Установка программного комплекса «КИБ Серчинформ»

руководство пользователя

SEARCHINFORM
INFORMATION SECURITY

Оглавление

1 Введение

Перед установкой компонентов программного комплекса «Контур информационной безопасности Серчинформ» (далее КИБ Серчинформ) должны быть обеспечены следующие условия:

а) Установлена одна из поддерживаемых операционных систем (см. п. 2.1).
б) Установлена и настроена СУБД Microsoft SQL Server 2008 R2 или выше (см. п. 2.2).
в) Разрешены взаимодействия между компонентами КИБ Серчинформ (см. п. 2.3).
г) Создана и настроена учетная запись для работы КИБ Серчинформ (см. п. 2.4).
д) Компоненты КИБ Серчинформ внесены в исключения антивирусного ПО (см. п. 2.5).
е) Установлена поддержка русского языка в региональных настройках (см. п. 2.6).
ж) Подключен и настроен дополнительный сетевой адаптер (при использовании перехвата через зеркало) (см. п. 2.7).
з) Настроены рабочие станции, на которые будут устанавливаться агенты (см. п. 2.9)
и) Для сервера КИБ Серчинформ рекомендуется выделить статический IP адрес или зарезервировать в DHCP.

Отсутствие вышеперечисленных пакетов на Search Server не нарушает его работоспособность. Но установка данных фильтров рекомендуется, поскольку они могут быть задействованы в случае, когда встроенная библиотека не отработала и вернула ошибку.

Функция оптического распознавания текста реализуется благодаря включенному в дистрибутив сервиса OCR.

Для локальной работы на Search Server с оригиналами перехваченных текстовых и PDF-документов, потребуется наличие установленных приложений для их просмотра (например, Microsoft Office, OpenOffice и Adobe Reader).

2 Подготовка к установке

2.1 Поддерживаемые операционные системы

Компоненты КИБ Серчинформ могут работать под управлением следующих операционных систем семейства Windows:

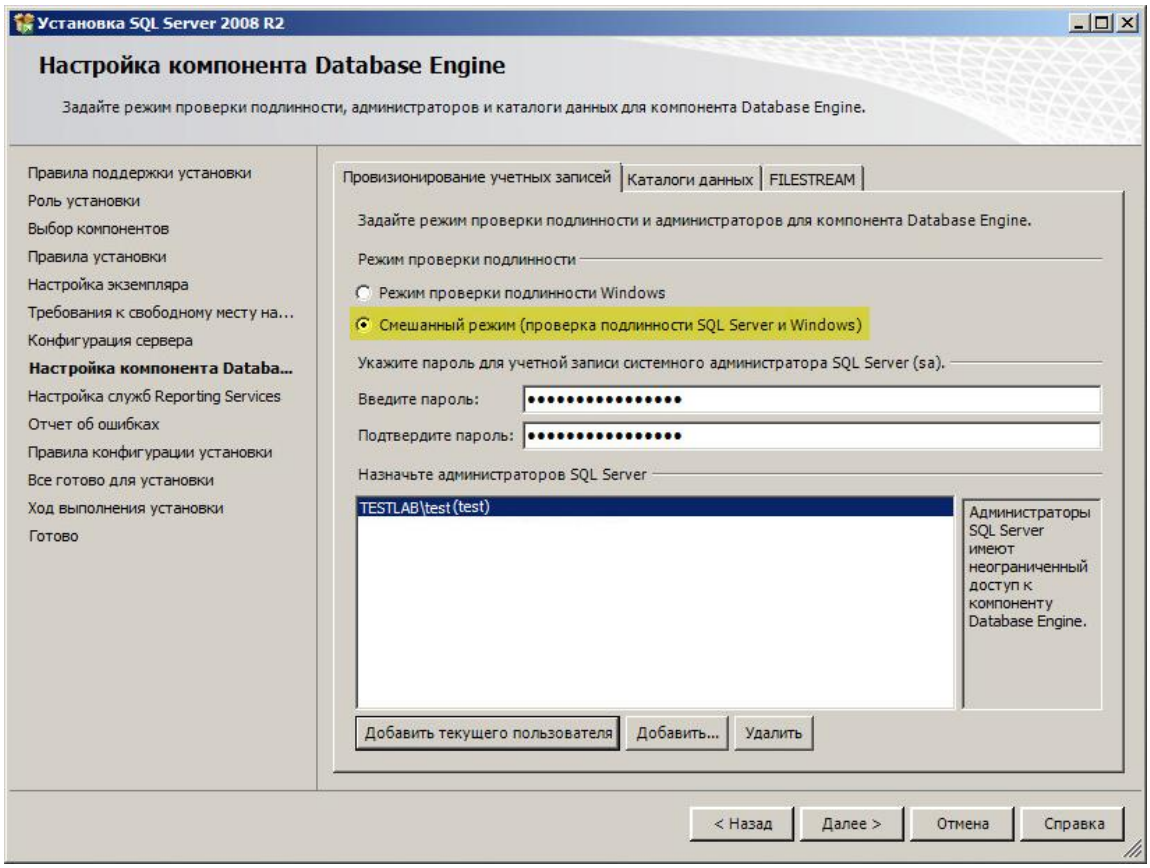
Компоненты	XP x32/ x64	Vista x32/ x64	7 x32/ x64	8, 8.1 x32/ x64	10 x32/ x64	2003 x32/ x64	2008 R1 x32/ x64	2008 R2	2012, 2012 R2	2016
Search Server								+	+	+
Сервер DataCenter								+	+	+
Сервер EndpointSniffer								+	+	+
Сервер NetworkSniffer								+	+	+
Сервер AlertCenter								+	+	+
Сервер ReportCenter								+	+	+
SearchInform Client	+	+	+	+	+	+	+	+	+	+
Клиент AlertCenter	+	+	+	+	+	+	+	+	+	+
Клиент ReportCenter	+	+	+	+	+	+	+	+	+	+
Агенты Endpoint	+	+	+	+	+	+	+	+	+	+
Агенты Search Server (ИРС)	+	+	+	+	+	+	+	+	+	+

2.2 Установка и настройка СУБД Microsoft SQL Server

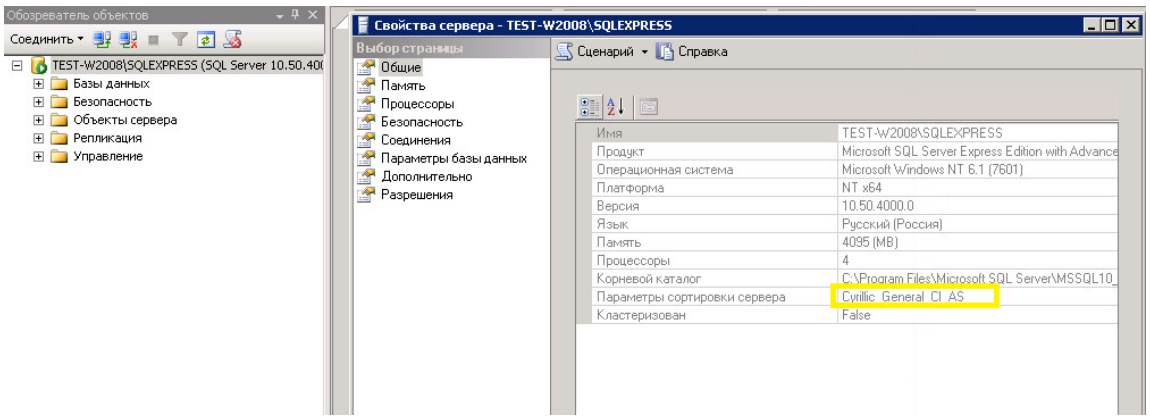
Для работы КИБ Серчинформ должен быть установлен сервер СУБД Microsoft SQL Server версий 2008 R2 / 2012 / 2014 / 2016.

Рекомендуется устанавливать версию со средствами управления SQL Server Management Studio.

При установке SQL-сервера необходимо выбрать смешанный режим аутентификации (mixed mode). Пароль учетной записи **sa** (или учетной записи, которая выделяется для нужд КИБ Серчинформ в SQL) не должен содержать кириллические символы.

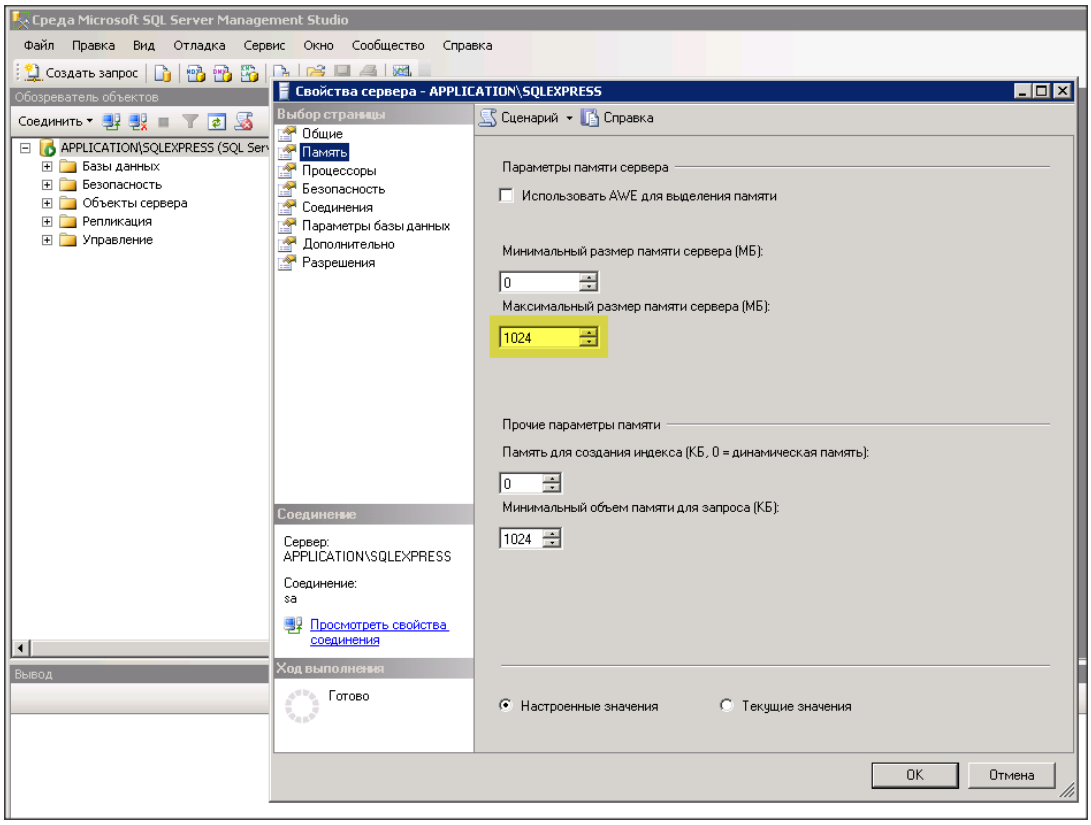


Необходимо убедиться, что параметры сортировки сервера (Collation) установлены в Cyrillic_General_CI_AS.

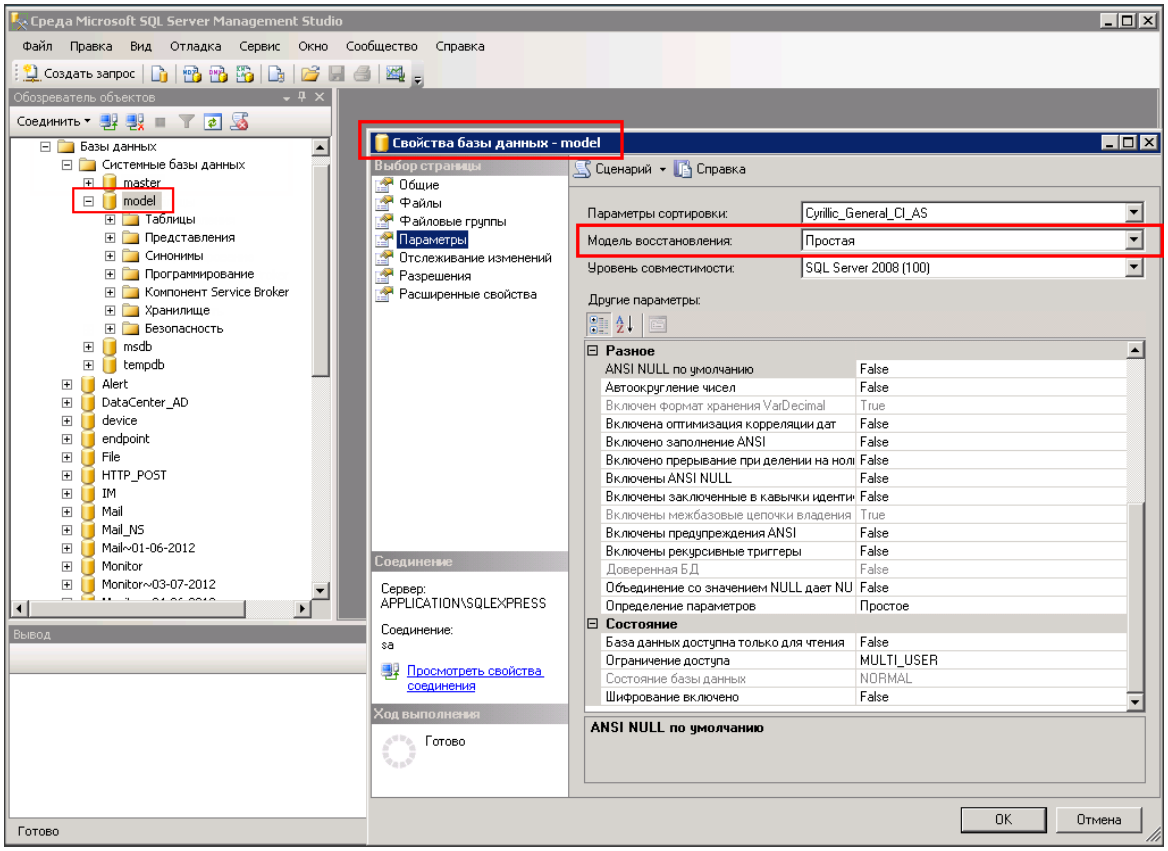


При нехватке RAM рекомендуется ограничить объем памяти, потребляемой Microsoft SQL Server. Для Express версий MS SQL – не более 1Gb, для других версий – приблизительно 50-60% от объема ОЗУ сервера.

Настройка производится в консоли MS SQL Server Management Studio.



Для системной базы **model** должна быть установлена простая модель восстановления:
Базы данных → Системные базы данных → model → Свойства → Параметры



2.3 Взаимодействие компонентов системы

Существуют следующие формы взаимодействия основных и смежных компонентов системы:

а) Установка агентов на рабочие станции пользователей.
б) Перехват данных и передача данных серверу EndpointSniffer.
в) Запись перехваченных данных в базы под управлением Microsoft SQL Server.
г) Индексирование базы данных.
д) Выполнение поисковых запросов.
е) Получение результатов поиска.
ж) Генерация и отправка уведомлений по электронной почте.

Компонент	Протокол/Порт	Компонент	Протокол/Порт
Установка агентов сервером SearchInform EndpointSniffer			
Сервер EndpointSniffer	TCP/*	Рабочие станции	TCP
Сервер EndpointSniffer	UDP/*	Рабочие станции	UDP
Передача информации от агентов на сервер SearchInform EndpointSniffer			
Рабочие станции	TCP/*	Сервер EndpointSniffer	HTTP(S)
Запись информации в базу данных			
Сервер EndpointSniffer	TCP/*	Сервер баз данных	TCP/1433
Индексирование базы данных			
Сервер индексации	TCP/*	Сервер баз данных	TCP/1433
Контроль содержимого экранов рабочих станций в режиме реального времени			
Рабочие станции	TCP/*	АРМ администратора	TCP
Контроль речи сотрудников в режиме реального времени			
Рабочие станции	TCP/*	АРМ администратора	TCP
Отправка уведомлений по инцидентам (AlertCenter) по электронной почте			
Сервер AlertCenter	TCP/*	Почтовый сервер	SMTP (25)
Запрос для получения имени контроллера домена[1]			
Сервер NetworkSniffer	CLDAP/19**	Контроллер домена	CLDAP/389
Получение имен пользователей домена			
Сервер NetworkSniffer	SMB/2002	Контроллер домена	SMB/445
Передача информации в базу данных			
Сервер NetworkSniffer	TCP/*	Сервер баз данных	TCP/1433
Передача поискового запроса			
SearchInform Client	TCP/*	Сервер индексации	TCP

[1] Порты, скорее всего, будут открыты по умолчанию. В противном случае, сервер NetworkSniffer не сможет войти в домен.

* – назначаемый пользователем либо динамически назначаемый порт.

Компонент	Протокол/Порт	Компонент	Протокол/Порт
AlertCenter	TCP/*	Сервер индексации	TCP
Получение уведомлений по электронной почте			
АРМ администратора	TCP/*	Почтовый сервер	POP3 (110)[2]
Подключение к серверу баз данных			
Сервер AlertCenter	TCP/*	Сервер Microsoft SQL	TCP/1433
Клиент AlertCenter	TCP/*	Сервер Microsoft SQL	TCP/1433
Получение результатов проверки			
Сервер AlertCenter	TCP/*	Search Server	TCP
Передача настроек и команд			
Клиент DataCenter	TCP/*	Сервер DataCenter	TCP
Передача статуса контролируемых компонентов			
Агенты DataCenter	TCP/*	Сервер DataCenter	TCP
Отправка уведомлений			
Сервер DataCenter	TCP/*	Почтовый сервер	SMTP
Получение уведомлений от сервера DataCenter по электронной почте[3]			
Почтовый сервер	TCP/*	АРМ администратора	POP3, IMAP, HTTP(S)
Запрос лицензии сервером индексации			
Search Server	TCP/*	Сервер DataCenter	TCP
Установка агентов индексации рабочих станций (IWS)			
Сервер индексации	TCP/*	Рабочие станции	TCP TCP
Индексирование (Search Server)			
Рабочие станции	TCP/1111	Search Server	TCP

Если в сети установлен брандмауэр, соответствующие порты должны быть открыты.

При использовании удаленных консолей для подключения к серверам с компонентами КИБ Серчинформ, наряду с указанными портами на сервере баз данных Microsoft SQL необходимо открыть порт UDP/1434.

2.4 Учётная запись для работы КИБ Серчинформ

Для установки и запуска компонентов КИБ Серчинформ необходима учетная запись, обладающая определенными правами. Создаваемая учетная запись должна обладать как минимум правами локального администратора на сервере КИБ Серчинформ и на рабочих станциях, на которые будут

[2] Порт определяется настройками почтового клиента.

[3] Протокол и порт определяются настройками почтового клиента администратора.

* – назначаемый пользователем либо динамически назначаемый порт

устанавливаться агенты. Или можно использовать учетную запись администратора домена. Добавьте созданную учётную запись в следующие групповые политики:

- Вход в качестве службы
- Управление аудитом и журналом безопасности (только для следующих компонентов NetworkSniffer: сетевой перехват через зеркало и ADSniffer).

2.5 Внесение исключений в антивирусное ПО

Для того чтобы совместная работа КИБ Серчинформ (в том числе агента контроля КИБ Серчинформ) и корпоративных антивирусных программ не приводила к взаимным конфликтам, необходимо внести установленные компоненты КИБ Серчинформ в исключения используемого антивирусного ПО.

- Настройка исключений в Kaspersky Security Center 10
- Настройка исключений в ESET Endpoint Security 5
- Настройка исключений в ESET Endpoint Security 6
- Список исключений для Dr.Web

В случае использования антивирусного ПО, не указанного в перечне выше, настройте исключения самостоятельно.

Если антивирус не поддерживает указание путей через переменные окружения, каждую переменную необходимо заменить на прямой путь.

Если антивирус не поддерживает указание папок, а только файлов, для каждой перечисленной ниже папки необходимо указать все файлы, расположенные как в самой папке, так и во вложенных папках.

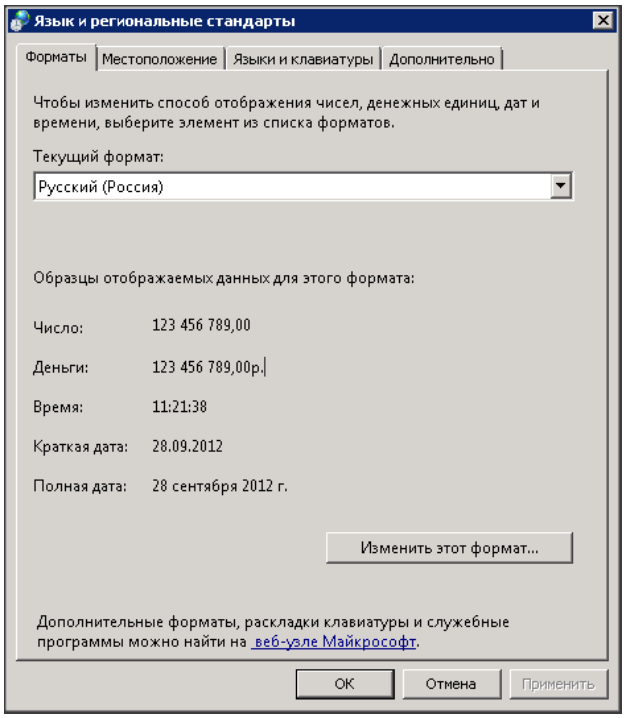
2.6 Поддержка русского языка в региональных настройках

Для выполнения поиска по русским текстам и корректного отображения кириллических символов на сервере КИБ Серчинформ в региональных настройках должны быть установлены Русский и Россия.

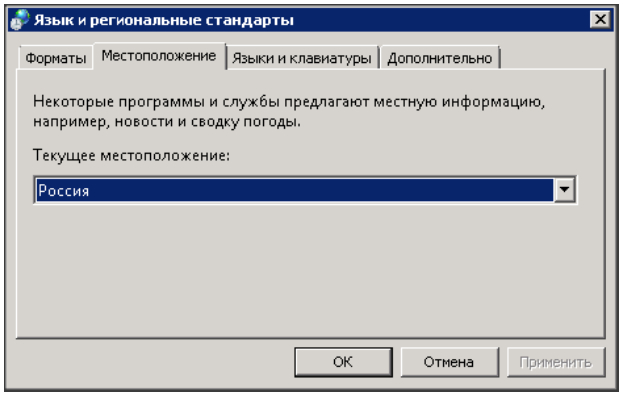
Настройка стандартов для Windows Server 2008 R2:

Пуск → Панель управления → Язык и региональные стандарты

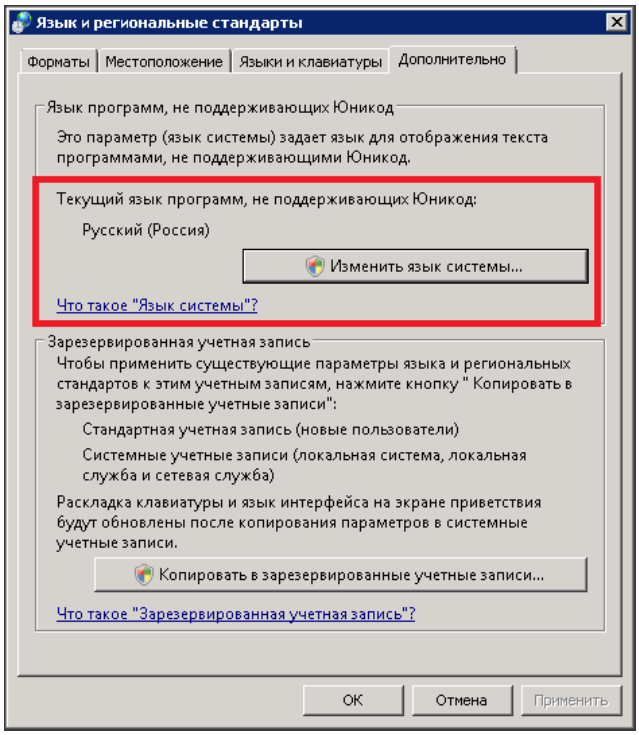
1. Вкладка «Форматы». Выберите значение «Русский (Россия)» в качестве текущего формата.



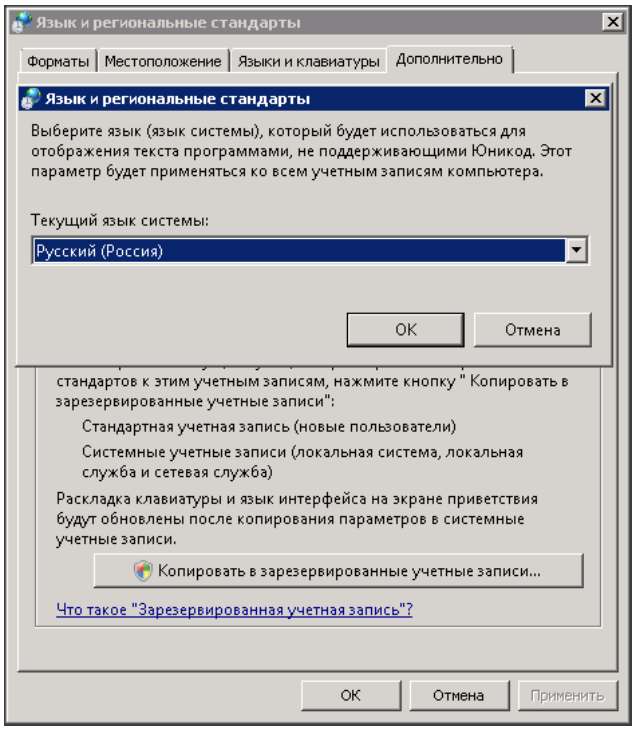
2. Вкладка «Местоположение». Выберите значение «Россия» в качестве текущего местоположения.



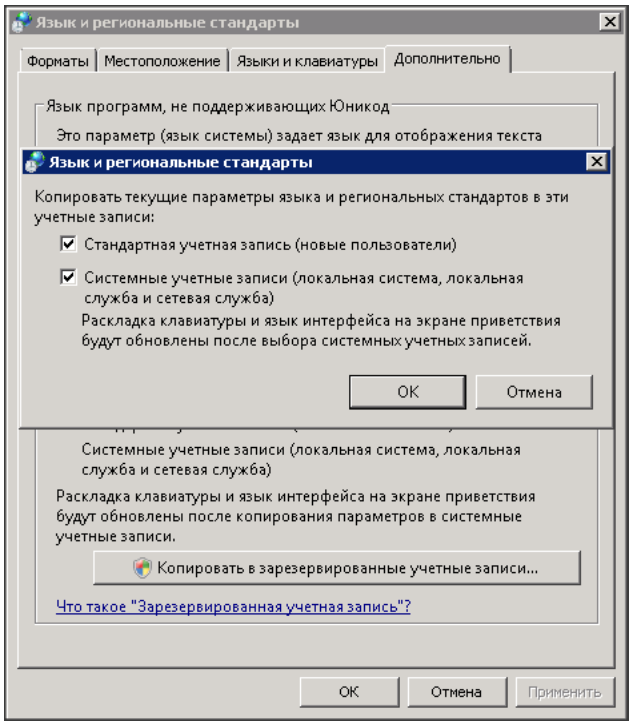
3. Вкладка «Дополнительно». В качестве текущего языка программ, не поддерживающих Юникод, должен стоять «Русский (Россия)».



Если это не так, щелкните по кнопке «Изменить язык системы…» и в открывшемся окне выберите значение «Русский (Россия)».



4. Вкладка «Дополнительно». Щелкните по кнопке «Копировать в зарезервированные учетные записи…» и в открывшемся окне установите флажки «Стандартная учетная запись» и «Системные учетные записи».

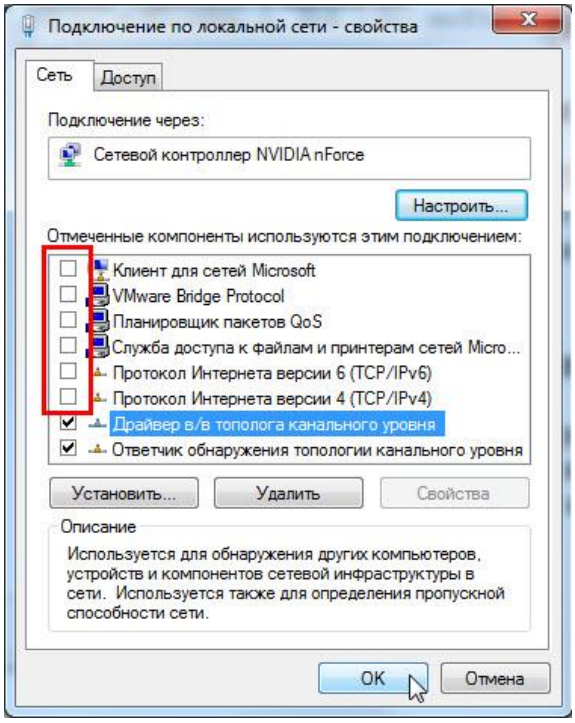


В случае внесения изменений по пунктам 3 и 4 (на нелокализованных системах) – обязательно нужно перезагрузить сервер, чтобы данные настройки применились.

2.7 Настройка перехвата методом зеркалирования сетевого трафика

При использовании схемы перехвата на уровне сетевых шлюзов необходимо обеспечить наличие на сервере NetworkSniffer как минимум двух сетевых адаптеров. Один будет использоваться для обычного приема и передачи данных, управления перехватом и хранения настроек КИБ Серчинформ, второй – для зеркалирования сетевого трафика.

Для сетевого адаптера, используемого для зеркалирования сетевого трафика, необходимо отключить все функции, относящиеся к транспортному уровню, оставив только канальный уровень. Это связано с тем, что адаптер будет использоваться исключительно для забора передаваемых данных.

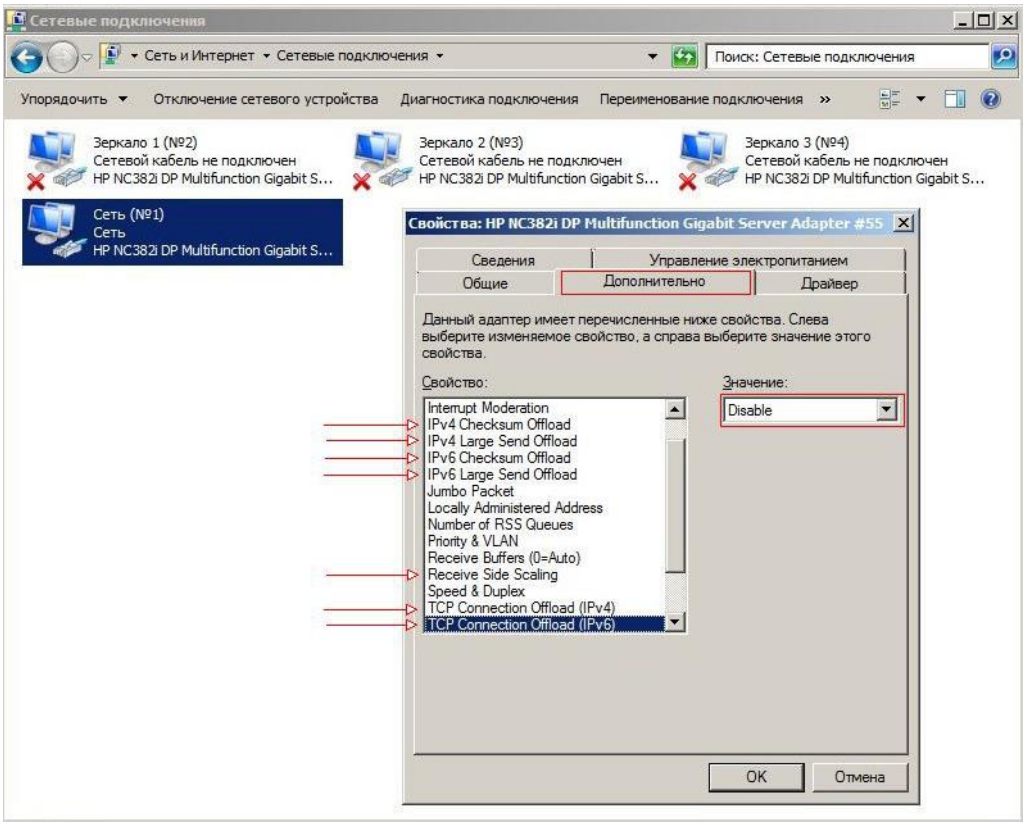


Для предотвращения потери пакетов в настройках сетевых карт опция «**Offload TCP segmentation**» и/или аналогичные ей параметры должны быть отключены.

Перечень «offload»-параметров может меняться в зависимости от производителя сетевой карты. В этом случае следует отключать все опции, в наименовании которых встречаются слова «offload» и «segmentation».

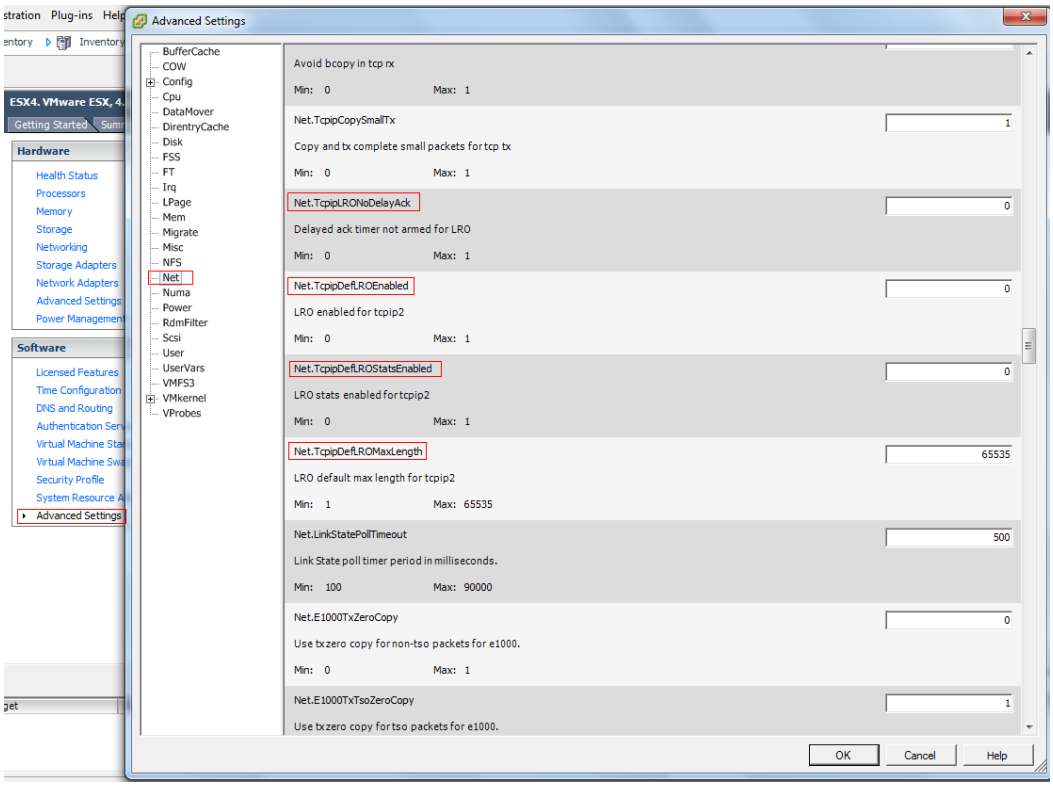
Вызовите свойства сетевого соединения из контекстного меню и щелкните кнопку «Настроить». Перейдите на вкладку «Дополнительно» для просмотра доступных свойств сетевого адаптера.

Для отключения параметра установите значение «Disable» или «None».



Receive Side Scaling (RSS) – технология, которая равномерно распределяет нагрузку по обработке сетевых пакетов между ядрами процессора, позволяя оптимизировать производительность. Ее также рекомендуется отключать. После настроек перезапустите сетевое соединение.

В настройках VMware ESX/ESXi Server данный параметр обозначен как «LRO» (Large Receive Offload).



2.8 Настройка интеграции с почтовыми серверами

Интеграция с почтовыми серверами производится в случае, если данные нужно получать напрямую с почтовых серверов, а не только путем сетевого перехвата.

На данный момент в NetworkSniffer присутствуют 2 метода интеграции с почтовыми серверами:

- с помощью почтового ящика (см. п. 2.8.1);
- по SMTP (см. п. 2.8.2).

	Интеграция с помощью почтового ящика	SMTP-интеграция
Суть метода	Создание служебного почтового ящика и настройка правил копирования сообщений в этот ящик. NetworkSniffer подключается к созданному ящику, принимает все поступившие сообщения и записывает их в свою базу данных. Теневая копия почтовых сообщений хранится и на почтовом сервере (какое-то время) и в базе данных NetworkSniffer.	При интеграции по SMTP инициатором отправки сообщений выступает почтовый сервер. Почтовые сообщения отправляются по протоколу SMTP на заданный узел и порт сервера NetworkSniffer, который принимает данные и сохраняет их в свою базу. Теневая копия почтовых сообщений хранится только в базе данных NetworkSniffer.
Плюсы	▪ Надежность: почта не теряется, если сервер NetworkSniffer неисправен. Почтовые сообщения будут храниться в почтовом ящике до тех пор, пока не будут получены или не поступит команда очистки ящика; ▪ Множество доступных реализаций: POP3, IMAP, EWS, их надстройки (TLS, StartTLS, без шифрования) и методы аутентификации – PLAIN, CRAM-MD5.	▪ Не происходит дублирования почты на уровне почтового сервера.

Минусы	▪ В случае неисправности сервера NetworkSniffer почтовые сообщения не будут удаляться из служебного ящика, и он может занять всё свободное место на почтовом сервере.	▪ В случае неисправности сервера NetworkSniffer почта будет копиться в очереди на отправку, что негативно сказывается на производительности почтового сервера; ▪ SMTP-протокол менее защищен, так как на данный момент со стороны NetworkSniffer нет поддержки TLS-соединения.

2.8.1 Интеграция с помощью почтового ящика

Настройка интеграции почтового сервера с сервером NetworkSniffer обычно включает следующие шаги:

а) Создание отдельного почтового ящика, на который будут поступать почтовые сообщения.

б) Настройка переадресации всех сообщений, обработанных почтовым сервером, на созданный почтовый ящик.

в) Установка компонентов интеграции сервера NetworkSniffer с почтовыми серверами.

Подробные пошаговые инструкции по настройке различных почтовых серверов можно загрузить по ссылкам ниже:

- Настройка интеграции MS Exchange 2007 с сервером NetworkSniffer
- Настройка интеграции MS Exchange 2010 с сервером NetworkSniffer
- Настройка интеграции MS Exchange 2013 с сервером NetworkSniffer
- Настройка интеграции MS Exchange 2016 с сервером NetworkSniffer
- Настройка интеграции Lotus Domino с сервером NetworkSniffer
- Настройка интеграции Kerio 7 с сервером NetworkSniffer
- Настройка интеграции Zimbra с сервером NetworkSniffer
- Настройка интеграции Postfix с сервером NetworkSniffer
- Настройка интеграции MDaemon/MDaemon Pro с сервером NetworkSniffer

Внимание!

При использовании Exchange необходимо обязательно ограничить исходящую почту с настраиваемого почтового ящика. В противном случае пользователи могут получать сообщения от данного ящика, что ведет к рассекречиванию системы.

2.8.2 SMTP-интеграция

Функция *журналирования* почтового севера позволяет хранить копии сообщений в центральном почтовом ящике для различных целей, включая архивацию почты. Благодаря интеграции почтового сервера с сервером NetworkSniffer, второй способен выступать в роли SMTP-сервера, получающего пересылаемые контейнеры отчетов журнала, а впоследствии – обрабатывающего их и помещающего в базу данных.

Общий алгоритм действий при настройке SMTP-интеграции:

а) Создание нового почтового контакта

б) Создание соединителей отправки

в) Создание правила журнала.

Подробные пошаговые инструкции по настройке почтовых серверов Microsoft Exchange можно загрузить по ссылкам ниже:

- Настройка SMTP-интеграции MS Exchange 2010 с сервером NetworkSniffer
- Настройка SMTP-интеграции MS Exchange 2013 с сервером NetworkSniffer
- Настройка SMTP-интеграции MS Exchange 2016 с сервером NetworkSniffer

2.9 Настройка рабочих станций

Для установки агента на рабочие станции необходимо достижение двух условий:

1. Рабочая станция должна пинговаться;
2. На рабочей станции должна открываться системная шара admin$.

Если рабочие станции находятся в домене, все действия, производимые в консоли EndpointSniffer, осуществляются по полному доменному имени. Соответственно проверки 1 и 2 также должны производиться по полному имени рабочей станции.

2.9.1 Настройка брандмауэра Windows

Для достижения вышеприведенных условий в брандмауэре Windows должны быть либо отключены все профили, либо созданы два правила для входящих соединений:

1. Правило настраиваемого типа → Все программы → Тип протокола: ICMPv4;
2. Правило для порта → Протокол TCP, определенный локальный порт: 445.

2.9.2 Доступ к системным шарам на рабочей станции

Для доступа к системным шарам на рабочей станции должна быть запущена служба «Сервер».

В случае недоступности системной шары на компьютере, находящемся в составе рабочей группы, следует на этом компьютере в ветку реестра

`[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System]`

добавить

параметр `LocalAccountTokenFilterPolicy`,

тип: `DWORD`,

значение: `1`.

2.9.3 Службы

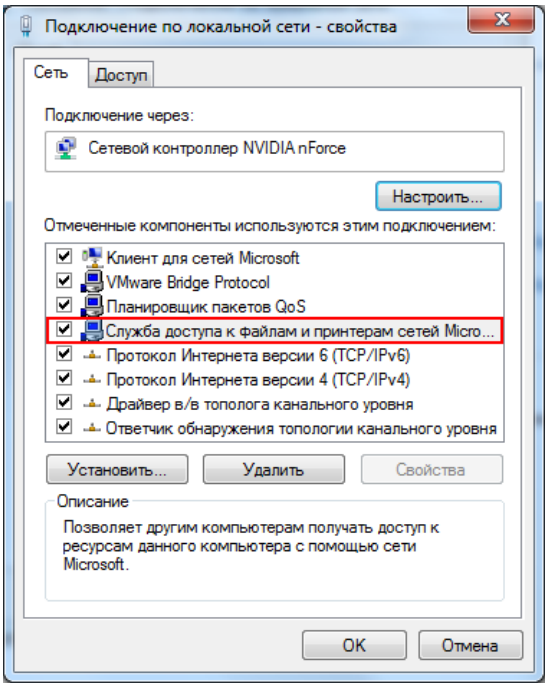
Для корректной установки агентов EndpointSniffer на рабочих станциях пользователей должны быть запущены следующие службы:

- Удаленный вызов процедур (RPC);
- Служба доступа к файлам и принтерам сетей Microsoft.

Для установки агентов индексации рабочих станций необходим также доступ к службе «Удаленный реестр».

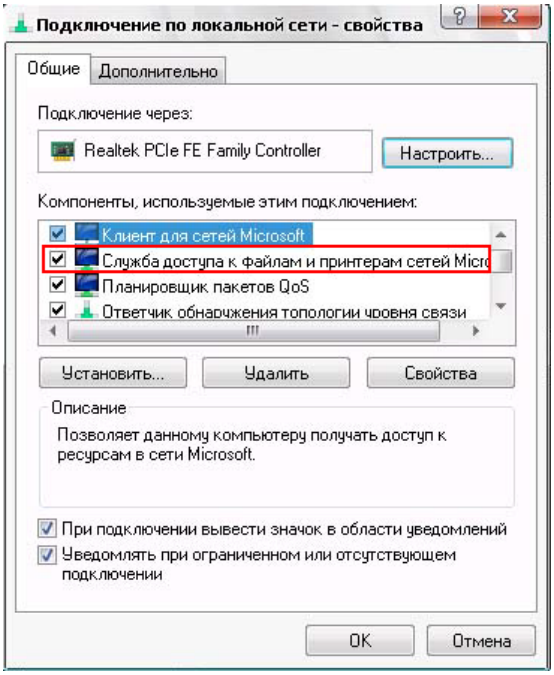
Последовательность действий (для Windows 7):

1) Меню «Пуск» → Панель управления → Система и безопасность → Администрирование → Службы.
2) Проверить состояние службы «Удаленный вызов процедур (RPC)». Запустить их в случае необходимости.
3) Меню «Пуск» → Панель управления → Сеть и Интернет → Центр управления сетями и общим доступом → Подключение по локальной сети → Свойства
4) Отметить флажком «Служба доступа к файлам и принтерам сетей Microsoft».



Последовательность действий (для Windows XP):

1) Меню «Пуск» → Панель управления → Администрирование → Службы.
2) Проверить состояние службы «Удаленный вызов процедур (RPC)». Запустить их в случае необходимости.
3) Меню «Пуск» → Панель управления → Сеть и подключения к Интернету → Сетевые подключения → Подключение по локальной сети → Свойства
4) Отметить флажком «Служба доступа к файлам и принтерам сетей Microsoft»

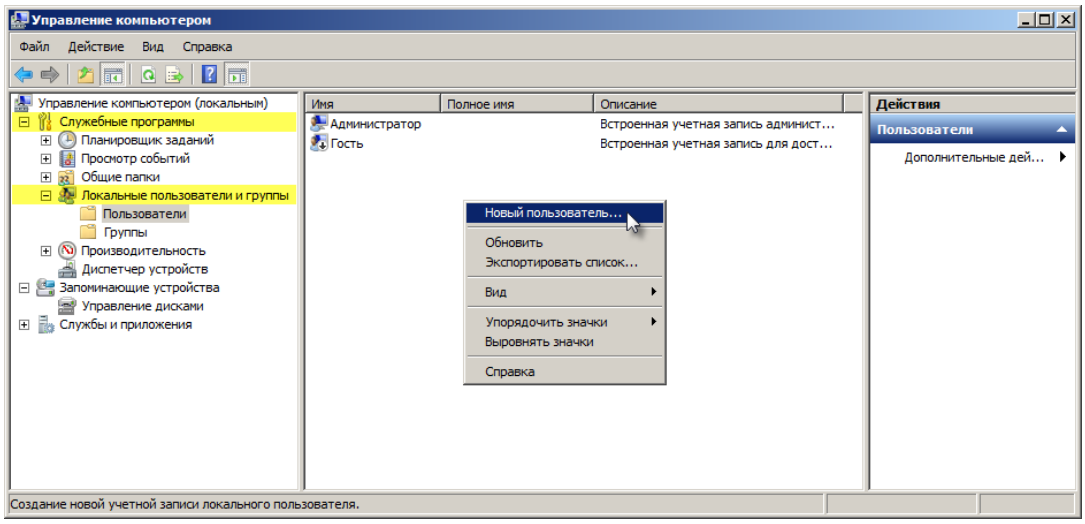


2.9.4 Настройка локальных учетных записей на ПК в рабочей группе

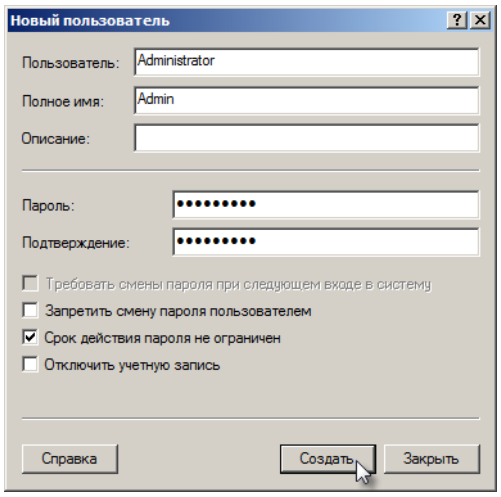
Для установки агентов на компьютеры, находящиеся в составе рабочей группы, необходимо на компьютерах рабочей группы создать учетную запись с правами локального администратора.

Откройте оснастку «Управление компьютером» и перейдите по пути «Служебные программы | Локальные пользователи | Пользователи».

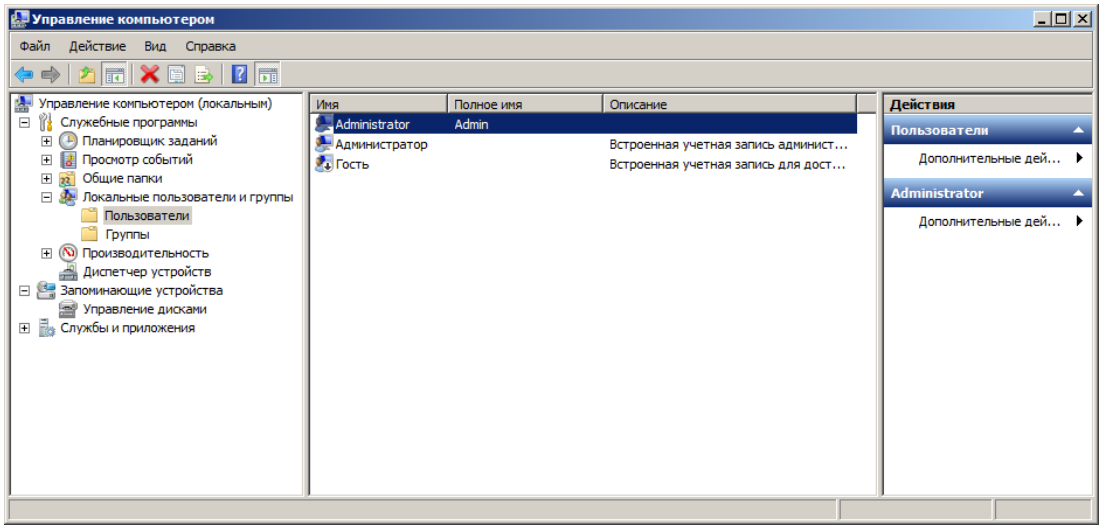
Воспользуйтесь меню «Действие | Новый пользователь» или выберите команду «Новый пользователь» в контекстном меню.



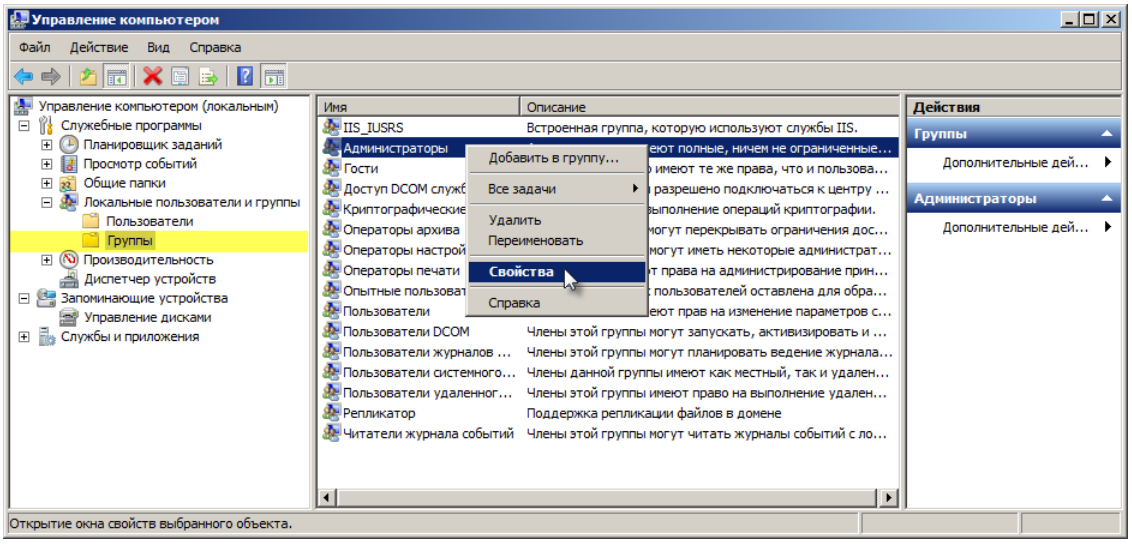
Для создания новой локальной учетной записи, введите имя пользователя, пароль и щелкните кнопку «Создать».



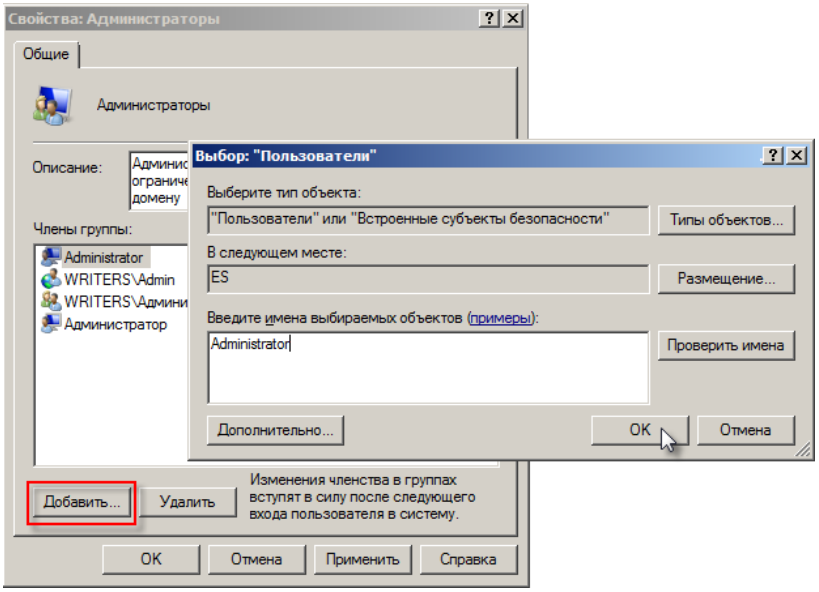
Локальный пользователь будет добавлен в список.



Перейдите в папку «Служебные программы | Локальные пользователи | Группы» и откройте свойства группы «Администраторы».



Добавьте созданного пользователя в список членов группы.



Данную операцию повторите для остальных компьютеров рабочей группы, на которые планируется установка агентов.

2.9.5 Системные требования

Минимальные требования к рабочим станциям с установленными агентами EndpointSniffer:

а) Процессор: 1-ядерный частотой не ниже 2 ГГц

б) ОЗУ: не менее 1 ГБ[4]

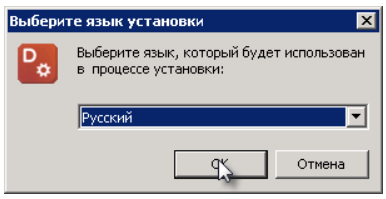
в) Общее дисковое пространство: 250 ГБ (системный раздел диска – не менее 50 ГБ).

[4] В случае, когда включена запись видео либо парсинг на агентах, требуется минимум 2 ГБ.

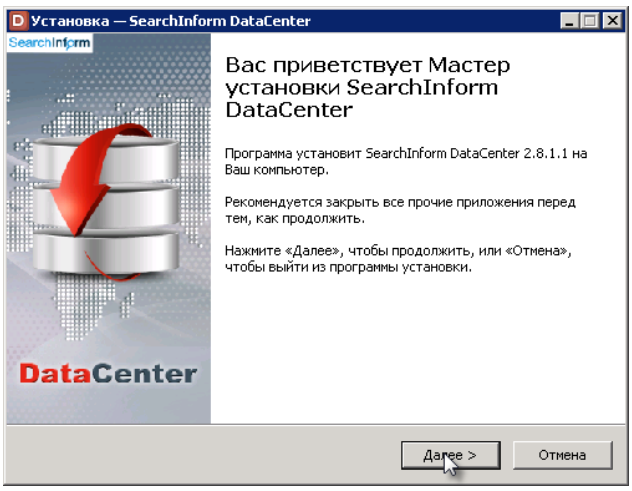
3 Установка

3.1 Установка DataCenter

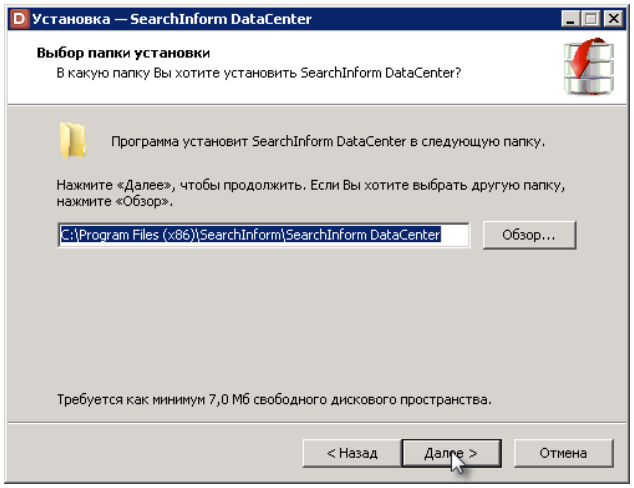
Установка SearchInform DataCenter осуществляется из дистрибутива



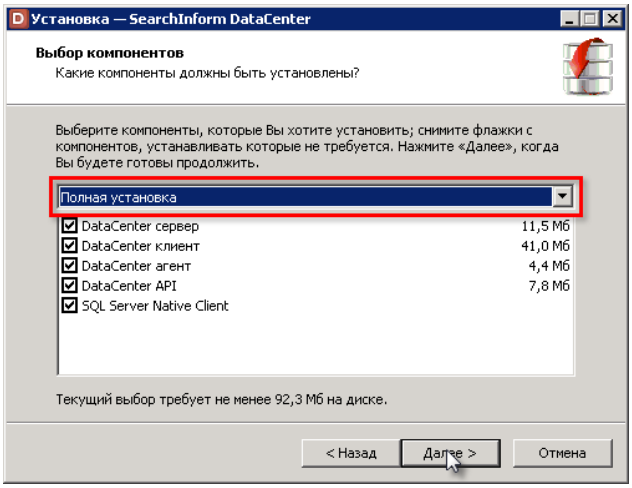
Выберите Русский, щёлкните **OK**.



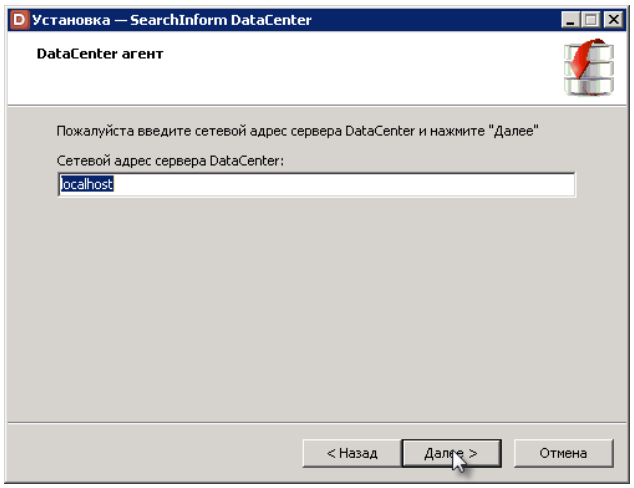
Щёлкните **Далее**.



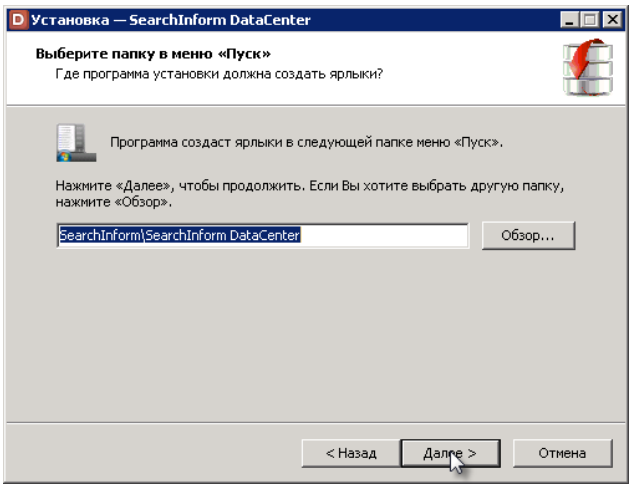
Щёлкните **Далее**.



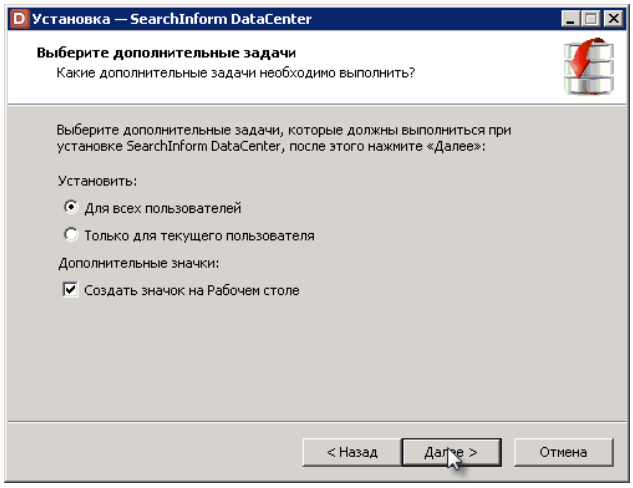
Выберите полную установку (все компоненты), щёлкните **Далее**.



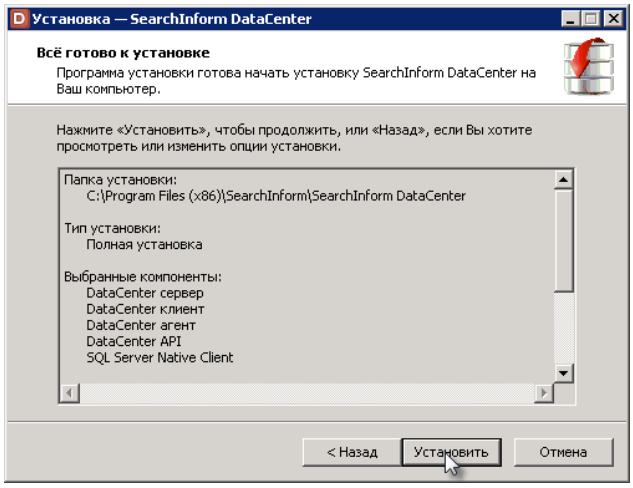
Введите **localhost**, щёлкните **Далее**.



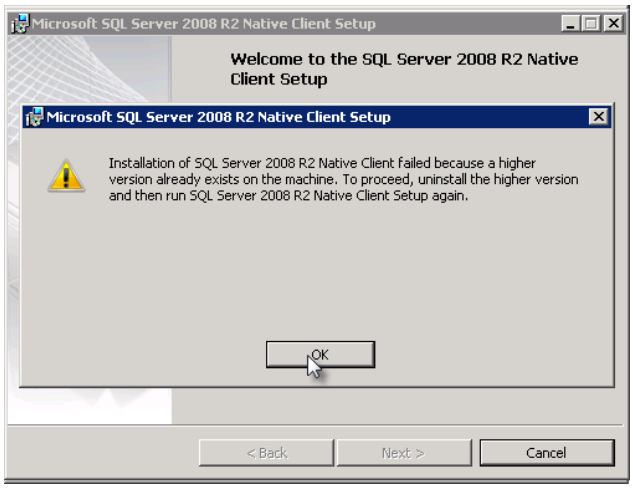
Щёлкните **Далее**.



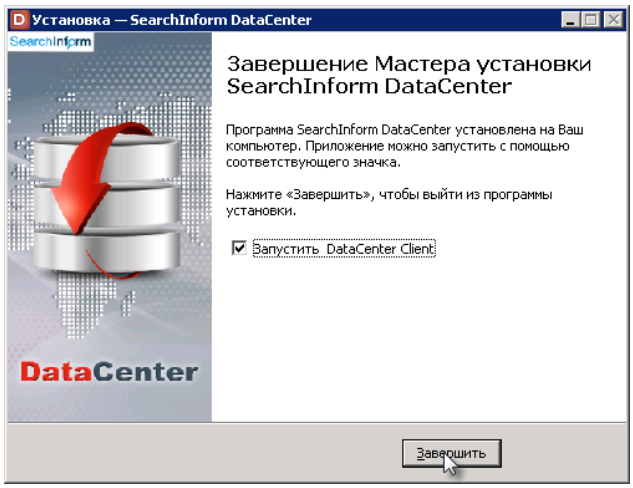
Отметьте необходимые параметры, щёлкните **Далее**.



Проверьте параметры и щёлкните **Установить**.



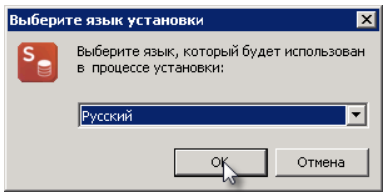
В процессе установки во всех окнах с сообщениями MS SQL Native Client щёлкните **OK**.



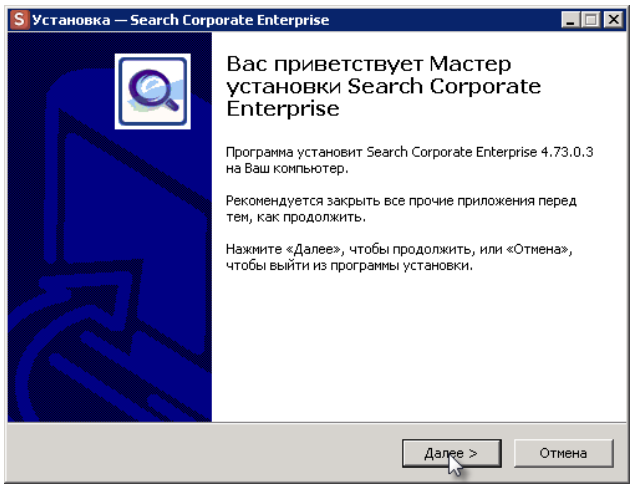
Отметьте флажком **Запустить DataCenter Client** и щёлкните **Завершить**.

3.2 Установка Search Server

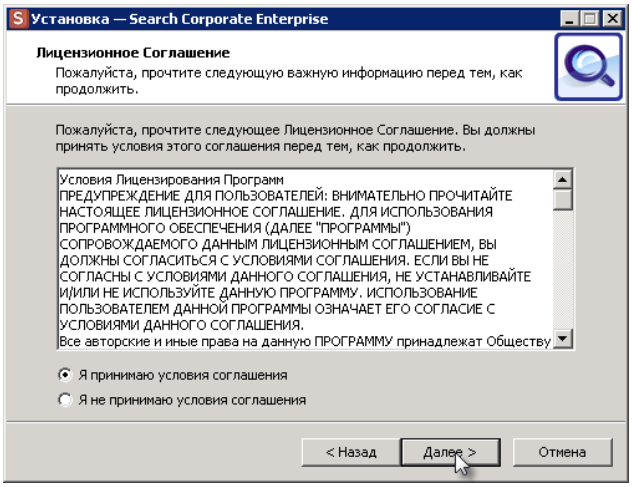
Установка Search Server осуществляется из дистрибутива



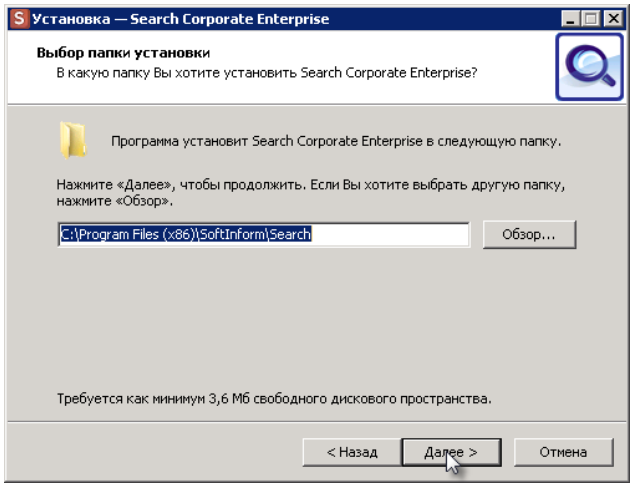
Выберите язык установки, щёлкните **OK**.



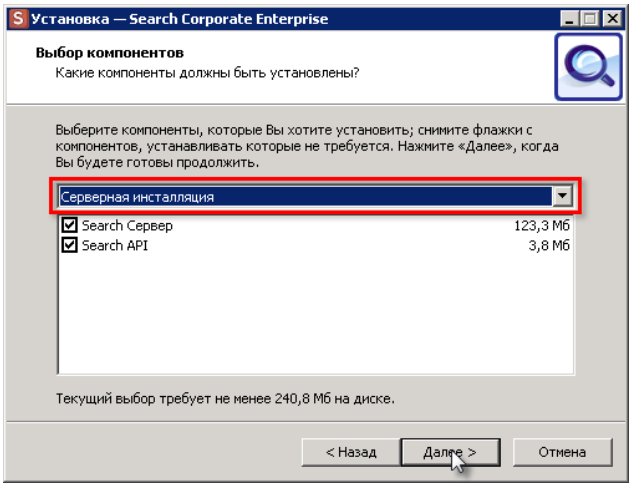
Щёлкните **Далее**.



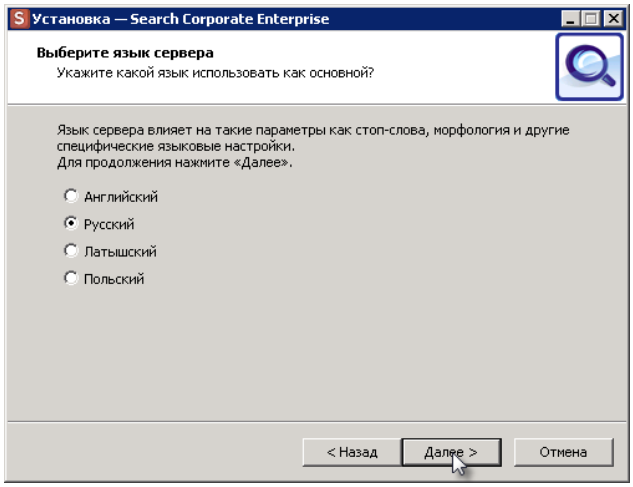
Примите условия соглашения, щёлкните **Далее**.



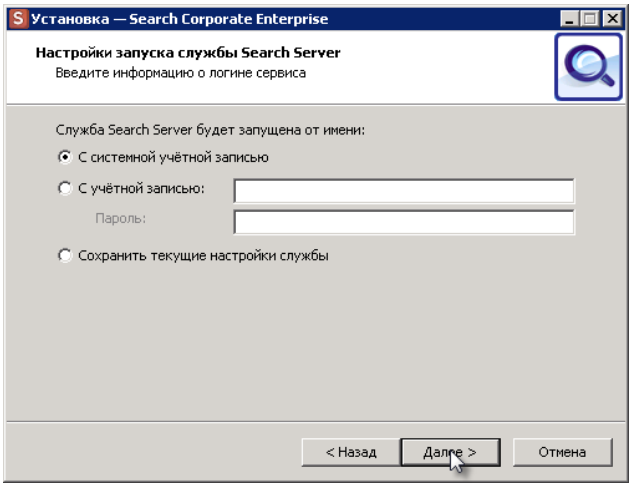
Щёлкните **Далее**.



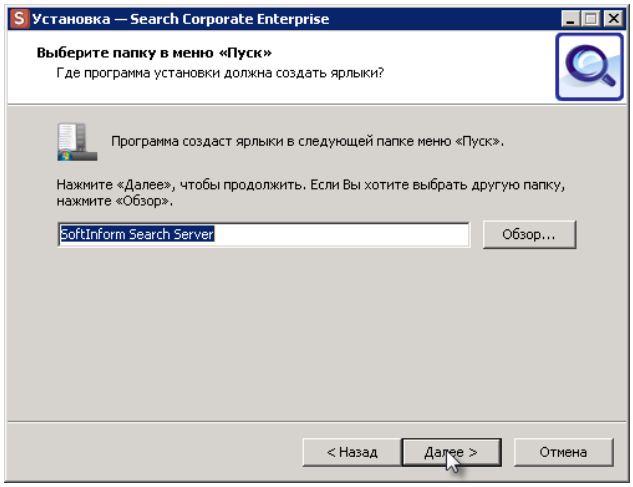
Выберите серверную инсталляцию (все компоненты), щёлкните **Далее**.



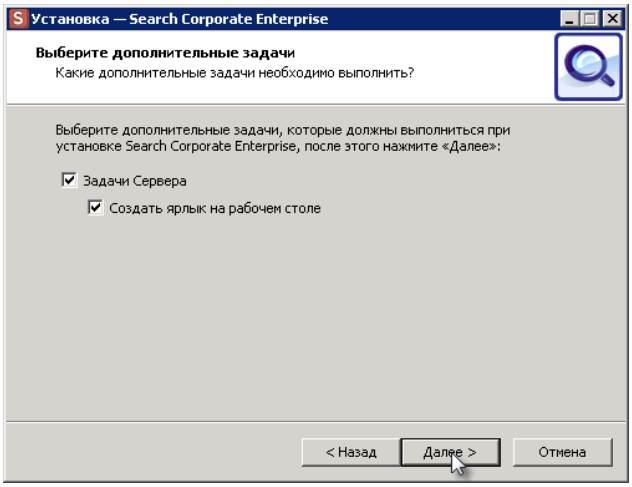
Отметьте параметр **Русский**, щёлкните **Далее**.



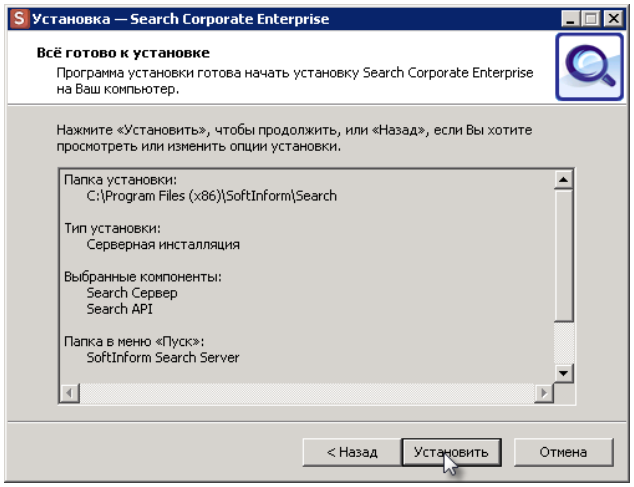
Выберите параметр **С системной учётной записью**, щёлкните **Далее**.



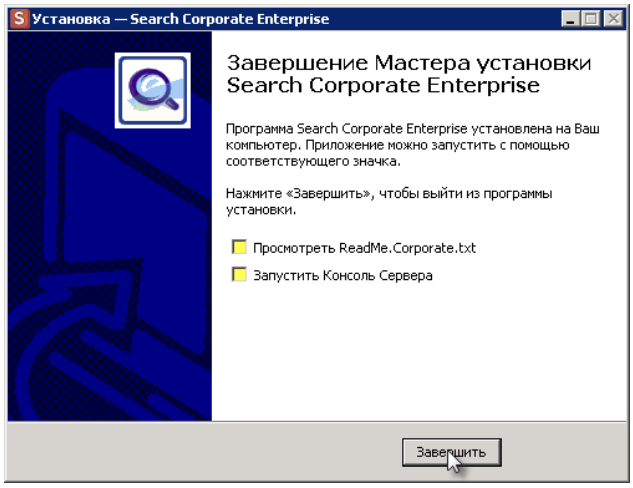
Щёлкните **Далее**.



Щёлкните **Далее**.



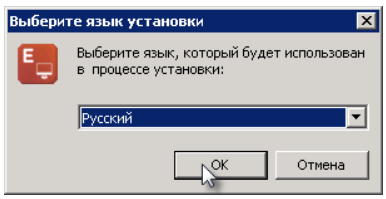
Проверьте параметры и щёлкните **Установить**.



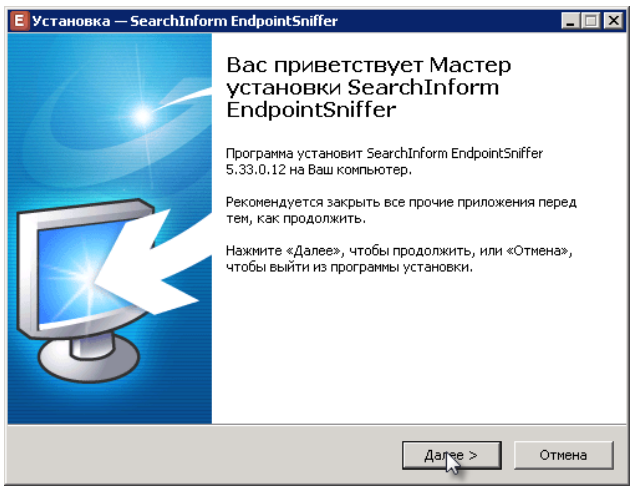
По завершении установки снимите флажки с параметров **Просмотреть Readme.Corporate.txt** и **Запустить Консоль Сервера**, щёлкните **Завершить**.

3.3 Установка EndpointSniffer

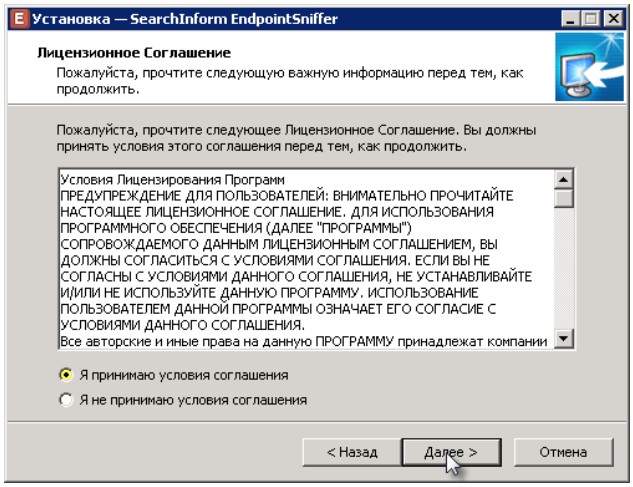
Установка SearchInform EndpointSniffer осуществляется из дистрибутива



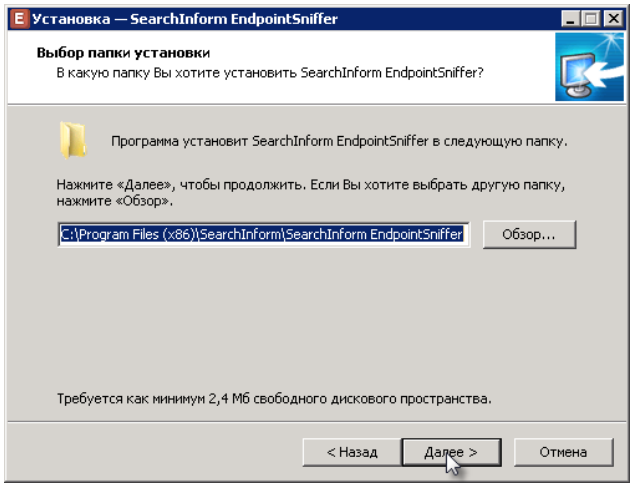
Выберите язык установки, щёлкните **OK**.



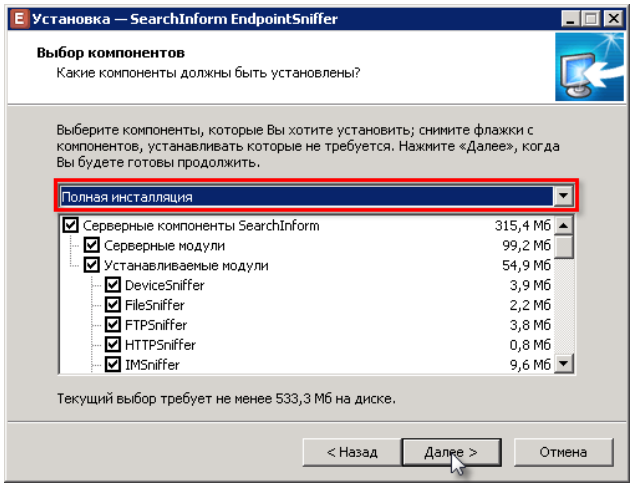
Щёлкните **Далее**.



Примите условия соглашения, щёлкните **Далее**.

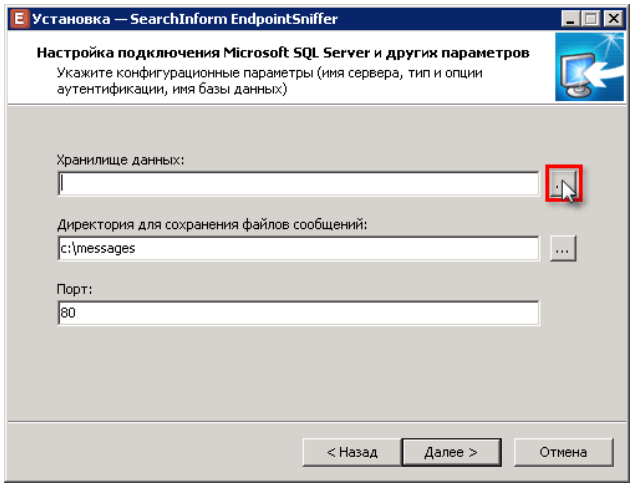


Щёлкните **Далее**.



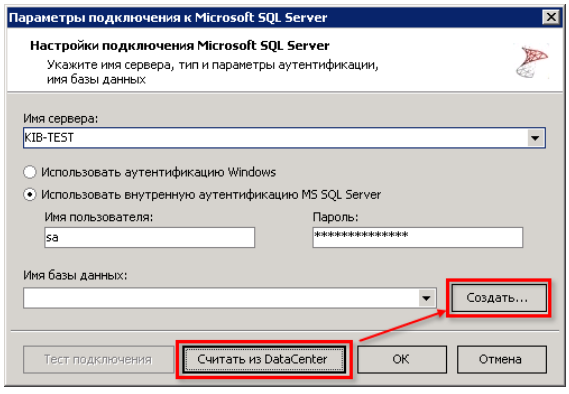
Выберите полную инсталляцию (все компоненты),

щёлкните **Далее**.



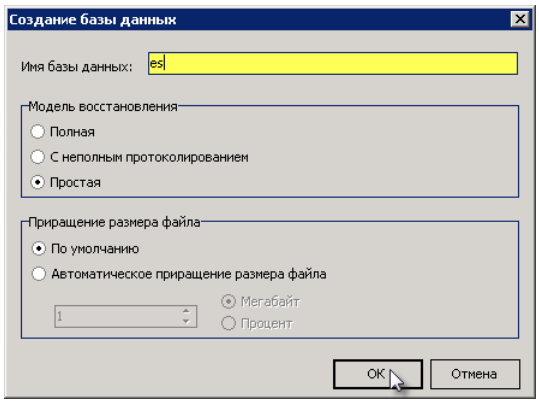
Щёлкните кнопку справа от поля **Хранилище данных**.

В появившемся окне **Параметры подключения к Microsoft SQL Server** щёлкните **Считать из DataCenter**. Поля **Имя сервера**, **Имя пользователя** и **Пароль** будут заполнены автоматически.



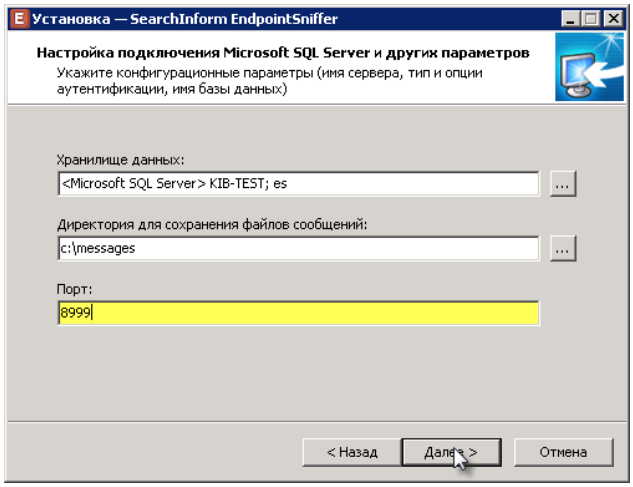
Щёлкните кнопку **Создать**.

В окне **Создание базы данных** введите Имя базы данных: *es.* Остальные параметры оставьте неизменными. Щёлкните **OK**.



Появится информационное сообщение **База данных успешно создана**.

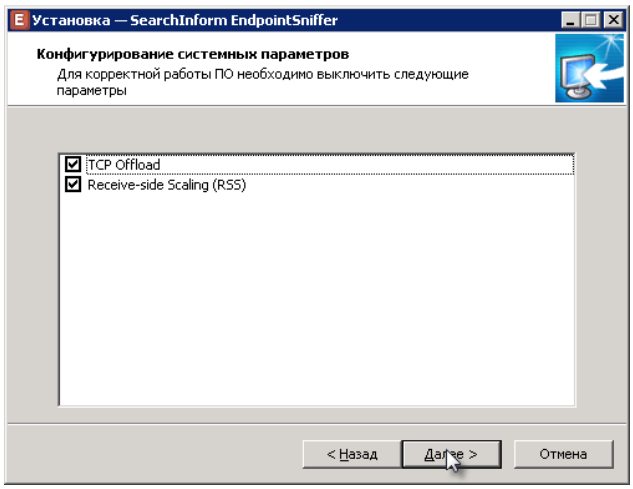
Примените заданные настройки кнопкой **OK**.



В поле **Директория для сохранения файлов сообщений** укажите папку на наиболее свободном локальном диске.

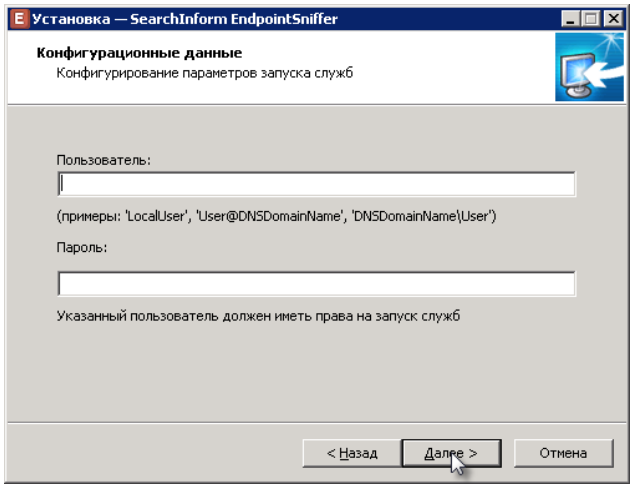
В поле **Порт** укажите значение 8999.

Щёлкните **Далее**.

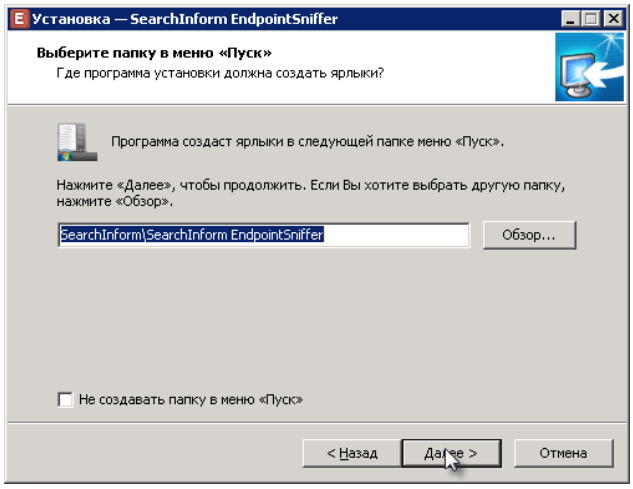


Оставьте настройки по умолчанию.

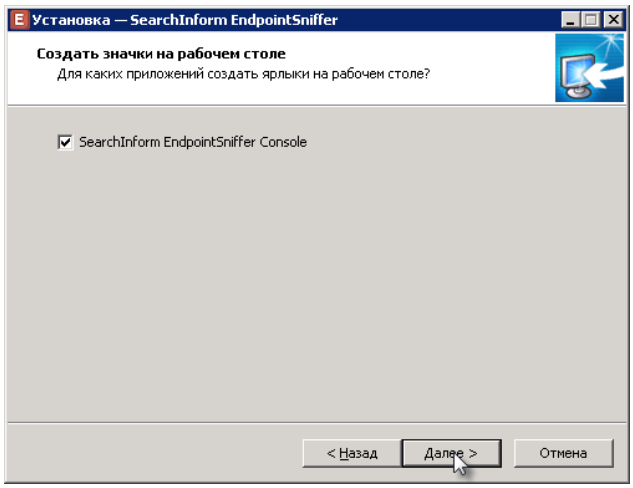
Щёлкните **Далее**.



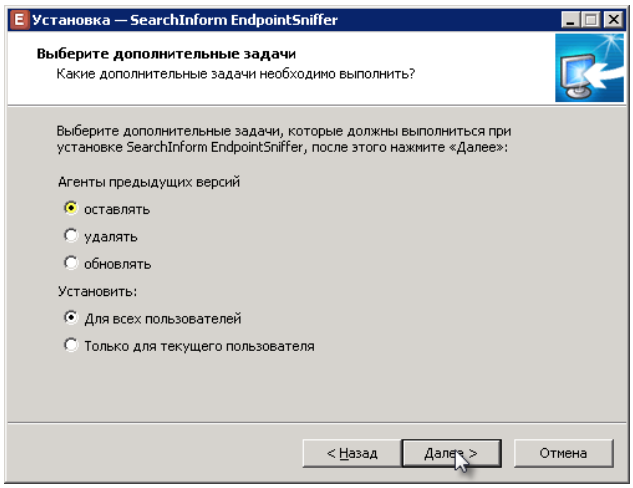
Оставьте поля **Пользователь** и **Пароль** пустыми, щёлкните **Далее**.



Щёлкните **Далее**.

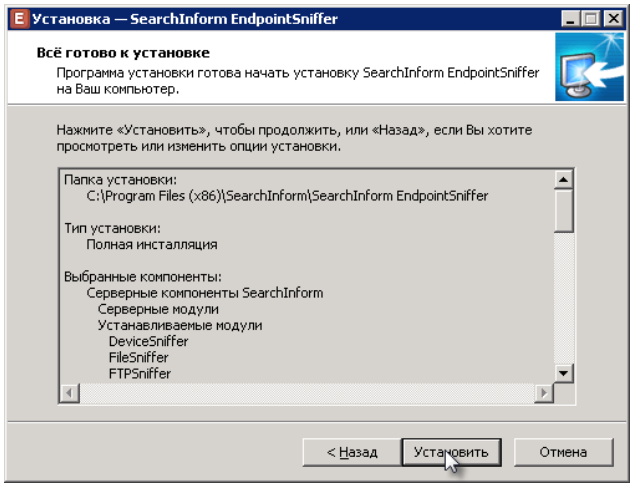


Щёлкните **Далее**.

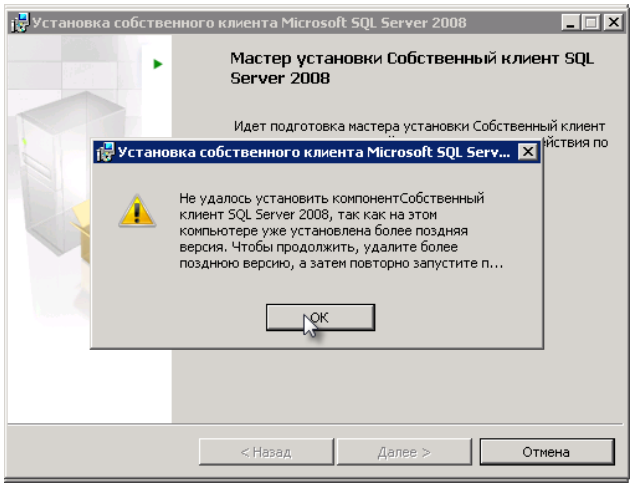


Выберите параметр **оставлять**.

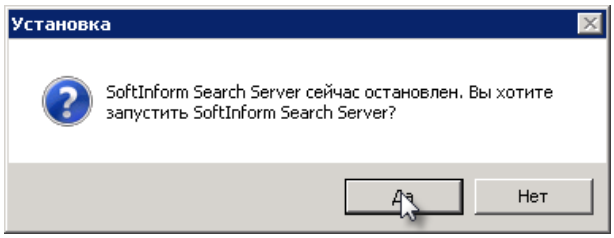
Щёлкните **Далее**.



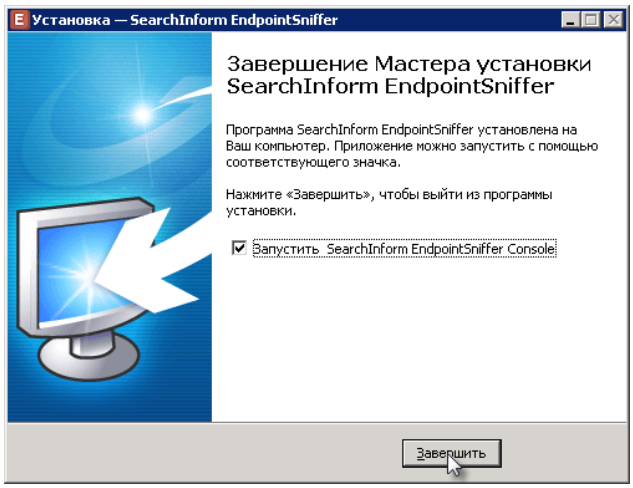
Проверьте параметры и щёлкните **Установить**.



В процессе установки щёлкните **ОК** в окне **Установка собственного клиента...**



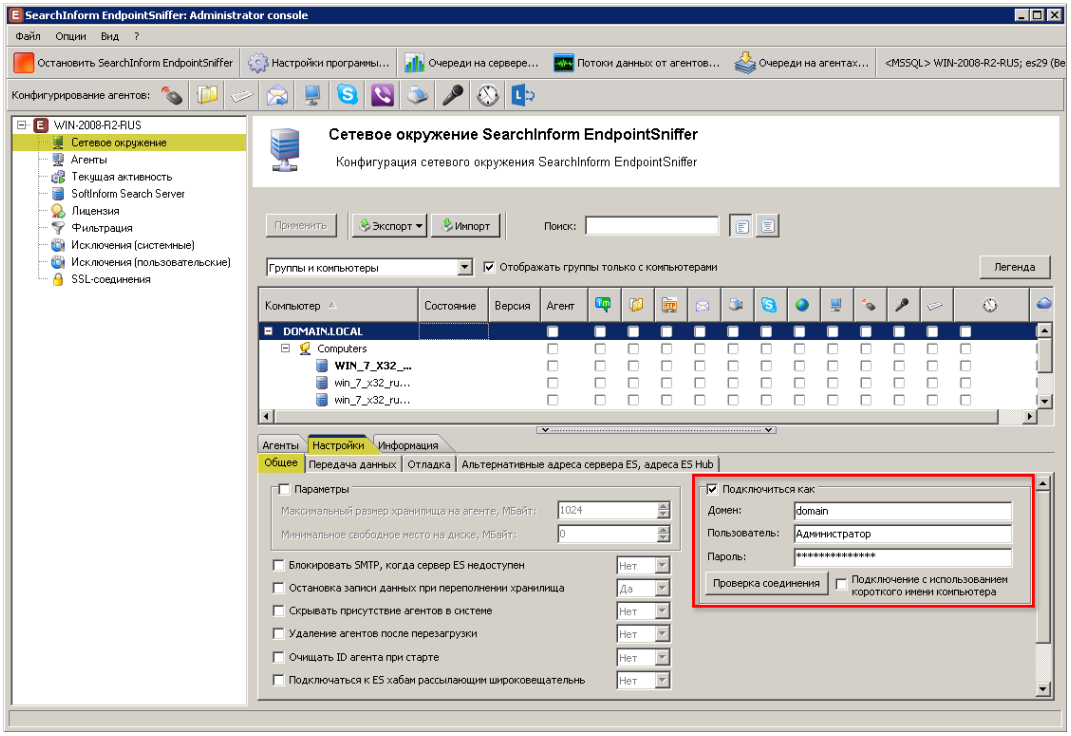
Подтвердите запуск службы SoftInform Search Server.



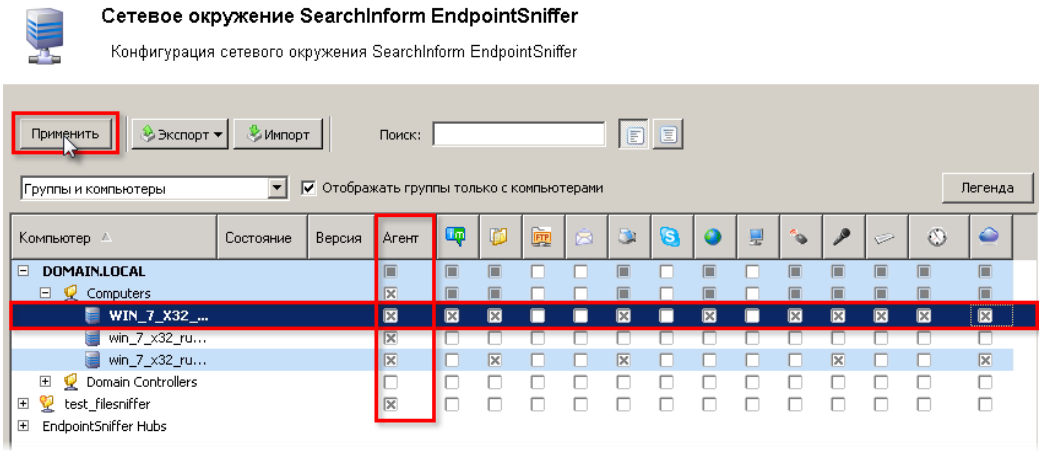
По завершении установки щёлкните **Завершить**.

3.3.1 Установка агента на доменный ПК

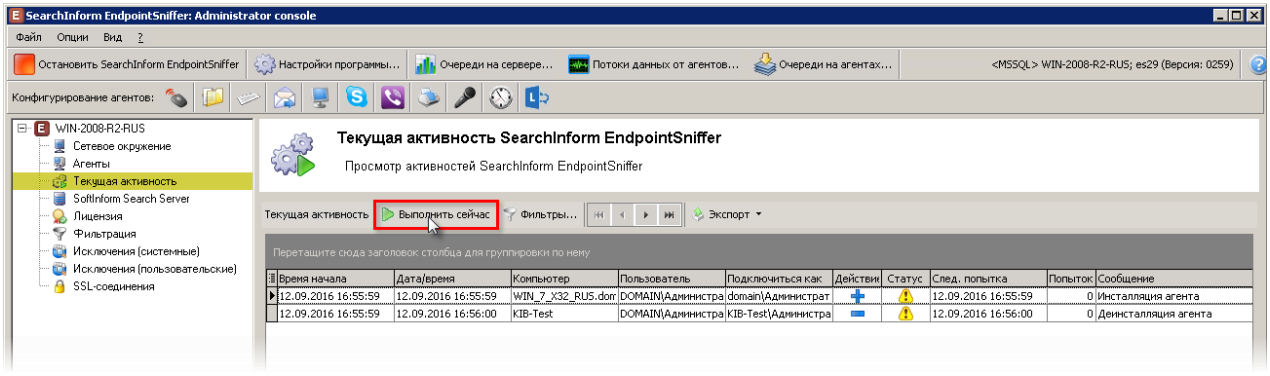
Перейдите на вкладку **Сетевое окружение**. Выделите необходимый домен, в нижней части консоли на вкладке **Настройки → Общее** отметьте флажком параметр **Подключиться как** и укажите данные учётной записи (пользователь, пароль), от имени которой будет выполняться установка агентов. Данная учётная запись должна обладать правами локального администратора на целевой рабочей станции.



Выделите требуемые группы или рабочие станции и установите флажки в столбце **Агент**, также отметьте флажками необходимые каналы передачи данных. После того, как список будет сформирован, щёлкните **Применить**.

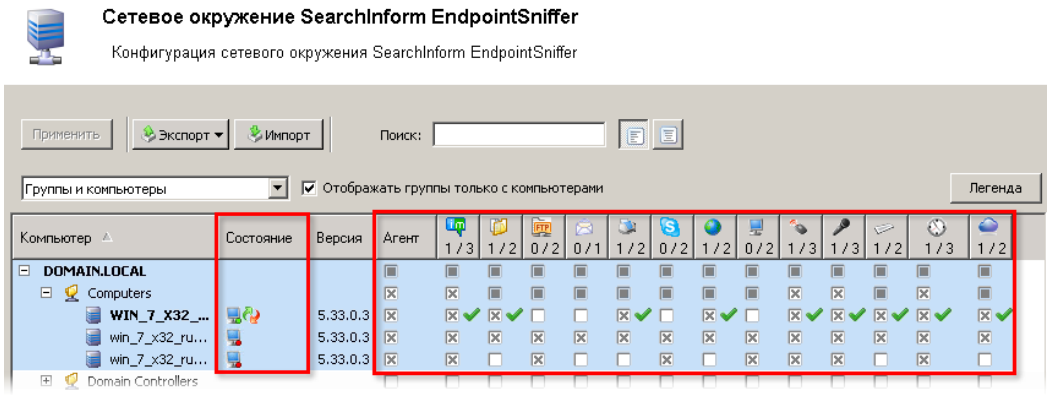


Перейдите на вкладку **Текущая активность**. На данной вкладке отображается журнал совершаемых действий над агентами, а также список неудачных попыток установки/удаления/обновления агентов. Для того, чтобы запустить операцию над агентом, не дожидаясь времени следующей попытки, щёлкните кнопку **Выполнить сейчас**.



В течение некоторого времени будет происходить установка агентов. Активированные модули перехвата отображаются при помощи маркера «✔», рабочие станции, на которые установлены

агенты или модули перехвата, подсвечиваются бледно-голубым цветом. Значок в столбце **Состояние** свидетельствует об активности/неактивности установленного агента.



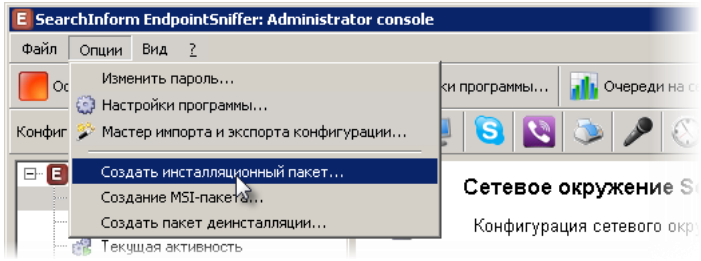
- агент установлен и запущен (происходит перехват данных).

- агент установлен, но не запущен (перехват данных не происходит).

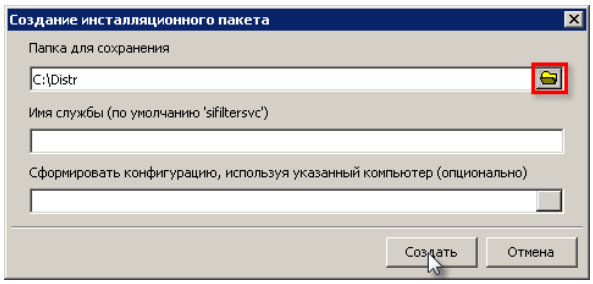
После установки агента необходимо перезагрузить целевую рабочую станцию.

3.3.2 Установка агента на недоменный ПК

Для установки агента локально необходимо создать дистрибутив агента. Выберите команду **Создать инсталляционный пакет** в меню **Опции**.



Выберите директорию для размещения создаваемых файлов.



Задайте имя службы агента[5]. При пустом поле используется имя службы по умолчанию.

Щёлкните **Создать**. Инсталлятор агента будет сохранен в выбранной директории.

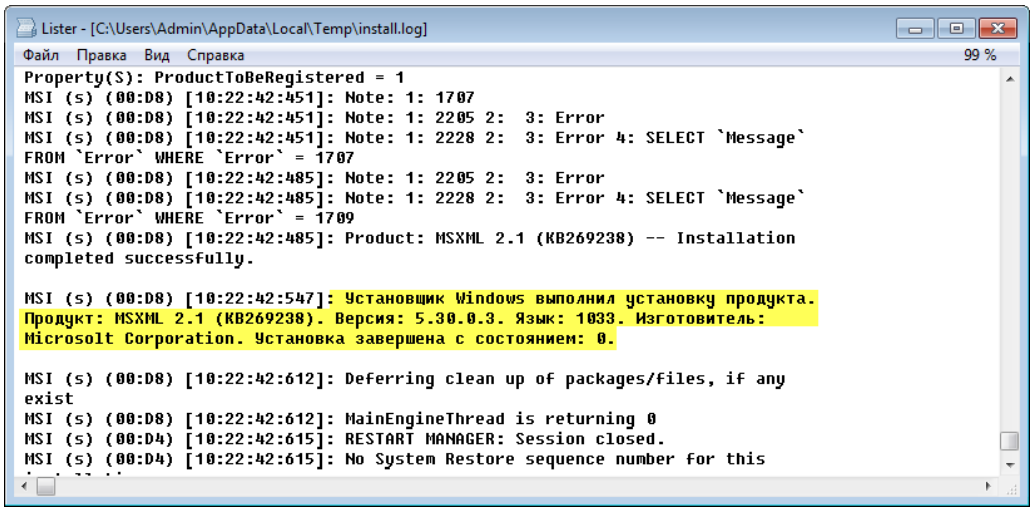
Скопируйте инсталлятор на целевую рабочую станцию. *Путь к установочным файлам не должен содержать кириллические символы!*

Запустите файл **install_agent.exe** на целевой рабочей станции. Запуск должен производиться пользователем с правами локального администратора. Также для установки на ОС Windows XP папка «Documents and Settings» не должна быть переименована.

Ход установки записывается в файл **install.log**. Файл создается во временной папке операционной системы.

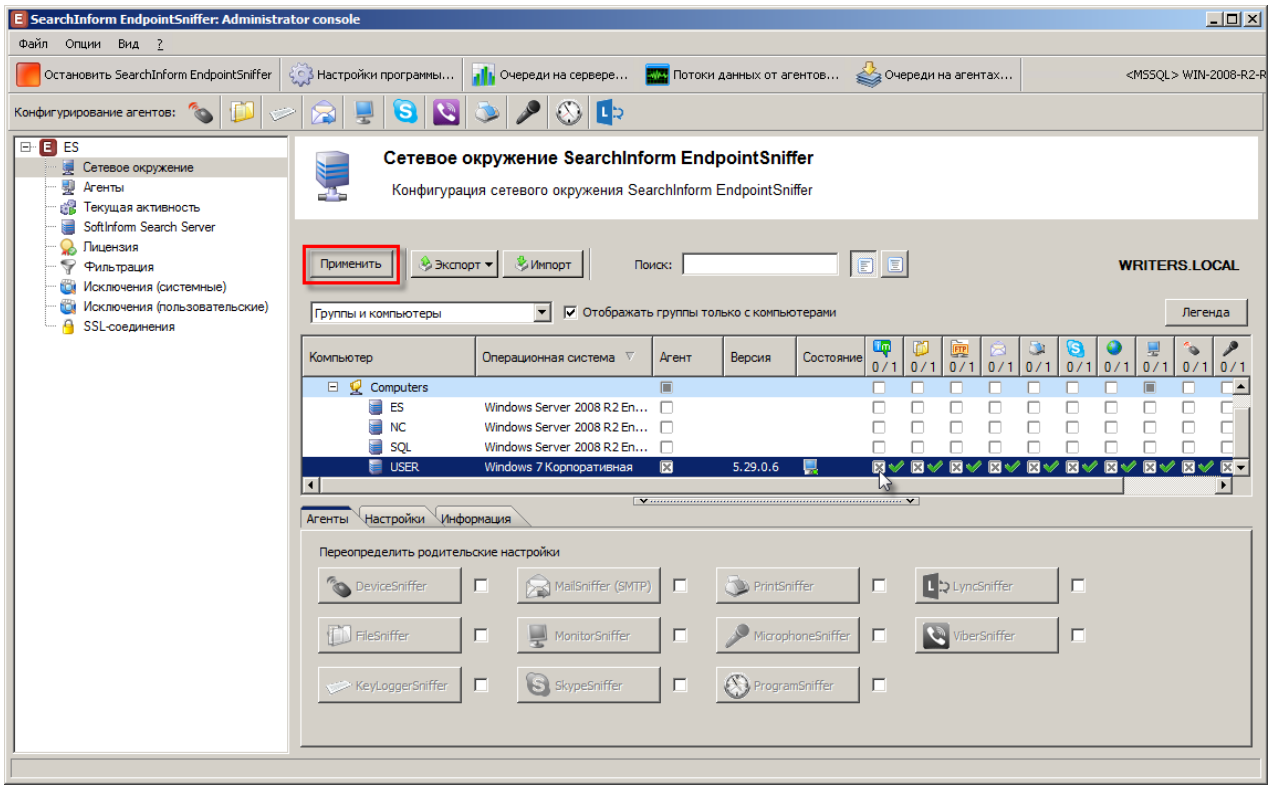
[5] Заданное имя службы должно совпадать с именем, указанным в настройках EndpointSniffer (Настройки → Настройки агента → Маскировка агентов). В противном случае агент будет автоматически переустановлен с указанным в настройках именем.

Установка может занять некоторое время. При успешной установке в логе будет записана информация вида **Установка завершена с состоянием: 0**. В случае завершения установки с ошибкой – код ошибки.



Если пользовательская конфигурация агента не создавалась, в консоли администрирования EndpointSniffer напротив рабочей станции с установленным агентом отметьте флажками требуемые модули перехвата.

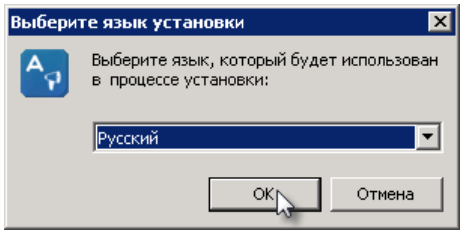
Щёлкните кнопку **Применить**.



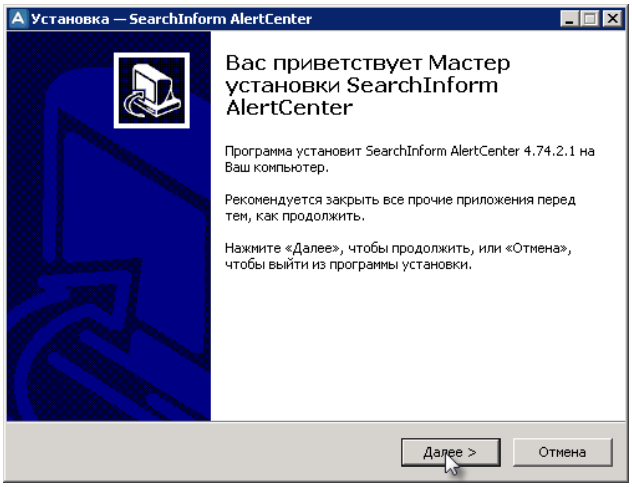
После установки агента перезагрузите целевую рабочую станцию.

3.4 Установка AlertCenter

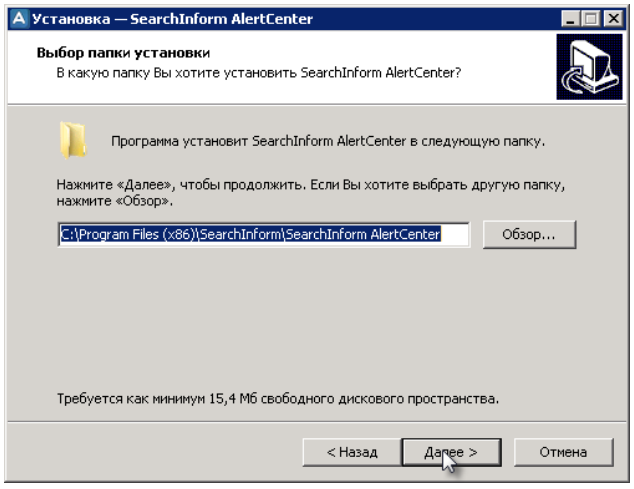
Установка SearchInform AlertCenter осуществляется из дистрибутива



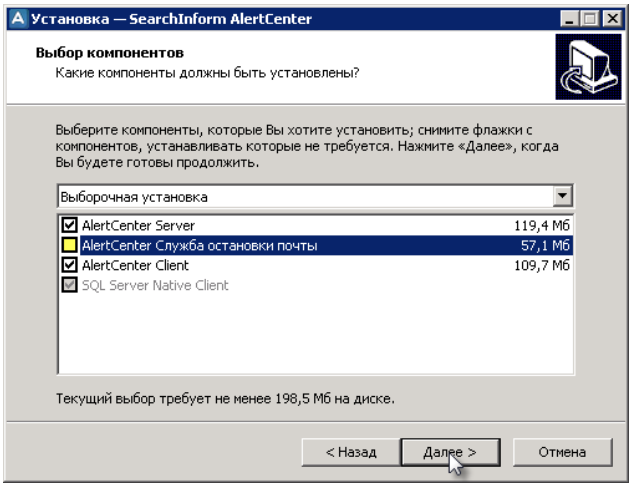
Выберите язык установки, щёлкните **OK**.



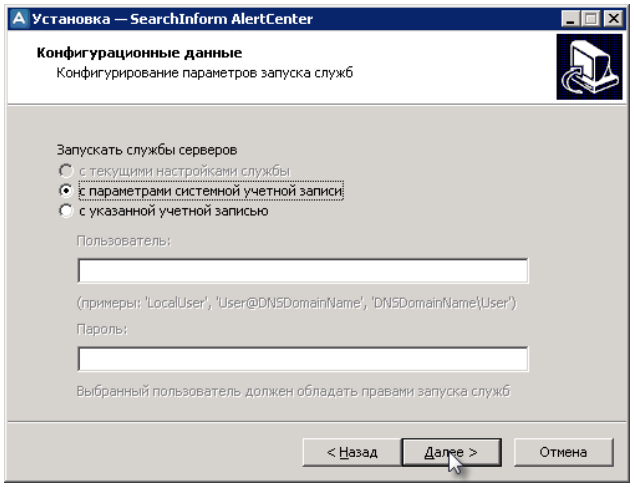
Щёлкните **Далее**.



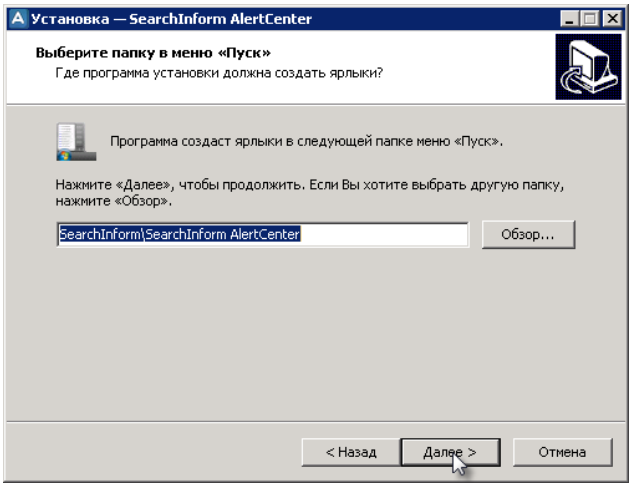
Щёлкните **Далее**.



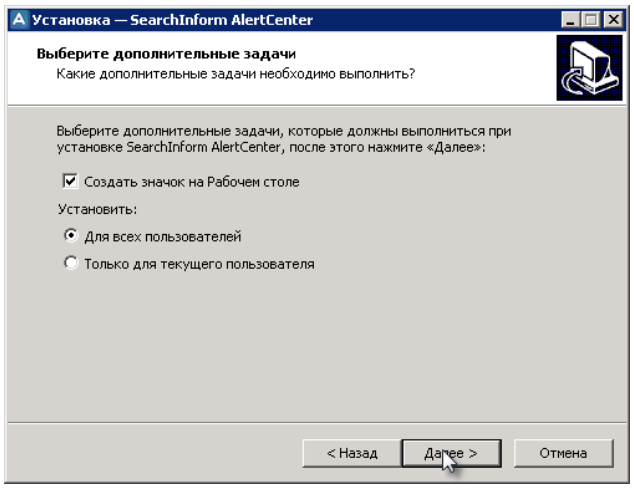
Выберите полную инсталляцию (все компоненты) или, если карантин не нужен, снимите флажок **AlertCenter Служба остановки почты**. Щёлкните **Далее**.



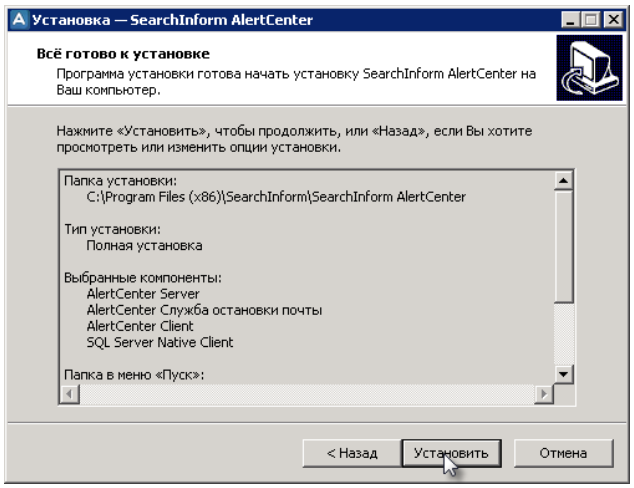
Оставьте настройки по умолчанию, щёлкните **Далее**.



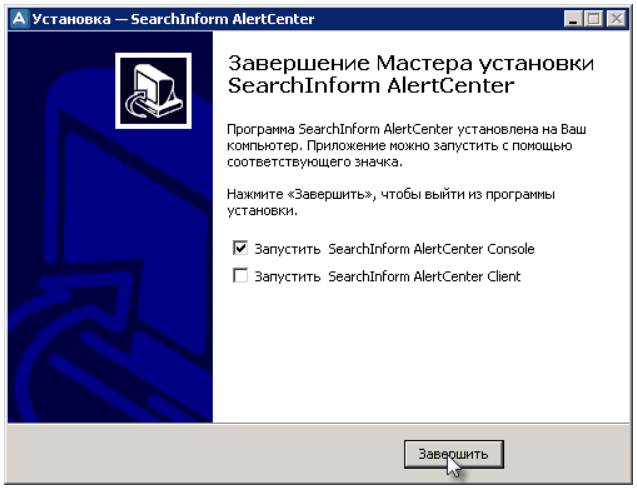
Щёлкните **Далее**.



Щёлкните **Далее**.



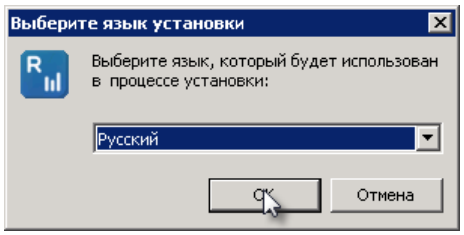
Проверьте параметры и щёлкните **Установить**.



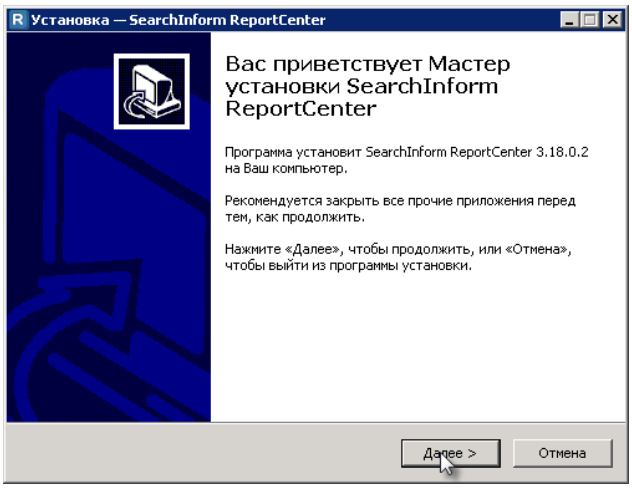
По завершении установки снимите флажок с параметра **Запустить SearchInform AlertCenter Client** и щёлкните **Завершить**.

3.5 Установка ReportCenter

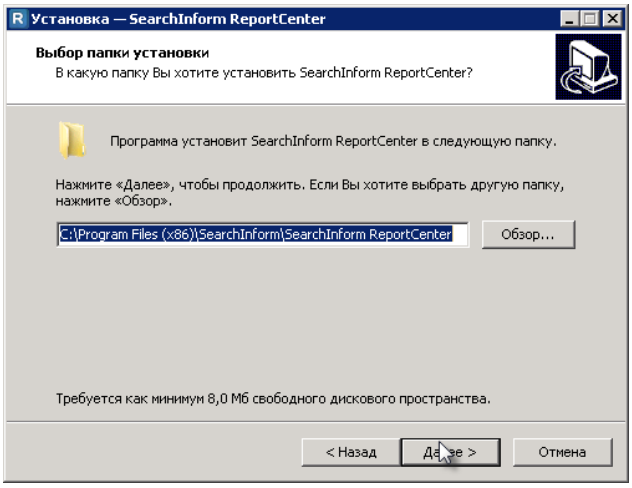
Установка SearchInform ReportCenter осуществляется из дистрибутива.



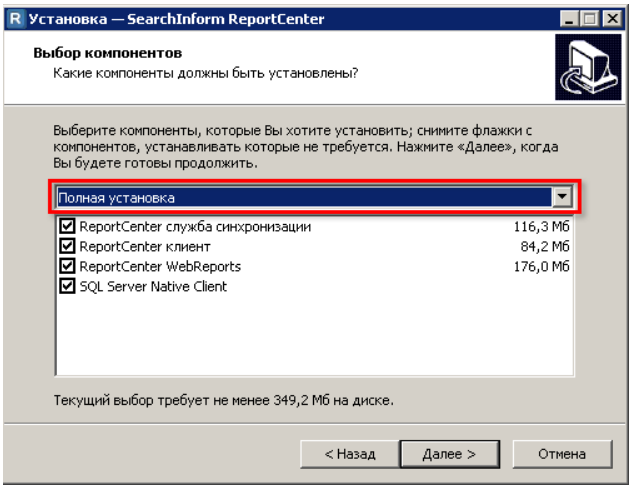
Выберите язык установки, щёлкните **OK**.



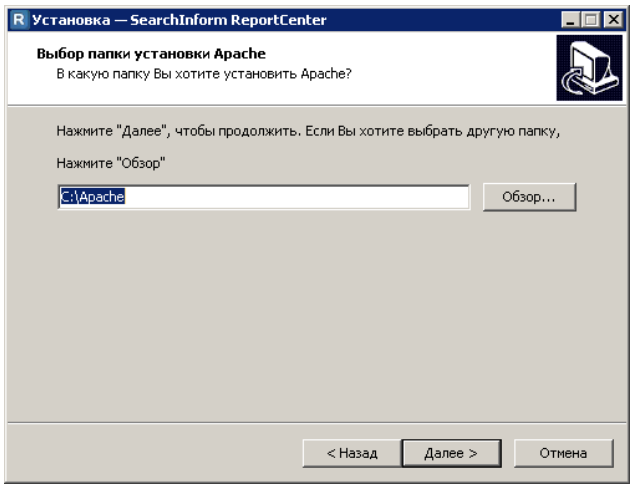
Щёлкните **Далее**.



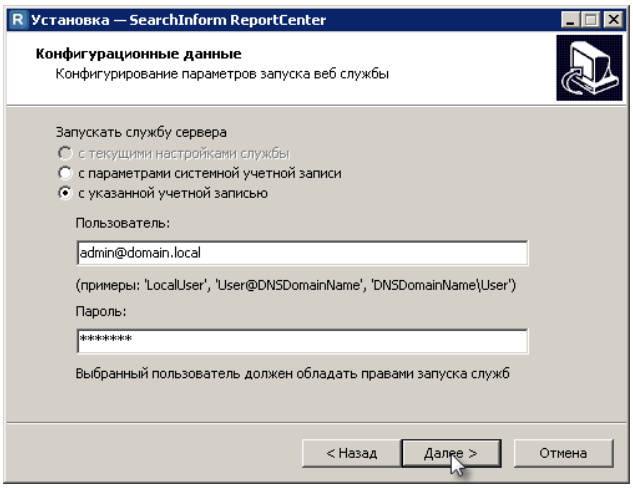
Щёлкните **Далее**.



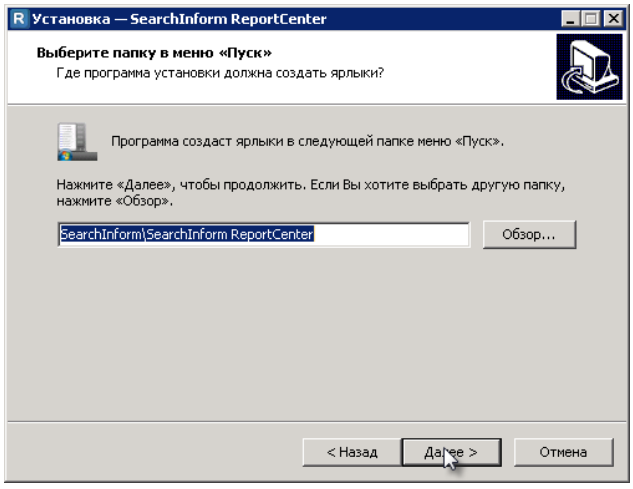
Выберите полную инсталляцию (все компоненты), щёлкните **Далее**.



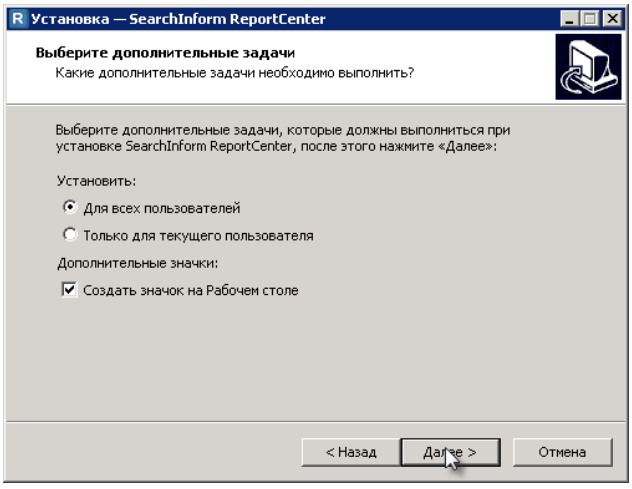
Выберите директорию, в которую будет установлен веб-сервер Apache (необходим для компонента Web отчёты).



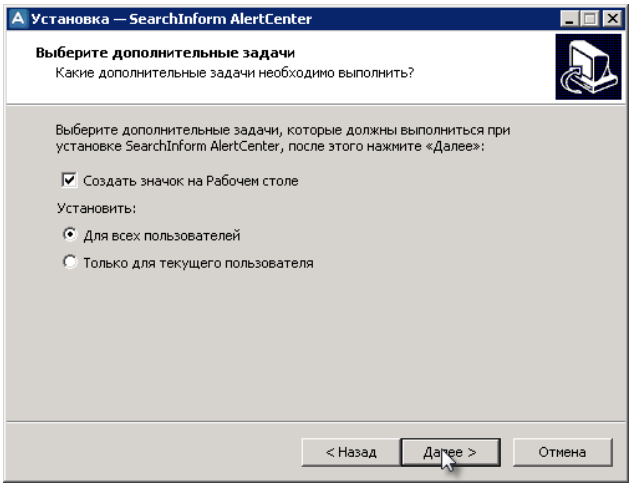
Укажите параметры учётной записи, обладающей правом запуска служб (для использования своего рабочего календаря, а не по умолчанию и т. д.).



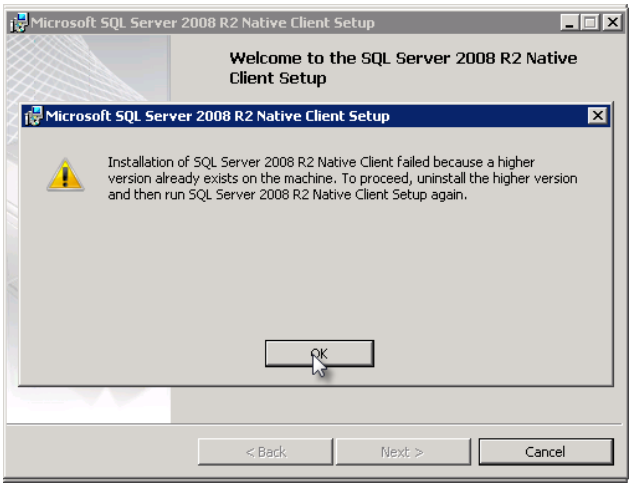
Щёлкните **Далее**.



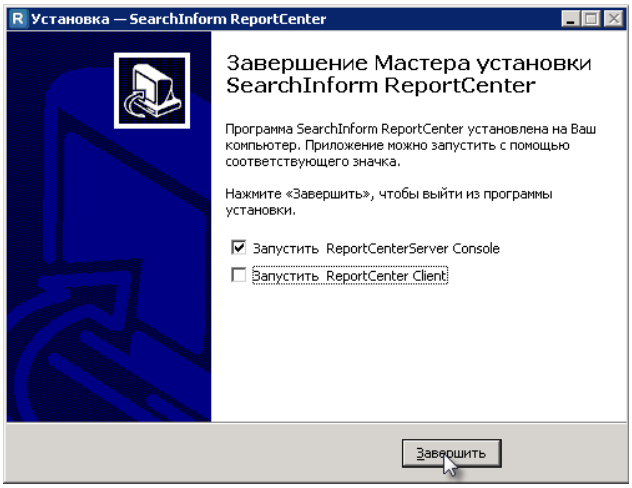
Щёлкните **Далее**.



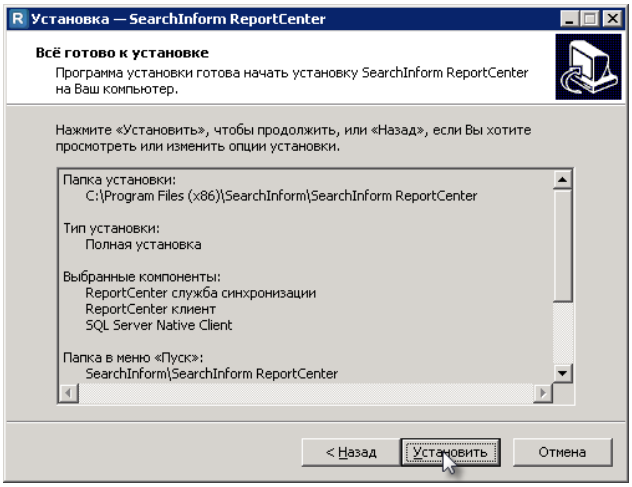
Щёлкните **Далее**.



В процессе установки появится сообщения от MS SQL Native Client, щёлкните **ОК**.

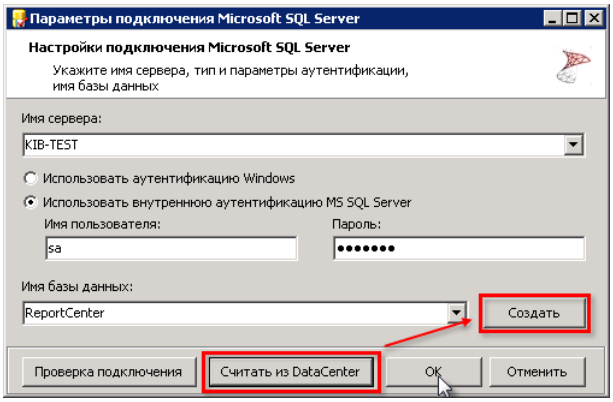


По завершении установки снимите флажок с параметра **Запустить SearchInform ReportCenter Client** и щёлкните **Завершить**.



Проверьте параметры и щёлкните **Установить**.

В появившемся окне **Параметры подключения к Microsoft SQL Server** щёлкните **Считать из DataCenter**. Поля **Имя сервера**, **Имя пользователя** и **Пароль** будут заполнены автоматически.

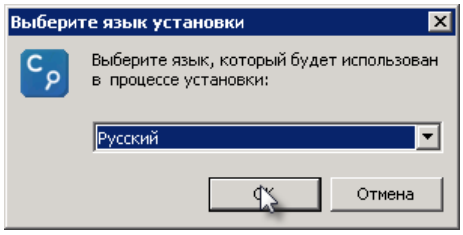


Щёлкните кнопку **Создать**, после чего появится информационное сообщение **База данных успешно создана**.

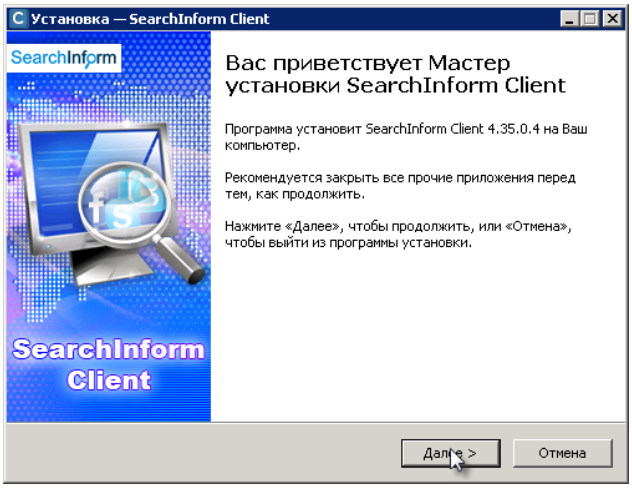
Примените заданные настройки кнопкой **ОК**.

3.6 Установка SearchInform Client

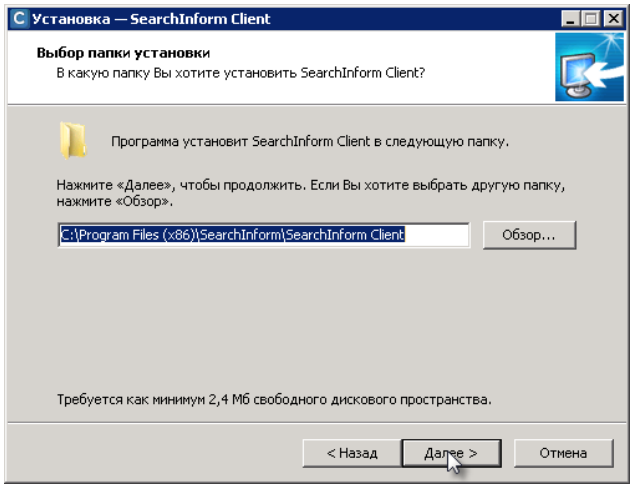
Установка SearchInform Client осуществляется из дистрибутива.



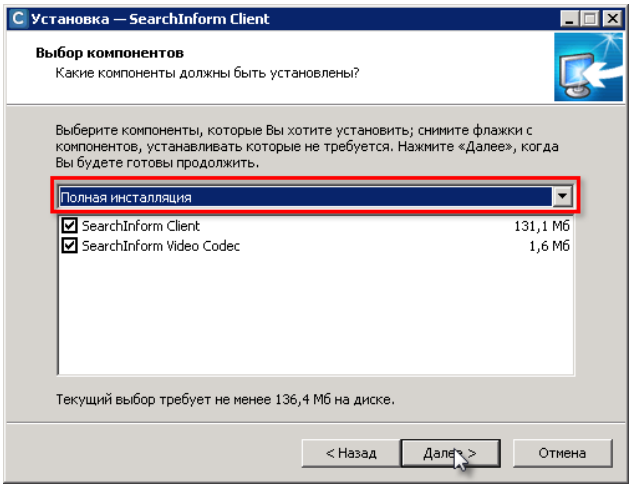
Выберите язык установки, щёлкните **OK**.



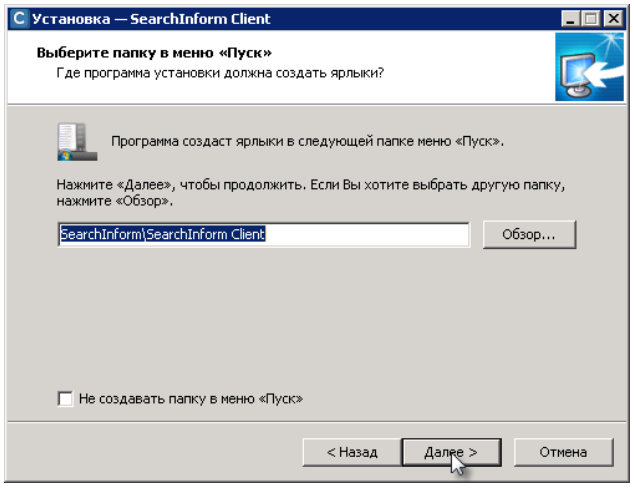
Щёлкните **Далее**.



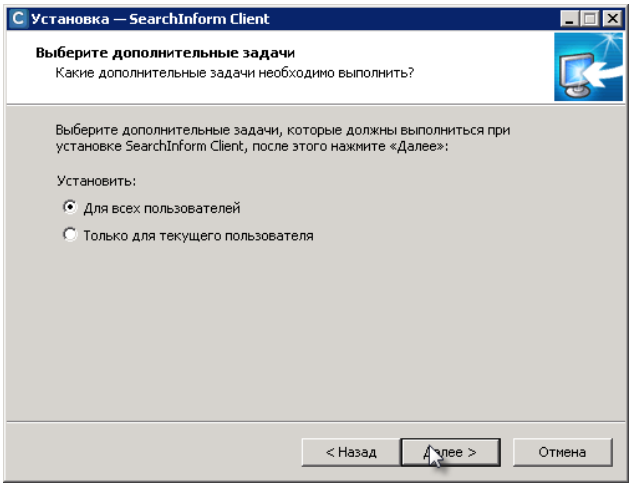
Щёлкните **Далее**.



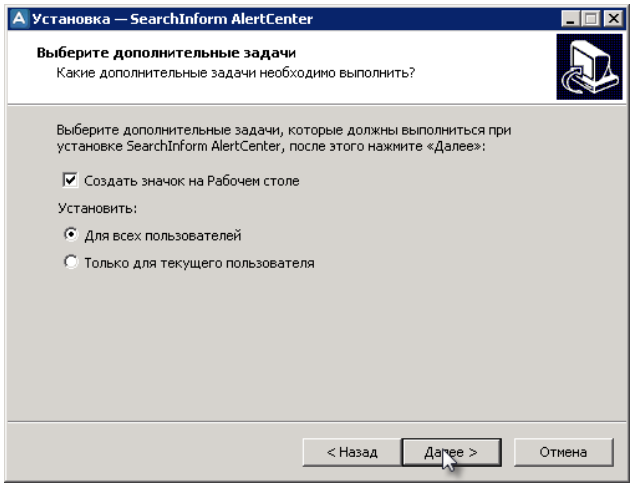
Выберите полную инсталляцию (все компоненты), щёлкните **Далее**.



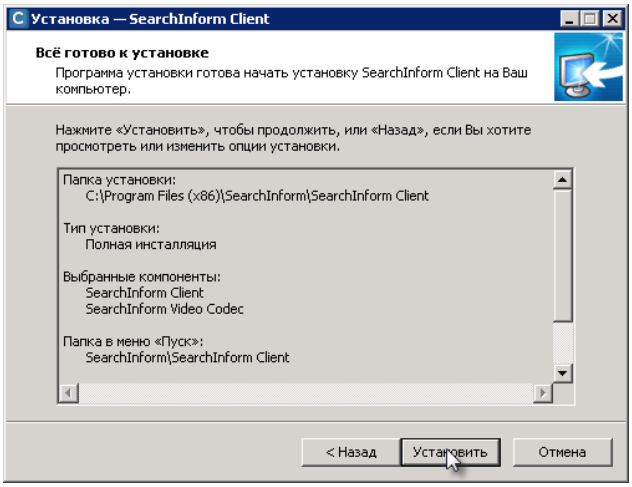
Щёлкните **Далее**.



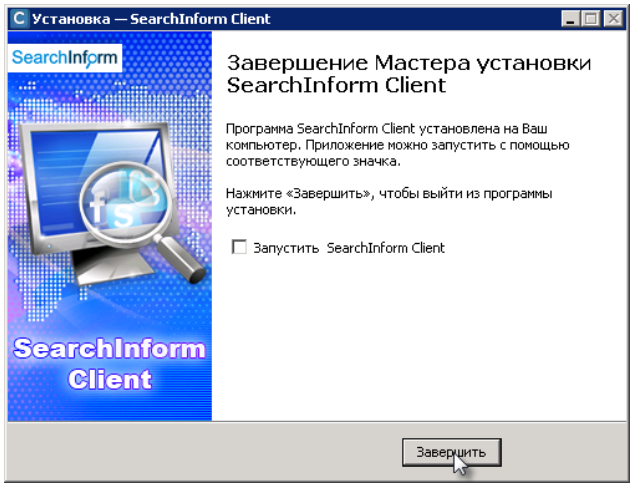
Щёлкните **Далее**.



Щёлкните **Далее**.



Проверьте параметры и щёлкните **Установить**.



По завершении установки щёлкните **Завершить**.