ООО Научно-производственное предприятие «Ижинформпроект»

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

КриптоВеб: описание функциональных характеристик ПО

(извлечение из Руководства пользователя)

Ижевск 2019

1. Назначение и функционал системы

Система защищенного электронного юридически значимого документооборота «КриптоСвязь-Веб» («КриптоВеб») – это защищенная информационная система на базе веб-технологий, предназначенная для выполнения следующих функций:

- электронный юридически значимый документооборот между организациями – отправка зашифрованных и подписанных сообщений (писем);
- электронная отчетность в контролирующие организации без дублирования на бумаге;
- автоматизация медицинских осмотров в соответствии с Приказом Минздравсоцразвития РФ от 12.04.2011 №302н.

Система КриптоВеб является системой *внешнего* документооборота и предназначена для создания защищенной среды обмена документами между предприятиями и организациями. Ключевым компонентом системы является обеспечение безопасности и юридической значимости всех передаваемых документов, в том числе, отчетов, передаваемых в контролирующие организации.

Система КриптоВеб имеет государственную регистрацию программы для ЭВМ №2013618985 от 24.09.2013 в Федеральном институте по правам собственности (ФИПС) и сертификат в системе ГОСТ Р №РОСС RU.НА36.Н01001. Товарный знак «КриптоВеб» зарегистрирован в Федеральном институте по правам собственности, регистрационный №618943 от 05.06.2017.

Система КриптоВеб подходит для передачи конфиденциальных сведений, в том числе коммерческой, служебной, банковской, врачебной и иной защищаемой законом тайны, персональных данных и т.п. Система КриптоВеб имеет аттестат соответствия классу защищенности 1Г, регистрационный №02/17К-АЗИ от 13.02.2017.

В настоящее время в системе КриптоВеб действуют следующие направления отчетности:

- отчетность в Федеральную миграционную службу России
- отчетность в Управление Росприроднадзора по Удмуртской Республике
- отчетность в МУП г. Ижевска «Ижводоканал»
- передача заявлений об изготовлении сертификата квалифицированной электронной подписи в УЦ InfoTrust ООО НПП «Ижинформпроект»

Перечень контролирующих организаций, в которые возможно представление отчетности организациями и индивидуальными предпринимателями, расширяется.

Официальный сайт системы: cryptoweb.ru

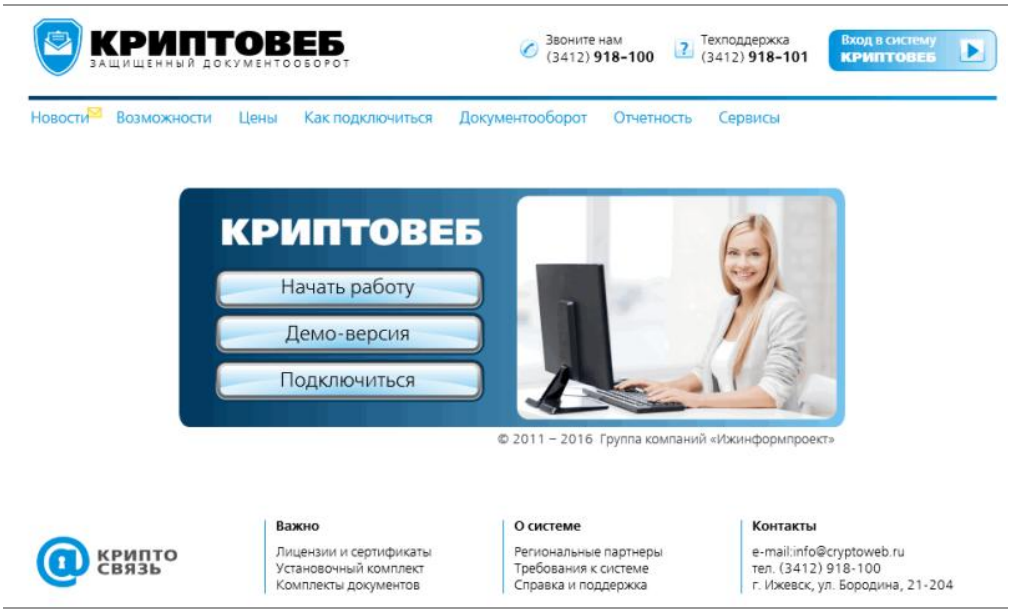

Рис. 1. Официальный сайт системы КриптоВеб.

1.1. Защищенный документооборот

Система КриптоВеб предназначена для организации защищенного электронного юридически значимого документооборота с контрагентами (государственными и муниципальными органами, предприятиями, организациями и индивидуальными предпринимателями различных форм собственности). Благодаря своей архитектуре и функционалу система обеспечивает полную юридическую аналогию традиционной почтовой (курьерской) связи с уведомлением.

Электронная корреспонденция (письмо) может в системе передаваться как отдельное отправление либо как отправление с документами-вложениями (сопроводительное письмо). Для удостоверения авторства и подлинности сообщения текст письма и д окументы-вложения подписываются усиленной квалифицированной электронной подписью отправителя. Согласно ст. 6 Федерального закона от 06.04.2011 №63-ФЗ, электронный документ, подписанный усиленной квалифицированной электронной подписью, юридически приравнивается документу на бумажном носителе, подписанному собственноручной подписью уполномоченного должностного лица и заверенному печатью организации.

Для обеспечения конфиденциальности передаваемой корреспонденции перед отправкой документ зашифровывается в адрес отправителя и получателя (получателей) на их публичных криптографических ключах, а при получении – расшифровывается приватным ключом получателя (получателей) или отправителя. Подписание, проверка подписи, зашифрование и расшифрование писем и документов-вложений к ним осуществляется криптографическими алгоритмами ГОСТ. С целью защиты каналов связи п ередача шифрограмм, формирующихся при отправке корреспонденции, осуществляется по защищенному каналу связи TLS/ГОСТ.

Применяемый в системе КриптоВеб принцип «двойного» шифрования (шифрование корреспонденции, шифрование каналов связи) гарантирует безопасность передаваемой корреспонденции от третьих лиц, в том числе и от специализированного оператора связи – оператора электронного документооборота. Прочесть исходный расшифрованный документ в системе гарантированно может только отправитель и получатель (получатели) корреспонденции.

Факт отправления корреспонденции подтверждается в системе специализированным оператором связи путем формирования Подтверждения специализированного оператора связи с указанием даты и времени отправки письма. Подтверждение оператора связи является

юридически значимым документом, который можно представить третьим сторонам, в том числе в суде.

Подписи, используемые в системе КриптоВеб, признаются на всей территории Российской Федерации.

В системе КриптоВеб документооборот можно вести в двух разделах:

ПИСЬМА – юридически значимый документооборот с контрагентами.
ОТЧЕТЫ – представление отчетности в контролирующие организации.

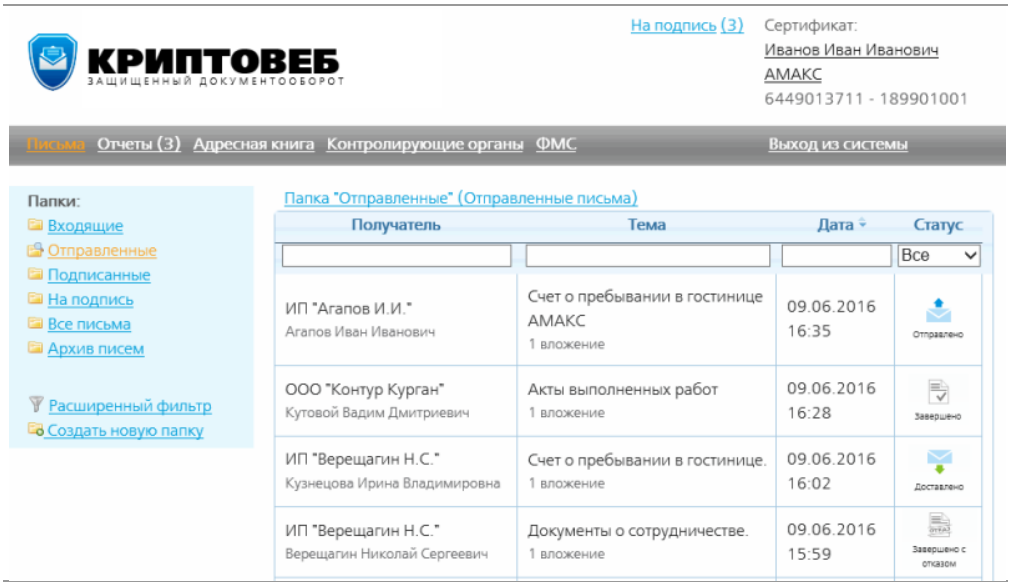

Рис. 1. Раздел ПИСЬМА.

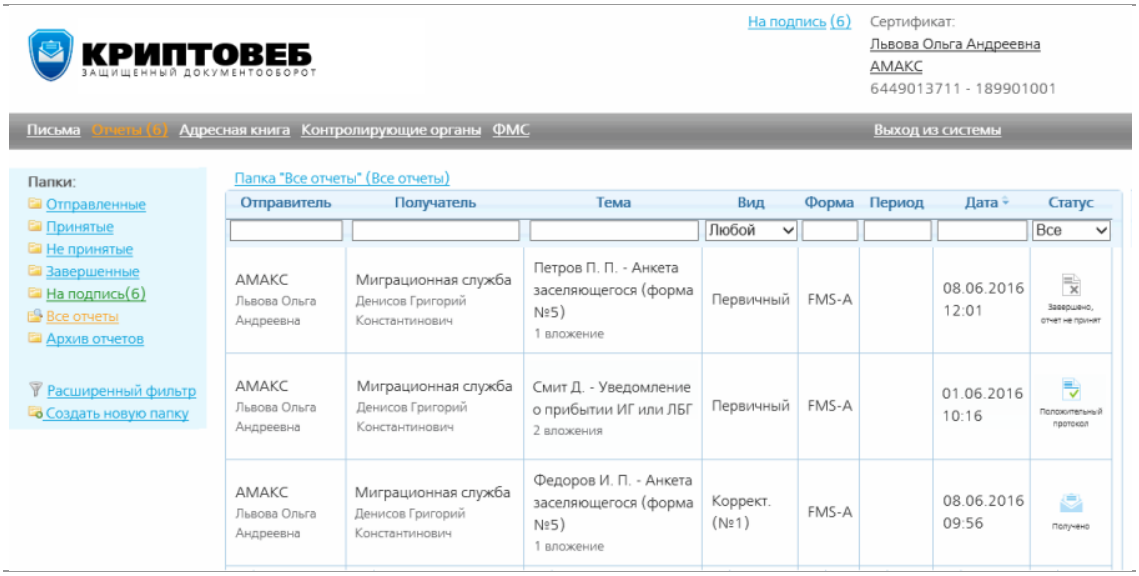

Рис. 2. Раздел ОТЧЕТЫ.

1.2. Отчетность в Федеральную миграционную службу

Сервис отправки отчетности позволяет гостиницам и приравненным к ним учреждениям (санаториям, домам отдыха, кемпингам, туристским базам и проч.) своевременно представлять сведения гостиницам и в ФМС/МВД с минимальными затратами времени.
В любой момент времени вы можете видеть статус отправленного отчета.

Оператор электронного документооборота гарантированно доставит отчет в Управление по вопросам миграции МВД субъекта РФ.

Управления по вопросам миграции МВД по субъектам Российской Федерации, на основании Договора о взаимодействии и Регламента информационного взаимодействия территориальных органов ФМС России с поставщиками учетных данных от 05.03.2014 г., предлагают абонентам системы КриптоВеб представление отчетности в электронном виде без дублирования на бумаге.

Виды отчетов в ФМС/МВД

При прибытии и убытии граждан нужно в установленные законодательством сроки представлять следующие отчеты в ФМС/МВД :

- Анкета заселяющегося (форма №5) – при прибытии граждан Российской Федерации, в течение суток после заселения. Гостиницы и приравненные к ним учреждения не представляют сведения об убытии граждан Российской Федерации.
- Уведомление о прибытии ИГ или ЛБГ – при прибытии иностранных граждан (ИГ) и лиц без гражданства (ЛБГ), в течение одного рабочего дня, следующего за днем прибытия иностранного гражданина или лица без гражданства в место пребывания.
- Уведомление об убытии ИГ или ЛБГ – при убытии иностранных граждан (ИГ) и лиц без гражданства (ЛБГ), до 12 (двенадцати) часов дня, следующего за днем убытия иностранного гражданина или лица без гражданства.

1.3. Отчетность в Росприроднадзор

Управление Росприроднадзора по Удмуртской Республике, на основании Федерального закона от 10.01.2001 № 7-ФЗ «Об охране окружающей среды» и Приказа Минприроды РФ от 09.01.2017 г. № 3 «Об утверждении Порядка представления декларации о плате за негативное воздействие на окружающую среду и ее формы», предлагает предприятиям и организациям Удмуртской Республики представление декларации по негативному воздействию на окружающую среду (декларации по НВОС) в электронном виде по телекоммуникационным каналам связи без дублирования на бумаге.

Категории объектов природопользователей

Федеральным законом от 21.07.2014 № 219-ФЗ внесены изменения в Федеральный закон от 10.01.2001 №7-ФЗ и определены категории объектов природопользователей. Объекты, оказывающие негативное воздействие на окружающую среду, в зависимости от уровня такого воздействия подразделяются на следующие категории:

- Объекты, оказывающие значительное негативное воздействие на окружающую среду и относящиеся к областям применения наилучших доступных технологий;
- Объекты, оказывающие умеренное негативное воздействие на окружающую среду;
- Объекты, оказывающие незначительное негативное воздействие на окружающую среду;
- Объекты, оказывающие минимальное негативное воздействие на окружающую среду.

Критерии отнесения объектов, оказывающие негативное воздействие на окружающую среду, к объектам I, II, III и IV категорий, утверждены Постановлением Правительства РФ от 28.09.2015 № 1029.

Порядок представления отчетности

Организации и индивидуальные предприниматели обязаны представлять отчетность по расчету платы негативному воздействию на окружающую среду (НВОС) в следующие сроки:

- за период до 2015 года включительно – ежеквартально, до 20 числа месяца, следующего за отчетным периодом, независимо от категории объекта;
- за период с 2016 года – ежегодно, до 10 марта года, следующего за отчетным периодом, лицами, обязанными вносить плату за негативное воздействие на окружающую среду (для объектов I, II, III категорий). Природопользователи объектов IV категории плату за НВОС не вносят и отчетность по расчету платы не представляют.

Обращаем Ваше внимание, что в системе КриптоВеб реализован только один вид отчетности: Декларация (расчет) платы за НВОС. Прочие виды отчетности в Росприроднадзор, как то: 2-ТП (отходы), отчет субъектов малого и среднего предпринимательства (МСП) и другие – могут быть представлены в электронном виде по телекоммуникационным каналам связи только через Портал Росприроднадзора.

1.4. Технические требования

Для подключения к системе КриптоВеб нужно иметь современный компьютер с установленной операционной системой Microsoft Windows, подключенный к сети Интернет.

Для работы с сервисом «Электронный медосмотр»

- процессор: Intel-совместимый, тактовая частота процессора: не менее 2 ГГц;
- оперативная память: не менее 3 Гб;
- скорость соединения с сетью Интернет: не менее 2 Мбит/с;
- операционная система: Windows 7, Windows 8, Windows 8.1, Windows 10;
- среда исполнения: Microsoft .net Framework версии 3.5 или выше;
- браузер сети Интернет: Microsoft Internet Explorer версии 11 или выше;
- сетевая безопасность: требуется открытый доступ по порту 443 на сайты *.cryptoweb.ru;
- офисный пакет приложений: Microsoft Office версии не ниже 2003 (включая компоненты Microsoft Word, Microsoft Excel).

Для работы с сервисами «Отчетность в ФМС», «Защищенный документооборот»

- процессор: Intel-совместимый, тактовая частота процессора: не менее 1,8 ГГц;
- оперативная память: не менее 2 Гб;
- скорость соединения с сетью Интернет: не менее 1 Мбит/с;
- операционная система: Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10;
- среда исполнения: Microsoft .net Framework версии 3.5 или выше;
- браузер сети Интернет: Microsoft Internet Explorer версии 9 или выше;
- сетевая безопасность: требуется открытый доступ по порту 443 на сайты *.cryptoweb.ru

Минимальные технические требования к рабочему месту

Предупреждение. Использование компьютера с минимальными техническими требованиями для гостиничных учреждений и медицинских организаций с большими потоками граждан настоятельно не рекомендуется.

Внимание. Сертификация средств криптографической защиты информации КриптоПро CSP версий 3.6 и 3.9, совместимых с операционной системой Windows XP, заканчивается 31 декабря 2018 года

- процессор: Intel-совместимый, тактовая частота процессора: не менее 1,5 ГГц;
- оперативная память: не менее 1 Гб;

- скорость соединения с сетью Интернет: не менее 256 Кбит/с;
- операционная система: Windows XP SP3;
- среда исполнения: Microsoft .net Framework версии 3.5 или выше;
- браузер сети Интернет: Microsoft Internet Explorer версии 8 или выше;
- сетевая безопасность: требуется открытый доступ по порту 443 на сайты *.cryptoweb.ru

1.5. Методы защиты информации

К методам защиты передаваемой информации в системе КриптоВеб относятся:

- использование защищенных сертифицированных серверов для организации документоборота;
- использование квалифицированных сертификатов для идентификации пользователей в системе;
- использование усиленных квалифицированных электроннных подписей;
- шифрование текста корреспонденции и документов-вложений;
- шифрование каналов связи.

Вышеуказанные криптографические методы защиты информации обеспечиваются сертифицированным в РФ средством криптографической защиты информации (СКЗИ) КриптоПро CSP. Для аутентификации пользователей, использования электронных подписей, шифрования данных и шифрования каналов связи применяются исключительно алгоритмы ГОСТ.

Использование сертифицированных серверов для организации электронного документооборота является одним из важнейших условий для обеспечения защиты передаваемой корреспонденции в системе КриптоВеб. Серверная площадка, обеспечивающая функционирование системы, удовлетворяет всем необходимым нормативным требованиям для обеспечения конфиденциальности информации. Аттестат соответствия системы автоматизированной системы «КриптоВеб» классу защищенности 1Г подтверждает соответствие 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.) (регистрационный №02/17К-АЗИ от 13.02.2017).

Использование квалифицированных сертификатов для идентификации пользователей в системе позволяет обеспечить целый ряд требований, предъявляемых к защищенным информационным системам, в том числе требований по идентификации личности, получающей доступ к защищенной информационной системе. Поскольку квалифицированный сертификат ключа проверки электронной подписи содержит сведения о фамилии, имени, отчестве, СНИЛС, информацию об организации-работодателе, ее ИНН, ОГРН и ряд других сведений, это позволяет однозначно установить лицо, получающее доступ к данным системы.

Требования к аккредитованным удостоверяющим центрам, указанные в ст.ст. 15, 18 Федерального закона от 06.04.2011 №63-ФЗ, позволяют достоверно установить, что квалифицированный сертификат, используемый для идентификации, применяется именно должностным лицом, указанным в теле сертификата.

Квалифицированная электронная подпись – это реквизит документа, удостоверяющий *автора подписи* и обеспечивающий *подлинность* содержимого документа. Электронная подпись является квалифицированной в том случае, если сертификат, удостоверяющий личность автора подписи (подписанта), выдан аккредитованным удостоверяющим центром, или доверенным лицом аккредитованного удостоверяющего центра, либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи.

Использование квалифицированного сертификата, согласно российскому законодательству, позволяет юридически приравнивать электронный документ, подписанный усиленной квалифицированной электронной подписью, к документу на бумажном носителе, подписанному собственноручной подписью уполномоченного должностного лица и заверенному печатью организации.

В системе КриптоВеб используются только квалифицированные сертификаты ключей проверки электронной подписи, выданные аккредитованным удостоверяющим центром InfoTrust ООО НПП «Ижинформпроект» или другими удостоверяющими центрами, включенными в перечень доверенных удостоверяющих центров системы КриптоВеб.

Сертификат ключа проверки электронной подписи выдается, как правило, на 12 месяцев и по истечении данного срока становится недействительным. Для того чтобы продолжить работать в системе электронного документооборота, следует изготовить новый сертификат. Для плановой или внеплановой замены сертификата следует обратиться в тот удостоверяющий центр, который выдал вам действующий сертификат ключа проверки электронной подписи.

Шифрование текста и вложений письма обеспечивает конфиденциальность передаваемой корреспонденции. Каждое письмо после подписания квалифицированной электронной подписью зашифровывается публичными ключами отправителя и получателя (получателей), тем самым передается уже шифрограмма текста и его вложений. Расшифровать исходное письмо и вложения к нему можно только, предъявив приватный ключ, составляющий пару к ключу шифрования, поэтому ни один участник системы, кроме отправителя и получателя (получателей), не сможет его восстановить.

Это применимо и к специализированному оператору связи – оператору электронного документооборота. Несмотря на то, что в системе КриптоВеб все документы хранятся на серверах спецоператора, получить доступ он к ним не сможет. Все, что доступно спецоператору – это идентификационные данные письма: номер документа, дата передачи, наименования отправителя и получателя (получателей), тема документа, тип и период отчетности (для отчетов).

Шифрование канала связи составляет еще один существенный раздел безопасности в системе КриптоВеб. При каждом соединении рабочего места пользователя с серверами системы КриптоВеб (при входе в систему) создается безопасное соединение по протоколу TLS/ГОСТ, причем сервер идентифицирует пользователя по сертификату его электронной подписи, а клиентское рабочее место идентифицирует сам сервер по сертификату сервера. Таким образом, организация шифрованного канала связи обеспечивает невозможность перехвата конфиденциальных сообщений третьими лицами в процессе передачи.

В рамках каждого безопасного соединения клиентское рабочее место получает одноразовый токен авторизации – своеобразный «билет» на вход в систему. Действие токена авторизации ограничено по времени: если клиентское рабочее место не выполняет никаких действий на сервере в течение 1 часа, сервер автоматически приостанавливает доступ к системе, после чего выполнение каких-либо действий без ключа электронной подписи становится невозможным. Это защищает конфиденциальные данные пользователя от действий третьих лиц, если компьютер остается включенным длительное время.

1.5.1. Электронная подпись

Электронная подпись – это специальная запись в электронном документе, которая служит для защиты данного документа от фальсификации. Электронная подпись для каждого документа уникальна и формируется методом шифрования документа с использованием закрытого ключа подписи лица, подписывающего документ. Все это позволяет однозначно определить подписанта документа и быть уверенным, что сам документ после подписания не изменялся посторонними лицами.

Проще говоря, при помощи электронной подписи можно обеспечить подлинность документа, защитить его от изменений и определить автора подписи. В случае, если электронная подпись является квалифицированной (т.е. сертификат ключа проверки электронной подписи выдан аккредитованным удостоверяющим центром), то такие документы имеют юридическую силу, а электронная подпись в них приравнивается собственноручной подписи уполномоченного должностного лица, скрепленной печатью организации.

Использование электронной подписи регламентируется Федеральным законом Российской Федерации от 06.04.2011 №63-ФЗ «Об электронной подписи».

1.5.2. Программы для работы с электронной подписью

Чтобы использовать квалифицированную электронную подпись в электронных документах, требуется наличие средства криптографической защиты информации (СКЗИ), разрешенное к использованию в Российской Федерации.

В системе КриптоВеб используются следующие средства защиты информации:

- СКЗИ «КриптоПро CSP», изготовитель – компания «КРИПТО-ПРО», г.Москва;
- ПО «КриптоПро .Net», изготовитель – компания «КРИПТО-ПРО», г.Москва (для сервиса «Отчетность в ФМС»).

1.5.3. Хранение ключа электронной подписи

Вы должны осознавать, что все функции сертификата ключа проверки электронной подписи могут быть обеспечены только при условии сохранения вами в тайне вашего закрытого ключа на ключевом носителе. В связи с этим особо обращаем ваше внимание на некоторые правила пользования сертификатом.

Выбор носителя. В процессе изготовления сертификата вы получаете его в Личном кабинете Удостоверяющего центра InfoTrust. Для надежного хранения закрытого криптографического ключа рекомендуется использовать специально предназначенные для этих целей устройства (eToken, ruToken, JaCarta и т.п.) Хранение закрытых криптографических ключей в виде файлов в операционной системе (реестр Windows) допускается только в случае принятия дополнительных мер по обеспечению защиты компьютера от несанкционированного доступа с помощью сертифицированных в установленном порядке средств.

Хранение ключей. Носители ключей необходимо хранить в условиях, исключающих доступ к ним посторонних лиц (сейф, металлический шкаф, персональный ящик и т.п.) Использование. Для безопасного использования криптографических ключей рекомендуется принять меры по оборудованию, охране и организации режима в помещении, где установлены СКЗИ и хранятся ключевые документы.

Взаимодействие с удостоверяющим центром. Пользователь должен незамедлительно сообщать в установленном порядке о фактах доступа (вероятного доступа) к закрытому ключу посторонних лиц. При этом, до выяснения фактов наличия компрометации ключей действие сертификата приостанавливается. В случае, если компрометации ключей не было – сертификат возобновляется, в противном случае – отзывается (аннулируется), с последующим выпуском нового сертификата.

Наличие резервной копии ключа. На случай утери основного ключа (или сбоя носителя) рекомендуется иметь резервную копию. Копия должна находиться с соблюдением должной осторожности при хранении; рекомендуется хранить ее в сейфе.

Пользователь должен своевременно сообщать об изменении значимых атрибутов (параметров), в том числе включаемых в сертификат (изменение ФИО, паспортных данных, должности, наименования и реквизитов организации и т.п.)

1.6. Юридическая значимость

Все электронные документы, которыми абоненты обмениваются через КриптоВеб, имеют такую же юридическую значимость, как традиционные (бумажные) документы с собственноручной подписью уполномоченного должностного лица, скрепленной печатью организации.

Юридическая значимость документов обеспечивается принятием участниками документооборота единого регулирующего документа: Регламента системы КриптоВеб , а также следующими составляющими:

Авторство документа. Доказывается составом сертификата усиленной квалифицированной электронной подписи в документе. Когда электронный документ подписан цифровой подписью, выданной организации, — это доказательство того, что документ создан именно этой организацией и подписан должностным лицом, указанным в сертификате электронной подписи.

Целостность документа. Обеспечивается наличием электронной подписи, поскольку она, помимо данных сертификата, содержит в себе хэш документа — уникальный идентификатор документа, вычисляемый в зависимости от содержимого самого документа. Если в подписанном документе изменить хотя бы один символ, при получении документа электронная подпись будет неверна. Специализированный оператор связи дополнительно вычисляет хэш криптограммы документа и публикует его в Подтверждении оператора связи . Таким образом, в спорных ситуациях всегда можно доказать, какой именно документ был направлен средствами системы.

Неотрекаемость . Доказывается подписями сторон документооборота: отправителя, получателя (получателей) и специализированного оператора связи в Подтверждении оператора связи. Подтверждение — это служебный документ, который выдается при отправке письма. Участник документооборота подписывает Подтверждение оператора связи при отправке (получении) документа, тем самым признает существование электронного документа и, в дальнейшем, не может отречься от этого факта.

Конфиденциальность. Третьи лица, в том числе специализированный оператор связи, не могут просмотреть переданный через систему КриптоВеб документ. Конфиденциальность обеспечивается принципом двойного шифрования: шифрованием содержимого письма и шифрованием канала связи. Письмо — его текст и вложения — могут просмотреть только сами участники документооборота: отправитель и получатель (получатели).

Гарантия отправки письма. Доказывается указанием времени отправки письма в Подтверждении оператора связи. Подтверждение подписывается всеми тремя сторонами документооборота: отправителем, получателем и специализированным оператором связи, и является юридическим аналогом квитанции об отправке традиционного письма с уведомлением в почтовом отделении.

Гарантия получения письма. Доказывается подписанием Квитанции о получении письма получателем (получателями). Квитанция подписывается в момент получения документа Получателем письма и является юридическим аналогом уведомления о вручении письма адресату при традиционном документообороте (почтовой или курьерской связи).

1.7. Отличия от иных систем документооборота

Для успешного применения системы электронного документооборота в делопроизводстве полезно придерживаться следующего принципа: *каждый объект, используемый в традиционном (бумажном) документообороте, должен иметь свой аналог в электронном документообороте.* Именно поэтому при выборе системы внешнего электронного документооборота следует обращать особое внимание не только на простоту и удобство работы в системе, не только сравнивать ценовые предложения различных систем, но и особо

рассмотреть моменты, которые будут необходимы при взаимодействии с третьими лицами, в том числе в судебных разбирательствах.

Наиболее существенными аспектами при изучении системы внешнего электронного документооборота является надежная структурная организация системы и качество оказания услуг оператором.

КриптоВеб – это информационная система, а не просто программа для ЭВМ. Это означает, что абонент не остается один-на-один с программой на свой страх и риск, а получает качественные услуги электронного документооборота от Специализированного оператора связи, включающие в себя:

- *работу системы в режиме 24/7/365,* за исключением времени технического сопровождения серверов. Пользователи системы в обязательном порядке уведомляются о дате и времени технического сопровождения за 3 дня до начала работ путем размещения объявления на стартовой странице системы;
- *гарантированную доставку конфиденциальной корреспонденции* от отправителя до получателя в установленные Регламентом системы сроки с использованием усиленной квалифицированной электронной подписи и шифрования передаваемых сообщений;
- *консультационную и техническую поддержку* пользователей по телефону и электронной почте, а также, при наличии заявки абонента, выездную техническую поддержку (оплачивается по отдельному тарифу).

Выбирая иного оператора электронного документооборота, в первую очередь всегда обращайте внимание на предмет договора. Если предметом договора является исключительно поставка программно-аппаратного комплекса или передача лицензионных прав на использование программы для ЭВМ, помните, что ответственность за целостную и конфиденциальную доставку документов до получателя такой оператор не несет.

КриптоВеб – это защищенная информационная система , полностью соответствующая действующему законодательству Российской Федерации и действующим нормативным актами, использующая для подписи и шифрования данных исключительно алгоритмы ГОСТ и аттестованная по классу защиты 1Г для работы с конфиденциальными сведениями:

- персональные данные;
- коммерческая тайна;
- профессиональная тайна;
- врачебная тайна;
- банковская тайна;
- иная защищаемая законом тайна.

Системой КриптоВеб пользуются государственные и муниципальные учреждения, коммерческие предприятия и организации, индивидуальные предприниматели и иные абоненты. При работе в системе КриптоВеб важно понимать, что доступ к электронной корреспонденции, передаваемой в системе, предоставляется *только отправителю и получателю*, так как все документы в системе зашифровываются с применением сертифицированных алгоритмов шифрования ГОСТ. Третьи лица, в том числе и сам оператор, доступа к конфиденциальной информации абонентов не имеют.

КриптоВеб – это юридически значимая информационная система, следовательно, электронные документы, направляемые через данную систему, способны вызывать правовые последствия. Использование электронных документов при гражданско-правовом взаимодействии между предприятиями, организациями, индивидуальными предпринимателями регламентировано целым рядом законодательных и нормативных актов, одним из центральных в которых является

Федеральный закон от 06.04.2011 г. № 63-ФЗ «Об электронной подписи». Система позволяет подтвердить следующие юридические факты:

- подтвердить авторство документа – удостоверить личность автора электронной подписи в документе;
- подтвердить факт отправки документа от отправителя к получателю, а также зафиксировать дату и время такой отправки;
- обеспечить целостность отправки, т.е. зафиксировать содержимое отправленного документа с невозможностью его подмены;
- подтвердить факт получения документа получателем;
- обеспечить неотказуемость отправителя и получателя от факта существования документа, его отправки и получения.

Использование системы КриптоВеб гарантирует, что электронные документы, которыми обмениваются абоненты в системе, имеют такую же юридическую значимость, как традиционные (бумажные) документы с собственноручной подписью уполномоченного должностного лица, скрепленной печатью организации.

В системе КриптоВеб абонент и пользователь – не одно и то же. Уже на уровне архитектуры системы определяется, что абонент (а точнее, участник системы) – это *организация или индивидуальный предприниматель*, а пользователь системы – это *должностное лицо*, получающее доступ к системе. Таким образом, юридически мы не просто отправляем письмо на адрес организации, где получатель может быть любым, а указываем одно или несколько должностных лиц, в адрес которых направляется письмо.

Если отправитель не знает, кому конкретно должно быть направлено письмо, он может адресовать письмо руководителю организации либо направить ее в подразделение в случае, если получатель создал соответствующие группы доступа. Скажем, если получатель заранее создал группы доступа «Бухгалтерия», «Канцелярия», «Отдел продаж», то отправителю будет заметно удобнее посылать корреспонденцию, а получатель сможет в любое время изменять состав групп доступа.

1.8. Приобретение системы КриптоВеб

Для приобретения системы КриптоВеб необходимо сделать следующее:

- **Проверьте готовность рабочего места.**
  Перед оформлением документов ознакомьтесь с техническими требованиями к системе КриптоВеб и убедитесь, что компьютер, на котором будет установлено рабочее место системы, соответствует заданным требованиям.
- **Приобретите лицензию на СКЗИ КриптоПро CSP.**
  Для работы в системе требуется средство криптографической защиты информации (СКЗИ) КриптоПро CSP версии 4.0 или выше. Вы можете использовать уже имеющуюся у Вас лицензию или приобрести ее, в том числе и в Группе компаний Ижинформпроект.
- **Подготовьте документы на пользователей системы КриптоВеб.**
  Для обеспечения безопасности конфиденциальных данных и юридической значимости документов каждый участник системы обязан получить квалифицированный сертификат ключа проверки электронной подписи в Удостоверяющем центре InfoTrust или другими удостоверяющими центрами, включенными в перечень доверенных удостоверяющих центров системы КриптоВеб. Оформите комплект документов в соответствии с рекомендациями.
- **Заключите договор на доступ к системе КриптоВеб.**
  Определите тариф, по которому Вы будете получать услуги доступа к системе и заполните комплект документов на подключение. Вам выставят счет на предоплату услуг предоставления доступа к системе КриптоВеб по выбранному Вами тарифному плану.

- Оплатите предоставленные счета.
  Подключение к системе будет выполнено в течение двух рабочих дней. Вы можете заказать дополнительно выезд специалиста, который выполнит установку системы «под ключ» и окажет консультационные услуги по порядку пользования программой непосредственно на Вашем рабочем месте.

Ознакомиться с действующими ценами на услуги доступа к системе КриптоВеб можно на сайте системы в разделе Цены.

Ознакомиться с комплектами документов на подключение и скачать их можно на сайте системы в разделе Комплекты документов.