованном участниками соответствующего обмена) формате (например, doc, xls, pdf, jpg и т.п.). Электронная цифровая подпись формируется в отдельный файл, имеющий соответствующее расширение, для обеспечения совместимости с приложениями MS Windows. После подписания электронного документа ЭЦП внесение изменений в его содержание запрещается.

Корреспонденция, предназначенная для отправки по электронной почте, должна содержать в правом верхнем углу пометку «по электронной почте».

Документ (все файлы, в т.ч. приложения) передаются на подпись уполномоченному должностному лицу, имеющему право подписывать данный вид документов, являющемуся владельцем сертификата ключа подписи.

При представлении электронного документа на дискете, на ней должны содержаться только файлы, подлежащие подписанию ЭЦП. Дискета не должна содержать сбойных секторов и в обязательном порядке проверяется исполнителем антивирусными средствами для предотвращения распространения компьютерных вирусов. В имени файла рекомендуется использовать только латинские буквы и цифры в количестве не больше восьми символов.

Имя файла, содержащего электронный документ, располагается под реквизитами исполнителя в левом нижнем углу первой страницы соответствующего

файла. Имена отдельных файлов, содержащих приложения к документу, должны быть указаны в основном документе (вместе с приложениями).

Документ (все файлы, в т.ч. приложения) подписываются ЭЦП с использованием криптографического менеджера.

Подписанный электронный документ передается оператору, осуществляющему передачу документа по электронной почте.

Перед отправкой электронного документа, оператор проверяет файлы антивирусными средствами во избежание распространения компьютерных вирусов.

Оператор с использованием криптографического менеджера проверяет действительность подписи уполномоченного лица. При корректности подписи оператор регистрирует документ в соответствии с внутренними правилами документооборота. Рекомендуется к регистрационному номеру добавлять знак @, указывающий на отправку документа по электронной почте.

Регистрационный номер, дата документа и другие дополнительные параметры записываются в служебный файл (doc). В имя служебного файла рекомендуется включать регистрационный номер (его часть) документа. Дополнительный файл является неотъемлемой частью документа, подписывается ЭЦП оператора и отправляется вместе с документом. Если электронный документ, подписанный ЭЦП, содержит регистрационный номер и дату, то служебный файл не создается.

После указанных процедур зарегистрированным защищенным электронным документом считается комплект файлов содержащих собственно документы и ЭЦП к ним, а также служебный файл с подписью. Электронный документ для уменьшения объема передаваемой информации и фиксации состояния упаковывается (сжимается) в файл-архив (rar, zip), Имя файла-архива должно включать в себя регистрационный номер (его часть) документа.

Копия помещается в хранилище электронных документов. Сроки и условия хранения электронных документов устанавливаются внутренними нормативными документами Абонента (как правило, срок аналогичен сроку хранения документа на бумажном носителе).

Документ (файл-архив) направляется оператором адресату с использованием защищенного почтового сообщения.

На соответствующих этапах формирования документа, внутреннего согласования и т.п. возможно формирование мультиподписи (несколько ЭЦП на один файл) и соподписи (заверяющая подпись).

5 Порядок отправки защищенного почтового сообщения

Почтовые сообщения формируются с вложенными файлами (архивами).

В графе «тема сообщения» указывается номер и дата направляемого документа.

В теле письма указывается Наименование документа и при необходимости другие вспомогательные параметры и комментарии. В случае ответа на запрос в теле письма указывается также номер и дата письма, на которое направляется ответ.

К созданному сообщению присоединяется файл-архив, содержащий направляемый документ.

Адресат выбирается из адресной книги (участники обмена должны предварительно обменятся сертификатами ключей подписи).

Устанавливаются требования получения уведомлений о доставке, прочтении почтового сообщения.

Контролируются параметры защиты отправляемого сообщения (включение режимов шифрования и электронной цифровой подписи).

Факт получения электронного документа подтверждается путем передачи безопасного уведомления адресатом.

Отправитель периодически контролирует доставку сообщения и связывается с оператором адресата в случае неполучения необходимых уведомлений. В случае неполучения сообщения адресатом отправитель производит повторную отправку сообщения.

При необходимости учет отправки электронных документов может производиться оператором в соответствующем Журнале.

6 Порядок приема защищенного почтового сообщения

При получении сообщения оператор с помощью почтового клиента производит его расшифрование и проверку ЭЦП.

Факт получения электронного документа подтверждается путем передачи автоматически формируемого безопасного уведомления (с ЭЦП получателя).

Полученный электронный документ (файл-архив) распаковывается. С помощью криптографического менеджера производится проверка ЭЦП всех входящих в документ файлов, а также проверка сертификата уполномоченного должностного лица на предмет возможности использования этого сертификата применительно к этому виду документов. В случае нарушения ЭЦП документ не принимается к дальнейшей обработке и отправителю направляется соответствующее сообщение о необходимости повторного направления документа.

В случае корректности ЭЦП документ регистрируется оператором в соответствии с правилами внутреннего документооборота.

Копия помещается в хранилище электронных документов. Сроки и условия хранения электронных документов устанавливаются внутренними нормативными документами Абонента.

При необходимости распечатывания документа на бумажный носитель оператор указывает на нем из служебного файла номер и дату документа, делает заверяющую запись о получении документа по электронной почте и верности электронной цифровой подписи.

Документ передается для последующего рассмотрения или обработки в соответствии правилами внутреннего документооборота.

При необходимости учет приема электронных документов может производиться оператором в соответствующем Журнале.

7 Дополнительные условия

Абоненты системы перед организацией обмена защищенными электронными документами должны согласовать параметры, не установленные настоящим

регламентом. Рекомендуется такую договоренность закрепить договором/соглашением, которое необходимо согласовать с ООО НПП «Ижинформпроект».

Данный документ должен содержать:

— Перечень видов документов, обмен которыми осуществляется через систему;

— Требования к содержанию/оформлению соответствующих документов;

— Требования к форматам/формам файлов с учетом конкретных приложений и их версий, обеспечивающих автоматизированную обработку;

— Перечень уполномоченных должностных лиц, владельцев сертификатов ключа подписи, наделенных правом подписывать соответствующие электронные документы;

— Адреса электронной почты абонентов;

— Перечень операторов электронной почты, владельцев сертификатов ключа подписи, наделенных правом подписывать соответствующие электронные сообщения (их координатами для оперативного взаимодействия);

— Периодичность обмена информацией;

— Требования внутреннего учета документов;

— Требования к обеспечению конфиденциальности передаваемых сведений.

Кроме того, при необходимости стороны могут определить иные средства защиты информации, криптографические менеджеры, при условии их сертификации в установленном порядке и совместимости по форматам сертификатов ключей подписи. Указанные вопросы должны быть согласованы с НПП «Ижинформпроект».

8 Рекомендации по организации защищенного электронного документооборота

Для организации защищенного электронного документооборота НПП «Ижинформпроект» рекомендует назначать необходимое количество

уполномоченных должностных лиц, имеющих право подписывать соответствующие электронные документы, при котором обеспечивается бесперебойная работа.

Для хранения ключевой информации пользователей рекомендуется применять надежные электронные устройства хранения.

На рабочих местах пользователей, производящих обработку зашифрованных документов, должны быть решены вопросы по антивирусной защите.

Хранилища электронных документов должны иметь надежные сертифицированные средства защиты информации, а также регламентированные условия резервирования.

Журналы учета отправки/получения почтовых сообщений должны использоваться при обмене конфиденциальной информацией. Форма журналов должна соответствовать требованиям, установленным для конфиденциального документооборота.

При вводе в эксплуатацию на рабочие места абонентов системы устанавливаются и настраиваются компоненты защиты информации и телекоммуникационные средства, проводится обучение пользователей правилам работы с СКЗИ, изготовляются и выдаются уполномоченным пользователям криптографические ключи и соответствующие сертификаты ключей подписи, производится настройка, проверка работоспособности и тестирование системных и телекоммуникационных компонентов и средств защиты информации автоматизированных рабочих мест пользователей для работы в системе защищенного электронного документооборота.

В целях принятия обоснованного решения о выборе технологии защищенного обмена электронными документами НПП «Ижинформпроект» возможно проведение пилотного проекта. В ходе пилотного проекта выполняется установка, проверка работоспособности, тестирование всех функциональных компонентов, производительности и операционных регламентов, а также требований по защите информации в системе, производится оценка системы на предмет защищенности, совместимости и удобства работы с системой, уточняются вопросы обеспечения юридической значимости электронных документов.

9 Технические условия

Требования к средству вычислительной техники (СВТ):

— IBM PC-совместимый компьютер с процессором Pentium-200 или выше;

— ОЗУ не менее 64 Мбайт;

— не менее 150 Мбайт свободного дискового пространства;

— Привод для гибких магнитных дисков 3,5”;

— Привод компакт дисков (на период установки и настройки);

— Свободный порт USB (в случае использования eToken/ruToken);

— Свободный слот PCI (в случае использования ЭЗ Соболь);

— Операционная система MS Windows 98, NT, 2000, XP Professional (рекомендуется MS Windows XP Professional Service Pack 2);

— WEB–обозреватель MS Internet Explorer версии 6 или выше;

— Почтовый клиент с поддержкой S/MIME — Outlook Express, MicroSoft Outlook, The Bat! (рекомендуется Outlook Express и MicroSoft Outlook) (в случае использования электронной почты).

Требования к обеспечению сетевого взаимодействия СВТ:

— Подключение к сети Internet (через модем, выделенную линию или локальную сеть) на скорости не менее 28800 бит/сек;

— Подключение к почтовому серверу (организации или провайдера) по протоколам SMTP/POP3;

— Наличие зарегистрированного адреса электронной почты, на который имеется сертификат ключа подписи.

— Работа используемого почтового сервера с поддержкой S/MIME.

Базовое программно-аппаратное обеспечение:

— Средство криптографической защиты информации «КриптоПро CSP» и модуль поддержки сетевой аутентификации «КриптоПро TLS»(клиент);

— Криптографический менеджер КриптоАРМ.

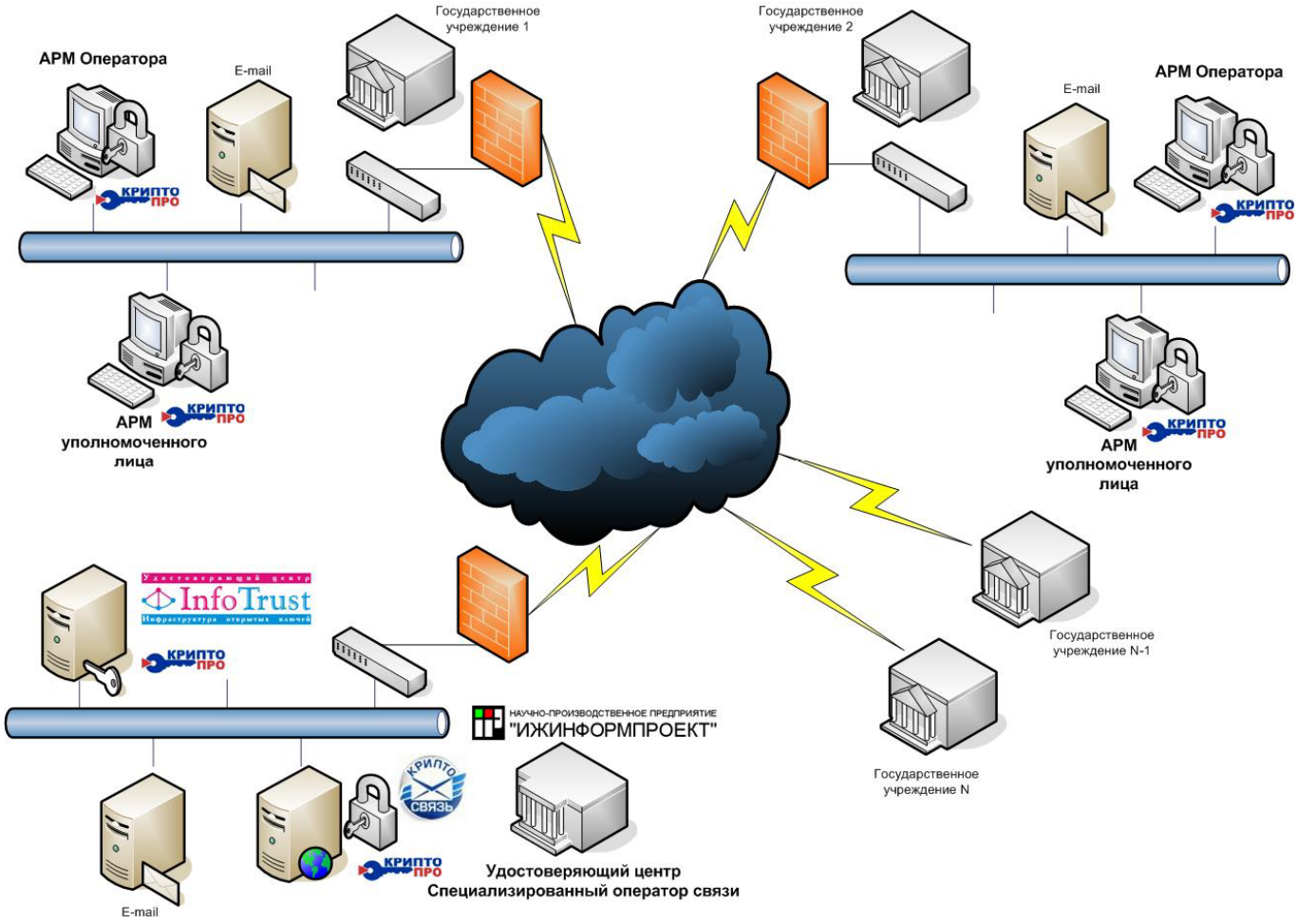
Дополнительное программно-аппаратное обеспечение:

— Устройства защищенного хранения ключевых документов (электронные идентификаторы) USB — eToken PRO, ruToken;

— Средства защиты от несанкционированного доступа — Электронный замок Соболь, Аккорд, Secret Disk NG, Блокпост, Панцирь, Secret Net и т.п.;

— Средства сетевой защиты — ViPNet [Personal Firewall], Блокпост-Экран.

10 Схема взаимодействия абонентов



11 Примеры наименования файлов, содержащих электронный документ

11.1 При формировании и отправке

1 Формирование исполнителем электронного документа, подлежащего передаче и сопроводительного письма к нему.

Например: peredach.xml + pism0001.doc

2 Передача указанного комплекта файлов уполномоченному лицу

3 Формирование ЭЦП уполномоченным лицом на передаваемых файлах и возврат их исполнителю.

Например:

peredach.xml + peredach.p7s + pism0001.doc + pism0001.p7s

4 Регистрация передаваемых конфиденциальных документов в соответствии с правилами делопроизводства.

5 Передача подписанных электронных документов оператору электронной почты.

6 Проверка ЭЦП на представленных файлах.

Например:

peredach.xml + peredach.p7s + pism0001.doc + pism0001.p7s

7 Формирование оператором электронной почты дополнительного файла с регистрационными реквизитами и формирование к нему ЭЦП (оператора).

Например: num0001.doc + num0001.p7s

8 Архивирование комплекта указанных файлов для передачи.

Например:

pism0001.rar = peredach.xml + peredach.p7s + pism0001.doc + pism0001.p7s + num0001.doc + num0001.p7s

9 Занесение информации в журнал учета.

10 Передача архивного файла адресату.

11.2 При приеме

1 Прием архивного файла.

Например: pism0001.rar

2 Проверка ЭЦП уполномоченных лиц, указанных в сопроводительном письме и оператора.

Например:

peredach.xml + peredach.p7s + pism0001.doc + pism0001.p7s + num0001.doc + num0001.p7s

3 Занесение информации в журнал учета.

4 Распечатывание полученной информации (сопроводительного письма) и регистрация документов в соответствии с правилами делопроизводства с отметкой в журнале учета.

5 Передача электронных документов исполнителю с отметкой в журнале учета.