**План работ**

06.06 – 12.06 – Развертывание основной архитектуры системы

13.06 – 19.06 – Развертывание блока управления пользователями

20.06 – 26.06 – Реализация функций документооборота

27.06 – 03.07 – Реализация функций документооборота

04.07 – 10.07 – Внедрение модуля ЭЦП

11.07 – 17.07 – Реализация прочих функциональных требований

18.07 – 24.07 – Разработка системы уведомлений

25.07 – 31.07 – Тестирование и устранение выявленных недочетов

1. **Общие требования.**
   1. Программа должна позволять вести юридически значимый электронный документооборот (далее – ЭДО) между Лицензиатом и контрагентами Лицензиата. Используемый для ЭДО вид электронной подписи должен соответствовать усиленной квалифицированной электронной подписи в соответствии с Федеральным законом от 06.04.2011г. №63-ФЗ.
   2. Стороной (контрагентом) Лицензиата по ЭДО может являться как юридическое лицо, индивидуальный предприниматель, так и физическое лицо.
   3. Программа должна быть установлена на серверах Лицензиата. Пользователи Лицензиата и контрагентов Лицензиата получают доступ к Программе посредством подключения по зашифрованному протоколу через WEB-интерфейс на домене 3-его уровня сайта Лицензиата, например, <https://edo.xxxxxx.ru>.
   4. Составить, подписать и направить электронный документ в Программе может как Лицензиат, так и контрагент Лицензиата, при этом контрагент Лицензиата может направить электронный документ только Лицензиату.
   5. Электронный документ должен иметь признаки типа документа (например, договор, соглашение, письмо и пр.).
   6. Электронному документу может быть присвоен статус «Удален» в случае, если он не подписан направляющей стороной.
   7. Программа не должна удалять физически файлы из хранилища используемые при ЭДО, только скрывать документы со статусом удален.
   8. Программа должна иметь возможность направлять уведомления на электронную почту пользователя (при получении нового документа, при необходимости совершить действие с документом, при завершении документооборота и пр.).
   9. Программа должна логировать и протоколировать все действия пользователей, а также действия самой Программы по передаче/обработки документа. В Программе должен быть предусмотрен журнал для просмотра событий или возможность отправки событий по syslog. Минимальный уровень логирования:

* Вход в систему (*дата, время, IP-адрес, логин*);
* Выход из системы (*дата, время, IP-адрес, логин*);
* Настройка системы (*дата, время, IP-адрес, логин, измененный параметр (что было, что стало)*);
* Работа с пользователями (*дата, время, IP-адрес, логин, операция (создание, удаление, блокировка, изменение параметров, назначение ролей и т.п.)*);
* Работы с документами (*дата, время, название/номер, тип действия*).
  1. Программа должна иметь функционал по ручной блокировке пользователей.
  2. Необходимо установить время жизни сессии – 10 минут.
  3. Программа должна работать по HTTPS протоколу.

1. **Политики в отношении используемых паролей.**
   1. В Программе должно быть установлено ограничение на использование в качестве пароля идентификатора пользователя.
   2. Пароли пользователей должны меняться каждые 90 дней. Установление для пользовательских учетных записей опции «Не менять пароль пользователя» – не допустимо.
   3. При вводе пароль должен быть маскированным.
   4. При первом входе Программа должна предложить поменять пароль.
   5. Установление для пользовательских учетных записей опции «Не менять пароль пользователя» – не допустимо.
   6. Требования к сложности пароля:

* минимальная длина пароля - настраиваемое значение (не менее 12);
* пароль должен содержать буквы в различном регистре, цифры и спецсимволы (не менее 2 каждого типа символов);
* пароль не должен совпадать с логином пользователя;
* пароль в БД не должен храниться в открытом виде (комментарий: base64 не является шифрованием, приравнивается к отрытому виду). Предпочтительный вид - sha256 (solt+password);
* срок жизни пароля - настраиваемое значение (начальное значение 90 дней)
* Программа не должна позволять задавать N-предыдущих паролей (настраиваемое значение, не менее 5);
* первоначальный пароль должен соответствовать парольной политике, обязательная смена при первом входе (аналогично для пароля восстановления);
* при сбросе пароля пользователю должна приходить ссылка с токеном на сброс. Ссылка должна быть временной.
  1. Парольная политика может быть различной для различной роли (например, для сотрудников Лицензиата политика может отличаться, т.е. быть более строгой).
  2. В Программе должна быть реализована защита от подбора пароля:
* временная задержка после 3 неуспешной попытки входа в систему для логина или IP-адреса пользователя - 1 минута;
* временная задержка после 4 неуспешной попытки входа в систему для логина или IP-адреса пользователя - 10 минута;
* блокировка логина или IP-адреса после 5 неуспешной попытки входа на 1 час
* использование CAPTCHA-проверки;

1. **Роли и привилегии пользователей Программы.**
   1. Роли:
      1. Пользователь: вход в Программу, просмотр документов.
      2. Сотрудник: вход в Программу, просмотр всех документов.
      3. Администратор: управление (добавление/редактирование/удаление) уполномоченных лиц, управление профилем организации, настройка типов документов, настройка парольной политики.
   2. Привилегии (могут быть даны любому пользователю, для доступных документов):
      1. Создание, удаление (без физического удаления документа) новых документов.
      2. Подписание электронного документа (при наличии УКЭП у уполномоченного лица).
   3. Любой пользователь контрагента Лицензиата в Программе может иметь доступ (для просмотра/редактирования/создания и пр.) только к документам контрагента, пользователем которого он является.
2. **Подключение.**
   1. При регистрации учетной записи пользователя в системе должны быть предусмотрены следующие обязательные поля для заполнения:

* имя учетной записи пользователя (email);
* ФИО владельца учетной записи;
* уникальный идентификатор пользователя, позволяющий однозначно идентифицировать сотрудника и сопоставить учетную запись с его учетными записями в других системах (только для сотрудников Лицензиата);
* юридическое лицо (организация) пользователя;
* подразделение (опционально);
* должность (опционально);
* контактный телефон (опционально).
  1. Регистрация контрагента Лицензиата и его уполномоченных лиц в Программе осуществляется Лицензиатом самостоятельно непосредственно в Программе.
  2. После регистрации уполномоченному лицу по электронной почте, указанной при регистрации, направляется уникальная ссылка для авторизации (подтверждения учетной записи).
  3. Уполномоченное лицо пройдя по ссылке авторизуется в Программе.

1. **Авторизация.**
   1. Авторизация уполномоченного лица Лицензиата/контрагента Лицензиата осуществляется либо по логину и паролю, либо по сертификату УКЭП. Без аутентификации вход должен быть запрещен.
   2. Программа не должна позволят авторизоваться:

* по истекшему сертификату (допускается вход по логину и паролю);
* блокированному пользователю.
  1. Программа должна предложить поменять пароль при первом входе.

1. **Электронная подпись.**
   1. Программа должна позволять обмениваться электронными документами с электронной подписью с двух сторон. Электронная подпись должна соответствовать требованиям усиленной квалифицированной электронной подписи в соответствии с Федеральным законом от 06.04.2011 №63-ФЗ «Об электронной подписи» (далее- 63-ФЗ). Электронная подпись может быть выдана любым аккредитованным согласно требованиям 63-ФЗ удостоверяющим центром.
   2. Программа должна использовать ПО КриптоПро CSP v5 КС2.
   3. Участники ЭДО (со стороны Лицензиата и контрагента Лицензиата) должны иметь возможность проверить подписи под документом, выгруженном на локальный компьютер без авторизации в Программе.
2. **Требования к пользовательскому интерфейсу.**
   1. Программа должна иметь web-интерфейс брендированный в соответствии с требованиями Лицензиата (для Лицензиата и контрагента Лицензиата).
   2. Интерфейс Программы у участников ЭДО:

* Должен иметь список документов, отображаемый в виде структуры: тип получателя документа (в структуре организации), тип документа с возможностью фильтрации и поиска.
* должен отображать уведомления о событиях ЭДО (получен документ, необходимо согласовать/подписать документ и пр.).
* под документом должен отображаться текущий статус, информации о подписании (указание лиц, подписавших документ и результат проверки электронной подписи).
* Должен позволять совершить действия с документом в части электронного документооборота (в зависимости от наличия полномочий у уполномоченного лица, текущего статуса документа, нахождение у направляющей или у принимающей стороны): создать (с загрузкой файлов), сохранить как черновик, направить на согласование, согласовать, направить на подписание, подписать, отказать, отклонить, отказать, проверить подпись.
* документ можно просмотреть, распечатать, сохранить копию, сохранить оригинал (с электронной подписью).
* должен иметь административный раздел: изменение структуры организации, создание/редактирование/удаление пользователей, смена логина/пароля/адреса электронной почты/телефона.
  1. Лицензиат должен иметь список документов всех контрагентов Лицензиата с фильтрацией по контрагенту.