ООО Научно-производственное предприятие «Ижинформпроект»

Система защищенного электронного юридически значимого документооборота
«КриптоСвязь-Веб» («КриптоВеб»)

КриптоВеб: техническое руководство

Приложение к Руководству пользователя

Ижевск 2019

Данный документ содержит описание процессов, обеспечивающих поддержание жизненного цикла клиентского модуля Системы защищенного электронного юридически значимого документооборота «КриптоСвязь-Веб» («КриптоВеб») (далее — «системы КриптоВеб» или «системы»), в том числе:

- организационно-методическое обеспечение системы;
- подготовку рабочего места и установку клиентского модуля системы;
- установке при нестандартной конфигурации системы;
- устранение неисправностей, выявленных в ходе эксплуатации программного обеспечения;
- совершенствование программного обеспечения;
- информацию о персонале, необходимом для обеспечения такой поддержки;
- гарантии Оператора.

Документ предназначен для обеспечения бесперебойной работы абонента с системой путем соблюдения технических, документационных и организационных мер.

Документ является дополнением к Руководству пользователя, опубликованному по адресу: http://www.cryptoweb.ru/document/CryptoWeb-Manual.pdf (далее — Руководство).

В настоящем документе содержатся ссылки на разделы и пункты основного Руководства.

Основной сайт системы: http://cryptoweb.ru/

1. Организационно-методическое обеспечение

Для эксплуатации системы требуется ознакомиться со следующими документами, относящимися к системе:

- КриптоВеб: руководство пользователя: http://www.cryptoweb.ru/document/CryptoWeb-Manual.pdf
- Регламент системы защищенного электронного юридически значимого документооборота «КриптоСвязь-Веб» («КриптоВеб»): http://www.cryptoweb.ru/document/Reglament-CryptoWeb.pdf
- Руководство по безопасности системы защищенного электронного юридически значимого документооборота «КриптоСвязь-Веб» («КриптоВеб») http://www.cryptoweb.ru/document/CryptoWeb-Security-Guide.pdf
- Положение о порядке использования средств криптографической защиты информации и ключевой информации к ним: https://www.infotrust.ru/data/Docs/IIP_Crypto.pdf
- Требования по обеспечению безопасности автоматизированного рабочего места: https://www.infotrust.ru/data/Docs/IIP_ARM_Security.pdf

Регламентирующие, законодательные и нормативные документы:

- Федеральный закон Российской Федерации от 06.04.2011 № 63-ФЗ «Об электронной подписи»;

- Федеральный закон Российской Федерации от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный Закон Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Федеральный закон Российской Федерации от 29.07.2004 № 98-ФЗ «О коммерческой тайне»;
- Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»;
- Указ Президента РФ от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы»
- Приказ ФСБ России от 09.02.2005 № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации» (Положение ПКЗ-2005);
- Приказ ФАПСИ от 13.06.2001 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».

2. Подготовка рабочего места и установка системы

Для работы в системе требуется наличие автоматизированного рабочего места (компьютера, ноутбука, планшета), подключенного к сети Интернет и удовлетворяющего требованиям системы. Перечень технических требований описан в разделе 1.4 Руководства. Актуальные технические требования также доступны на сайте Системы по адресу: http://www.cryptoweb.ru/requirements.

Обращаем внимание, что ключевыми техническими требованиями для установки системы является наличие операционной системы Windows версии не ниже Windows XP SP3 (для демо-версии) и Windows 7 (для полной версии системы), а также установленного браузера Microsoft Internet Explorer версии не ниже 8 (для демо-версии) и не ниже 11 (для полной версии системы), наличие действующего подключения к сети Интернет.

Пожалуйста, будьте ответственны и не используйте рабочие места в минимальной конфигурации для работы медицинских организаций с большим количеством работников организаций, проходящих медицинские осмотры, или для работы гостиничных учреждений с большим потоком заселения.

Особенности подготовки для работы в полной версии

Для работы в полной версии системы требуется заключение договора с Оператором системы ООО НПП «Ижинформпроект»; порядок заключения договора описан в разделе 5.3 Руководства. С технической стороны дополнительно требуется:

- наличие лицензии на право пользования СКЗИ «КриптоПро CSP» версии 4.0 или выше с поддержкой криптографических алгоритмов формирования электронных подписей ГОСТ Р 34.10-2012 и выработкой хэш-значений согласно ГОСТ Р 34.11-2012. Порядок приобретения лицензии описан в разделе 5.1 Руководства;

- для работы с сервисом «Отчетность в ФМС/МВД» дополнительно требуется наличие лицензии на ПО «КриптоПро .Net» версии 1.6. Порядок приобретения лицензии описан в разделе 5.1 Руководства;
- наличие квалифицированного сертификата ключа проверки электронной подписи, выпущенного удостоверяющим центром, входящим в Перечень доверенных удостоверяющих центров Системы. Порядок получения сертификата описан в разделе 5.2 Руководства;

Установка демо-версии системы для автоматизированных рабочих мест, удовлетворяющих требованиям системы, осуществляется непосредственно с сайта системы по адресу: http://demo-cryptoweb.ru/ Дополнительная информация по установке демо-версии системы доступна в разделе 2 Руководства.

Установка полной версии системы осуществляется согласно порядку, опубликованному в разделе «Установочный комплект» по адресу: http://www.cryptoweb.ru/setup-full Дополнительная информация по установке полной версии системы опубликована в разделе 3 Руководства.

По вопросам, связанным с установкой системы, Вы можете обратиться в техническую поддержку по телефону (3412) 918-101 (для абонентов Удмуртской Республики) или на линию 8 (800) 301-81-01 (для остальных регионов Российской Федерации, звонок бесплатный). Также Вы можете оставить заявку по электронной почте support@cryptoweb.ru

По вопросам, связанным с подключением к системе, заключением договора на работу в системе КриптоВеб, приобретением лицензий на СКЗИ и специальное ПО, услуг по изготовлению квалифицированного сертификата ключа проверки электронной подписи, обращайтесь по телефону (3412) 918-100 или по электронной почте info@cryptoweb.ru

3. Установка при нестандартной конфигурации системы

При стандартных настройках операционной системы Microsoft Windows и браузера Microsoft Internet Explorer по окончании установки (см. предыдущий пункт либо разделы 2 и 3 Руководства) никаких дополнительных действий не требуется, и система сразу будет готова к работе.

В случае если на компьютере либо в локальной сети предприятия имеются специализированные настройки безопасности либо сетевого доступа, могут потребоваться дополнительные действия по окончании установки системы.

Техническая настройка окружения клиентского модуля

Загрузка клиентского модуля системы «Компоненты КриптоВеб», выполненным по технологии Microsoft ActiveX, является необходимым условием для успешного функционирования системы.

Данный компонент, имеющий маркировку CPW.ActiveX[N], где N — целое число, должен быть разрешен в надстройках Microsoft Internet Explorer после установки системы. Также данный компонент (со всеми библиотеками, входящими в состав компонента) должен быть

добавлен в исключения настроек безопасности антивирусного либо иного антишпионского программного обеспечения.

Настройка параметров браузера

Поскольку работа системы КриптоВеб осуществляется через сеть Интернет с использованием технологии JavaScript, для корректной работы программы требуется разрешить использование сценариев JavaScript для сайтов *.cryptoweb.ru при работе в полной версии системы и сайта demo-cryptoweb.ru при работе в демо-версии системы.

Если Вы пропустили шаг установки параметров безопасности при установке системы КриптоВеб, Вы можете включить сайт *.cryptoweb.ru в надежные узлы в случае если Вы работаете с полной версией системы, или сайт demo-cryptoweb.ru в надежные узлу в случае если Вы работаете с демо-версией.

Если же Вы планируете использовать сервис Электронный медосмотр в полной версии системы, дополнительно требуется установить разрешение «Отображение разнородного содержимого» в положение включить как в зоне «Защищенные узлы», так и в зоне «Интернет».

Настройка параметров прокси-сервера

Система документооборота КриптоВеб для своей работы требует интернет-взамодействие автоматизированного рабочего места пользователя с защищенным сервером системы. В случае если компьютер пользователя подключен к сети Интернет напрямую либо параметры прокси-сервера указаны в настройках браузера Microsoft Internet Explorer, никаких дополнительных настроек не требуется.

При необходимости указания параметров прокси-сервера напрямую следует воспользоваться дополнительным модулем настройки соединения, который доступен по окончании установки Компонентов КриптоВеб по следующему адресу: Пуск -> Все программы -> КриптоВеб -> Компоненты -> Настройки соединения.

Модуль настройки соединения позволяет указать имя пользователя и пароль, который следует использовать Компонентам КриптоВеб при обращении к прокси-серверу. Также данный модуль имеет дополнительные настройки, которые могут использоваться при нестандартных конфигурациях сетевого оборудования.

Настройка параметров сетевого доступа

Поскольку модуль системы КриптоВеб, установленный на рабочем месте пользователя, обращается к защищенному серверу системы, то для работы могут потребоваться специальные разрешения для передачи данных со стороны антивирусного программного обеспечения и межсетевых экранов.

Для работы с демо-версией системы требуется разрешение на передачу данных по протоколу HTTP (порт 80) на адрес http://demo-cryptoweb.ru/ Как правило, никаких специальных разрешений устанавливать не требуется.

Чтобы выдать верные разрешения для работы в полной версии системы, требуется проверить следующие настройки:

- разрешение на доступ по протоколу HTTPS (порт 443) по адресам *.cryptoweb.ru в настройках межсетевых экранов;
- запрет на проверку содержимого HTTPS-трафика для антивирусных и антишпионских программ при работе с серверами *.cryptoweb.ru

Настройка полномочий доступа к папкам и файлам

Система КриптоВеб при отправке документов выполняет их подготовку, подписание и зашифрование на рабочем месте пользователя, а при получении документов — проверку подписи и расшифрование. Для этих операций Компонентам КриптоВеб требуется доступ к папкам пользователя на чтение и запись, а также создание и удаление объектов.

В стандартной конфигурации компьютера Компоненты КриптоВеб используют для работы с временными файлами папку: C:\Users\ИМЯ_ПОЛЬЗОВАТЕЛЯ\Documents\CPWActiveX, в которой автоматически создаются подпапки для хранения временных файлов. Данная папка должна быть разрешена на все операции с файлами и папками: создание, удаление, чтение и запись, а также сопутствующие операции (например, вход в папку).

Обращаем внимание, что наличие временных файлов не снижает конфиденциальность при работе с данными пользователя, поскольку временные файлы система КриптоВеб также хранит в зашифрованном виде, следовательно, без ключа подписи получить доступ к конфиденциальным данным этих файлов невозможно.

Журналы работы системы

Система КриптоВеб при своей работе автоматически создает системные журналы, по которым можно устанавливать причину возможных отказов либо неисправностей в работе системы.

В стандартной конфигурации компьютера журналы работы создаются в папке: C:\Users\ИМЯ_ПОЛЬЗОВАТЕЛЯ\AppData\Roaming\Infotrust\CPWActiveX. Создаваемые журналы в своем имени содержат дату и время начала журналирования, что упрощает поиск возможных неисправностей.

Если настроить систему не удается

Обратитесь в техническую поддержку по телефону (3412) 918-101 (для абонентов Удмуртской Республики) или на линию 8 (800) 301-81-01 (для остальных регионов Российской Федерации, звонок бесплатный). Также Вы можете оставить заявку по электронной почте support@cryptoweb.ru

4. Устранение неисправностей, выявленных в ходе эксплуатации программного обеспечения

При возникновении сбоев (ошибок, неисправностей) в системе КриптоВеб Вы можете обратиться в техническую поддержку по телефону (3412) 918-101 (для абонентов Удмуртской Республики) или на линию 8 (800) 301-81-01 (для остальных регионов Российской Федерации, звонок бесплатный). Также Вы можете оставить заявку по электронной почте support@cryptoweb.ru

Ограничения настоящего документа

Данный документ не предусматривает действий персонала при возникновении сбоев (ошибок, неисправностей), возникших за пределами системы КриптоВеб, как то:

- сбои и неполадки электропитания;
- сбои и неполадки ЛВС, в т.ч. доступа к сети Интернет;
- сбои и неполадки в техническом устройстве автоматизированного рабочего места пользователя;
- сбои и неполадки в операционной системе, драйверах либо базового программного обеспечения автоматизированного рабочего места пользователя (в том числе браузера сети Интернет), за исключением их настройки для работы системы КриптоВеб;
- сбои и неполадки установленного антивирусного, антишпионского программного обеспечения, межсетевых экранов, средств криптографической защиты информации (СКЗИ), иного программного обеспечения, за исключением их настройки для работы системы КриптоВеб.

Подобные неисправности следует выявлять и устранять согласно инструкциям к соответствующим техническим устройствам и программному обеспечению.

В СЛУЧАЕ УТЕРИ КЛЮЧА ЭЛЕКТРОННОЙ ПОДПИСИ ПРИ БЛОКИРОВКЕ ДОСТУПА К КОНФИДЕНЦИАЛЬНЫМ ДАННЫМ ПОЛЬЗОВАТЕЛЯ, ПЕРЕДАННЫМ ЧЕРЕЗ ЗАЩИЩЕННУЮ СИСТЕМУ КРИПТОВЕБ, ОПЕРАТОР СИСТЕМЫ ОТВЕТСТВЕННОСТИ НЕ НЕСЕТ.

Оператор системы сохраняет за собой право не оказывать технические консультации в случае обнаружения сбоев (неполадок, неисправностей) программного обеспечения, не относящегося к системе КриптоВеб.

Если Вы приняли решение устранить неисправность самостоятельно

При возникновении ошибки (сбоя, неисправности) на первом этапе следует по внешнему виду сообщения об ошибке или неисправности определить, в какой ситуации (при каком действии) она возникает, и предположить источник возникновения ошибки.

Очень часто начинающие пользователи принимают за ошибку любой текст, напечатанный красным цветом либо напечатанный на красном фоне. В этой ситуации обратите внимание на сообщение, которое напечатала система КриптоВеб: как правило, оно свидетельствует об ошибке самого пользователя при работе (например, пользователь некорректно заполнил поля).

Рассмотрим наиболее часто встречающиеся сообщения.

«Сервер не найден»

В данной ситуации при, казалось бы, полностью настроенной системе Ваш браузер выдает чистую страницу с сообщением о том, что связаться с сервером не удалось (внешний вид страницы может различаться в зависимости от версии браузера).

В данной ситуации следует проследить всю цепочку:
Компоненты КриптоВеб -> СКЗИ -> Браузер -> Узел связи с Интернет -> Канал связи

Неисправность может быть вызвана работой любого из этих компонентов либо работой третьих программных (технических) средств, влияющих на них: антивирусной или антишпионской программы, межсетевого экрана. Встречаются ситуации, когда сервер системы КриптоВеб недоступен ввиду работы сразу двух антивирусных программ либо физического отсутствия доступа к Интернету.

Если до настоящего момента система работала штатно, а затем появилась данная ошибка, проверьте, устанавливались ли новые программы на компьютер, выполнялось ли их обновление или перенастройка.

Полезно проверить пункты, описанные в разделе установки при нестандартной конфигурации (стр. 4). Также проверьте, не истек ли срок действия лицензии на СКЗИ КриптоПро CSP: Пуск -> Все программы -> Крипто-Про -> Управление лицензиями КриптоПро PKI. В случае если срок лицензии истек, обратитесь к Оператору за приобретением новой лицензии.

«Нет сертификатов, удовлетворяющих требованиям системы»

Ситуация может возникнуть при работе в полной версии системы. Данное сообщение означает, что система КриптоВеб не опознает ни один из квалифицированных сертификатов ключа проверки электронной подписи, установленных на Вашем рабочем месте.

Причиной могут быть следующие ситуации:

- сертификат ключа подписи только что изготовлен, и еще не зарегистрирован в системе КриптоВеб. Для регистрации сертификата обратитесь в техническую поддержку, сообщите ИНН организации, которая заключила договор с Оператором;
- срок действия сертификата ключа подписи закончился, а Вы еще не получили новый сертификат. В этом случае обратитесь в удостоверяющий центр, который Вам выдал предыдущий сертификат, и оплатите услугу изготовления нового сертификата;
- компьютер был перенастроен, и на него не установлены сертификаты, с которыми Вы работаете ранее. В этом случае обратитесь к системному администратору для повторной установки Ваших сертификатов на компьютер.

«Алгоритм ключа подписи не поддерживается»

Данное сообщение встречается при работе с сервисом «Отчетность в ФМС/МВД» и проявляется при подписании уведомлений в МВД.

Это означает, что специальное ПО КриптоПро .Net либо не установлено, либо у него закончился срок действия лицензии. Проверьте наличие лицензии на данное программное обеспечение: Пуск -> Все программы -> Крипто-Про -> Управление лицензиями КриптоПро PKI. В случае если срок лицензии истек, обратитесь к Оператору за приобретением новой лицензии.

Также данная ошибка может проявиться, если на операционные системы Microsoft Windows версий 8, 8.1, 10 установлено программное обеспечение КриптоПро .Net устаревшей версии. В этом случае переустановите его с Установочного комплекта системы КриптоВеб.

«Отображается только безопасное содержимое»

Это сообщение браузера Microsoft Internet Explorer встречается у пользователей, начавших работу в полной версии системы с сервисом «Электронный медосмотр». Оно говорит о том, что браузер настроен не полностью и не поддерживает одновременные запросы по протоколам HTTP и HTTPS.

Откройте настройки браузера: Сервис -> Свойства браузера. Перейдите на вкладку «Безопасность», затем выберите зону «Надежные узлы» и нажмите кнопку «Другой...». Пролистайте список до пункта «Отображение разнородного содержимого» и переведите переключатель в положение «Включить». Затем нажмите «ОК».

Повторите данную настройку для зоны «Интернет», затем сохраните изменения, нажав кнопку «ОК».

После этих действий следует перезапустить браузер.

Если настроить систему не удается

Обратитесь в техническую поддержку по телефону (3412) 918-101 (для абонентов Удмуртской Республики) или на линию 8 (800) 301-81-01 (для остальных регионов Российской Федерации, звонок бесплатный). Также Вы можете оставить заявку по электронной почте support@cryptoweb.ru

5. Совершенствование программного обеспечения

Система КриптоВеб находится в постоянном развитии. Большинство функций в системе КриптоВеб появляются «прозрачно» для пользователей, т.е. никаких действий по перенастройке установленных компонентов от пользователей не требуются.

Вы всегда можете узнавать о новинках системы из новостной ленты по адресу: http://www.cryptoweb.ru/news

Кроме того, три последних (наиболее актуальных) новости всегда отображаются в окне при входе в систему КриптоВеб. В случае, если новость является важной для пользователей системы, она отображается красным цветом. Например, красным цветом при входе в систему КриптоВеб отображаются новости о техническом обслуживании серверов, которые проводятся во время наименьшей нагрузки на систему (такие уведомления выдаются не менее чем за 3 суток до начала технических работ).

Обновления системы, требующие действия пользователей

Несмотря на то, что Оператор заботится о комфорте пользователей системы и выпускает обновления таким образом, чтобы все новинки в системе работали без перенастройки программного комплекса у конечных пользователей, встречаются ситуации, которые требуют действий и от пользователей.

В случае если в новом выпуске системы КриптоВеб происходит обновление клиентских компонентов, пользователи об этом уведомляются одним из двух способов:

- **в случае если обновление является обязательным**, при входе в систему автоматически предлагается обновить существующие Компоненты КриптоВеб, выполняется загрузка обновленной программы на компьютер пользователя, а затем происходит автоматическая их установка;
- **если обновление является опциональным** и требуется только для некоторых пользователей, то большинство пользователей никаких уведомлений не получают, а те пользователи, для которых оно требуется, получают уведомление о необходимости обновить Компоненты КриптоВеб при активации новой функции. В этом случае пользователям предлагается перейти в раздел «Установочный комплект» и установить обновленные компоненты.

Обновление СКЗИ

Средства криптографической защиты информации (СКЗИ) в некоторых случаях тоже нуждаются в обновлении. Например, с 1 января 2019 года в связи с Приказом ФСБ России для использования новых ГОСТ Р 34.10-2012 и ГОСТ Р 34.11-2012 требуется обновить СКЗИ КриптоПро CSP до версии 4.0.

О подобных обновлениях пользователи предупреждаются как сообщениями, которые выдаются на компьютер пользователя самими СКЗИ, так и при получении новых сертификатов ключей подписи в удостоверяющем центре.

6. Информация о персонале

Система КриптоВеб разработана для максимального удобства конечных пользователей, и при стандартной настройке Microsoft Windows, Microsoft Internet Explorer не требует специальных навыков и познаний от персонала для своей установки и эксплуатации.

К услугам пользователей системы работает техническая поддержка по телефону (3412) 918-101 (для абонентов Удмуртской Республики) или на линию 8 (800) 301-81-01 (для остальных регионов Российской Федерации, звонок бесплатный). Также Вы можете оставить заявку по электронной почте support@cryptoweb.ru

Требования к пользователям системы

От пользователей системы требуются базовые навыки работы с персональным компьютером, а также навыки:

- эксплуатации операционной системы Microsoft Windows для управления файлами и папками, открытия приложений и документов;
- работы в интернет-браузере Microsoft Internet Explorer;
- использования ключей электронной подписи и сертификатов ключей проверки электронной подписи;
- обеспечения конфиденциальности и сохранности ключей электронной подписи.

Требования к техническому персоналу

В случае если абонент принимает решение доверить настройку компьютера для работы в системе КриптоВеб наемному техническому персоналу, от такого персонала требуется наличие следующих навыков:

- установка прикладных программ, настройка полномочий доступа к файлам и папкам, сетевой безопасности в операционной системе Windows;
- настройка полномочий доступа и безопасности в интернет-браузере Microsoft Internet Explorer;
- установка и настройка параметров антивирусного (антишпионского) программного обеспечения (при необходимости);
- установка и настройка параметров межсетевых экранов (при необходимости);
- установка и настройка параметров прокси-серверов (при необходимости);
- установка и настройка средств криптографической защиты информации (СКЗИ);
- работа с ключами электронной подписи, сертификатами ключей проверки электронной подписи.

7. Гарантии Оператора

Обязанности Оператора при использовании абонентами системы КриптоВеб определяется условиями заключенного договора между Оператором и абонентом.

Гарантии работоспособности системы (SLA)

Оператор гарантирует, что защищенный сервер документооборота системы КриптоВеб функционирует в режиме 24/7/365, за исключением периода профилактических работ. О проведении профилактических работ Оператор системы уведомляет пользователей системы не позднее чем за 3 (трое) суток до момента начала проведения работ путем публикации объявлений в новостной ленте на сайте системы и дополнительного уведомления на окне входа в систему КриптоВеб.

Плановые профилактические работы проводятся, как правило, в период минимальной загрузки системы: в вечернее, ночное время, выходные дни. Общая продолжительность плановых профилактических работ не может превышать 7 часов в месяц (SLA 99%).

Экстренные (аварийные) работы проводятся в момент фиксации сбоя (аварии) в системе. Оператор выполняет экстренные (аварийные) работы по восстановлению доступа пользователей к системе в течение 4 (четырех) часов после отключения доступа к сервису.

Гарантии конфиденциальности передаваемых данных

Оператор гарантирует, что ввиду особой архитектуры системы, при условии соблюдения абонентом-отправителем и абонентом-получателем писем требований к обеспечению конфиденциальности информации на своем рабочем месте, передача сведений другому абоненту будет осуществляться при условии невозможности доступа третьих лиц (в том числе Оператора) к передаваемой информации.

Передаваемые сообщения зашифровываются таким образом, что доступ к ним может иметь только отправитель и получатель (получатели). При зашифровании тела сообщений используются сертифицированные средства криптографической защиты информации и алгоритмы ГОСТ. Установление связи используется по защищенному каналу TLS/ГОСТ. Аутентификация пользователей осуществляется исключительно по предъявленному пользователем сертификату ключа проверки электронной подписи. Иные средства аутентификации, в том числе пары «логин-пароль», в системе КриптоВеб не применяются.

Автоматизированная система КриптоВеб, имеющая класс защищенности 1Г, соответствует требованиям нормативной документации по безопасности информации, что позволяет организовать защищенную обработку конфиденциальной информации: коммерческая, служебная, банковская, врачебная и другая профессиональная тайна, персональные данные и т.п.

Гарантии доставки сообщений

Оператор гарантирует, что отправленная абонентом корреспонденция будет доставлена в адрес получателя (доступна для получения) непосредственно после отправки письма отправителем и подписания отправителем Подтверждения специализированного оператора связи. Выданное оператором Подтверждение фиксирует факт отправки документа абонентом-отправителем и может быть использовано для третьих лиц, в том числе в суде. Подтверждение подписывается квалифицированными электронными подписями отправителя и получателя (получателей).

Получатель после получения письма подписывает Квитанцию, в которой фиксируется факт получения абонентом-получателем отправленного письма. Данный факт подписывается квалифицированной электронной подписью получателя.

Гарантии авторства сообщений

Оператор гарантирует, что при условии соблюдения конфиденциальности ключевой информации конечными пользователями сообщение направляет именно то лицо, которое указано в квалифицированном сертификате ключа проверки электронной подписи, поставленной в письме. Факт авторства сообщений можно доказать в третьих организациях, в том числе, в суде.

Гарантии целостности сообщений

Оператор гарантирует, что направленная абонентом корреспонденция будет доставлена в адрес получателя (получателей) в неизменном виде. Контроль целостности сообщений осуществляется на уровне пользователя (корректность электронной подписи) и на уровне оператора (неизменность хэш-кода зашифрованного сообщения).

Вычисленный оператором хэш-код зашифрованного сообщения вносится в Подтверждение специализированного оператора связи и может быть проверен независимыми программными средствами при проведении исследования или судебной экспертизы подлинности электронного сообщения.