

Инструкция по настройке модуля расширения Bicrypt Signing

Назначение документа

В системе DIRECTUM для подписания электронной подписью (ЭП) можно использовать средство криптографической защиты информации (СКЗИ) Бикрипт-КСБ-С.

Бикрипт-КСБ-С имеет сертификат соответствия ФСБ, на основании которого может использоваться для обеспечения целостности и подлинности информации, не содержащей сведений, составляющих государственную тайну. Поэтому Бикрипт целесообразно использовать вместо стандартных встроенных в Microsoft Windows СКЗИ при организации юридически значимого документооборота на предприятиях.

Для хранения ключей в Бикрипт-КСБ-С используются контейнеры. Контейнеры можно создавать на различных устройствах, в зависимости от установленных драйверов (Touch Memory, дискета). Контейнеры могут быть защищены паролем, что обеспечивает двухуровневую аутентификацию и, как следствие, большую достоверность ЭП по сравнению с СКЗИ Microsoft Windows.

Бикрипт-КСБ-С полностью поддерживается модулем расширения Bicrypt Signing системы DIRECTUM. Бикрипт-КСБ-С может использоваться как вместо стандартных СКЗИ Microsoft Windows, так и совместно с ними.

Описание настройки модуля расширения Bicrypt Signing см. в разделе [«Настройка модуля расширения Bicrypt Signing»](#).

Перечень терминов и сокращений

Электронная подпись

Реквизит электронного документа, удостоверяющий автора подписи и гарантирующий неизменность документа после его подписания.

СКЗИ

Средство криптографической защиты информации.

Настройка модуля расширения Bitcrypt Signing

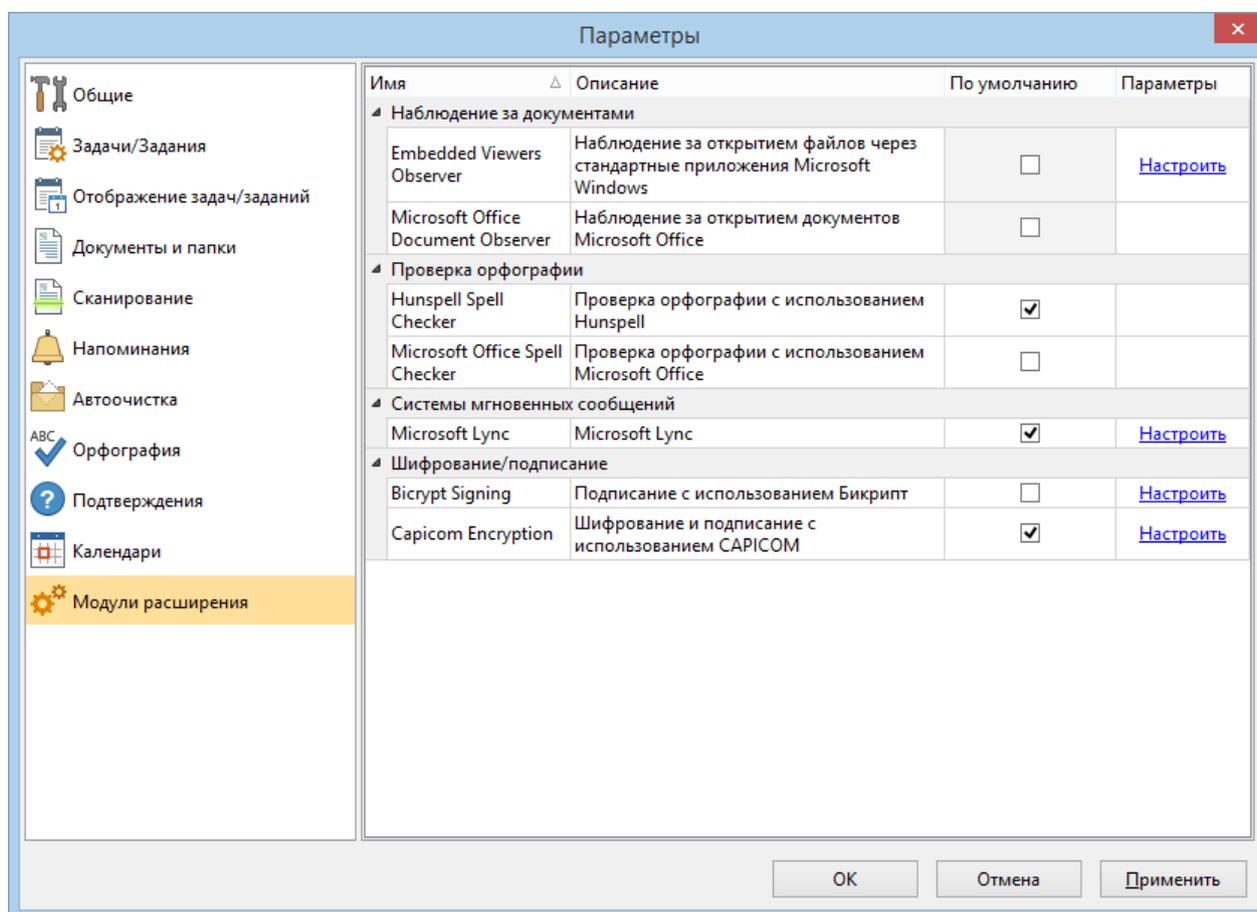
Настройка модулей расширения осуществляется из окна параметров проводника системы.

Для любой настройки модуля расширения может быть задано два значения:

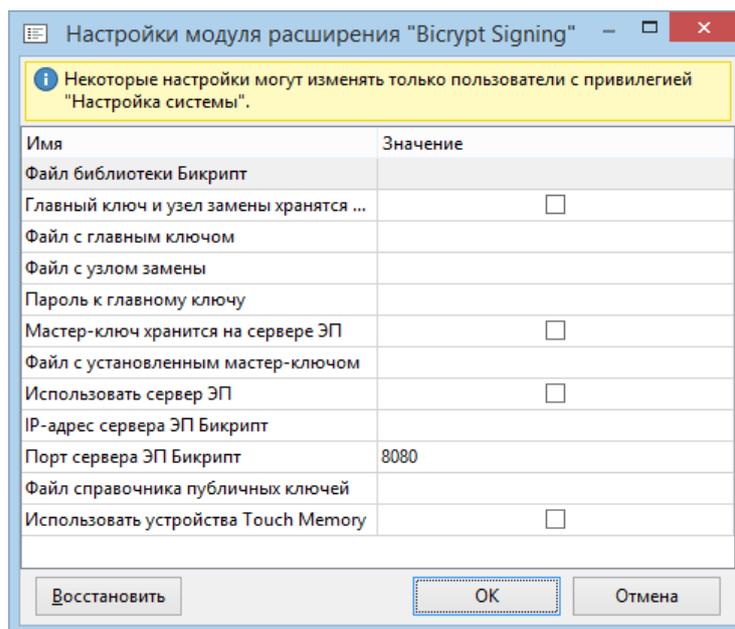
- **Личное.** Значение будет действовать только на текущем рабочем месте пользователя. Значение по умолчанию задает администратор. Пользователь может изменить значение, если в системе не установлен запрет на изменение личных настроек;
- **Общее.** Значение действует для системы в целом. Его может задавать только администратор системы.

Чтобы настроить модуль расширения Bitcrypt Signing:

1. В проводнике системы в меню **Сервис** выберите пункт **Параметры**. Откроется окно «Параметры».
2. Перейдите на закладку «Модули расширения»:



3. В строке **Bicrypt Signing** перейдите по ссылке **Настроить**. Откроется окно «Настройки модуля расширения «Bicrypt Signing». Для пользователей окно имеет вид:



Для администраторов – см. раздел [«Параметры модуля расширения Bicrypt Signing»](#).

При наличии только одного значения настройки (только личного или только общего) модуль расширения будет использовать указанное значение. Это позволяет быстро произвести первоначальную настройку: администратору следует задать общие значения для всех необходимых настроек, после чего эти значения автоматически будут применяться на всех рабочих местах системы, так как пользовательские настройки на них будут не определены.

При наличии одновременно и личного и общего значения, используемое в работе значение выбирается согласно приоритету. Приоритетное значение настройки определяет модуль расширения, для администратора приоритет отображается в режиме «Только чтение».

При настройке модуля расширения пользователем системы, не являющимся администратором, отображается упрощенное окно настройки, не содержащее колонок «Общее значение» и «Приоритетное значение». В этой ситуации можно изменять значения только тех настроек, для которых приоритетным является личное значение. Изменять значения можно, если в системе не установлен запрет на изменение личных настроек.

Администратор системы может установить запрет на изменение настроек модуля пользователям системы. Настройка задается в карточке константы **UserCanChangePluginSettings** в поле **Значение**. Возможные значения константы:

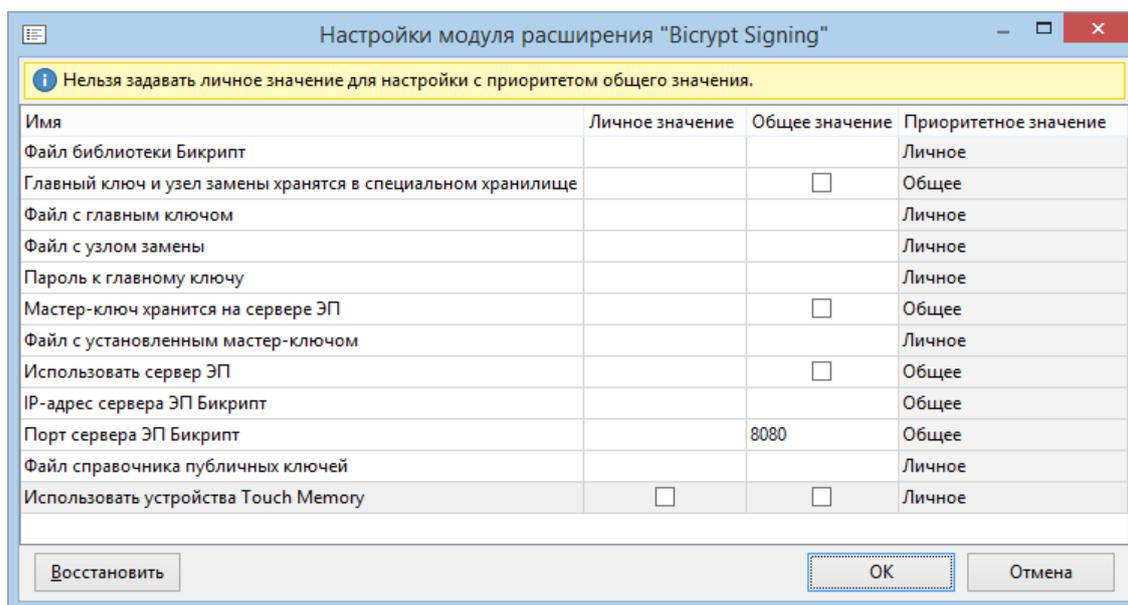
- **Да** – пользователю доступно изменение личных настроек модулей расширения;
- **Нет** – изменение личных и общих настроек модулей расширения доступно только администратору системы. Для изменения личных настроек необходимо выполнить вход на локальный компьютер пользователя под его учетной записью Windows и зайти в систему под учетной записью администратора с SQL-аутентификацией.

По умолчанию установлено значение **Да**.

Модуль расширения определяет первоначальные значения настроек. Чтобы восстановить значения настроек, предлагаемые модулем расширения, нажмите на кнопку **Восстановить**.

Параметры модуля расширения Bcrypt Signing

Окно настройки модуля расширения Bcrypt Signing имеет вид:



Для каждого рабочего места можно переопределить значения параметров:

- **Файл библиотеки Бикрипт.** Путь к файлу динамической библиотеки Бикрипт. Обычно файл называется **bicr_adm.dll**;
- **Файл с главным ключом.** Путь к файлу с главным ключом. Параметр не используется, если:
 - указан признак использования главного ключа и узлов замены с сервера ЭП;
 - используется версия библиотеки Бикрипт без шифрования;
- **Файл с узлом замены.** Путь к файлу с узлами замены. Параметр не используется, если:
 - указан признак использования главного ключа и узлов замены с сервера ЭП;
 - используется версия библиотеки Бикрипт без шифрования;
- **Пароль к главному ключу.** Пароль, на котором зашифрован главный ключ;
- **Файл с установленным мастер-ключом.** Путь к файлу с установленным мастер-ключом. Устанавливать мастер-ключ для использования следует стандартными средствами Бикрипт. Если мастер-ключ не используется, то параметр следует оставить пустым. Если используется мастер-ключ с сервера ЭП, то параметр игнорируется;
- **Файл справочника публичных ключей.** Путь к файлу-справочнику публичных ключей. Если используется справочник публичных ключей, хранящийся на сервере ЭП, то в параметр записывается идентификатор базы сервера ЭП для использования;
- **Использовать устройства Touch Memory.** Признак использования устройств Touch Memory на данном рабочем месте.

Значения остальных параметров устанавливаются администратором и являются общими для всех рабочих мест:

- **Главный ключ и узел замены хранятся в специальном хранилище.** Признак использования главного ключа и узлов замены из специального хранилища (устройств Touch Memory или сервера ЭП);
- **Мастер-ключ хранится на сервере ЭП.** Признак использования в системе мастер-ключа, хранящегося на сервере ЭП;

- **Использовать сервер ЭП.** Признак использования сервера ЭП в системе;
- **IP-адрес сервера ЭП Бикрипт.** IP-адрес сервера ЭП. Если сервер ЭП не используется или на всех машинах настроен IP-адрес сервера ЭП средствами Бикрипт, то данный параметр можно не заполнять;
- **Порт сервера ЭП Бикрипт.** Порт сервера ЭП. Если не установлен параметр **Использовать сервер ЭП**, то IP-адрес сервера можно не указывать. Если сервер ЭП не используется или на всех машинах настроен IP-адрес сервера ЭП средствами Бикрипт, то данный параметр можно не заполнять.

Порядок подписания с использованием Бикрипт см. в разделе [«Подписание с использованием Бикрипт»](#).

Подписание с использованием Бикрипт

После первоначальной настройки модуля расширения необходимо зарегистрировать сертификаты пользователей. Подробнее см. в руководстве администратора DIRECTUM, в инструкции по работе с сертификатами пользователей в системе DIRECTUM, раздел «Регистрация сертификатов в системе DIRECTUM».

После регистрации сертификата пользователи могут выполнять подписание. Подробнее см. в руководстве пользователя:

- в главе «Документы», раздел «Подписание документов»;
- в главе «Задачи и задания», раздел «Подписание задач и заданий».