Телефон в Ижевске: +7 (3412) 72-11-00
Телефон в Москве: +7 (499) 277-1560
Сайт: www.directum.ru
E-mail: support@directum.ru

Настройка протокола аутентификации Kerberos для работы с Портальными компонентами DIRECTUM для SharePoint

Назначение документа

В документе описан порядок настройки сетевого протокола аутентификации Kerberos для работы с Портальными компонентами DIRECTUM для SharePoint 2010 и 2013, а также возможные способы решения при возникновении проблем.

Содержание

Перечень терминов и сокращений

Service Principal Name (SPN)

Имя службы. Позволяет однозначно идентифицировать экземпляр службы.

Internet Information Service (IIS)

Службы являются компонентами Windows и облегчают публикацию информации и внедрение деловых предложений в Интернете. IIS упрощает создание платформы для сетевых приложений.

Настройка протокола аутентификации Kerberos

Настройка протокола аутентификации Kerberos при работе с Портальными компонентами DIRECTUM для SharePoint необходима, если будет происходить запуск процессов SBRte. Настройка протокола разрешает возможные проблемы:

- при открытии страницы для создания задачи возникает ошибка «Неправильное имя пользователя или пароль»;
- документы размещаются в DIRECTUM от имени общего пользователя, несмотря на то, что пользователь SharePoint обладает необходимыми правами доступа на систему DIRECTUM;
- на SQL-сервере в событиях системы в журнале Windows «Приложение» регистрируется событие об отказе в доступе для анонимного пользователя.

Порядок настройки см. в разделе «Настройка для работы с Портальными компонентами DIRECTUM для SharePoint 2010» или «Настройка для работы с Портальными компонентами DIRECTUM для SharePoint 2013», в зависимости от версии приложения.

Список возможных проблем при работе с Портальными компонентами DIRECTUM и предложенные решения см. в разделе «Возможные проблемы при работе Портальных компонентов DIRECTUM для SharePoint и способы их решения».

Настройка для работы с Портальными компонентами DIRECTUM для SharePoint 2010

1. Настройте имена участников службы SPN
2. Настройте доверие для делегирования служб Kerberos

Настройка имен участников службы Service Principal Name (SPN)

1. Установите утилиту Setspn на компьютер в домене, с которого планируется настраивать имена SPN. Утилиту можно бесплатно скачать с сайта компании Microsoft.
2. Настройте учетную запись пользователя пула приложений.
3. Настройте имена SPN для веб-сервера.
4. Настройте имена SPN для SQL-сервера.

Добавлять и удалять имена SPN может только администратор домена. Просматривать список зарегистрированных имен SPN может любой пользователь домена.

Настройка учетной записи пользователя пула приложений SharePoint 2010

1. На контроллере домена запустите оснастку «Active Directory – Пользователи и компьютеры».
2. Если в свойствах учетной записи пользователя пула приложений отсутствует закладка «Делегирование», то выполните команду:

   setspn -R SPAdmin

   где **SPAdmin** – имя пользователя, которому необходимо доверить делегирование служб.
3. Проверьте список имен SPN, назначенных для учетной записи пользователя. Выполните команду:

   setspn -L SPAdmin

   где **SPAdmin** – учетная запись, от имени которой работает пул приложений.

   В списке должны присутствовать записи:

   - HOST/SPAdmin;
   - HOST/SPAdmin.domain.local, где **domain.local** – DNS-суффикс домена; **SPAdmin** – учетная запись, от имени которой работает пул приложений;
   - HTTP/SPServer;
   - HTTP/SPServer.domain.local, где **domain.local** – DNS-суффикс домена; **SPServer** – имя сервера, на котором размещен веб-сервер SharePoint.
4. Если одной или нескольких указанных записей нет, то зарегистрируйте имена SPN для каждой записи, выполнив команды:

   ```
   setspn -A HTTP/SPServer SPAdmin
   setspn -A HTTP/SPServer.domain.local SPAdmin
   setspn -A HOST/SPAdmin SPAdmin
   setspn -A HOST/SPAdmin.domain.local SPAdmin
   ```
5. Зарегистрируйте имя SPN для учетной записи пользователя пула приложений:

   setspn -A http/www.mysite.com SPAdmin, где:

   - **SPAdmin** – учетная запись, от имени которой работает пул приложений;
   - **www.mysite.com** – URL, по которому идет обращение к сайту.

Настройка имен SPN для веб-сервера

1. На контроллере домена запустите оснастку «Active Directory – Пользователи и компьютеры».
2. Проверьте список имен SPN, зарегистрированных на веб-сервере. Выполните команду:

   setspn -L SPServer

   где **SPServer** – имя сервера, на котором размещен веб-сервер SharePoint.

   В списке должны присутствовать следующие записи:

   - HOST/SPServer;
   - HOST/SPServer.domain.local, где **domain.local** – DNS суффикс домена; **SPServer** – имя сервера.
3. Если указанных записей нет, то добавьте имена SPN. Выполните команды:

   ```
   setspn -A HOST/SPServer SPServer
   setspn -A HOST/SPServer.domain.local SPServer
   ```

Настройка имен SPN для SQL-сервера

1. На контроллере домена запустите оснастку «Active Directory – Пользователи и компьютеры».
2. Проверьте правильность задания имени SPN:
   a) установите утилиту Procexp. Утилиту можно бесплатно скачать с сайта компании Microsoft;
   b) запустите утилиту и в контекстном меню процесса sqlservr.exe выберите пункт **Properties**;
   c) перейдите на закладку «TCP/IP». В столбце **Local Address** отображаются записи в формате <Имя SQL-сервера>:<номер порта, через который работает SQL-сервер>.

      По умолчанию SQL-сервер работает через порт 1433. Номер 1433 может отображаться в виде «ms-sql-s». В некоторых случаях, например если на сервере используется несколько экземпляров SQL-сервера, номер порта будет отличаться от стандартного.
3. Проверьте наличие записи «MSSQLSvc/SQLServerName.domain.local:1433» в списке всех имен SPN для данной учетной записи:
   - если SQL-сервер работает от имени служебной учетной записи «Локальная система» («Local System»), то выполните команду:

     setspn -L SQLServerName

     где **SQLServerName** – это имя SQL-сервера;
   - если SQL-сервер работает от имени доменной учетной записи, то выполните команду:

     setspn -L SQLAdmin

     где **SQLAdmin** – учетная запись, от имени которой работает служба SQL-сервера.

   В результате выполнения команды отображается список всех имен SPN для данного компьютера или данной учетной записи.
4. Настройте имя SPN по полученному номеру порта:
   - если в списке для записи «MSSQLSvc/SQLServerName.domain.local:1433» указан другой порт или в списке нет записей:

     MSSQLSvc/SQLServerName.domain.local:1433

     MSSQLSvc/SQLServerName.domain.local

     HOST/SQLAdmin или HOST/SQLServerName, если SQL-сервер запущен от учетной записи «Локальная система»

     HOST/SQLAdmin.domain.local или HOST/SQLServerName.domain.local, если SQL-сервер запущен от учетной записи «Локальная система», где:
     - **domain.local** – DNS-суффикс домена;
     - **SQLAdmin** – учетная запись, от имени которой работает служба SQL-сервера.
   - если SQL-сервер работает от имени служебной учетной записи «Локальная система», то выполните команду:

     setspn -A MSSQLSvc/SQLServerName.domain.local:1433 SQLServerName

     setspn –A MSSQLSvc/SQLServerName.domain.local SQLServerName

     setspn –A HOST/SQLServerName SQLServerName

setspn –A HOST/SQLServerName.domain.local SQLServerName

- если SQL-сервер работает от имени доменной учетной записи, то выполните команду:

  setspn -A MSSQLSvc/SQLServerName.domain.local:1433 SQLAdmin

  setspn –A MSSQLSvc/SQLServerName.domain.local SQLAdmin

  setspn –A HOST/SQLAdmin SQLAdmin

  setspn –A HOST/SQLAdmin.domain.local SQLAdmin

Настройка доверия для делегирования служб Kerberos

1. На контроллере домена запустите оснастку «Active Directory – пользователи и компьютеры».
2. Последовательно в свойствах каждого из серверов SharePoint и SQL-сервера перейдите на закладку «Делегирование» и установите переключатель **Этот компьютер доверенный для делегирования служб (Kerberos)**.
3. В свойствах учетной записи пользователя пула приложений SharePoint и пользователя, от имени которого работает служба SQL Server, на закладке «Делегирование»:
   - установите переключатель **Доверять этому пользователю делегирование служб (только Kerberos)**.
   - выберите службу, для которой нужно настроить делегирование. Для этого:
     - последовательно нажмите на кнопки **Добавить...**, **Пользователи и компьютеры**. Откроется окно «Выбор: “Пользователи” или “Компьютеры”»;
     - с помощью поиска найдите и выберите пользователя или компьютер, для которого настроено имя SPN, затем нажмите на кнопку **ОК**;
     - в списке служб выберите запись **MSSQLSvc**, напротив которой указан порт SQL-сервера с базой данных DIRECTUM;
     - нажмите на кнопку **ОК**, затем **Применить**.

Настройка для работы с Портальными компонентами DIRECTUM для SharePoint 2013

1. Настройте имена участников службы SPN.
2. Настройте доверие для делегирования служб Kerberos.
3. Выполните дополнительную настройку сервера SharePoint. Настройка необходима для обеспечения возможности старта задач и интеграции.

Настройка имен участников службы Service Principal Name (SPN)

1. Установите программу Setspn на компьютер в домене, с которого планируется настраивать имена SPN. Утилиту можно бесплатно скачать с сайта компании Microsoft.
2. Настройте имя SPN для учетной записи пользователя пула приложений.
3. Настройте имя SPN для SQL-сервера.

Добавлять и удалять имена SPN может только администратор домена. Просматривать список зарегистрированных имен SPN может любой доменный пользователь.

Настройка имени SPN для учетной записи пользователя пула приложений SharePoint 2013

1. На контроллере домена запустите оснастку «Active Directory – Пользователи и компьютеры».
2. Если в свойствах учетной записи пользователя пула приложений отсутствует закладка «Делегирование», то выполните команду:

   setspn -R SPAdmin

   где **SPAdmin** – имя пользователя, которому необходимо доверить делегирование служб.
3. Проверьте список имен SPN, назначенных учетной записи пользователя. Выполните команду:

   setspn -L SPAdmin

   где **SPAdmin** – учетная запись, от имени которой работает пул приложений.

   В списке должны присутствовать записи:

   - HOST/SPAdmin;
   - HOST/SPAdmin.domain.local, где **domain.local** – DNS-суффикс домена; SPAdmin – учетная запись, от имени которой работает пул приложений;
   - HTTP/SPServer;
   - HTTP/SPServer.domain.local, где **domain.local** – DNS-суффикс домена; SPServer – имя сервера, на котором размещен веб-сервер SharePoint.
4. Если одной или нескольких указанных записей нет, то зарегистрируйте имена SPN для каждой записи. Выполните команды:

   ```
   setspn -A HTTP/SPServer SPAdmin
   setspn -A HTTP/SPServer.domain.local SPAdmin
   setspn -A HOST/SPAdmin SPAdmin
   setspn -A HOST/SPAdmin.domain.local SPAdmin
   ```
5. Зарегистрируйте имя SPN для учетной записи пользователя пула приложений:

   setspn -A http/www.mysite.com SPAdmin, где:

   - **SPAdmin** – учетная запись, от имени которой работает пул приложений;
   - **www.mysite.com** – URL, по которому идет обращение к сайту.

Настройка имени SPN для SQL-сервера

1. На контроллере домена запустите оснастку «Active Directory – Пользователи и компьютеры».
2. Проверьте правильность задания имени SPN:
   - с помощью утилиты Procexp определите порт, через который работает SQL-сервер;
   - запустите утилиту и отобразите свойства экземпляра службы SQL-сервера (процесс – sqlservr.exe);
   - перейдите на закладку «TCP/IP». В столбце **Local Address** отображаются записи в формате <Имя SQL-сервера>:<номер порта, через который работает SQL-сервер>.

     По умолчанию SQL-сервер работает через порт 1433. Номер 1433 может отображаться в виде «ms-sql-s». В некоторых случаях, например, если на сервере используется несколько экземпляров SQL-сервера, номер порта будет отличаться от стандартного.

3. Проверьте наличие записи «MSSQLSvc/SQLServerName.domain.local:1433» в списке всех имен SPN для данной учетной записи:
   - если SQL-сервер работает от имени служебной учетной записи «Локальная система» («Local System»), то выполните команду:

     setspn -L SQLServerName

     где SQLServerName – это имя SQL-сервера;
   - если SQL сервер работает от имени доменной учетной записи, то выполните команду:

     setspn -L SQLAdmin

     где SQLAdmin – учетная запись, от имени которой работает служба SQL-сервера.

   В результате выполнения команды отображается список всех имен SPN для данного компьютера или данной учетной записи.
4. Настройте имя SPN по полученному номеру порта:
   - если в списке для записи «MSSQLSvc/SQLServerName.domain.local:1433» указан другой порт или в списке нет записей:

     MSSQLSvc/SQLServerName.domain.local:1433

     MSSQLSvc/SQLServerName.domain.local

     HOST/SQLAdmin или HOST/SQLServerName, если SQL-сервер запущен от учетной записи «Локальная система»

     HOST/SQLAdmin.domain.local или HOST/SQLServerName.domain.local, если SQL-сервер запущен от учетной записи «Локальная система», где:
     - **domain.local** – DNS-суффикс домена;
     - **SQLAdmin** – учетная запись, от имени которой работает служба SQL-сервера.
   - если SQL-сервер работает от имени служебной учетной записи «Локальная система», то выполните команду:

     setspn -A MSSQLSvc/SQLServerName.domain.local:1433 SQLServerName

     setspn –A MSSQLSvc/SQLServerName.domain.local SQLServerName

     setspn –A HOST/SQLServerName SQLServerName

     setspn –A HOST/SQLServerName.domain.local SQLServerName
   - если SQL-сервер работает от имени доменной учетной записи, то выполните команду:

     setspn -A MSSQLSvc/SQLServerName.domain.local:1433 SQLAdmin

     setspn –A MSSQLSvc/SQLServerName.domain.local SQLAdmin

     setspn –A HOST/SQLAdmin SQLAdmin

     setspn –A HOST/SQLAdmin.domain.local SQLAdmin

Настройка доверия для делегирования служб Kerberos

1. На контроллере домена запустите оснастку «Active Directory – Пользователи и компьютеры».
2. В свойствах сервера, на котором размещается SQL-сервер, перейдите на закладку «Делегирование» и установите переключатель **Этот компьютер доверенный для делегирования служб (Kerberos)**.

3. В свойствах учетной записи пользователя, от имени которого работает служба SQL Server, на закладке «Делегирование» установите переключатель **Доверять этому пользователю делегирование служб (только Kerberos)**.

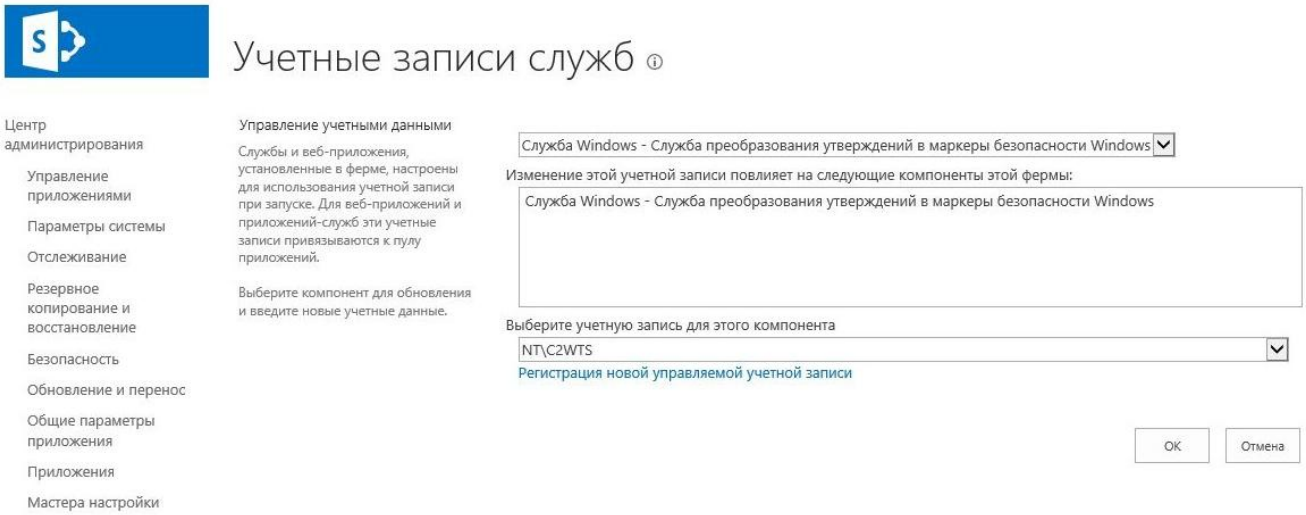
   Если в свойствах учетной записи пользователя отсутствует закладка «Делегирование», то зарегистрируйте для этого пользователя имя участника службы SPN. Подробнее см. раздел «Настройка имен SPN для SQL-сервера».

4. В свойствах учетной записи пользователя, от имени которого работает пул приложений SharePoint, на закладке «Делегирование»:
   - установите переключатели **Доверять этому пользователю делегирование указанных служб** и **Использовать любой протокол проверки подлинности**;
   - выберите службу, для которой нужно настроить делегирование. Для этого:
     - последовательно нажмите на кнопки **Добавить...**, **Пользователи и компьютеры**. Откроется окно «Выбор: "Пользователи" или "Компьютеры"»;
     - с помощью поиска найдите и выберите пользователя пула приложений или компьютер, для которого настроено имя SPN, затем нажмите на кнопку **ОК**;
     - в списке служб выберите запись **MSSQLSvc**, напротив которой указан порт SQL-сервера с базой данных DIRECTUM;
     - нажмите на кнопку **ОК**, затем **Применить**.

Настройка службы Claims to Windows Token Service для работы веб-частей DIRECTUM на портале SharePoint

1. На контроллере домена запустите оснастку «Active Directory – пользователи и компьютеры» и создайте учетную запись пользователя для запуска **Службы преобразования утверждений в маркеры безопасности Windows** (Claims to Windows Token Service).
2. Включите пользователя в группу локальных администраторов на сервере SharePoint.
3. Выдайте пользователю права:
   - **Работа в режиме операционной системы (Act as a part of the operating system)**;
   - **Вход в качестве службы (Log on as a service)**.
5. На странице «Центр администрирования SharePoint» выберите пункт меню **Безопасность>Общая безопасность>Настройка учетных записей служб** и перейдите по ссылке **Регистрация новой управляемой учетной записи**. Откроется окно «Регистрация управляемой учетной записи».
6. Укажите учетные данные пользователя в полях **Имя пользователя** и **Пароль** и нажмите на кнопку **ОК**.

7. На странице «Центр администрирования SharePoint» выберите пункт меню **Управление приложениями>Приложения-службы>Управление службами на сервере**. Откроется окно «Учетные записи служб»:



8. Укажите параметры настройки:
   - в выпадающем списке выберите значение **Служба Windows – Служба преобразования утверждений в маркеры безопасности Windows**;
   - выберите учетную запись созданного пользователя;
   - нажмите на кнопку **OK**.
9. Откроется список служб на сервере. В строке со **Службой преобразования утверждений в маркеры безопасности Windows** нажмите на кнопку **Запустить**.
10. Перезагрузите компьютер с SharePoint.

Возможные проблемы при работе Портальных компонентов DIRECTUM для SharePoint и способы их решения

При решении проблем обратитесь к документации:

- руководство по Портальным компонентам DIRECTUM для SharePoint, входит в комплект поставки;
- Kerberos в среде SharePoint;
- Технология Kerberos для обеспечения безопасности MOSS 2007: OSP.

Нет доступа к веб-узлу

Если пул приложений SharePoint работает от имени доменной учетной записи и используется протокол аутентификации Kerberos, то невозможно получить доступ к пулу приложений по сети. Локально пул приложений работает корректно.

Возможные причины и способы их решения:

1. Не настроены имена SPN для пользователя пула приложений. Проверьте правильность настройки имен SPN, см. разделы «Настройка доверия для делегирования служб Kerberos» и «Настройка учетной записи пользователя пула приложений SharePoint».
2. В сети зарегистрированы дублирующие записи имен SPN. Чтобы проверить наличие дублирующих записей в операционной системе Windows Server 2008, выполните команду:

   Setspn -X

   Чтобы удалить дублирующие записи, выполните команду:

   Setspn -D <SPN> <Уч.запись>

   Например:

   setspn -D HTTP/SPServer SQLAdmin
3. На IIS в настройках веб-узла не включена проверка подлинности в режиме ядра. Необходимые меры:
   a) в файле <%SystemDrive%>\System32\inetsrv\config\applicationHost.config в группе настроек веб-узла, для которого включается проверка подлинности в режиме ядра, в настройках Windows-аутентификации укажите значение **true** для параметров:
      - **useKernelMode**;
      - **useAppPoolCredentials**;
   b) перед изменением файла applicationHost.config рекомендуется сохранить его резервную копию, т.к. некорректное изменение файла может привести к неработоспособности веб-сервера.

```
<system.webServer>
  <security>
  <authentication>
  <windowsAuthentication
    enabled="true"
    useKernelMode="true"
    useAppPoolCredentials="true">
  </authentication>
  </security>
</system.webServer>
```

4. Не настроен браузер пользователя. Если возникли проблемы на стороне клиентской части, то при попытке обращения к узлу веб-доступа происходит запрос реквизитов подключения или вход в систему произведен, но создание задач и документов недоступно. В лог-файлах фиксируются ошибки создания приложения.

   Предпринимаемые меры зависят от используемого браузера. Список поддерживаемых браузеров см. в документе «DIRECTUM 5.1. Типовые требования к аппаратному и программному обеспечению», входит в комплект документации.

Internet Explorer

Добавить адрес или маску адресов в зону, для которой разрешен автоматический вход в сеть от имени текущего пользователя (обычно это местная интрасеть). Для этого в свойствах браузера в окне «Параметры безопасности – зона местной интрасети» для переключателя **Проверка подлинности пользователя** установите значение **Автоматический вход в сеть с текущим именем пользователя**.

Google Chrome

Для работы Google Chrome используются системные настройки безопасности Windows. Чтобы получить уровень токена, доверенный на делегирование:

1. В редакторе реестра Windows перейдите по ветке:

   HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome

2. Для параметра **AuthNegotiateDelegateWhitelist** укажите адрес или маску адресов, например ***.yourcompany.ru**.

Firefox

В адресной строке введите **about:config**. На открывшейся странице:

- если требуется аутентификация по DNS-имени, то для настройки **network.negotiate-auth.allow-non-fqdn** укажите значение **true**;
- в значении настройки **network.negotiate-auth.trusted-uris** укажите адрес или маску адресов, ***.yourcompany.ru**, для которых разрешена negotiate-аутентификация;
- в значении настройки **network.negotiate-auth.delegation-uris** укажите адрес или маску адресов, ***.yourcompany.ru,** для которых разрешено делегирование.

Chromium-браузеры

Браузеры на основе Chromium позволяют указать маску адресов, доверенных для делегирования, через параметры запуска. Например:

```
browser --auth-server-whitelist="yourcompany.ru" --auth-negotiate-delegate-whitelist="yourcompany.ru"
```

Opera

Для настройки запуска Opera используется утилита Launcher.exe. Чтобы добавить узел в доверенные адреса, нужно в ярлыке запуска браузера указать:

```
launcher --auth-server-whitelist="yourcompany.ru" --auth-negotiate-delegate-whitelist="yourcompany.ru"
```

Яндекс.Браузер

Яндекс.Браузер является Chromium-браузером и поддерживает задание маски через параметры запуска. Также маску адресов для делегирования можно задать в реестре. Для этого:

1. В редакторе реестра Windows перейдите по ветке:

   HKEY_LOCAL_MACHINE\SOFTWARE\Policies\YandexBrowser

2. Для параметра **AuthNegotiateDelegateWhitelist** укажите адрес или маску адресов для делегирования, например ***.yourcompany.ru**.

Safari

Браузер Safari для сквозной аутентификации поддерживает только NTLM-аутентификацию. Корректная работа Kerberos (Negotiate-аутентификация) не поддерживается.

Прекращение работы процесса SBRte при работе Портальных компонентов на IIS7

Если пул приложений работает от имени Network Service, то при удаленном запуске процесс SBRte прекращает работу.

Решения:

1. Действия, описанные в разделе «Нет доступа к веб-узлу».
2. Запускать пул приложений от имени доменной учетной записи. Подробнее см. раздел «Настройка учетной записи пользователя пула приложений SharePoint 2010» или «Настройка учетной записи пользователя пула приложений SharePoint 2013».