RedCheck

СРЕДСТВО АНАЛИЗА ЗАЩИЩЕННОСТИ

Руководство администратора

АЛМЮ.501410.RC02-01.РА

Версия документа 2.6.9.ru

ALTEX SOFT

Содержание

Аннотация

Данное руководство является помощником для системных администраторов и администраторов ИБ, осуществляющих установку, настройку и эксплуатацию программного средства анализа защищенности RedCheck (далее – RedCheck, Система).

Руководство состоит из следующих разделов:

- 1 Знакомство с RedCheck
- 2 Состав дистрибутива RedCheck
- 3 Системные требования
- 4 Установка RedCheck
- 5 Сопровождение Системы
- 6 Решение проблем
- 7 Термины и сокращения

Производитель может вносить в Руководство изменения, связанные с улучшением ПО. Актуальная версия документации для новой редакции Руководства находится на сайте компании.

Производитель:	АО «АЛТЭКС-СОФТ»
Почтовый адрес:	ул. Маяковского, д. 10, пом. VII, мкр. Болшево, г. Королев, Московская обл., 141067
Электронная почта:	info@altx-soft.ru / support@altx-soft.ru
Телефон:	+7(495) 543-31-01
Адрес сайта производителя:	altx-soft.ru
Адрес сайта товара:	redcheck.ru

1 Знакомство с RedCheck

Содержание

1.1 Основные сведения

RedCheck представляет собой комплексное решение для анализа защищённости и управления ИБ для предприятий любого масштаба.

Система предназначена для использования ИТ-специалистами, службами ИБ, а также органами по аттестации объектов информатизации.

Система применима для решения следующих задач:

- централизованное сетевое или локальное определение уязвимостей системного и прикладного ПО, аппаратных платформ;
- контроль настроек параметров безопасности, соблюдения требований политик и стандартов ИБ;
- инвентаризация оборудования и ПО;
- контроль целостности файлов и каталогов;
- создание отчетов по результатам аудитов.

Объектами сканирования для RedCheck являются:

- ОС Microsoft Windows и Linux, в том числе отечественные;
- сетевое оборудование;
- протоколы АСУ ТП;
- средства виртуализации;
- средства контейнеризации и оркестрации;
- СУБД;
- офисные пакеты и другое прикладное ПО;

Система может использоваться для реализации мер защиты информации в ИС и АСУ, а также для обеспечения безопасности персональных данных в соответствии с приказами ФСТЭК России:

- № 17 от 11 февраля 2013 г.;
- № 21 от 18 февраля 2013 г.;
- № 31 от 14 марта 2014 г.;
- № 239 от 25 декабря 2017 г.;

в части:

1. ограничения программной среды (ОПС):

- управление установкой (инсталляцией) компонентов ПО, в том числе:
  - определение компонентов, подлежащих установке;
  - настройка параметров установки компонентов;
  - контроль за установкой компонентов ПО;

2. регистрации событий безопасности (РСБ):

- сбор, запись и хранение информации о событиях безопасности в течении установленного времени хранения;
- мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них;

3. контроля (анализа) защищенности информации (АНЗ):

- выявление, анализ уязвимостей ИС и оперативное устранение вновь выявленных уязвимостей;
- контроль установки обновлений ПО, включая обновление ПО средств защиты информации;
- контроль работоспособности, параметров настройки и правильности функционирования ПО и СЗИ;
- контроль состава технических средств, ПО и СЗИ;

4. обеспечения целостности ИС и информации (ОЦЛ):

- контроль целостности ПО, включая ПО СЗИ;

5. защиты среды виртуализации (ЗСВ):

- контроль целостности виртуальной инфраструктуры и её конфигураций;

6. управления конфигурацией ИС и системы защиты персональных данных (УКФ):

- управление изменениями конфигурации ИС и системы защиты персональных данных;
- документирование информации (данных) об изменениях в конфигурации ИС и системы защиты персональных данных.

Система может использоваться для реализации мер по обеспечению безопасности значимых объектов критической информационной инфраструктуры в соответствии с приказом ФСТЭК России № 239 от 25 декабря 2017 г., в части:

1. идентификация и аутентификация (ИАФ):

- инвентаризация информационных ресурсов;
- анализ уязвимостей и их устранение;
- регистрация событий безопасности;
- мониторинг безопасности;
- проведение внутренних аудитов;
- проведение внешних аудитов;

2. обеспечение целостности (ОЦЛ):

- контроль целостности ПО;
- контроль целостности информации;

3. управление конфигурацией (УКФ):

- идентификация объектов управления конфигурацией;
- управление изменениями;
- контроль действий по внесению изменений;

4. управление обновлениями ПО (ОПО):

- поиск, получение обновлений ПО от доверенного источника;
- контроль целостности обновлений ПО;
- установка обновлений ПО.

RedCheck внесен в государственный реестр системы сертификации средств защиты информации по требованиям безопасности информации и имеет сертификат соответствия № 3172 от 23.06.2014.

RedCheck внесен в Единый реестр российских программ для электронных вычислительных машин и баз данных, номер регистрации 2013661684

СИСТЕМА СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ № 3172

Внесен в государственный реестр системы сертификации средств защиты информации по требованиям безопасности информации 23 июня 2014 г.

Выдан: 23 июня 2014 г.
Действителен до: 23 июня 2020 г.
Срок действия продлён до: 23 июня 2025 г.

Настоящий сертификат удостоверяет, что **средство анализа защищенности RedCheck**, разработанное и производимое АО «АЛТЭКС-СОФТ», является средством контроля (анализа) защищенности информации, не содержащей сведений, составляющих государственную тайну, соответствует требованиям по безопасности информации, установленным в документе «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2018) - по 4 уровню доверия и технических условиях ТУ АЛМЮ.501410.RC02-01 при выполнении указаний по эксплуатации, приведенных в формуляре АЛМЮ.501410. RC02-01.30.

Сертификат выдан на основании технического заключения от 10.03.2014, оформленного по результатам сертификационных испытаний испытательной лабораторией ООО «ЦБИ» (аттестат аккредитации от 11.04.2016 № СЗИ RU.0001.01БИ00.Б004), экспертного заключения от 19.05.2014, оформленного органом по сертификации ФАУ «ГНИИИ ПТЗИ ФСТЭК России» (аттестат аккредитации от 05.05.2016 № СЗИ RU.0001.01БИ00.А002), технических заключений от 25.05.2017, 13.09.2018 и 30.09.2020, оформленных по результатам испытаний испытательной лабораторией ООО «ЦБИ», и экспертного заключения от 17.11.2020, оформленного органом по сертификации ФАУ «ГНИИИ ПТЗИ ФСТЭК России».

Заявитель: АО «АЛТЭКС-СОФТ»
Адрес: 141067, Московская обл., г. Королев, мкр-н Болшево, ул. Маяковского, д. 10А, пом. VII
Телефон: (495) 543-3101

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ

В.Лютиков

Применение сертифицированной продукции, указанной в настоящем сертификате соответствия, на объектах (объектах информатизации) разрешается при наличии сведений о ней в государственном реестре средств защиты информации по требованиям безопасности информации

Система сертифицирована на территории Республики Беларусь и имеет сертификат соответствия № BY/112 02.02. 036 01130 от 05.06.2020.

НАЦИОНАЛЬНАЯ СИСТЕМА ПОДТВЕРЖДЕНИЯ СООТВЕТСТВИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Аккредитованный орган по сертификации
средств защиты информации и продукции по требованиям безопасности информации
Оперативно-аналитический центр при Президенте Республики Беларусь
Республика Беларусь, 220030, г. Минск, ул. Кирова, 49, т. 309-24-24
(аттестат аккредитации № BY/112 036.01, дата регистрации 15.10.1997 г.)

СЕРТИФИКАТ СООТВЕТСТВИЯ

TP BY

Зарегистрирован в реестре **№ BY/112 02.02. 036 01130**

Дата регистрации **5 июня 2020 г.**

Настоящий сертификат соответствия удостоверяет, что идентифицированная должным образом продукция, изготовленная акционерным обществом «АЛТЭКС-СОФТ», Российская Федерация, 141067, Московская область, г.Королев, мкр-н Болшево, ул.Маяковского, д.10А, пом.VII

и представленная на сертификацию под наименованием Программный комплекс «Средство анализа защищенности RedCheck» версии 2, партия продукции 50 (пятьдесят) шт. (s/n R3000-R3049, акт от 18.09.2019 № 1809)

код ОКП РБ – 62.01.29
код ТН ВЭД ЕАЭС – 8523494500

соответствует требованиям: технического регламента ТР 2013/027/BY (СТБ 34.101.1-2014, СТБ 34.101.2-2014, СТБ 34.101.3-2014 (номенклатура показателей указана в разделе 9 документа «Программный комплекс «Средство анализа защищенности RedCheck» версии 2. Задание по безопасности. ЗБ.ПК RedCheck_2-2019»)).

Заявитель (изготовитель, продавец) акционерное общество «АЛТЭКС-СОФТ», Российская Федерация, 141067, Московская область, г.Королев, мкр-н Болшево, ул.Маяковского, д.10А, пом.VII.

Сертификат соответствия выдан на основании: протокола оценки от 09.08.2019 № 22/19 испытательной лаборатории закрытого акционерного общества «БЕЛТИМ СБ», аттестат аккредитации BY/112 2.4941 срок действия с 28.07.2017 по 28.07.2022, протокола испытаний от 15.05.2020 № ПИ 011/2020 испытательной лаборатории общества с ограниченной ответственностью «Некст Нетворк», аттестат аккредитации BY/112 1.1798 срок действия с 02.06.2017 по 23.09.2021.

Особые отметки Продукцию не допускается использовать в информационных системах класса 1 согласно СТБ 34.101.30-2017.

Дополнительная информация Контрольные характеристики файлов в соответствии с Приложением.

Заместитель начальника Центра С.В.Жерносек

Эксперт-аудитор Д.Н.Вяткин

№ 0248993

1.2 Репозиторий OVALdb

Информационной базой Системы является Репозиторий проблем безопасности OVALdb (далее – Репозиторий, OVALdb), разработанный и сопровождаемый АО «АЛТЭКС-СОФТ».

Репозиторий OVALdb является открытым и размещен на сайте https://ovaldbru.altx-soft.ru.

Информация в Репозитории представлена на основе языков и классификаторов, входящих в Протокол Автоматизации Контента Безопасности (SCAP, Security Content Automation Protocol). Определения уязвимостей выполнены на языке OVAL (Open Vulnerability and Assessment Language).

Кроме контента, разработанного компанией АЛТЭКС-СОФТ, его содержание синхронизировано с экспертными ресурсами, такими как БДУ ФСТЭК России, НКЦКИ, бюллетени производителей и ряд других международных экспертных справочников. Периодичность публикации новых определений составляет 2-3 дня в соответствии с публикациями экспертных ресурсов и производителей. В случае обнаружения критической и распространенной уязвимости, информация в репозитории появляется в тот же день.

Информация является общедоступной и может свободно использоваться любым заинтересованным частным или юридическим лицом в исследовательских или собственных целях, исключая коммерческое использование, в том числе встраивание в виде компонентов в другие программные продукты.

Обнаружение хостов

RedCheck выполняет поиск активных хостов и контроль целостности сети по заданному пулу сетевых адресов. Для обнаруженных в сети хостов определяется их IP-адрес, DNS, FQDN, NetBIOS, тип операционной системы. Также имеется возможность определить наличие агента RedCheck. По результатам выполнения задания впервые выявленные хосты могут быть импортированы в одну из существующих групп Системы, или экспортированы во внешний файл.

Сканирование выполняется без привилегий в режиме Черного ящика.

Аудит в режиме «Пентест»

В рамках данного аудита RedCheck позволяет выполнить сетевое сканирование без привилегий в режиме Черного ящика. Аудит в режиме «Пентест» может выполнить следующие типы сканирований в рамках одного задания:

- Сканирование портов — проведение сетевой инвентаризации без привилегий для опубликованных служб каждого хоста, выявление ПО и его версии;
- Поиск уязвимостей — проведение аудита уязвимостей без привилегий с выполнением дополнительных скриптов для выявленного по итогам сетевой инвентаризации ПО.
- Подбор паролей — выполнение подбора паролей на основе указанных словарей для требуемых сетевых служб.

Аудит уязвимостей

RedCheck выполняет централизованное сетевое или локальное сканирование хостов на наличие уязвимостей ОС, общесистемного и прикладного ПО, а также сетевого оборудования. Сканирование выполняется либо с использованием агента RedCheck, либо на основе безагентной технологии с использованием привилегированных учетных записей (Белый ящик). Во время сканирования сопоставляется состояние параметров системы сигнатурам уязвимостей, содержащихся в открытом Репозитории OVALdb и описанных в формате SCAP.

Аудит обновлений

RedCheck позволяет обнаружить неустановленные обновления безопасности на узлах сети и сформировать необходимые ссылки для загрузки недостающих обновлений. Объектами аудита являются актуальные клиентские и серверные Windows и Linux операционные системы, а также широкий перечень другого общесистемного и прикладного ПО или сетевого оборудования (1.9 Перечень

поддерживаемых платформ). Результат аудита обновлений содержит: наименования обновлений, сведения о рисках, связанных с отсутствием недостающего обновления на узле сети, ссылку на производителя, заявившего о выходе обновления, ссылку на репозиторий (базу), где хранятся доступные для загрузки обновления.

Сканирование выполняется либо с использованием агента RedCheck, либо на основе безагентной технологии с использованием привилегированных учетных записей (Белый ящик).

В RedCheck реализован механизм управления обновлениями совместно со службой WSUS.

Аудит конфигураций

RedCheck позволяет автоматизировать процесс контроля параметров безопасности и осуществлять оценку соответствия информационных систем, ее отдельных компонентов или хостов, стандартам, политикам безопасности, рекомендациям вендоров или другим «признанным практикам» (best practices). RedCheck содержит большое количество готовых конфигураций, разработанных на основе требований международных стандартов и рекомендаций. Поддержка стандартизованного формата SCAP позволяет пользователям загружать сторонние конфигурации, или использовать собственные.

Сканирование выполняется либо с использованием агента RedCheck, либо на основе безагентной технологии с использованием привилегированных учетных записей (Белый ящик).

Инвентаризация

RedCheck позволяет получать детальную информацию об аппаратных и программных средствах сканируемых хостов, включая: типы и описание оборудования, версии и редакции операционных систем, установленные пакеты обновлений и исправлений, установленное ПО, запущенные службы, пользователей и групп, сведения об общих папках. Глубокая детализация отчетов и использование функции Контроль позволяет отслеживать самые незначительные изменения в составе программного и аппаратного обеспечения сети. Реализована возможность инвентаризации образов Docker.

Сканирование выполняется либо с использованием агента RedCheck, либо на основе безагентной технологии с использованием привилегированных учетных записей (Белый ящик).

Фиксация (контроль целостности)

RedCheck может обнаружить и оповестить о несанкционированных изменениях целостности в конфигурационных файлах, папках, ветках реестра (автозагрузка, файл hosts, файл конфигурации межсетевого экрана). Включение режима Контроль позволяет с заданной периодичностью осуществлять проверку целостности эталонных файлов.

Контроль целостности папок и файлов осуществляется по выбранной маске наименования методом контрольного суммирования по алгоритмам MD5, SHA1, SHA256, SHA512, ГОСТ 34.11-2012.

Сканирование выполняется либо с использованием агента RedCheck, либо на основе безагентной технологии с использованием привилегированных учетных записей (Белый ящик).

Аудит СУБД

Функция Аудит СУБД в RedCheck предназначена для проверки соответствия параметров конфигурации или политике безопасности, например:

- требованию к парольной политике;
- требованию к методам аутентификации;
- требованию к разграничению доступа БД;
- требованию к резервному копированию и восстановлению БД.

Сканирование выполняется либо с использованием агентов RedCheck, либо на основе безагентной технологии с использованием привилегированных учетных записей (Белый ящик).

Аудит систем контейнеризации

RedCheck позволяет проводить комплексный аудит безопасности для образов и контейнеров, реализованных на базе платформы контейнеризации Docker, а также системы оркестрации и масштабирования Kubernetes. В рамках данной функции доступны проверки на уязвимости, критичные неустановленные обновления безопасности, неверные настройки параметров конфигураций, инвентаризация, фиксация и контроль целостности. В рамках штатных функциональных возможностей доступна отдельная задача проверки уязвимостей файлов-образов Docker с учетом архитектуры слоев.

Сканирование выполняется либо с использованием агента RedCheck, либо на основе безагентной технологии с использованием привилегированных учетных записей (Белый ящик).

Аудит уязвимостей АСУ ТП

Аудит уязвимостей АСУ ТП предназначен для проведения проверок на наличие уязвимостей протоколов АСУ ТП.

Выявление уязвимостей проводится путем сопоставления сигнатур, хранящихся в БД RedCheck, с идентификационными сведениями о запущенном и опубликованном на сканируемом хосте ПО.

Сканирование выполняется на сетевом уровне, без использования привилегий или учетных записей (Черный ящик).

Проверка доступности

RedCheck обладает возможностью проверки доступности добавленных хостов для любых системных режимов сканирования с привилегиями **(**Белый ящик), учитывая настроенные транспорты/протоколы доступа и учетные записи RedCheck для сканирования.

Результатом выполнения задания является информация о доступности хоста для выполнения сканирования с привилегиями (Белый ящик), либо конкретный отсутствующий параметр настройки.

Сканирование выполняется в комбинированном режиме на сетевом уровне, без использования привилегий (Черный ящик) и с использованием привилегий (Белый ящик).

Задания могут выполняться как по расписанию, так и по требованию.

Документирование результатов аудита (Отчеты)

Функция Документирование результатов аудита позволяет по итогу проверок сформировать отчет в Системе и сохранить его в файл формата HTML, PDF, MHT, CSV или XML.

Система позволяет осуществлять отправку отчетов по электронной почте, а также экспортировать результаты проверок в программы сторонних организаций.

Функция Контроль

Данная опция позволяет выбрать результат сканирования необходимого задания для сравнения с последующими результатами того же задания (эталон). Контроль работает с заданиями Аудит уязвимостей и обновлений, Аудит конфигураций, Инвентаризация и Фиксация. Сравнение новых отчетов с эталоном позволяет увидеть произошедшие изменения на хосте.

1.4 Ролевая модель RedCheck

В RedCheck для разграничения прав доступа реализована ролевая модель. Пользователями Системы могут быть доменные и локальные учетные записи ОС, а также локальные пользователи RedCheck (5.1 Настройка ролевой модели). Роль пользователя в Системе определяется его принадлежностью к одной из четырех групп безопасности RedCheck:

- **REDCHECK_ADMINS** – Суперпользователь;
- **REDCHECK_ADMINIS** – Администратор ИБ;
- **REDCHECK_SYSTEMS** – Системный Администратор;
- **REDCHECK_USERS** – Пользователь ИБ.

Перечень возможностей ролей пользователей RedCheck

Название роли	Администратор ИБ
Суперпользователь	• Обладает всеми возможностями в рамках работы с консолью управления RedCheck
Администратор ИБ	• Управление хостами; • Управление группами; • Просмотр учетных записей; • Управление заданиями; • Просмотр и удаление результатов сканирования; • Управление функцией Контроль для выполненного задания • Управление отчетами; • Управление профилями для Аудита уязвимостей / конфигураций; • Управление шаблонами отчетов (менеджер шаблонов недоступен); • Управление пользователями для работы с RedCheck • Добавление и удаление доп. служб сканирования (доступно только в редакции Enterprise) • Запуск синхронизации и импортирование OVAL-сигнатур; • Просмотр журнала событий и справки о программе;

Системный администратор	• Управление хостами; • Управление группами; • Управление учетными записями; • Просмотр результатов сканирования; • Просмотр работы функции Контроль для отчета выполненного задания • Просмотр отчетов; • Управление профилями для Аудита уязвимостей / конфигураций (допустимо удаление только пользовательских профилей); • Управление шаблонами отчетов (менеджер шаблонов доступен); • Изменять настройки RedCheck; • Просмотр журнала событий и справки о программе;
Пользователь ИБ	• Просмотр хостов; • Просмотр групп; • Просмотр и запуск заданий; • Просмотр результатов сканирования; • Просмотр работы функции Контроль для отчета выполненного задания • Просмотр отчетов; • Просмотр профилей для Аудита уязвимостей / конфигураций; • Просмотр справки о программе;

1.5 Отличия между версиями RedCheck

Desktop – дистрибутив, способный выполнять задачи, требующие больших аппаратных мощностей, но обладающий меньшими возможностями в сравнении с Web-версией RedCheck. Все компоненты Системы устанавливаются и функционируют на одном устройстве.

Web - дистрибутив, основанный на клиент-серверной архитектуре, за счет чего уменьшается аппаратная нагрузка. Развертывание Web-версии подразумевает установку обязательных компонентов RedCheck с помощью отдельных инсталляторов на один сервер, или несколько (физических или виртуальных). Работа с Системой происходит в интерфейсе Web-консоли управления через веб-браузер, поддерживаемый программой.

Web-версия является рекомендуемым вариантом использования RedCheck для редакций **Professional** и обязательным для **Enterprise**, так как обеспечивает лучшую безопасность, удобство эксплуатации, включая многопользовательский доступ, и производительность при работе с большим набором данных.

Функционал, отсутствующий в Desktop-версии RedCheck
Отправка отчетов на сетевой ресурс
Отдельный менеджер шаблонов отчетов (в Desktop виден только список созданных шаблонов)
Функция отображения всех пользователей из групп REDCHECK в домене
В Web есть локальные пользователи, в Desktop есть возможность входа по одной паре логин/пароль (помимо доменных пользователей)
Сообщение, что добавляемый хост уже существует
В пункте **Справка** → **О программе** нет информации об удаленных службах сканирования и синхронизации
Возможность совместной работы нескольких учетных записей одновременно
Автоматическая генерация и отправка отчетов на e-mail
Задания Аудит Docker и Обнаружение хостов

В Desktop может быть только по одной службе сканирования и синхронизации

Начиная с версии RedCheck 2.6.9 возможна только раздельная установка Desktop или Web версии. Если используется Desktop, то установка Web невозможна, и наоборот.

1.6 Редакции RedCheck

RedCheck доступен в четырех редакциях:

Base – предоставляет необходимые инструменты для аудита уязвимостей и обновлений Windows и Linux систем при повседневном контроле защищённости ИС.

Professional – включает в себя основной набор возможностей Системы для мониторинга и управления защищённостью сетей корпоративного уровня.

Expert – включает все функции и сканируемые платформы, позволяет проводить комплексный аудит безопасности образов на базе платформы контейнеризации Docker и системы оркестрации Kubernetes.

Enterprise – обладает всеми имеющимися функциональными возможностями Системы. Редакция ориентирована на крупные и распределённые ИС и обладает возможностью подключения дополнительных модулей сканирования.

Функциональные возможности	Base	Professional	Expert	Enterprise
ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ				
Обнаружение хостов	+	+	+	+
Аудит в режиме «Пентест»	+	+	+	+
Аудит уязвимостей	+	+	+	+
Аудит обновлений	+	+	+	+
Аудит конфигураций	–	+	+	+
Инвентаризация	+	+	+	+
Фиксация и контроль	+	+	+	+

Аудит СУБД	–	+	+	+
Аудит уязвимостей АСУ ТП	–	за дополнительную плату		
Аудит уязвимостей образов Docker	–	–	+	+
Проверка доступности	+	+	+	+
Отчеты по результатам аудитов	+	+	+	+
ОБЪЕКТЫ СКАНИРОВАНИЯ				
ОС Windows и Linux	+	+	+	+
Сетевое оборудование	–	+	+	+
Протоколы АСУ ТП	–	за дополнительную плату		
Средства виртуализации	–	–	+	+
Средства контейнеризации и оркестрации	–	–	+	+
СУБД	–	+	+	+
ДОПОЛНИТЕЛЬНЫЙ СЕРВИС				
Сертифицированная версия Системы	+	+	+	+
Адаптация конфигураций	за дополнительную плату			+
Разработка индивидуальных конфигураций безопасности	–	за дополнительную плату		
Расширенная поддержка	за дополнительную плату			+

АРХИТЕКТУРА И МАСШТАБИРУЕМОСТЬ				
Подключение дополнительных служб сканирования (лицензируются отдельно)	–	–	+	+
Многопоточное сканирование Windows-систем	+	+	+	+
Многопоточное сканирование «Пентест»	+	+	+	+
Возможность интеграции с помощью RestAPI	–	+	+	+
Web-консоль управления	–	+	+	+

Информация о версии и установленных службах программы, а также об ограничениях использующейся редакции RedCheck, находится в пункте **Справка** → **О программе**.

1.7 Лицензирование

Система лицензируется:

- Редакции Base, Professional и Expert по количеству IP (FQDN) – адресов, добавленных в качестве активов (хостов) в RedCheck;
- Редакция Enterprise включает один сервер сканирования (с возможностью подключения дополнительных) и все основные компоненты RedCheck, без ограничения количества сканируемых хостов. Дополнительные модули сканирования RedCheck, модуль сканирования АСУ ТП и Сервер обновлений RedCheck приобретаются отдельно.

Модуль сканирования АСУ ТП лицензируется по количеству хостов с протоколами АСУ ТП.

Срок действия лицензии составляет 1-3 года, возможно приобретение RedCheck на 2 года или более. В период действия лицензии пользователю RedCheck бесплатно предоставляется базовая техническая поддержка, доступ к актуальному контенту безопасности и обновления версий RedCheck.

Сведения об актуальных лицензиях на СА3 RedCheck и ценах приведены в официальном прайс-листе, опубликованном сайте продукта https://www.redcheck.ru и официальном сайте компании

ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ С КОНЕЧНЫМ ПОЛЬЗОВАТЕЛЕМ REDCHECK (EULA)

1.8 Как получить тестовую версию?

Для приобретения лицензии RedCheck необходимо обратиться в отдел продаж АО «АЛТЭКС-СОФТ» в свободной форме – sales@altx-soft.ru или к партнерам в вашем регионе - https://www.altx-soft.ru/company/partner_net/

Чтобы получить тестовую версию RedCheck, необходимо:

Шаг 1. Перейти на сайт RedCheck → Скачать тестовую версию.

Шаг 2. Через форму обратной связи заполнить обязательные поля для выдачи тестовой лицензии.

Шаг 3. В течение рабочего дня на электронную почту, указанную при запросе, будет отправлено сообщение с тестовым лицензионным ключом и краткой инструкцией по использованию.

RedCheck доступен в следующих версиях:

- Сертифицированная ФСТЭК России версия (для других государств могут быть доступны сертифицированные версии по требованиям собственного регулятора, информацию о доступности можно получить у соответствующего дистрибьютора);
- Несертифицированная старшая версия (обладает новыми функциями и находится на сертификации).

Сертифицированная ФСТЭК России версия RedCheck поставляется в течении 5-10 рабочих дней. В поставку входят:

- сертифицированная версия дистрибутива на USB-носителе;
- лицензия на бланке с уникальным ключом;
- комплект сопроводительной и эксплуатационной документации (на USB-носителе);
- копия Сертификата соответствия ФСТЭК России;
- абонемент на расширенную техническую поддержку (при заказе).

При необходимости обновления контента ИБ в офлайн режиме используется пара логин/пароль для доступа к Центру сертифицированных обновлений.

Несертифицированная версия RedCheck поставляется в электронном виде в течении 1-3 рабочих дней. В поставку входят:

- лицензия/ии на бланке с уникальным ключом (электронно, pdf);
- абонемент на расширенную техническую поддержку (при заказе, электронно).

1.9 Перечень поддерживаемых платформ

Microsoft Windows

- XP / XP Embedded / Vista / 7 / 8/ 8.1 / 10 / 11
- Server 2003 / 2008 / 2008 R2 / 2012 / 2012 R2 / 2016 / 2019 / 2022

Linux

- AlmaLinux 8.x / 9.x
- Amazon Linux 2 / AMI / 2023
- CentOS Linux 5 / 6 / 7 / 8
- CentOS Stream 8 / 9
- Debian 6.0 / 7 / 8 / 9 / 10 / 11 / 12
- Debian GNU/Linux 2.2 / 3.0 / 3.1 / 4.0 / 5.0 / 6.0 / 7
- FreeBSD 10 / 11 / 12
- Linux Mint 17 / 18 / 19 / 20
- Mageia 4 / 5 / 6 / 7 / 8 / 9
- openSUSE 10.2 / 10.3 / 11.0 / 11.1 / 11.2 / 11.3 / 11.4 / 12.1 / 12.2 / 12.3 / 13.1 / 13.2
- openSUSE Leap 15.0 / 15.1 / 15.3 / 15.4 / 42.1 / 42.2 / 42.3
- Oracle Solaris 10 / 11 / 11.1 / 11.2 / 11.3 / 11.4
- Oracle Linux 4 / 5 / 6 / 7 / 8 / 9
- Red Hat Enterprise Linux 3 / 4 / 5 / 6.x / 7.x / 8.x / 9.x
- Rocky Linux 8 / 9
- Solaris 10 / 11
- SUSE CaaS Platform 3 / 4
- SUSE Linux Enterprise Desktop 10 / 11 / 12 / 15
- SUSE Linux Enterprise Server 10 / 11 / 12 / 15
- SUSE Linux Enterprise Server for SAP 11 / 12 / 15
- SUSE Linux Enterprise Point of Service 11
- SUSE Linux Enterprise Real Time 11 / 15
- SUSE Linux Enterprise High Performance Computing 15
- Ubuntu 4.10 / 5.04 / 5.10 / 6.06 / 6.10 / 7.04 / 7.10 / 8.04 / 8.10 / 9.04 / 9.10 / 10.04 / 10.10 / 11.04 / 11.10 / 12.04 / 12.10 / 13.04 / 13.10 / 14.04 / 14.10 / 15.04 / 15.10 / 16.04 / 16.10 / 17.04 / 17.10 / 18.04 / 18.10 / 19.04 / 19.10 / 20.04 / 20.10 / 21.04 / 21.10 / 22.04 / 22.10 / 23.04 / 23.10

Отечественные ОС

- ALT Linux SPT 6 / 7
- ALT 8 SP / 10 SP
- ALT 9 / 10
- Astra Linux CE Орёл 2.12
- Astra Linux SE 1.5 / 1.6 / 1.7 Орел / Воронеж / Смоленск
- RED OS MUROM 7.1 / 7.2 / 7.3
- ROSA DX COBALT 1.0
- ROSA SX COBALT 1.0
- ROSA Cobalt 7.9
- ROSA Enterprise Linux Desktop 7.3
- ROSA Enterprise Linux Server 7.3

Сетевое оборудование

- Check Point GAiA
- Cisco IOS
- Cisco NX-OS
- FortiGate FortiOS 5.0 и выше
- Huawei VRP
- UserGate UTM 6.1.0.10123F / 6.1.5.11134R и выше

Виртуализация

- Microsoft Hyper-V Server 2008 / Hyper-V Server 2008 R2 / Hyper-V Server 2012 / Hyper-V Server 2012 R2
- как роль Windows Server 2008 / Windows Server 2008R2 / Windows Server 2012 / Windows Server 2012 R2
- ROSA Virtualization 2.1
- VMware ESXi Server 5.0 / 5.1 / 5.5 / 6.0 / 6.5 / 6.7 / 7
- VMware vCenter Server 5.1 / 5.5 / 6.0 / 6.5 / 6.7 / 7
- VMware NSX
- VMware Photon OS 1.0 / 2.0 / 3.0 / 4.0

СУБД

- IBM Db2
- Microsoft SQL Server 2005 / 2008 / 2008 R2 / 2012 / 2014 / 2016 / 2017 / 2019 / 2022
- MySQL Server 4.1 / 5.0 / 5.1 / 5.5 / 5.6 / 5.7 / 6.0 / 8.0 / 8.1 / 8.2
- Oracle Database Server 11 / 12 / 18 / 19
- PostgreSQL 8 / 9 / 10 / 11 / 12 / 13 / 14 / 15 / 16
- SAP HANA

АСУ ТП

- Citect SCADA
- Iconics GENESIS (32/64)
- IGSS
- Siemens Automation License Manager
- Siemens SICAM PAS
- Siemens Simatic WinCC
- Siemens Simatic WinCC flexible
- Siemens STEP7
- Wonderware InTouch

ПЛК

- ПЛК Advantech APAX-xxxxKW, ADAM-xxxxKW
- ПЛК Omron
- ПЛК Rockwell Automation
- ПЛК Siemens Simatic S7
- ПЛК Schneider Electric Modicon
- ПЛК Yokogawa FCN

Контейнеризация

- Docker 1.13.0 и выше (Storage Driver overlay2)
- Kubernetes 1.18 / 1.19 / 1.20 / 1.21 / 1.22 / 1.23 / 1.24

[1]*RedCheck не поддерживает сканирование Windows XP при помощи WinRm-туннеля;*

[2]*Для Windows Server 2019 не применим функционал PatchManagment;*

[3]*Для VMware ESXi 7, отсутствует возможность проведения задания "Аудит конфигураций";*

Полный перечень поддерживаемого ПО доступен по ссылке.

В Таблицах 1-3 представлены возможные режимы сканирования для соответствующих типов заданий.

Таблица 1 Операционные системы

Цели сканирований/Типы заданий	Windows	Linux	FreeBSD	Solaris
Аудит уязвимостей	A/AL/RE	AL	AL	AL
Аудит обновлений	A/AL/RE	AL	NA	NA
Аудит конфигураций	A/RE	AL	NA	AL
Инвентаризация	A/AL/RE	AL	NA	NA
Фиксация	A/RE	AL	NA	NA
Аудит в режиме Пентест	BB	BB	BB	BB

Таблица 2 Сетевое оборудование

Цели сканирований/Типы заданий	Huawei	Check Point	Cisco	FortiOS	UserGate
Аудит уязвимостей	NA	AL	AL	AL	AL
Аудит обновлений	NA	NA	NA	NA	NA

Аудит конфигураций	AL	AL	AL	AL	AL
Инвентаризация	NA	AL	AL	AL	AL
Фиксация	NA	NA	NA	NA	NA
Пентест	BB	BB	BB	BB	BB

Таблица 3 Системы виртуализации и контейнеризации

Цели сканирований/Типы заданий	VMWare	Docker
Аудит уязвимостей	AL	AL
Аудит обновлений	AL	NA
Аудит конфигураций	AL	AL
Инвентаризация	AL	AL
Фиксация	NA	NA
Аудит в режиме Пентест	BB	BB

Условные обозначения

«A» – агент;

«AL» – безагент (WMI, SSH);

«RE» – безагент (WinRM);

«NA» – режим сканирования и тип задания не применимы;

«BB» – аудит методом черного ящика.

1.10 Перечень интегрируемых систем

RedCheck имеет действующие интеграции со следующими SIEM-системами:

- Kaspersky KUMA (официальный сайт);
- Neurodat SIEM (сайт на реконструкции);
- R-Vision (официальный сайт);
- Security Vision; (официальный сайт)

Инструкцию по интеграции и конфигурации можно найти на сайте разработчика SIEM-системы или при обращении к ним в техническую поддержку.

1.11 Служба технической поддержки

Технические вопросы, связанные с использованием сканера безопасности RedCheck, можно задать нашей службе технической поддержки удобным для Вас способом:

- Web-портал: portal.altx-soft.ru
- Электронная почта: support@altx-soft.ru
- Web-сайт продукта: redcheck.ru

При обращении в службу технической поддержки необходимо указать:

- номер лицензии;
- номер купона для расширенной технической поддержки;
- наименование представляемой организации;
- прикрепить полные скриншоты окна консоли, где зафиксирована проблема и описать действия, которые приводят к такому результату
- в случае ошибок в работе Системы, прикрепить файл журнала событий соответствующей службы, в котором зафиксирована проблема.

С Регламентом оказания технической поддержки можно ознакомиться на сайте производителя.

Дистрибутив имеет модульную структуру, каждый модуль является функциональным компонентом, устанавливаемым в соответствии с выбранной архитектурой и производительностью Системы.

Каждый модуль имеет отдельный инсталляционный пакет. Структура названия установочного файла:

RedCheck-X.X.X.XXXX.msi

1 2 3

- аббревиатура компонента;
- цифровое обозначение версии модуля;
- номер сборки.

Состав дистрибутива СА3 RedCheck, версия 2.6.9

Перечень обязательных компонентов RedCheck, подлежащих установке, зависит от выбранной версии RedCheck: Desktop или Web.

Наименование файла	Наименование дистрибутива	Назначение	Редакция
Desktop-версия (Обязательные компоненты)			
RedCheck-2.6.9.XXXX.msi	СА3 RedCheck Desktop	Включает полный набор компонентов для Desktop версии сканера. В процессе установки создает новую БД программы (требуется отдельная установка СУБД) или обеспечивает настройки подключения к существующей БД (при переустановке	Base Professional

		программы)	
Web-версия (Обязательные компоненты)			
RedCheck.WebRest-x64-2.6.9.XXXX.msi	Серверный компонент (REST API)	Основной модуль взаимодействия с БД RedCheck. Создает новую БД программы или обеспечивает подключение к существующей БД (при переустановке программы). Реализует взаимодействие компонентов RedCheck между БД и другими модулями, а также предоставляет возможность интеграции с внешними системами	Professional Expert Enterprise
RedCheck.WebClient-x64-2.6.9.XXXX.msi	Web-консоль управления	Представляет собой приложение для Web-сервера и позволяет администраторам выполнять подключение к консоли с помощью веб-браузера. Обеспечивает взаимодействие пользователя с REST API сервером	Professional Expert Enterprise

RedCheckScanService-2.6.9.XXXX.msi	Служба сканирования / Дополнительный модуль сканирования	Основной функциональный компонент web-версии сканера, реализует: - выполнение сканирования; - обработку и представление результатов сканирования Данный инсталляционный пакет используется также при установке Дополнительных модулей сканирования на отдельные сервера и рабочие станции конечной инфраструктуры в случае масштабирования (при наличии дополнительных лицензий на указанный модуль)	Professional Expert Enterprise Дополнительный модуль: Enterprise
RedCheckSyncService-2.6.9.XXXX.msi	Служба синхронизации	Обеспечивает обновление базы решающих правил (определений), активацию и обновление параметров лицензии	Professional Expert Enterprise
Дополнительные компоненты			

RedCheckAgent-2.6.9-x64.XXXX.msi	Агент сканирования для Windows x64	Обеспечивает быстрое и надежное сканирование и передачу данных с хоста, ограниченного политикой ИБ организации	Base Professional Expert Enterprise
RedCheckAgent-2.6.9-x86.XXXX.msi	Агент сканирования для Windows x86		
RedCheckUpdateAgent-2.6.9-x64.XXXX.msi	Агент обновления для Windows x64	Обеспечивает установку обновлений безопасности на хост под управлением Windows	Base Professional Expert Enterprise
RedCheckUpdateAgent-2.6.9-x86.XXXX.msi	Агент обновления для Windows x86		
WsusKit-0.6.8.92.msi	Модуль взаимодействия со WSUS-сервером (Patch-manager)	Надстройка над WSUS-сервером для установки выявленных в результате аудита обновлений	Base Professional Expert Enterprise
RedCheckUpdateServer.msi	Промежуточный сервер обновлений в DMZ (off-line). Лицензируется отдельно.	Используется для обновления базы данных решающих RedCheck в режиме offline (без прямого подключения к сети Интернет) через DMZ-сегмент, в том числе для обновления нескольких экземпляров RedCheck	Base Professional Expert Enterprise

Содержание

3.1 Требования к аппаратному обеспечению

Требования к аппаратным ресурсам, которые необходимы для корректной работы RedCheck:

Компоненты	Платформа	Аппаратные требования
Desktop версия		
RedCheck	ПЭВМ	ЦП не ниже Intel Core i5, частота не ниже 3,00 ГГц ОЗУ не менее 8 ГБ ПЗУ не менее 12 ГБ
Web-версия (обязательные к установке компоненты Системы)		
Совместная установка		
Серверный компонент Консоль управления Служба сканирования Служба синхронизации	Серверная	ЦП Xeon, частота не ниже 1,86 ГГц, не менее 4 ядер ОЗУ не менее 12 ГБ ПЗУ не менее 2 ГБ
Раздельная установка		
Серверный компонент Консоль управления	Серверная	ЦП Xeon, частота не ниже 1,86 ГГц, не менее 2 ядер ОЗУ не менее 6 ГБ ПЗУ не менее 1 ГБ

Служба сканирования	Серверная	ЦП Xeon, частота не ниже 1,86 ГГц, не менее 2 ядер ОЗУ не менее 6 ГБ ПЗУ не менее 1 ГБ
Служба синхронизации	Серверная	ЦП Xeon, частота не ниже 1,86 ГГц,не менее 2 ядер ОЗУ не менее 4 ГБ ПЗУ не менее 1 ГБ
Сервер СУБД[1]	Серверная	ЦП Xeon, частота не ниже 1,86 ГГц, не менее 2 ядер ОЗУ не менее 6 ГБ ПЗУ не менее 10 ГБ (рекомендации по расчету объема БД приведены ниже)
Дополнительные компоненты		
Дополнительный модуль сканирования	Серверная	ЦП Xeon, частота не ниже 1,86 ГГц, не менее 2 ядер ОЗУ не менее 6 ГБ ПЗУ не менее 1 ГБ

RedCheck Agent	ПЭВМ, Серверная	ЦП не ниже Intel Pentium/ AMD Phenom, частота не ниже 2,00 ГГц ОЗУ не менее 2 ГБ ПЗУ не менее 500 МБ
RedCheck Update Agent	ПЭВМ, Серверная	ЦП не ниже Intel Pentium/ AMD Phenom, частота не ниже 2,00 ГГц ОЗУ не менее 2 ГБ ПЗУ не менее 500 МБ
WSUSkit (Patch-manager)	ПЭВМ, Серверная	ЦП не ниже Intel Pentium/ AMD Phenom, частота не ниже 2,00 ГГц ОЗУ не менее 2 ГБ ПЗУ не менее 500 МБ
RedCheck Update Server (офлайн-синхронизация)	Серверная	ЦП Xeon, частота не ниже 1,86 ГГц, не менее 2 ядер ОЗУ не менее 6 ГБ ПЗУ не менее 5 ГБ

Требования к объему HDD представлены без учета размещения на ЭВМ операционных систем, СУБД и другого системного и прикладного ПО.

[1] - *В случае размещения сервера СУБД совместно с компонентами RedCheck аппаратные требования складываются.*

Значения в таблице являются рекомендуемыми, реальное потребление может отличаться в зависимости от сценариев использования Системы. Рекомендуется выполнять мониторинг потребления CPU и памяти на хостах для оптимизации потребления ресурсов.

Выделяемый объем HDD на сервере БД предназначен для хранения контента ИБ и результатов сканирования. При определении необходимого объема HDD следует учитывать следующие факторы:

- количество сканируемых хостов + количество типов аудитов для каждого хоста;
- частота проводимых сканирований;
- период хранения результатов сканирования в БД.

Ориентировочно необходимый объем HDD (для одного типа аудита) можно определить по следующей формуле:

VHDD ≈ Vcp NT

где VHDD – необходимый объем HDD, ГБ; Vcp – средний объем результатов сканирования одного хоста,
Vcp ≈ 2 МБ; N – количество сканируемых хостов, ед.
T – период хранения результатов сканирования в БД, нед.

Так, для хранения результатов еженедельного сканирования 100 хостов в течение полугода, необходимо выделить 0,002*100*26 = 5,2 ГБ свободного дискового пространства.

Значения выделяемого объема HDD на сервере БД в зависимости от количества сканируемых хостов (для одного типа аудита) представлены в таблице.

Количество сканируемых хостов	Частота сканирования	HDD*, ГБ
Не более 200	1 раз в квартал	3
	1 раз в месяц	6
	1 раз в неделю	22
От 200 до 500	1 раз в квартал	5
	1 раз в месяц	13
	1 раз в неделю	53
От 500 до 2000	1 раз в квартал	20
	1 раз в месяц	52
	1 раз в неделю	212
2000**	1 раз в квартал	35
	1 раз в месяц	100
	1 раз в неделю	400

* Значения представлены из условия хранения результатов сканирования в течении одного года.

** Для обеспечения быстродействия и уменьшения временных интервалов выполняемых операций с БД рекомендуется СУБД располагать на SSD. Использование SSD должно применяться совместно с выполнением работ по оптимизации и тонкой настройке СУБД.

3.2 Требования к программному обеспечению

Требования к ПО для корректного функционирования основных серверных компонентов RedCheck:

- ОС:
  - Microsoft Windows 10 и выше;
  - Microsoft Windows Server 2012R2 и выше;
- СУБД:
  - Microsoft SQL Server версия 2014 и выше;
  - PostgreSQL версия 12.5 – 16;
  - Postgres Pro версия 14 / 15;
- Браузеры Google Chrome или Edge;
- Web-сервер IIS;
- Microsoft .NET Framework 4.8 и выше (актуальную версию пакета можно скачать с официального сайта);
- Microsoft Visual C++ 2013 Redistributable (актуальную версию пакета можно скачать с официального сайта, выбрать файл для 32-битной версии: **vcredist_x86.exe**);
- Microsoft Visual C++ 2015 Redistributable (актуальную версию пакета можно скачать с официального сайта, выбрать файл для 32-битной версии: **vc_redist.x86.exe**);
- Microsoft ASP.NET Core Runtime (актуальную версию пакета можно скачать с официального сайта).

Требования к ПО для корректного функционирования агента сканирования и агента обновления:

- ОС:
  - Microsoft Windows 7 и выше;
  - Microsoft Windows Server 2008r2 и выше;
- Microsoft .NET Framework 4.8 и выше (актуальную версию пакета можно скачать с официального сайта).

3.3 Требования к сетевой инфраструктуре

Взаимодействие осуществляется по протоколам стека сетевых протоколов TCP/IP. Инициация сетевых взаимодействий осуществляется Источником с использованием динамических портов, определенных в ОС, для Microsoft Windows используется стандартный диапазон портов 49152-65535, определенный IANA (Internet Assigned Numbers Authority — «Администрация адресного пространства Интернет»).

Все порты назначения могут быть переопределены, кроме обращений к компоненту WSUSkit, безагентного сканирования транспортом WMI и получения обновлений с официального репозитория производителя (Сервис синхронизации - https://sync.altx-soft.ru).

Таблица 1 – перечень сетевых портов взаимодействия компонентов RedCheck

Источник	Назначение	Порт назначения	Прикладной протокол/комментарий
Графическая консоль RedCheck	База данных	1433/TCP	Взаимодействие с базой данных
Графическая консоль RedCheck	Компонент WSUSkit	8737/TCP	Взаимодействие с компонентом управления Microsoft WSUS
Рабочие станции администраторов ИБ	Веб-консоль RedCheck	8080/TCP	HTTP/Взаимодействие с веб-консолью (рекомендуется установить SSL-сертификат и переопределить порт)
Веб-консоль RedCheck	Служба REST RedCheck	8081/TCP	HTTP/Взаимодействие со службой REST RedCheck (рекомендуется установить SSL-сертификат и переопределить порт)

Веб-консоль RedCheck	Сервис DNS	53/TCP	DNS/Запросы в службу разрешения имен
Веб-консоль RedCheck	Сервис Active Directory	88, 135, 389/TCP	LDAP/Взаимодействие с Active Directory при работе службы от имени доменной учетной записи
Служба REST RedCheck	База данных	1433/TCP	Взаимодействие с базой данных
Служба REST RedCheck	Сервис DNS	53/TCP	DNS/Запросы в службу разрешения имен
Служба REST RedCheck	Сервис Active Directory	88, 135, 389/TCP	LDAP/Взаимодействие с Active Directory при работе службы от имени доменной учетной записи
Служба сканирования RedCheck	База данных	1433/TCP	Взаимодействие с базой данных
Служба сканирования RedCheck	Агент RedCheck на сканируемом объекте сети	8732/TCP	Взаимодействие с агентом сканирования RedCheck
Служба сканирования RedCheck	Агент RedCheck Update на сканируемом объекте сети	8733/TCP	Взаимодействие с агентом обновлений RedCheck
Служба сканирования RedCheck	Безагентное сканирование объектов сети	135, 445/TCP	WMI/Безагентное сканирование Microsoft Windows
		5985, 5986/TCP	WinRM/Безагентное сканирование Microsoft

			Windows
		22/TCP	SSH/Безагентное сканирование Linux
		80, 443/TCP	HTTP/HTTPS/Безагентное сканирование объектов с веб-доступом
		1433/TCP	Сканирование баз данных Microsoft SQL Server
		3306/TCP	Сканирование баз данных MySQL
		5432/TCP	Сканирование баз данных Postgres SQL
		1521/TCP	Сканирование баз данных Oracle Database
		50000/TCP	Сканирование баз данных IBM DB2
		39015/TCP	Сканирование баз данных SAP HANA
Служба сканирования RedCheck	Сканирование в режиме «Пентест»	0-65535/UDP-TCP	Сканирование объектов сети в режиме Пентест
Служба сканирования RedCheck	Сетевой каталог	445/TCP	SMB/Взаимодействие с каталогом в сетевом размещении для хранения отчетов о результатах сканирования
Служба сканирования RedCheck	Сервис электронных почтовых	25/TCP	SMTP/Отправка почтовых уведомлений о результатах работы

	сообщений, e-mail		службы
Служба сканирования RedCheck	Сервис DNS	53/TCP	DNS/Запросы в службу разрешения имен
Служба сканирования RedCheck	Сервис Active Directory	88, 135, 389/TCP	LDAP/Взаимодействие с Active Directory при работе службы от имени доменной учетной записи
Служба синхронизации RedCheck	База данных	1433/TCP; 5432/TCP	Взаимодействие с базой данных
Служба синхронизации RedCheck	Сетевой каталог	445/TCP	SMB/Взаимодействие с каталогом обновлений в сетевом размещении с офлайн-контентом
Служба синхронизации RedCheck	Сервер обновлений RedCheck	445/TCP	SMB/Взаимодействие с каталогом обновлений на сервере обновлений RedCheck
Служба синхронизации RedCheck	Прокси-сервер	3128/TCP (порт зависит от службы прокси)	HTTPS/Доступ к сервису синхронизации производителя через прокси-сервер (https://sync.altx-soft.ru)
Служба синхронизации RedCheck NIX	Прокси-сервер	3128/TCP (порт зависит от службы прокси)	HTTPS/Доступ к сервису синхронизации производителя через прокси-сервер (https://syncn.altx-soft.ru)
Служба синхронизации RedCheck	Сервис синхронизации (https://sync.altx-	443/TCP	HTTPS/Доступ к сервису синхронизации производителя

	soft.ru)		(https://sync.altx-soft.ru)
Служба синхронизации RedCheck NIX	Сервис синхронизации (https://syncn.altx-soft.ru)	443/TCP	HTTPS/Доступ к сервису синхронизации производителя (https://syncn.altx-soft.ru)
Служба синхронизации RedCheck	Сервис электронных почтовых сообщений, e-mail	25/TCP	SMTP/Отправка почтовых уведомлений о результатах работы службы
Служба синхронизации RedCheck	Сервис DNS	53/TCP	DNS/Запросы в службу разрешения имен
Служба синхронизации RedCheck	Сервис Active Directory	88, 135, 389/TCP	LDAP/Взаимодействие с Active Directory при работе службы от имени доменной учетной записи

Для обеспечения стабильной работы RedCheck, сетевая инфраструктура организации должна обеспечивать пропускную способность линий передачи, не ниже приведенной в таблице.

	Сканирование посредством WMI	Сканирование посредством SSH	Сканирование в режиме Remote Engine (WinRM)	Сканирование посредством Агента сканирования
Скорость передачи данных, Кбит/с	10 200	160	637	121
Суммарный объем трафика на узел, КБ	434 000	5 000	16 800	8 400

Приведенные в таблице значения рассчитаны для выполнения наиболее ресурсоемкого задания Аудит уязвимостей (полное сканирование).

4 Установка RedCheck

Для установки Redcheck требуется установленная СУБД из списка поддерживаемых программой. Учетная запись, под которой производится инсталляция Системы, должна иметь административные привилегии.

Не рекомендуется устанавливать компоненты RedCheck на контроллер домена Microsoft Active Directory.

Начиная с RedCheck 2.6.9 возможна только раздельная установка Desktop или Web версии. Если используется Desktop, то установка Web невозможна, и наоборот.

Содержание

4.1 Установка СУБД

Установка СУБД производится на выбранном сервере в инфраструктуре, имеющем необходимую сетевую доступность, в соответствии с используемой архитектурой развёртывания.

> Смена СУБД возможна только при переустановке RedCheck.

Содержание

4.1.1 Установка СУБД Microsoft SQL Server

RedCheck работает на всех редакциях (в том числе бесплатных) СУБД Microsoft SQL Server. Поддерживаемые версии указаны в 3.2 Требования к программному обеспечению.

Взаимодействие Системы с СУБД Microsoft SQL Server возможно в режиме доменной или смешанной авторизации.

Под доменной авторизацией здесь и далее понимается авторизация в СУБД посредством доменной учетной записи Active Directory. Под смешанной авторизацией понимается авторизация средствами ОС Microsoft Windows и/или внутренними средствами СУБД Microsoft SQL Server.

В общем случае, если в организации используется единый каталог Active Directory, рекомендуется использовать режим доменной авторизации в целях удобства администрирования и безопасности. Используемый режим авторизации можно задать в процессе установки СУБД и в дальнейшем изменить при необходимости.

В режиме авторизации внутренними средствами СУБД создаются имена входа, которые не основаны на учетных записях единого каталога Active Directory; в указанном режиме имя пользователя и пароль создаются с помощью Microsoft SQL Server и хранятся в СУБД. Режим доменной авторизации отключает проверку авторизации внутренними средствами СУБД Microsoft SQL Server.

Не рекомендуется выполнять установку СУБД на сервере, являющемся контроллером домена.

Далее приводятся инструкции по установке СУБД на примере версии Microsoft SQL Server 2019 Evaluation Edition. Установка СУБД Microsoft SQL Server других версий и редакций производится аналогичным образом.

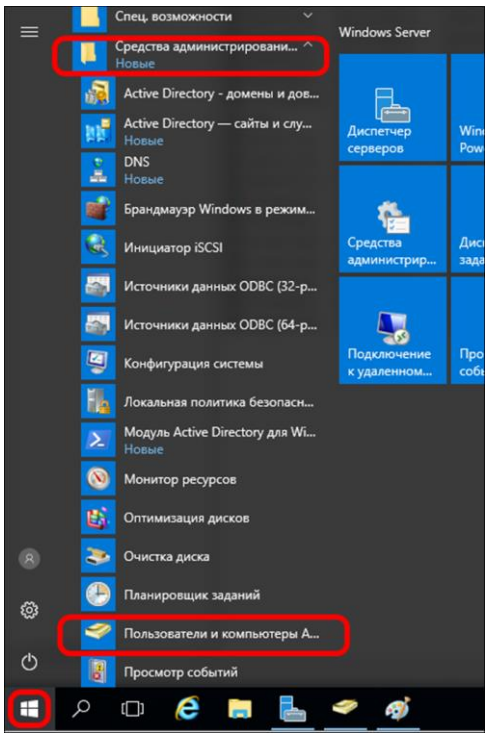
Содержание

4.1.1.1 Установка в режиме доменной авторизации

Для установки и управления СУБД Microsoft SQL Server необходима доменная учётная запись.

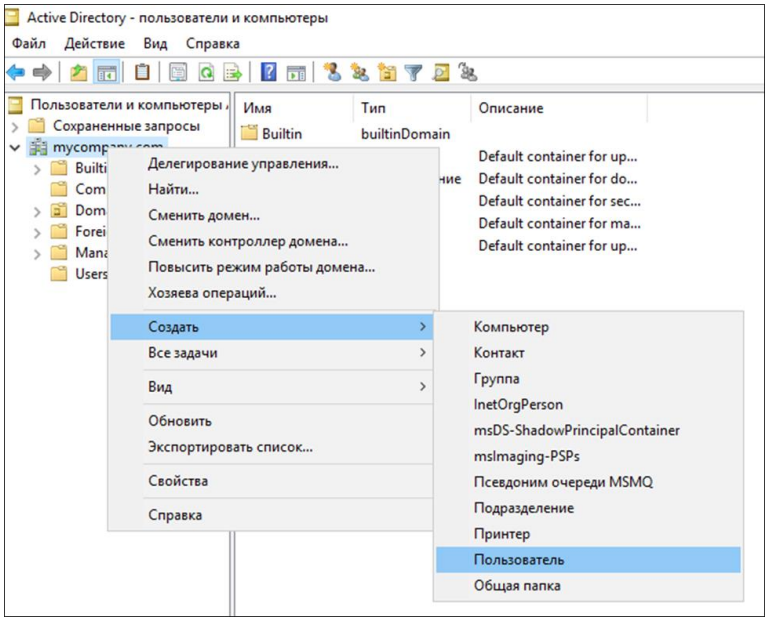
Создание доменной учётной записи для управления СУБД

Шаг 1. Пуск → Средства администрирования → Пользователи и компьютеры Active Directory;

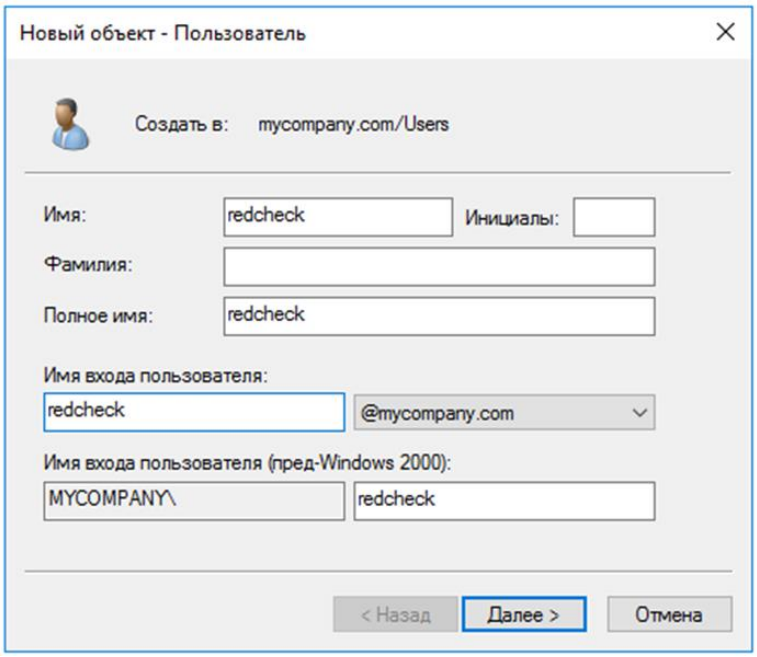


Возможно на управляющем АСУ ТП администратора домена или на сервере БД войти с разрешенной учётной записью, запустить консоль управления MMC от имени доменного администратора и добавить в консоль соответствующую оснастку Пользователи и компьютеры Active Directory).

Шаг 2. Нажмите **Пользователи и компьютеры Active Directory** → ПКМ по названию домена → **Создать** → **Пользователь**;

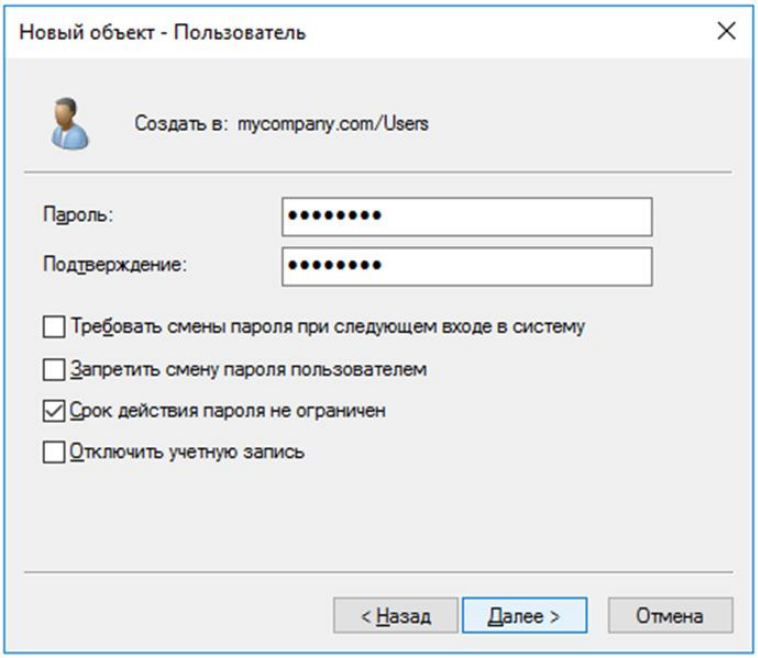


Шаг 3. Укажите имя нового пользователя в полях **Имя**, **Полное имя**, **Имя входа пользователя** (например, **redcheck**) → **Далее**;

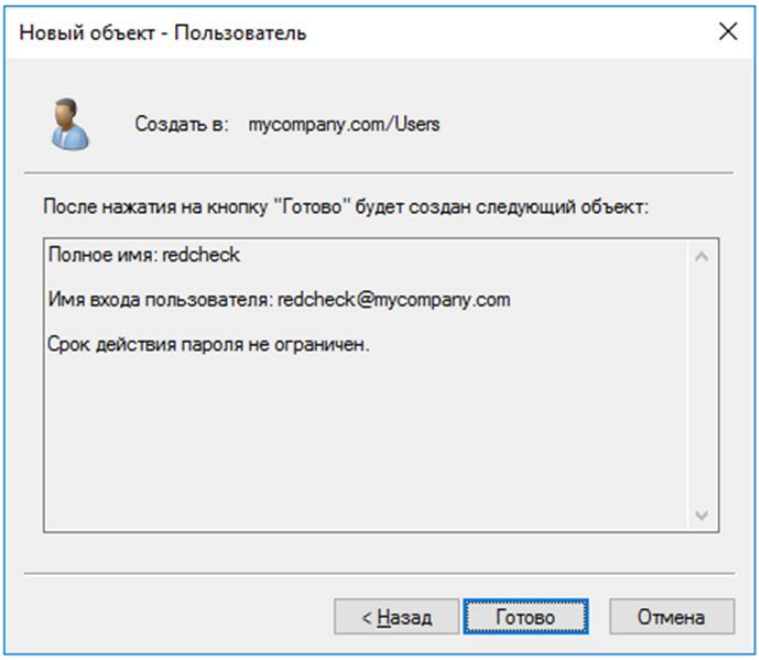


Шаг 4. Задайте пароль и необходимые параметры входа → **Далее** → **Готово**;

Для взаимодействия сервера СУБД и RedCheck длина пароля пользователя не должна превышать 128 символов

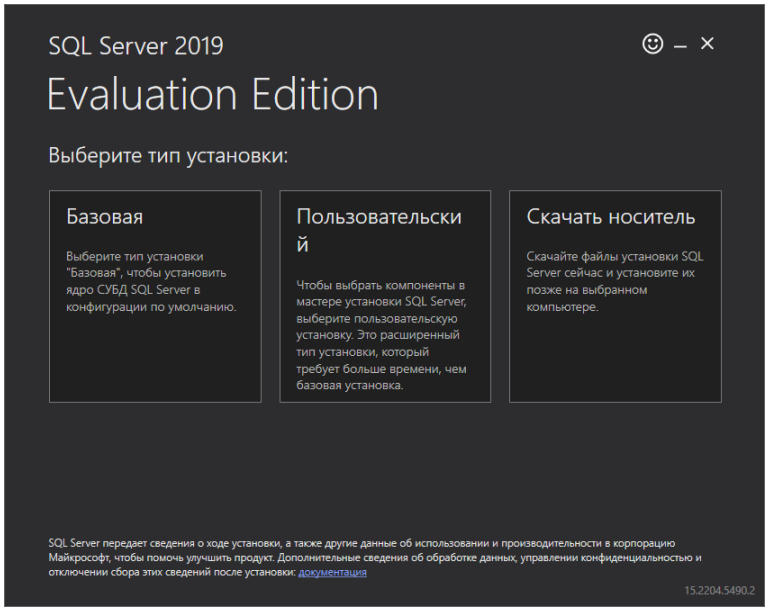


Шаг 5. Проверьте параметры создаваемого объекта-пользователя → **Готово**.

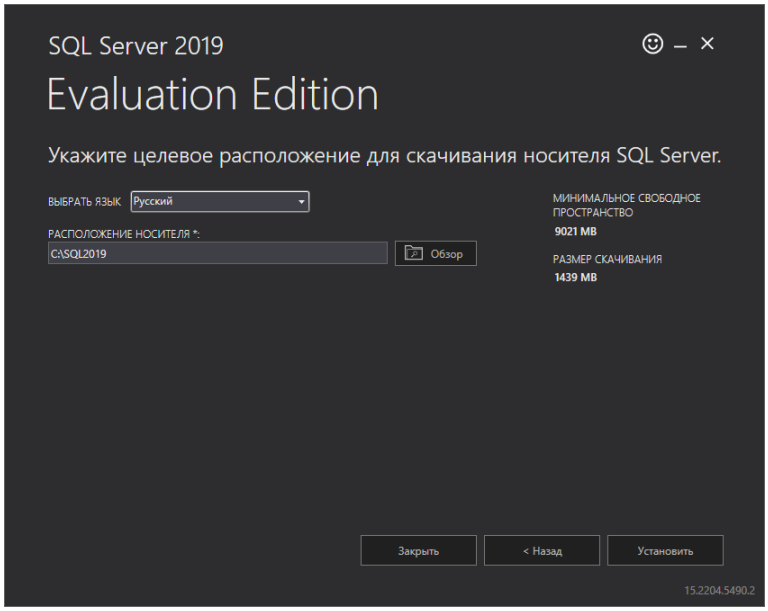


Загрузка файлов установки СУБД

Шаг 1. Выберите **Пользовательский** тип установки;



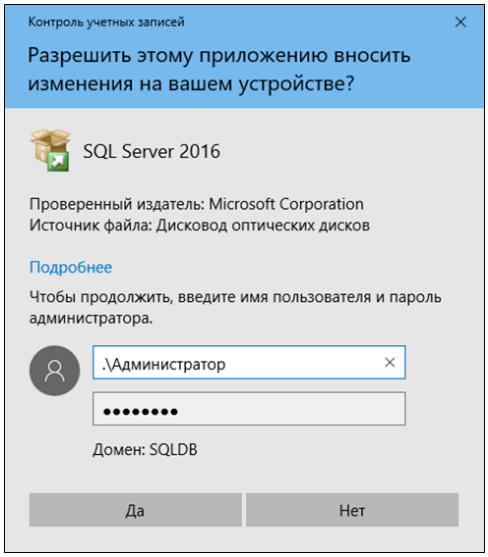
Шаг 2. При необходимости измените язык и расположение файлов установки → **Установить**;



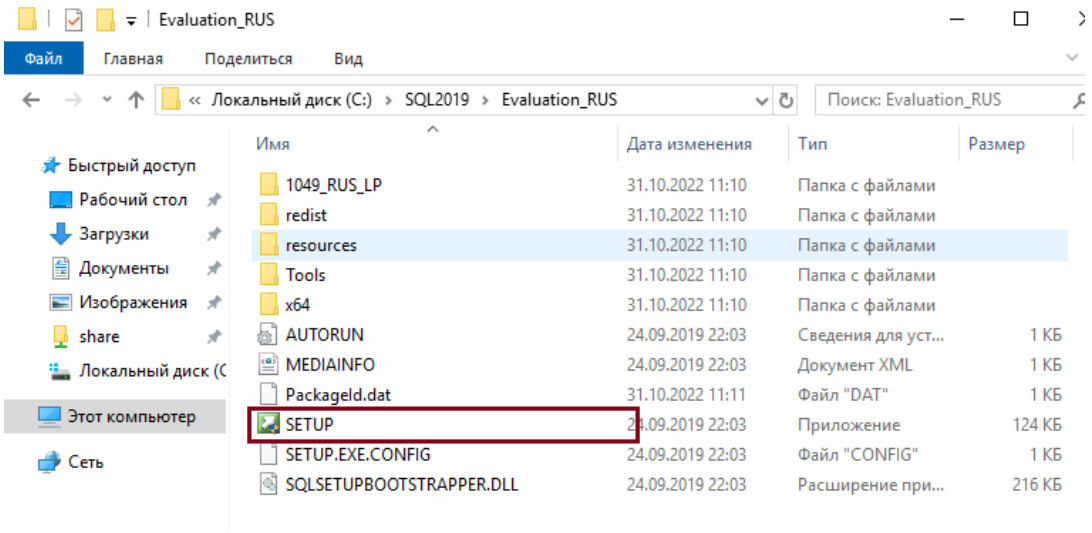
Шаг 3. После окончания установки откроется **Центр установки SQL Server**.

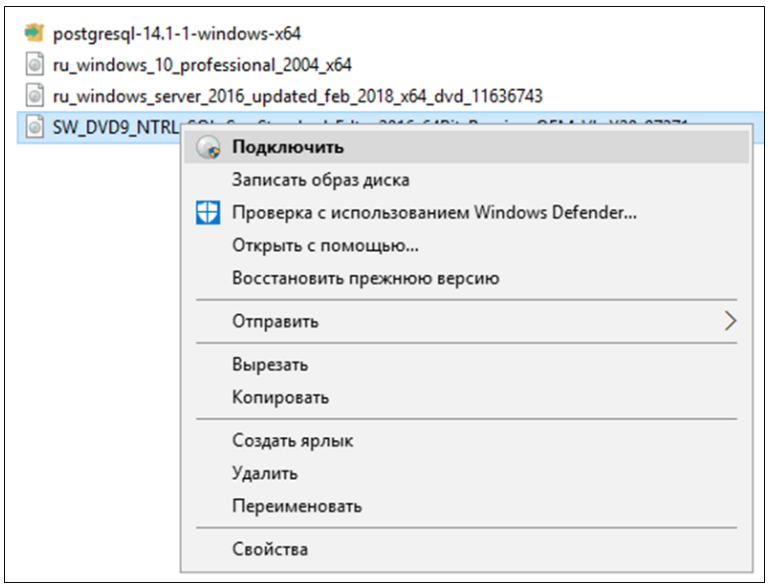
Установка СУБД на целевом сервере/АСУ ТП

Для установки СУБД Microsoft SQL Server должна использоваться учётная запись, имеющая права локального администратора. В случае запуска установки от другой учётной записи, не имеющей прав администратора, необходимо их предоставить в соответствующем диалоге.



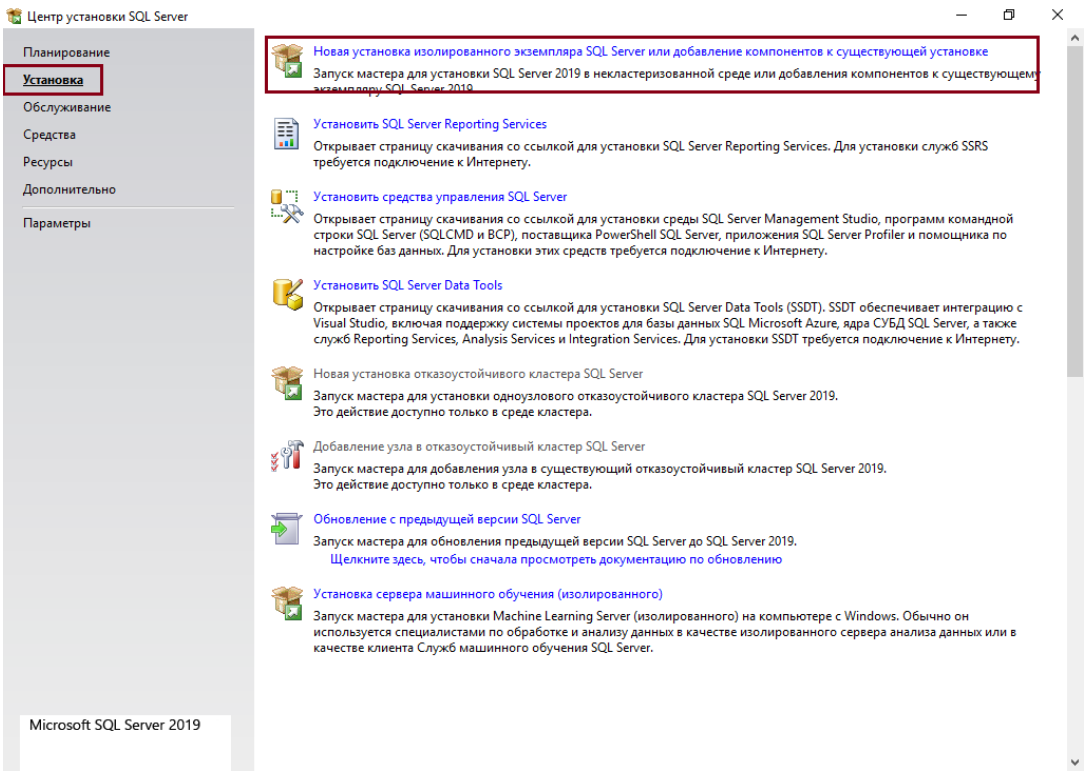
Если Центр установки SQL Server не открылся, запустите инсталляционный пакет SETUP.exe из директории с файлами установки Microsoft SQL Server. При необходимости подключите виртуальный образ дистрибутива с расширением .iso.



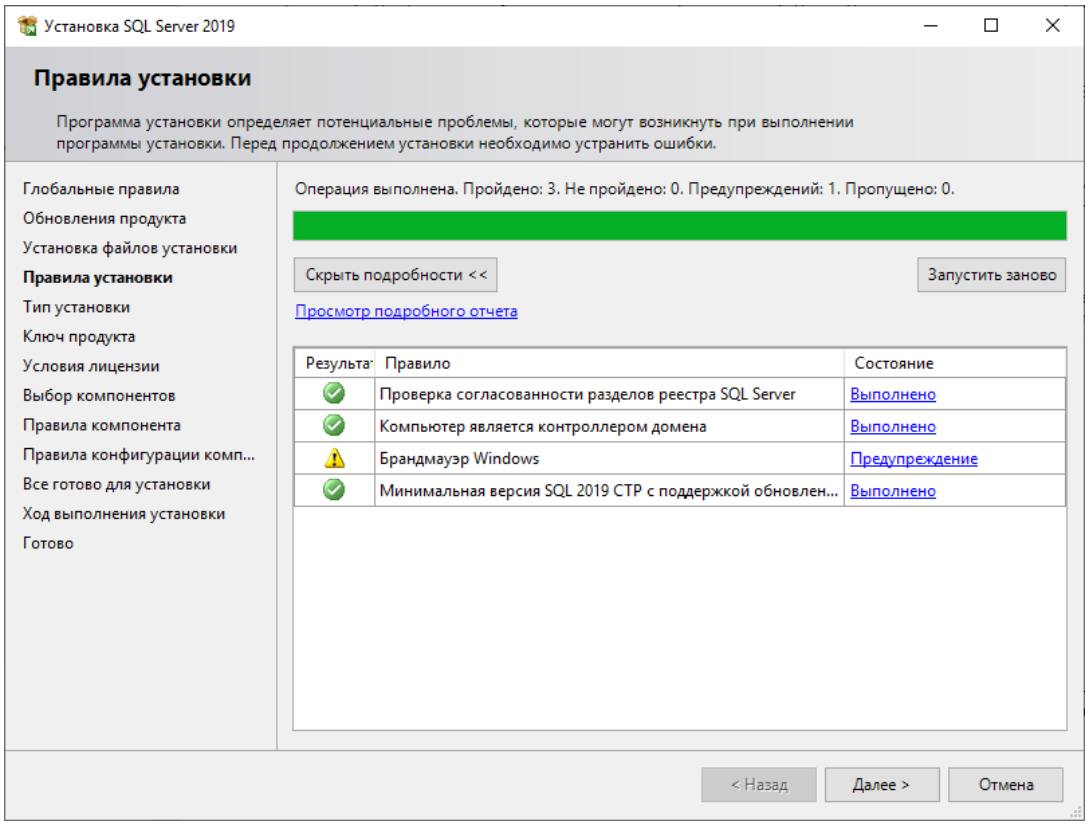


По умолчанию в ОС настроен контроль привилегий (UAC – User Account Control); в этом случае при запуске файла инсталлятора в диалоговом окне запроса на повышение привилегий нажмите **OK**.

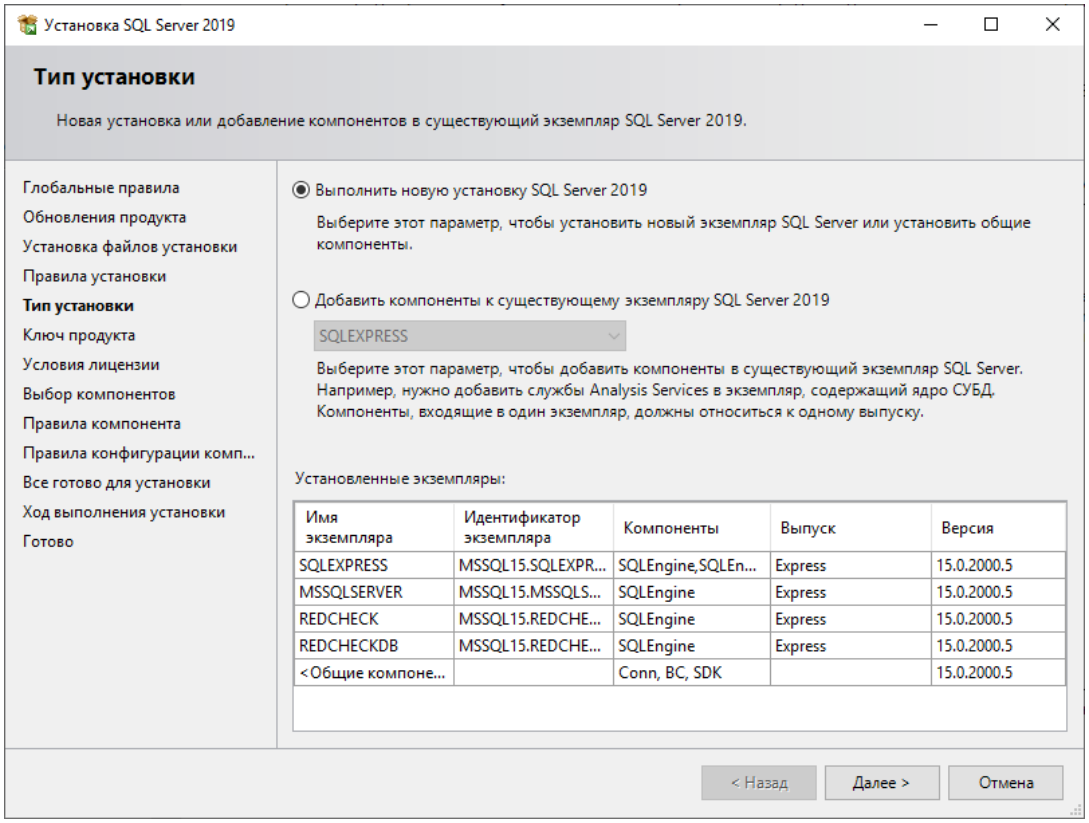
Шаг 1. В Центре установки SQL Server перейдите в **Установка** → **Новая установка**.



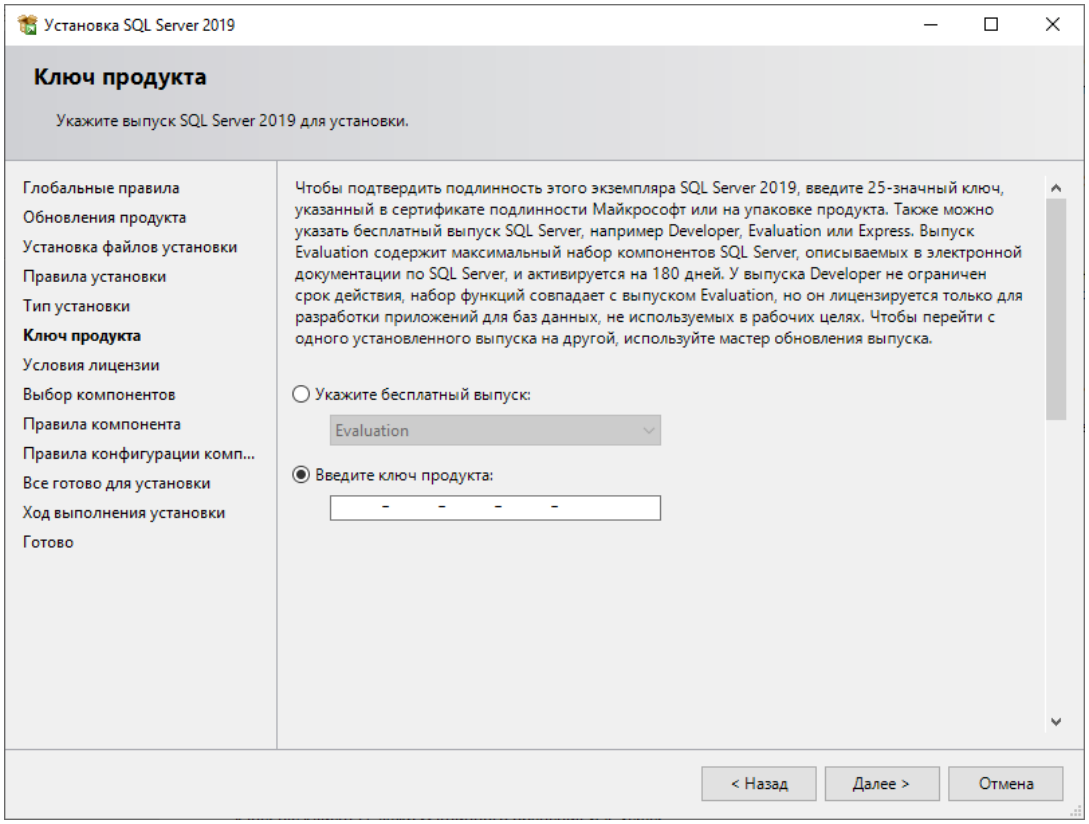
Шаг 2. Установщик проверит наличие проблем, которые могут помешать инсталляции. В случае, если все требования удовлетворены, нажмите **Далее**;



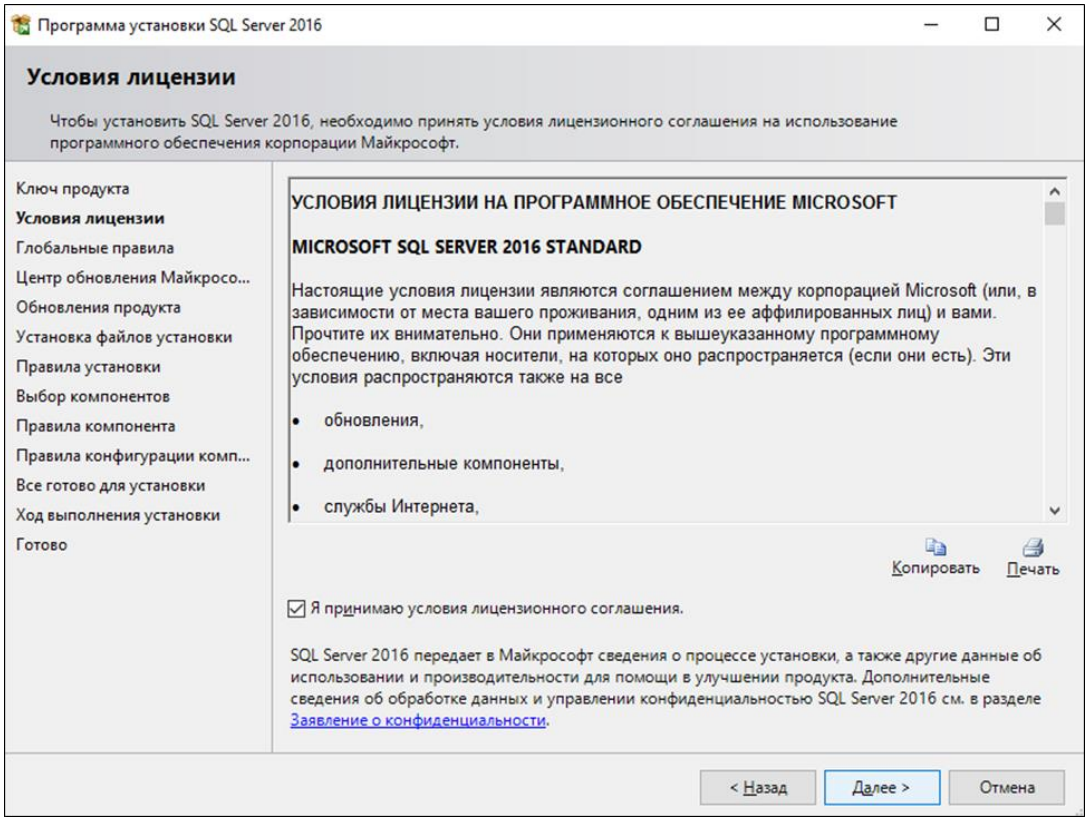
Шаг 3. Выберите тип установки **Выполнить новую установку SQL Server 2019 → Далее**;



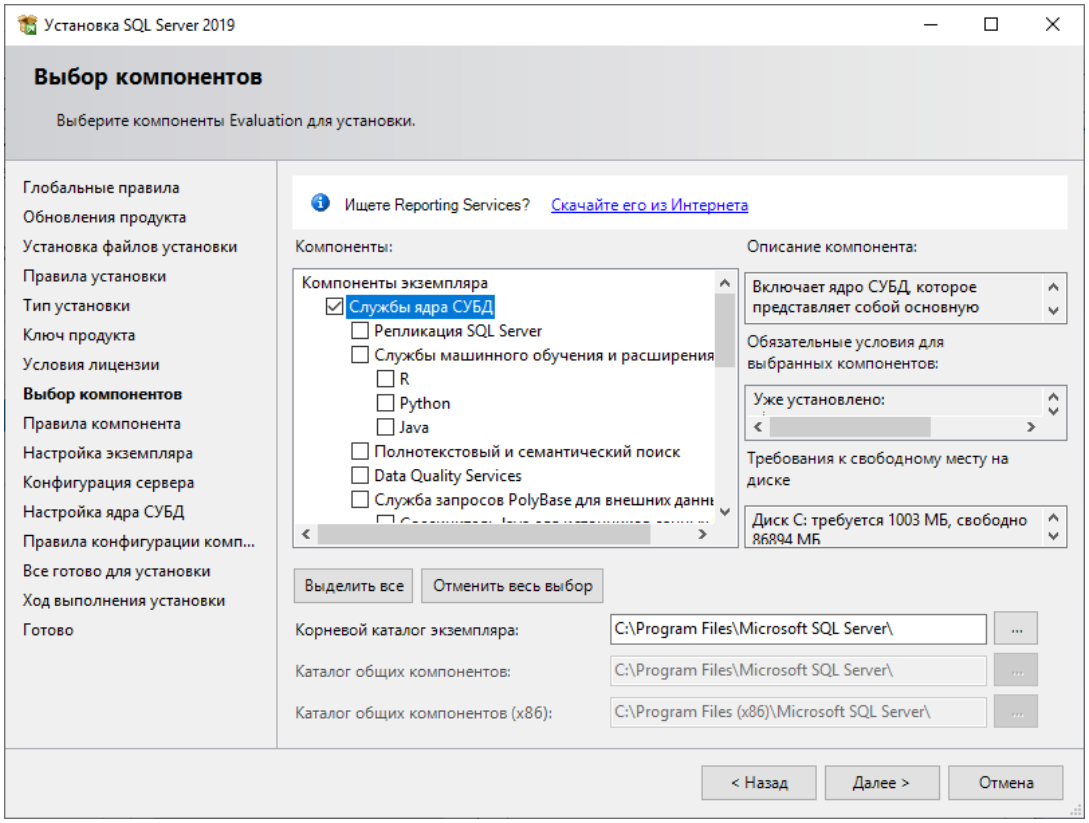
Шаг 4. Укажите лицензионный ключ СУБД. Как правило, необходимый ключ заранее задан в конфигурации установщика и заполняется инсталлятором автоматически → **Далее**;



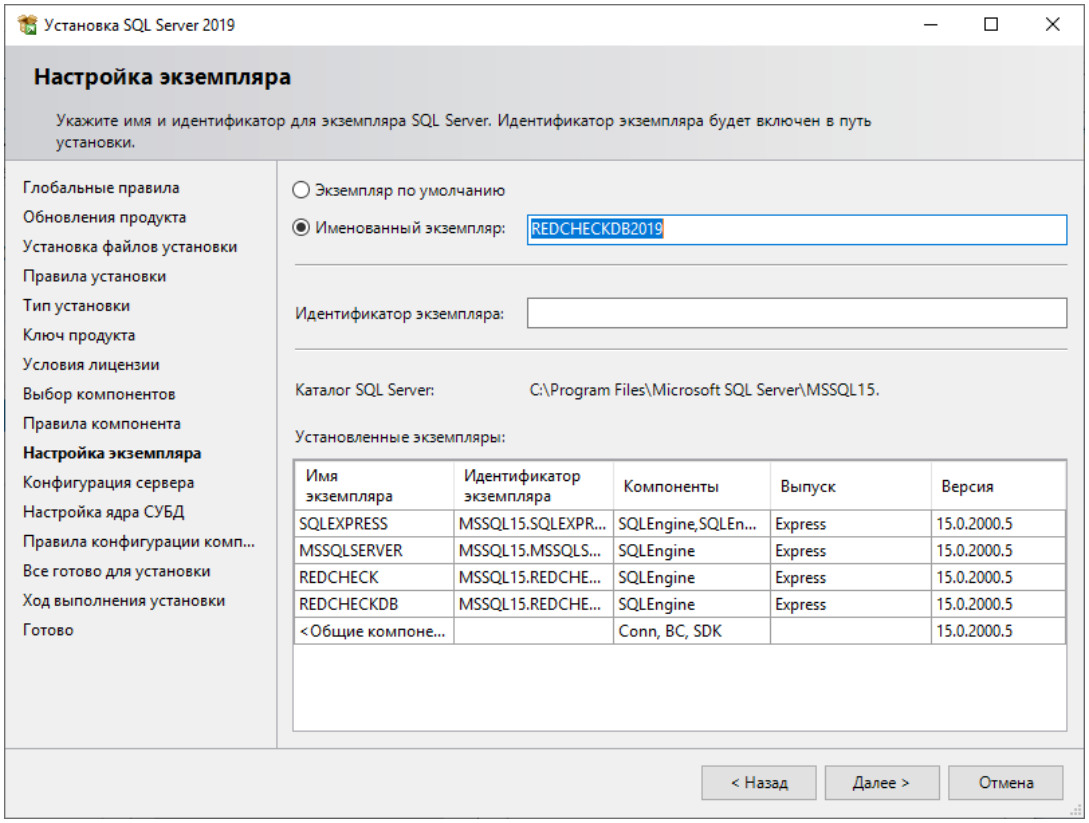
Шаг 5. Отметьте **Я принимаю условия лицензионного соглашения → Далее**;



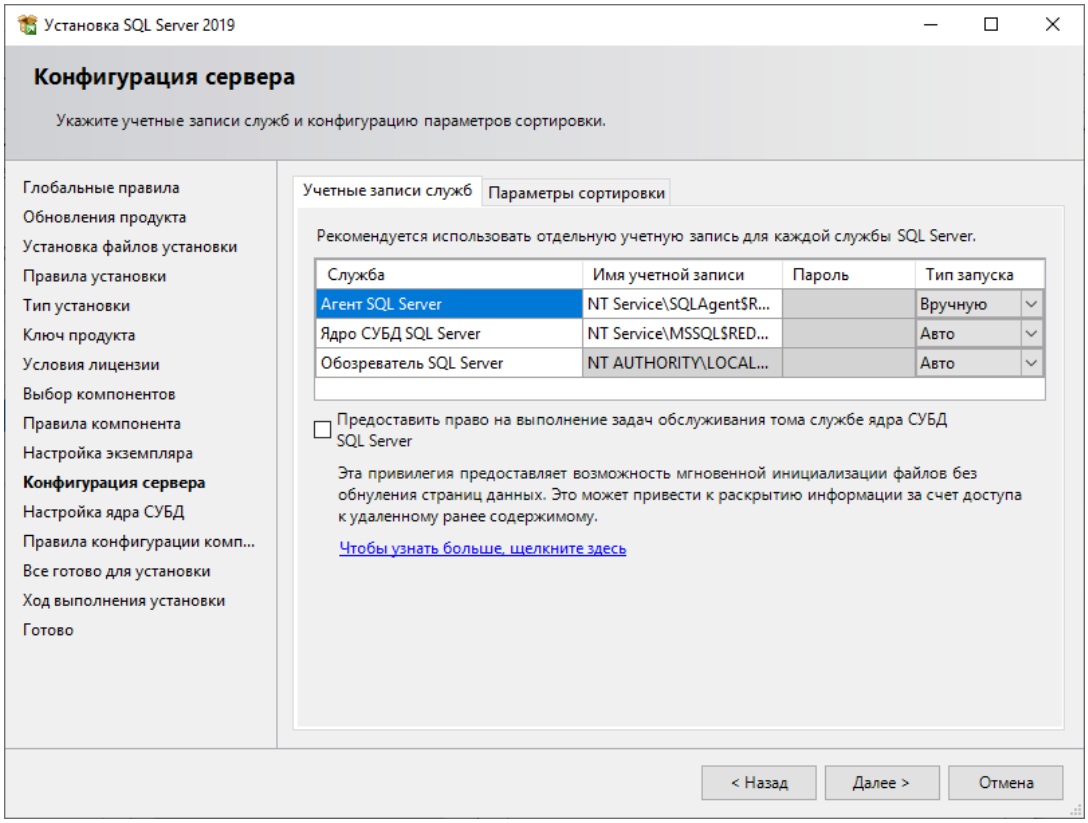
Шаг 6. Отметьте **Службы ядра СУБД → Далее**;



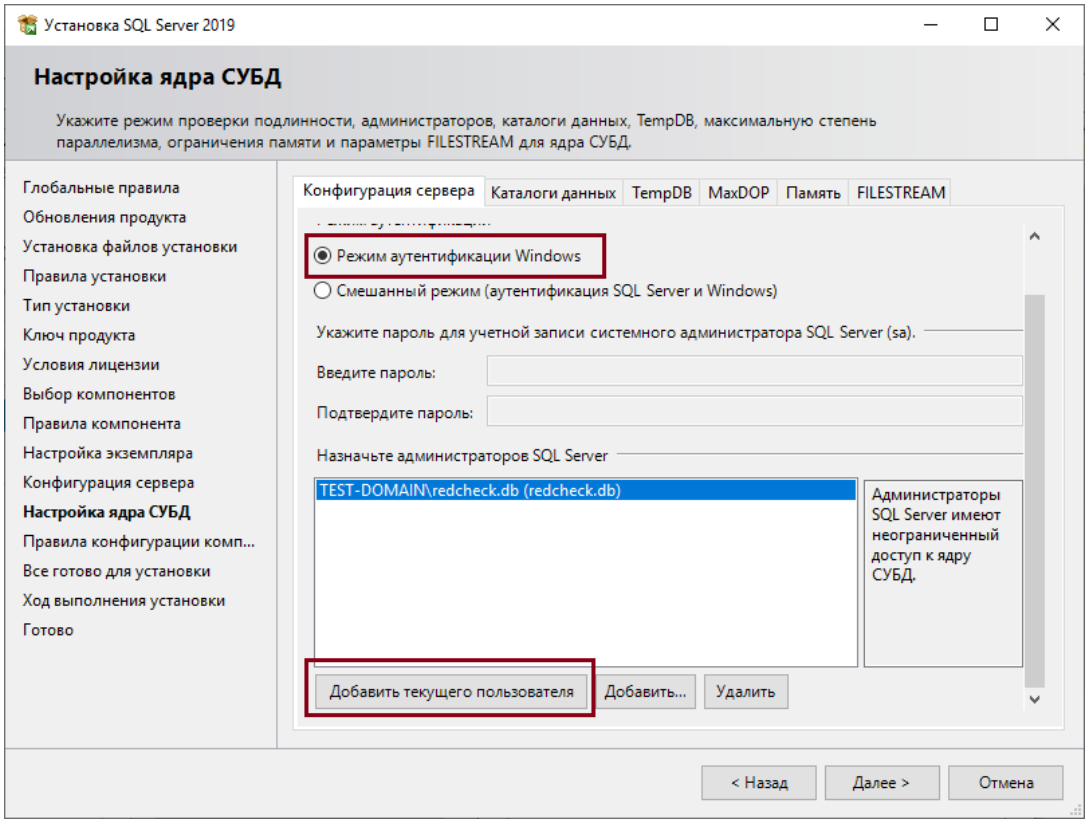
Шаг 7. Укажите соответствующее имя и идентификатор экземпляра (рекомендуется использовать именованный экземпляр БД) → **Далее**;



Шаг 8. Конфигурацию сервера рекомендуется оставить со значениями по умолчанию → **Далее**;

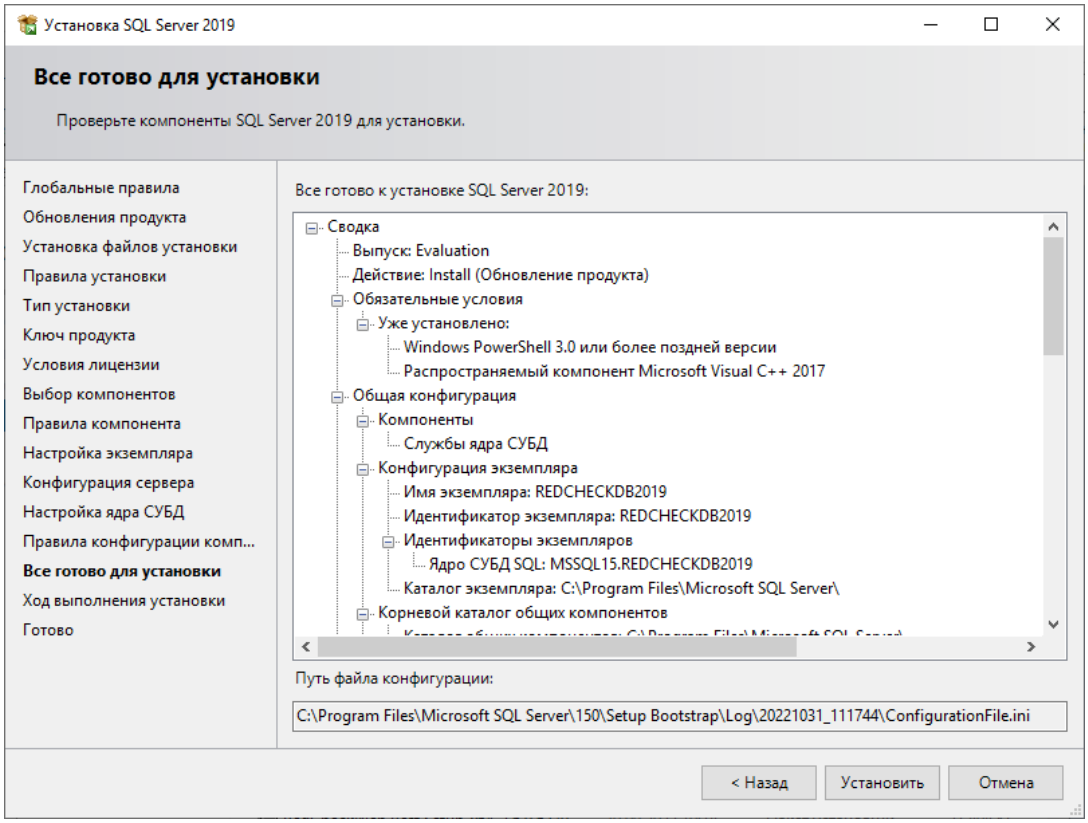


Шаг 9. Выберите **Режим проверки подлинности Windows → Добавить текущего пользователя → Далее**;

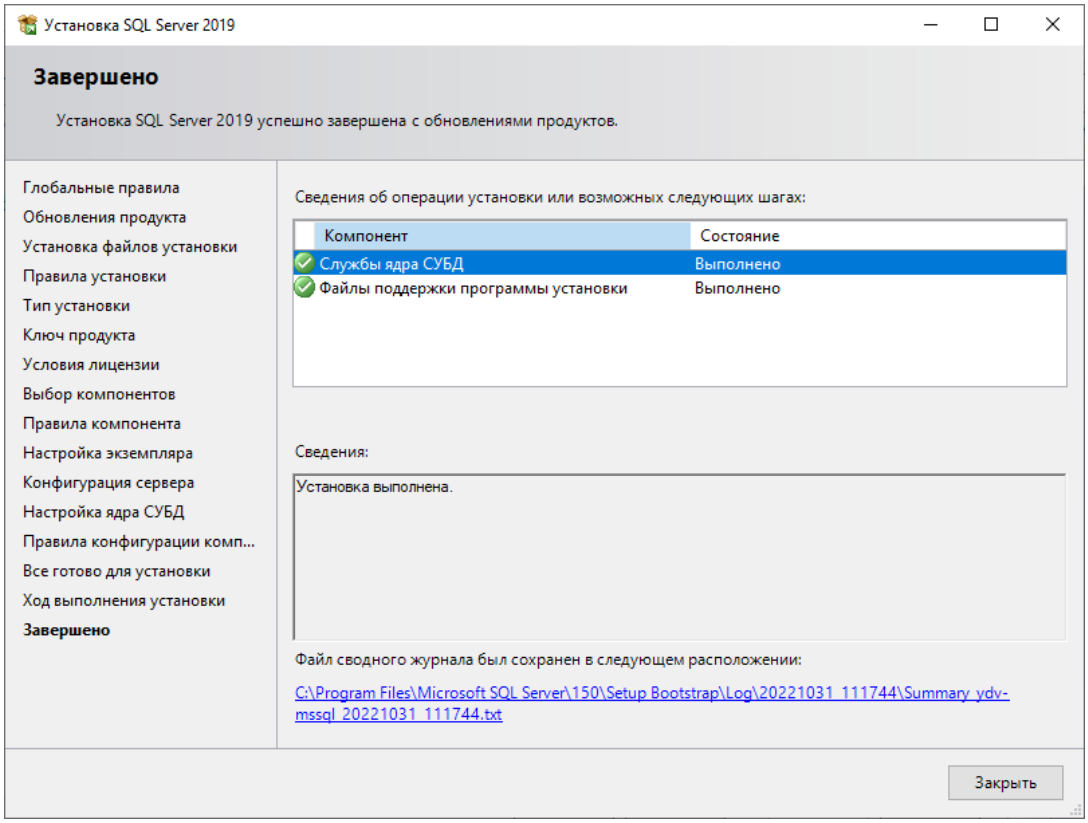


Если кнопки добавления пользователей отсутствуют, необходимо раздвинуть рабочую область окна инсталлятора, потянув мышью за правый нижний угол окна.

Шаг 10. Проверьте параметры инсталляции СУБД → **Установить**;



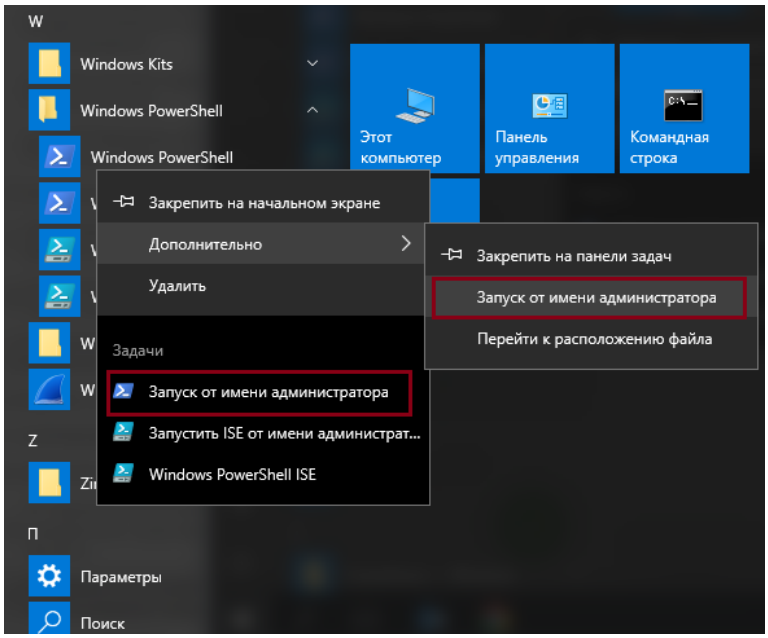
Нажмите **Закрыть** для выхода из программы установки;



После установки сервера рекомендуется установить средство управления сервером СУБД (4.1.1.3 Установка средства управления сервером СУБД).

Разрешение порта СУБД на межсетевом экране

Шаг 11. Пуск → Windows PowerShell → ПКМ по **Windows PowerShell → Запуск от имени администратора**;

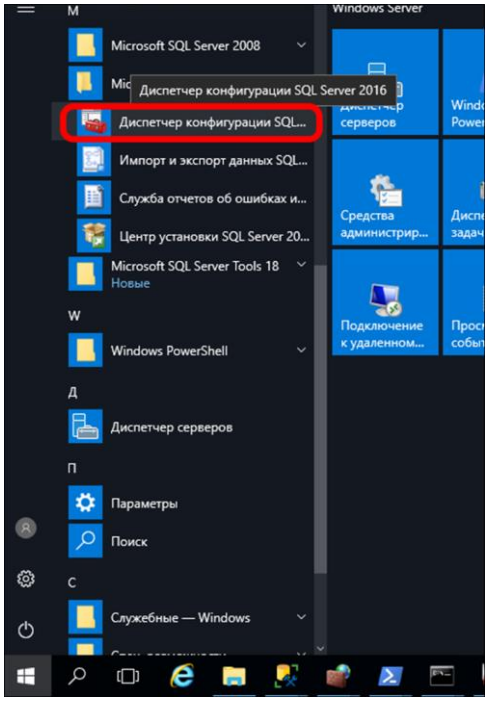


Шаг 12. Выполните следующую команду:

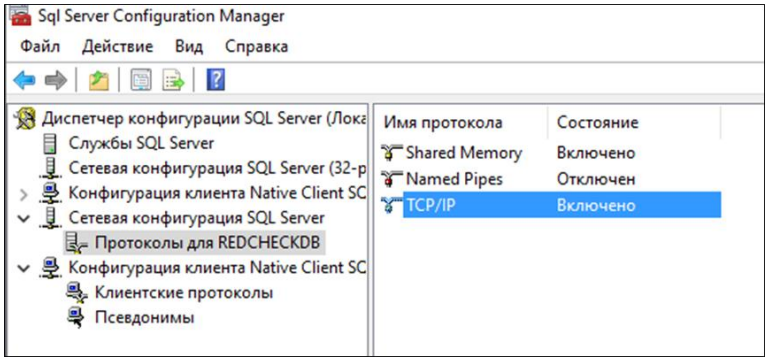
Код

```
netsh advfirewall firewall add rule name="Microsoft SQL Server port"
dir=in action=allow protocol=TCP localport=1433
```

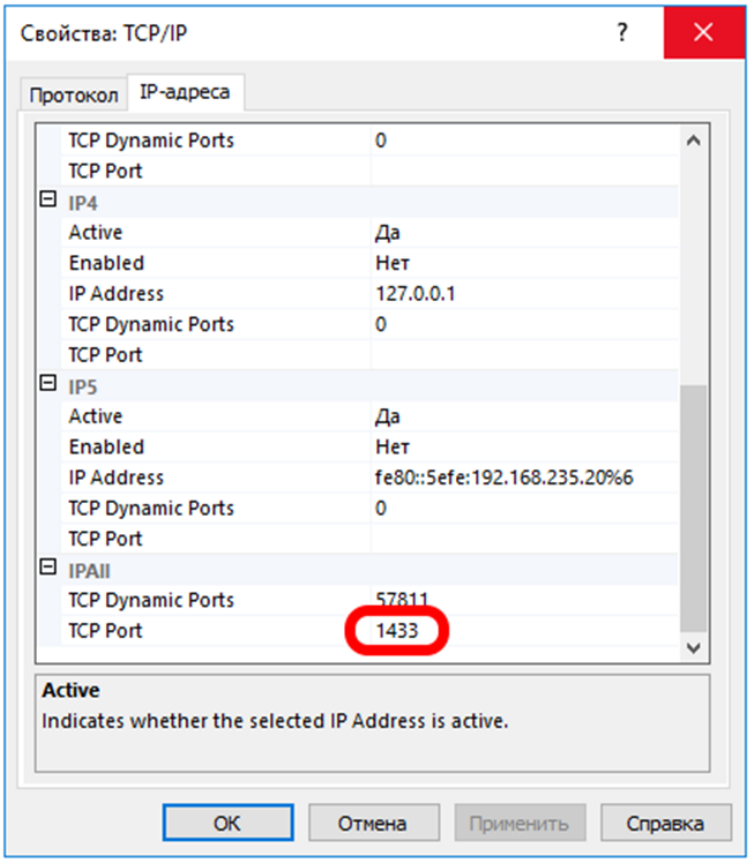
Шаг 13. Пуск → Microsoft SQL Server → Диспетчер конфигурации SQL Server;



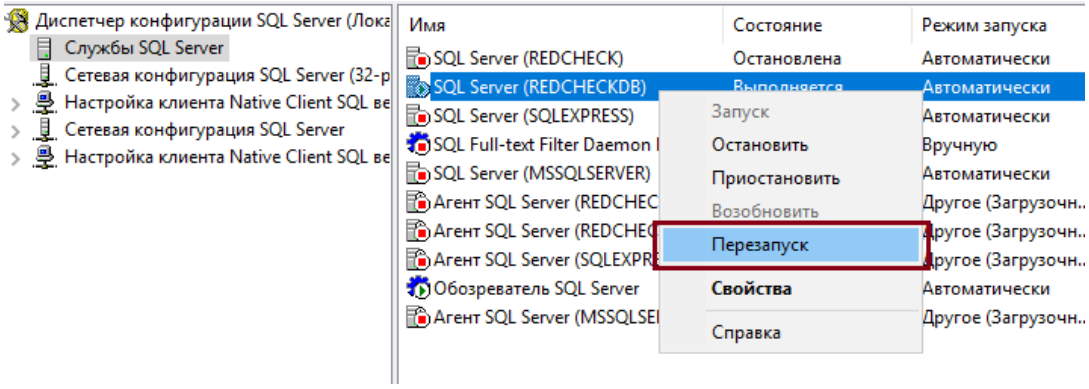
Шаг 14. Раскройте **Сетевая конфигурация SQL Server → Протоколы для <имя-экземпляра-БД> → TCP/IP**;



Шаг 15. Перейдите в **IP-адреса** → **IPAll** → укажите в **TCP Port** порт СУБД (по умолчанию 1433) → **OK**;



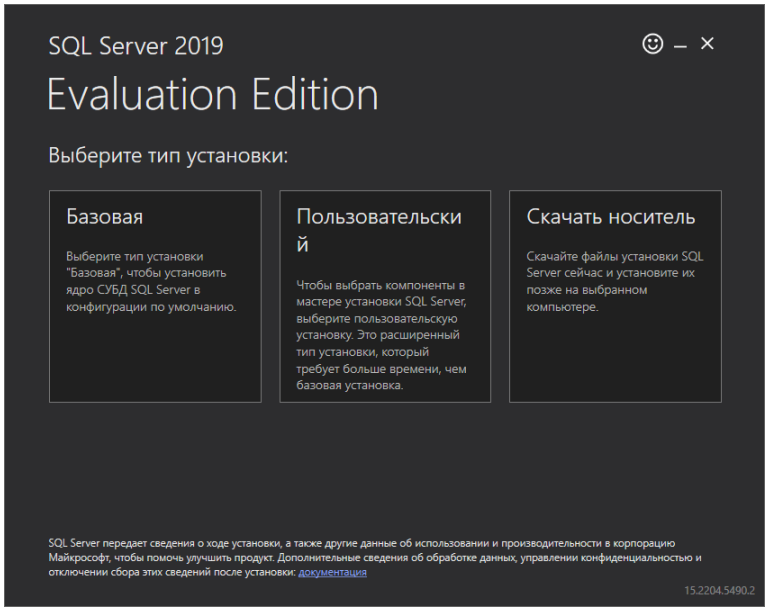
Шаг 16. Службы SQL Server → ПКМ по необходимому экземпляру → **Перезапуск**.



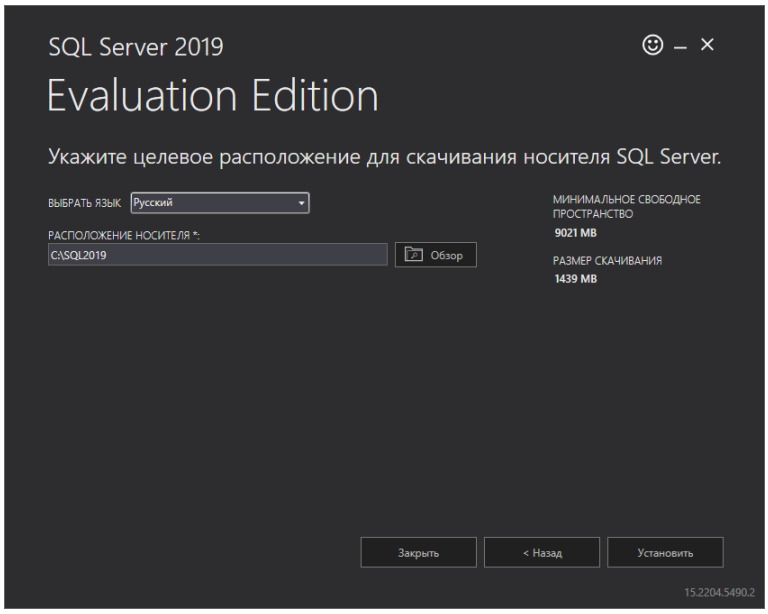
4.1.1.2 Установка в режиме смешанной авторизации

Загрузка файлов установки СУБД

Шаг 1. Выберите **Пользовательский** тип установки;



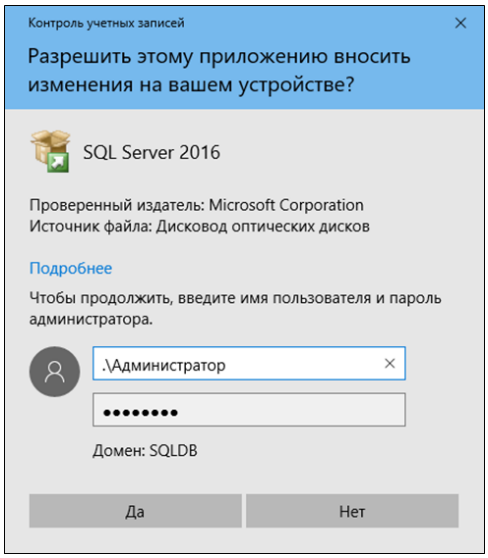
Шаг 2. При необходимости измените язык и расположение файлов установки → **Установить**;



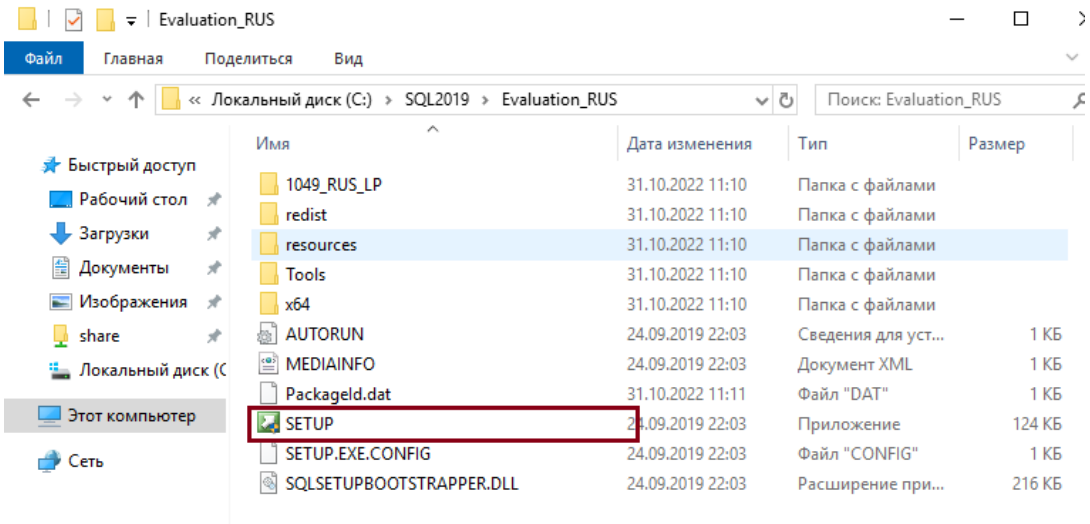
Шаг 3. После окончания установки откроется **Центр установки SQL Server**.

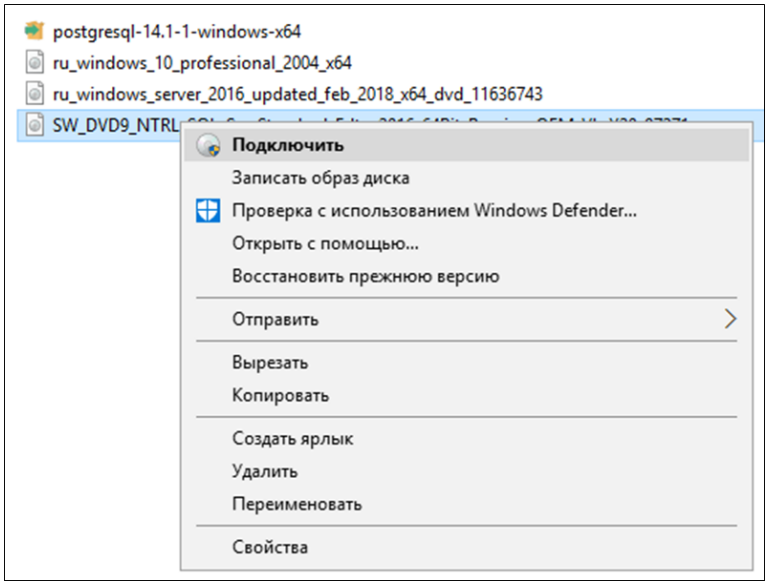
Установка СУБД на целевом сервере/АСУ ТП

Для установки СУБД Microsoft SQL Server должна использоваться учётная запись, имеющая права локального администратора. В случае запуска установки от другой учётной записи, не имеющей прав администратора, необходимо их предоставить в соответствующем диалоге.



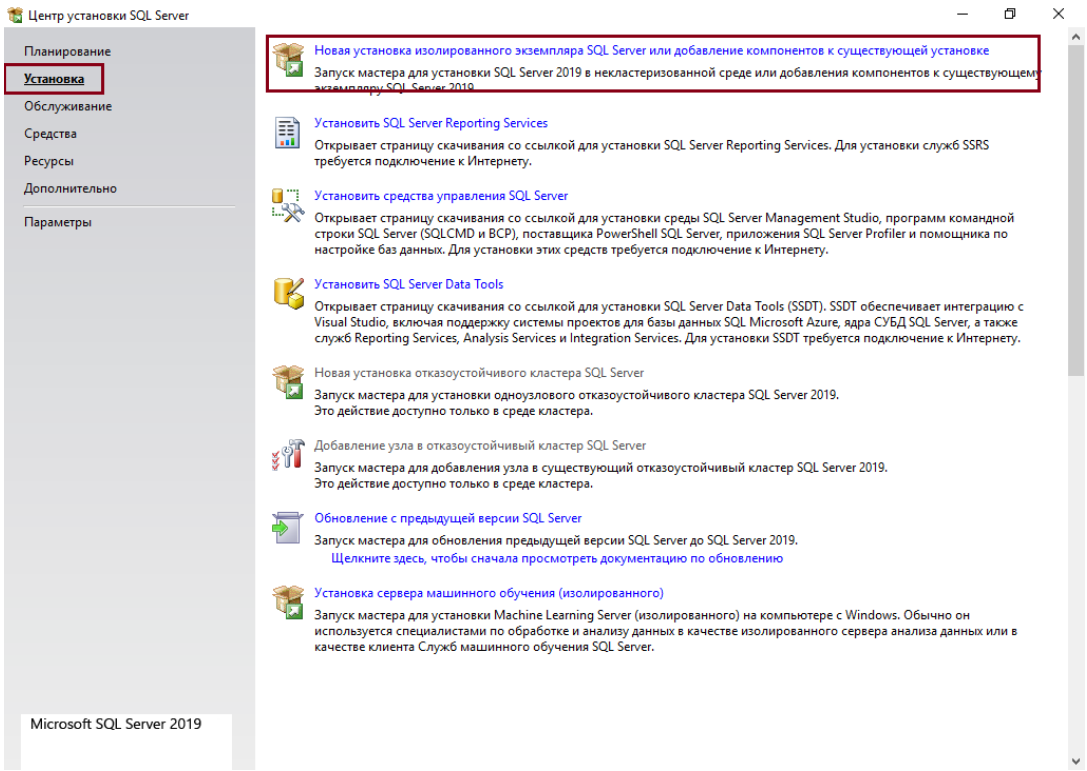
Если **Центр установки SQL Server** не открылся, запустите инсталляционный пакет **SETUP.exe** из директории с файлами установки Microsoft SQL Server. При необходимости подключите виртуальный образ дистрибутива с расширением **.iso**



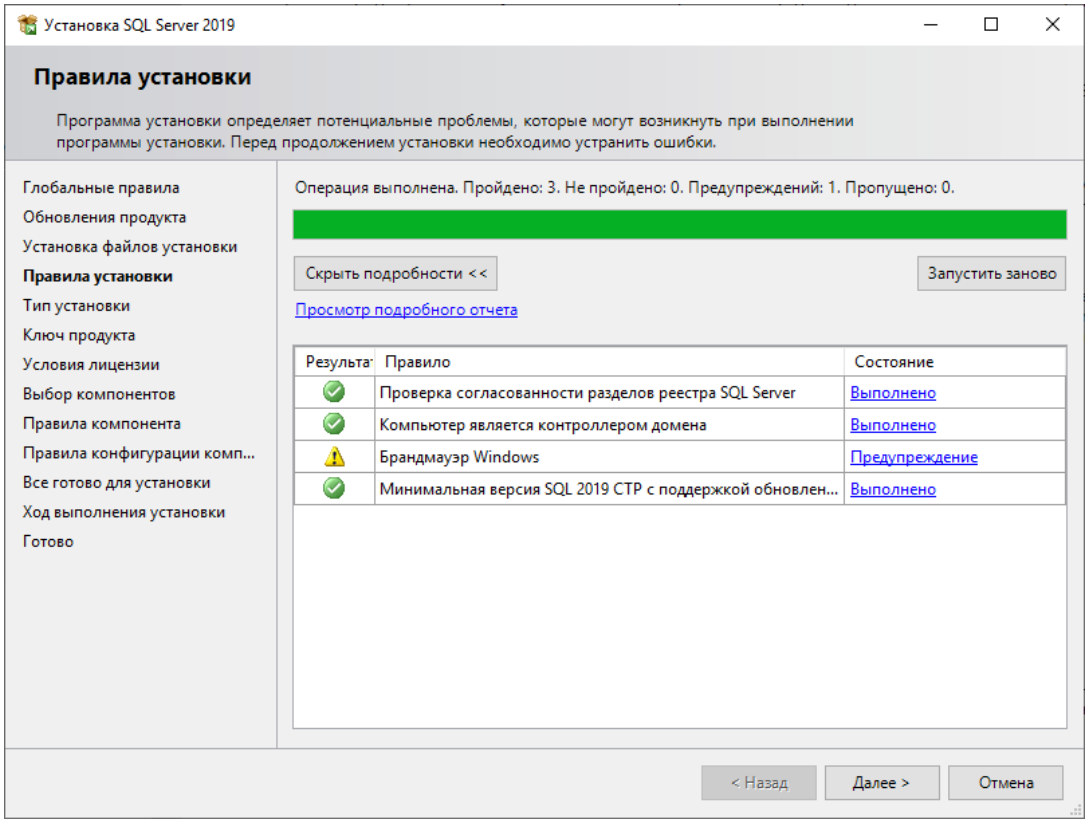


По умолчанию в ОС настроен контроль привилегий (UAC – User Account Control); в этом случае при запуске файла инсталлятора в диалоговом окне запроса на повышение привилегий нажмите **OK**.

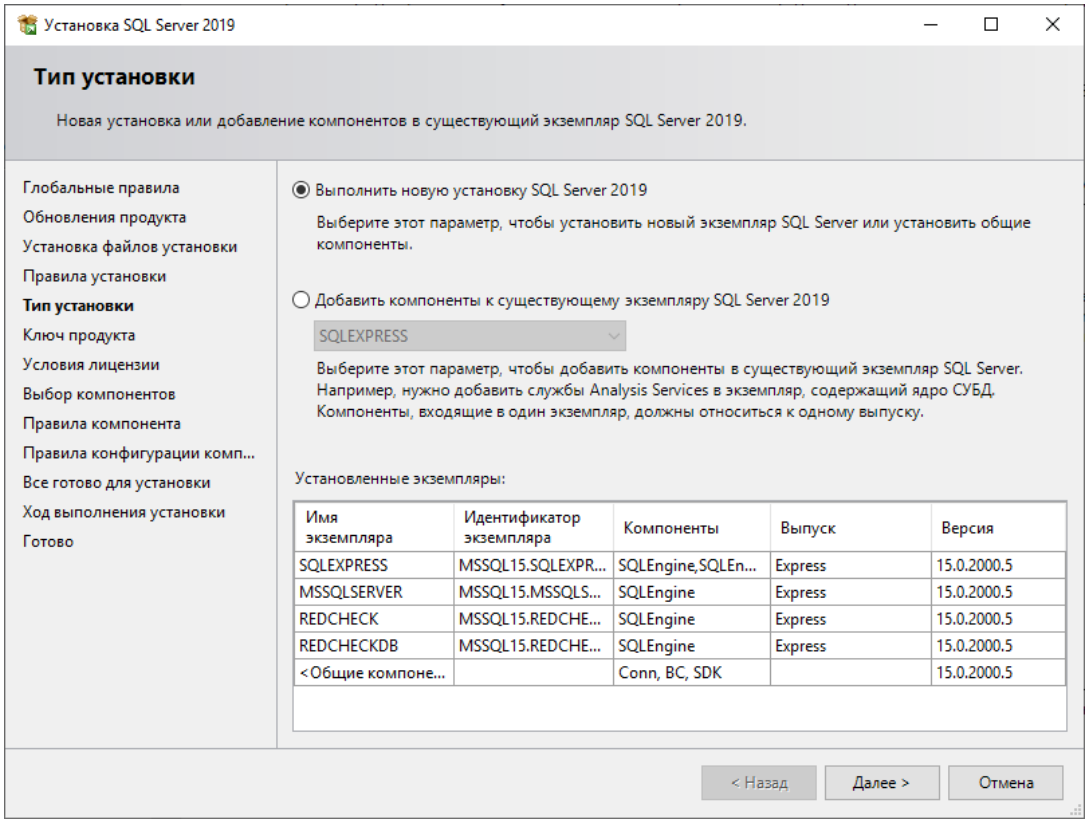
Шаг 1. В Центре установки SQL Server перейдите в **Установка** → **Новая установка**;



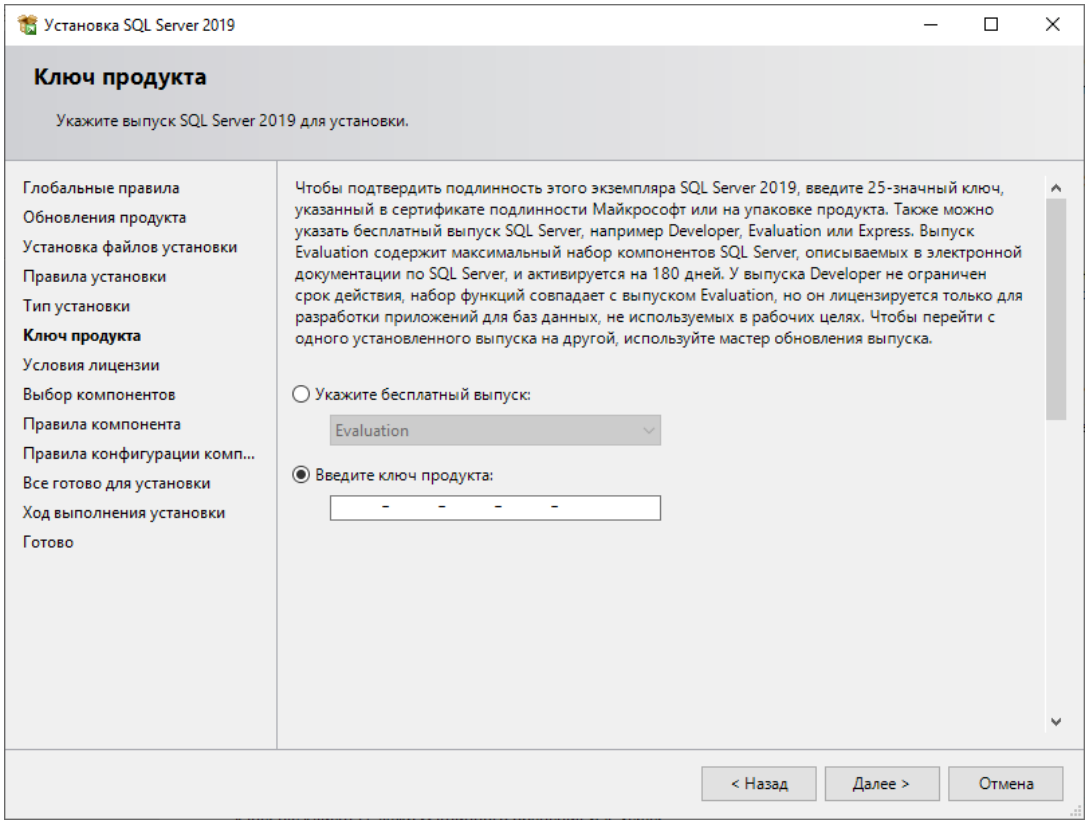
Шаг 2. Установщик проверит наличие проблем, которые могут помешать инсталляции. В случае, если все требования удовлетворены, нажмите **Далее**;



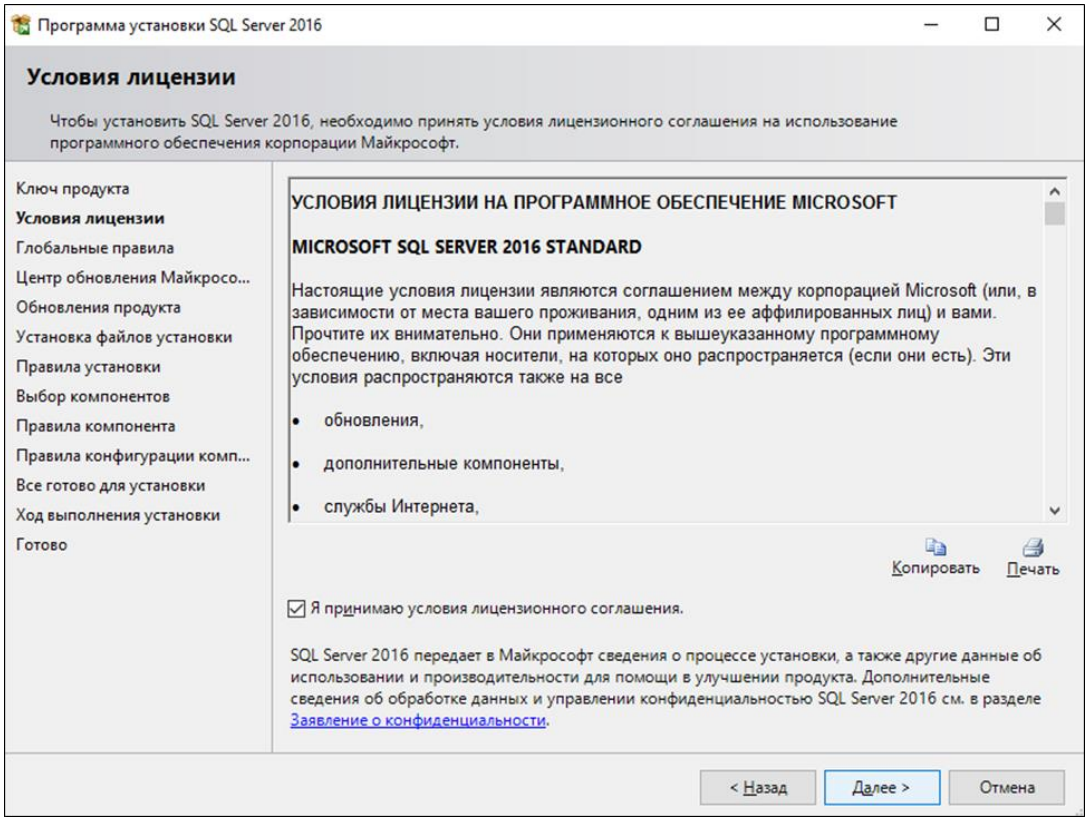
Шаг 3. Выберите тип установки **Выполнить новую установку SQL Server 2019 → Далее**;



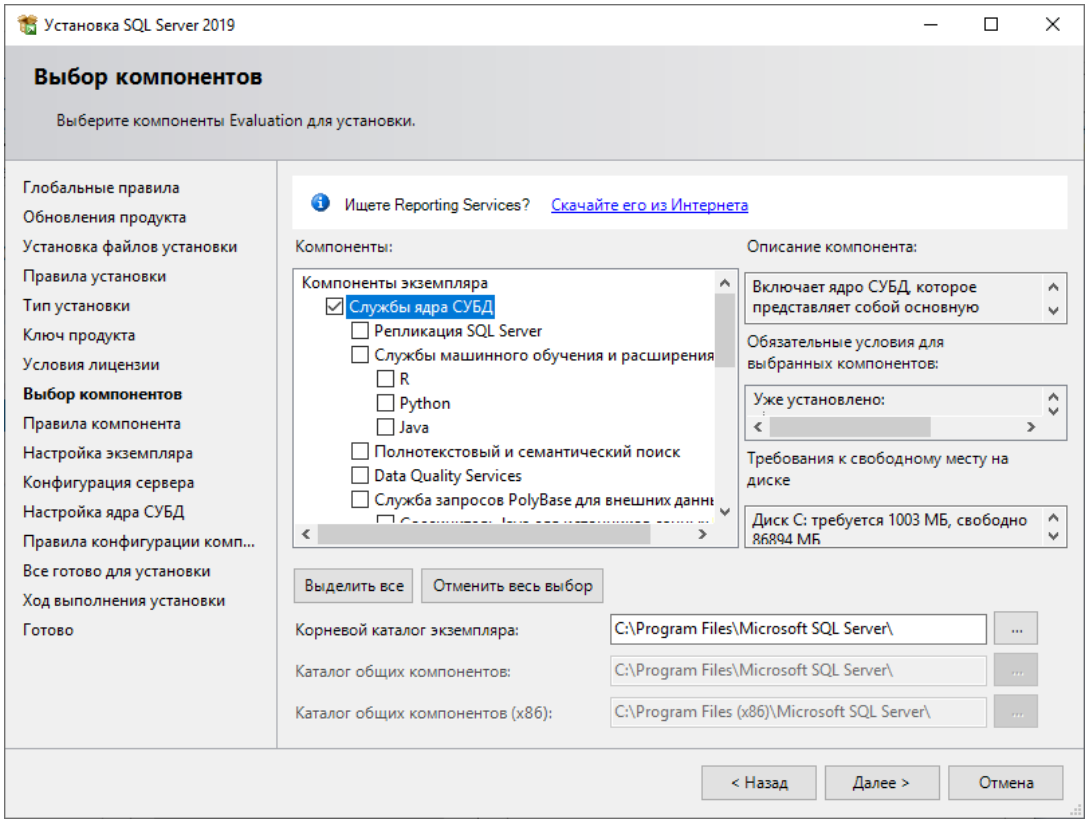
Шаг 4. Укажите лицензионный ключ СУБД. Как правило, необходимый ключ заранее задан в конфигурации установщика и заполняется инсталлятором автоматически → **Далее**;



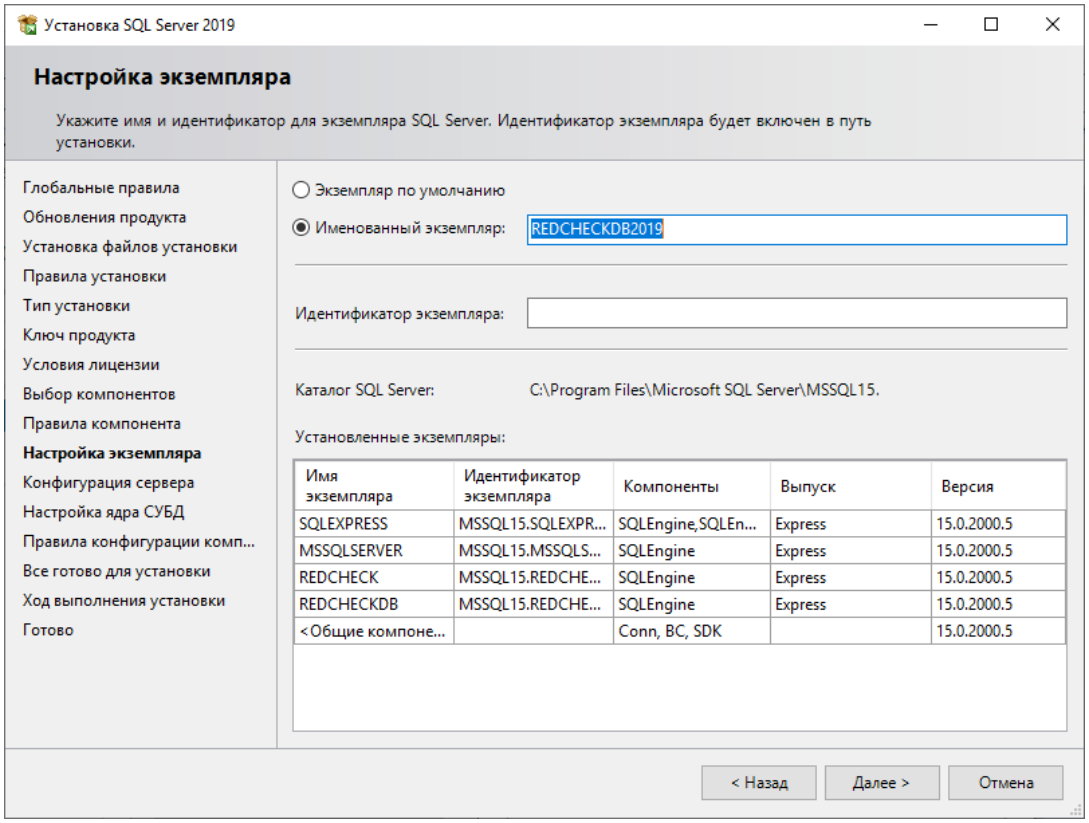
Шаг 5. Отметив **Я принимаю условия лицензионного соглашения → Далее**;



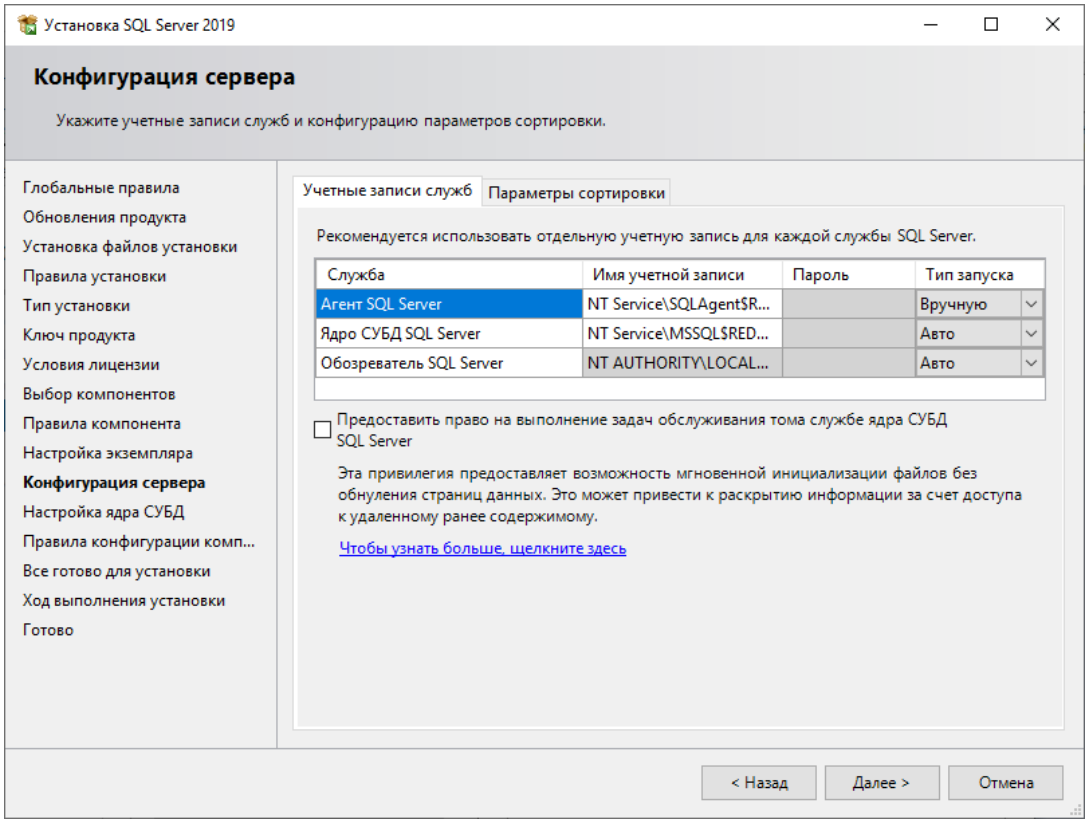
Шаг 6. Отметьте **Службы ядра СУБД → Далее**;



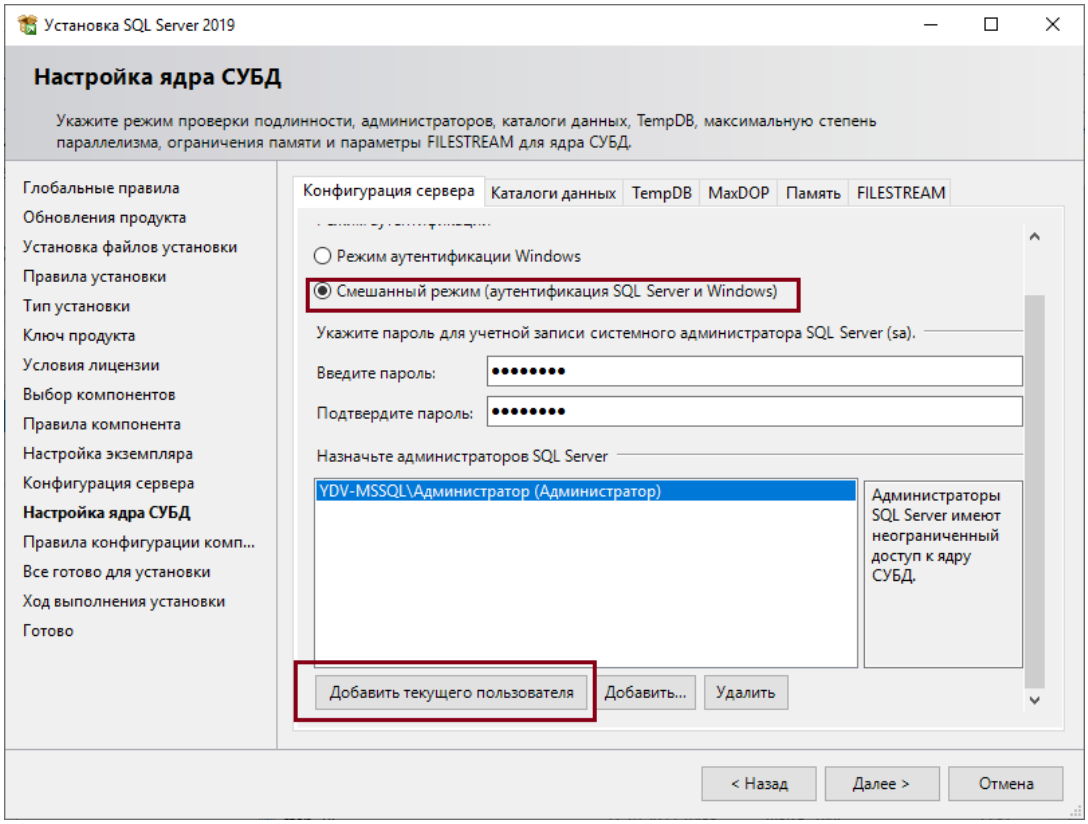
Шаг 7. Укажите соответствующее имя и идентификатор экземпляра (рекомендуется использовать именованный экземпляр БД) → **Далее**;



Шаг 8. Конфигурацию сервера рекомендуется оставить со значениями по умолчанию → **Далее**;

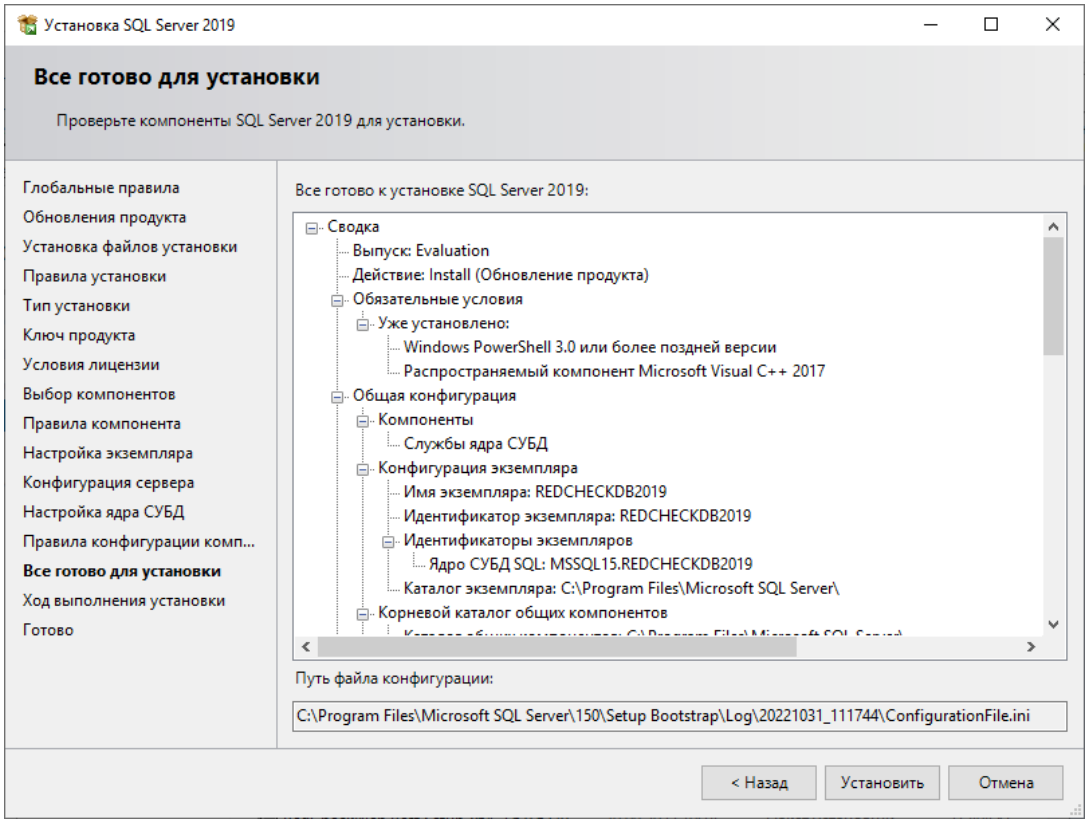


Шаг 9. Выберите **Смешанный режим проверки подлинности** → укажите и подтвердите пароль администратора СУБД (учётная запись по умолчанию с именем **sa**);

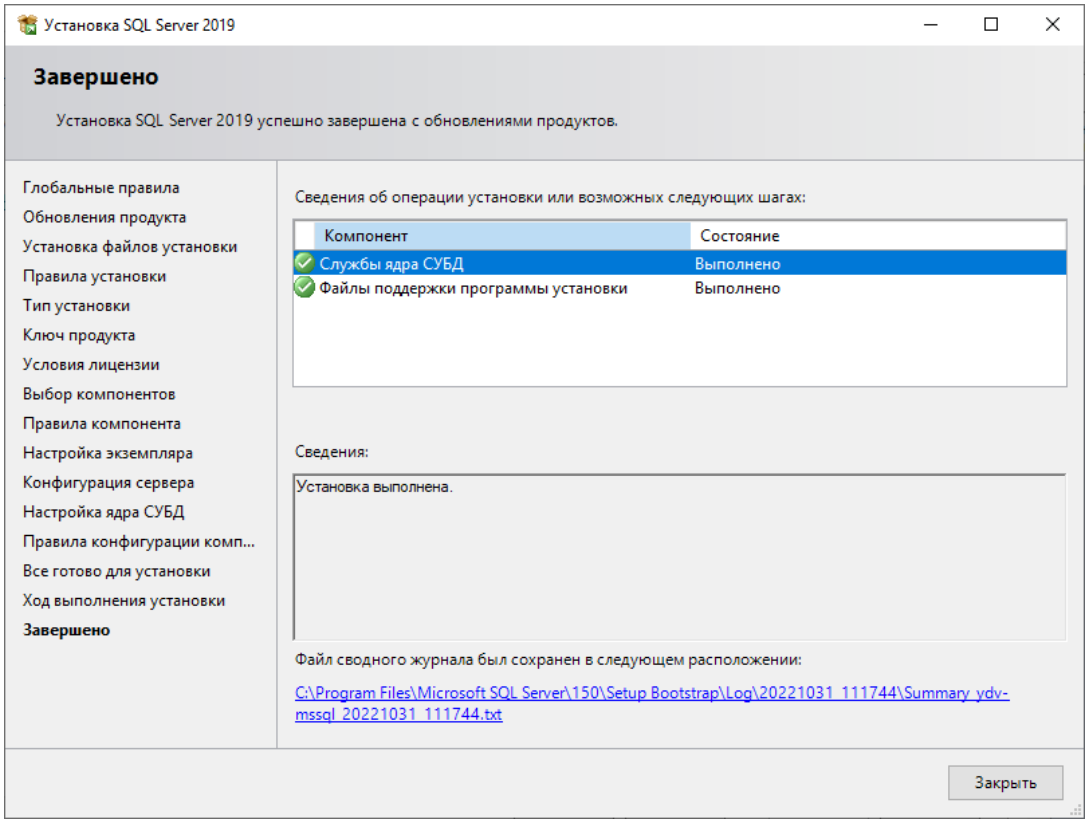


Если кнопки добавления пользователей отсутствуют, необходимо раздвинуть рабочую область окна инсталлятора, потянув мышью за правый нижний угол окна.

Шаг 10. Проверьте параметры инсталляции СУБД → **Установить**;



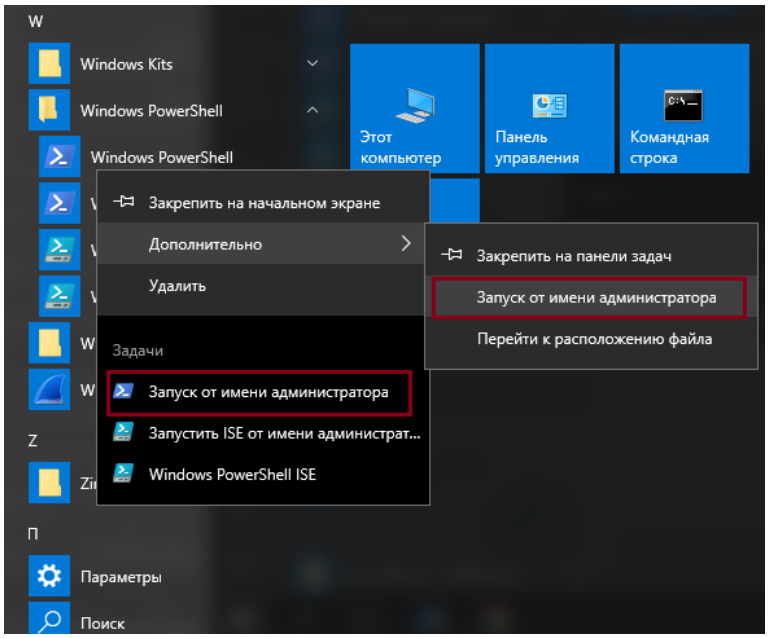
После завершения установки будет выведено окно сводных результатов. Нажмите **Закрыть** для выхода из программы установки;



После установки сервера рекомендуется установить средство управления сервером СУБД (4.1.1.3 Установка средства управления сервером СУБД).

Разрешение порта СУБД на межсетевом экране

Шаг 11. Пуск → Windows PowerShell → ПКМ по **Windows PowerShell → Запуск от имени администратора**;

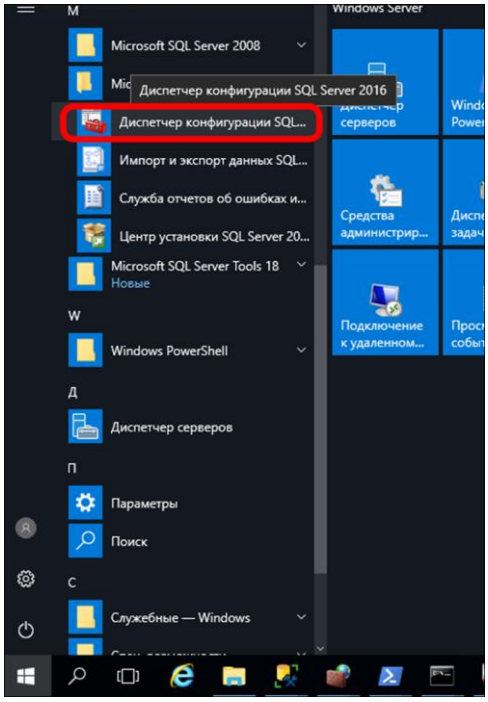


Шаг 12. Выполните следующую команду:

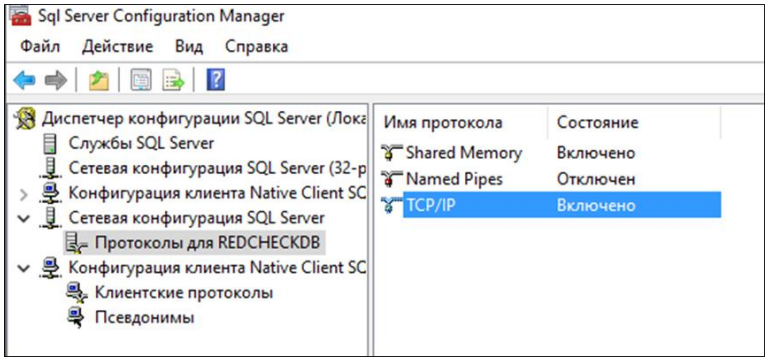
Код

```
netsh advfirewall firewall add rule name="Microsoft SQL Server port"
dir=in action=allow protocol=TCP localport=1433
```

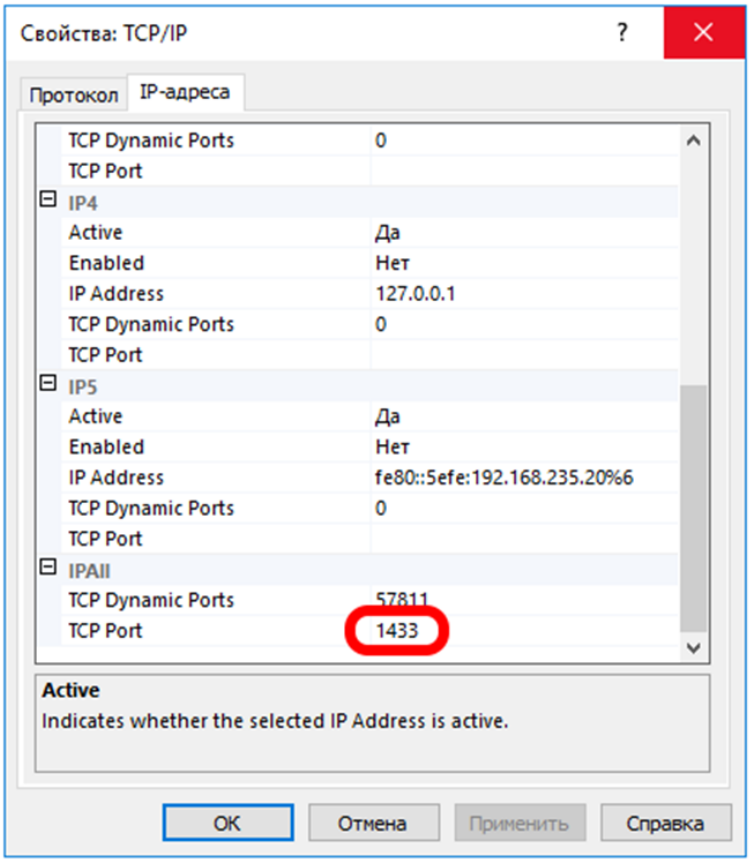
Шаг 13. Пуск → Microsoft SQL Server → Диспетчер конфигурации SQL Server;



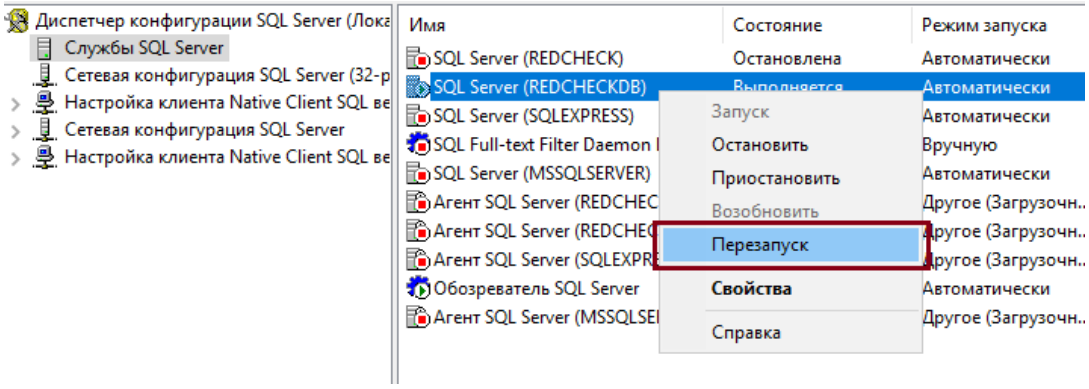
Шаг 14. Сетевая конфигурация SQL Server → Протоколы для <имя-экземпляра-БД> → TCP/IP;



Шаг 15. Перейдите в **IP-адреса** → **IPAII** → укажите в **TCP Port** порт СУБД (по умолчанию 1433) → **OK**;



Шаг 16. Службы SQL Server → ПКМ по необходимому экземпляру → **Перезапуск**.



4.1.1.3 Установка средства управления сервером СУБД

Чтобы эффективно управлять СУБД Microsoft SQL Server рекомендуется установить SSMS (SQL Server Management Studio). Данное ПО позволяет настраивать, администрировать и осуществлять мониторинг экземпляров СУБД Microsoft SQL Server, а также выполнять запросы к БД.

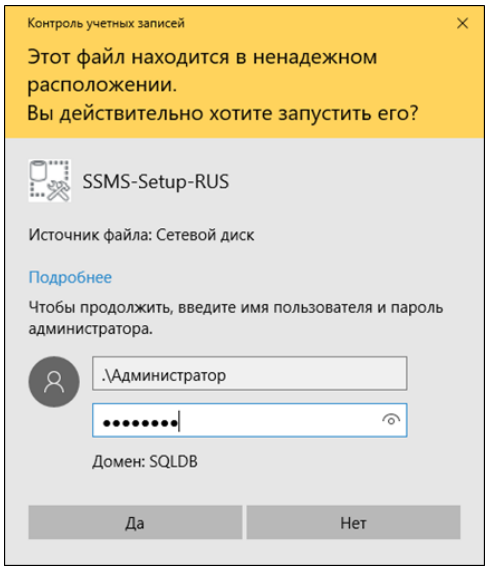
SSMS может быть установлен на АСУ ТП администратора или на сервер СУБД (в таком случае требуется наличие прав администратора).

Скачать дистрибутив SSMS необходимой локализации можно на странице разработчика.

Для управления СУБД посредством SSMS учётная запись должна иметь соответствующую роль безопасности СУБД.

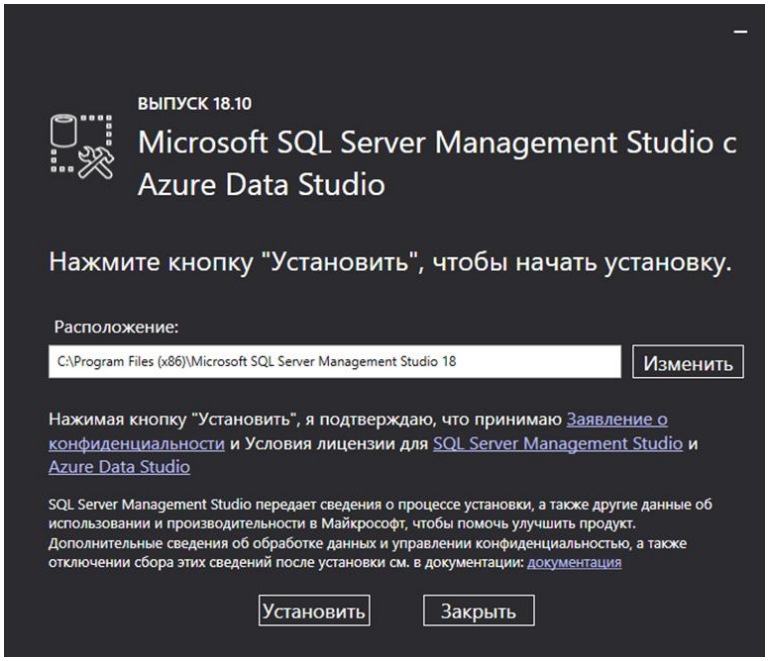
Установка средства управления SSMS

Шаг 1. Запустите инсталляционный пакет **SSMS-Setup-RUS.exe** или другой необходимой локализации;

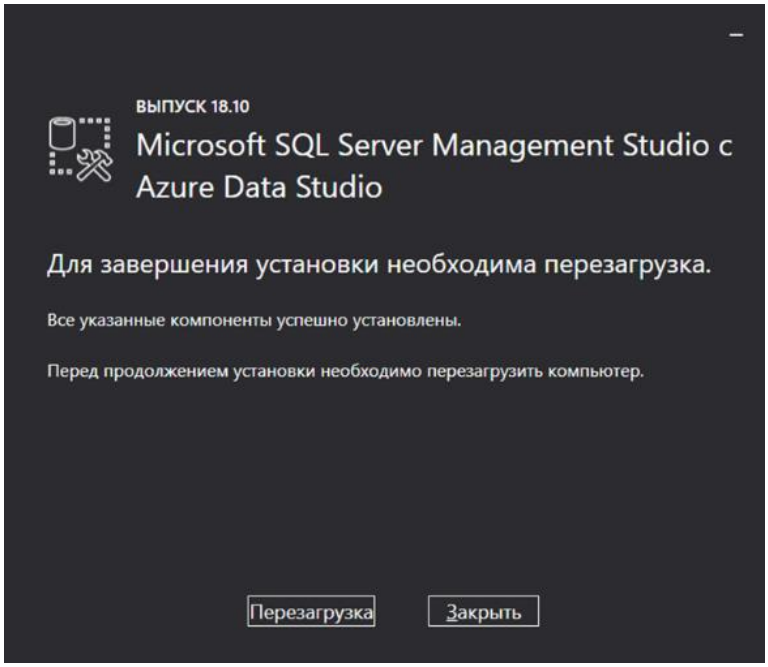


При необходимости в окне повышения прав укажите соответствующую учётную запись, имеющую права администратора.

Шаг 2. Укажите целевой путь для установки (рекомендуется оставить значение по умолчанию) → **Установить**;



Шаг 3. По завершении установки нажмите **Перезагрузка**.



4.1.2 Установка СУБД PostgreSQL на Windows

Далее приводится инструкция по установке СУБД на примере PostgreSQL 14. Поддерживаемые версии указаны в 3.2 Требования к программному обеспечению.

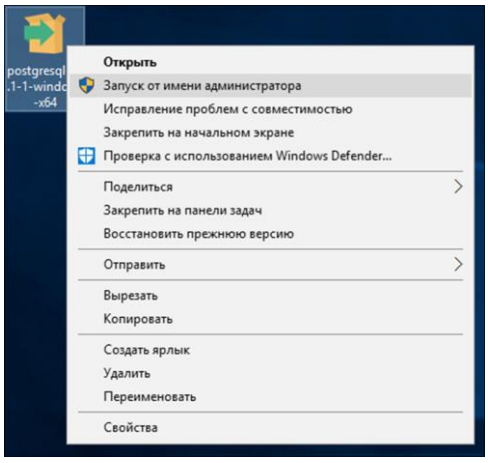
Загрузить необходимый инсталляционный пакет СУБД PostgreSQL можно на соответствующей странице сайта разработчика.

Рекомендуется использовать режим авторизации средствами СУБД. При необходимости можно использовать режим доменной авторизации посредством GSSAPI.

Не рекомендуется выполнять установку СУБД на сервере, являющемся контроллером домена.

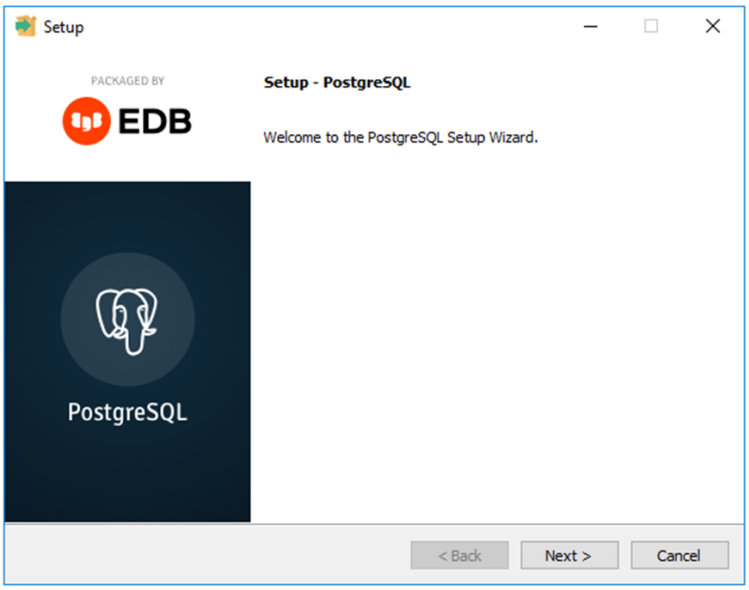
Установка PostgreSQL

Шаг 1. Запустите инсталляционный пакет СУБД на сервере/АСУ ТП от имени администратора.

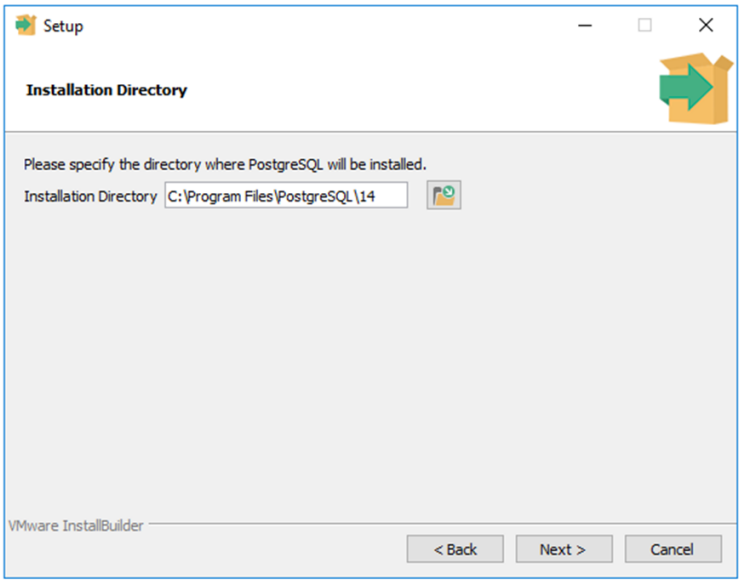


По умолчанию в системе настроен контроль привилегий (UAC – User Account Control); в этом случае при запуске инсталлятора будем выведено окно соответствующего запроса на повышение привилегий, в котором необходимо нажать **OK**.

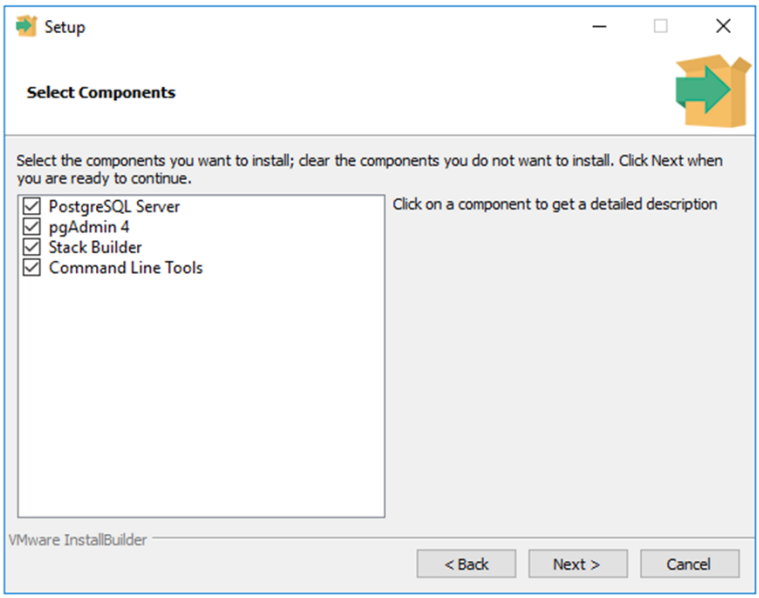
Шаг 2. В открывшемся окне инсталлятора нажмите **Next**;



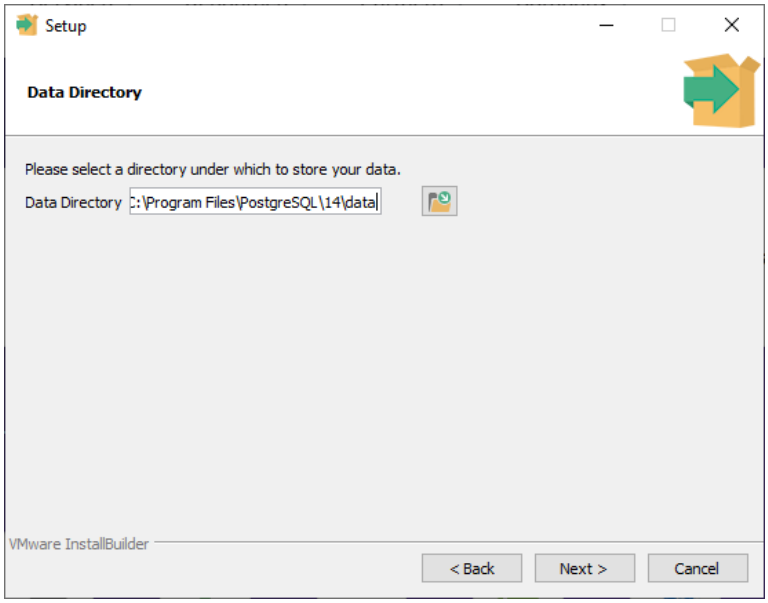
Шаг 3. Выберите директорию для установки СУБД → **Next**;



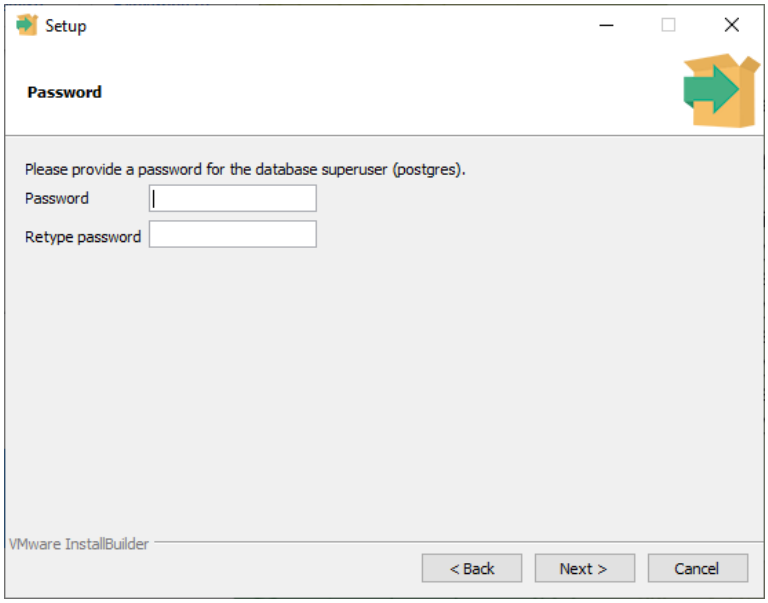
Шаг 4. Выберите устанавливаемые компоненты (рекомендуется оставить значения по умолчанию) → **Next**;



Шаг 5. Выберите каталог для размещения данных СУБД (рекомендуется оставить значение по умолчанию) → **Next**;

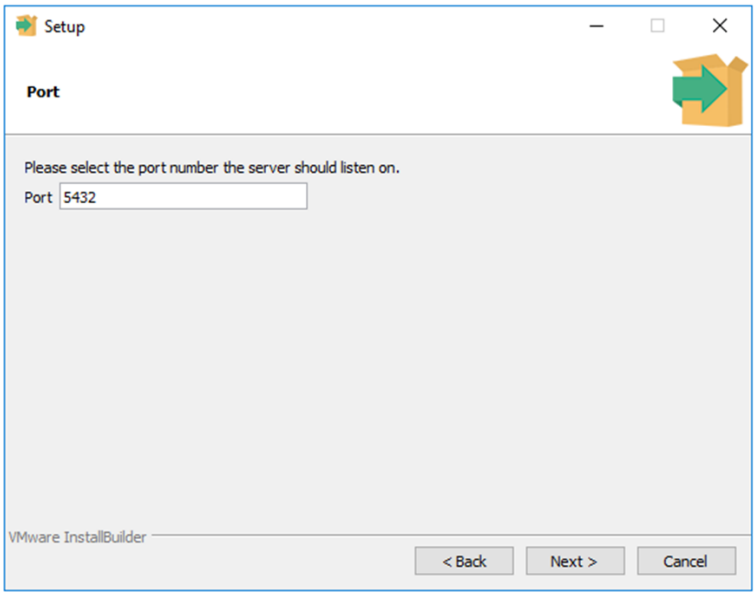


Шаг 6. Укажите пароль для администратора СУБД → **Next**;

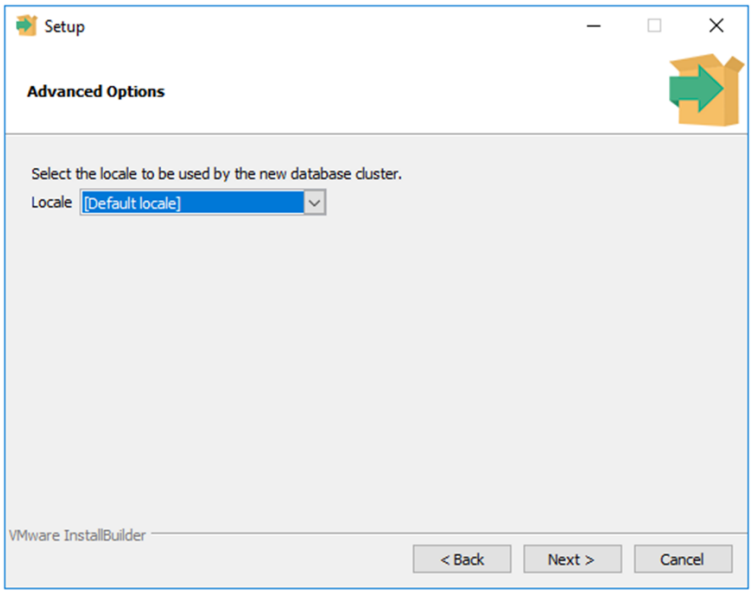


Администратором СУБД по умолчанию является учётная запись с именем **postgres**.

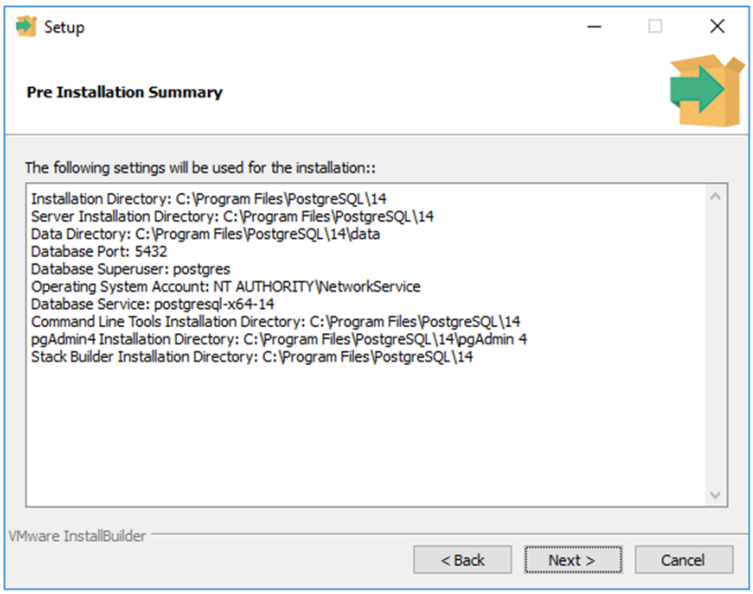
Шаг 7. Задайте порт для входящих подключений сервера СУБД (рекомендуется оставить по умолчанию) → **Next**;



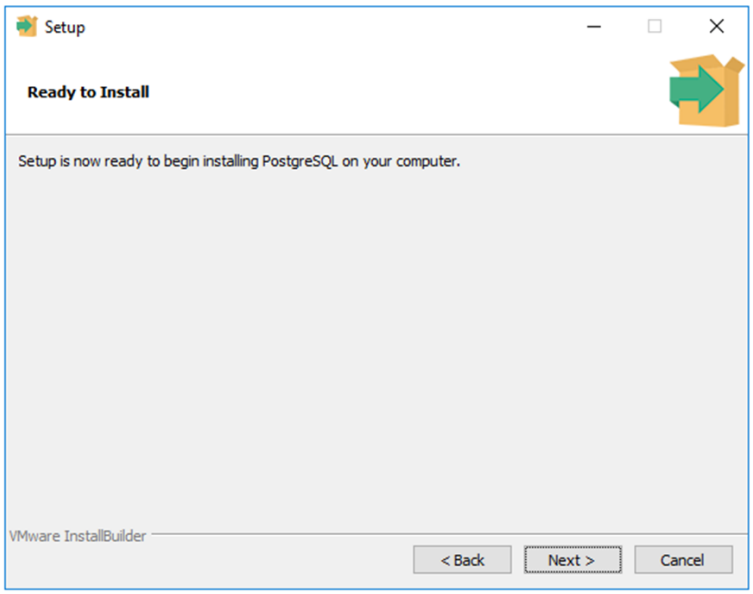
Шаг 8. Выберите настройки локализации (**locale**) для вновь создаваемых БД (рекомендуется оставить значение по умолчанию) → **Next**;



Шаг 9. Проверьте предварительные настройки инсталлятора → **Next**;

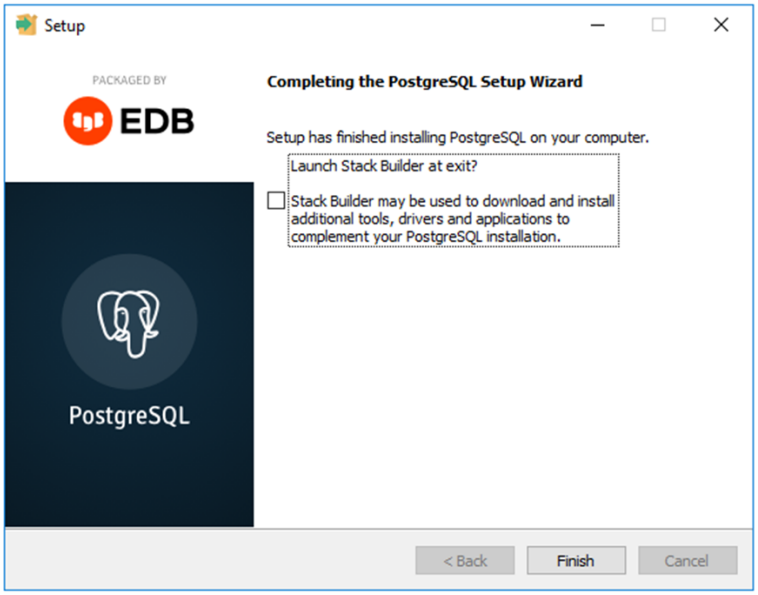


Шаг 10. Нажмите **Next**;

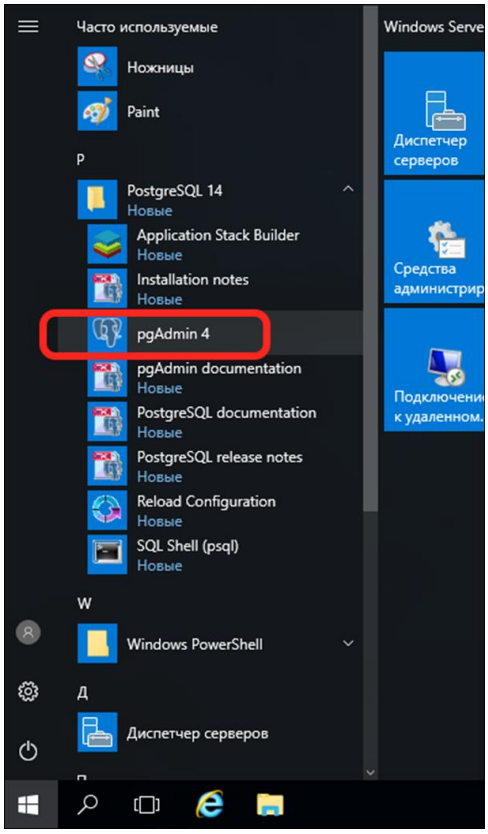


Будет запущен процесс инсталляции и запуска сервера СУБД.

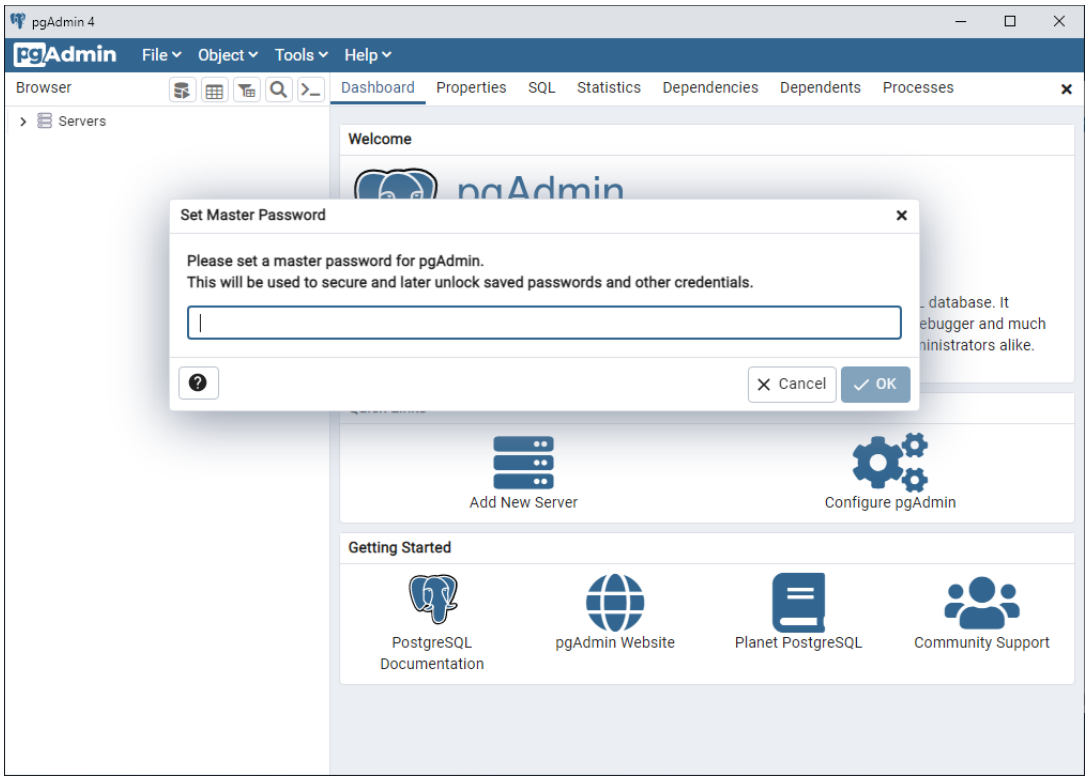
Шаг 11. Снимите отметку с **Launch Stack Builder...** → **Finish**;



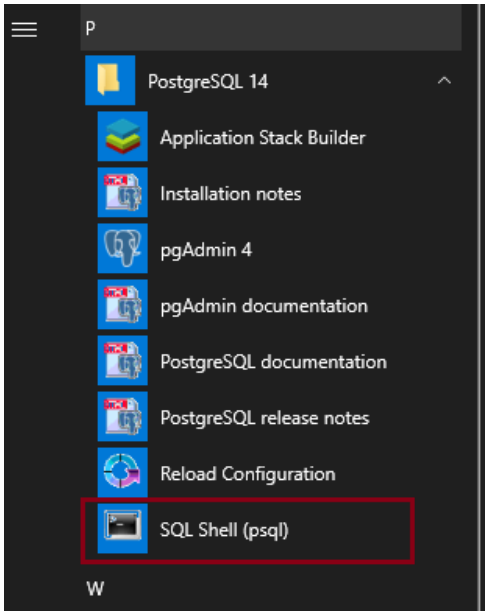
Шаг 12. После завершения инсталляции задайте мастер-пароль для консоли администратора СУБД **pgAdmin4**. **Пуск** → **PostgreSQL 14** → **pgAdmin4**;



Шаг 13. Введите нужный пароль → **OK**.

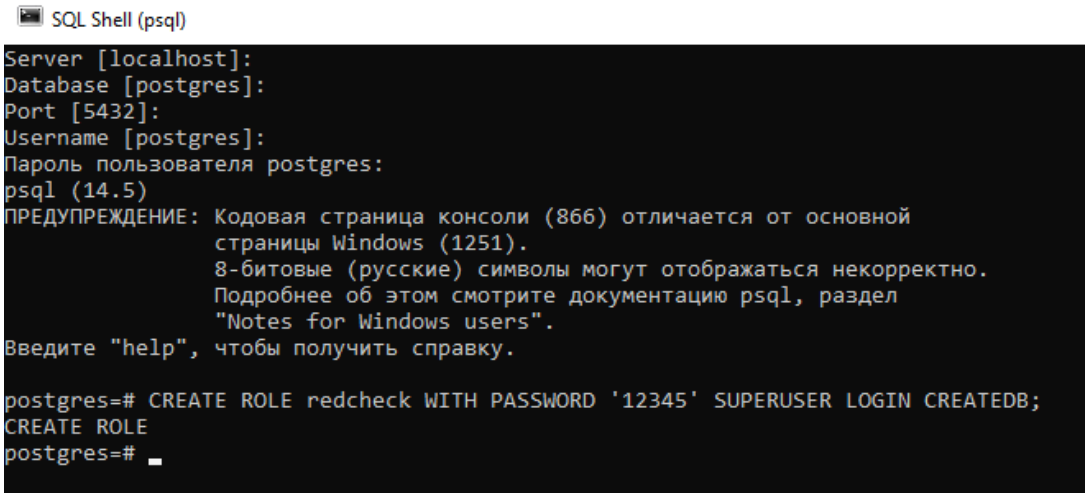


Шаг 14. Создайте пользователя для администрирования БД RedCheck. **Пуск** → **PostgreSQL 14** → **SQL Shell (psql)**;

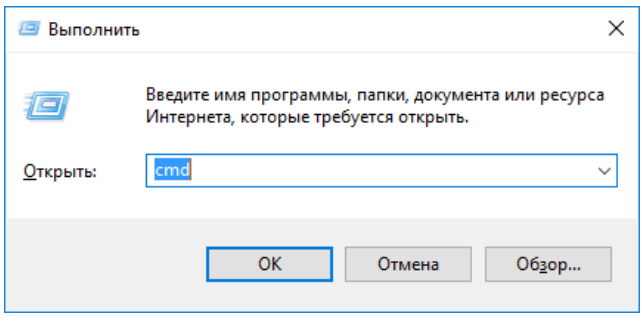


Шаг 15. Зайдите в консоль под суперпользователем postgres, пароль для которого указывается при установке СУБД. Введите команду:

```
PL/SQL

CREATE ROLE redcheck WITH PASSWORD 'пароль' SUPERUSER LOGIN CREATEDB;
```



Шаг 16. Откройте доступ по сети для хостов, на которых планируется установка REST-компонента и служб сканирования и синхронизации RedCheck.
Нажмите **Win + R** → введите **cmd**;



Шаг 17. В открывшемся окне введите команду:

Код

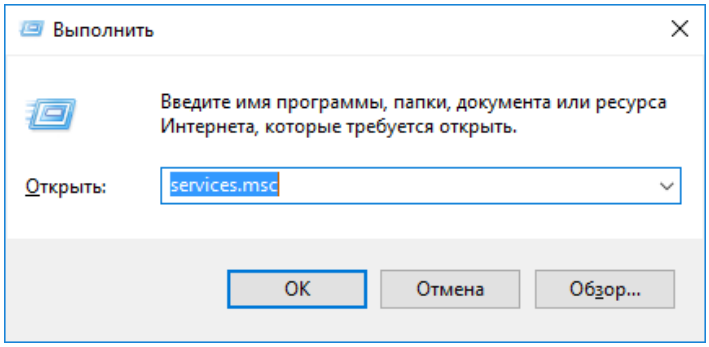
```
echo host <имя_базы_данных> <имя_пользователя_СУБД> <имя_сети/маска>
md5 >> "C:\Program Files\PostgreSQL\14\data\pg_hba.conf"
```

<имя_базы_данных> – имя базы данных, которая создается при установке RedCheck (по умолчанию RedCheck),
<имя_пользователя_СУБД> – имя созданного ранее пользователя,
<имя_сети/маска> – сеть или один адрес, которым разрешается доступ к СУБД. К примеру, 192.168.100.0/24 или 192.168.100.15/32;

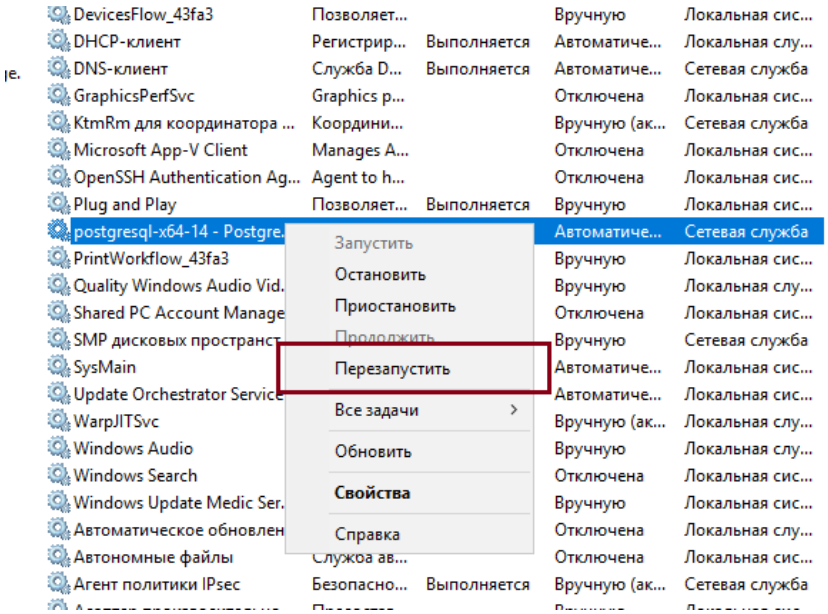
```
C:\Users\ydv>echo host RedCheck redcheck 192.168.1.0/24 md5 >> "C:\Program Files\PostgreSQL\14\data\pg_hba.conf"
```

Если база данных еще не создана, укажите вместо **RedCheck** значение **all**. После создания БД можно будет изменить этот параметр.

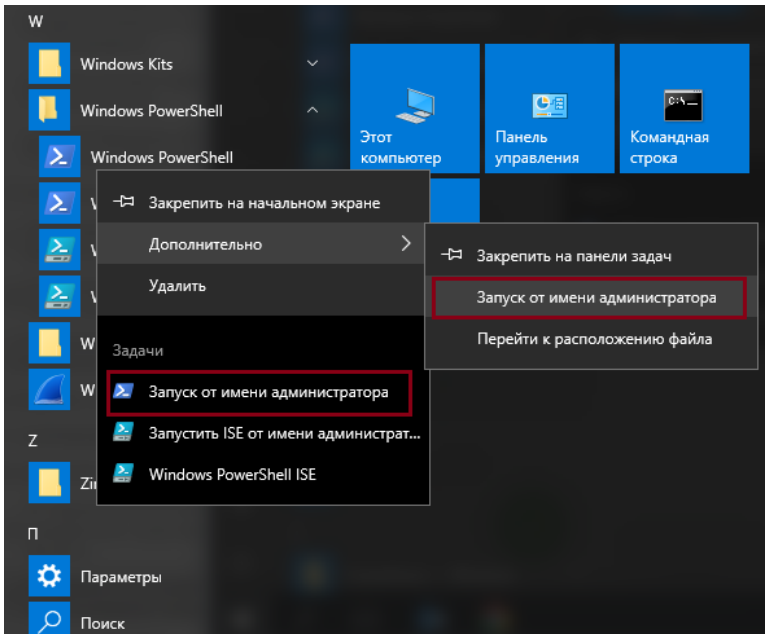
Шаг 18. Нажмите **Win + R** → введите **services.msc**;



Шаг 19. ПКМ по **postgresql-x64-14 - PostgreSQL Server 14 → Перезапустить**;



Шаг 20. Разрешите порт СУБД на межсетевом экране: **Пуск → Windows PowerShell** → ПКМ по **Windows PowerShell → Запуск от имени администратора**;



Шаг 21. Выполните следующую команду:

Код

```
netsh advfirewall firewall add rule name="PostgreSQL port" dir=in
action=allow protocol=TCP localport=5432
```

4.1.3 Установка СУБД PostgreSQL на Linux

Поддерживаемые версии СУБД PostgreSQL указаны в 3.2 Требования к программному обеспечению.

Далее приводятся инструкции по установке СУБД на примере PostgreSQl 14. Установка других версий производится аналогичным образом.

Содержание

4.1.3.1 Установка СУБД PostgreSQL на Astra Linux

Лог терминала находится в файле **~/.bash_history**. В случае возникновения ошибки создайте файл, содержащий лог, и обратитесь в службу [технической поддержки](#).

Bash (оболочка Unix)

```
sudo cat ~/.bash_history >>
/home/имя_пользователя/Загрузки/log.file
```

Установка СУБД PostgreSQL с репозитория Astra Linux

Добавьте официальный репозиторий Astra Linux для доступа к PostgreSQL 14. Для этого выполните следующие шаги:

Шаг 1. Откройте терминал комбинацией **Alt + T**;

Шаг 2. Войдите под root пользователем;

Bash (оболочка Unix)

```
sudo su
```

Перед подключением репозиториев необходимо установить дополнительные пакеты. Если у вас имеется образ с репозиторием Astra Linux, обновите пакеты, используя команду **apt update**, а затем проведите установку:

Bash (оболочка Unix)

```
apt install ca-certificates apt-transport-https
```

Шаг 3. Добавьте адреса дополнительного репозитория в файл **/etc/apt/source.list**:

Bash (оболочка Unix)

```
deb https://dl.astralinux.ru/astra/stable/1.7_x86-64/repository-extended/ 1.7_x86-64 astra-ce
```

Для добавления репозиториев в файл рекомендуем использовать текстовый редактор **nano**.

Шаг 1. Откройте файл с помощью команды (sudo) **nano /etc/apt/sources.list**

Шаг 2. Скопируйте репозитории и вставьте их с помощью комбинации **Ctrl + U (Shift + Insert** или **Правка → Вставить)**;

Шаг 3. Сохраните файл с помощью комбинации **Ctrl + O**;

Для выхода используйте **Ctrl + X**;

Шаг 4. Обновите пакеты;

Bash (оболочка Unix)

```
apt update
```

Шаг 5. Установите PostgreSQL;

Bash (оболочка Unix)

```
apt install -y postgresql
```

Настройка PostgreSQL

Шаг 1. Добавьте службу **postgresql** в автозапуск;

Bash (оболочка Unix)

```
systemctl enable postgresql
```

```
root@astra-db:/etc/apt# systemctl enable postgresql
Synchronizing state of postgresql.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable postgresql
```

Шаг 2. Создайте пользователя для администрирования СУБД;

PostgreSQL по умолчанию создает супер-пользователя **postgres**.

Bash (оболочка Unix)

```
sudo su postgres
psql -U postgres
```

Bash (оболочка Unix)

```
CREATE ROLE redcheck WITH PASSWORD '12345' LOGIN CREATEDB SUPERUSER;
\q
```

```
root@astra-db:/etc/apt# sudo su - postgres
postgres@astra-db:~$ psql -U postgres
psql (14.5 (Debian 14.5-1.pgdg90+1))
Введите "help", чтобы получить справку.

postgres=# CREATE ROLE redcheck WITH PASSWORD '12345' SUPERUSER LOGIN CREATEDB;
CREATE ROLE
postgres=# \q
postgres@astra-db:~$ exit
Выход
root@astra-db:/etc/apt#
```

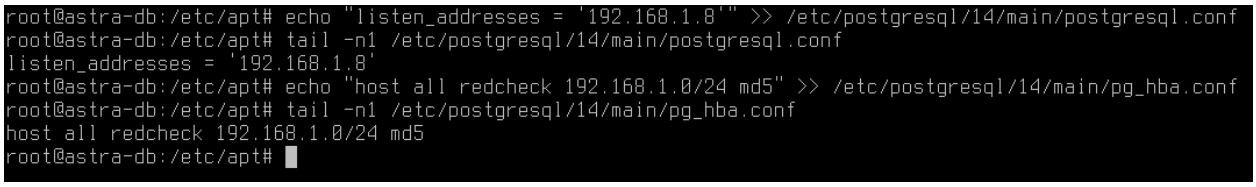
Шаг 3. Завершите сессию командой **exit**

Шаг 4. Откройте доступ по сети для серверов, на которых планируется установка REST-компонента и служб сканирования и синхронизации RedCheck;

Bash (оболочка Unix)

```
echo listen_addresses = 'ip_СУБД' >>
/etc/postgresql/14/main/postgresql.conf
echo host all имя_пользователя_СУБД имя_сети/маска md5 >>
/etc/postgresql/14/main/pg_hba.conf
```

ip_СУБД – IP-адреса хостов, на которых установлена СУБД, службы сканирования, служба синхронизации и серверный компонент RedCheck,
имя_базы_данных – имя базы данных, которая создается при установке RedCheck (по умолчанию RedCheck),
имя_пользователя_СУБД – имя созданного ранее пользователя,
имя_сети/маска – сеть или один адрес, которым разрешается доступ к СУБД. К примеру, 192.168.100.0/24 или 192.168.100.15/32;



Чтобы узнать ip-адрес устройства, используйте команду **ip address**.

Шаг 5. Перезапустите PostgreSQL.

Bash (оболочка Unix)

```
systemctl restart postgresql
```

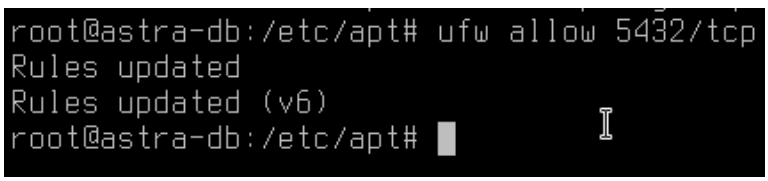
При необходимости разрешите доступ к сетевому порту postgresql. Для установки брандмауэра ufw используйте команду:

Bash (оболочка Unix)

```
apt install ufw
```

Bash (оболочка Unix)

```
ufw allow 5432/tcp
```



4.1.3.2 Установка СУБД PostgreSQL на BaseAlt

Лог терминала находится в файле **~/.bash_history**. В случае возникновения ошибки создайте файл, содержащий лог, и обратитесь в службу [технической поддержки](#).

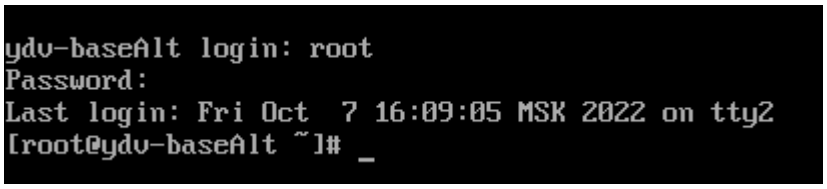
Bash (оболочка Unix)

```
sudo cat ~/.bash_history >>
/home/имя_пользователя/Загрузки/log.file
```

Установка PostgreSQL из репозитория «Сизиф»

Шаг 1. Откройте терминал комбинацией **Ctrl + Alt + F2**. Авторизуйтесь под **root**-пользователем;

Чтобы выйти из терминала, нажмите **Ctrl + Alt + F1**



Шаг 2. Выполните команды обновления пакетов и установки СУБД PostgreSQL;

Bash (Unix Shell)

```
apt-get update
```

Bash (Unix Shell)

```
apt-get install -y postgresql14 postgresql14-server postgresql14-
contrib
```

```
[root@ydv-baseAlt ~]# apt-get install -y postgresql14-contrib
Reading Package Lists... Done
Building Dependency Tree... Done
The following NEW packages will be installed:
  postgresql14-contrib
0 upgraded, 1 newly installed, 0 removed and 104 not upgraded.
Need to get 0B/605kB of archives.
After unpacking 2644kB of additional disk space will be used.
Committing changes...
Preparing...                          ################################################################################ [100%]
Updating / installing...
1: postgresql14-contrib-14.5-alt1     ################################################################################ [100%]
Done.
[root@ydv-baseAlt ~]# _
```

Шаг 3. Создайте системные базы данных;

Bash (оболочка Unix)

```
/etc/init.d/postgresql initdb
```

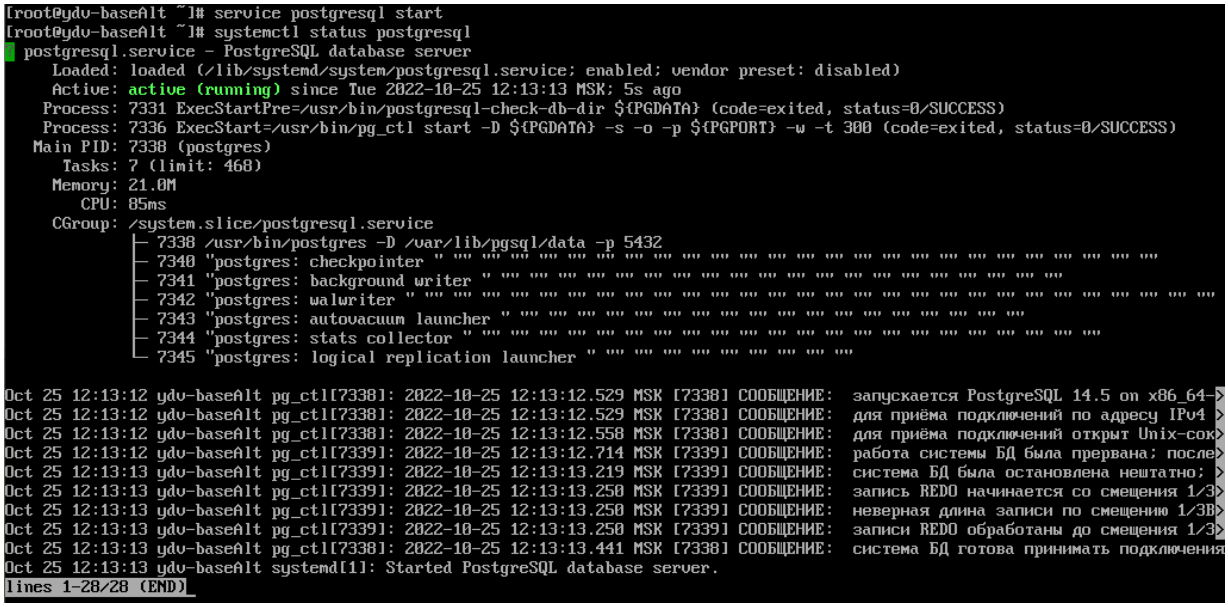
```
[root@ydv-baseAlt ~]# /etc/init.d/postgresql  initdb
Creating default database:
Файлы, относящиеся к этой СУБД, будут принадлежать пользователю "postgres".
От его имени также будет запускаться процесс сервера.

Кластер баз данных будет инициализирован с локалью "ru_RU.UTF-8".
Кодировка БД по умолчанию, выбранная в соответствии с настройками: "UTF8".
Выбрана конфигурация текстового поиска по умолчанию "russian".

Контроль целостности страниц данных отключён.

initdb: ошибка: каталог "/var/lib/pgsql/data" существует, но он не пуст
Если вы хотите создать новую систему баз данных,
удалите или очистите каталог "/var/lib/pgsql/data",
либо при запуске initdb в качестве пути укажите не "/var/lib/pgsql/data".
[root@ydv-baseAlt ~]#
```

Шаг 4. Запустите службы postgresql;

Bash (оболочка Unix)

```
service postgresql start
```

Чтобы посмотреть статус службы, используйте команду **systemctl status postgresql**



Шаг 5. Добавьте службу в автозагрузку;

Bash (оболочка Unix)

```
systemctl enable postgresql
```

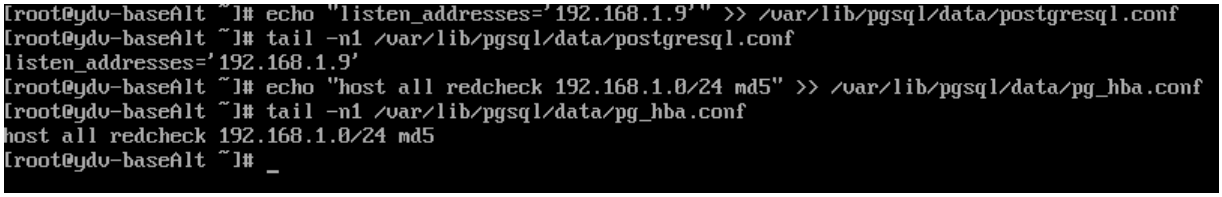
Настройка PostgreSQL

Шаг 6. Откройте доступ по сети для серверов, на которых планируется установка REST-компонента и служб сканирования и синхронизации RedCheck;

Bash (оболочка Unix)

```
echo “listen_addresses = ‘<ip_СУБД>’” >>
/var/lib/pgsql/data/postgresql.conf
echo “host all <имя_пользователя_СУБД> <имя_сети/маска> md5” >>
/var/lib/pgsql/data/pg_hba.conf
```

<ip_СУБД> – IP-адреса хостов, на которых установлена СУБД, службы сканирования, служба синхронизации и серверный компонент RedCheck,
<имя_базы_данных> – имя базы данных, которая создается при установке RedCheck (по умолчанию RedCheck),
<имя_пользователя_СУБД> – имя созданного ранее пользователя,
<имя_сети/маска> – сеть или один адрес, которым разрешается доступ к СУБД. К примеру, 192.168.100.0/24 или 192.168.100.15/32;



Чтобы узнать ip-адрес устройства, используйте команду **ip address**.

Шаг 7. Перезагрузите службу PostgreSQL;

Bash (оболочка Unix)

```
service postgresql restart
```

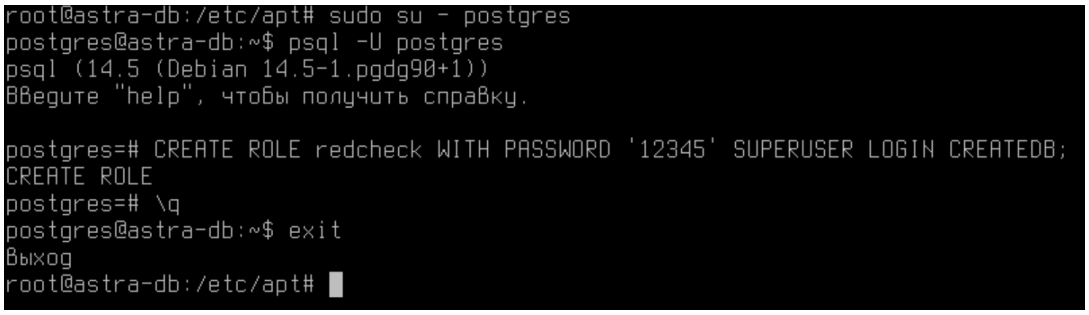
Шаг 8. Создайте пользователя для администрирования БД;

Bash (оболочка Unix)

```
psql -U postgres
```

Bash (оболочка Unix)

```
CREATE ROLE redcheck WITH PASSWORD '12345' LOGIN CREATEDB SUPERUSER;
\q
```

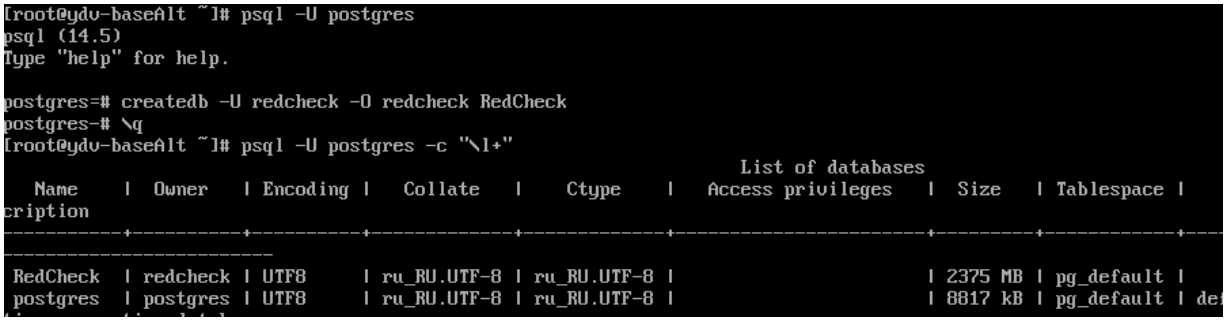


Шаг 9. Создайте базу данных для работы в RedCheck;

Создание базы данных заранее актуально только при установке СУБД на BaseALT. Для остальных Linux дистрибутивов шаги 9-10 рекомендуется пропустить.
Если же в процессе установки компонентов RedCheck происходит ошибка во время подключения к базе данных, шаги 9-10 обязательны для выполнения.

Bash (оболочка Unix)

```
createdb -U имя_пользователя -O имя_пользователя имя_БД
```



Шаг 10. Зайдите в базу данных RedCheck, чтобы установить расширение для шифрования **pgcrypto**;

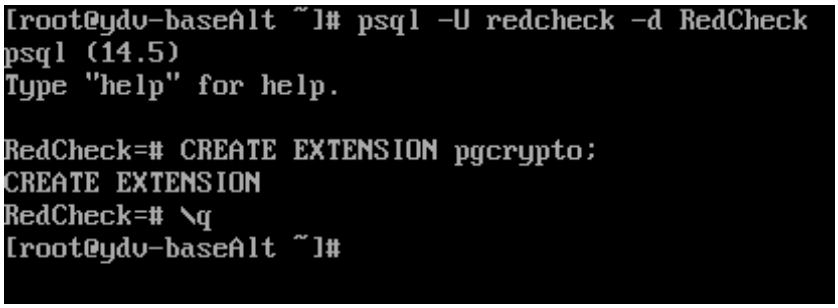
Bash (оболочка Unix)

```
psql -U redcheck -d RedCheck
```

PL/SQL

```
CREATE EXTENSION IF NOT EXISTS pgcrypto;
```

Созданная вручную БД пустая. В таком случае на шаге создания БД при установке RedCheck необходимо будет отметить поле **Очистить базу данных**.



Шаг 11. Перезапустите PostgreSQL;

Bash (оболочка Unix)

```
service postgresql restart
```

4.1.3.3 Установка СУБД PostgreSQL на Debian

Лог терминала находится в файле **~/.bash_history**. В случае возникновения ошибки создайте файл, содержащий лог, и обратитесь в службу [технической поддержки](#).

Bash (оболочка Unix)

```
sudo cat ~/.bash_history >>
/home/имя_пользователя/Загрузки/log.file
```

Установка СУБД PostgreSQL

Добавьте официальный репозиторий PostgreSQL. Для этого выполните следующие шаги:

Шаг 1. Войдите под root пользователем:

Bash (оболочка Unix)

```
su
```

Шаг 2. Откройте терминал и выполните следующие команды;

Bash (оболочка Unix)

```
apt install curl ca-certificates
```

Bash (оболочка Unix)

```
install -d /usr/share/postgresql-common/pgdg
```

Bash (оболочка Unix)

```
curl -o /usr/share/postgresql-common/pgdg/apt.postgresql.org.asc --
fail https://www.postgresql.org/media/keys/ACCC4CF8.asc
```

Bash (оболочка Unix)

```
sh -c 'echo "deb [signed-by=/usr/share/postgresql-
common/pgdg/apt.postgresql.org.asc]
https://apt.postgresql.org/pub/repos/apt $(lsb_release -cs)-pgdg
main" > /etc/apt/sources.list.d/pgdg.list'
```

Шаг 3. Обновите пакеты;

Bash (оболочка Unix)

```
apt update
```

Шаг 4. Установите PostgreSQL 14 или любой другой версии;

Bash (оболочка Unix)

```
apt -y install postgresql-14
```

Настройка PostgreSQL

Шаг 4. Добавьте службу **postgresql** в автозапуск;

Bash (оболочка Unix)

```
systemctl enable postgresql
```

```
root@astra-db:/etc/apt# systemctl enable postgresql
Synchronizing state of postgresql.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable postgresql
```

Шаг 5. Создайте пользователя для администрирования СУБД;

PostgreSQL по умолчанию создает супер-пользователя **postgres**.

Bash (оболочка Unix)

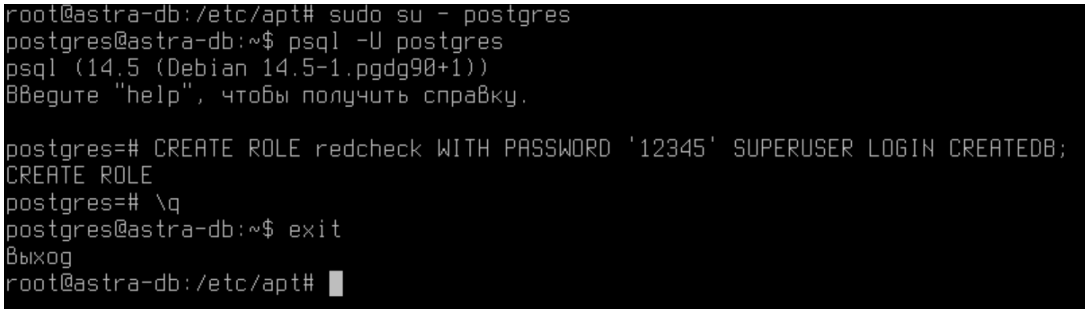
```
su postgres
```

Bash (оболочка Unix)

```
psql -U postgres
```

Bash (оболочка Unix)

```
CREATE ROLE redcheck WITH PASSWORD '12345' LOGIN CREATEDB SUPERUSER;
```



Для выхода из базы данных postgres введите **\q**

Шаг 6. Завершите сессию командой **exit**

Шаг 7. Откройте доступ по сети для серверов, на которых планируется установка REST-компонента и служб сканирования и синхронизации RedCheck;

Bash (оболочка Unix)

```
echo "listen_addresses = 'ip_СУБД'" >>
/etc/postgresql/14/main/postgresql.conf
```

Bash (оболочка Unix)

```
echo host all имя_пользователя_СУБД имя_сети/маска md5 >>
/etc/postgresql/14/main/pg_hba.conf
```

ip_СУБД – IP-адреса хостов, на которых установлена СУБД, службы сканирования, служба синхронизации и серверный компонент RedCheck,
имя_базы_данных – имя базы данных, которая создается при установке RedCheck (по умолчанию RedCheck),
имя_пользователя_СУБД – имя созданного ранее пользователя,
имя_сети/маска – сеть или один адрес, которым разрешается доступ к СУБД. К примеру, 192.168.100.0/24 или 192.168.100.15/32;

```
root@astra-db:/etc/apt# echo "listen_addresses = '192.168.1.8'" >> /etc/postgresql/14/main/postgresql.conf
root@astra-db:/etc/apt# tail -n1 /etc/postgresql/14/main/postgresql.conf
listen_addresses = '192.168.1.8'
root@astra-db:/etc/apt# echo "host all redcheck 192.168.1.0/24 md5" >> /etc/postgresql/14/main/pg_hba.conf
root@astra-db:/etc/apt# tail -n1 /etc/postgresql/14/main/pg_hba.conf
host all redcheck 192.168.1.0/24 md5
root@astra-db:/etc/apt#
```

Чтобы узнать ip-адрес устройства, используйте команду **ip a**

Шаг 8. Перезапустите PostgreSQL.

Bash (оболочка Unix)

```
systemctl restart postgresql
```

Чтобы проверить работоспособность СУБД, используйте команду:

Bash (оболочка Unix)

```
systemctl status postgresql
```

При необходимости разрешите доступ к сетевому порту postgresql. Для установки брандмауэра ufw используйте команду:

Bash (оболочка Unix)

```
apt install ufw
```

Bash (оболочка Unix)

```
ufw allow 5432/tcp
```

```
root@astra-db:/etc/apt# ufw allow 5432/tcp
Rules updated
Rules updated (v6)
root@astra-db:/etc/apt#
```

4.2 Установка Desktop-версии

Перед установкой ознакомьтесь с различиями между Desktop и Web версией RedCheck, а также с ролевой моделью Системы.

Перечень инсталляционных пакетов для установки RedCheck подлежащих добавлению в списки исключений средств защиты (антивирусов), используемых в сети предприятия:

Инсталляционные пакеты
Обязательные пакеты
RedCheck-....msi
Дополнительные пакеты
RedCheckAgent-...-x64.msi
RedCheckAgent-...-x86.msi
RedCheckUpdateAgent-...-x64.msi
RedCheckUpdateAgent-...-x86.msi
WsusKit-.....msi

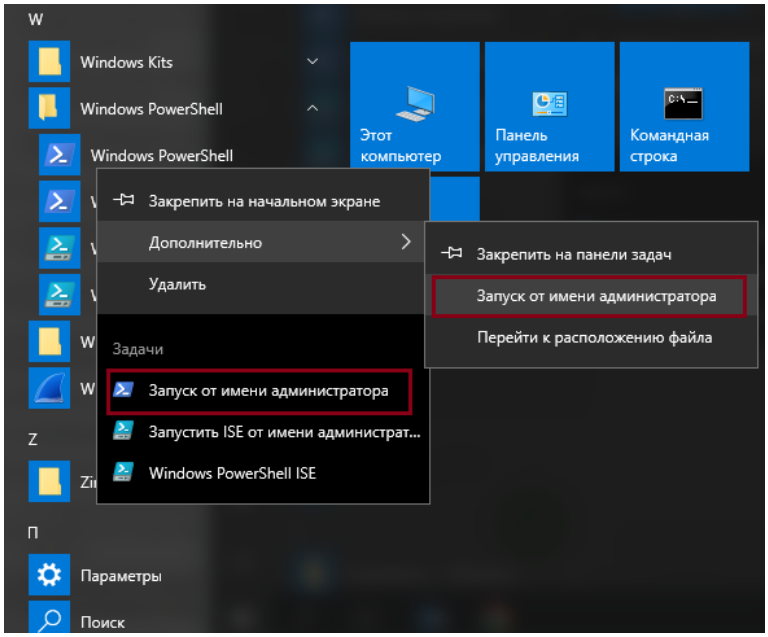
Рекомендуется внести исключения в средства защиты, чтобы устранить влияние СЗИ на установку.

Содержание

4.2.1 Установка Microsoft .NET Framework

Проверка имеющихся версий Microsoft .NET Framework 4.8 на хосте

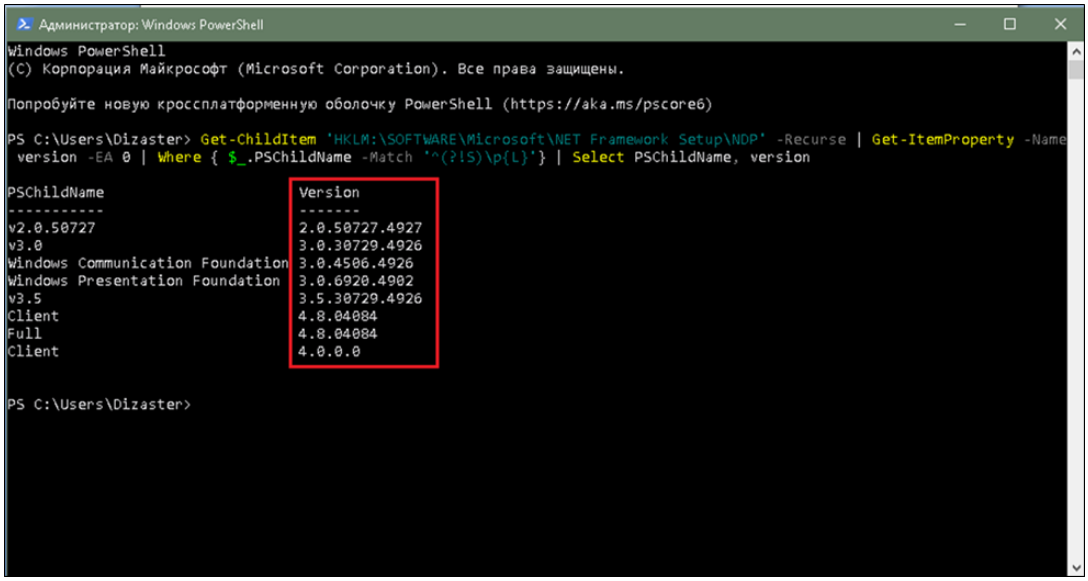
Шаг 1. Запустите консоль PowerShell. **Пуск → Windows PowerShell → Windows PowerShell**;



Шаг 2. В появившемся окне введите команду:

Код

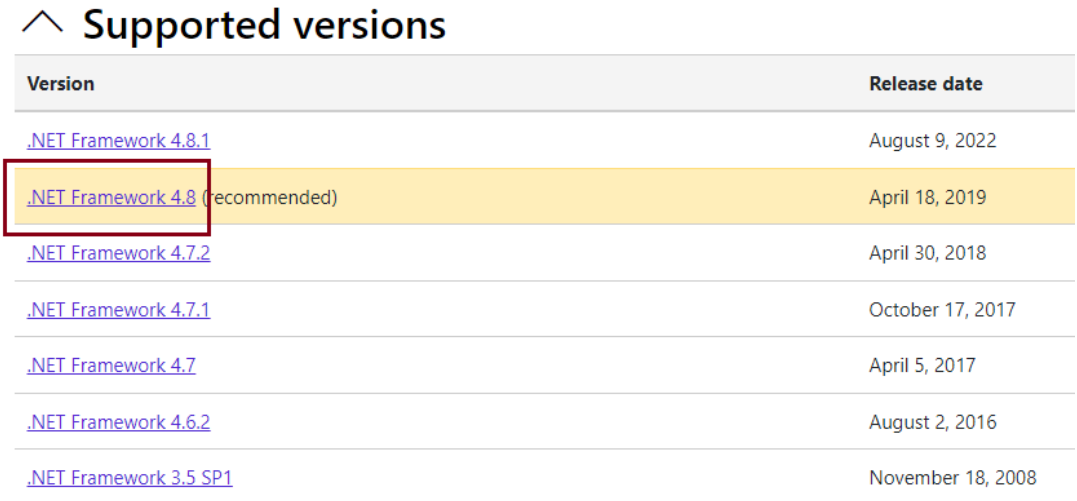
```
Get-ChildItem 'HKLM:\SOFTWARE\Microsoft\NET Framework Setup\NDP' -
Recurse | Get-ItemProperty -Name version -EA 0 | Where {
$_.PSChildName -Match '^(?!S)\p{L}'} | Select PSChildName, version
```



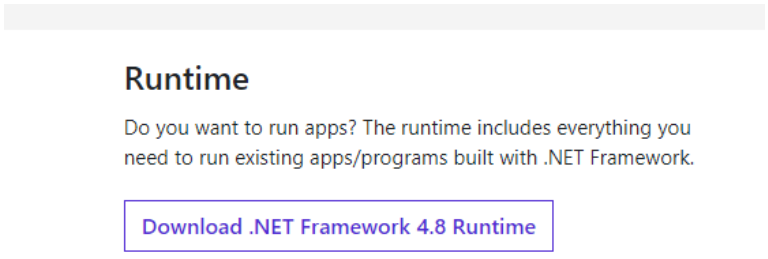
В окне отобразится список установленных версий Microsoft .Net Framework.

Загрузка инсталлятора

Шаг 1. Перейдите на страницу загрузки с сайта разработчика и выберите из списка дистрибутив необходимой версии;

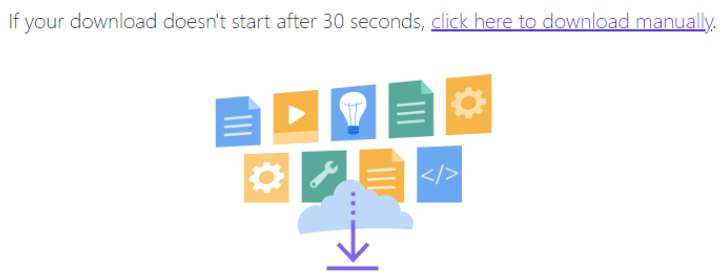


Шаг 2. Нажмите **Download .Net Framework Runtime**;



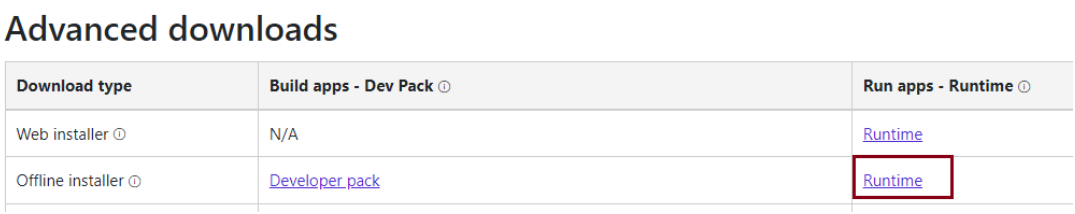
Шаг 3. Откроется страница загрузки выбранного дистрибутива. Дождитесь окончания загрузки.

Если процесс загрузки не начался автоматически, нажмите **click here to download manual**.



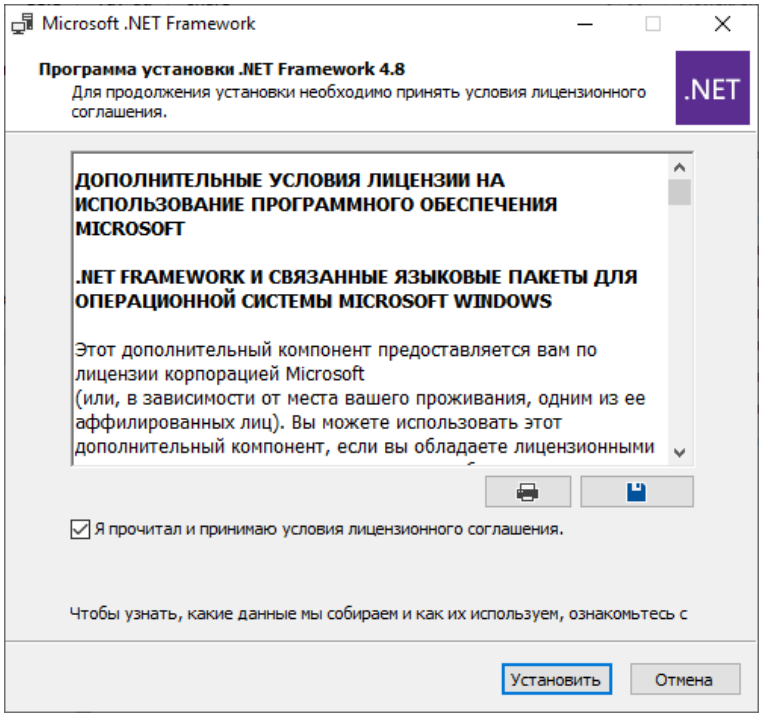
По умолчанию загружается онлайн-дистрибутив, для установки которого требуется доступ к сети Интернет.

Если доступа к сети нет, после выбора версии Microsoft .NET Framework найдите в таблице **Advanced downloads** строку **Offline installer** → **Runtime**.



Установка Microsoft .NET Framework

Шаг 1. Запустите инсталляционный пакет. В открывшемся окне согласитесь с лицензионным соглашением → **Установить**;



Шаг 2. Дождитесь окончания установки и перезагрузите компьютер.

4.2.2 Установка RedCheck

При обновлении RedCheck **обязательно** сделайте резервную копию БД (5.8 Резервное копирование и восстановление).

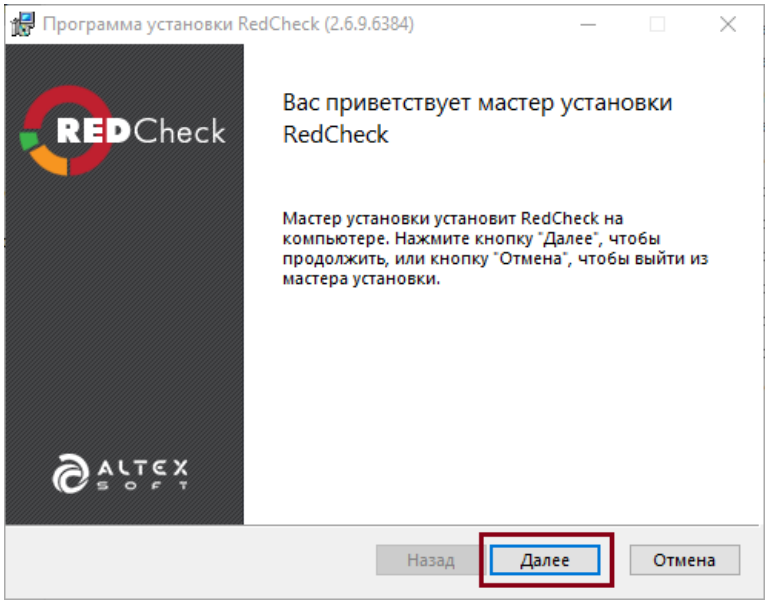
Перед установкой убедитесь, что на компьютере есть необходимые компоненты:

- СУБД (4.1 Установка СУБД);
- Microsoft .NET Framework 4.8 (4.2.1 Установка Microsoft .NET Framework);

Установка посторонних компонентов может мешать работе Системы.

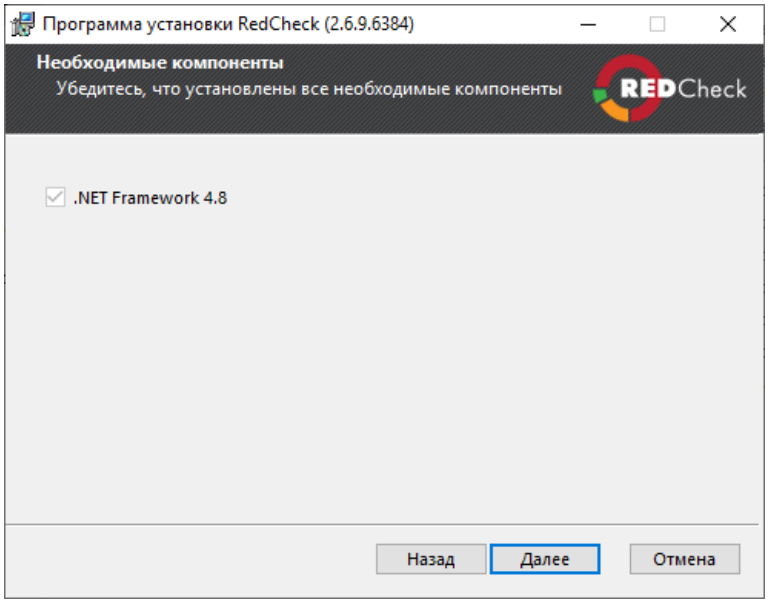
Возможна автоматическая установка через командную строку (4.6.1 Параметры установки Desktop-версии).

Шаг 1. Запустите инсталляционный пакет RedCheck.msi → **Далее**;

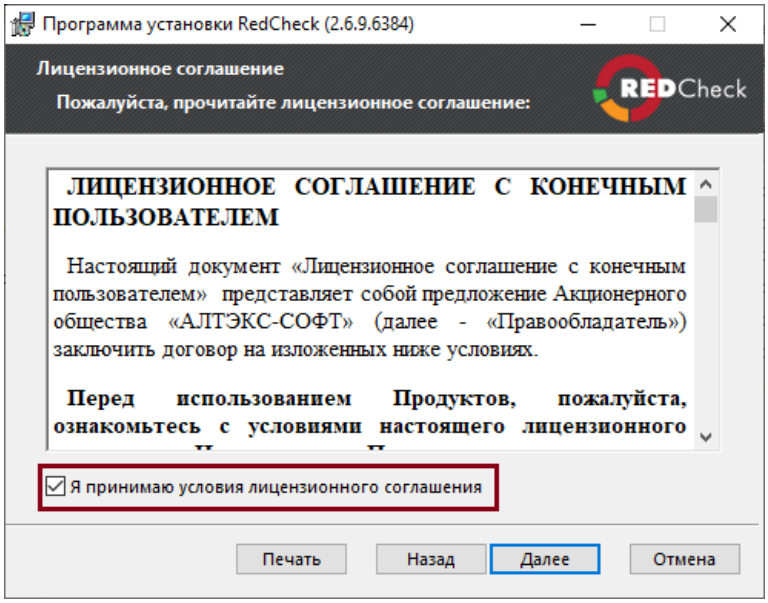


Если установка производится в домене, запускать установочный пакет необходимо от имени пользователя, который обладает правами на создание БД. **Shift + ПКМ → Запустить от имени другого пользователя** → введите учетные данные.

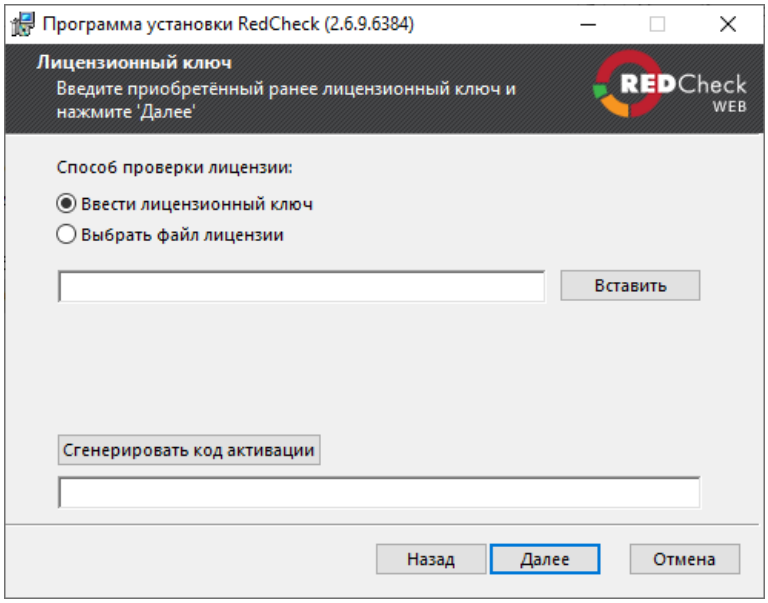
Шаг 2. Будет выполнена проверка наличия необходимых компонентов → **Далее**;



Шаг 3. Примите лицензионное соглашение, отметив соответствующее поле → **Далее**;

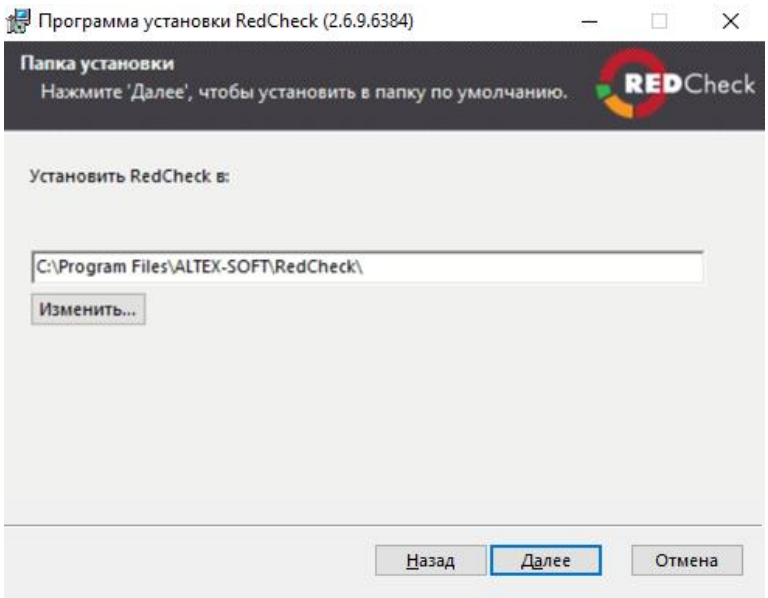


Шаг 4. Введите лицензионный ключ → **Далее**;

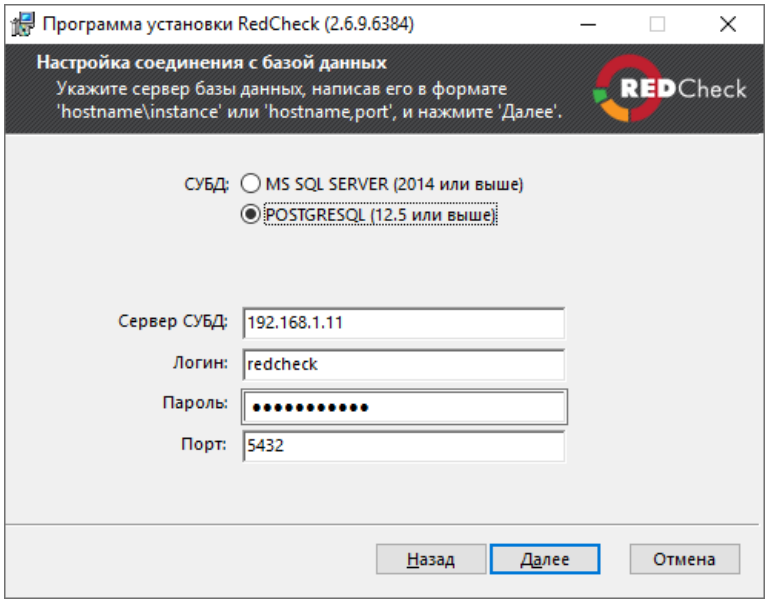


При отсутствии доступа к сети Интернет необходимо получить файл лицензии и указать способ проверки **Выбрать файл лицензии** (5.2 Активация лицензии, с 1 по 5 шаг).

Шаг 5. Укажите директорию для RedCheck → **Далее**;

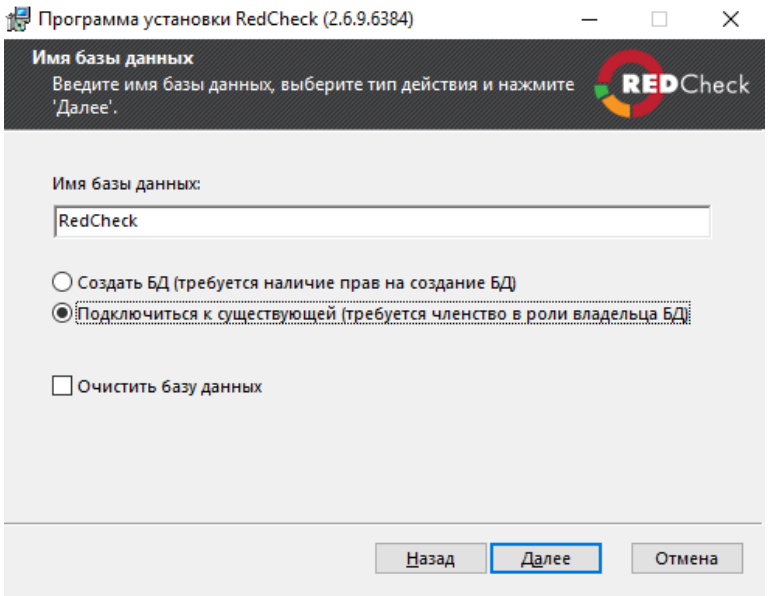


Шаг 6. Введите параметры для подключения к СУБД → **Далее**;



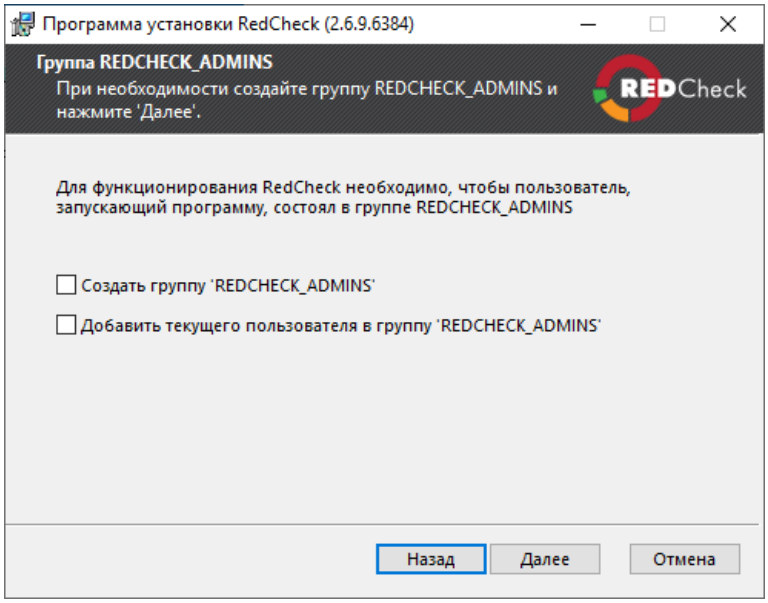
Сервер СУБД: имя узла/IP-адрес, на котором находится сервер СУБД;
Логин: имя пользователя с правами на создание БД. Данный пользователь будет владельцем БД RedCheck;
Пароль: пароль указанного пользователя;
Порт: сетевой порт для сервера СУБД (по умолчанию для Microsoft SQL Server - 1433, для PostgreSQL - 5432);

Шаг 7. Укажите имя БД (RedCheck по умолчанию) → **Далее**;



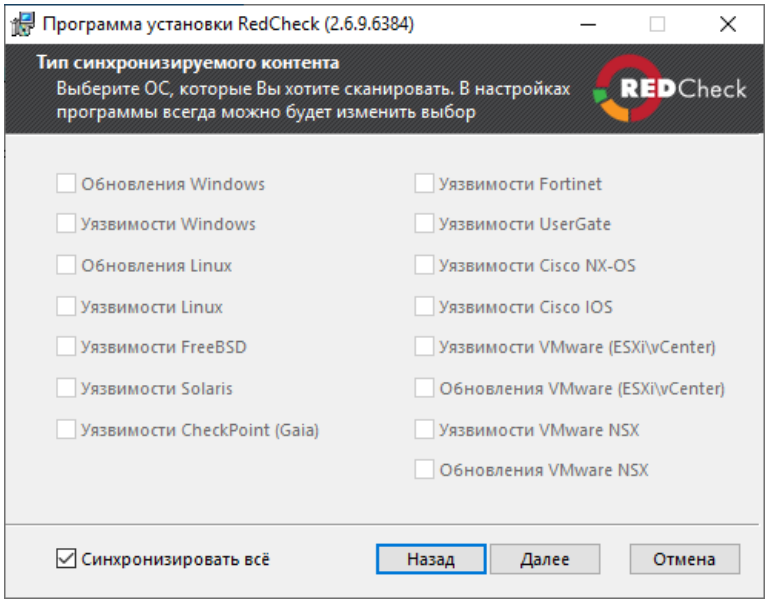
Если БД уже существует, выберите **Подключиться к существующей...**. При необходимости отметьте **Очистить базу данных** (Если СУБД развернута на BaseAlt, поле должно быть отмечено обязательно).

Шаг 8. Если указанный пользователь не был ранее добавлен в группу безопасности REDCHECK_ADMINS, выберите **Добавить текущего...**. В случае, если такая группа безопасности отсутствует на хосте, отметьте **Создать группу...** → **Далее**;

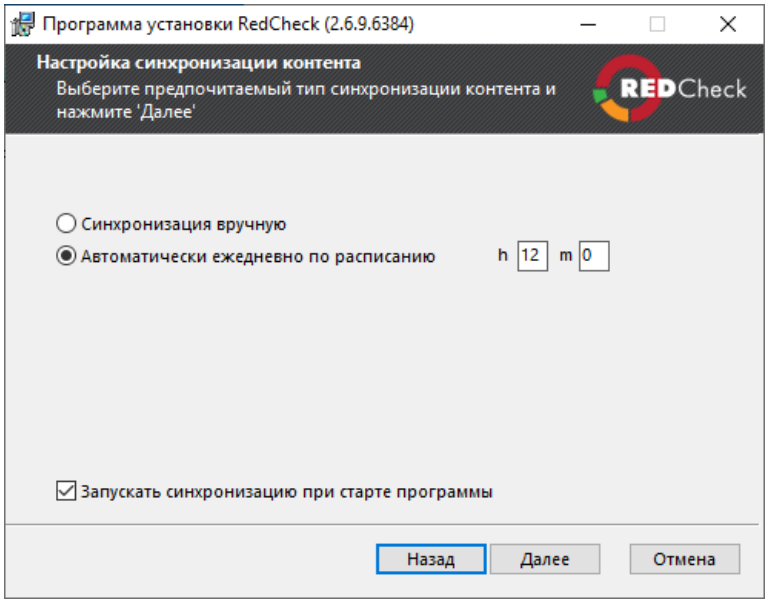


На этом шаге создаётся локальная группа. Доменные группы имеют приоритет над локальными. Создания групп в домене описано в 5.1.2 Создание групп безопасности для Windows аутентификации.

Шаг 9. Укажите необходимый для синхронизации контент безопасности → **Далее**;



Шаг 10. Настройте параметры синхронизации (рекомендуется оставить значения по умолчанию **Автоматически...**) → **Далее**;



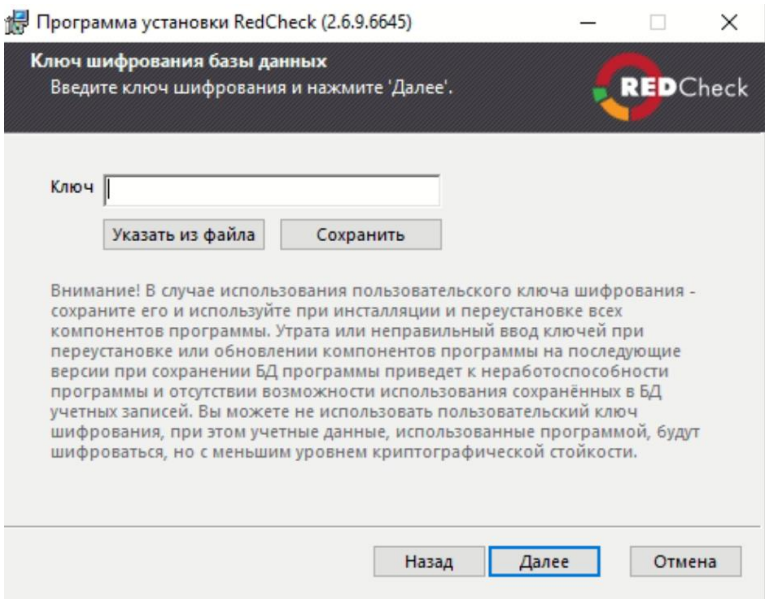
Шаг 11. Укажите ключ шифрования → **Далее**;

Ключ шифрования используется для шифрования учетных записей RedCheck для сканирования.

Нажмите **Указать из файла** (с расширением .xml), чтобы использовать уже имеющийся ключ шифрования.

Нажмите **Сохранить** для записи ключа в файл с расширением .xml. В поле **sckd** указан ключ шифрования.

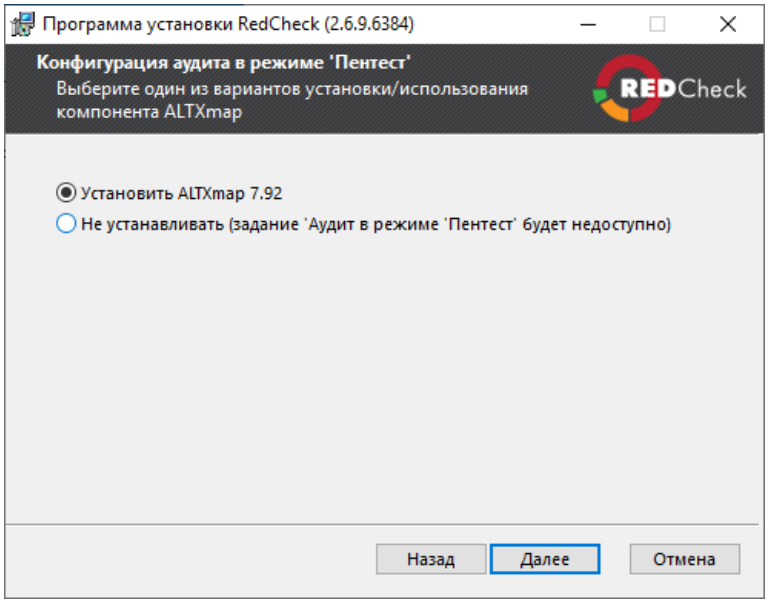
```
<?xml version="1.0" encoding="utf-8"?>
<sckd>N2v#kAp4</sckd>
```



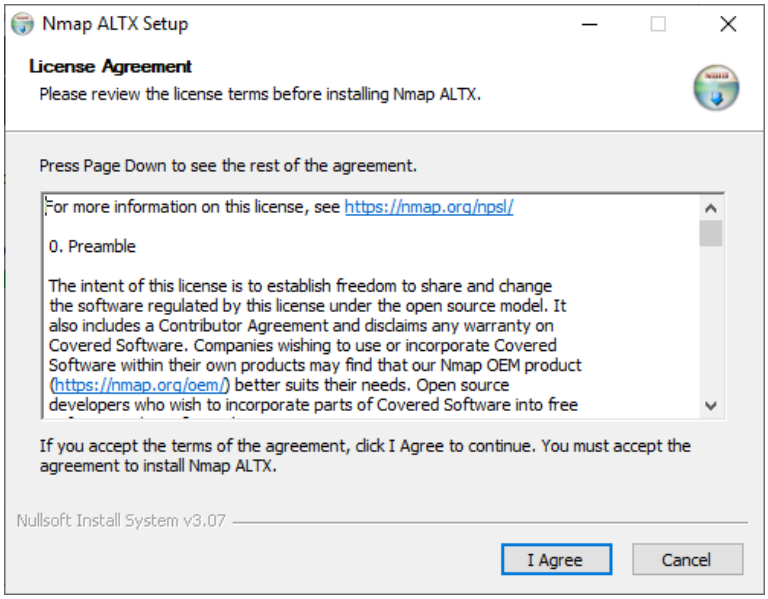
Если не указывать ключ шифрования, учетные записи RedCheck для сканирования все равно будут зашифрованы, но с меньшим уровнем криптографической стойкости.

Desktop-версия RedCheck **не позволяет сменить ключ шифрования в дальнейшем.**

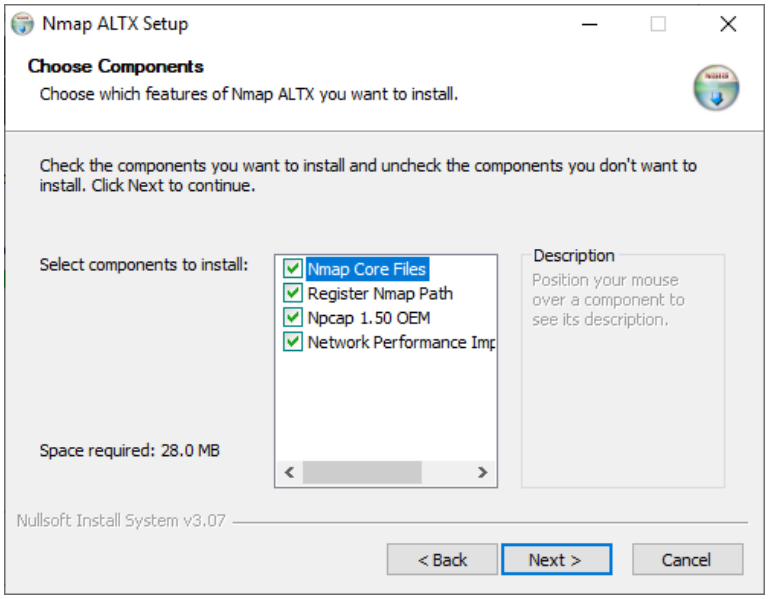
Шаг 12 . Отметьте при необходимости **Установить ALTXMAP** → **Далее** → **Установить**.



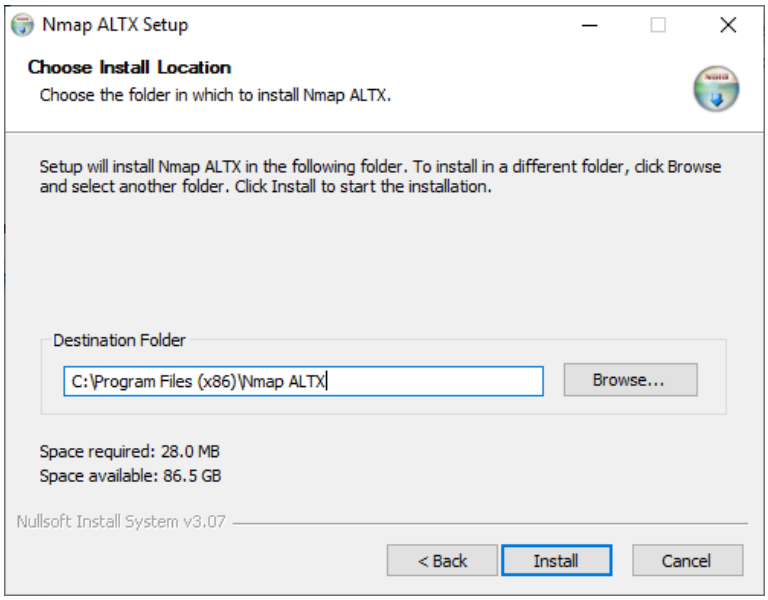
Шаг 13. Во время установки откроется дополнительный инсталлятор Nmap ALTX → **I Agree**;



Шаг 14. Выберите устанавливаемые компоненты (рекомендуется оставить значения по умолчанию) → **Next**;



Шаг 15. Укажите директорию для установки → **Install**;



Шаг 16. Дождитесь окончания установки всех компонентов и перезагрузите компьютер;

4.3 Установка Web-версии

Установка и настройка основных компонентов программы должна производится в последовательности, указанной в данном руководстве.

Перечень инсталляционных пакетов для установки RedCheck подлежащих добавлению в списки исключений средств защиты (антивирусов), используемых в сети предприятия:

Инсталляционные пакеты
Обязательные пакеты
RedCheckWebRest-....msi
RedCheckWebClient-....msi
RedCheckSyncService-....msi
RedCheckScanService-....msi
Дополнительные пакеты
RedCheckAgent-...-x64.msi
RedCheckAgent-...-x86.msi
RedCheckUpdateAgent-...-x64.msi
RedCheckUpdateAgent-...-x86.msi

Рекомендуется внести исключения в средства защиты, чтобы устранить влияние СЗИ на установку.

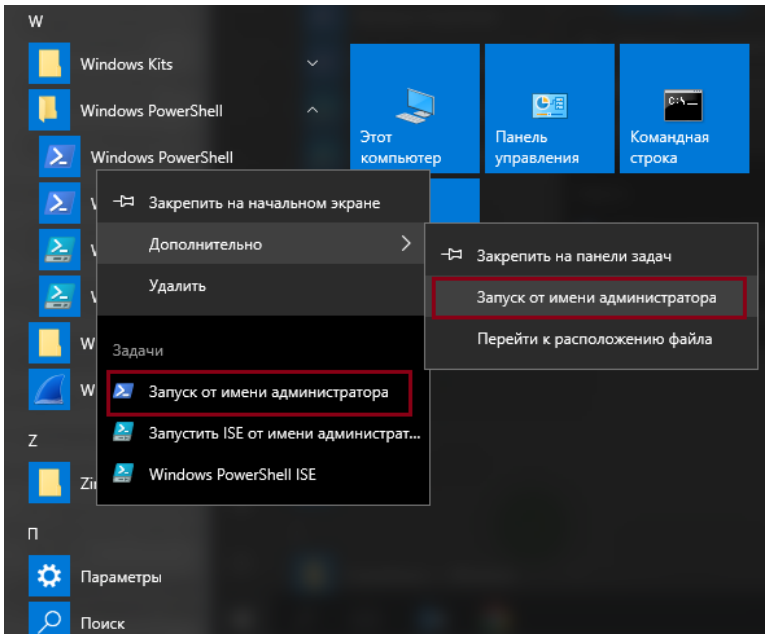
Содержание

4.3.1 Установка Web-сервера IIS

RedCheckWeb для взаимодействия между компонентами на ОС Microsoft WIndows использует web-сервер IIS.

Установка IIS через консоль

Шаг 1. Пуск → **Windows PowerShell** → ПКМ по **Windows PowerShell** → **Запуск от имени администратора**;



Шаг 2. Введите следующую команду:

Код

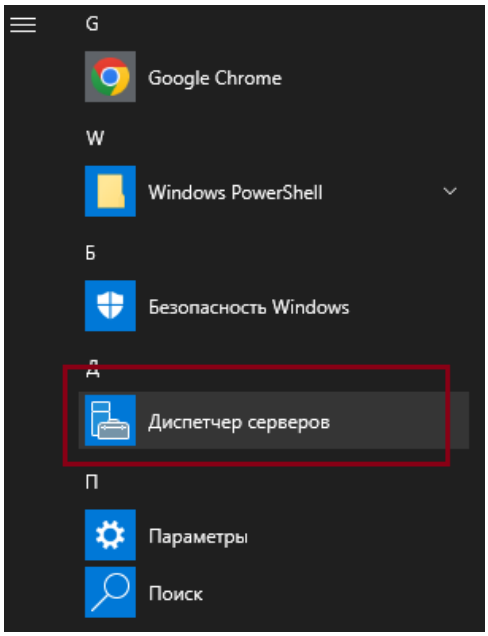
```
Install-WindowsFeature -Name Web-Server, Web-Mgmt-Console, Web-ASP,
Web-Asp-Net45, Web-ISAPI-Ext, Web-Net-Ext45, Web-ISAPI-Filter, Web-
Windows-Auth
```

```
Windows PowerShell
(C) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.

PS C:\Windows\system32> Install-WindowsFeature -Name Web-Server, Web-Mgmt-Console, Web-ASP, Web-Asp-Net45, Web-ISAPI-Ext
, Web-Net-Ext45, Web-ISAPI-Filter, Web-Windows-Auth

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    Yes            SuccessRest... {Разработка приложений, ASP, ASP.NET 4.7, ...
ПРЕДУПРЕЖДЕНИЕ: Чтобы завершить установку, вам необходимо перезапустить этот сервер.
```

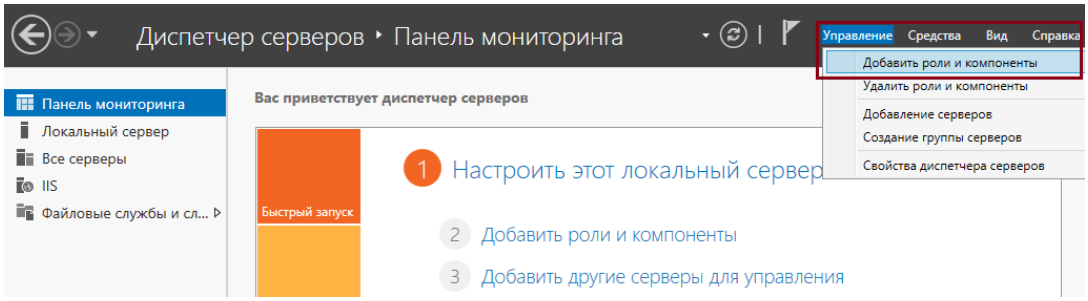
Шаг 3. Перезагрузите компьютер.

Графическая установка IIS

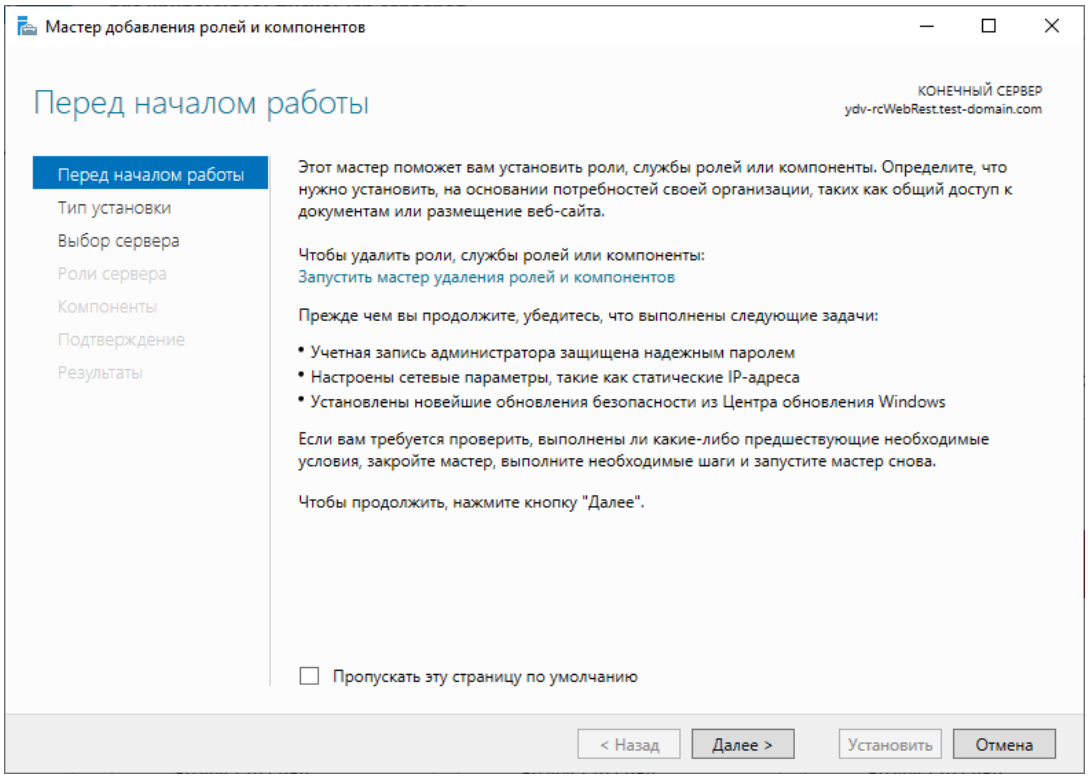
Шаг 1. Пуск → Диспетчер серверов;



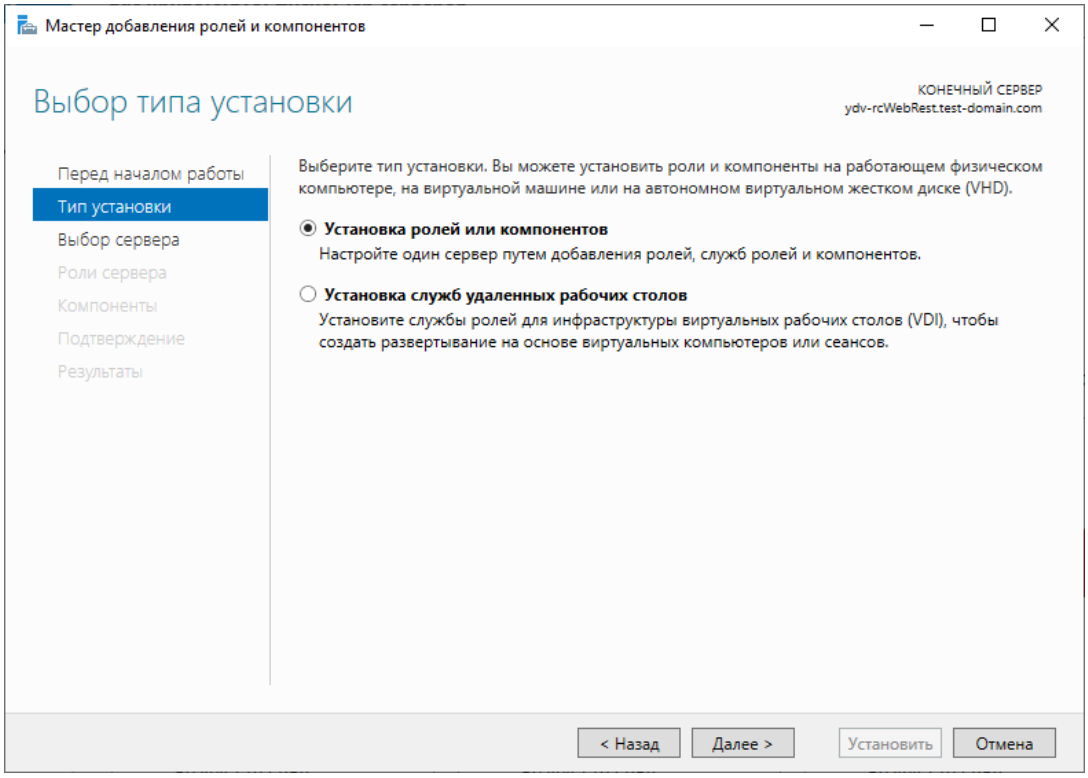
Шаг 2. Управление → Добавить роли и компоненты;



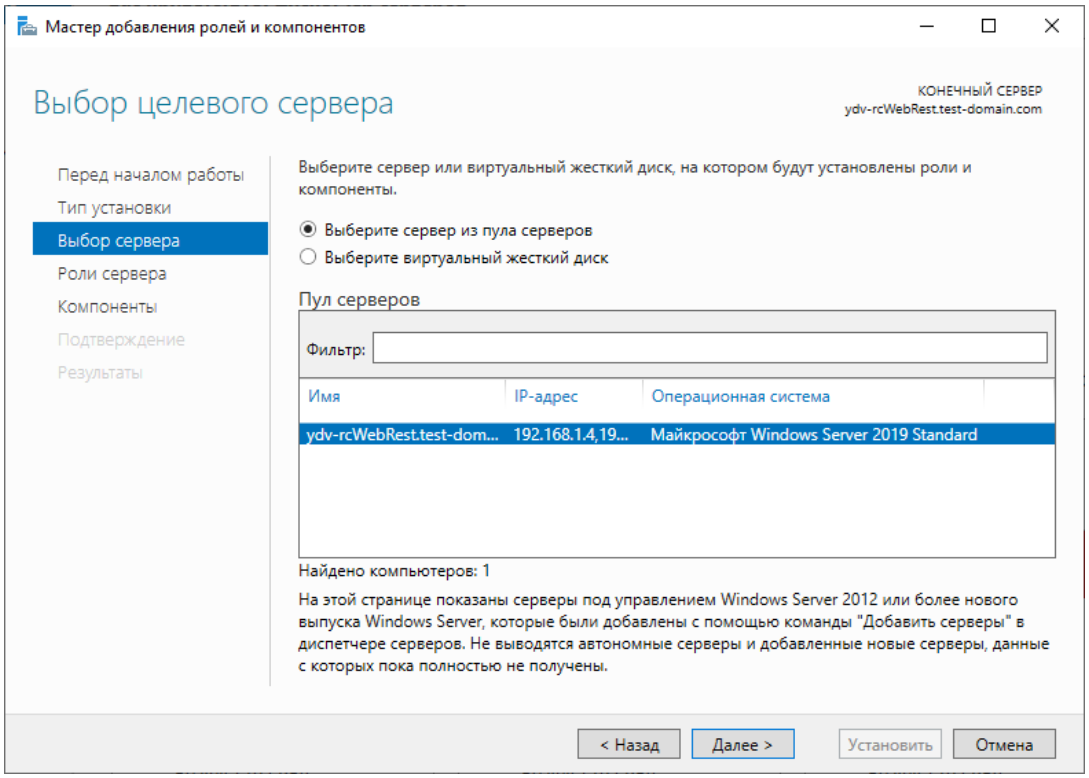
Шаг 3. В окне **Мастер добавления ролей и компонентов** нажмите **Далее**;



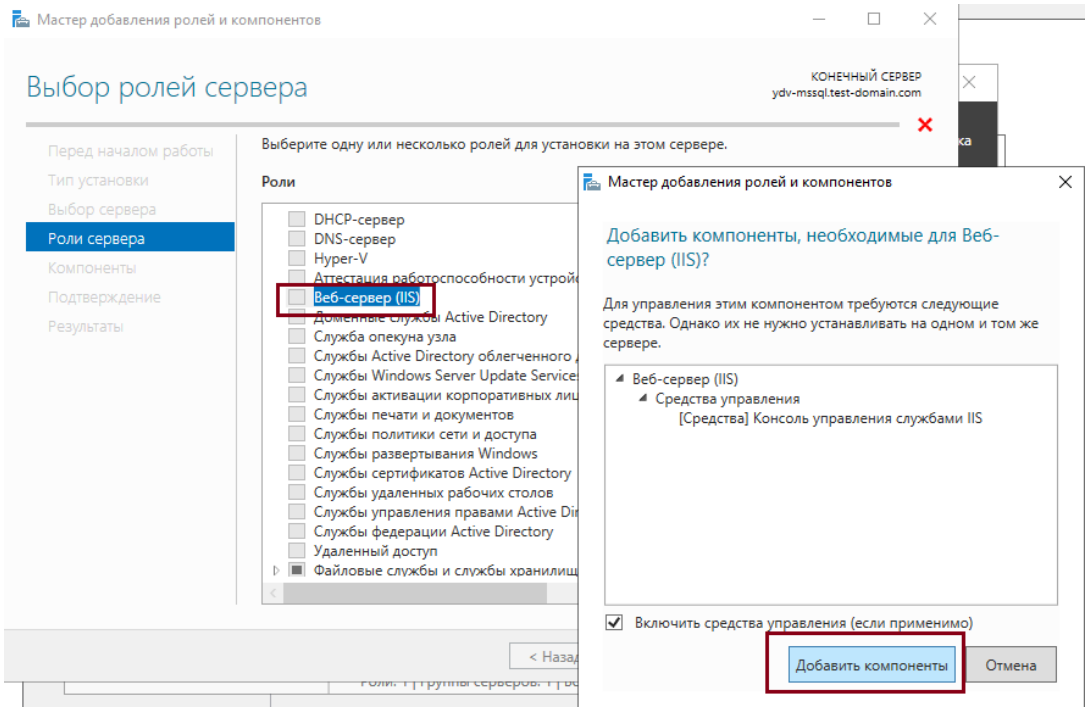
Шаг 4. Выберите **Установка ролей или компонентов → Далее**;



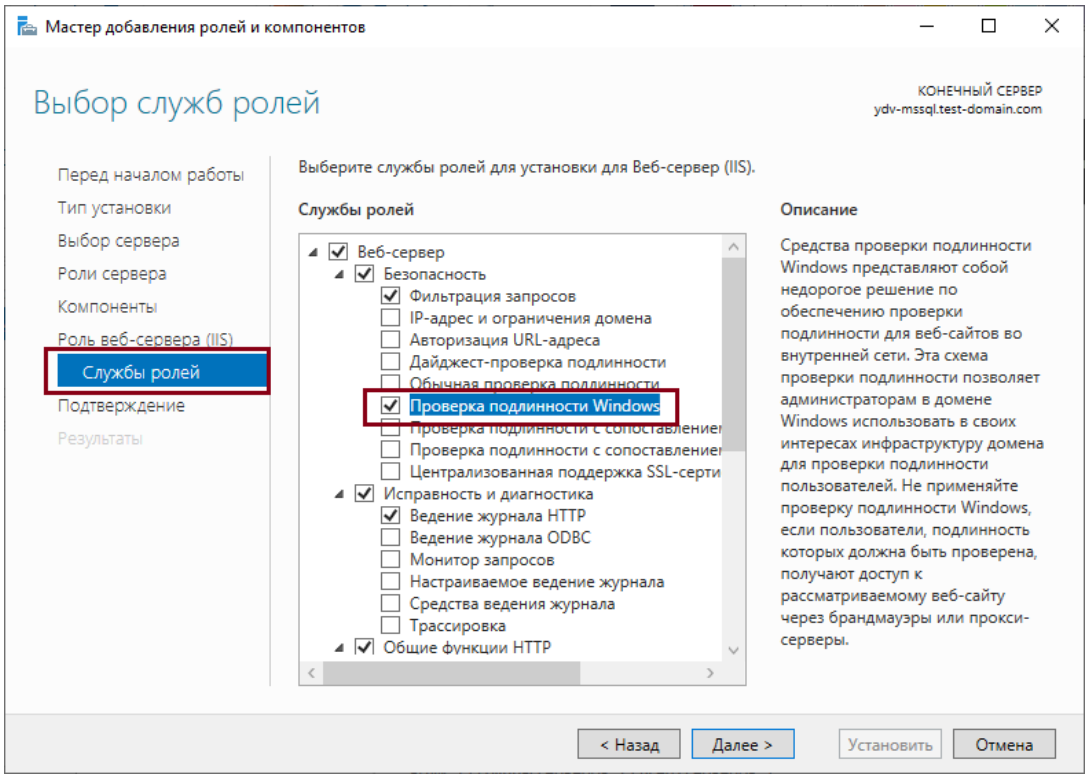
Шаг 5. Выберите необходимый сервер → **Далее**;



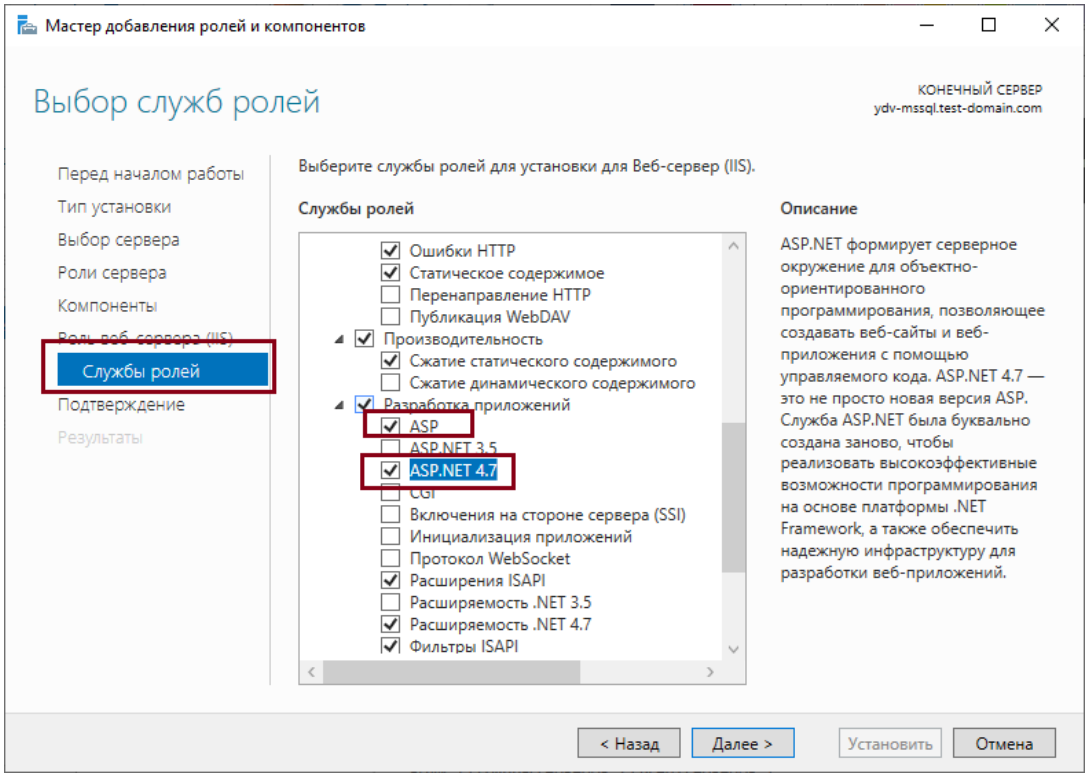
Шаг 6. Выберите **Веб-сервер (IIS)** → **Добавить компоненты** → **Далее**;



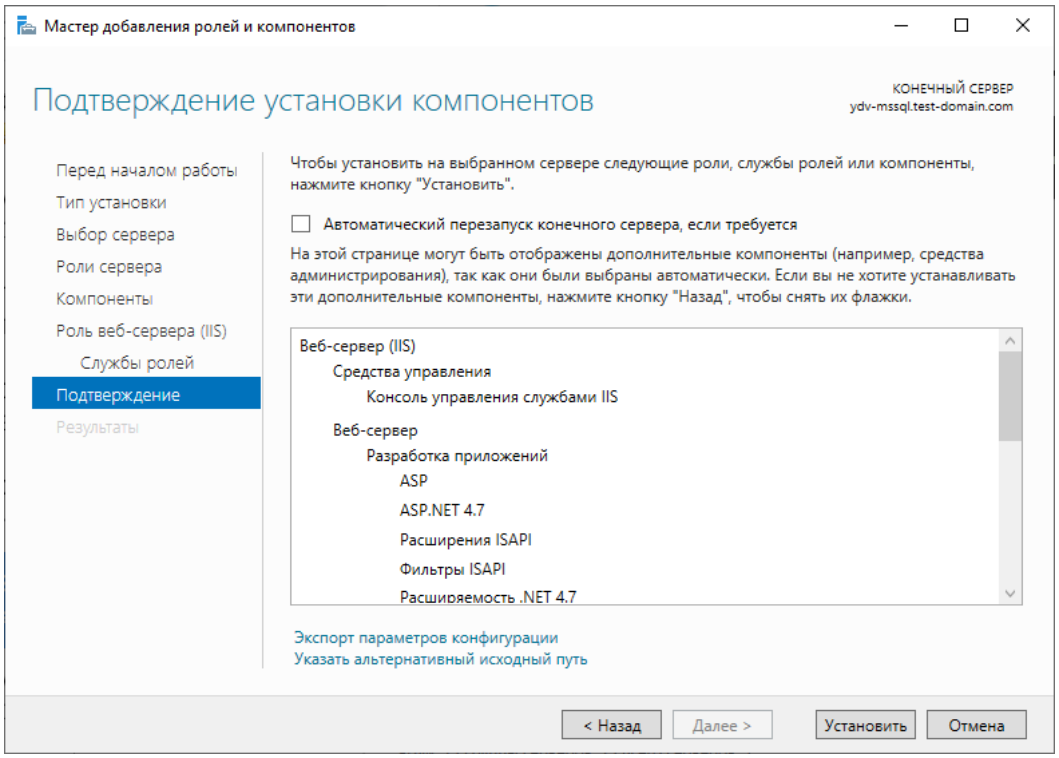
Шаг 7. В списке **Безопасность** отметьте **Проверка подлинности Windows**;



В списке **Разработка приложений** отметьте **ASP** и **ASP.NET 4.7**;

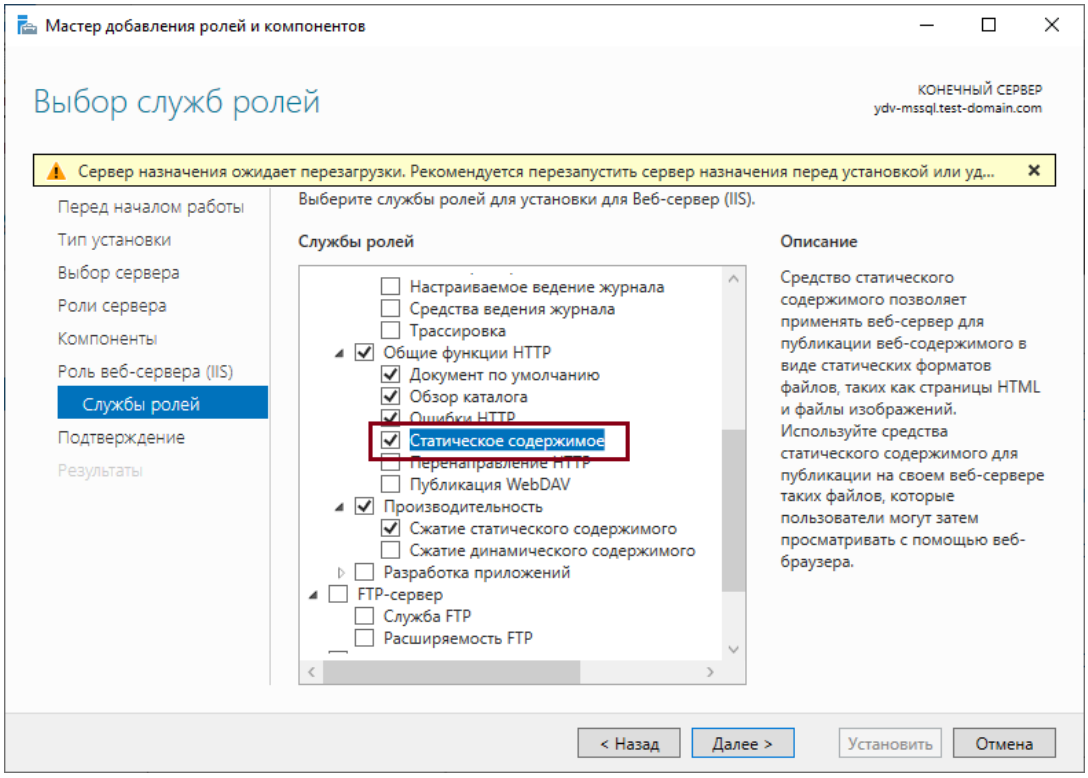


Шаг 8. Проверьте список устанавливаемых ролей и служб → **Установить**;



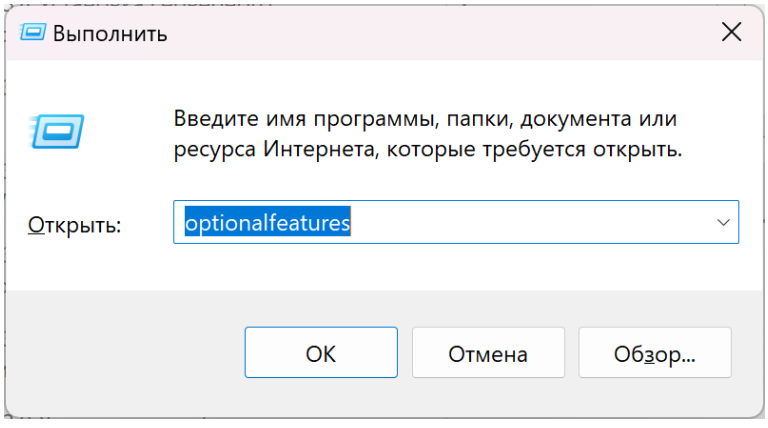
Шаг 9. После завершения установки нажмите **Закрыть** и перезагрузите компьютер.

В случаях установки RedCheckWeb на клиентскую ОС Microsoft Windows требуется при установке отметить следующий компонент: **Службы ролей → Общие функции HTTP → Статическое содержимое**.



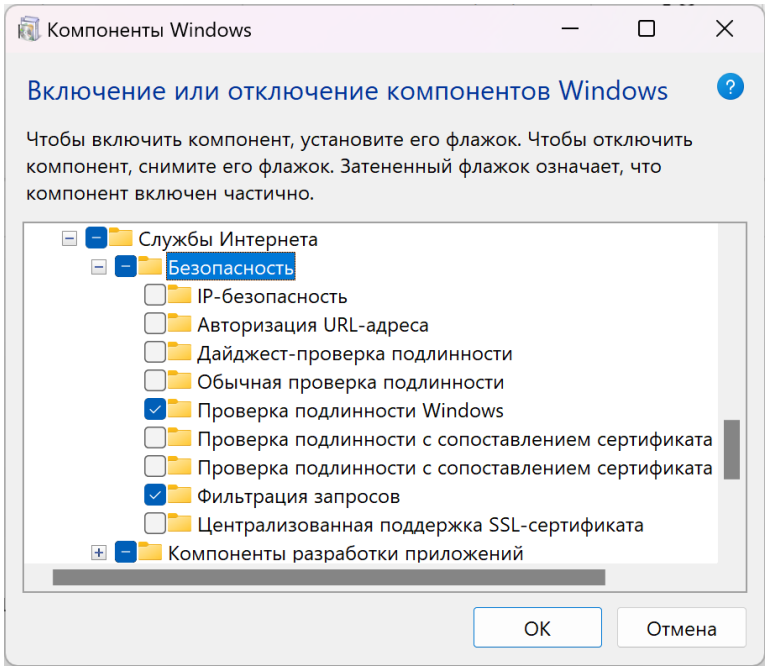
Установка IIS на клиентскую версию Microsoft Windows

Шаг 1. Нажмите Win + K → введите **optionalfeatures** → **OK**;

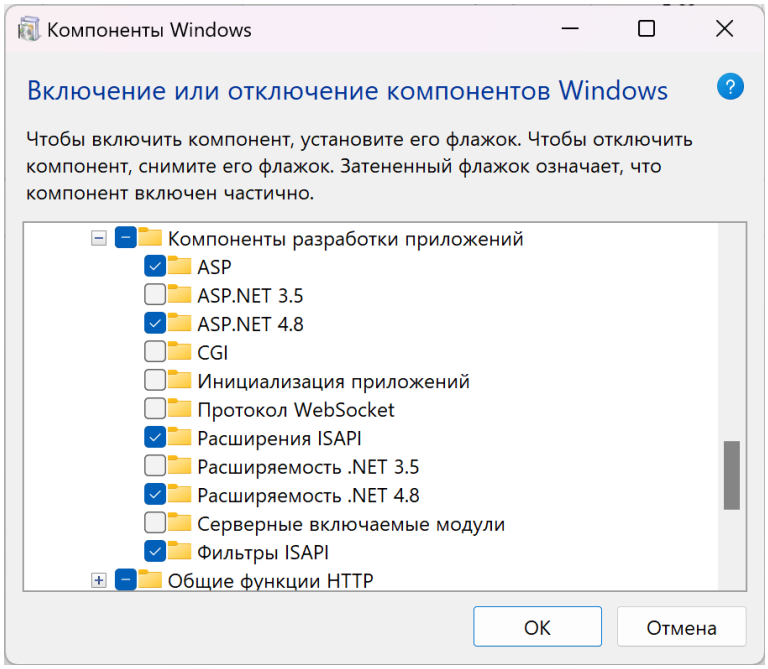


Шаг 2. Раскройте список **Службы IIS** → **Службы Интернета** → отметьте следующие компоненты:

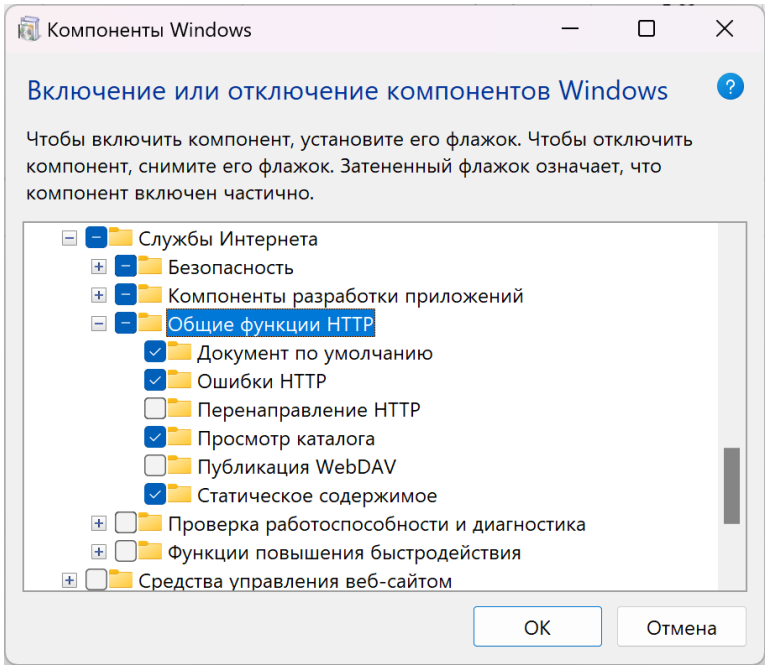
Безопасность → **Проверка подлинности Windows**;



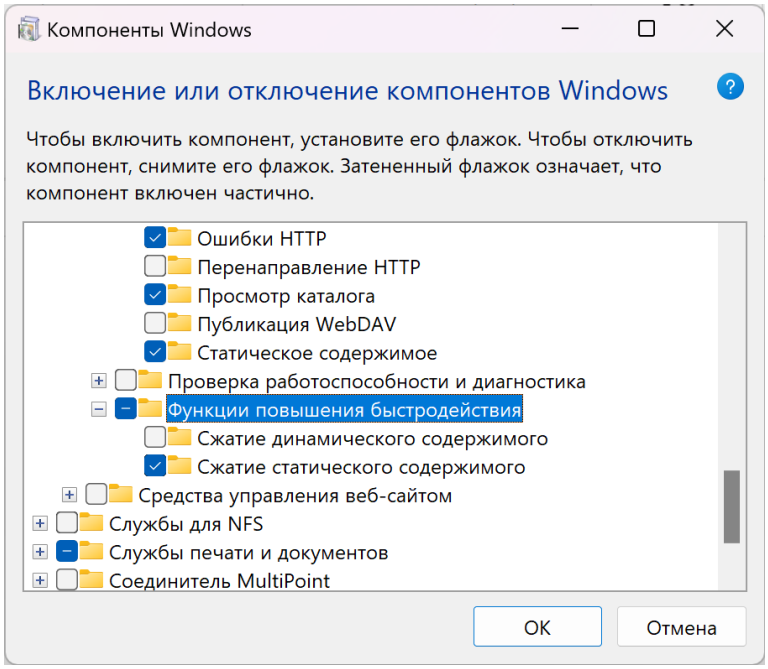
Компоненты разработки приложений → **ASP**, **ASP.NET 4.8**, **Расширения ISAPI**, **Расширяемость .NET 4.8**, **Фильтры ISAPI**;



Общие функции HTTP → Документ по умолчанию, **Ошибки HTTP**, **Просмотр каталога**, **Статическое содержимое**;



Функции повышения быстродействия → Сжатие статического содержимого;



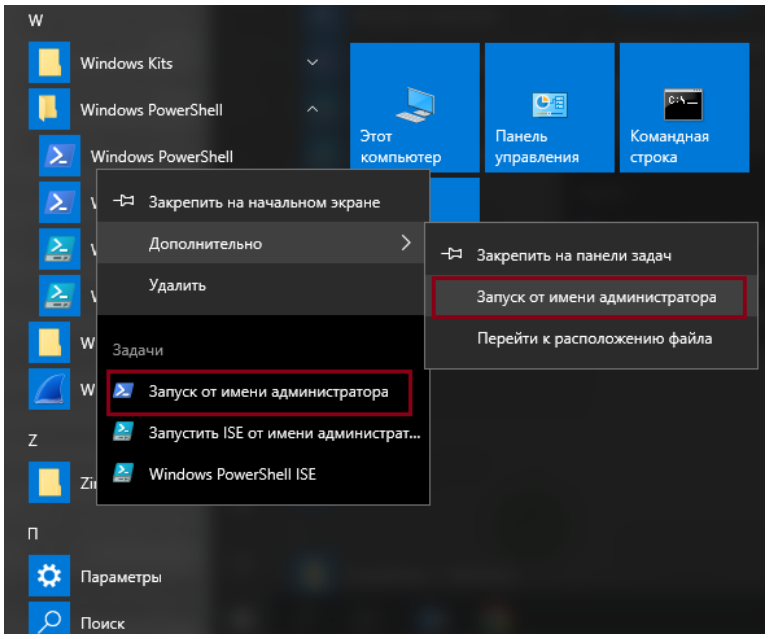
Дождитесь окончания применения изменений.

Рекомендуется отключить режим сна для корректной работы RedCheck.

4.3.2 Установка Microsoft .NET Framework

Проверка имеющихся версий Microsoft .NET Framework 4.8 на хосте

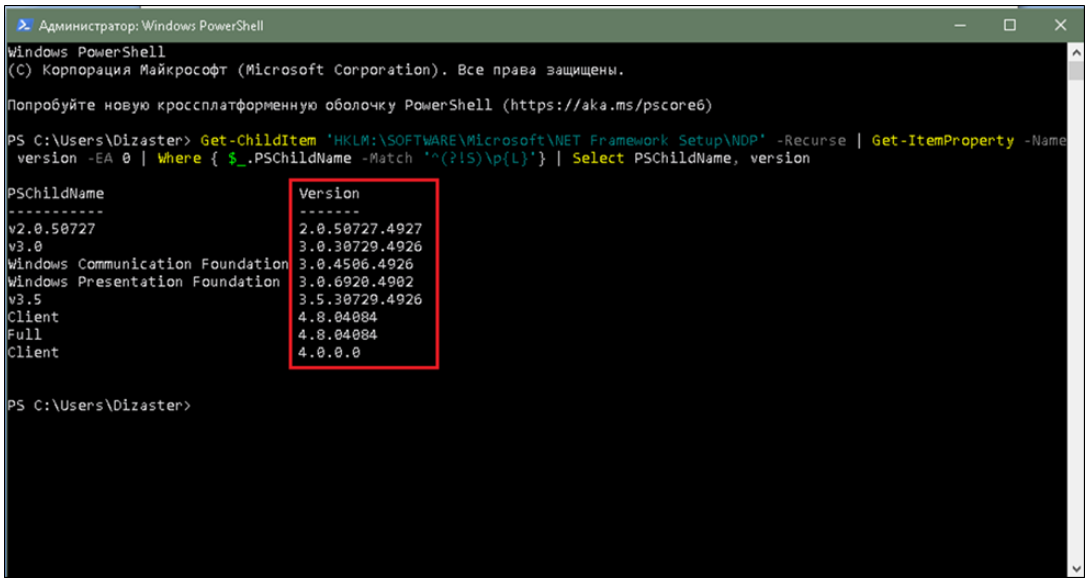
Шаг 1. Запустите консоль **PowerShell**. **Пуск → Windows PowerShell → Windows PowerShell**;



Шаг 2. Введите команду:

Код

```
Get-ChildItem "HKLM:\SOFTWARE\Microsoft\NET Framework Setup\NDP" -
Recurse | Get-ItemProperty -Name version -EA 0 | Where {
$_.PSChildName -Match "^(?!S)\p{L}"} | Select PSChildName, version
```



Отобразится список установленных версий Microsoft .NET Framework.

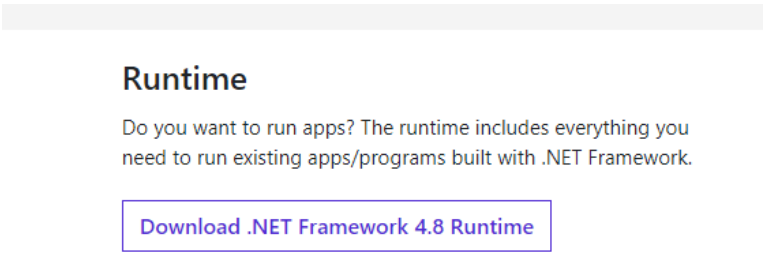
Загрузка инсталлятора

Шаг 3. На странице загрузки с сайта разработчика выберите из списка дистрибутив необходимой версии;

Supported versions

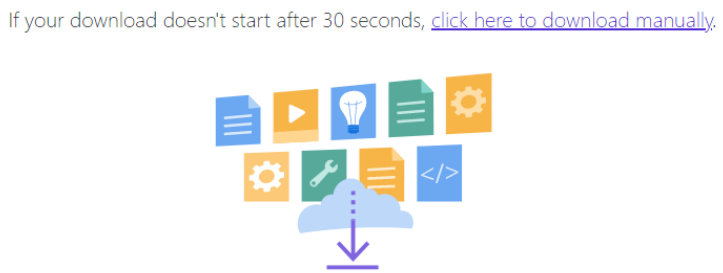
Version	Release date
.NET Framework 4.8.1	August 9, 2022
.NET Framework 4.8 (recommended)	April 18, 2019
.NET Framework 4.7.2	April 30, 2018
.NET Framework 4.7.1	October 17, 2017
.NET Framework 4.7	April 5, 2017
.NET Framework 4.6.2	August 2, 2016
.NET Framework 3.5 SP1	November 18, 2008

Нажмите **Download .Net Framework Runtime**;



Дождитесь окончания загрузки.

Если процесс загрузки не начался автоматически, нажмите **click here to download manual**.

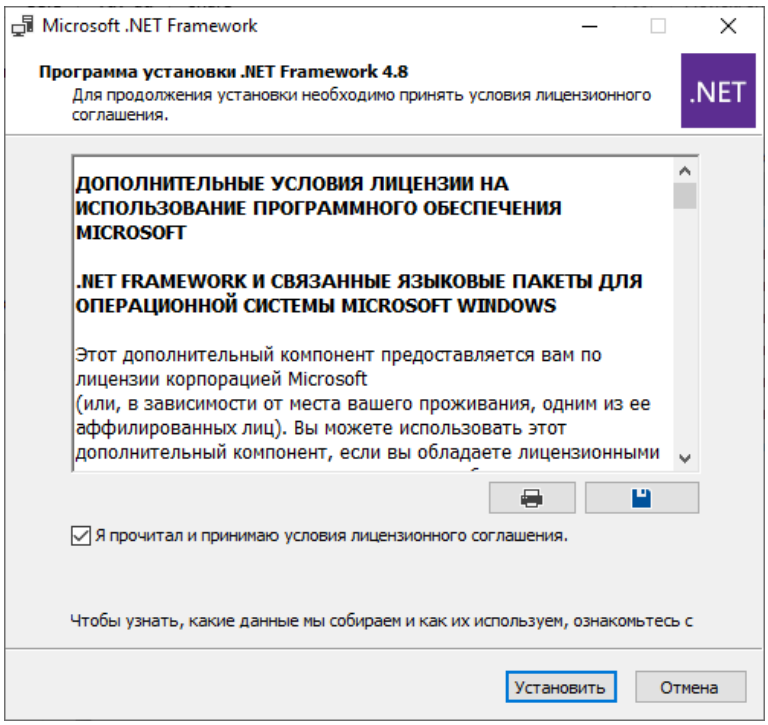


По умолчанию загружается онлайн-дистрибутив, для установки которого требуется доступ к сети Интернет.

Если доступа к сети Интернет нет, после выбора версии Microsoft .NET Framework найдите в таблице **Advanced downloads** строку **Offline installer** → **Runtime**.

Установка Microsoft .NET Framework

Шаг 4. Запустите инсталляционный пакет. Согласитесь с лицензионным соглашением → **Установить**;

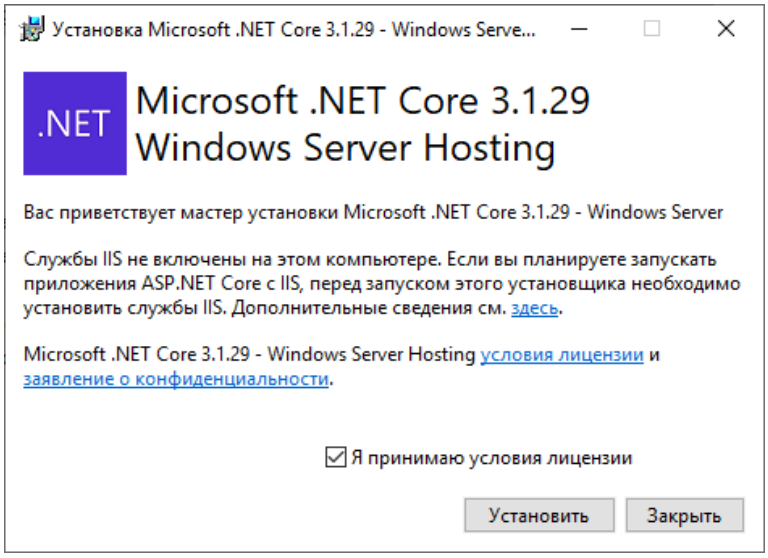


Дождитесь окончания установки и перезагрузите компьютер.

4.3.3 Установка Microsoft .NET Core

Шаг 1. Скачайте инсталляционный пакет **dotnet-hosting-3.1.4-win.exe** по ссылке;

Шаг 2. Откройте установочный пакет → отметьте **Я принимаю условия лицензии** → **Установить**;



Шаг 3. Дождитесь окончания установки и перезагрузите компьютер.

4.3.4 Установка серверного компонента

При обновлении RedCheck **обязательно** сделать резервную копию БД (5.8 Резервное копирование и восстановление).

Одновременная работа двух серверных компонентов RedCheck с одной БД невозможна.

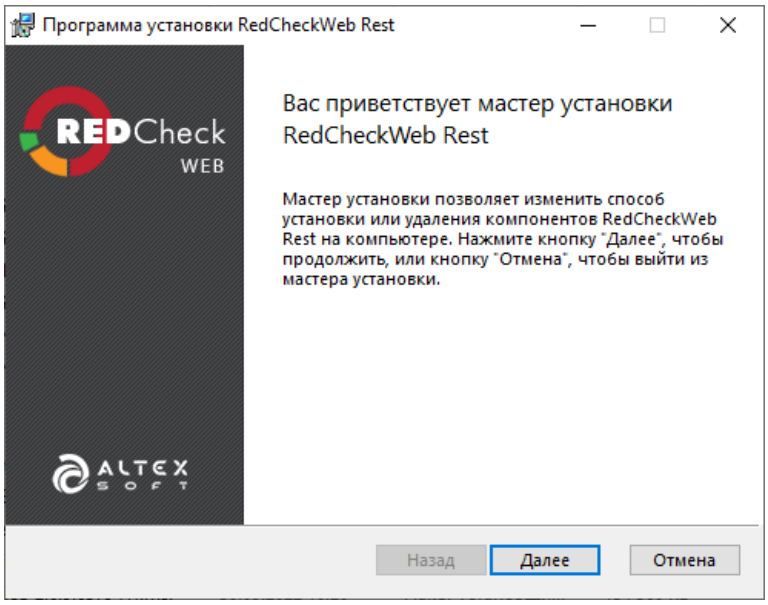
Перед установкой убедитесь, что на компьютере есть все необходимые компоненты:

- СУБД (4.1 Установка СУБД);
- Web-сервер IIS (4.3.1 Установка Web-сервера IIS);
- Microsoft .NET Framework 4.8 (4.3.2 Установка Microsoft .NET Framework);
- Microsoft ASP.NET Core Runtime (4.3.3 Установка Microsoft .NET Core);

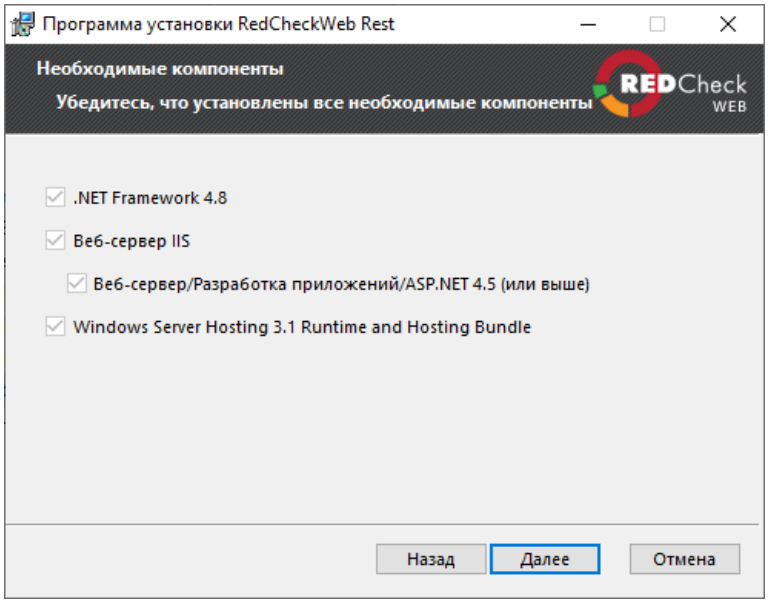
Установка посторонних компонентов может мешать работе Системы.

Возможна автоматическая установка через командную строку (4.6.2.1 Серверный компонент RestAPI)

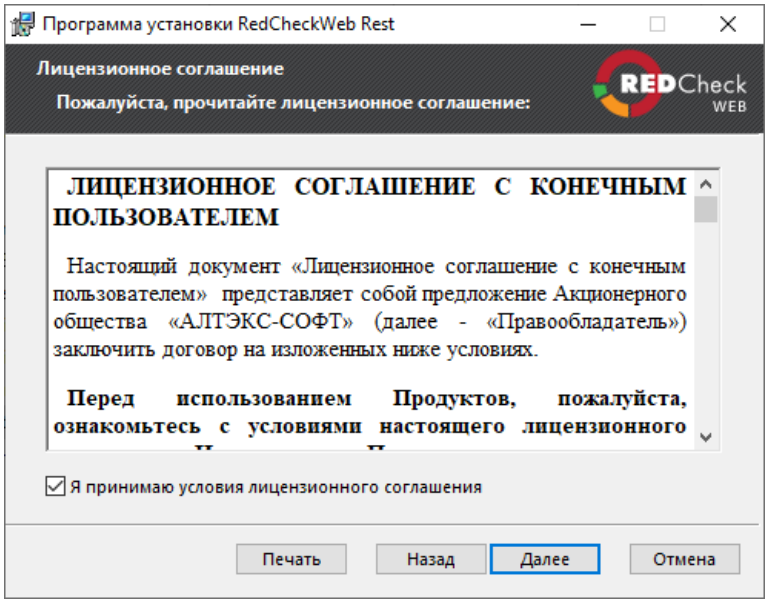
Шаг 1. Запустите установочный пакет RedCheckWeb.Rest.Setup.msi → **Далее**;



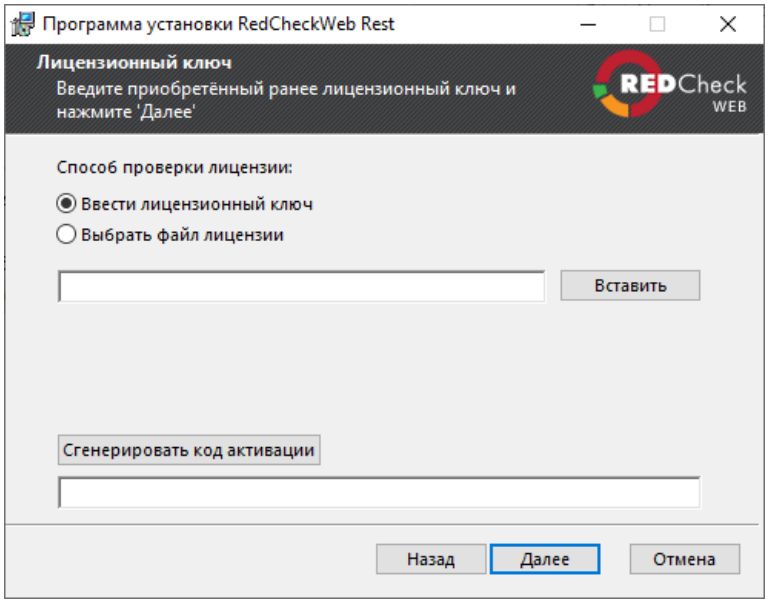
Шаг 2. Инсталлятор проверит наличие всех необходимых компонентов → **Далее**;



Шаг 3. Примите лицензионное соглашение, отметив соответствующее поле → **Далее**;

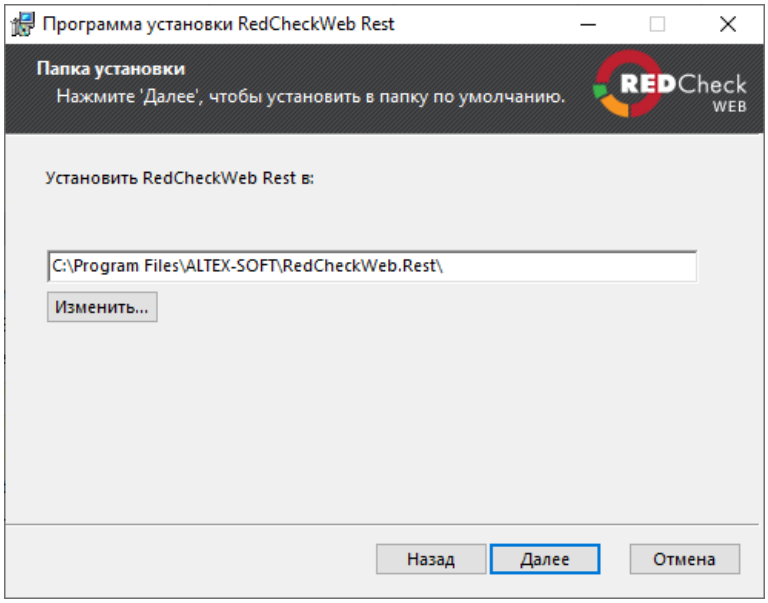


Шаг 4. Введите лицензионный ключ → **Далее**;

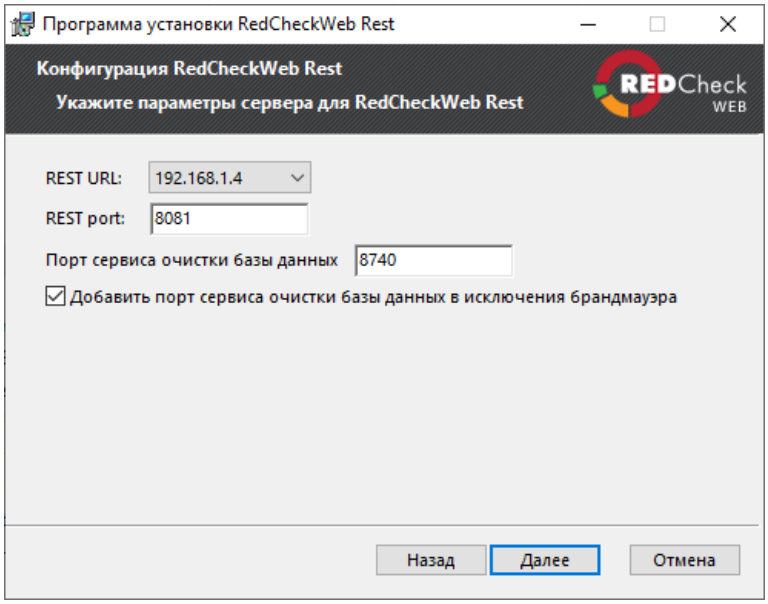


При отсутствии доступа к сети Интернет необходимо получить файл лицензии и указать способ проверки **Выбрать файл лицензии** (5.2 Активация лицензии, с 1 по 5 шаг).

Шаг 5. Укажите директорию для RedCheck → **Далее**;



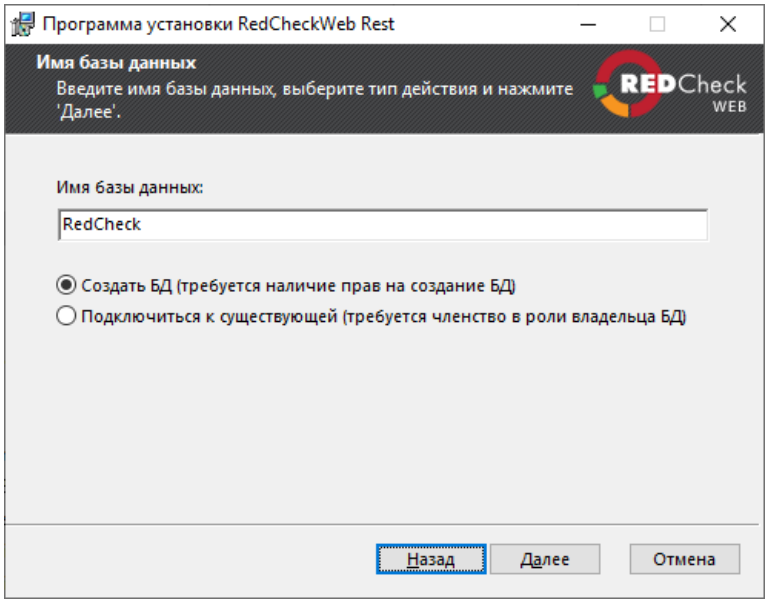
Шаг 6. Выберите ip-адрес, на котором будет находиться RestAPI. Измените по необходимости порт RestAPI и сервиса очистки базы данных, отметьте **Добавить порт сервиса очистки...** → **Далее**;



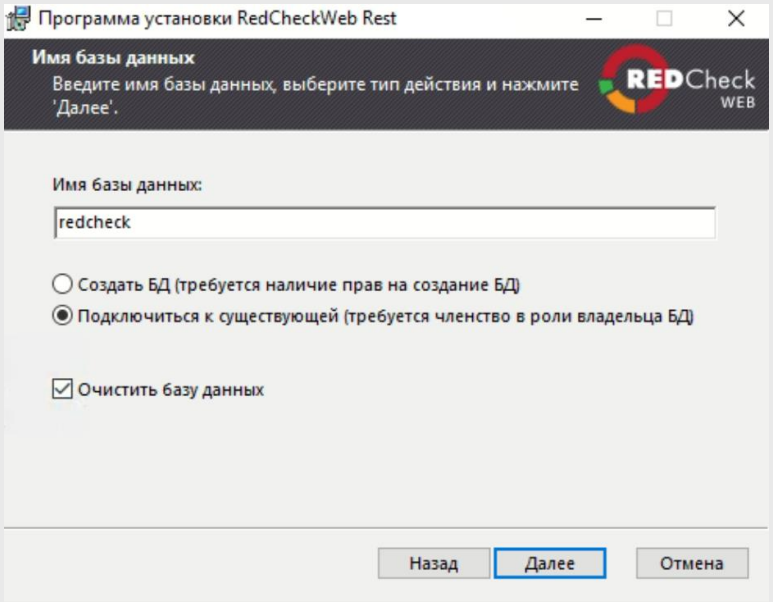
Шаг 7. Введите параметры для подключения к СУБД → **Далее**;

Сервер СУБД: имя узла/IP-адрес, на котором находится сервер СУБД;
Логин: имя пользователя с правами на создание БД. Данный пользователь будет владельцем БД RedCheck;
Пароль: пароль указанного пользователя;
Порт: сетевой порт для сервера СУБД (по умолчанию для Microsoft SQL Server - 1433, для PostgreSQL - 5432);

Шаг 8. Укажите имя БД (RedCheck по умолчанию) → **Далее**;



Если БД уже существует, выберите **Подключиться к существующей...** При необходимости отметьте **Очистить базу данных** (Если СУБД развернута на BaseAlt, поле должно быть отмечено обязательно).



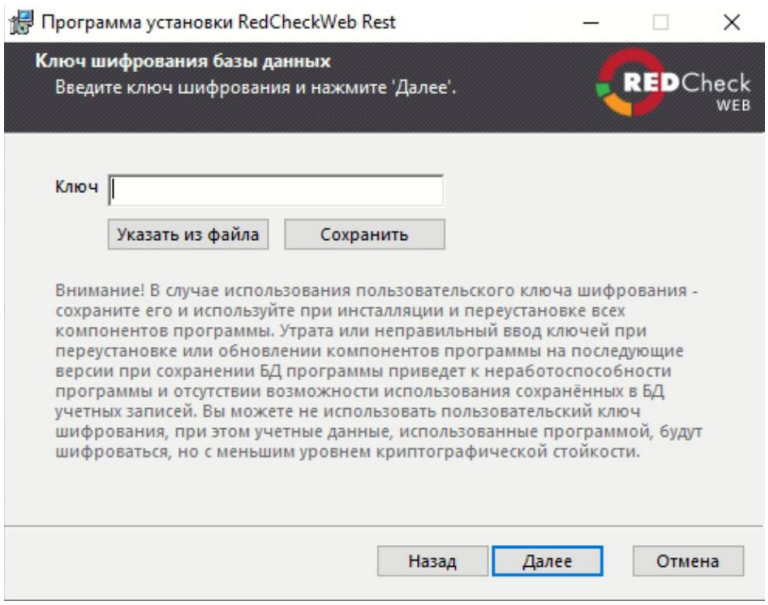
Шаг 9. Введите ключ шифрования → **Далее**;

Ключ шифрования используется для шифрования учетных записей RedCheck для сканирования.

Нажмите **Указать из файла** (с расширением .xml), чтобы использовать уже имеющийся ключ шифрования.

Нажмите **Сохранить** для записи ключа в файл с расширением .xml. В поле **sckd** указан ключ шифрования.

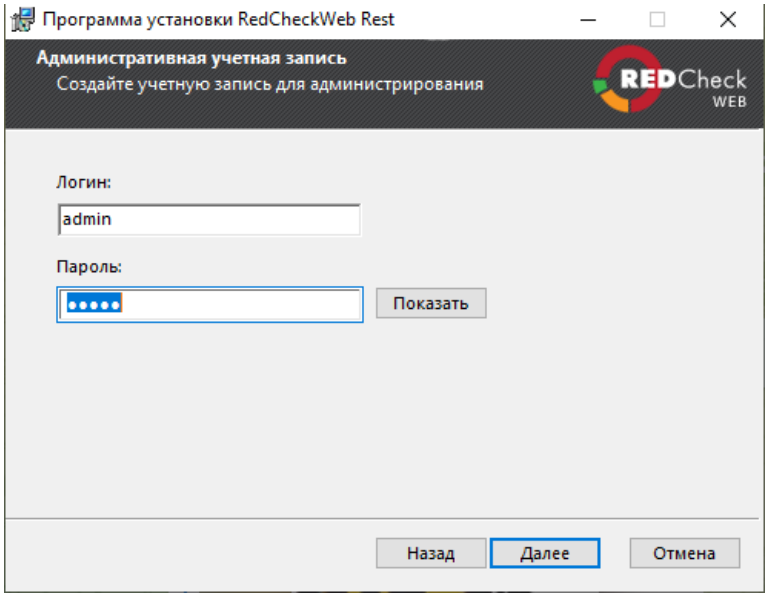
```
<?xml version="1.0" encoding="utf-8"?>
<sckd>N2v#kAp4</sckd>
```



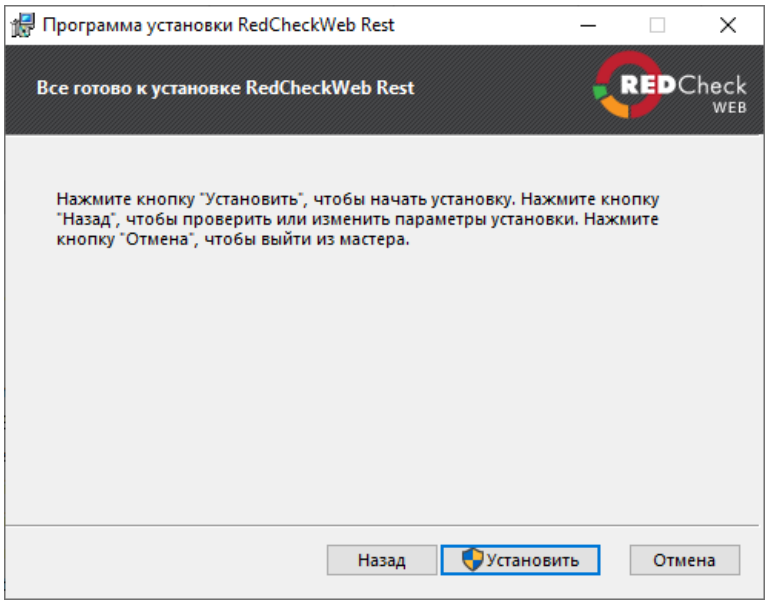
Если не указывать ключ шифрования, учетные записи RedCheck для сканирования все равно будут зашифрованы, но с меньшим уровнем криптографической стойкости.

В дальнейшем есть возможность сменить ключ шифрования (5.5 Смена ключа шифрования)

Шаг 10. Укажите логин и пароль для входа в консоль управления RedCheck → **Далее**;



Шаг 11. Нажмите **Установить**;



После окончания установки нажмите **Готово**.

В случае возникновения ошибок во время установки, обратитесь к журналу установки, расположенному по следующему пути: **%temp%/ALTEX-SOFT/RedCheckWeb.Rest.Setup.txt**
Для разрешения нештатной ситуации рекомендуется создать обращение на **Портале технической поддержки**. При обращении необходимо описать проблему и приложить файл **RedCheckWeb.Rest.Setup.txt**

4.3.5 Установка консоли управления (пользовательского интерфейса)

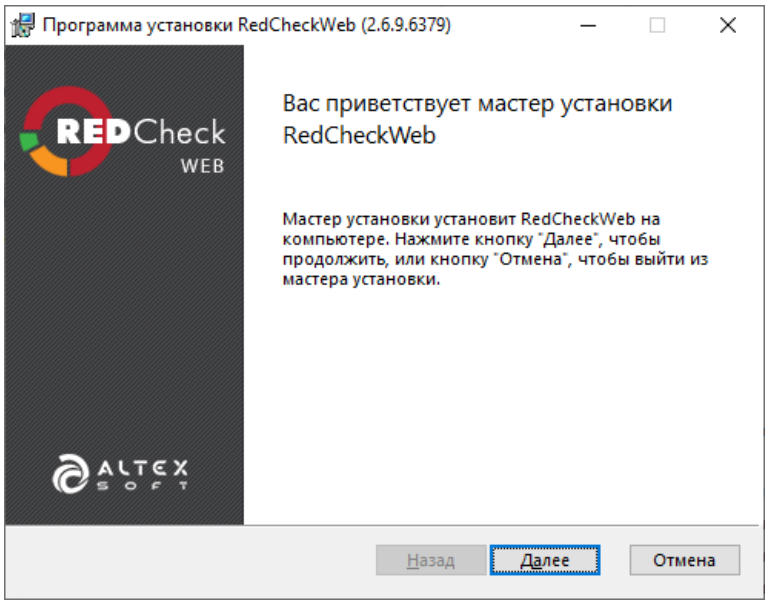
Перед установкой убедитесь, что на компьютере есть все необходимые компоненты:

- Web-сервер IIS (4.3.1 Установка Web-сервера IIS);
- Microsoft .NET Framework 4.8 (4.3.2 Установка Microsoft .NET Framework);
- Microsoft ASP.NET Core Runtime (4.3.3 Установка Microsoft .NET Core).

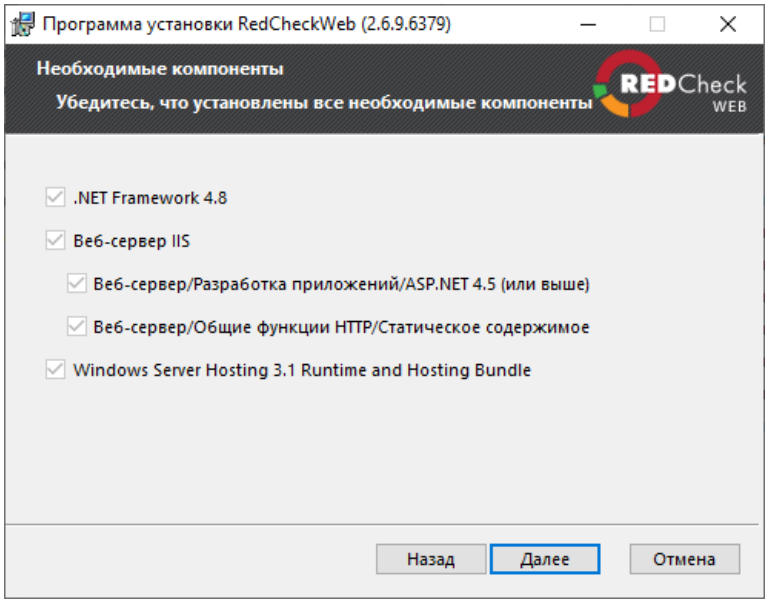
Установка посторонних компонентов может мешать работе Системы.

Возможна автоматическая установка через командную строку (4.6.2.2 Консоль управления).

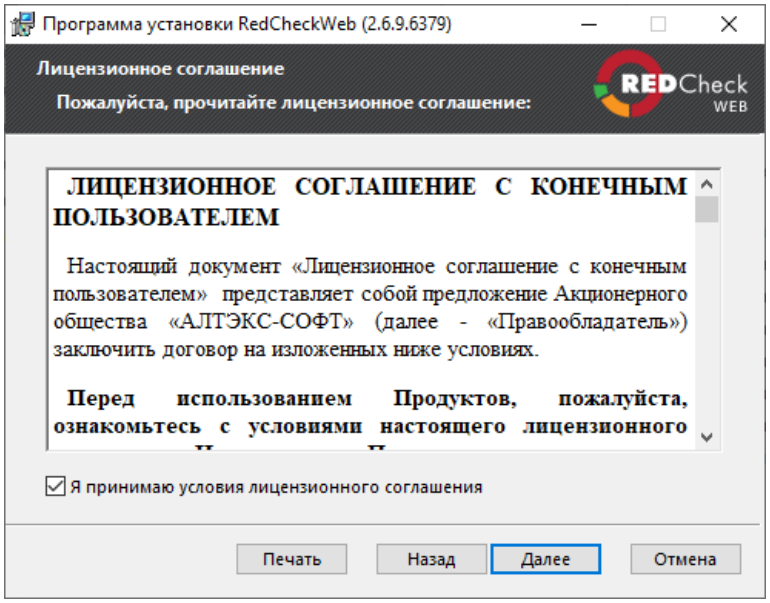
Шаг 1. Запустите установочный пакет RedCheckWeb.Client.Setup.msi → **Далее**;



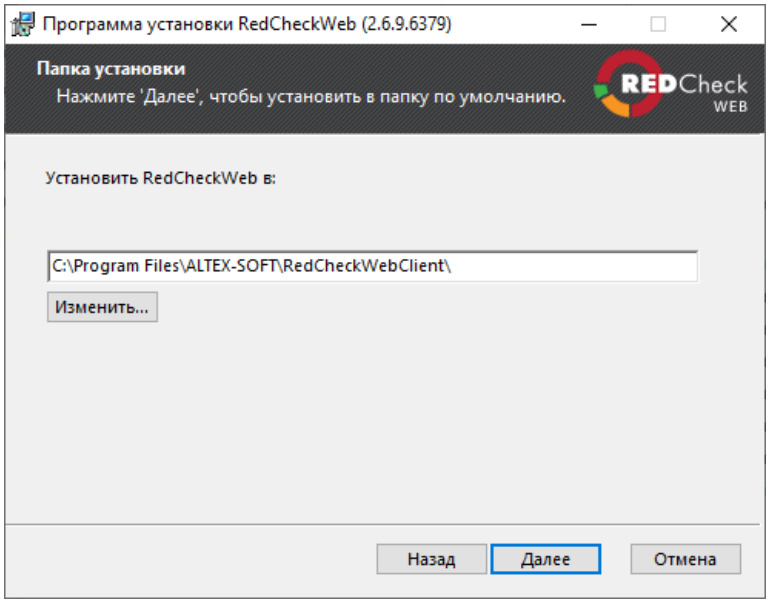
Шаг 2. Инсталлятор проверит наличие всех необходимых компонентов → **Далее**;



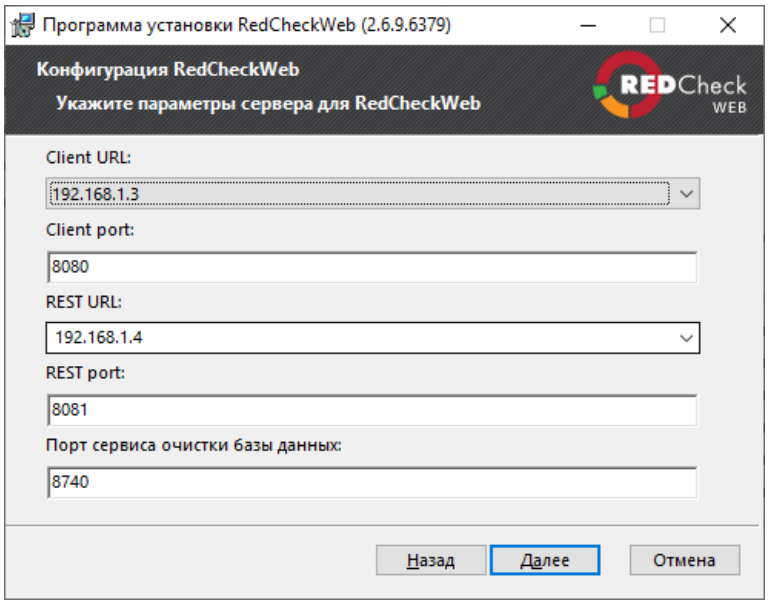
Шаг 3. Примите лицензионное соглашение, отметив соответствующее поле → **Далее**;



Шаг 4. Укажите директорию для RedCheck → **Далее**;

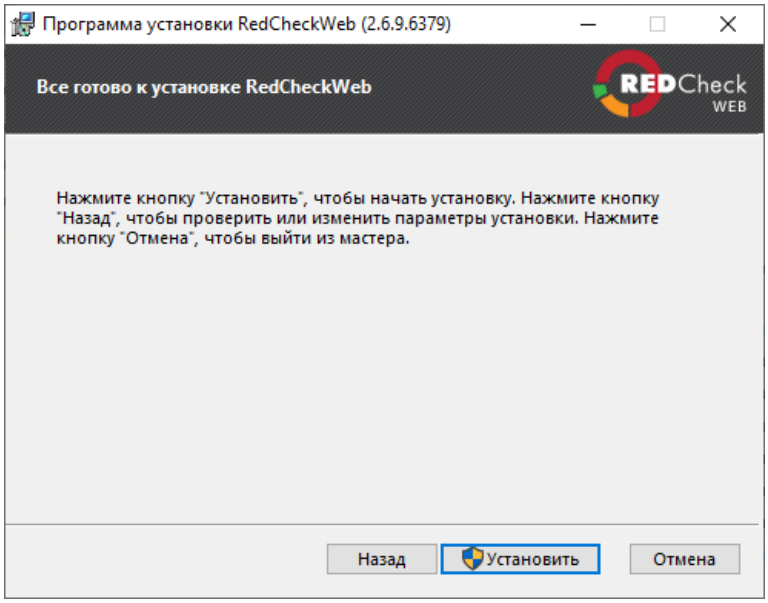


Шаг 5. Выберите в **Client URL** ip-адрес для консоли управления, к которому будет обращаться RestAPI. В **REST URL** выберите ip-адрес установленного ранее серверного компонента → **Далее**;



Если порт для RestAPI и сервиса очисти БД был изменен при установке серверного компонента, укажите новые значения.

Шаг 6. Нажмите **Установить**;



После окончания установки нажмите **Готово**.

В случае возникновения ошибок во время установки, обратитесь к журналу установки, расположенному по следующему пути: **%temp%/ALTEX-SOFT/RedCheckWeb.Client.Setup.txt**
Для разрешения нештатной ситуации рекомендуется создать обращение на **Портале технической поддержки**. При обращении необходимо описать проблему и приложить файл **RedCheckWeb.Client.Setup.txt**

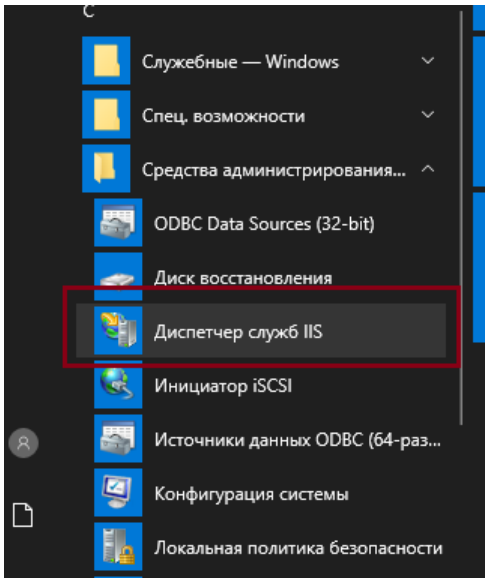
4.3.6 Включение возможности Windows-авторизации

Перед установкой убедитесь, что на компьютере есть все необходимые компоненты:

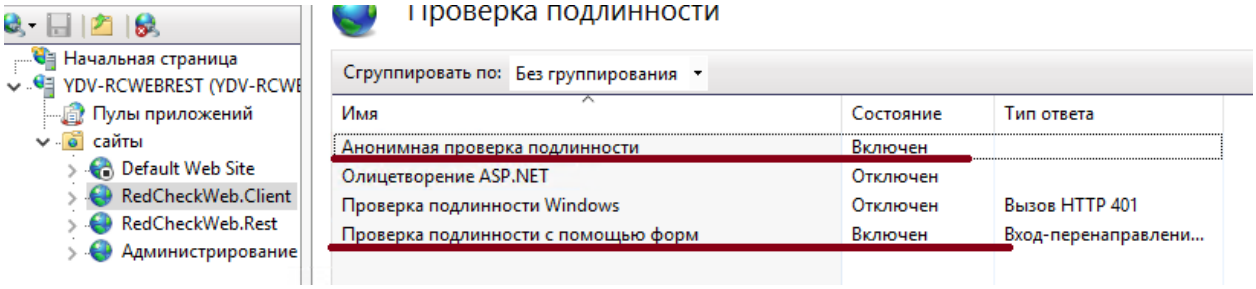
- Web-сервер IIS (4.3.1 Установка Web-сервера IIS);
- Серверный компонент RedCheck (4.3.4 Установка серверного компонента Web-версии RedCheck);
- Консоль управления (4.3.5 Установка Web-консоли управления).

В приведенной ниже инструкции серверный компонент и консоль управления RedCheck установлены на разных хостах.

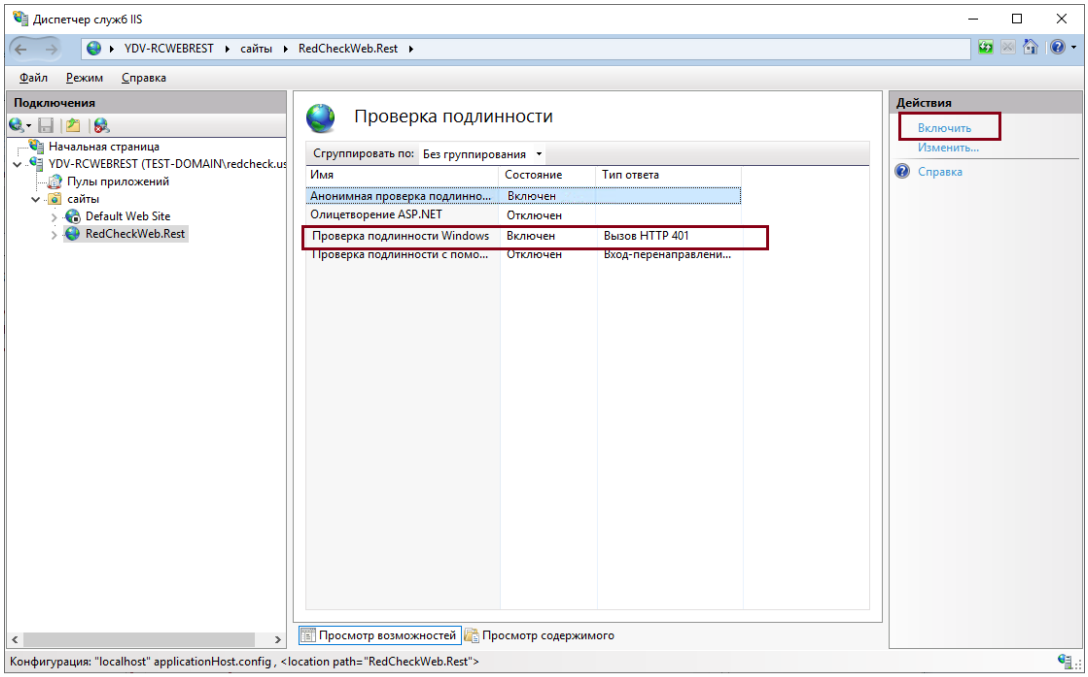
Шаг 1. Пуск → Средства администрирования Windows → Диспетчер служб IIS;



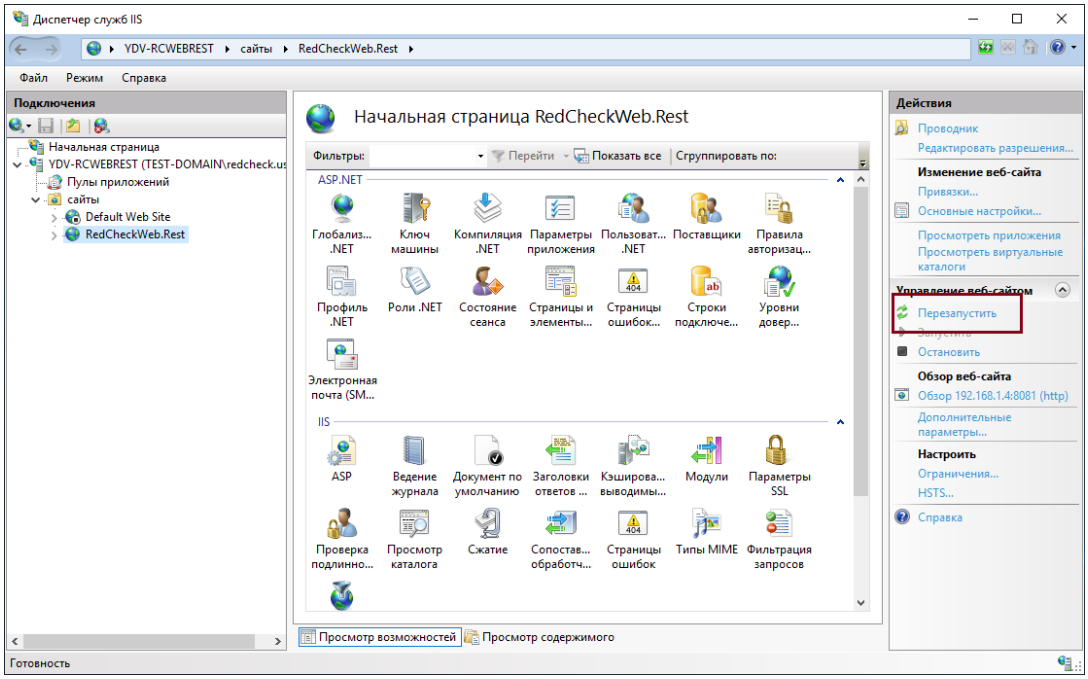
Шаг 2. Раскройте сайты → **RedCheckWeb.Client** → **Проверка подлинности** → убедитесь, что **Анонимная проверка подлинности** и **Проверка подлинности с помощью форм включены**;



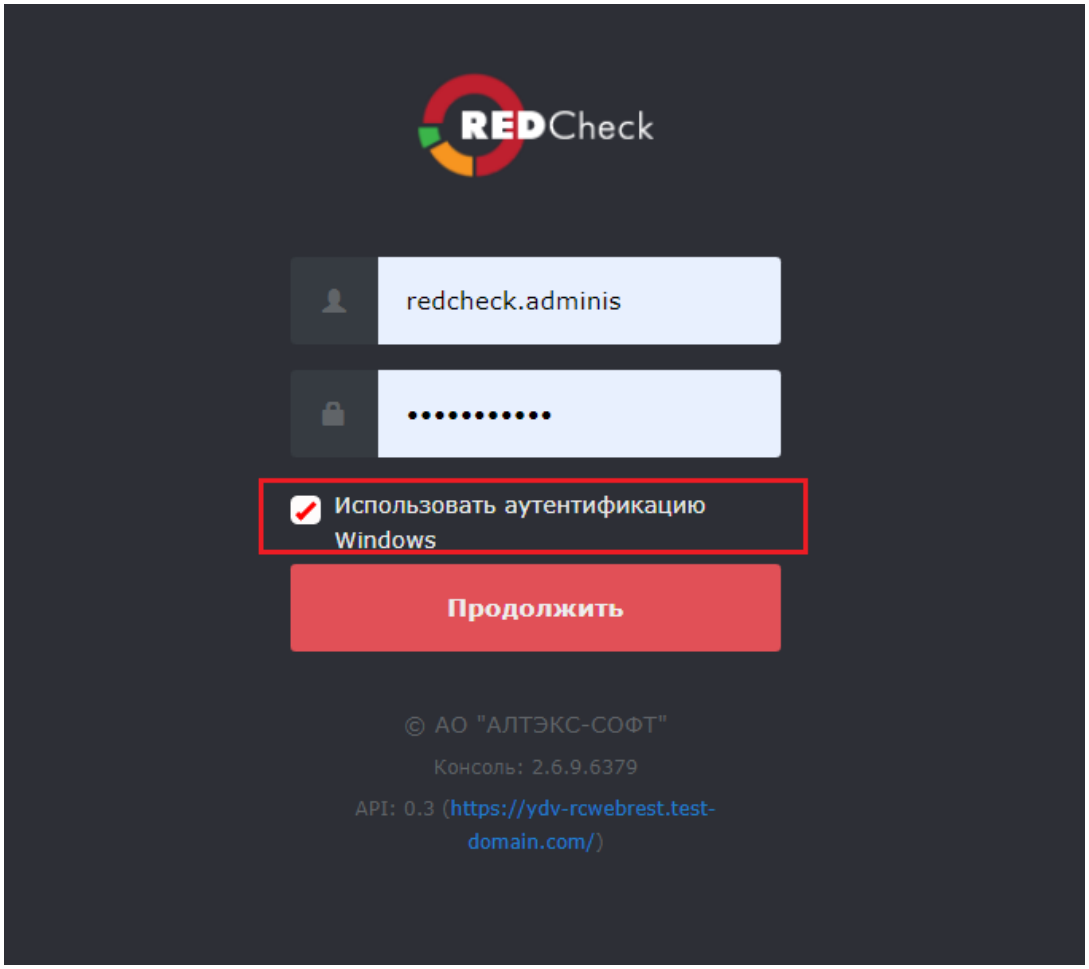
Шаг 3. Для **RedCheckWeb.Rest** необходимо включить **Анонимная проверка подлинности** и **Проверка подлинности Windows**;



Шаг 4. Нажмите **Перезапустить** в меню действий.



После выполненных действий вы сможете авторизоваться в консоли управления, используя локальную/доменную учетную запись Microsoft Windows. Для этого отметьте поле **Использовать аутентификацию Windows**.

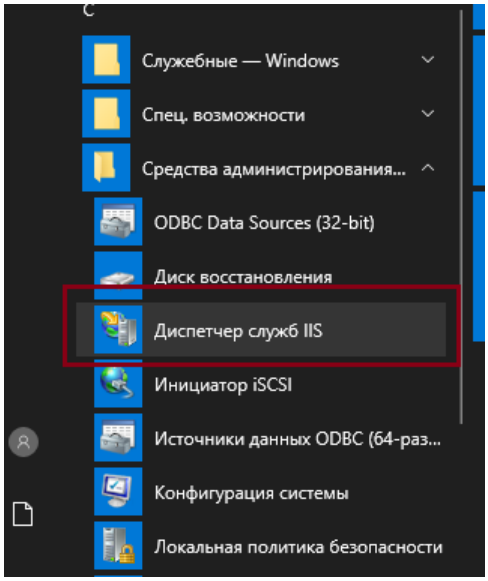


RedCheck поддерживает работу только с NTLM режимом авторизации. KERBEROS не поддерживается.

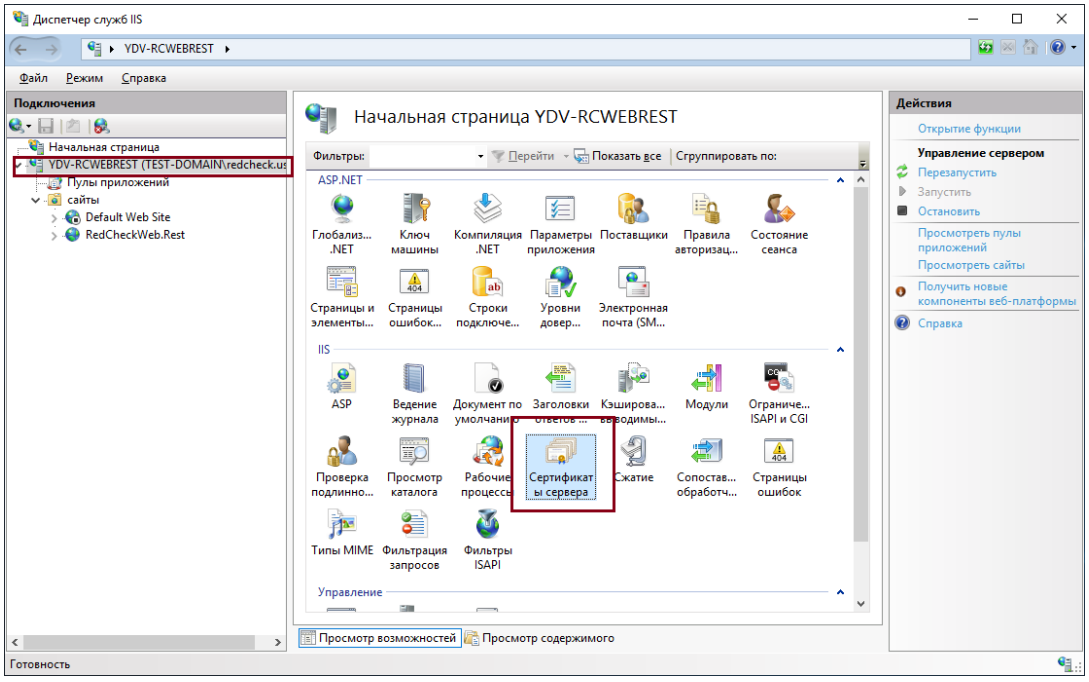
4.3.7 Включение обработки HTTPS-соединений

Создание самозаверенного сертификата

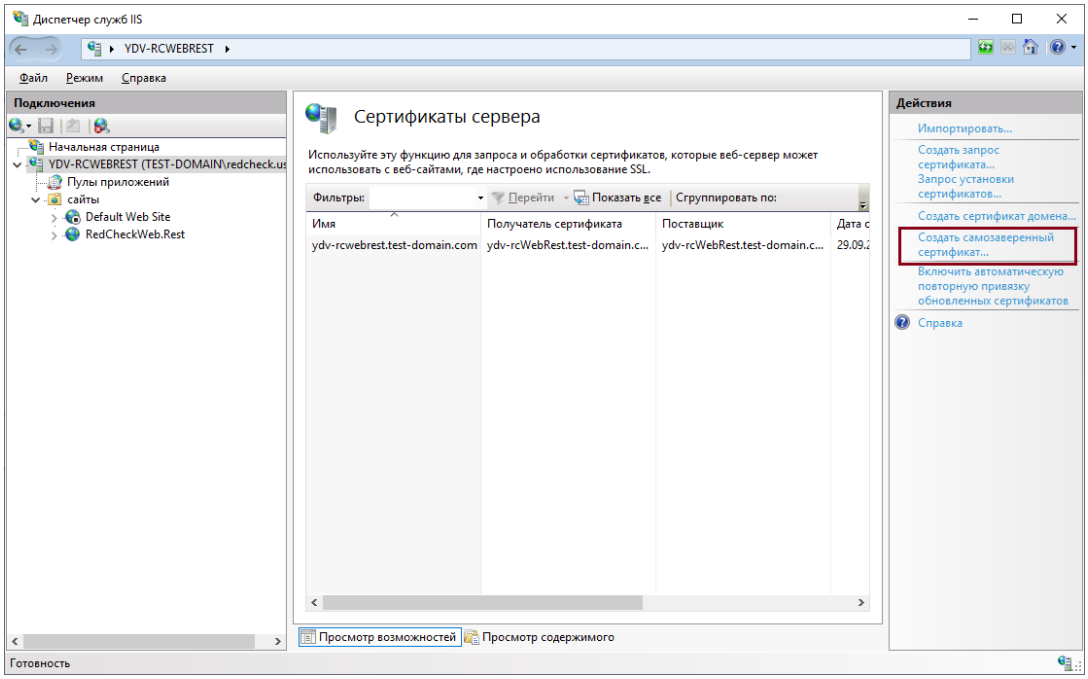
Шаг 1. Пуск → Средства администрирования Windows → Диспетчер служб IIS;



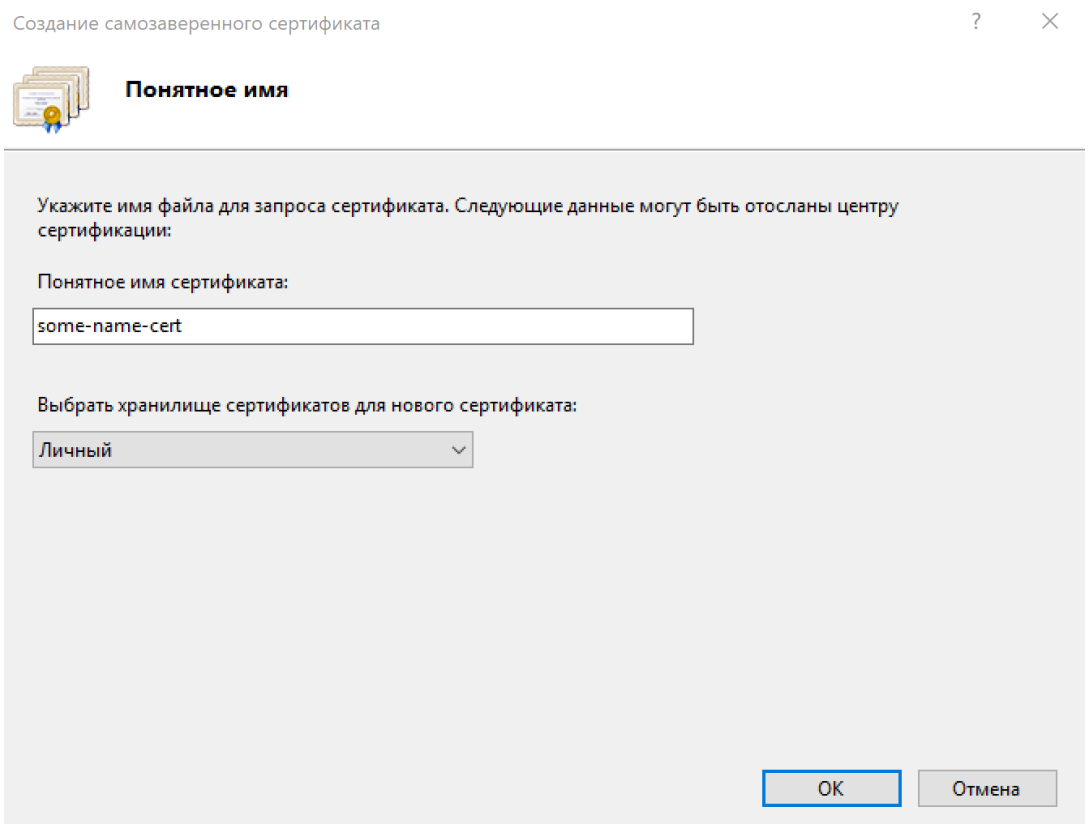
Шаг 2. Выберите сервер → **Сертификаты сервера**;



Шаг 3. Нажмите **Создать самозаверенный сертификат** в меню действий;



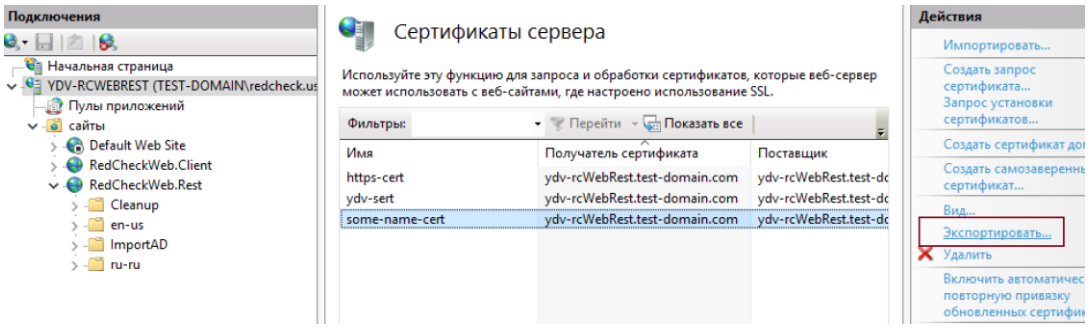
Шаг 4. Укажите название для сертификата → **OK**.



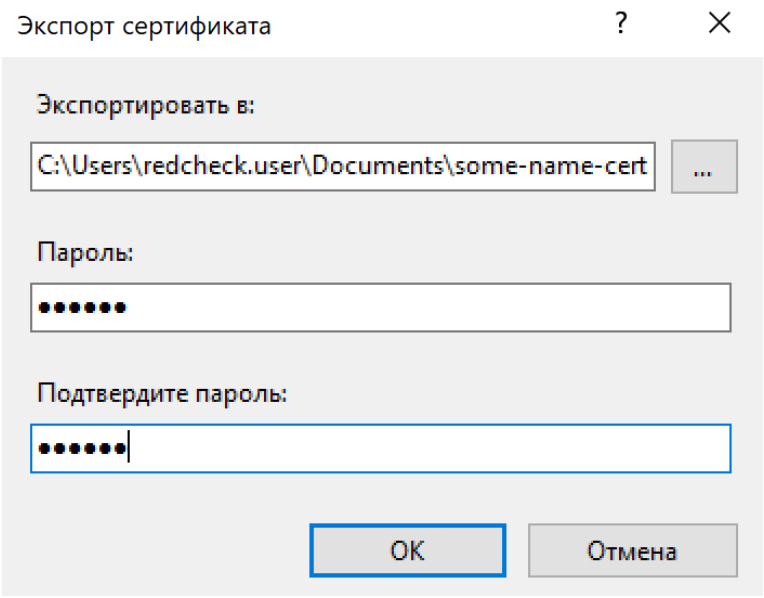
Значение в столбце **Получатель сертификата** будет являться именем узла.

Экспорт сертификатов

Шаг 5. Выберите созданный сертификат → **Экспортировать;**

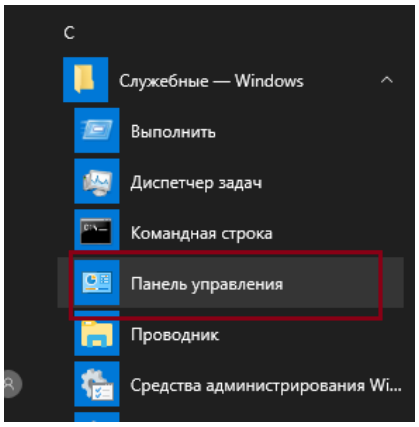


Шаг 6. Укажите директорию для экспорта → задайте и подтвердите пароль → **ОК**;

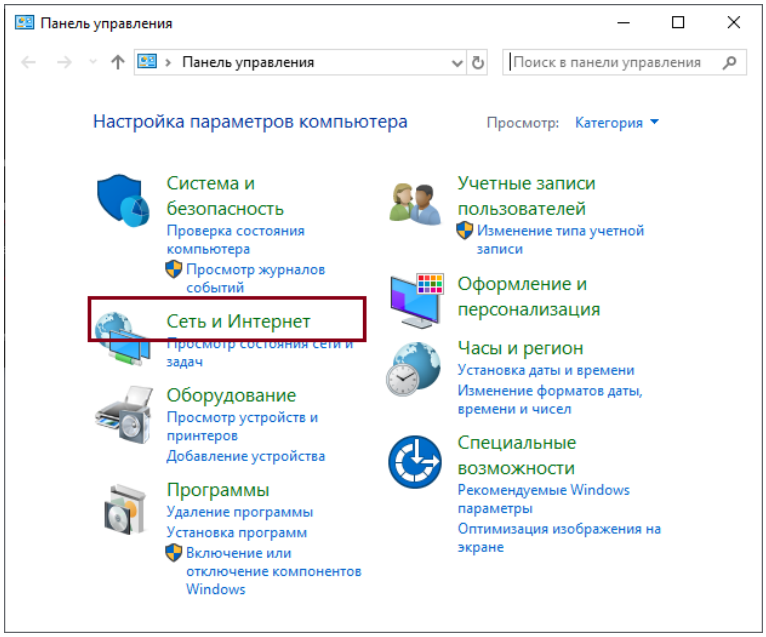


Импорт сертификатов

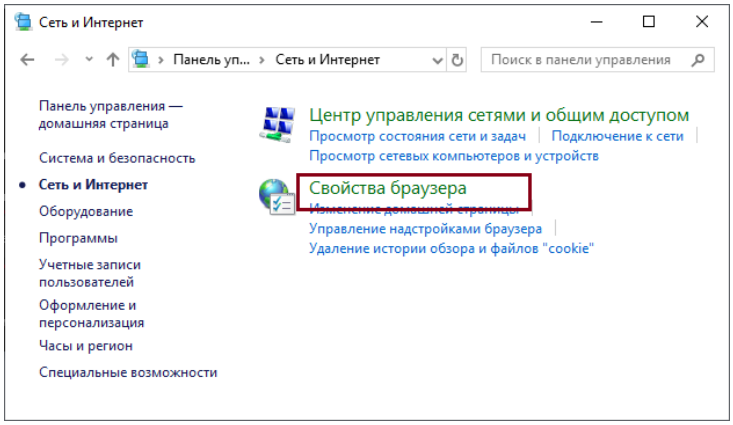
Шаг 7. Пуск → Служебные – Windows → Панель управления;



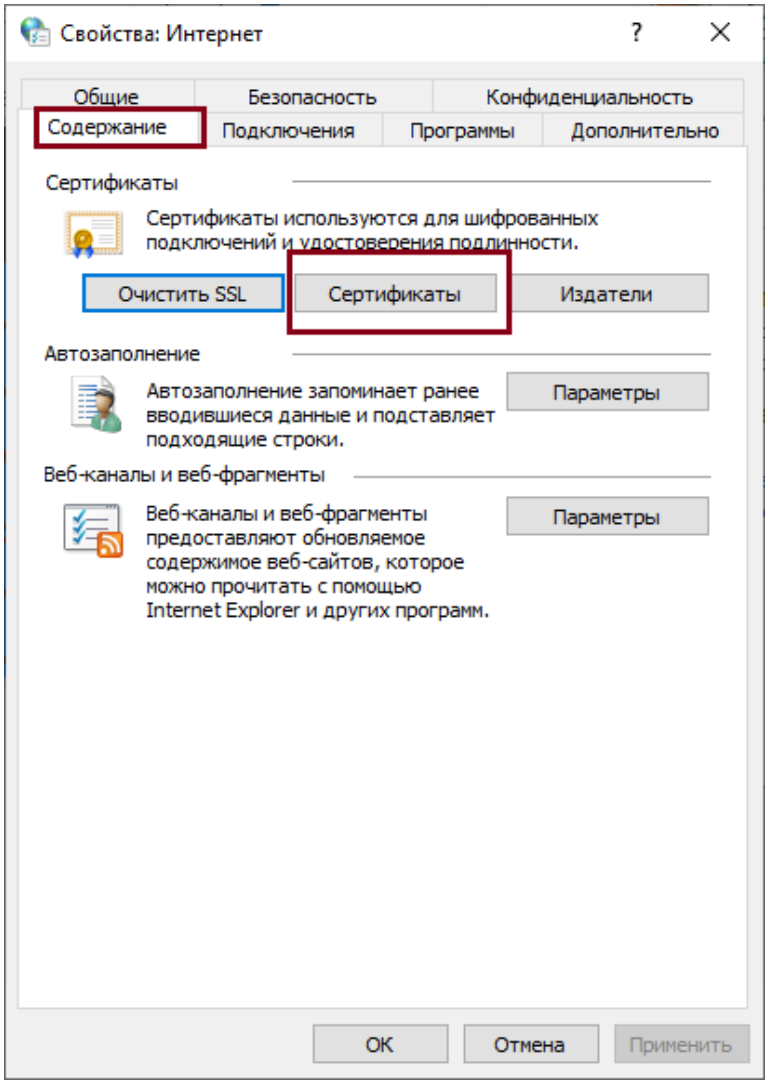
Выберите **Сеть и Интернет**;



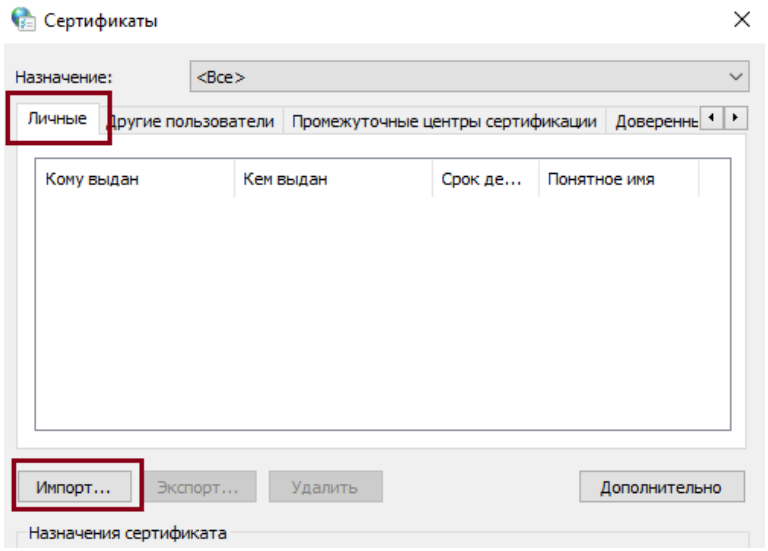
Нажмите **Свойства браузера**;



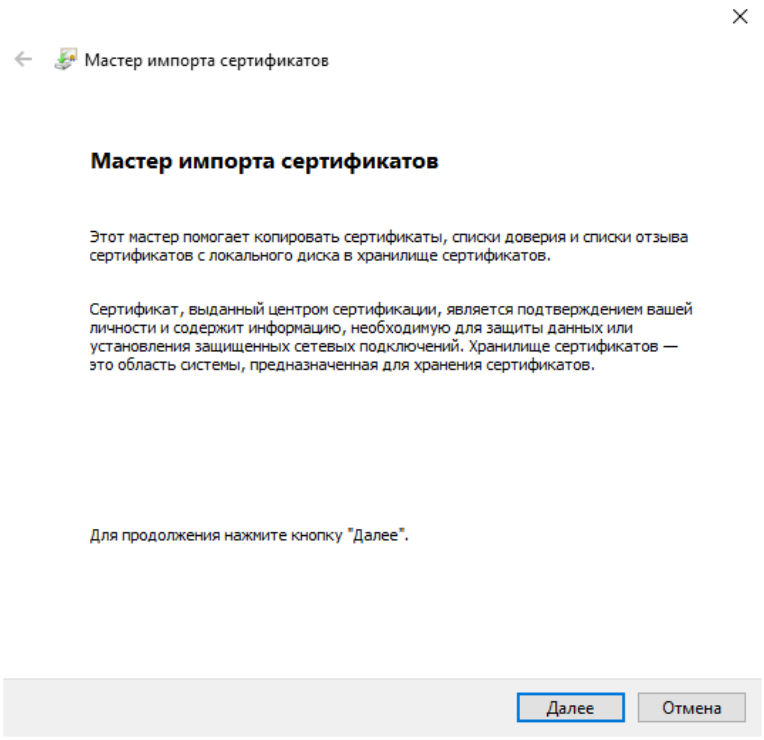
Шаг 8. Выберите **Содержание** → **Сертификаты**;



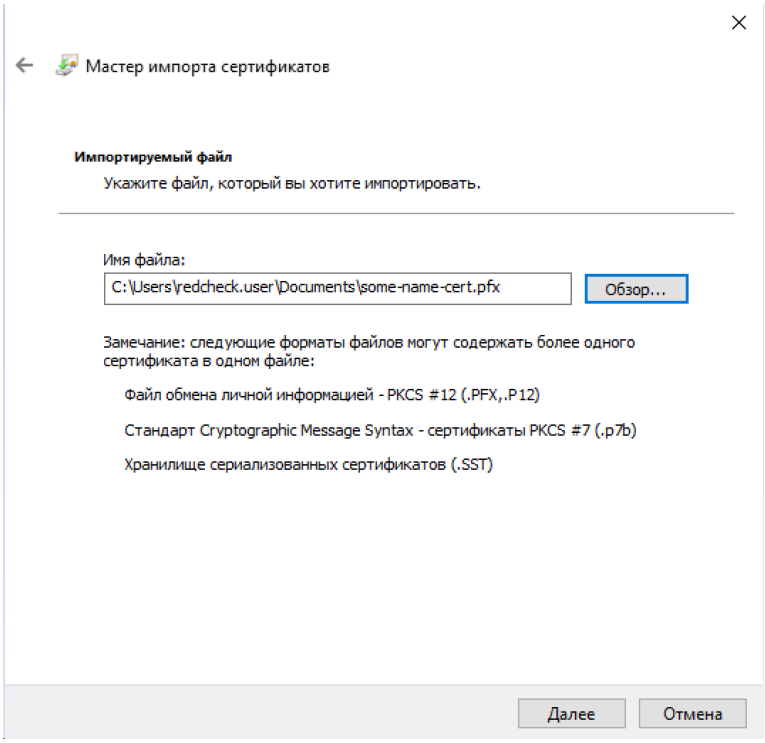
Шаг 9. Перейдите в **Личные** → **Импорт**;



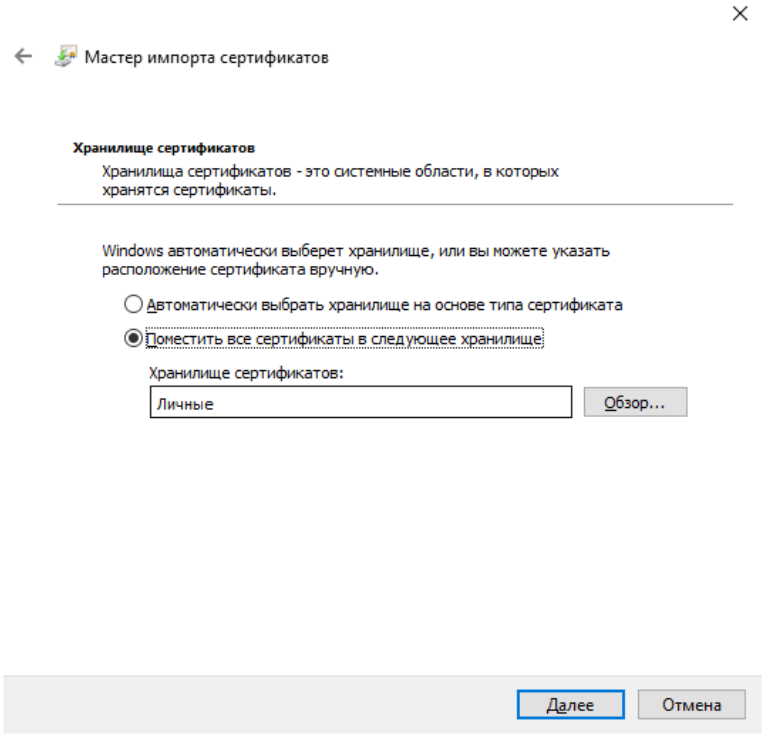
Шаг 10. Откроется **Мастер импорта сертификатов** → **Далее**;



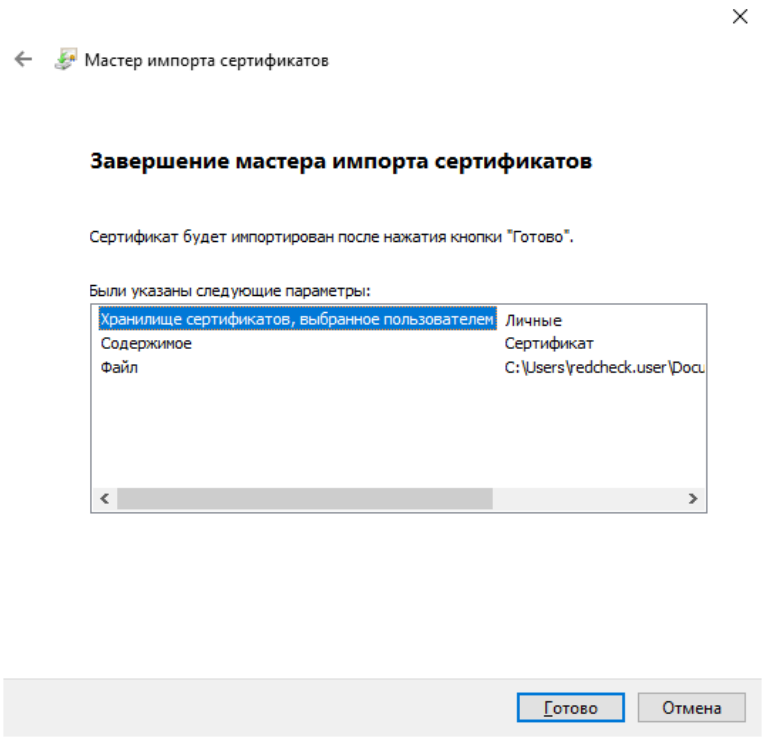
Укажите директорию с импортируемым сертификатом → **Далее**;



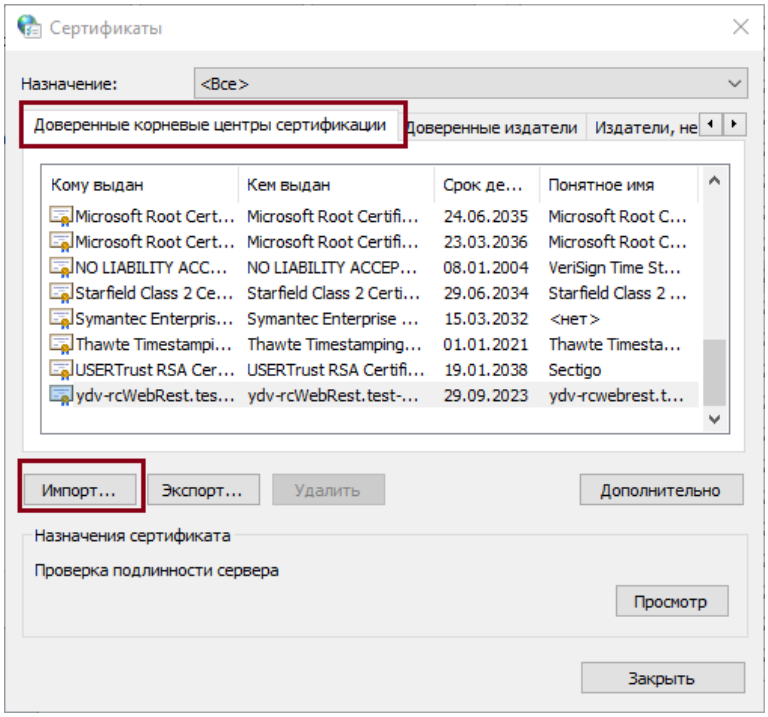
Поместите сертификат в хранилище **Личные** → **Далее**;



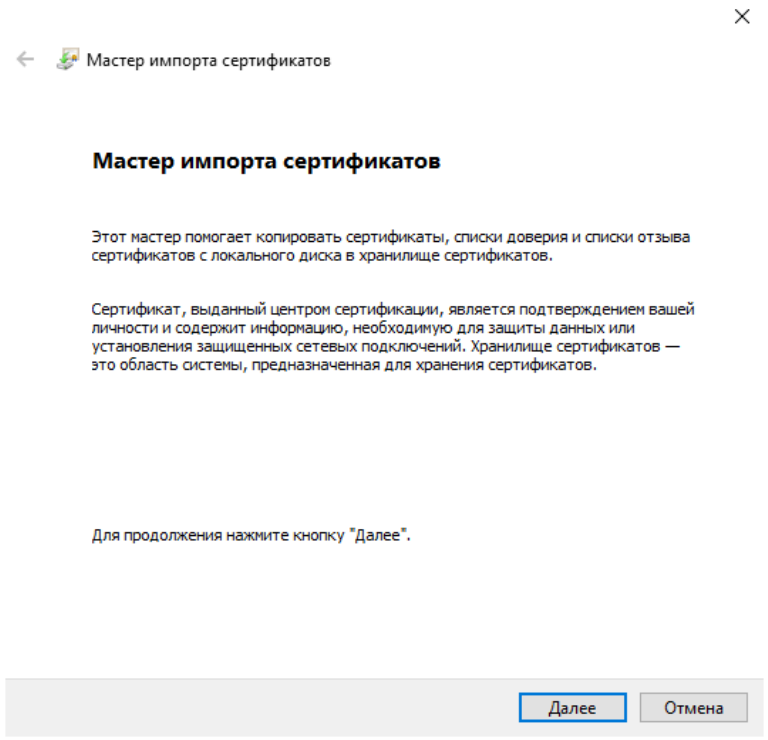
Завершите импорт сертификата, нажав **Готово**;



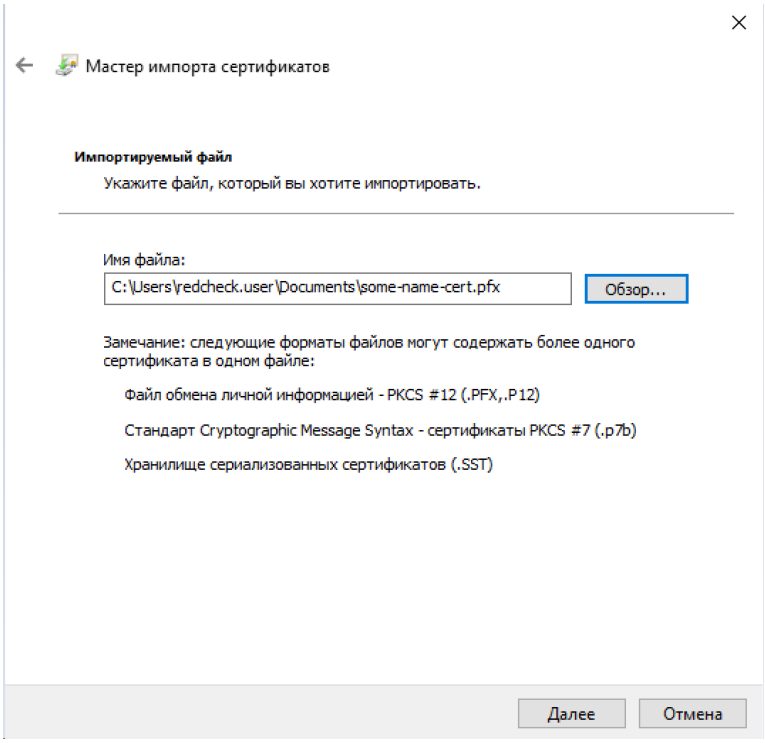
Шаг 11. Перейдите в **Доверенные корневые центры сертификации → Импорт**;



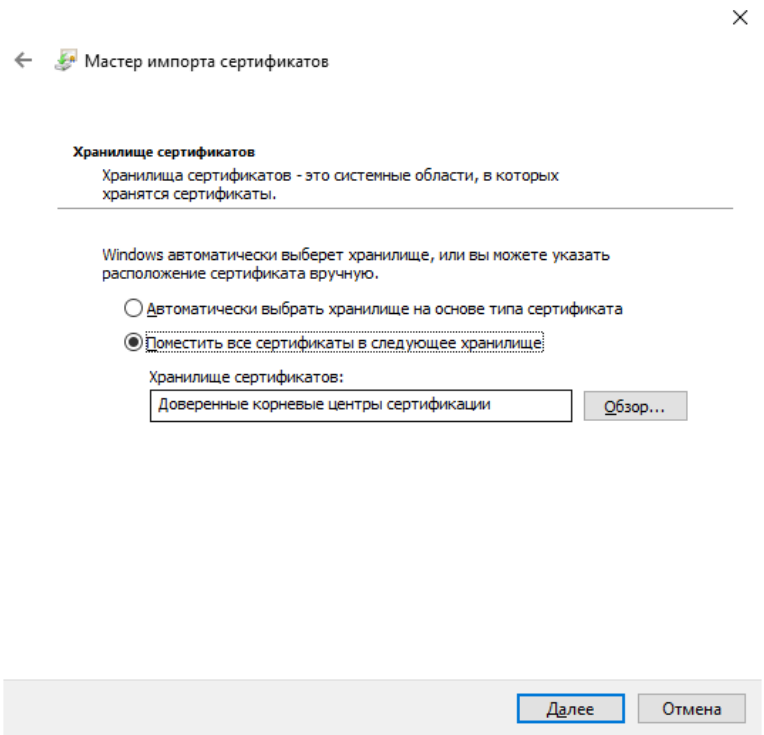
Шаг 12. Откроется **Мастер импорта сертификатов → Далее**;



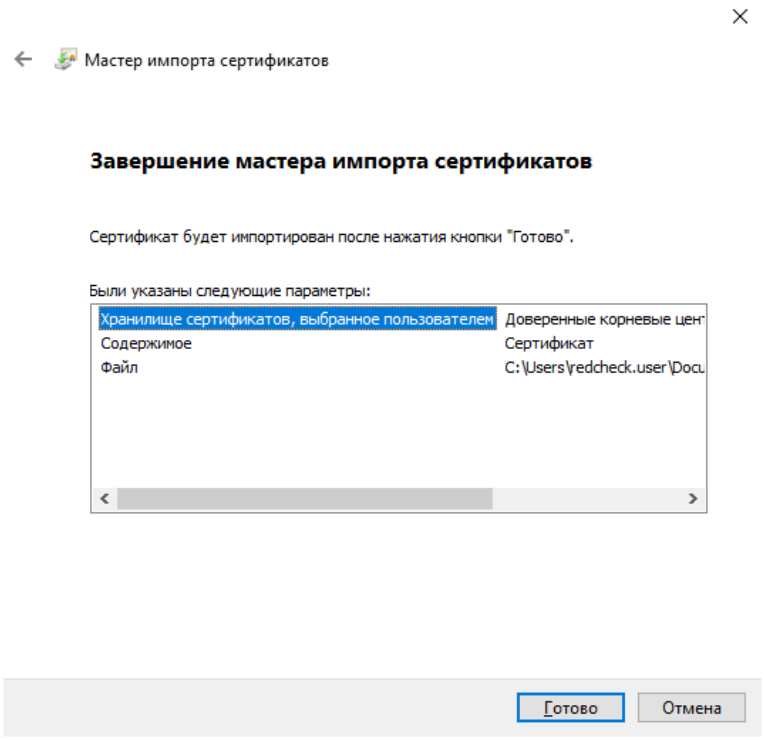
Укажите директорию с импортируемым сертификатом → **Далее**;



Поместите сертификат в хранилище **Доверенные корневые центры сертификации** → **Далее**;

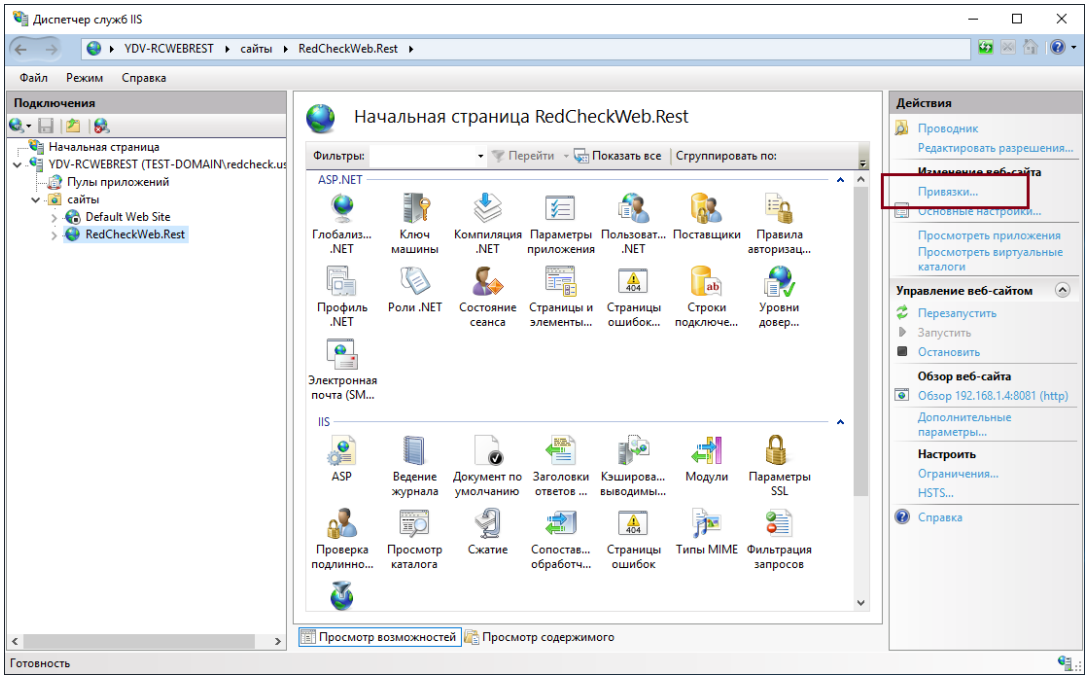


Завершите импорт сертификата, нажав **Готово**;

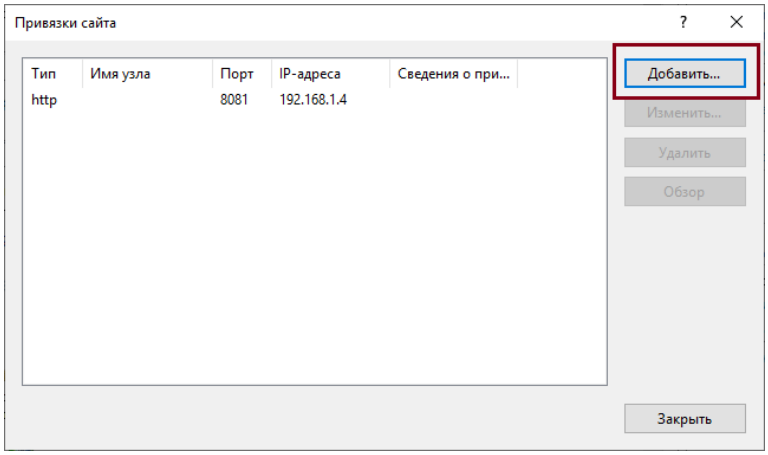


Подключение обработки https-соединений для серверной компоненты RedCheck

Шаг 13. Раскройте **сайты → RedCheckWeb.Rest → Привязки**;

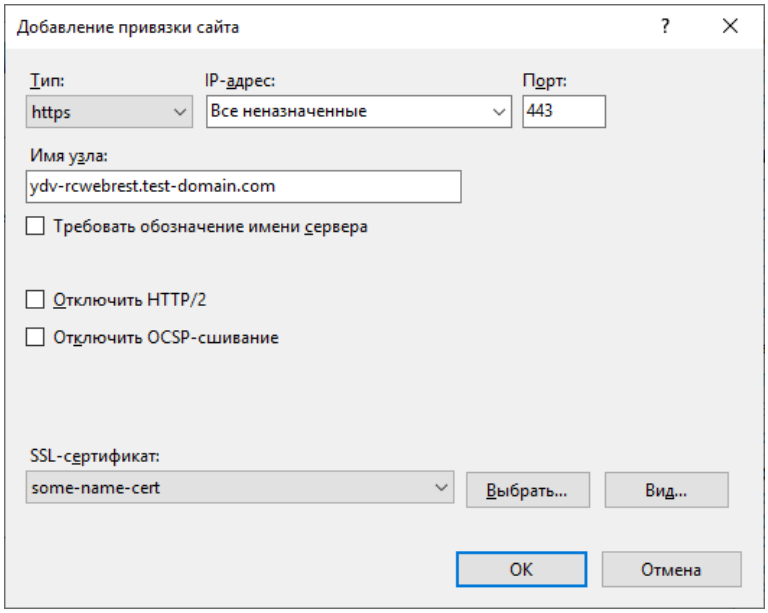


Шаг 14. Нажмите **Добавить**;

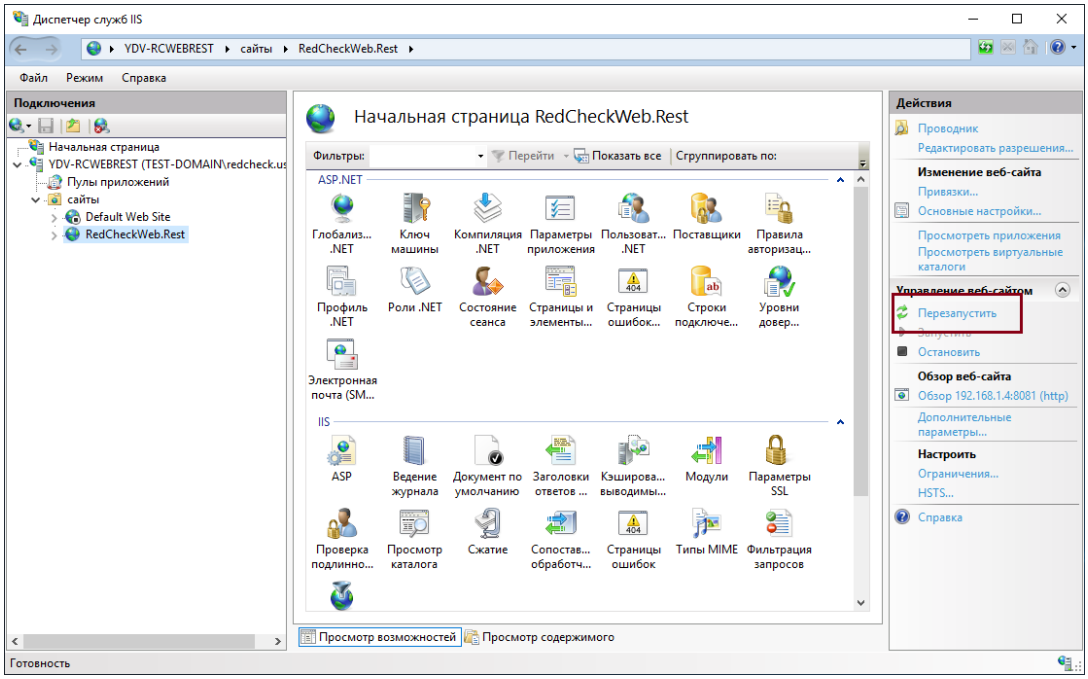


Шаг 15. Укажите параметры привязки → **OK**;

Тип: https;
IP-адрес: Все неназначенные;
Порт: по умолчанию 443;
Имя узла: значение в столбце **Получатель сертификата** (Шаг 4);
SSL-сертификат: созданный сертификат;

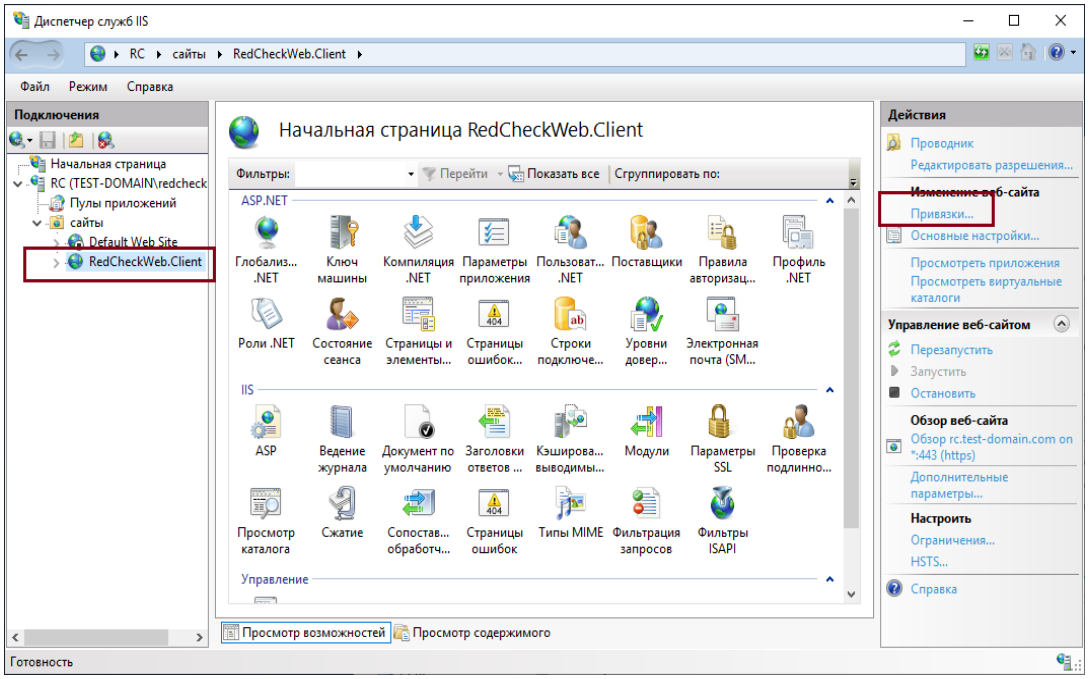


Шаг 16. Нажмите **Перезапустить** в меню действий;

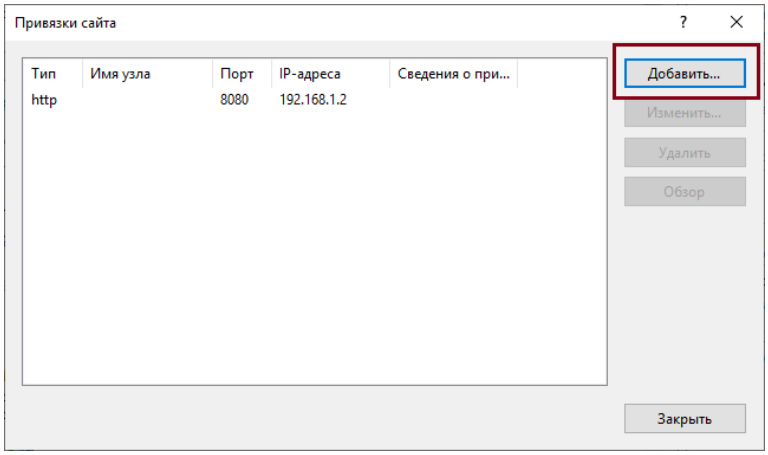


Подключение обработки https-соединений для консоли управления RedCheck

Шаг 17. Раскройте **сайты → RedCheckWeb.Client → Привязки**;

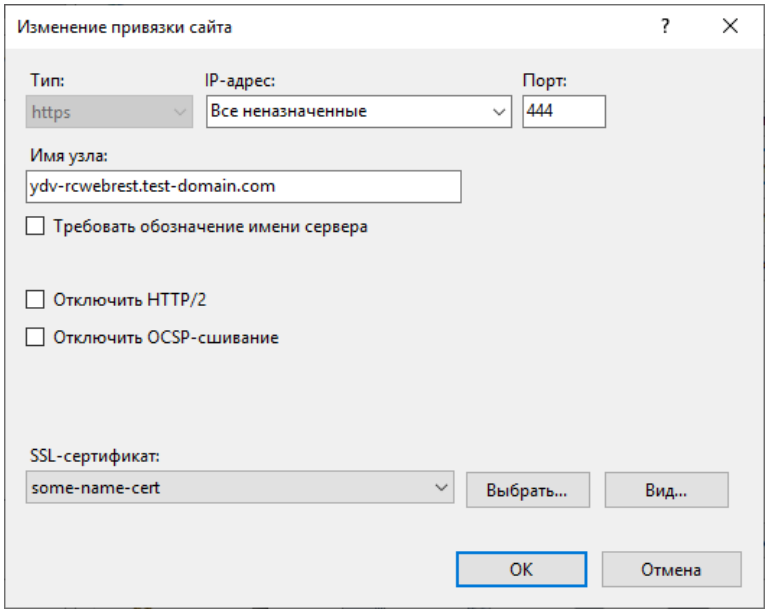


Шаг 18. Нажмите **Добавить**;

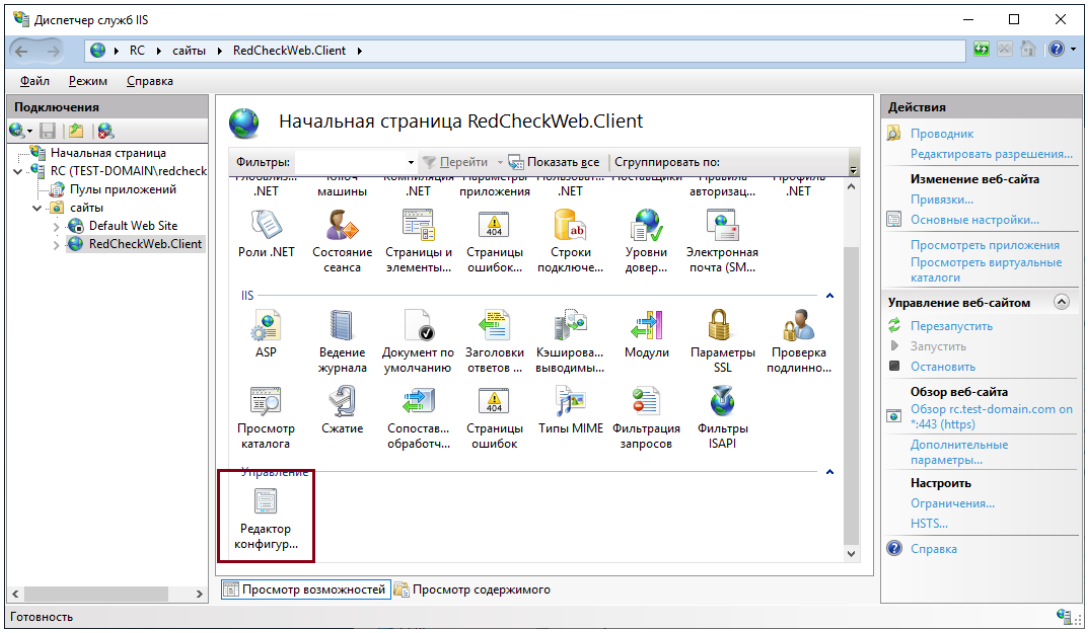


Шаг 19. Укажите параметры привязки → **OK**;

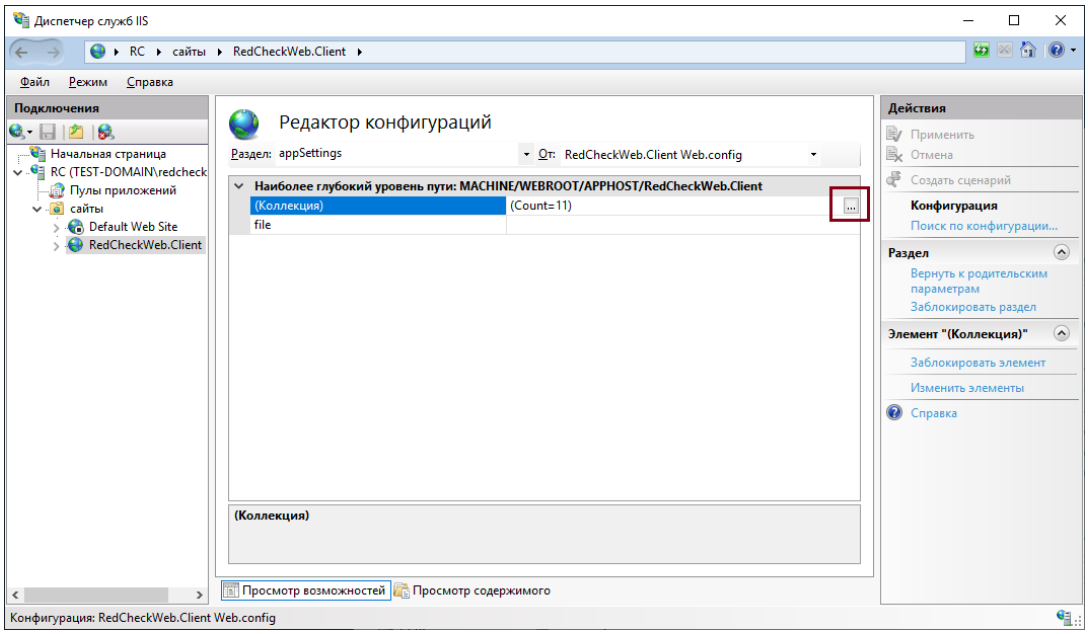
Тип: https;
IP-адрес: Все неназначенные;
Порт: по умолчанию 444;
Имя узла: значение в столбце **Получатель сертификата** (Шаг 4);
SSL-сертификат: созданный сертификат;



Шаг 20. Откройте **Редактор конфигураций**;

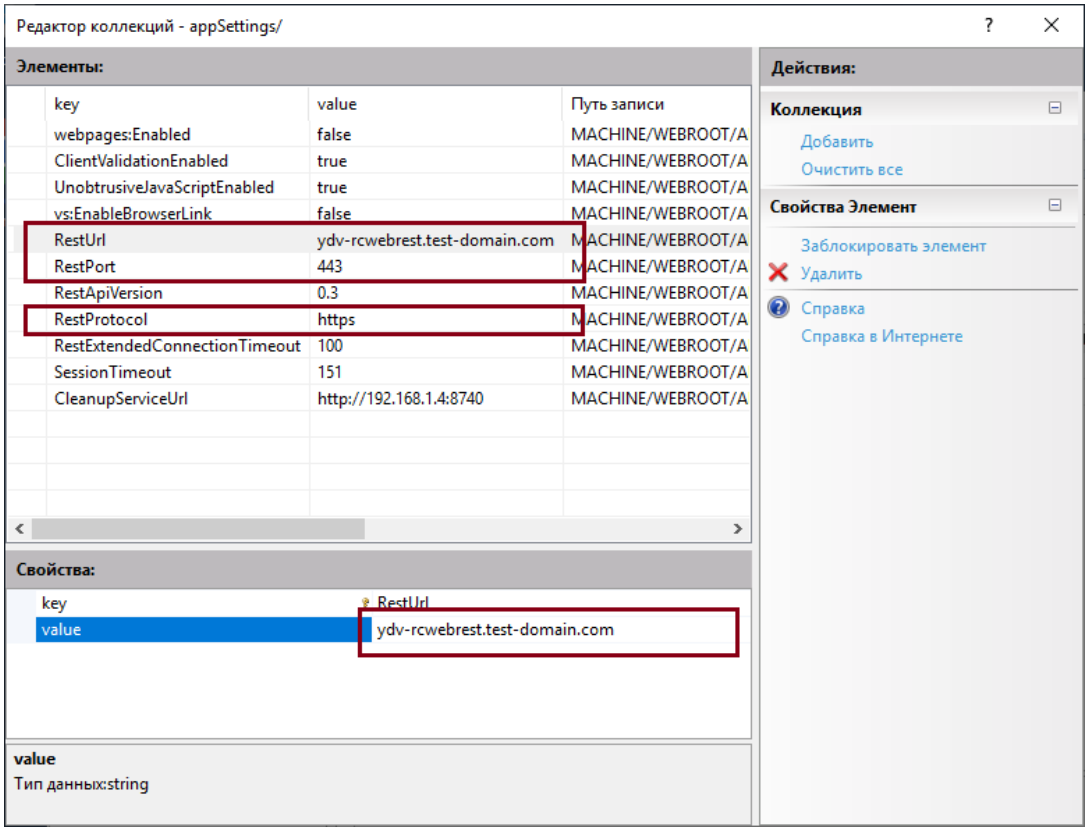


Шаг 21. Раскройте параметры конфигурации;

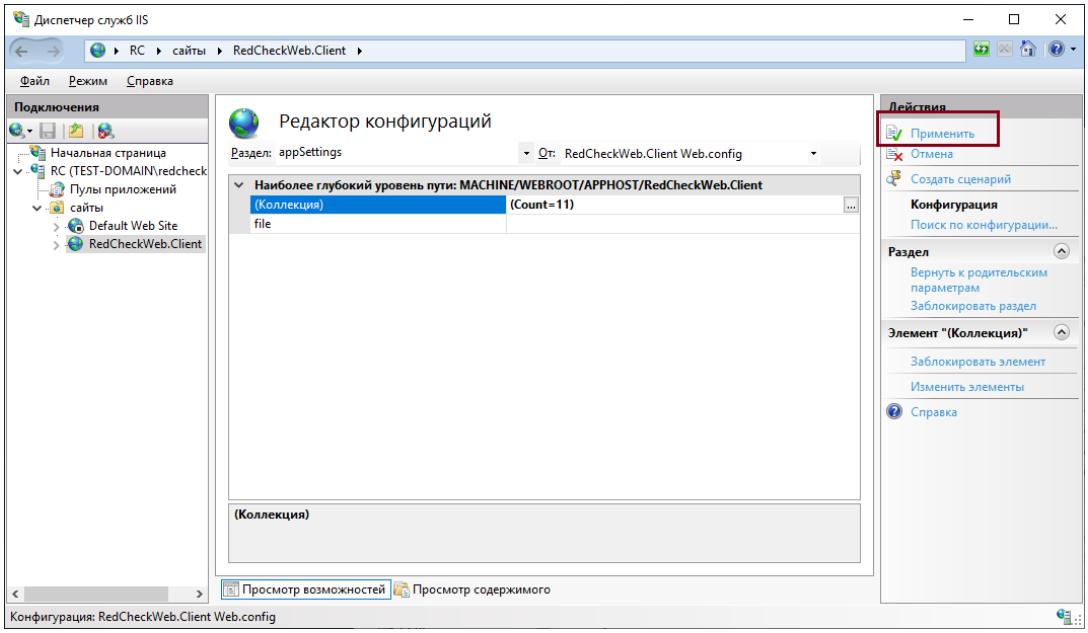


Шаг 22. Исправьте значения в полях:

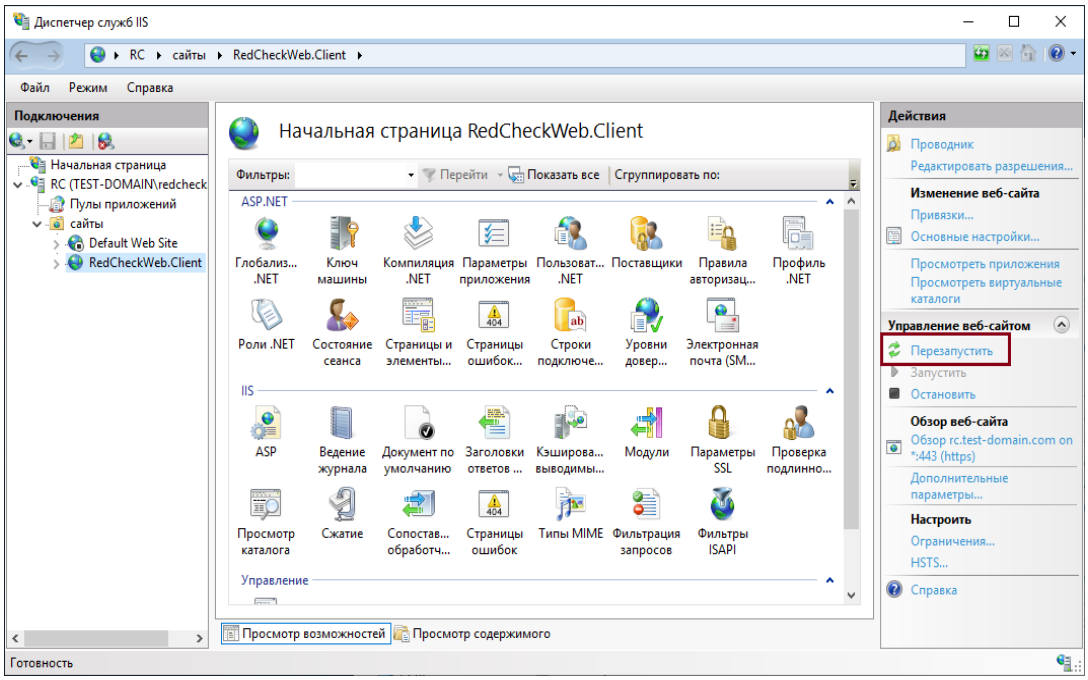
RestUrl: имя узла серверного компонента, указанное в привязке RestAPI;
RestPort: 443;
RestProtocol: https;



Шаг 23. Нажмите **Применить** в меню действий;



Шаг 24. Нажмите **Перезапустить** в меню действий.



4.3.8 Установка службы синхронизации

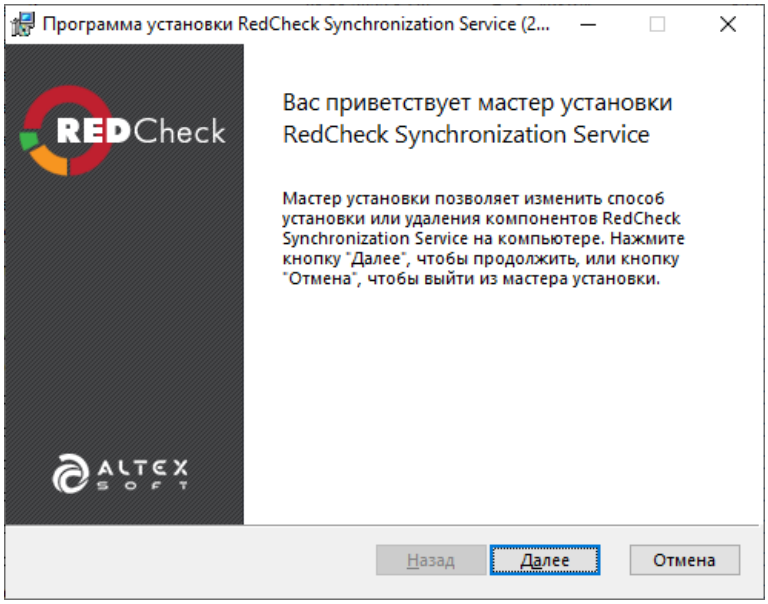
Перед установкой убедитесь, что на компьютере есть все необходимые компоненты:

- СУБД (4.1 Установка СУБД);
- Microsoft .NET Framework 4.8 (4.3.2 Установка Microsoft .NET Framework);
- Серверный компонент RedCheck (4.3.4 Установка серверного компонента Web-версии RedCheck).

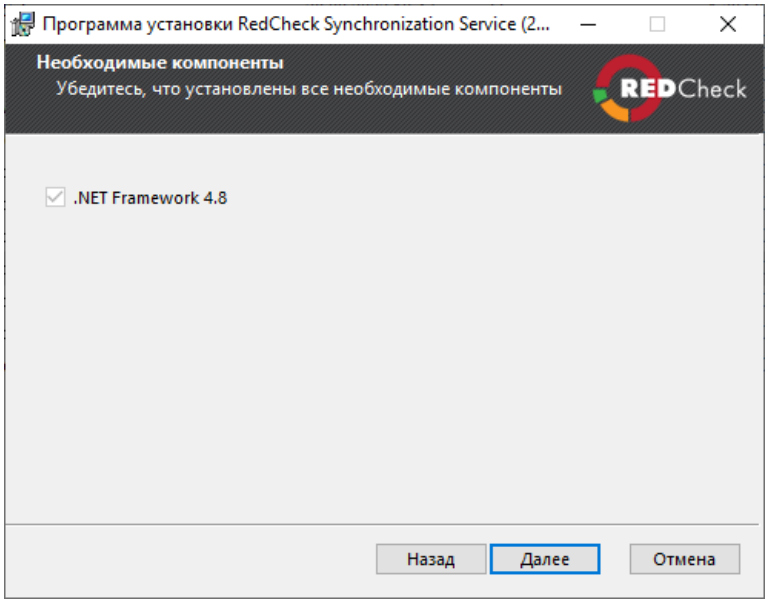
Установка посторонних компонентов может мешать работе Системы.

Возможна автоматическая установка через командную строку (4.6.2.4 Служба синхронизации).

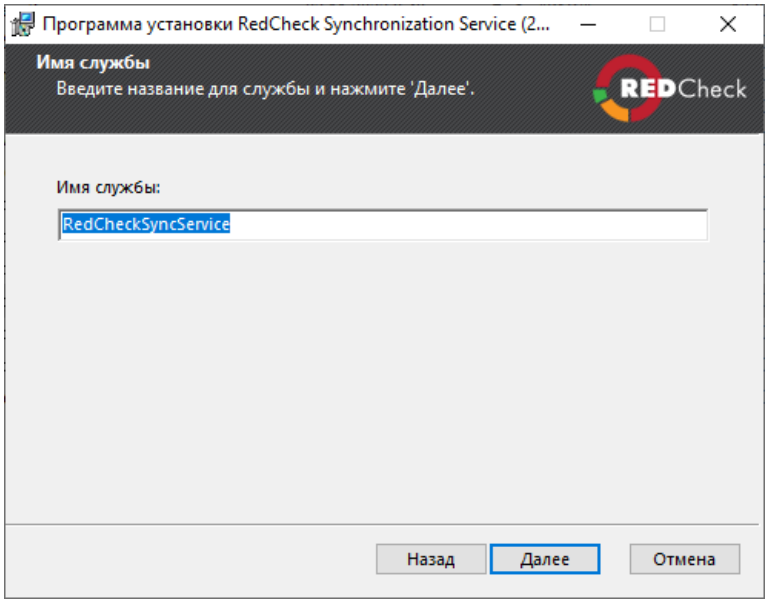
Шаг 1. Запустите установочный пакет RedCheckSyncService.msi → **Далее**;



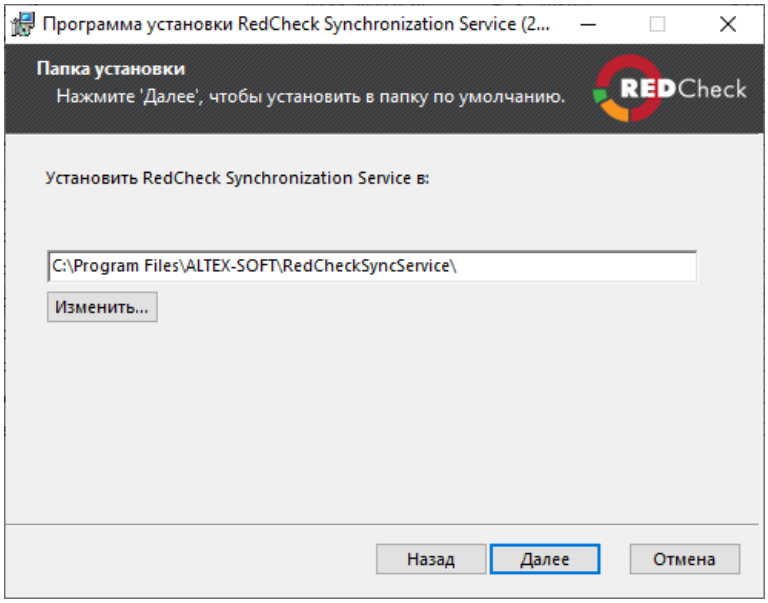
Шаг 2. Инсталлятор проверит наличие всех необходимых компонентов → **Далее**;



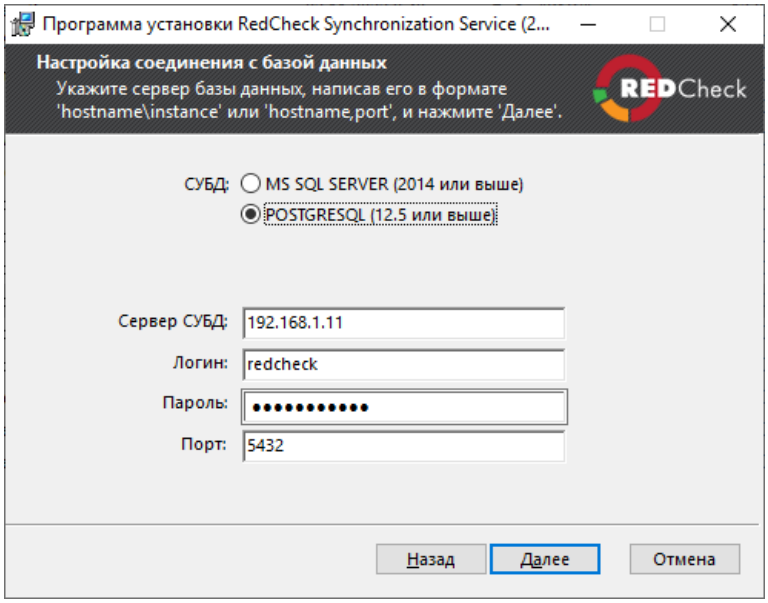
Шаг 3. Укажите название для службы синхронизации → **Далее**;



Шаг 4. Укажите директорию для службы синхронизации → **Далее**;

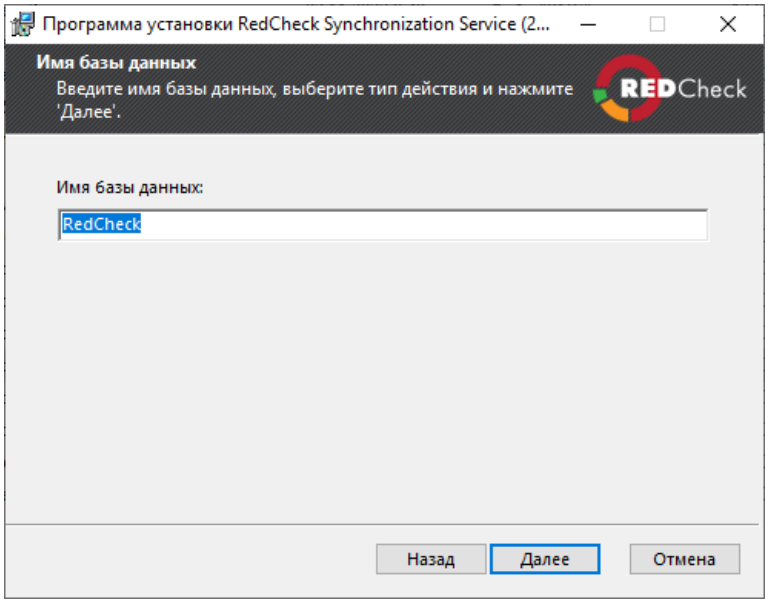


Шаг 5. Введите параметры для подключения к СУБД → **Далее**;



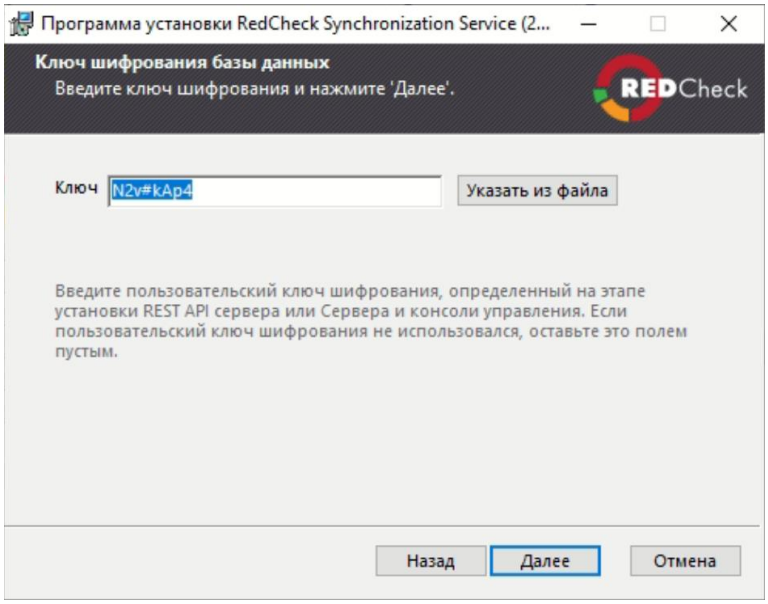
Сервер СУБД: имя узла/IP-адрес, на котором находится сервер СУБД;
Логин: имя пользователя, с правами на создание БД. Данный пользователь будет владельцем БД RedCheck;
Пароль: пароль указанного пользователя;
Порт: сетевой порт для сервера СУБД (по умолчанию для Microsoft SQL Server - 1433, для PostgreSQL - 5432);

Шаг 6. Укажите имя БД (RedCheck по умолчанию) → **Далее**;



Шаг 7. Введите текущий ключ шифрования → **Далее**;

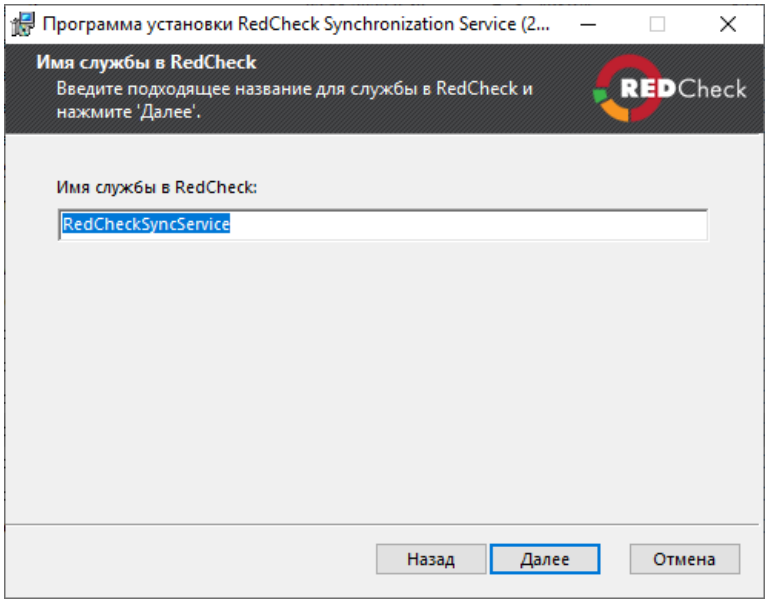
При установке серверного компонента указывается ключ шифрования, который необходим для корректной работы служб синхронизации и сканирования. При последовательной установке компонентов ключ шифрования будет подставлен в поле автоматически.



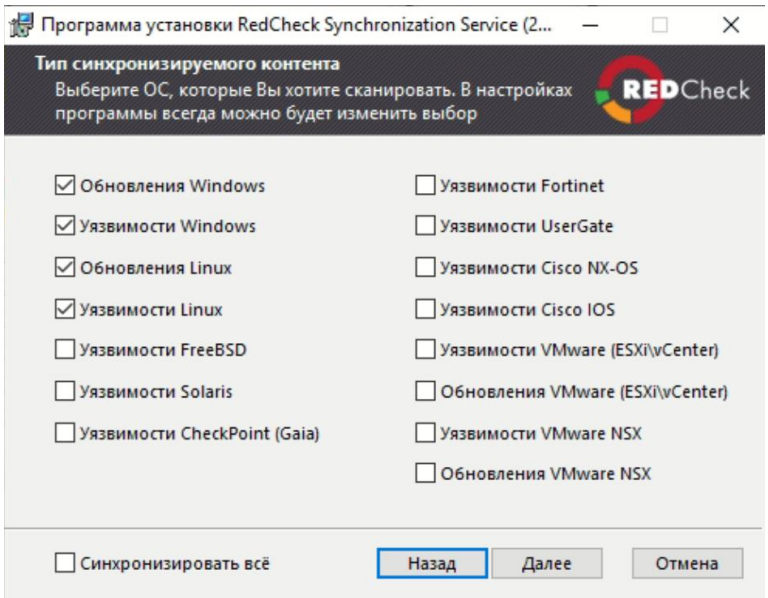
Нажмите **Указать из файла** (с расширением .xml), чтобы использовать уже имеющийся ключ шифрования.

```
<?xml version="1.0" encoding="utf-8"?>
<sckd>N2v#kAp4</sckd>
```

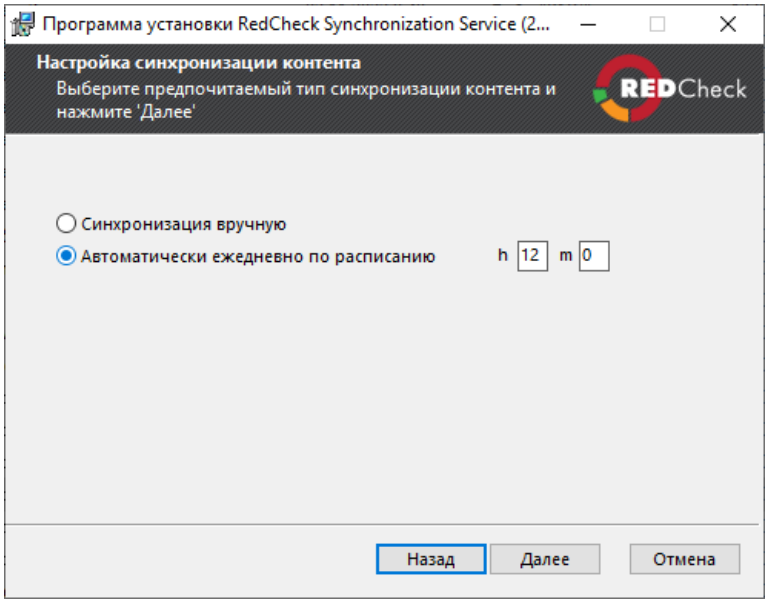
Шаг 8. Укажите название для службы синхронизации в RedCheck → **Далее**;



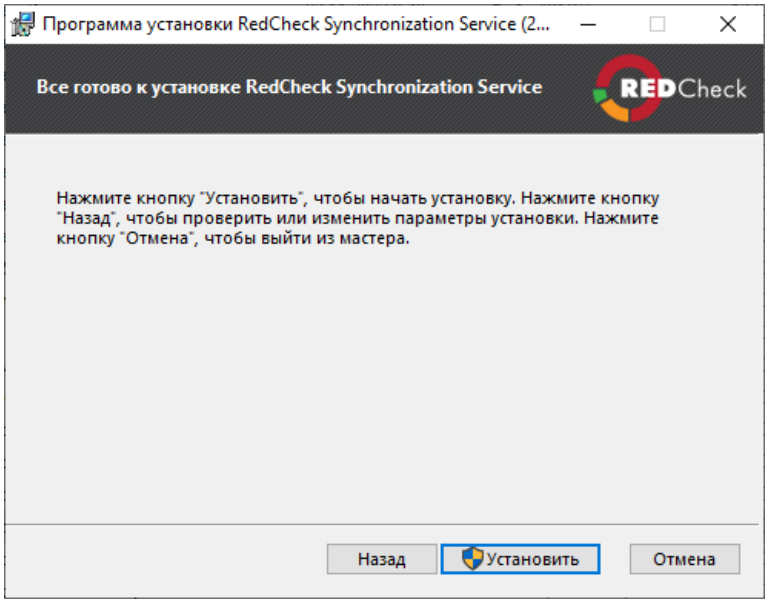
Шаг 9. Укажите синхронизируемый контент безопасности → **Далее**;



Шаг 10. Настройте параметры синхронизации (рекомендуется оставить значения по умолчанию **Автоматически...**) → **Далее**;



Шаг 11. Нажмите **Установить**;



После окончания установки нажмите **Готово**.

4.3.9 Установка службы сканирования

Установка двух и более служб сканирования на одном хосте не поддерживается.

Перед установкой убедитесь, что на компьютере есть все необходимые компоненты:

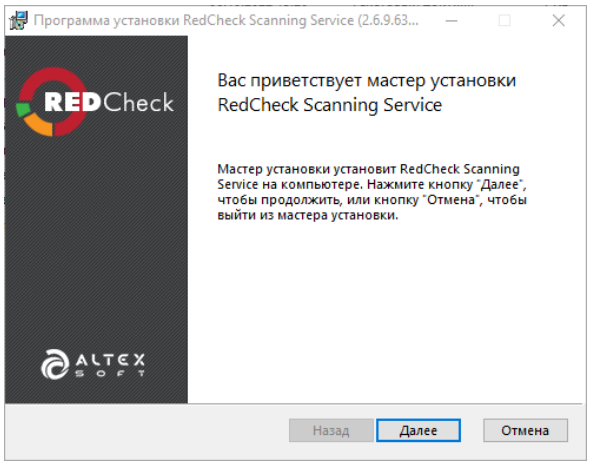
- СУБД (4.1 Установка СУБД);
- Microsoft .NET Framework 4.8 (4.3.2 Установка Microsoft .NET Framework);
- Серверный компонент RedCheck (4.3.4 Установка серверного компонента Web-версии RedCheck);
- VC++ 2013 Redistributable и VC++ 2015 Redistributable (4.3.9.2 Установка VC++ 2013 / 2015 Redistributable).

Установка посторонних компонентов может мешать работе Системы.

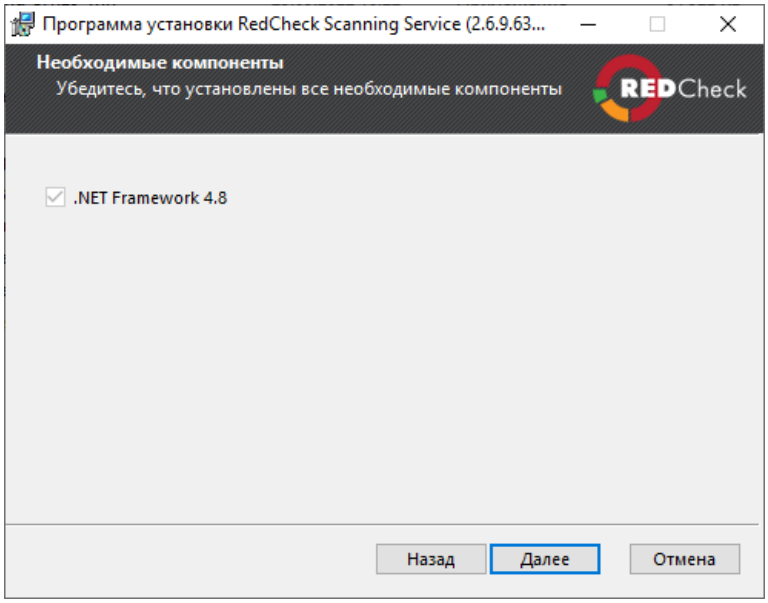
При использовании заданий **Аудит в режиме «Пентест»**, **Обнаружение хостов** обновление ALTXmap для службы сканирования выполняется обязательно.

Возможна автоматическая установка через командную строку (4.6.2.3 Служба сканирования)

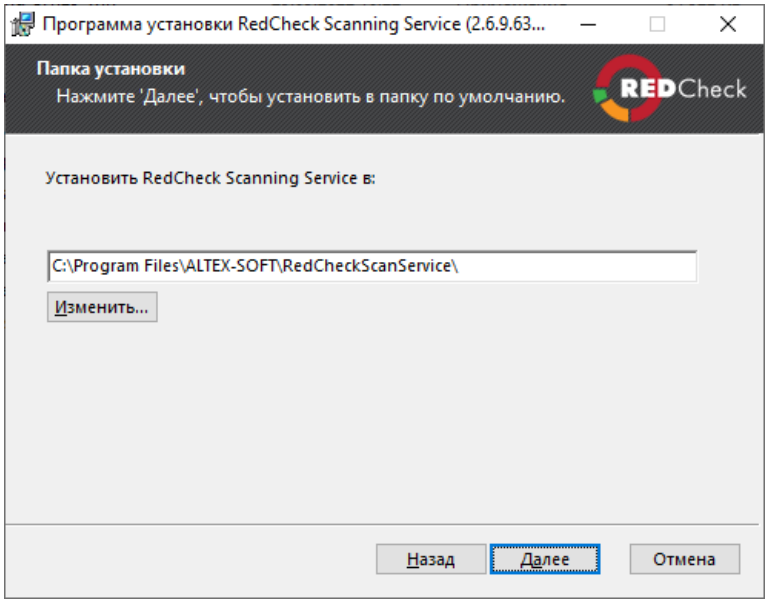
Шаг 1. Запустите установочный пакет RedCheckScanService.msi → **Далее**;



Шаг 2. Инсталлятор проверит наличие всех необходимых компонентов → **Далее**;

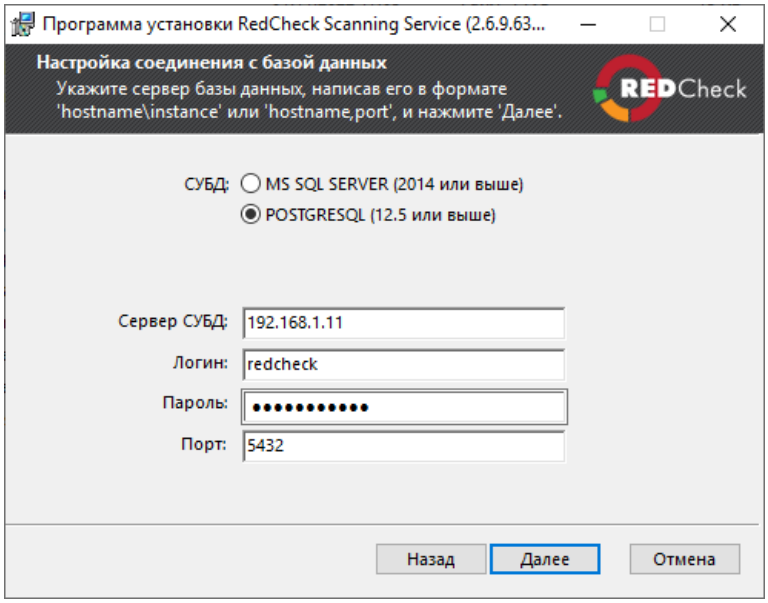


Шаг 3. Укажите директорию для сервера сканирования → **Далее**;

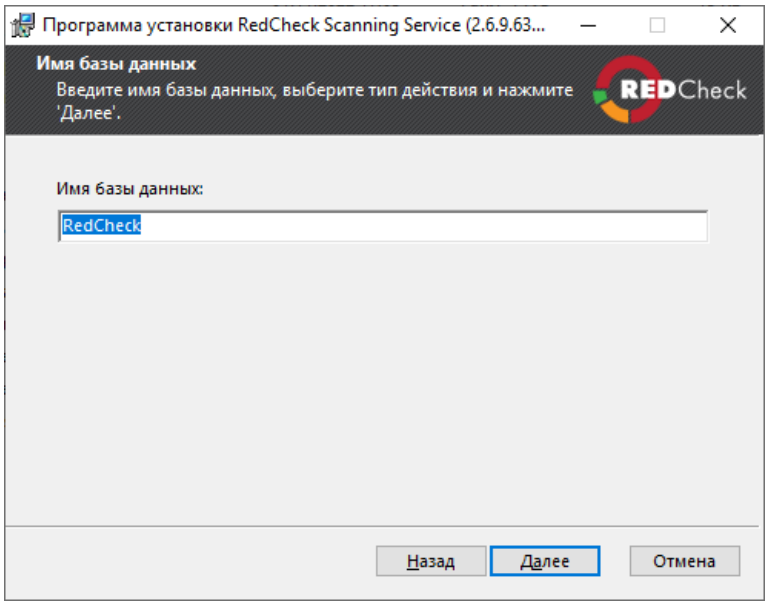


Шаг 4. Введите параметры для подключения к СУБД → **Далее**;

Сервер СУБД: имя узла/IP-адрес, на котором находится сервер СУБД;
Логин: имя пользователя, с правами на создание БД. Данный пользователь будет владельцем БД RedCheck;
Пароль: пароль указанного пользователя;
Порт: сетевой порт для сервера СУБД (по умолчанию для Microsoft SQL Server - 1433, для PostgreSQL - 5432);

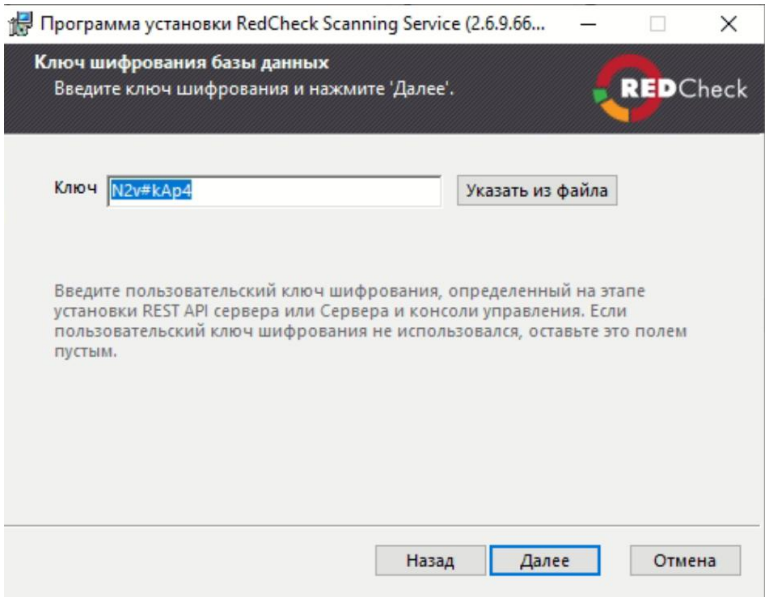


Шаг 5. Укажите имя БД (RedCheck по умолчанию) → **Далее**;



Шаг 6. Введите текущий ключ шифрования → **Далее**;

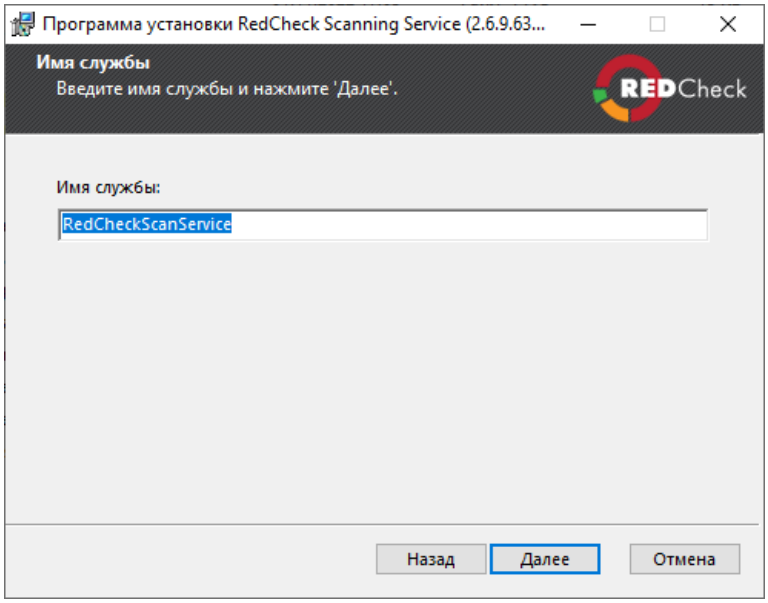
При установке серверного компонента указывается ключ шифрования, который необходим для корректной работы служб синхронизации и сканирования. При последовательной установке компонентов ключ шифрования будет подставлен в поле автоматически.



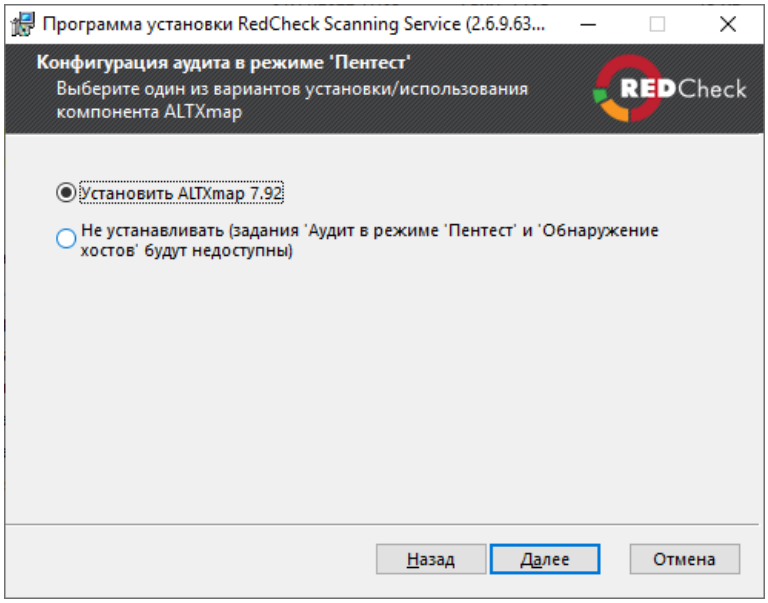
Нажмите **Указать из файла** (с расширением .xml), чтобы использовать уже имеющийся ключ шифрования.

```
<?xml version="1.0" encoding="utf-8"?>
<sckd>N2v#kAp4</sckd>
```

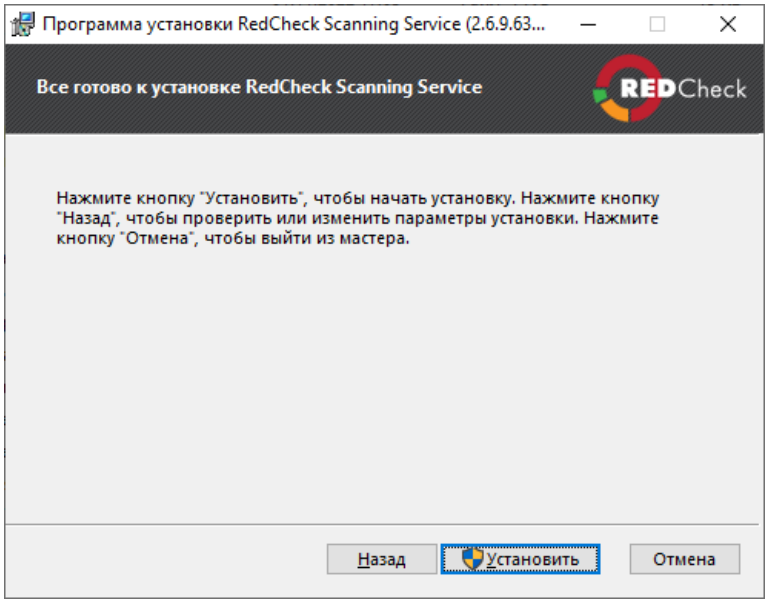
Шаг 7. Укажите название для сервера сканирования → **Далее**;



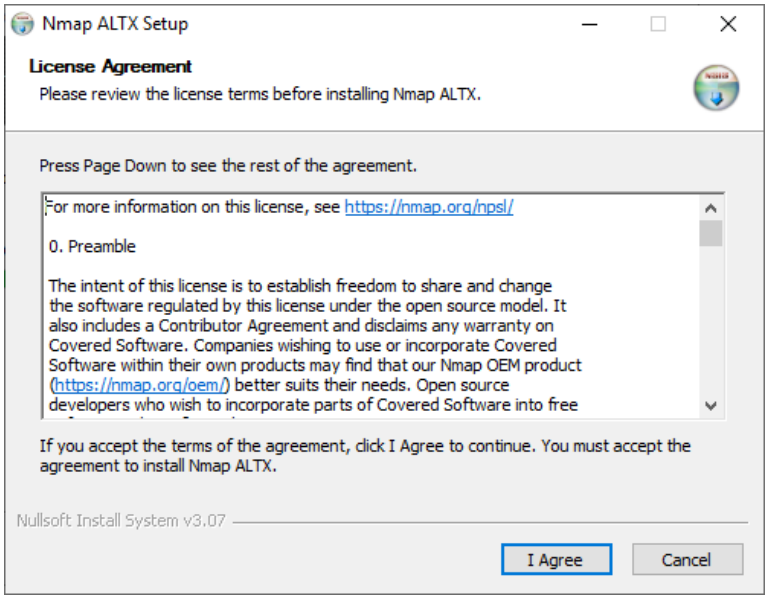
Шаг 8. При необходимости установите ALTXmap → **Далее**;



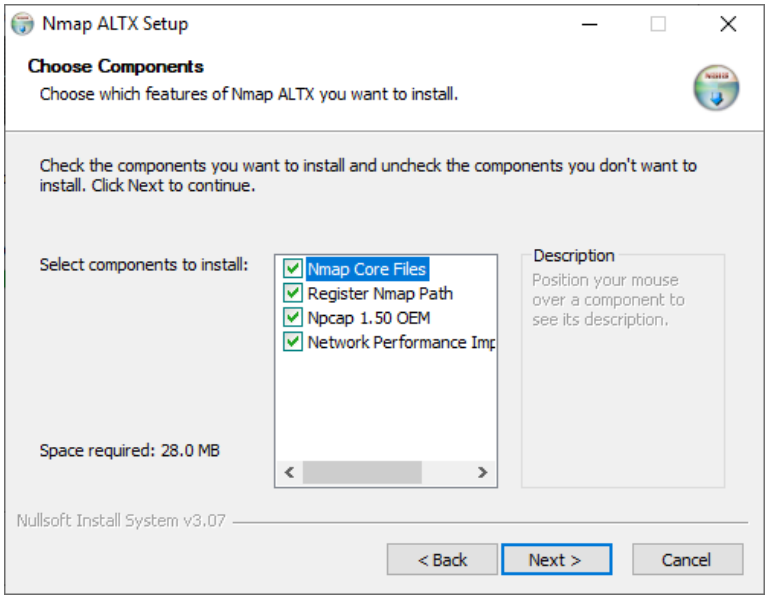
Шаг 9. Нажмите **Установить**;



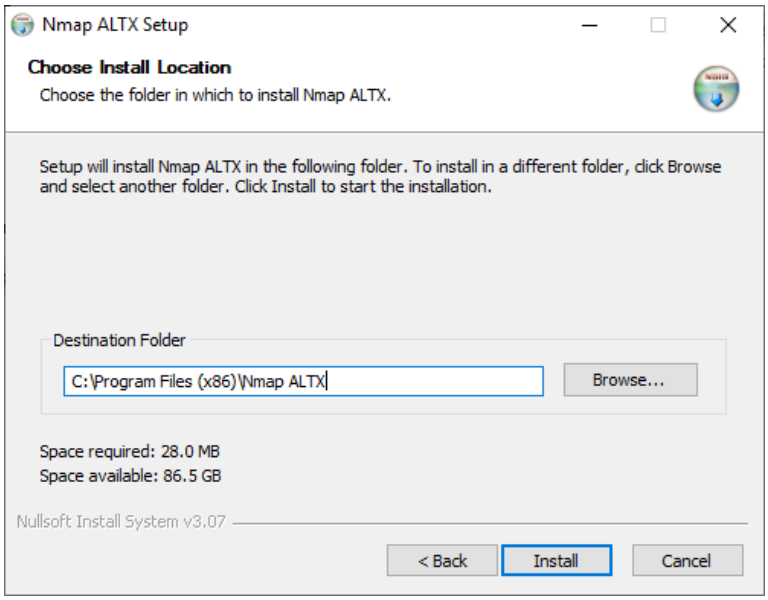
Шаг 10. Во время установки откроется дополнительный инсталлятор Nmap ALTX → **I Agree**;



Шаг 11. Выберите устанавливаемые компоненты (рекомендуется оставить значения по умолчанию) → **Next**;



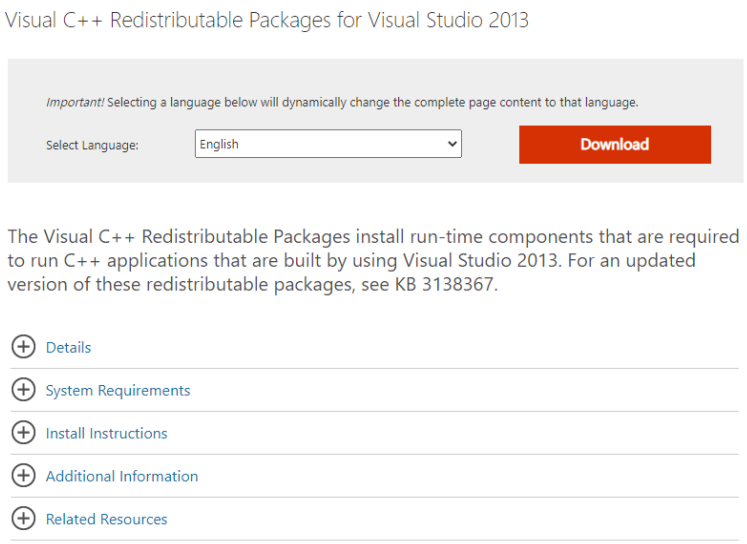
Шаг 12. Укажите директорию для установки → **Install**;



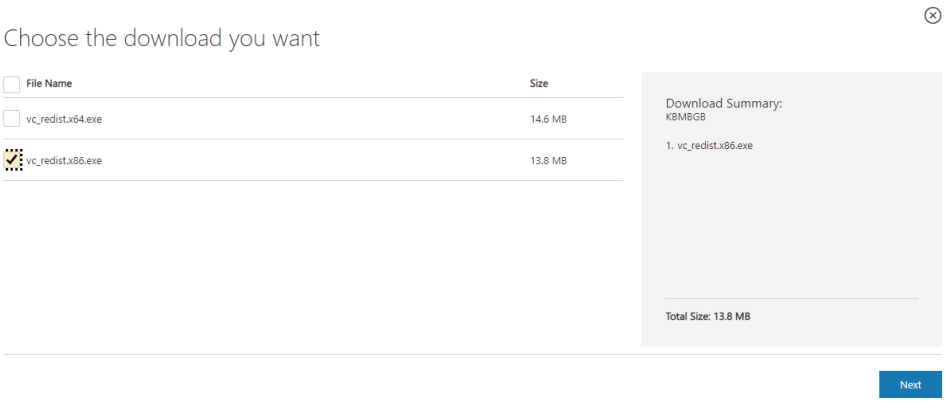
После окончания установки нажмите **Готово**.

4.3.9.1 Установка VC++ 2013 / 2015 Redistributable

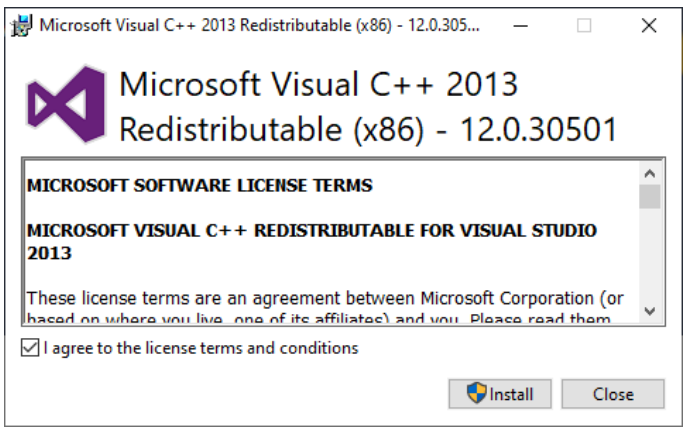
Шаг 1. Перейдите на страницу загрузки VC++ 2013 (или VC++ 2015) с сайта разработчика → **Download**;



Шаг 2. Выберите версию пакета **vcredist_x86.exe** / **vc_redist.x86.exe** → **Next**;



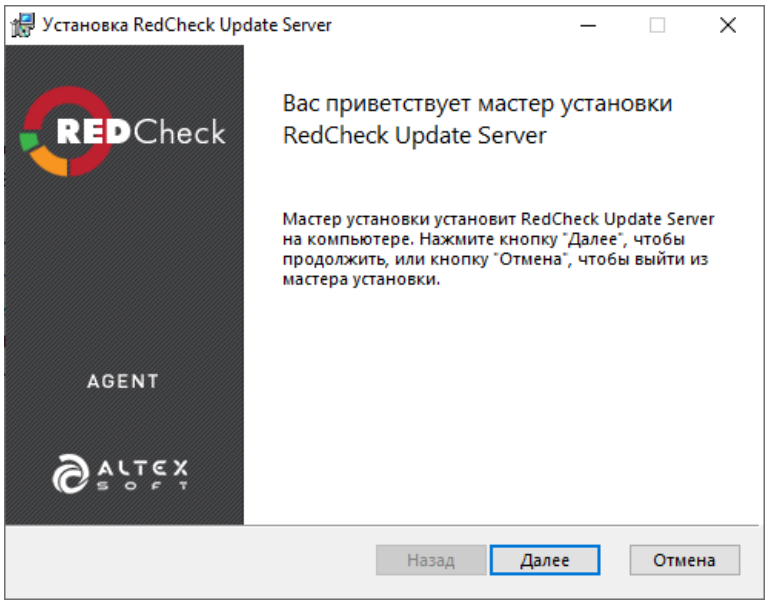
Шаг 3. Откройте скачанный файл → **Install** → дождитесь окончания установки;



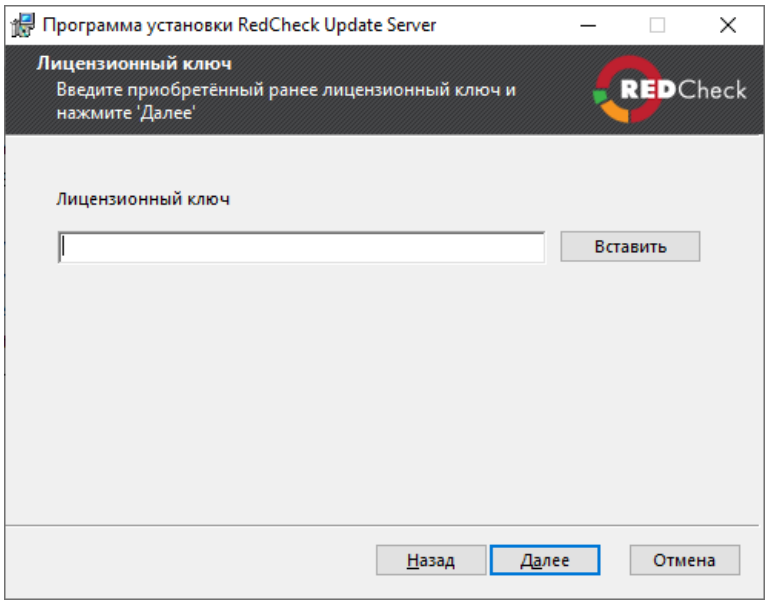
4.4 Установка RedCheck Update Server

Компонент не является обязательным и лицензируется отдельно. Установка RedCheck Update Server производится в DMZ-сегменте сети.

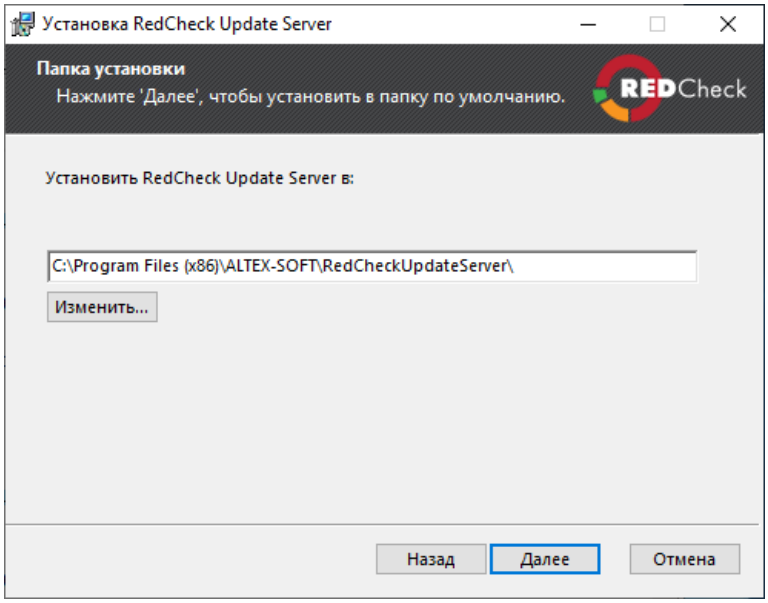
Шаг 1. Запустите инсталляционный пакет **RedCheckUpdateServer.msi**;



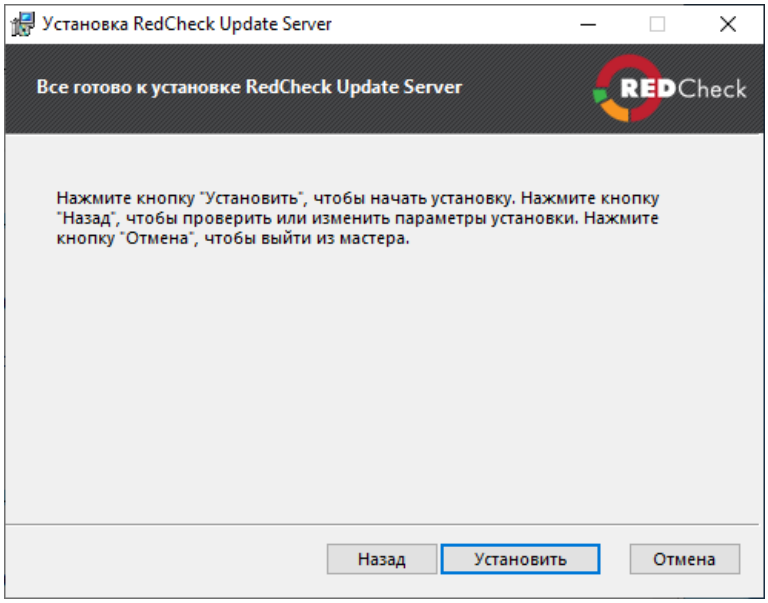
Шаг 2. Введите лицензионный ключ → **Далее**;



Шаг 3. Укажите директорию для установки;



Шаг 4. Нажмите **Установить**.



После установки необходимо произвести настройку (5.3.3 Синхронизация через RedCheck Update Server).

4.5 Установка агента RedCheck (Windows)

Агент сканирования – компонент RedCheck, предназначенный для сканирования хостов, ограниченных политикой ИБ организации (например, запрет или ограничение использования WMI, WinRM, отсутствие возможности использовать УЗ администратора), а также для обеспечения быстродействия и повышенной надёжности сканирования.

Данный компонент работает только по запросу от сервера сканирования в рамках назначенной задачи аудита.

Содержание

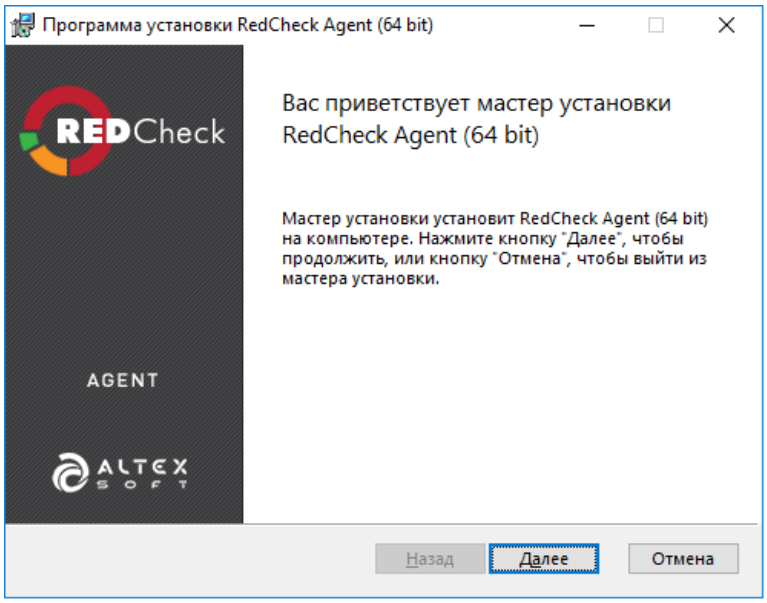
4.5.1 Установка на сканируемом хосте в ручном режиме

Перед установкой убедитесь, что на компьютере есть все необходимые компоненты:

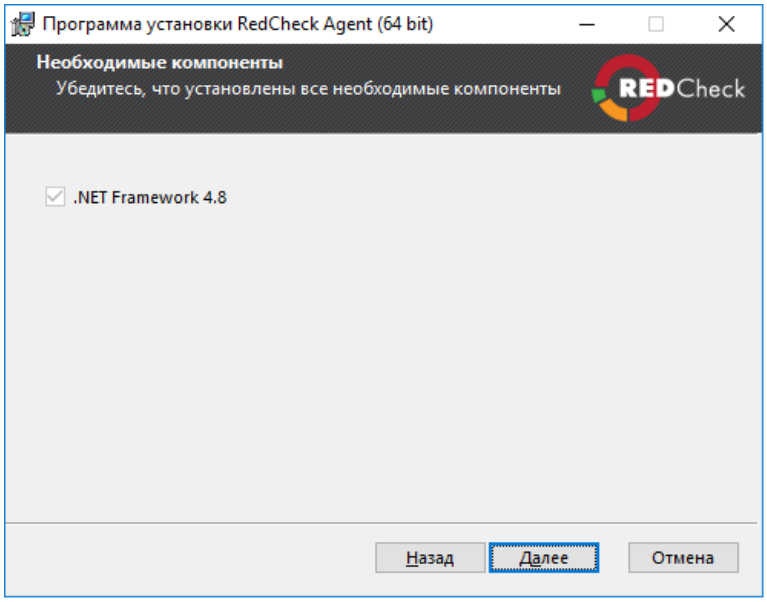
- Microsoft .NET Framework 4.8 (4.3.2 Установка Microsoft .NET Framework).

Возможна автоматическая установка через командную строку (4.6.3 Агент RedCheck)

Шаг 1. Запустите установочный файл RedCheckAgent.msi на сканируемом хосте → **Далее**;

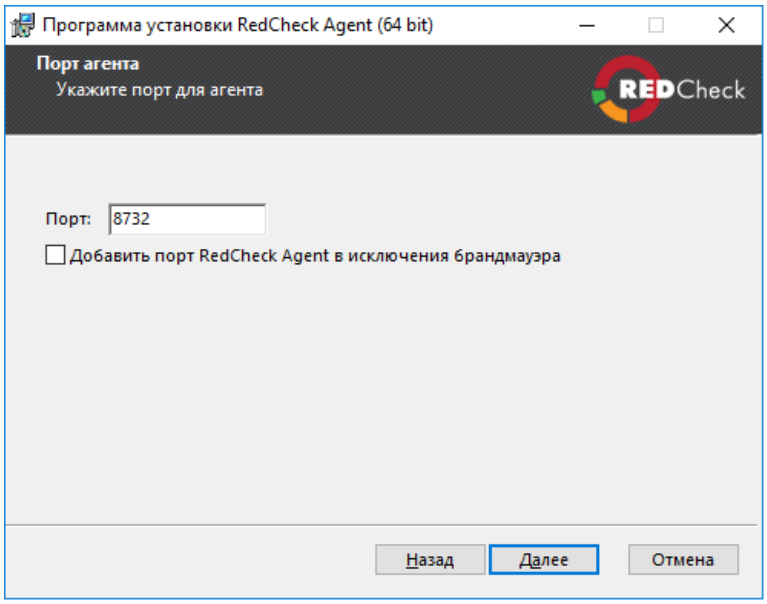


Шаг 2. Инсталлятор проверит наличие всех необходимых компонентов → **Далее**;

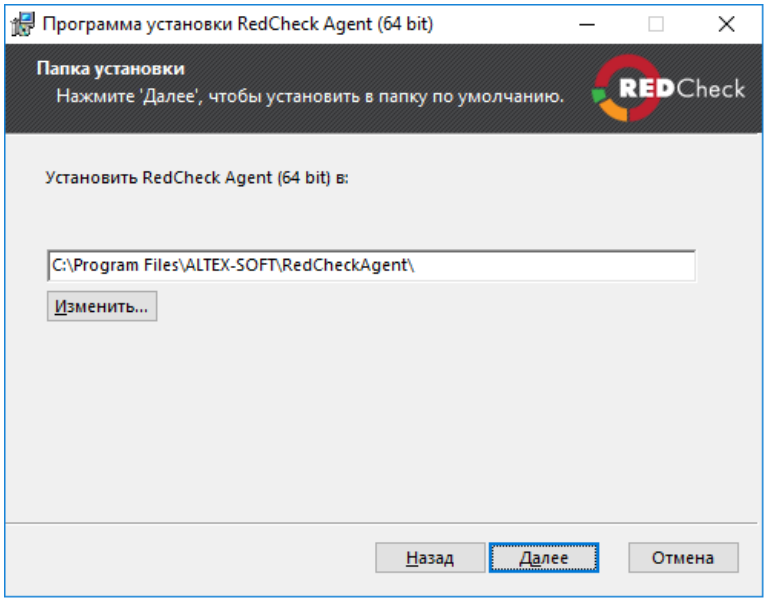


Шаг 3. Задайте порт агента (по умолчанию 8732) и отметьте поле **Добавить порт... в исключение брандмауэра** → **Далее**;

Изменить порт можно после установки (5.11.2 Изменение порта для агента RedCheck).

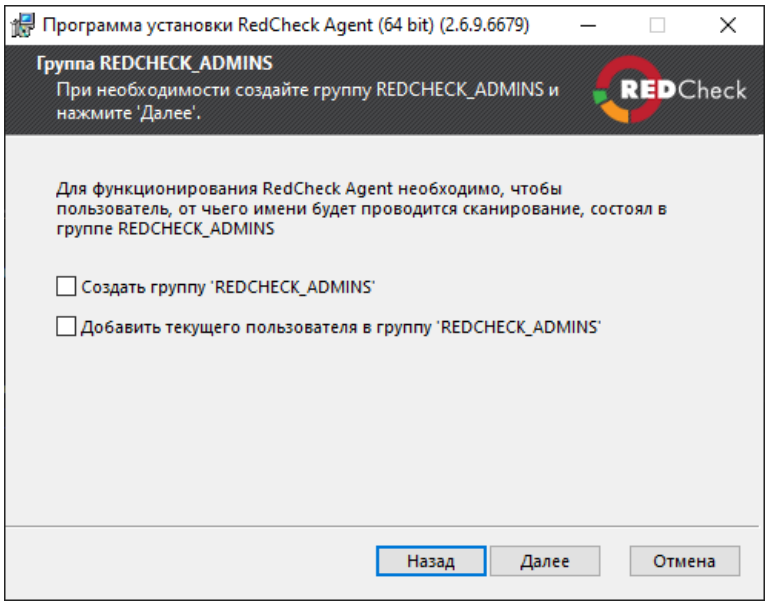


Шаг 4. Укажите директорию для установки агента → **Далее**;



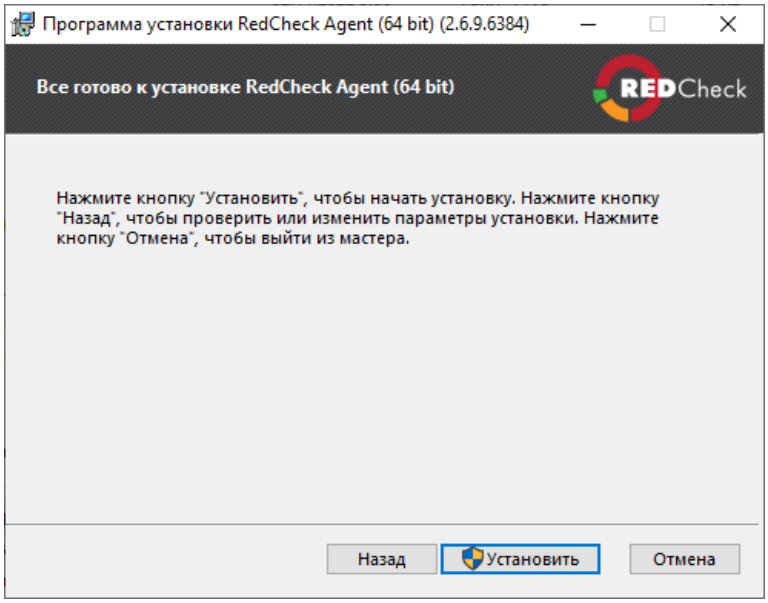
Шаг 5. По необходимости отметьте создание локальной группы безопасности REDCHECK_ADMINS и добавление в нее пользователя, из под которого производится установка агента → **Далее**;

Членство в группе безопасности REDCHECK_ADMINS требуется для корректной работы агента.



Если хост находится в домене или на нем уже имеется группа безопасности REDCHECK_ADMINS, данный раздел будет пропущен при установке.

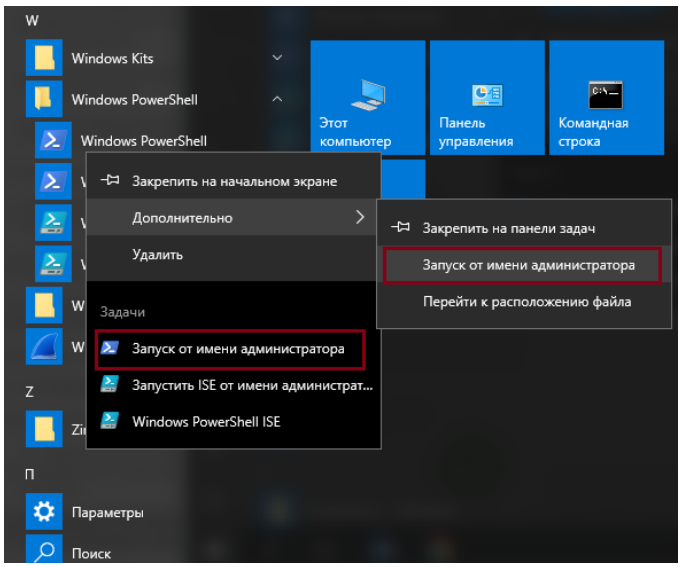
Шаг 6. Нажмите **Установить**;



После окончания установки нажмите **Готово**;

Добавление порта в исключения брандмауэра

Шаг 1. Откройте консоль **PowerShell**: **Пуск** → **Windows PowerShell** → ПКМ по **Windows PowerShell** → **Запуск от имени администратора**;



Шаг 7. Выполните следующую команду:

Код

```
netsh advfirewall firewall add rule name="RedCheck Agent port" dir=in
action=allow protocol=TCP localport=8732
```

4.5.2 Установка через групповые политики домена

Инсталляция агента сканирования RedCheck в доменном окружении осуществляется посредством групповых политик в несколько этапов:

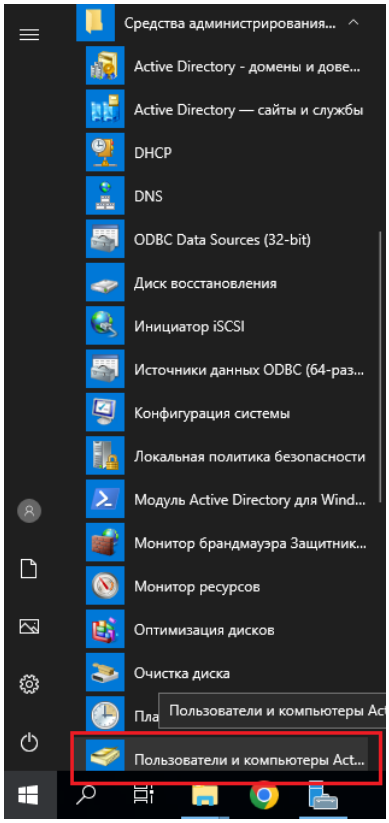
1. создание и настройка сетевой папки;

2. настройка групповой политики.

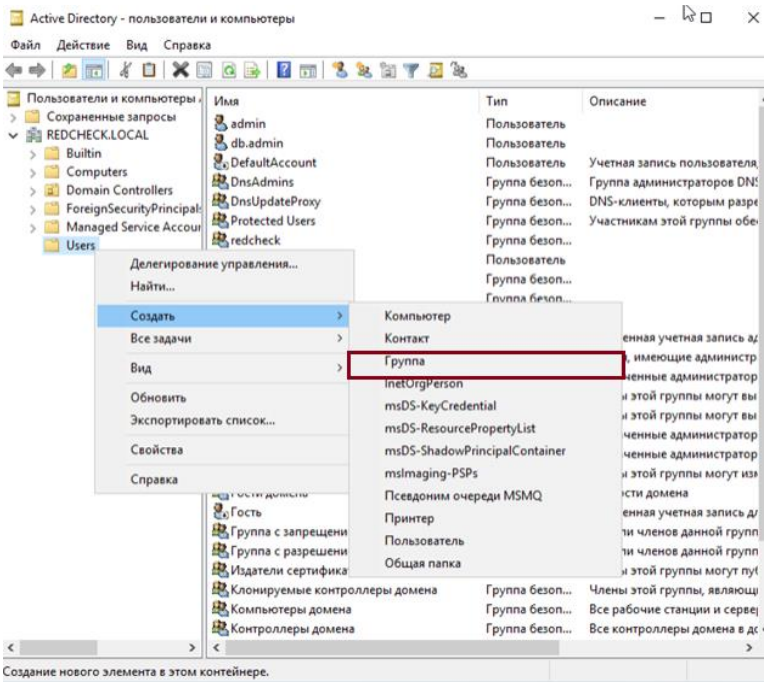
Для обеспечения большей безопасности и контроля за установкой Агента, создайте группу безопасности, в которой определите, какие устройства подлежат установке, а какие нет. Если такой ГБ не требуется, начните с шага 8.

Создание и настройка группы безопасности

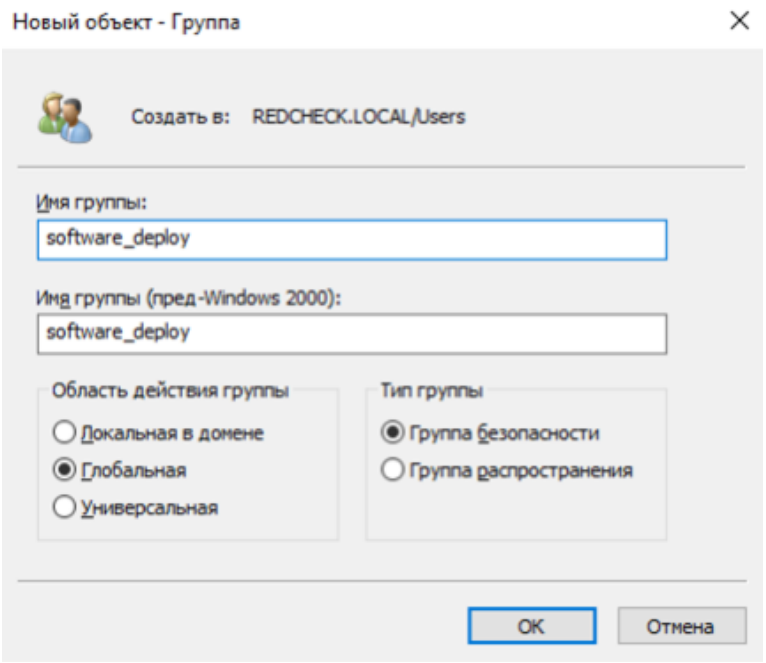
Шаг 1. Пуск → Средства администрирования Windows → Пользователи и компьютеры Active Directory;



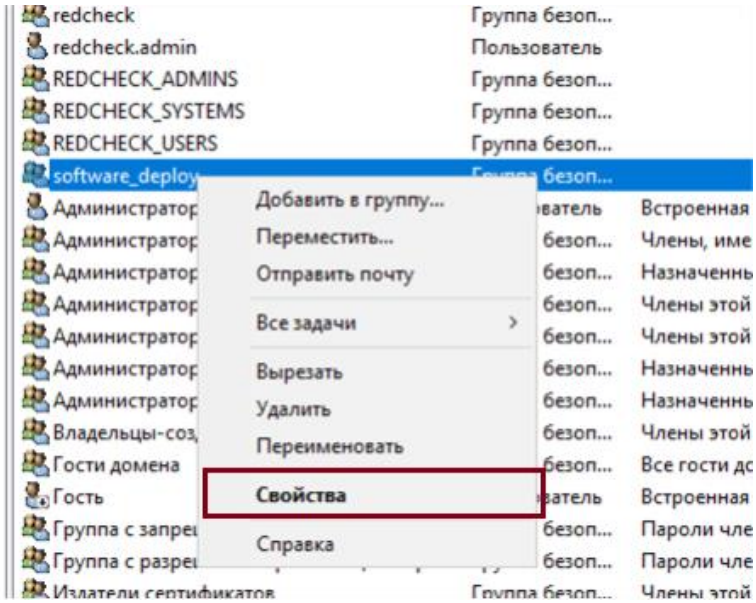
Шаг 2. ПКМ по **Users** → **Создать** → **Группа**;



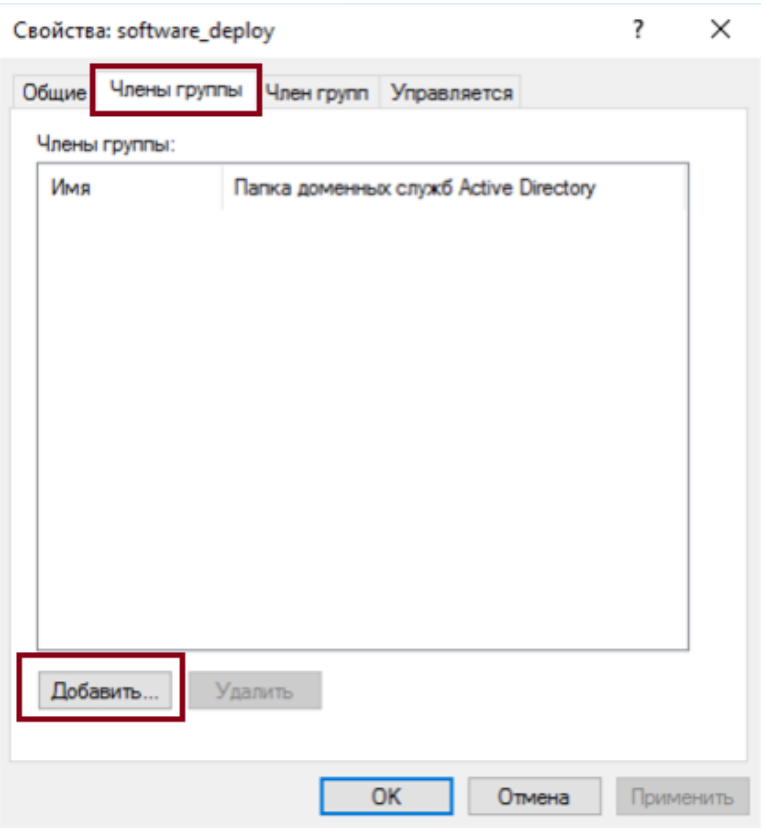
Шаг 3. В поле **Имя группы** укажите название группы (в примере **software_deploy**). Область действия группы **Глобальная**; тип группы **Группа безопасности** → **OK**.



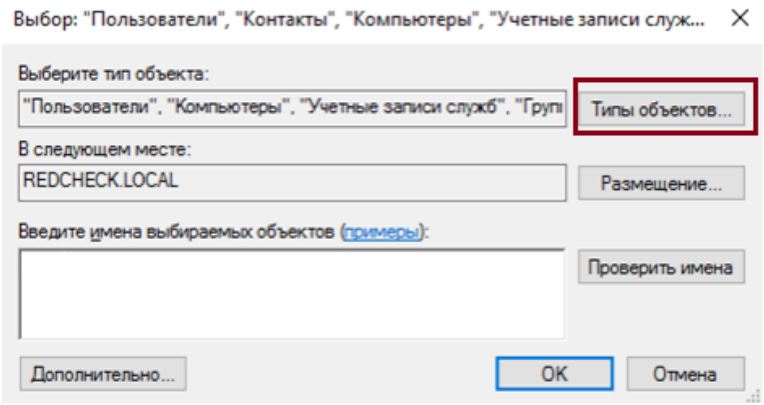
Шаг 4. ПКМ по **software_deploy** → **Свойства**;



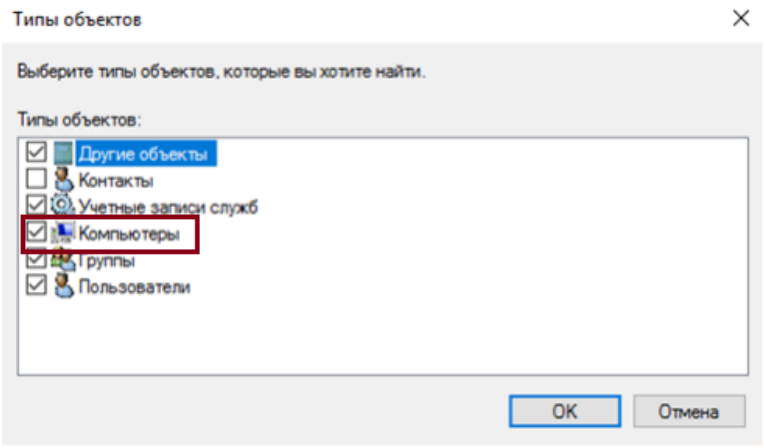
Шаг 5. Выберите **Члены группы** → **Добавить**;



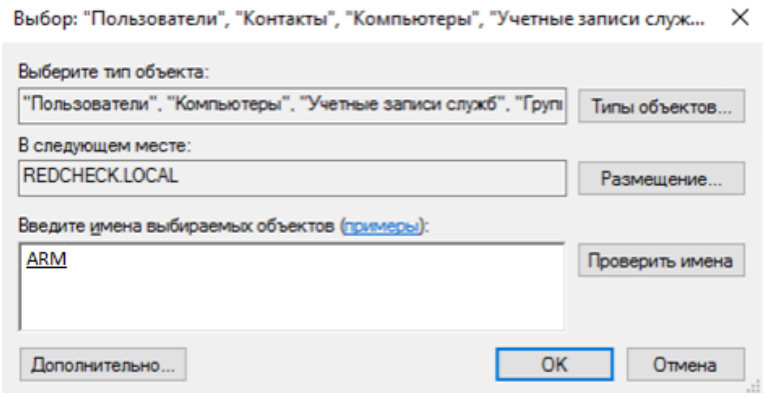
Шаг 6. Нажмите **Типы объектов**



Отметьте **Компьютеры**;

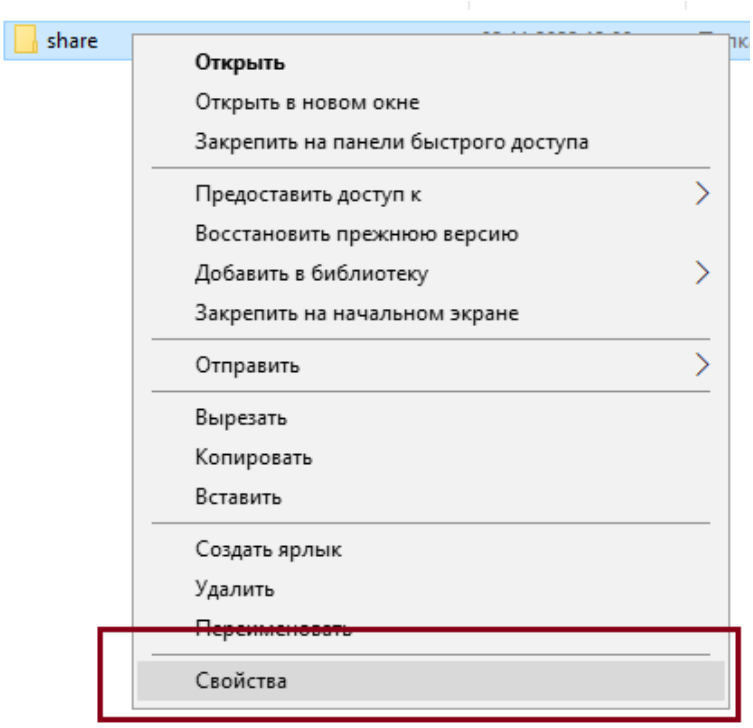


Шаг 7. Укажите имя компьютера, на котором планируется установка агента → **Проверить имена** → **ОК**.

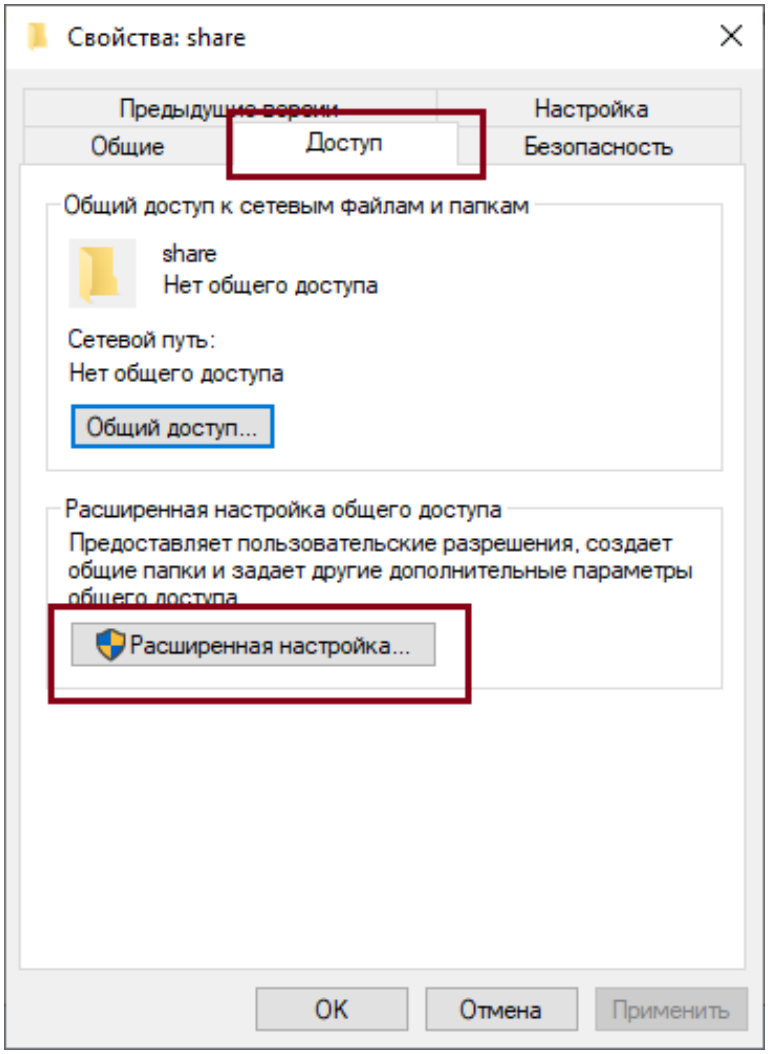


Создание и настройка сетевой папки

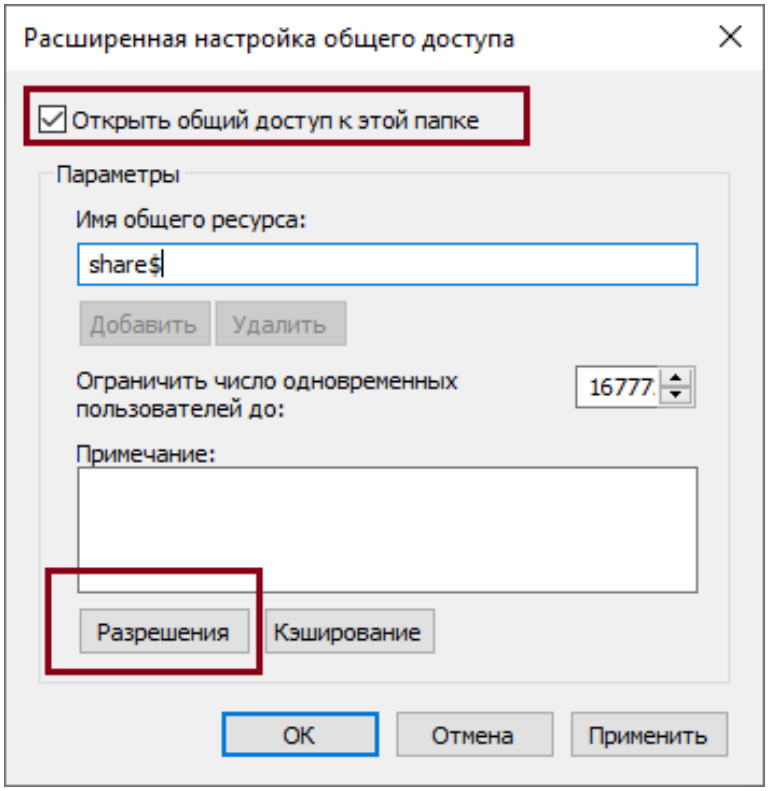
Шаг 8. Создайте директорию с произвольным названием (например, C:\share) → ПКМ по созданной директории → **Свойства**;



Шаг 9. Перейдите в **Доступ** → **Расширенная настройка**;

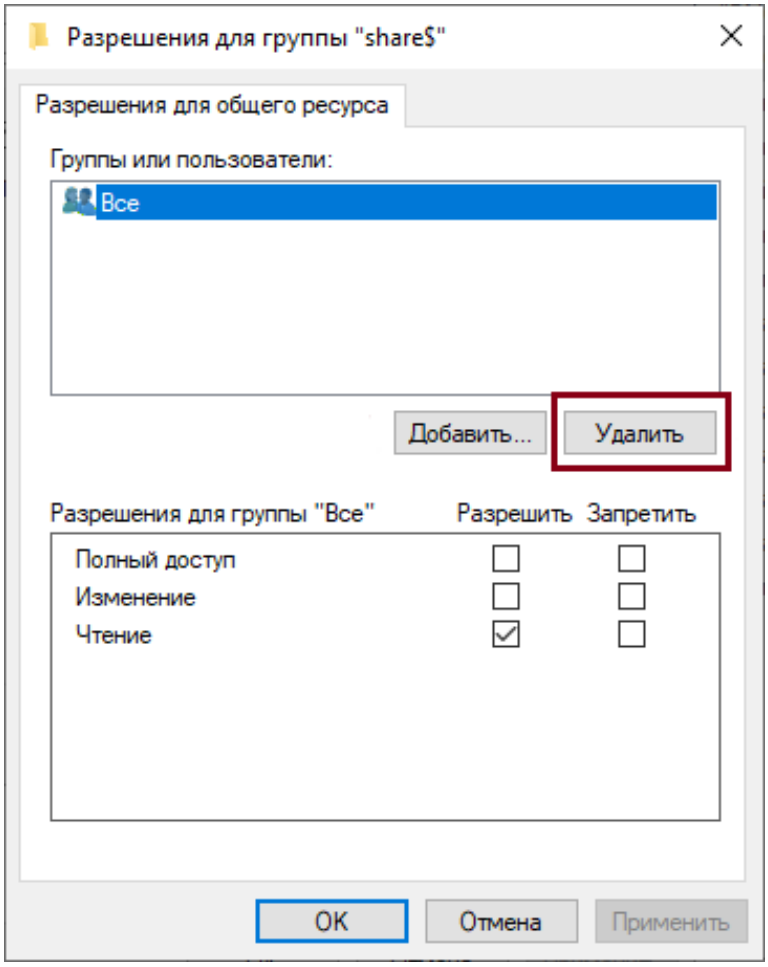


Шаг 10. Отметьте **Открыть общий доступ** → **Разрешения**;

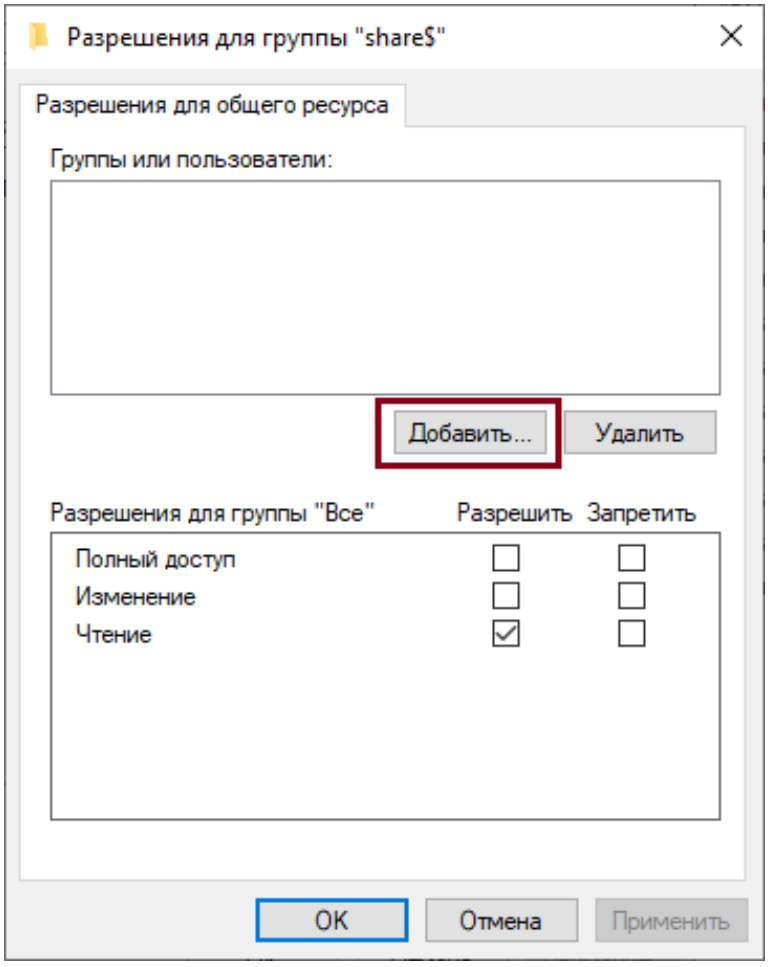


Символ **$** на конце имени папки позволяет скрыть её из сетевого окружения пользователей.

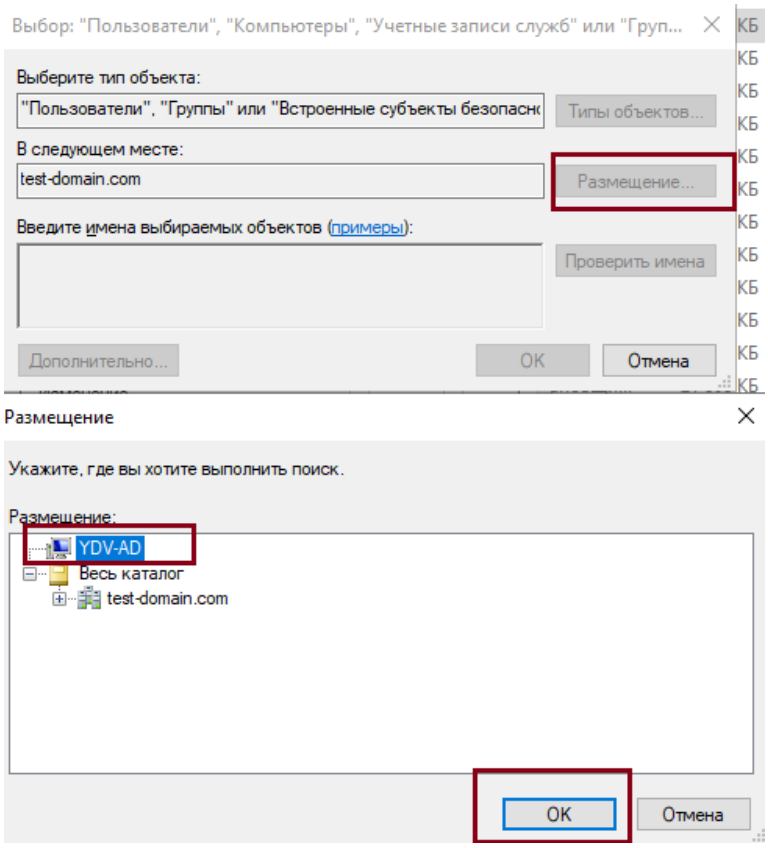
Шаг 11. Удалите группу **Все**;



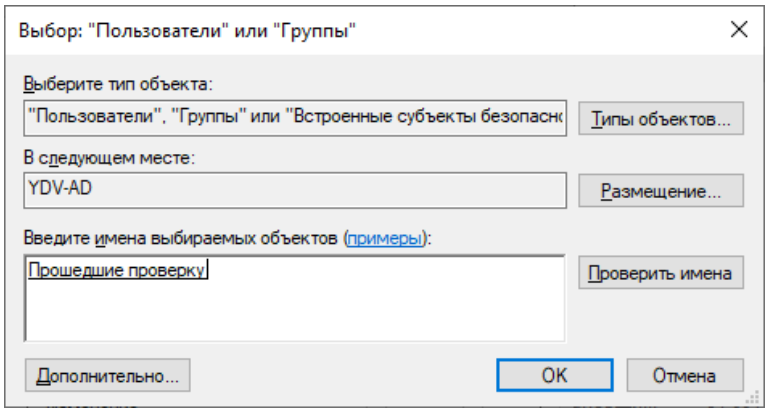
Нажмите **Добавить**;



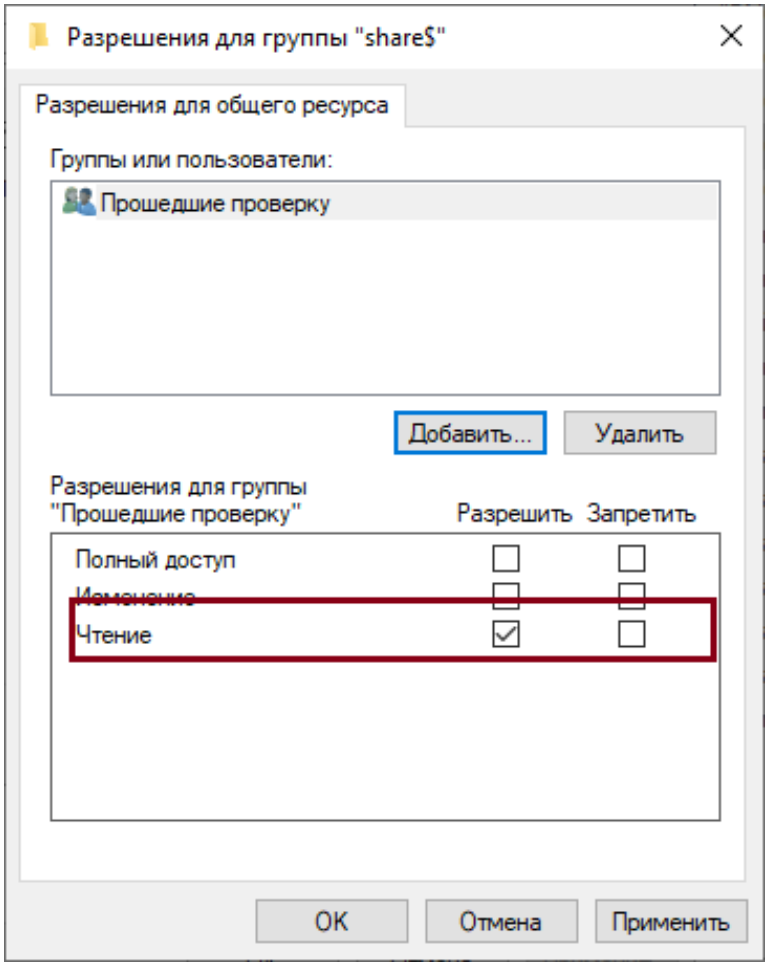
Шаг 12. Нажмите **Размещение** → выберите локальный компьютер → **ОК**;



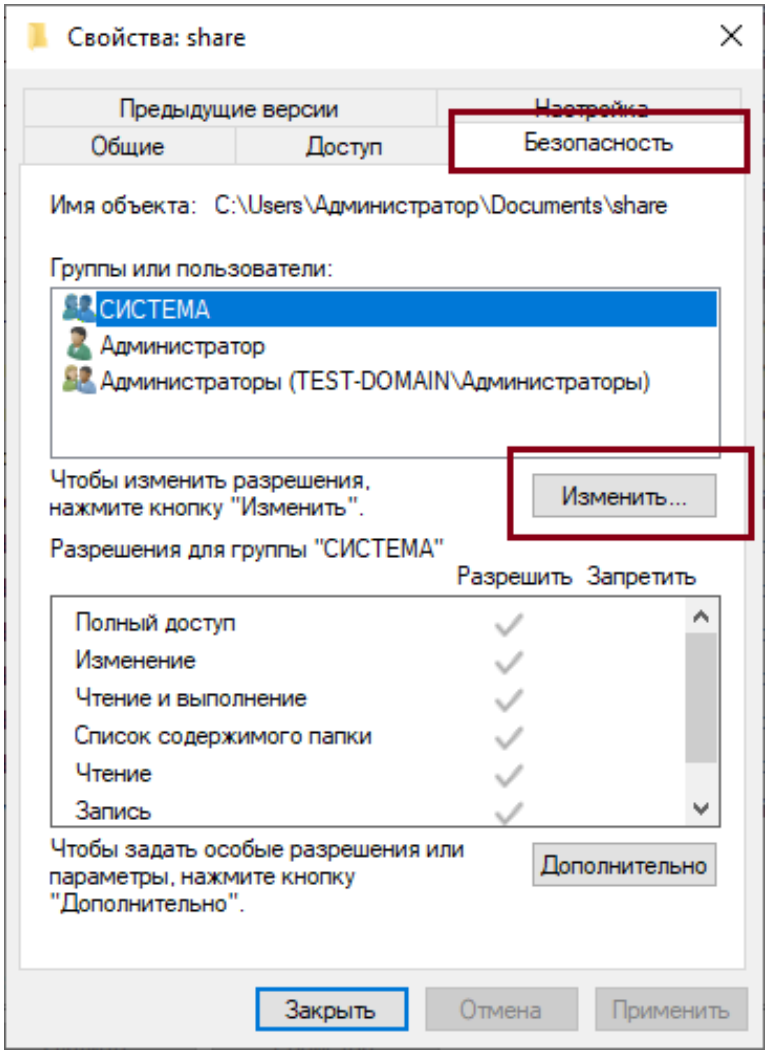
Шаг 13. Введите имя **Прошедшие проверку** → **Проверить имена** → **ОК**;



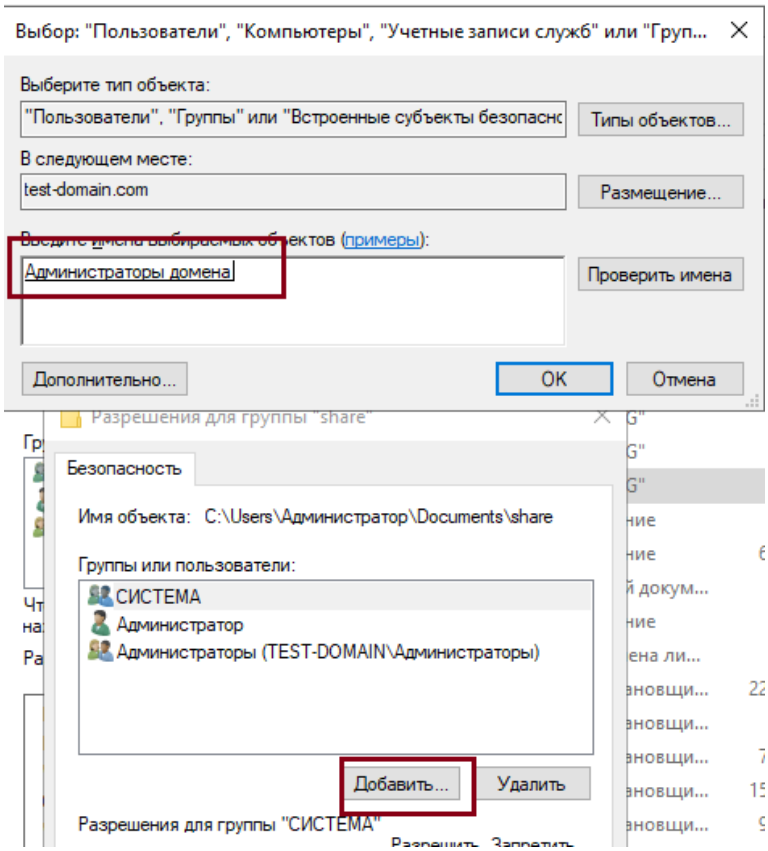
Предоставьте разрешение на **Чтение**;



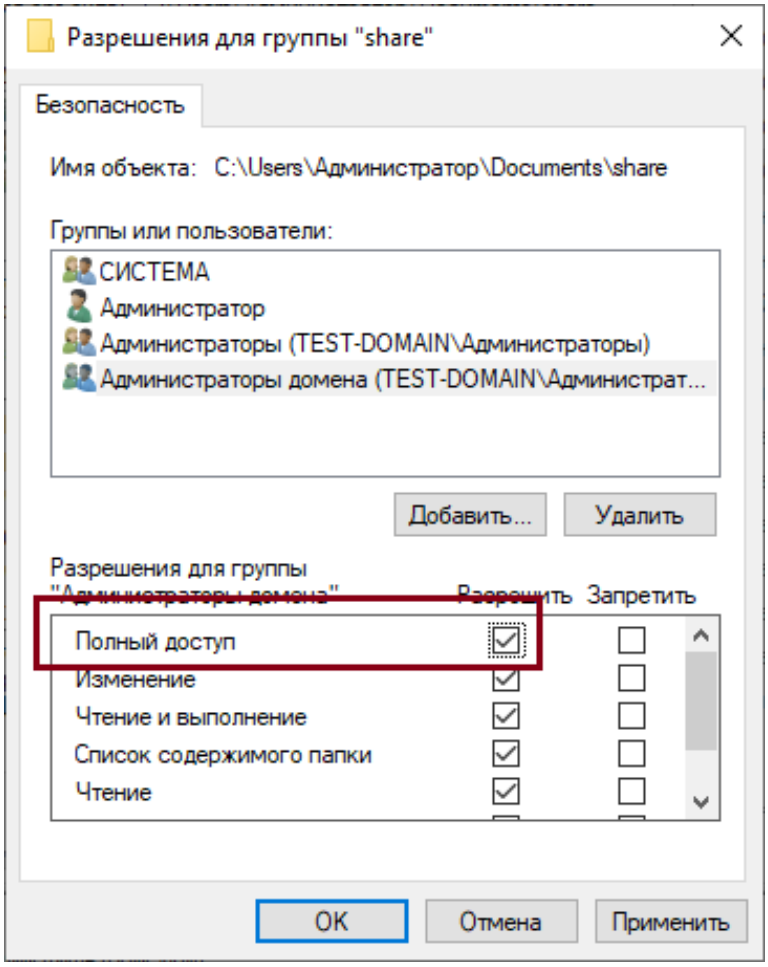
Шаг 14. В свойствах директории перейдите в **Безопасность** → **Изменить**;



Шаг 15. Нажмите **Добавить** → введите **Администраторы домена** → **ОК**;



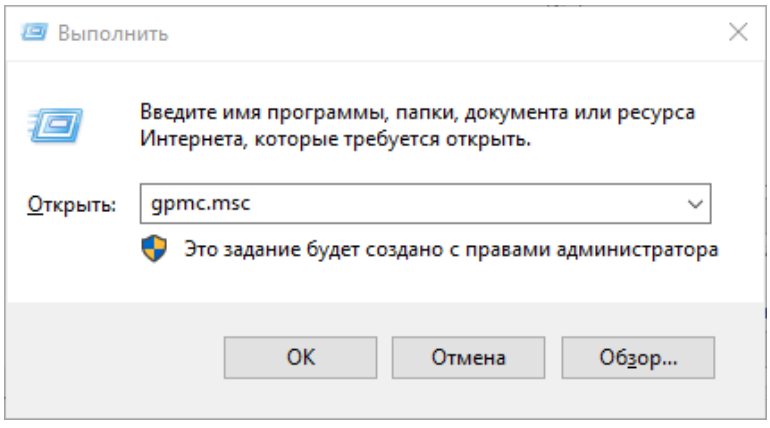
Шаг 16. Для **Администраторы домена** отметьте **Полный доступ** → **ОК**;



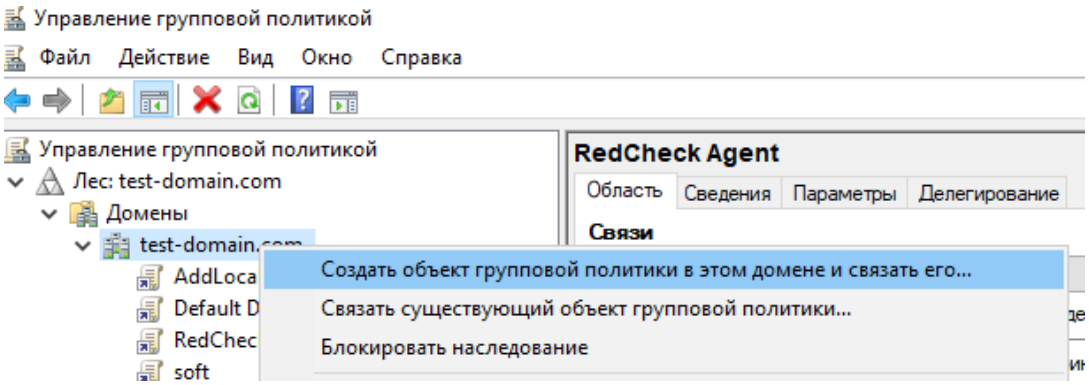
Шаг 17. Скопируйте в созданную директорию установочный файл Агента.

Настройка групповой политики

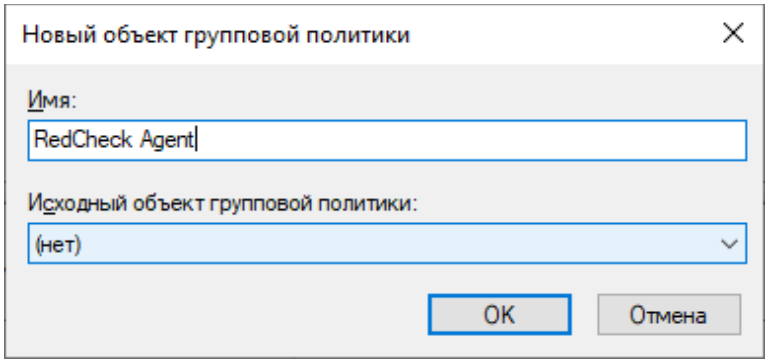
Шаг 18. Нажмите **Win + R** → введите **gpmc.msc**;



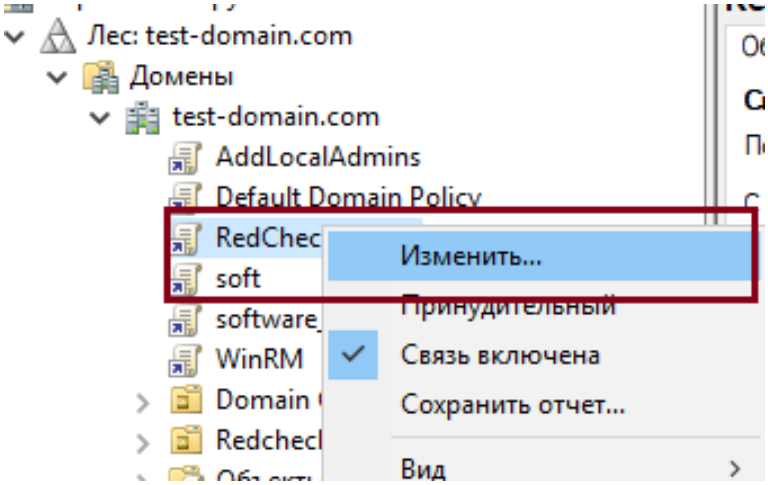
Шаг 19. Раскройте **Домены** → ПКМ по домену → **Создать объект групповой политики в этом домене...**;



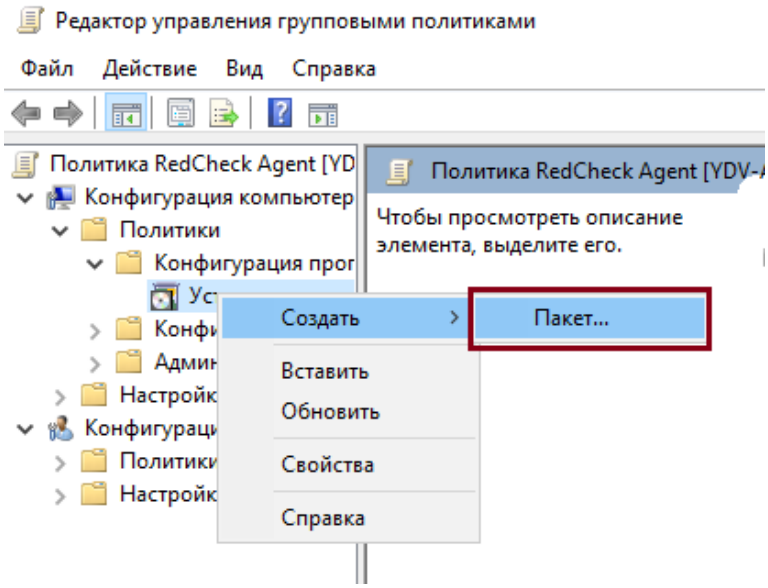
Введите имя для групповой политики → **OK**;



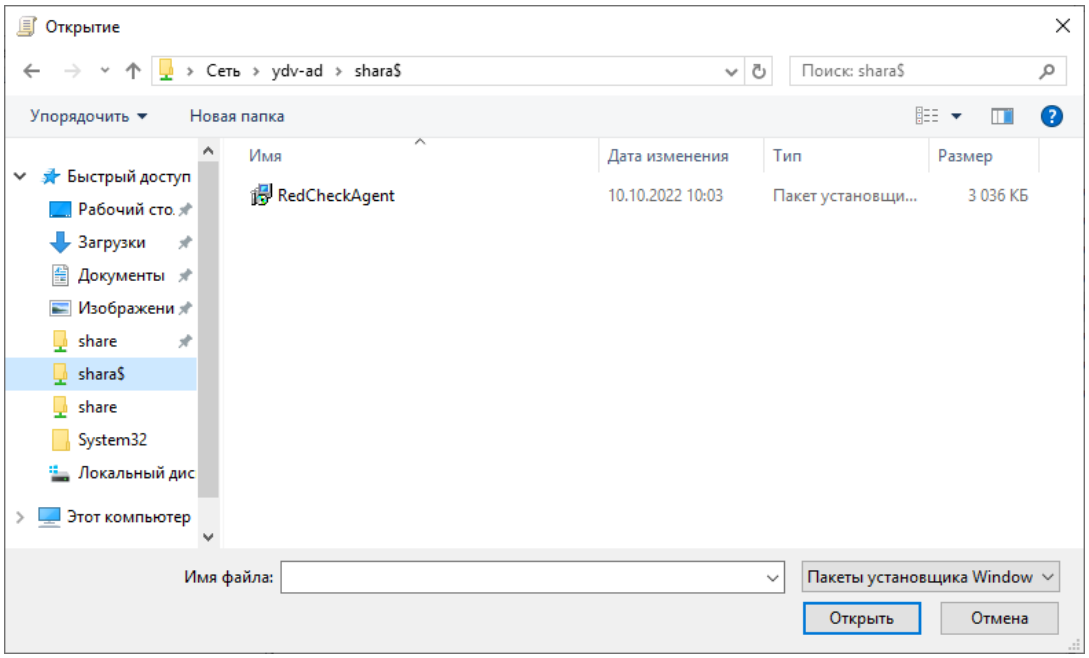
Шаг 20. ПКМ по созданной политике → **Изменить**;



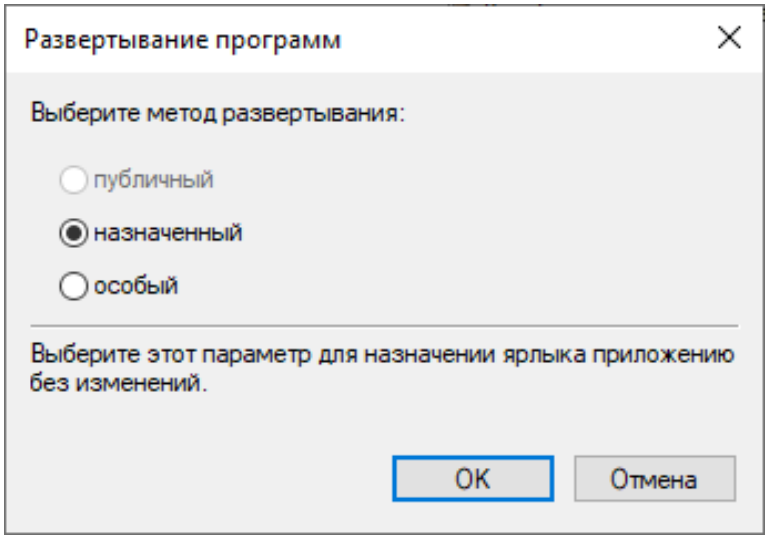
Шаг 21. Раскройте **Конфигурация компьютера** → **Политики** → **Конфигурация программ** → ПКМ по **Установка программ** → **Создать** → **Пакет**;



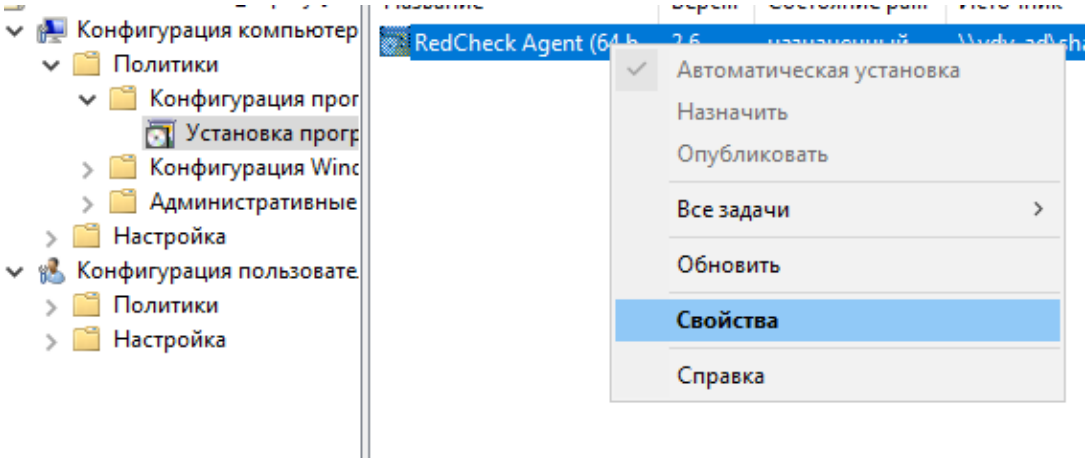
Шаг 22. Введите в адресной строке путь к сетевой папке: **\\<имя_компьютера>\<имя_папки>$** → выберите установочный файл Агента;



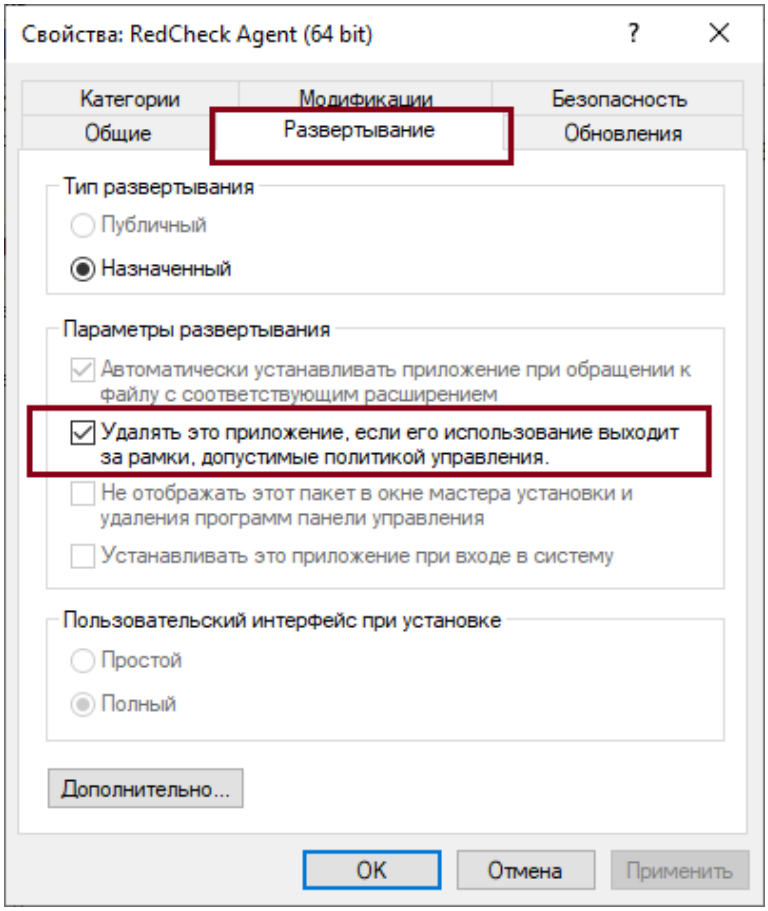
Метод развертывания – **назначенный**;



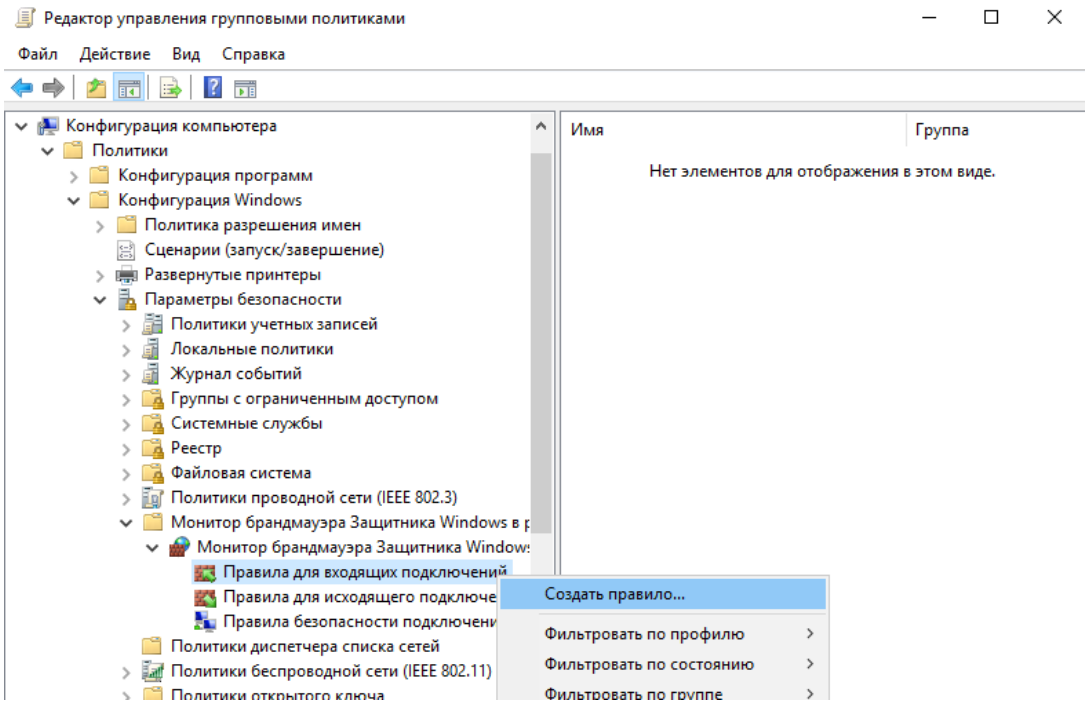
Шаг 23. ПКМ по появившемуся установочному файлу → **Свойства**;



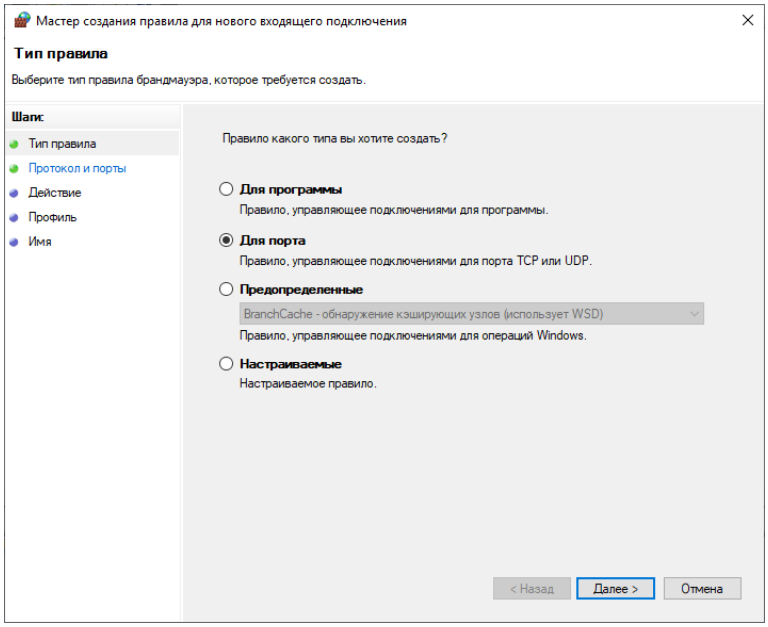
Шаг 24. В **Развертывание** отметьте **Удалять это приложение, если его использование... → ОК**;



Шаг 25. Перейдите в **Конфигурация компьютера → Политики → Конфигурация Windows → Параметры безопасности → Монитор брандмауэра Защитника Windows...** → ПКМ по **Правила для входящих подключений → Создать правило...**;

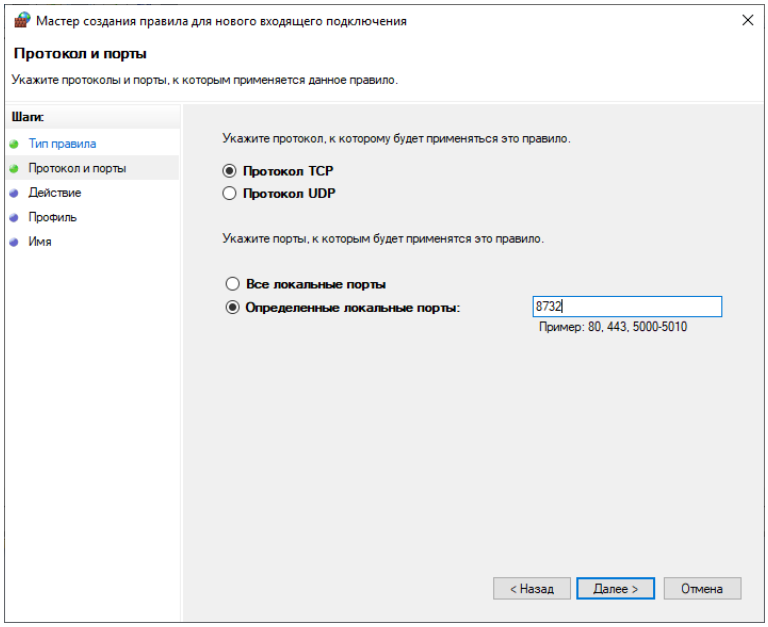


Шаг 26. Укажите тип правила **Для порта → Далее**;

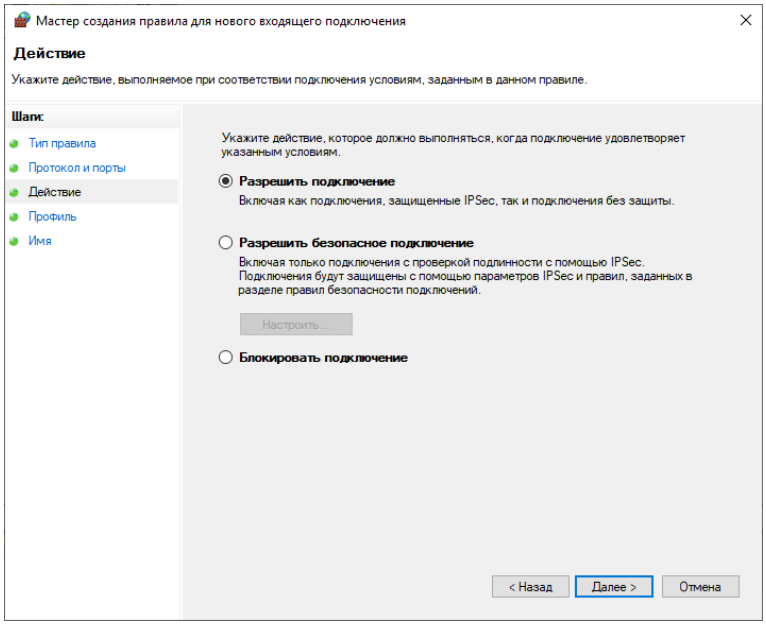


Отметьте **Протокол TCP** → укажите порт Агента (по умолчанию **8732)** → **Далее**;

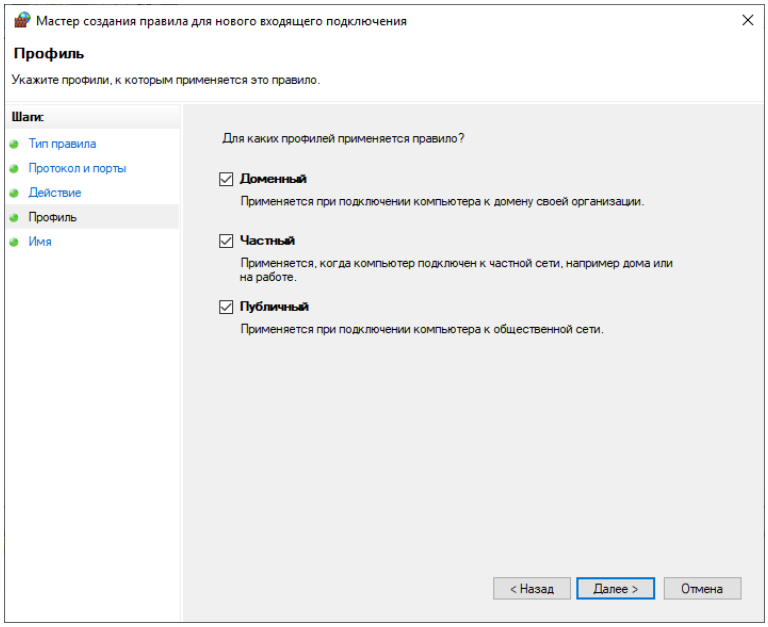
Можно, но не рекомендуется использовать другой порт Агента.



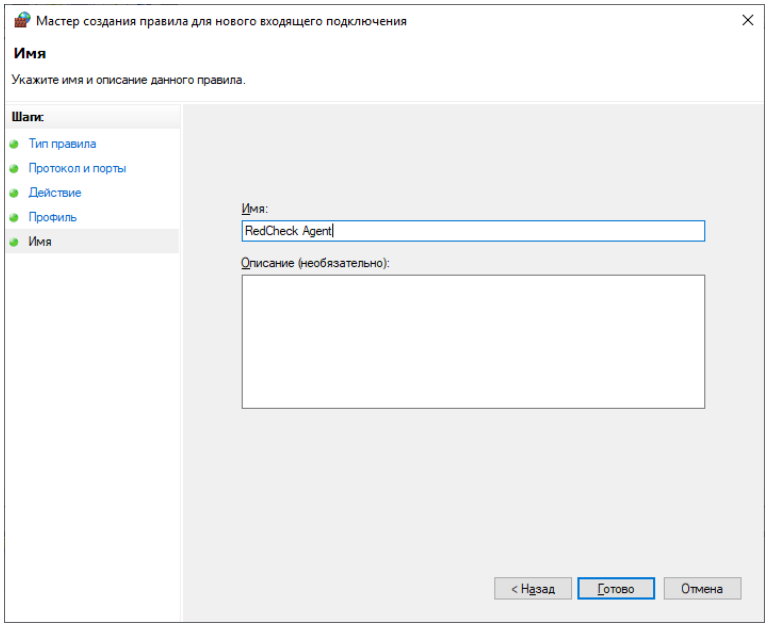
Выберите **Разрешить подключение** → **Далее**;



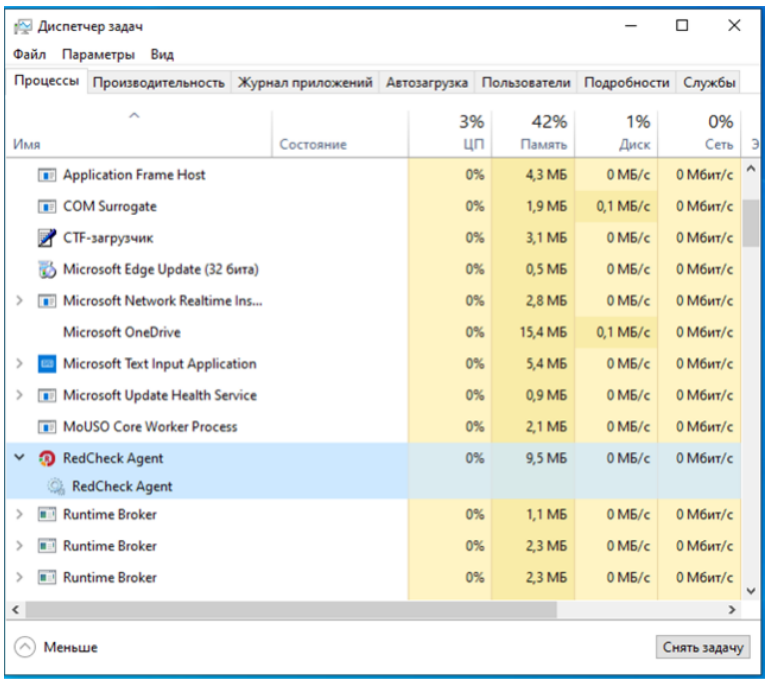
Выберите профили для применения правила (рекомендуется оставить по умолчанию) → **Далее**;



Задайте имя → **Готово**.



После установки Агента появится директория **RedCheckAgent** по адресу C:\Program Files\ALTEX-SOFT, а служба Агента будет отображаться в **Процессах** в **Диспетчере задач**.



Для ускорения применения групповой политики воспользуйтесь командой **gpupdate /force**. Данная команда выполняется от имени администратора домена на контроллере домена и на хосте, где производилась установка Агента RedCheck.

4.6 Автоматическая установка RedCheck и параметры инсталляции

Для установки RedCheck через командную строку необходимо указывать параметры для инсталляции. Каждый компонент имеет свой набор параметров.

Содержание

4.6.1 Параметры Desktop-версии

Запуск скриптов производится из командной строки / PowerShell

Установочный скрипт Desktop-версии для СУБД Microsoft SQL Server [смешанная авторизация]

Код

```
msiexec /i "путь_к_установщику" LICENSE_KEY="*" CREATEGROUP=1
ADDUSERTOGROUP=1 DB_PROVIDER="MSSQL" MSSQL_SERVER="*"
MSSQL_DATABASE="*" MSSQL_USERNAME="*" MSSQL_PASSWORD="*"
NMAP_ACTION="INSTALL" /qn
```

Вместо * подставьте свои значения

Установочный скрипт Desktop-версии для СУБД Microsoft SQL Server [доменная авторизация]

Код

```
msiexec /i "путь_к_установщику" LICENSE_KEY="*" CREATEGROUP=1
ADDUSERTOGROUP=1 DB_PROVIDER="MSSQL" MSSQL_SERVER="*"
MSSQL_DATABASE="*" AUTH_TYPE="WIN" USE_OTHER_USER_WIN_AUTH=1
CURRENT_USER="*" USER_PASSWORD="*" NMAP_ACTION="INSTALL" /qn
```

Установочный скрипт Desktop-версии для СУБД PostgreSQL

Код

```
msiexec /i "путь_к_установщику" LICENSE_KEY="*" CREATEGROUP=1
ADDUSERTOGROUP=1 DB_PROVIDER="POSTGRESQL" POSTGRESQL_SERVER="*"
POSTGRESQL_DATABASE="*" POSTGRESQL_USERNAME="*"
POSTGRESQL_PASSWORD="*" NMAP_ACTION="INSTALL" /qn
```

/q[n, b, f] – параметр отображения пользовательского интерфейса:
n – без интерфейса;
b – основной интерфейс (индикатор удаления);
f – полный интерфейс (по умолчанию);

Параметры установки

Параметр	Описание	Диапазон значений/формат
INSTALLFOLDER [C:\Program Files\ALTEX-SOFT\RedCheck\]	Определяет папку для установки	
LICENSE_KEY	Лицензионный ключ RedCheck. При указании ключа автоматически активирует параметр **LICENSE_CHECK_TYPE=KEY**	********_****_****_****_************
LICENSE_FILE	Путь к файлу License.key. Указывается в случае **LICENSE_CHECK_TYPE=FILE**	
LICENSE_CHECK_TYPE [KEY]	Тип проверки лицензии. При указании ключа, параметр можно не указывать	**KEY** - с помощью ключа **FILE** - с помощью файла лицензии
CREATEGROUP [0]	Создает локальную группу **REDCHECK_ADMINS**	**0** - группа не будет создана **1** - группа будет создана
ADDUSERTOGROUP [0]	Добавляет текущего пользователя в локальную группу **REDCHECK_ADMINS**	**0** - не будет добавлен **1** - будет добавлен
DB_PROVIDER	Определяет тип	**MSSQL** - Microsoft

[MSSQL]	используемой СУБД	SQL Server **POSTGRESQL** - PostgreSQL
NEED_CREATE_DATABASE [1]	Нужно ли создавать базу данных или будет использована существующая	**0** - использовать существующую БД **1** - создать новую БД
NEED_CLEAR_DATABASE [0]	Нужно ли очистить существующую БД. Указывается в случае **NEED_CREATE_DATABASE=0**	**0** - не очищать существующую БД **1** - очистить существующую БД
DB_COMMAND_TIMEOUT [600]	Параметр, определяющий таймаут времени ожидания действия над БД в процессе обновления	Время в секундах
SYNC_ALL_AVAILABLE [0]	Выбор всех типов контента, доступного для синхронизации	**0** - опция синхронизировать всё - отключена **1** - опция синхронизировать всё - включена
SYNC_SCHEDULE_TYPE [1]	Выбор расписания синхронизации	**0** - ручная синхронизация **1** - автоматическая синхронизация
RUN_SYNC_ON_START [1, если (SYNC_SCHEDULE_TYPE=1)]	Запускать синхронизацию при старте программы	**0** - не синхронизировать при старте программы **1** - синхронизировать при старте программы

SYNC_HOUR [12]	Час, когда будет проводиться автоматическая синхронизация	**0** - мин. значение **23** - макс. значение
SYNC_MINUTES [0]	Минуты, когда будет проводиться автоматическая синхронизация	**0** - мин. значение **59** - макс. значение
NMAP_ACTION [NONE]	Опция определяющая устанавливать Nmap, пропустить либо использовать существующий	**NONE** - пропустить установку Nmap **INSTALL** - установить Nmap **SET** - указать путь до установленного Nmap
NMAP_PATH	Опция, определяющая путь, по которому установить Nmap. Указывается в случае **NMAP_ACTION=SET**	
SKCD	**Необязательный**. Пользовательская часть ключа для шифрования учетных записей RedCheck для сканирования. Если БД уже зашифрована с указанием ключа, то при подключении к БД параметр **обязателен**.	

Значения, находящиеся в [] являются значениями по умолчанию. Они будут использоваться инсталлятором, если не указывать параметр в скрипте.

Параметры при использовании СУБД Microsoft SQL Server (DB_PROVIDER = MSSQL)

Параметр	Описание	Диапазон значений/формат
MSSQL_SERVER [localhost\SQLExpress]	Имя сервера базы данных	**IP** - указание только IP **IP,port** - указание IP и порта **hostname** - указание имени сервера **hostname,port** - указание имени сервера и порта **hostname\instance** - указание имени сервера с именем экземпляра
MSSQL_DATABASE [RedCheck]	Имя базы данных	
AUTH_TYPE [SQL]	Тип аутентификации	**SQL** - SQL Server Authentication **WIN** - Windows Authentication
При аутентификации SQL Server Authentucation (AUTH_TYPE = SQL)		
MSSQL_USERNAME	Логин пользователя базы данных	
MSSQL_PASSWORD	Пароль пользователя базы данных	
При аутентификации Windows Authentication (AUTH_TYPE = WIN)		

USE_OTHER_USER_WIN_AUTH [0]	Использование сервисной учетной записи	**0** - использовать УЗ, под которой производится установка **1** - использовать другую УЗ
CURRENT_USER [Имя пользователя, запустившего инсталлятор]	Имя пользователя, от которого будет производиться подключение к СУБД и установка служб Синхронизации и Сканирования Указывается в случае **USE_OTHER_USER_WIN_AUTH =1**	
USER_PASSWORD	Пароль от УЗ пользователя, указанного в качестве **CURRENT_USER**	

Параметры при использовании СУБД PostgreSQL (DB_PROVIDER = POSTGRESQL)

Параметр	Описание	Диапазон значений/формат
POSTGRESQL_SERVER [localhost]	Имя сервера базы данных	**IP** - указание только IP **hostname** - указание имени сервера
POSTGRESQL_PORT [5432]	Порт при подключении через PostgreSQL	**1** - мин. значение **65535** - макс. значение
POSTGRESQL_DATABASE [RedCheck]	Имя базы данных	
POSTGRESQL_USERNAME	Логин пользователя базы данных	

POSTGRESQL_PASSWORD	Пароль пользователя базы данных	

4.6.2 Параметры Web-версии

Установка Web-версии RedCheck подразумевает выполнение нескольких скриптов в определенной последовательности.

Содержание

4.6.2.1 Серверный компонент RestAPI

Запуск скриптов производится из командной строки / PowerShell

Установочный скрипт серверного компонента для СУБД Microsoft SQL Server [смешанная авторизация]

Код

```
msiexec /i "путь_к_установщику" LICENSE_KEY="*" REST_URL="*"
ADMIN_LOGIN="*" ADMIN_PASSWORD="*" CLEANUP_OPEN_PORT=1
DB_PROVIDER="MSSQL" MSSQL_SERVER="*" MSSQL_DATABASE="*"
MSSQL_USERNAME="*" MSSQL_PASSWORD="*" /qn
```

Вместо * подставьте свои значения

Установочный скрипт серверного компонента для СУБД Microsoft SQL Server [доменная авторизация]

Код

```
msiexec /i "путь_к_установщику" LICENSE_KEY="*" REST_URL="*"
ADMIN_LOGIN="*" ADMIN_PASSWORD="*" CLEANUP_OPEN_PORT=1
DB_PROVIDER="MSSQL" MSSQL_SERVER="*" MSSQL_DATABASE="*"
AUTH_DATABASE_TYPE="WIN" USE_OTHER_USER_WIN_AUTH=1 CURRENT_USER="*"
USER_PASSWORD="*" /qn
```

Установочный скрипт серверного компонента для СУБД PostgreSQL

Код

```
msiexec /i "путь_к_установщику" LICENSE_KEY="*" REST_URL="*"
ADMIN_LOGIN="*" ADMIN_PASSWORD="*" CLEANUP_OPEN_PORT=1
DB_PROVIDER="POSTGRESQL" POSTGRESQL_SERVER="*"
POSTGRESQL_DATABASE="*" POSTGRESQL_USERNAME="*"
POSTGRESQL_PASSWORD="*" /qn
```

/q[n, b, f] – параметр отображения пользовательского интерфейса:
n – без интерфейса;
b – основной интерфейс (индикатор удаления);
f – полный интерфейс (по умолчанию);

Параметры установки

Параметр	Описание	Диапазон значений/формат
INSTALLFOLDER [C:\Program Files\ALTEX-SOFT\RedCheck\]	Определяет папку для установки	
REST_URL*	Определяет адрес привязки при установке Rest	IP адрес
REST_PORT [8081]	Определяет порт привязки при установке Rest	**1** - мин. значение **65535** - макс. значение
LICENSE_KEY	Лицензионный ключ RedCheck. При указании ключа автоматически активирует параметр **LICENSE_CHECK_TYPE=KEY**	********-****-****-****-************
LICENSE_FILE	Путь к файлу License.key.	

	Указывается в случае **LICENSE_CHECK_TYPE=FILE**	
LICENSE_CHECK_TYPE [KEY]	Тип проверки лицензии. При указании ключа, параметр можно не указывать	**KEY** - с помощью ключа **FILE** - с помощью файла лицензии
CREATEGROUP [0]	Создает локальную группу **REDCHECK_ADMINS**	**0** - группа не будет создана **1** - группа будет создана
ADDUSERTOGROUP [0]	Добавляет текущего пользователя в локальную группу **REDCHECK_ADMINS**	**0** - не будет добавлен **1** - будет добавлен
DB_PROVIDER [MSSQL]	Определяет тип используемой СУБД	**MSSQL** - Microsoft SQL Server **POSTGRESQL** - PostgreSQL
NEED_CREATE_DATABASE [1]	Нужно ли создавать базу данных или будет использована существующая	**0** - использовать существующую БД **1** - создать новую БД
NEED_CLEAR_DATABASE [0]	Нужно ли очистить существующую БД. Указывается в случае **NEED_CREATE_DATABASE=0**	**0** - не очищать существующую БД **1** - очистить существующую БД
DB_COMMAND_TIMEOUT [600]	Параметр, определяющий таймаут времени ожидания действия с БД в процессе обновления	Время в секундах
ADMIN_LOGIN* [admin]	Логин локальной административной УЗ. Если УЗ нет, она будет создана	Не может быть пустым
ADMIN_PASSWORD*	Пароль локальной административной УЗ	Не может быть пустым

CLEANUP_PORT [8740]	Определяет используемый порт для сервиса очистки БД	**1** - мин. значение **65535** - макс. значени е
CLEANUP_OPEN_PORT [0]	Определяет необходимость создания разрешающего правила в локальном брандмауэре	**0** - Не создавать **1** - Создать
SKCD	**Необязательный**. Пользовательская часть ключа для шифрования учетных записей RedCheck для сканирования. Если БД уже зашифрована с указанием ключа, то при подключении к БД параметр **обязателен**.	

Значения, находящиеся в [] являются значениями по умолчанию. Они будут использоваться инсталлятором, если не указывать параметр в скрипте.

Параметры при использовании СУБД Microsoft SQL Server (DB_PROVIDER = MSSQL)

Параметр	Описание	Диапазон значений/формат
MSSQL_SERVER* [localhost\SQLExpress]	Имя сервера базы данных	**IP** - указание только IP **IP,port** - указание IP и порта **hostname** - указание имени сервера **hostname,port** - указание имени

		сервера и порта **hostname\instance** - указание имени сервера с именем экземпляра
MSSQL_DATABASE* [RedCheck]	Имя базы данных	
AUTH_DATABASE_TYPE [SQL]	Тип аутентификации	**SQL** - SQL Server Authentication **WIN** - Windows Authentication
При аутентификации SQL Server Authentucation (AUTH_DATABASE_TYPE = SQL)		
MSSQL_USERNAME*	Логин пользователя базы данных	
MSSQL_PASSWORD*	Пароль пользователя базы данных	
При аутентификации Windows Authentication (AUTH_DATABASE_TYPE = WIN)		
USE_OTHER_USER_WIN_AUTH [0]	Использование сервисной учетной записи	**0** - использовать текущую УЗ **1** - использовать другую УЗ
CURRENT_USER [Имя пользователя, запустившего инсталлятор]	Имя пользователя, от которого будет производиться подключение к СУБД и установка служб Синхронизации и Сканирования Указывается в случае **USE_OTHER_USER_WIN_AUTH**	

	=1	
USER_PASSWORD	Пароль УЗ пользователя, указанного в качестве **CURRENT_USER**	

Параметры при использовании СУБД PostgreSQL (DB_PROVIDER = POSTGRESQL)

Параметр	Описание	Диапазон значений/формат
POSTGRESQL_SERVER* [localhost]	Имя сервера базы данных	**IP** - указание только IP **hostname** - указание имени сервера
POSTGRESQL_PORT [5432]	Порт при подключении через PostgreSQL	**1** - мин. значение **65535** - макс. значение
POSTGRESQL_DATABASE* [RedCheck]	Имя базы данных	
POSTGRESQL_USERNAME*	Логин пользователя базы данных	
POSTGRESQL_PASSWORD*	Пароль пользователя базы данных	

4.6.2.2 Консоль управления (пользовательский интерфейс)

Запуск скриптов производится из командной строки / PowerShell

Установочный скрипт консоли управления

Код

```
msiexec /i "путь_к_установщику" REST_URL="*" DEFAULT_CLIENT_URL="*"
/qn
```

Вместо * подставьте свои значения;

/q[n, b, f] – параметр отображения пользовательского интерфейса:
n – без интерфейса;
b – основной интерфейс (индикатор удаления);
f – полный интерфейс (по умолчанию);

Параметры установки

Параметр	Описание	Диапазон значений/формат
INSTALLFOLDER [C:\Program Files\ALTEX-SOFT\RedCheck\]	Определяет папку для установки	
REST_URL*	Адрес установленного серверного компонента	IP адрес
REST_PORT [8081]	Порт установленного серверного компонента	**1** - мин. значение **65535** - макс. значение
DEFAULT_CLIENT_URL*	Адрес привязки при установке консоли управления	IP адрес

DEFAULT_CLIENT_PORT [8080]	Используемый порт для консоли управления	**1** - мин. значение **65535** - макс. Значение
CLEANUP_PORT [8740]	Определяет используемый порт для сервиса очистки БД	**1** - мин. значение **65535** - макс. значени е

Значения, находящиеся в [] являются значениями по умолчанию. Они будут использоваться инсталлятором, если не указывать параметр в скрипте.

4.6.2.3 Служба сканирования

Запуск скриптов производится из командной строки / PowerShell

Установочный скрипт службы сканирования для СУБД Microsoft SQL Server [смешанная авторизация]

Код

```
msiexec /i "путь_к_установщику" SERVICE_NAME="*"
SERVICE_FRIENDLY_NAME="*" NMAP_ACTION="INSTALL" DB_PROVIDER="MSSQL"
MSSQL_SERVER="*" MSSQL_DATABASE="*" MSSQL_USERNAME="*"
MSSQL_PASSWORD="*" /qn
```

Вместо * подставьте свои значения.

Установочный скрипт службы сканирования для СУБД Microsoft SQL Server [доменная авторизация]

Код

```
msiexec /i "путь_к_установщику" SERVICE_NAME="*"
SERVICE_FRIENDLY_NAME="*" NMAP_ACTION="INSTALL" DB_PROVIDER="MSSQL"
MSSQL_SERVER="*" MSSQL_DATABASE="*" USE_WIN_AUTH=1
USE_OTHER_USER_WIN_AUTH=1 CURRENT_USER="*" USER_PASSWORD="*" /qn
```

Установочный скрипт службы сканирования для СУБД PostgreSQL

Код

```
msiexec /i "путь_к_установщику" SERVICE_NAME="*"
SERVICE_FRIENDLY_NAME="*" NMAP_ACTION="INSTALL"
DB_PROVIDER="POSTGRESQL" POSTGRESQL_SERVER="*"
POSTGRESQL_DATABASE="*" POSTGRESQL_USERNAME="*"
POSTGRESQL_PASSWORD="*" /qn
```

/q[n, b, f] – параметр отображения пользовательского интерфейса:
n – без интерфейса;
b – основной интерфейс (индикатор удаления);
f – полный интерфейс (по умолчанию);

Параметры установки

Параметр	Описание	Диапазон значений/формат
INSTALLFOLDER [C:\Program Files\ALTEX-SOFT\RedCheck\]	Определяет папку для установки	
DB_PROVIDER [MSSQL]	Определяет тип используемой СУБД	**MSSQL** - Microsoft SQL Server **POSTGRESQL**

SERVICE_NAME	Имя службы для регистрации в ОС	
SERVICE_FRIENDLY_NAME*	Имя службы, которое будет отображаться в консоли управления	
NMAP_ACTION [NONE]	Опция определяющая устанавливать Nmap, пропустить либо использовать существующий	**NONE** - пропустить установку Nmap **INSTALL** - установить Nmap **SET** - указать путь до установленного Nmap
NMAP_PATH	опция определяющая путь по которому установлен Nmap Указывается в случае **NMAP_ACTION=SET**	
SKCD	**Необязательный**. Пользовательская часть ключа для шифрования учетных записей RedCheck для сканирования. Если БД уже зашифрована с указанием ключа, то при подключении к БД параметр **обязателен**.	

Значения, находящиеся в [] являются значениями по умолчанию. Они будут использоваться инсталлятором, если не указывать параметр в скрипте.

Параметры при использовании СУБД Microsoft SQL Server (DB_PROVIDER = MSSQL)

Параметр	Описание	Диапазон значений/формат
MSSQL_SERVER* [localhost\SQLExpress]	Имя сервера базы данных	**IP** - указание только IP **IP,port** - указание IP и порта **hostname** - указание имени сервера **hostname,port** - указание имени сервера и порта **hostname\instance** - указание имени сервера с именем экземпляра
MSSQL_DATABASE* [RedCheck]	Имя базы данных	
USE_WIN_AUTH [0]	Тип аутентификации	**0** - SQL Server Authentication **1** - Windows Authentication
При аутентификации SQL Server Authentucation (USE_WIN_AUTH = 0)		
MSSQL_USERNAME*	Логин пользователя базы данных	
MSSQL_PASSWORD*	Пароль пользователя базы данных	

При аутентификации Windows Authentication (USE_WIN_AUTH = 1)		
USE_OTHER_USER_WIN_AUTH [0]	Использование сервисной учетной записи	**0** - использовать УЗ, под которой производится установка **1** - использовать другую УЗ
CURRENT_USER [Имя пользователя, запустившего инсталлятор]	Имя пользователя, от которого будет производиться подключение к СУБД и установка служб Синхронизации и Сканирования Указывается в случае **USE_OTHER_USER_WIN_AUTH =1**	
USER_PASSWORD	Пароль УЗ пользователя, указанного в качестве **CURRENT_USER**	

Параметры при использовании СУБД PostgreSQL (DB_PROVIDER = POSTGRESQL)

Параметр	Описание	Диапазон значений/формат
POSTGRESQL_SERVER* [localhost]	Имя сервера базы данных	**IP** - указание только IP hostname - указание имени сервера
POSTGRESQL_PORT [5432]	Порт при подключении через PostgreSQL	**1** - мин. значение **65535** - макс. значение
POSTGRESQL_DATABASE* [RedCheck]	Имя базы данных	

POSTGRESQL_USERNAME*	Логин пользователя базы данных	
POSTGRESQL_PASSWORD*	Пароль пользователя базы данных	

4.6.2.4 Служба синхронизации

Запуск скриптов производится из командной строки / PowerShell

Код

```
msiexec /i "путь_к_установщику" DB_PROVIDER="MSSQL" MSSQL_SERVER="*"
MSSQL_DATABASE="*" MSSQL_USERNAME="*" MSSQL_PASSWORD="*" /qn
```

Вместо * подставьте свои значения.

Установочный скрипт службы синхронизации для СУБД Microsoft SQL Server [доменная авторизация]

Код

```
msiexec /i "путь_к_установщику" DB_PROVIDER="MSSQL" MSSQL_SERVER="*"
MSSQL_DATABASE="*" USE_WIN_AUTH=1 USE_OTHER_USER_WIN_AUTH=1
CURRENT_USER="*" USER_PASSWORD="*" /qn
```

Установочный скрипт службы синхронизации для СУБД PostgreSQL

Код

```
msiexec /i "путь_к_установщику" DB_PROVIDER="POSTGRESQL"
POSTGRESQL_SERVER="*" POSTGRESQL_DATABASE="*" POSTGRESQL_USERNAME="*"
POSTGRESQL_PASSWORD="*" /qn
```

/q[n, b, f] – параметр отображения пользовательского интерфейса:
n – без интерфейса;
b – основной интерфейс (индикатор удаления);
f – полный интерфейс (по умолчанию);

Параметры установки

Параметр	Описание	Диапазон значений/формат
INSTALLFOLDER [C:\Program Files\ALTEX-SOFT\RedCheck\]	Определяет папку для установки	
DB_PROVIDER [MSSQL]	Определяет тип используемой СУБД	**MSSQL** - Microsoft SQL Server **POSTGRESQL** - PostgreSQL
SERVICE_NAME [RedCheckSyncService]	Имя службы для регистрации в ОС	
SERVICE_FRIENDLY_NAME* [=SERVICE_NAME]	Имя службы, которое будет отображаться в консоли управления	
SKCD	**Необязательный**. Пользовательская часть ключа для шифрования учетных записей RedCheck для сканирования. Если БД уже зашифрована с указанием ключа, то при подключении к БД параметр **обязателен**.	

Значения, находящиеся в [] являются значениями по умолчанию. Они будут использоваться инсталлятором, если не указывать параметр в скрипте.

Параметры при использовании СУБД Microsoft SQL Server (DB_PROVIDER = MSSQL)

Параметр	Описание	Диапазон значений/формат
MSSQL_SERVER* [localhost\SQLExpress]	Имя сервера базы данных	**IP** - указание только IP **IP,port** - указание IP и порта **hostname** - указание имени сервера **hostname,port** - указание имени сервера и порта **hostname\instance** - указание имени сервера с именем экземпляра
MSSQL_DATABASE* [RedCheck]	Имя базы данных	
USE_WIN_AUTH [SQL]	Тип аутентификации	**0** - SQL Server Authentication **1** - Windows Authentication
При аутентификации SQL Server Authentucation (USE_WIN_AUTH = 0)		
MSSQL_USERNAME*	Логин пользователя базы данных	

MSSQL_PASSWORD*	Пароль пользователя базы данных	
При аутентификации Windows Authentication (USE_WIN_AUTH = 1)		
USE_OTHER_USER_WIN_AUTH [0]	Использование сервисной учетной записи	**0** - использовать УЗ, под которой производится установка **1** - использовать другую УЗ
CURRENT_USER [Имя пользователя, запустившего инсталлятор]	Имя пользователя, от которого будет производиться подключение к СУБД и установка служб Синхронизации и Сканирования Указывается в случае **USE_OTHER_USER_WIN_AUTH =1**	
USER_PASSWORD	Пароль УЗ пользователя, указанного в качестве **CURRENT_USER**	

Параметры при использовании СУБД PostgreSQL (DB_PROVIDER = POSTGRESQL)

Параметр	Описание	Диапазон значений/формат
POSTGRESQL_SERVER* [localhost]	Имя сервера базы данных	**IP** - указание только IP **hostname** - указание имени сервера
POSTGRESQL_PORT [5432]	Порт при подключении через PostgreSQL	**1** - мин. значение **65535** - макс. значение
POSTGRESQL_DATABASE* [RedCheck]	Имя базы данных	
POSTGRESQL_USERNAME*	Логин пользователя базы данных	
POSTGRESQL_PASSWORD*	Пароль пользователя базы данных	

4.6.3 Параметры Agent RedCheck

Запуск скриптов производится из командной строки / PowerShell

Установочный скрипт консоли управления

Код

```
msiexec /i "путь_к_установщику" /qn
```

/q[n, b, f] – параметр отображения пользовательского интерфейса:
n – без интерфейса;
b – основной интерфейс (индикатор удаления);
f – полный интерфейс (по умолчанию);

Параметры установки

Параметр	Описание	Диапазон значений/формат
INSTALLFOLDER [C:\Program Files\ALTEX-SOFT\RedCheck\]	Определяет папку для установки	
PORT [8732]	Определяет используемый порт	**1** - мин. значение **65535** - макс. значение
USER_AUTH_CACHE_LIFETIME [3600]	Настройка времени жизни кэша пользовательских ролей	**0** - выключить кэш **1** - мин. значение в секундах
CREATEGROUP	Создает локальную группу **REDCHECK_ADMIN**	**0** - группа не будет создана

[0]	**S**	**1** - группа будет создана
ADDUSERTOGROUP [0]	Добавляет текущего пользователя в локальную группу **REDCHECK_ADMINS**	**0** - не будет добавлен **1** - будет добавлен
OPEN_PORT [0]	Нужно ли создать правило для порта агента. Если порт уже открыт - новое правило создано не будет	**0** - не будет добавлено **1** - будет добавлено

Значения, находящиеся в [] являются значениями по умолчанию. Они будут использоваться инсталлятором, если не указывать параметр в скрипте.

4.6.4 Параметры WsusKit

Запуск скриптов производится из командной строки / PowerShell

Установочный скрипт консоли управления

Код

```
msiexec /i "путь_к_установщику" /qn
```

/q[n, b, f] – параметр отображения пользовательского интерфейса:
n – без интерфейса;
b – основной интерфейс (индикатор удаления);
f – полный интерфейс (по умолчанию);

Параметры установки

Параметр	Описание	Диапазон значений/формат
INSTALLFOLDER [C:\Program Files\ALTEX-SOFT\WsusKit\]	Определяет папку для установки	
PORT [8732]	Определяет используемый порт	**1** - мин. значение **65535** - макс. значение

Значения, находящиеся в [] являются значениями по умолчанию. Они будут использоваться инсталлятором, если не указывать параметр в скрипте.

Содержание

5.1 Настройка ролевой модели

Для корректного распределения прав доступа ознакомьтесь с перечнем возможностей каждой из ролей (1.4 Ролевая модель RedCheck).

Содержание

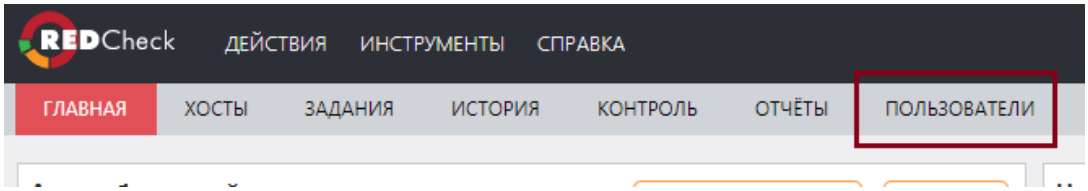
5.1.1 Создание локальных пользователей RedCheck

Локальные пользователи Системы не нуждаются в создании групп безопасности ОС Windows.

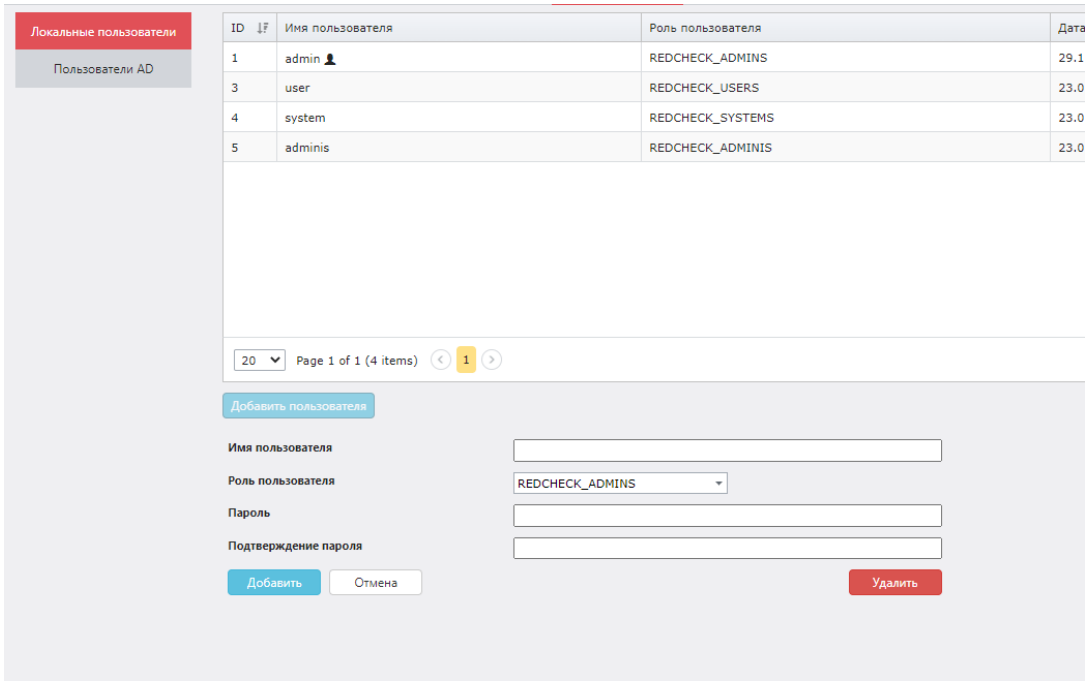
Добавить пользователя обладает возможностью только пользователь с ролью Admins.

Создание пользоваля

Шаг 1. Откройте консоль управления → **Пользователи**;



Шаг 2. Нажмите **Добавить пользователя** → укажите учетные данные для нового пользователя → **Добавить**;



Управление пользователя

Редактирование: нажмите ⚙ → **Редактировать**.

Удаление: нажмите ⚙ → **Удалить**;

5.1.2 Создание групп безопасности для Windows аутентификации

Содержание

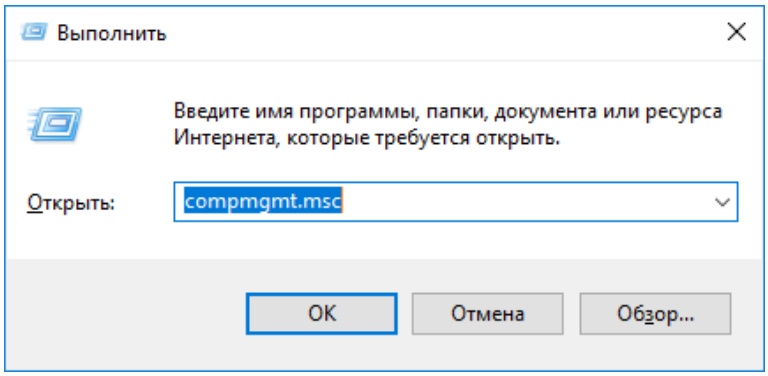
Для разграничения прав доступа RedCheck реализует ролевую модель (1.4 Ролевая модель RedCheck).

Если хосты, на которых установлены компоненты RedCheck, находятся в домене, рекомендуется создавать только доменные группы безопасности.

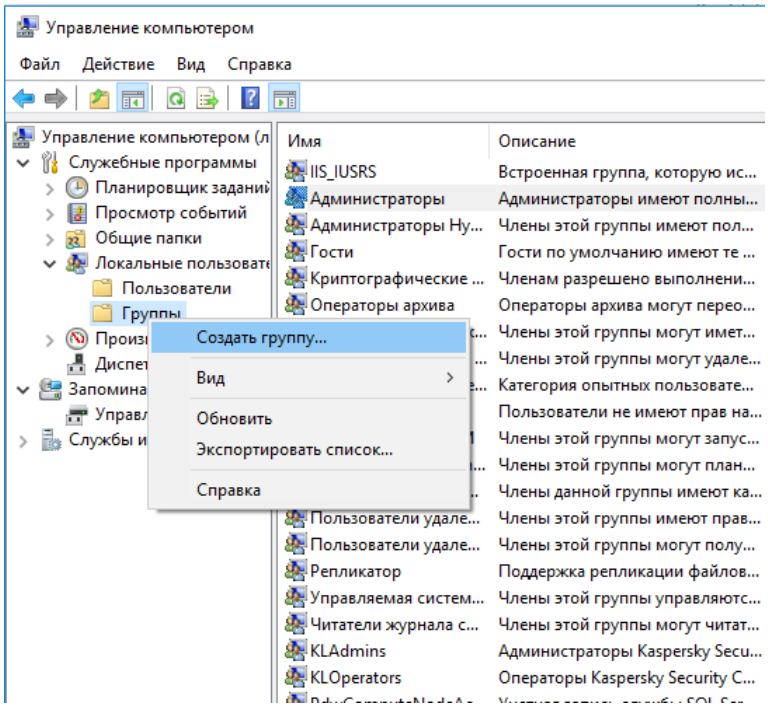
Создание локальных групп безопасности

Для Desktop версии группы создаются на устройстве с установленным RedCheck, а Web-версия требует их наличия на сервере, где установлен RestAPI компонент.

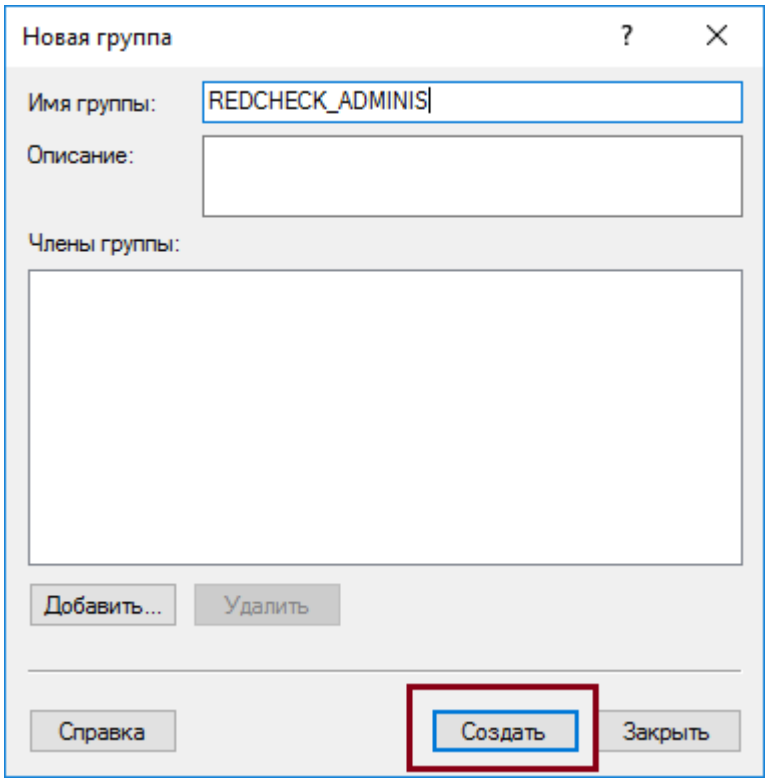
Шаг 1. Откройте **Управление компьютерами**. **Win + R** → введите **compmgmt.msc** → **OK**;



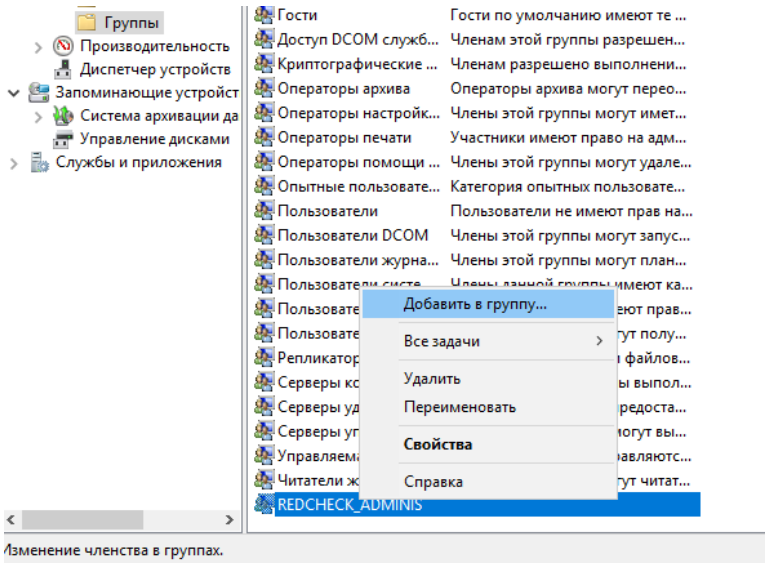
Шаг 2. Раскройте **Служебные программы** → **Локальные пользователи** → ПКМ по **Группы** → **Создать группу**;



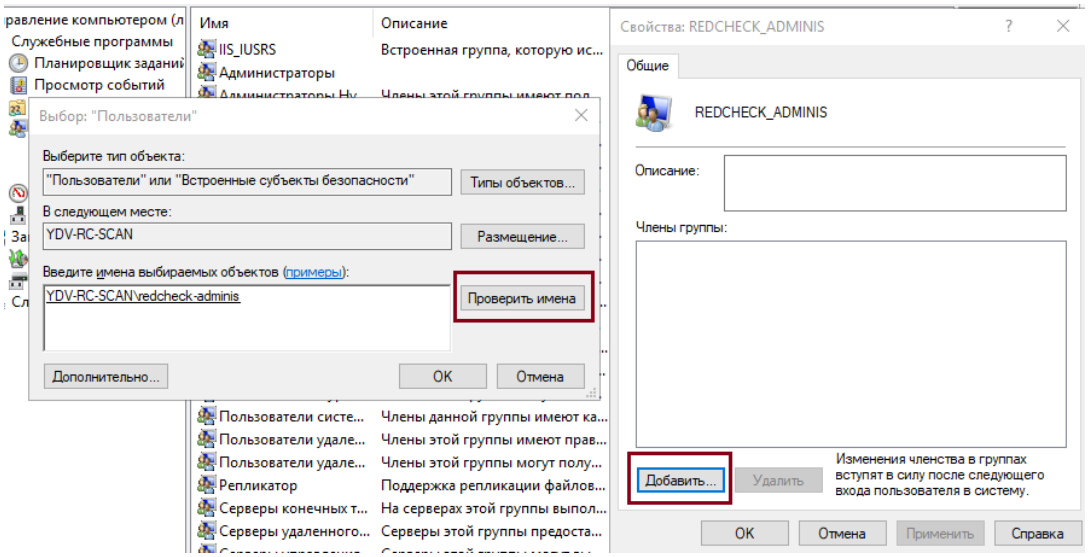
Шаг 3. Введите название группы безопасности в **Имя группы** → **Создать**;



Шаг 4. ПКМ по созданной группе → **Добавить в группу**;



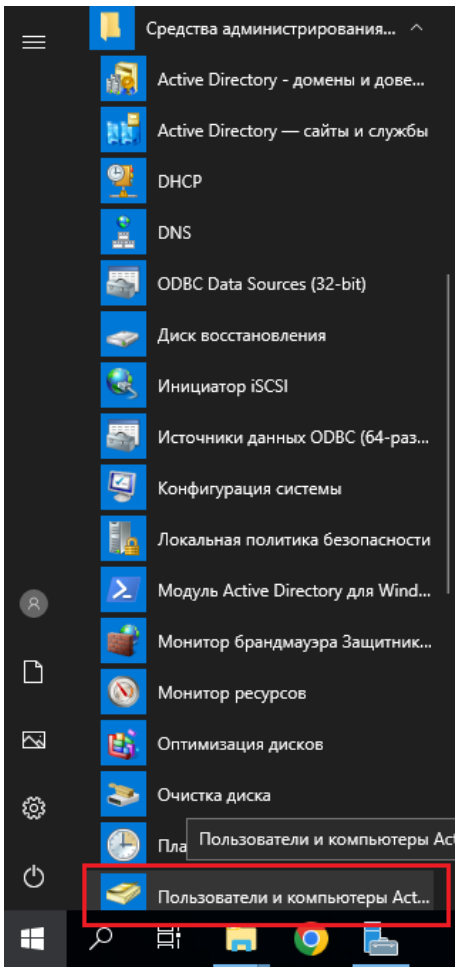
Шаг 5. Добавить → введите имя пользователя → **Проверить имена** → **ОК**.



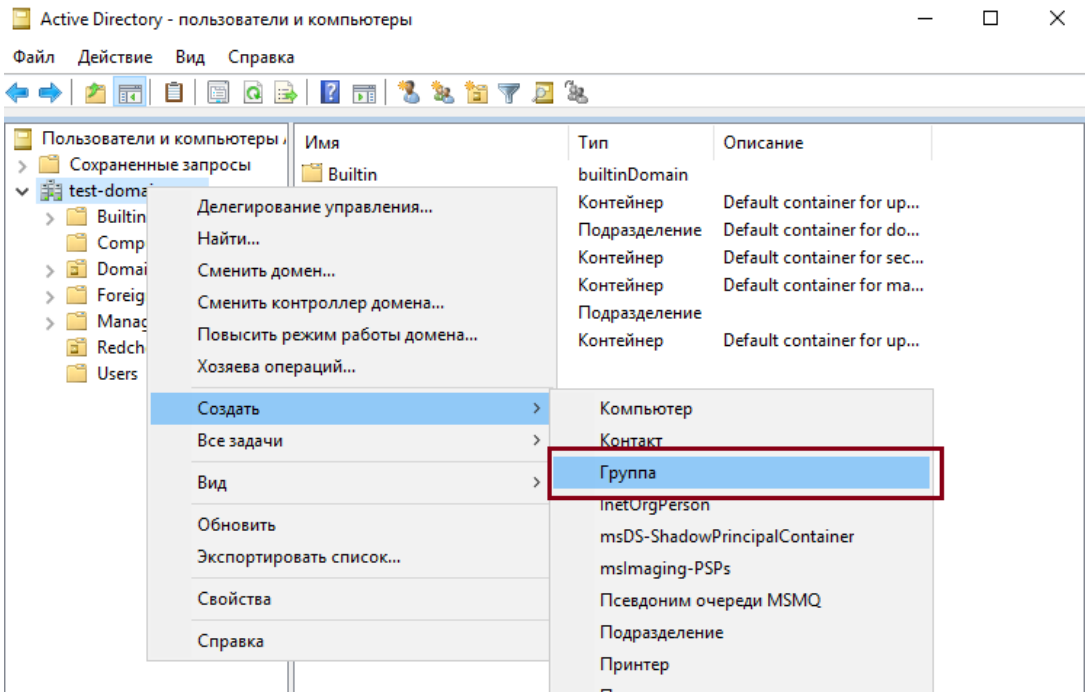
Чтобы зайти в RedCheckWeb, используя группы безопасности, нужно отметить при авторизации поле **Использовать аутентификацию Windows**.

Создание групп безопасности в домене

Шаг 1. Пуск → Средства администрирования Windows → выберите **Пользователи и компьютеры Active Directory**;

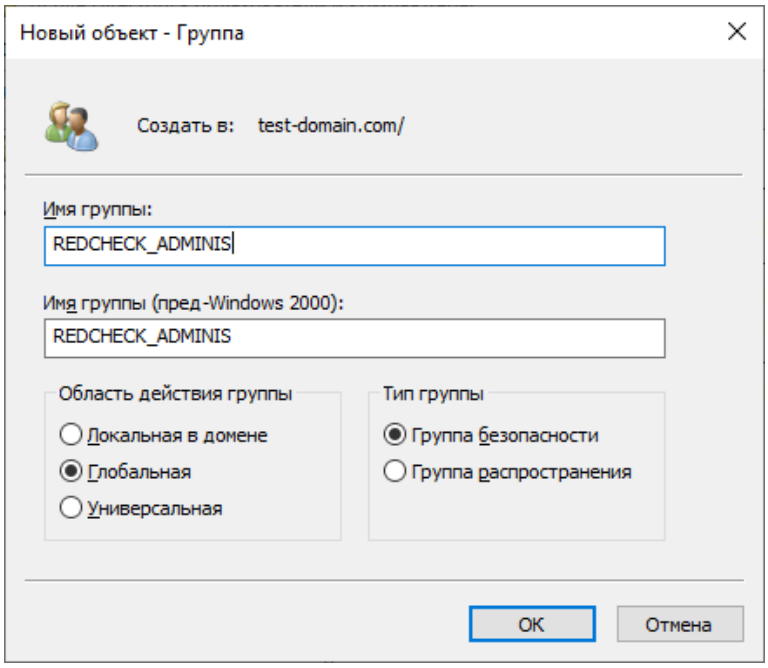


Шаг 2. ПКМ по созданному подразделению → **Создать** → **Группа**;

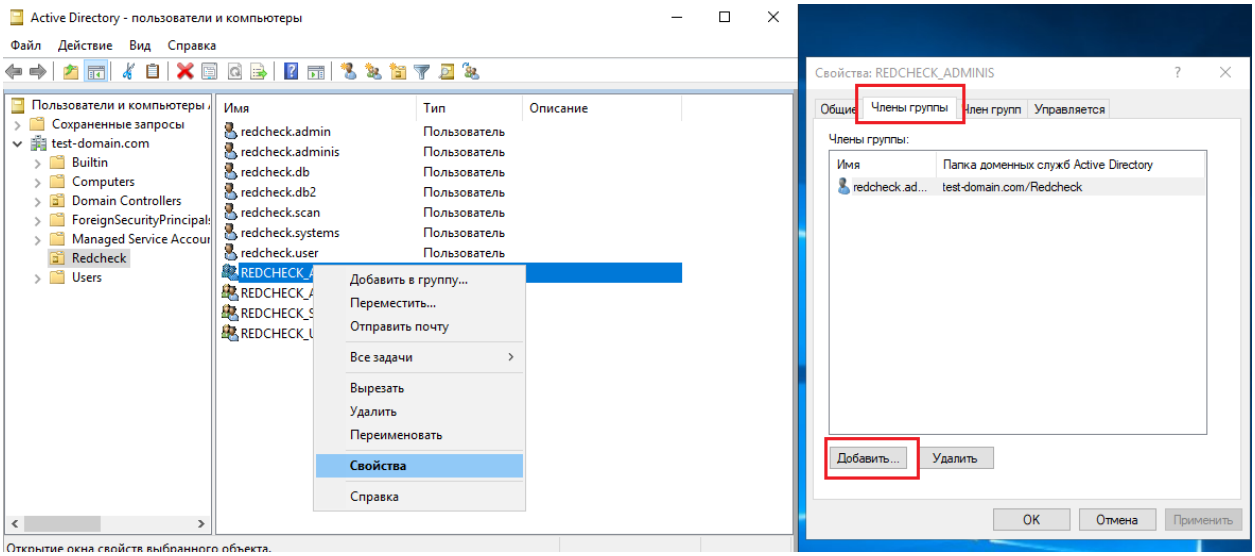


Рекомендуется создать подразделение для групп безопасности. ПКМ по названию домена → **Создать** → **Подразделение** → введите имя подразделения (к примеру, RedCheck) → **OK**

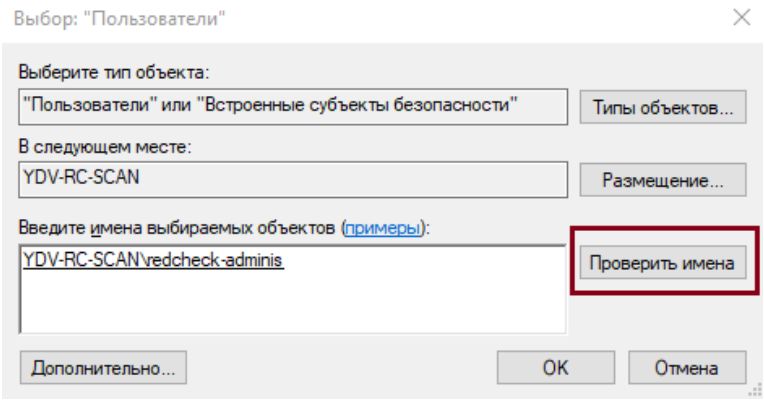
Шаг 3. Введите имя группы. Область действия группы должна быть **Глобальная**; тип группы **Группа безопасности** → **OK**;



Шаг 4. ПКМ по созданной группе → **Свойства** → **Члены группы** → **Добавить**;



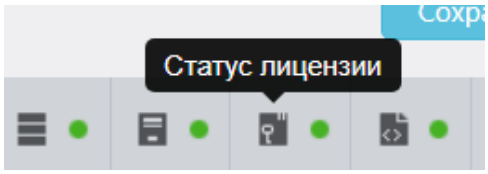
Шаг 5. Введите имя пользователя → **Проверить имена** → **ОК**.



Чтобы зайти в RedCheckWeb, используя группы безопасности, нужно отметить при авторизации поле **Использовать аутентификацию Windows**.

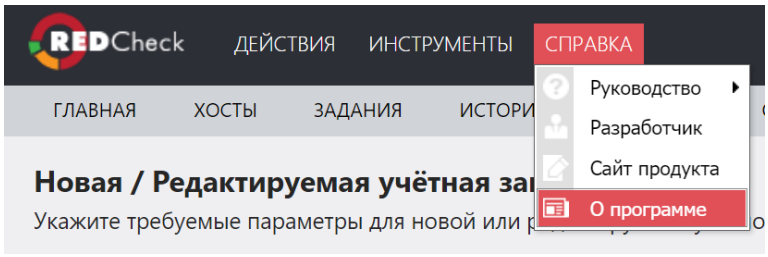
5.2 Активация лицензии

Статус лицензии отображается на статусной панели:

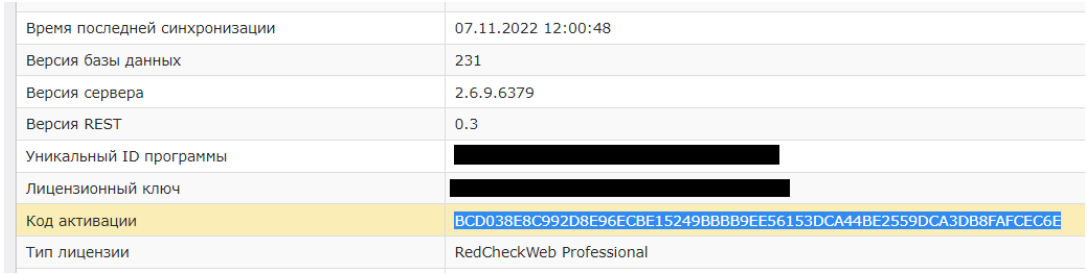


Активация лицензии через сеть Интернет происходит автоматически при запуске процесса синхронизации RedCheck. В случае отсутствия доступа к сети Интернет активация лицензии осуществляется посредством файла лицензии license.xml.

Шаг 1. На панели навигации выберите **Справка → О программе**;

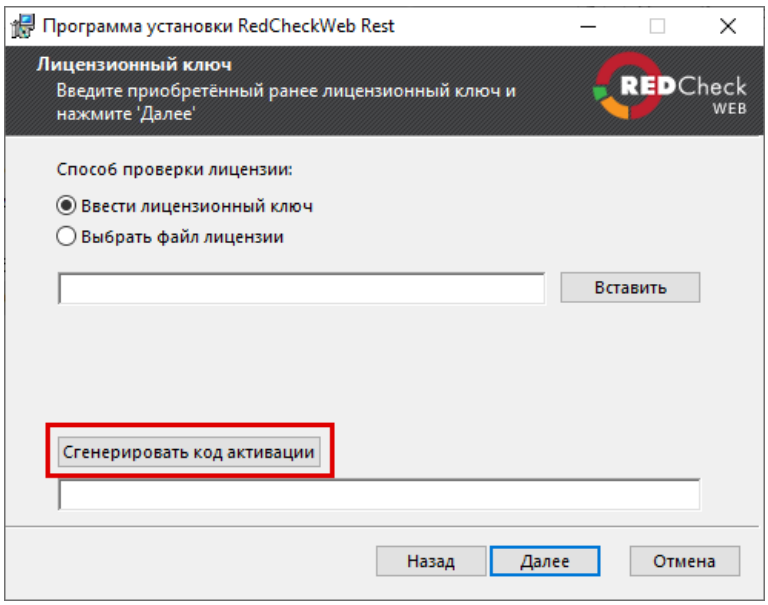


Скопируйте код активации в соответствующей строке таблицы;



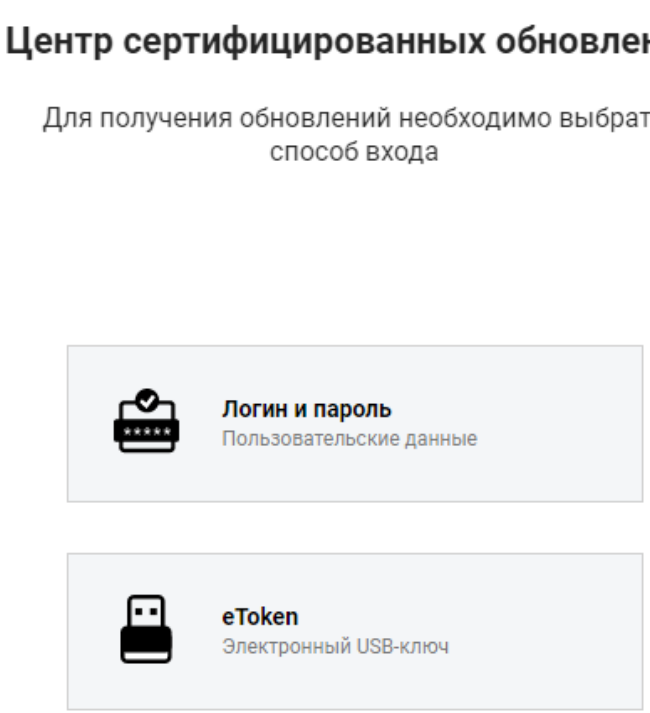
Время последней синхронизации	07.11.2022 12:00:48
Версия базы данных	231
Версия сервера	2.6.9.6379
Версия REST	0.3
Уникальный ID программы	[redacted]
Лицензионный ключ	[redacted]
Код активации	BCD038E8C992D8E96ECBE15249BBBB9EE56153DCA44BE2559DCA3DB8FAFCEC6E
Тип лицензии	RedCheckWeb Professional

Код активации можно получить во время установки серверного компонента RedCheck, нажав **Сгенерировать код активации**

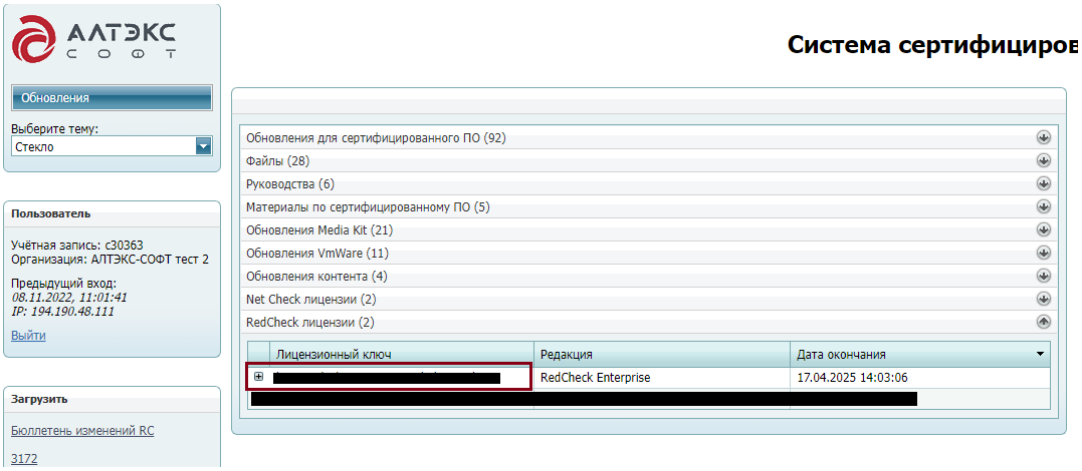


Шаг 2. Авторизуйтесь в [Центре сертифицированных обновлений]() с помощью логина и пароля;

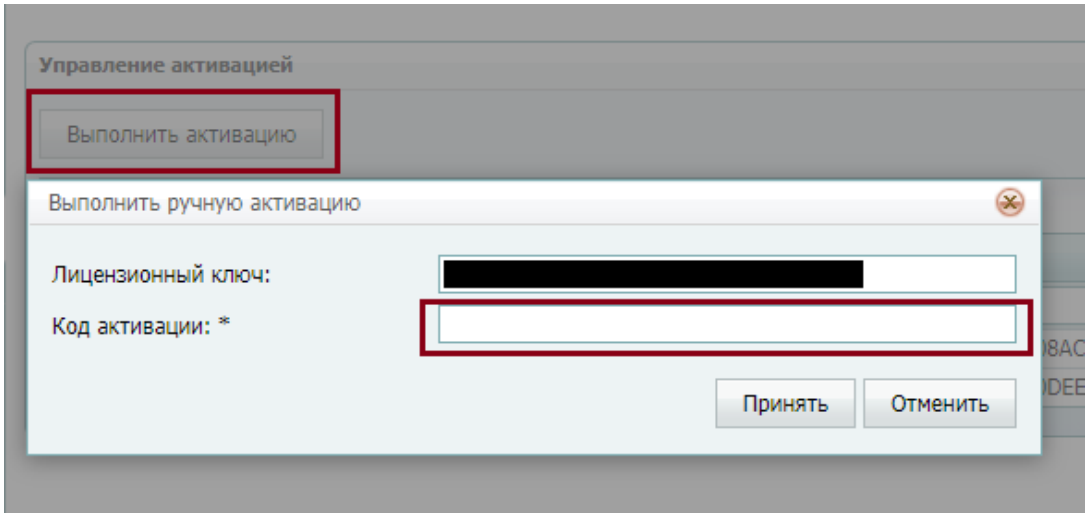
Логин/пароль поставляется всем коммерческим клиентам на последней странице формуляра (начиная с 18.05.2022).



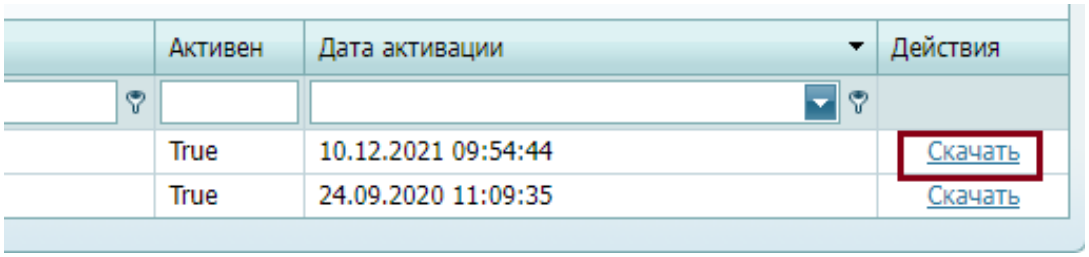
Шаг 3. Раскройте **RedCheck лицензии** → выберите интересующий Вас номер ключа RedCheck;



Нажмите **Выполнить активацию** → введите ранее скопированный код активации → **Принять**;



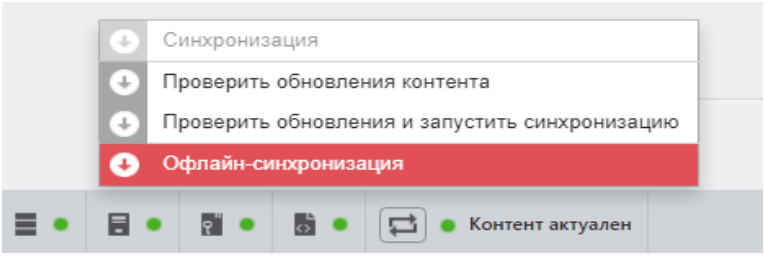
Шаг 4. Нажмите **Скачать**;



Шаг 5. Сохраните файл **license.xml** в директорию для офлайн синхронизации;

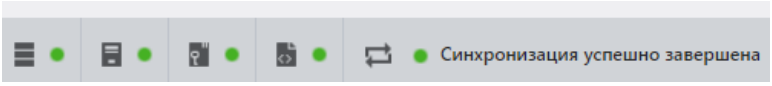
Директория может находиться в произвольном месте (например, корне системы) и должна быть доступна для чтения устройством, на котором установлена служба синхронизации.

Шаг 6. Откройте консоль управления RedCheck → нажмите на статусной панели кнопку синхронизации → **Офлайн-синхронизация**;



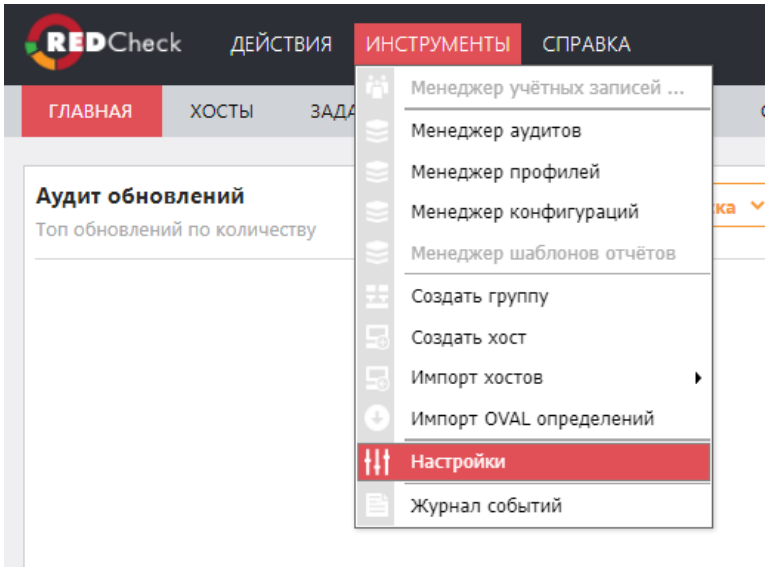
После завершения процесса синхронизации директория с контентом будет очищена. Не рекомендуется хранить в ней важные файлы.

Статус синхронизации отображается на статусной панели. Для создания новых заданий необходимо дождаться завершения процесса.



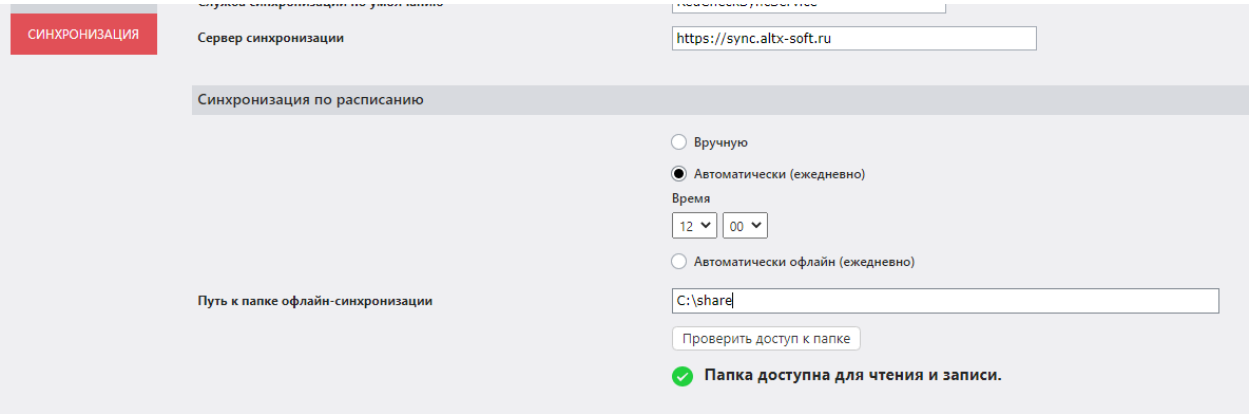
Если пункт **Офлайн-синхронизация** неактивен, нужно указать директорию для офлайн-синхронизации.

Шаг 7. На панели навигации выберите **ИНСТРУМЕНТЫ** → **Настройки**;



Для изменения настроек RedCheck авторизуйтесь под УЗ с ролью **REDCHECK_SYSTEMS** или **REDCHECK_ADMINS**

Шаг 8. Перейдите в **СИНХРОНИЗАЦИЯ** → укажите путь к директории для офлайн-синхронизации → **Проверить доступ к папке**;



Директория может находиться в произвольном месте в инфраструктуре сети и должна быть доступна для чтения хостом, на котором установлена служба синхронизации. В случае сетевой папки указывается учетная запись RedCheck, пользователь которой имеет разрешение на чтение.

5.3 Обновление контента информационной безопасности

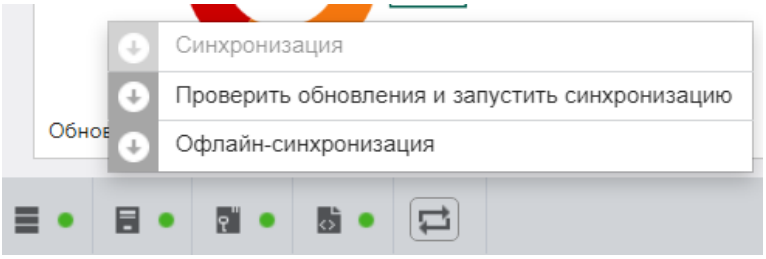
Перед началом работы в RedCheck необходимо обновить контент ИБ. Загрузка обновлений осуществляется посредством синхронизации с внешним сервером обновлений АО «АЛТЭКС-СОФТ».

Содержание

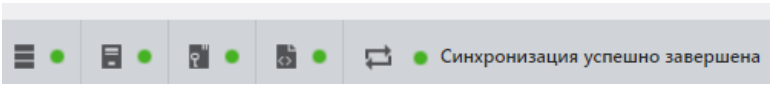
5.3.1 Синхронизация через сеть Интернет

Данный способ является предпочтительным и осуществляется по умолчанию.

Шаг 1. Откройте консоль управления RedCheck → нажмите на статусной панели кнопку синхронизации → **Проверить обновления и запустить синхронизацию**;



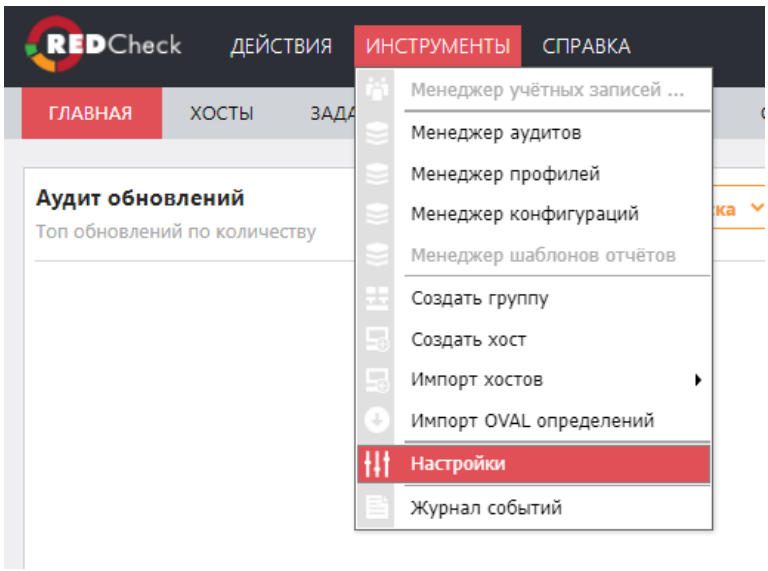
Статус синхронизации отображается на статусной панели. Для создания новых заданий необходимо дождаться завершения процесса.



5.3.2 Офлайн-синхронизация

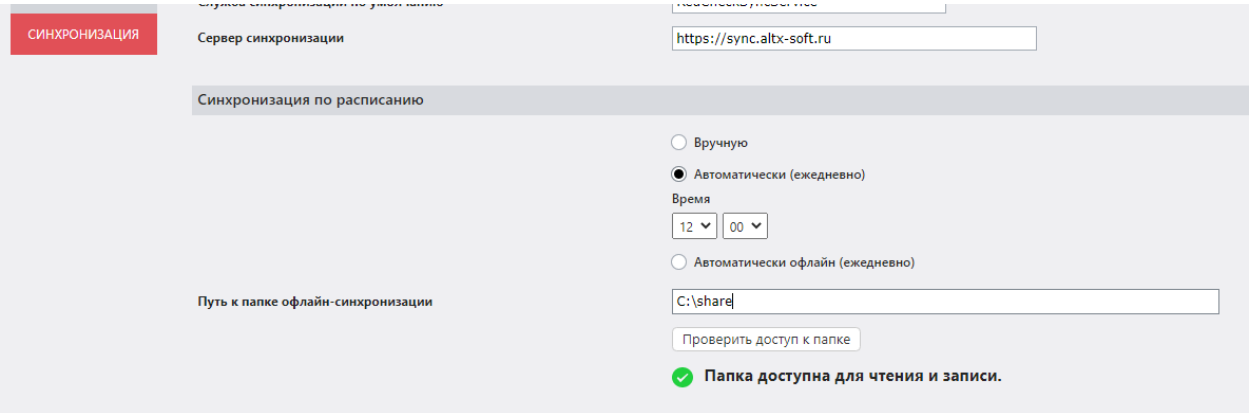
В случае отсутствия доступа к сети Интернет обновление контента ИБ осуществляется посредством архива с необходимым контентом.

Шаг 1. Откройте консоль управления RedCheck → на панели навигации выберите **ИНСТРУМЕНТЫ** → **Настройки**;



Для изменения настроек RedCheck авторизуйтесь под УЗ с ролью **REDCHECK_SYSTEMS** или **REDCHECK_ADMINS**

Шаг 2. Перейдите в **СИНХРОНИЗАЦИЯ** → укажите путь к директории для офлайн-синхронизации → **Проверить доступ к папке**;

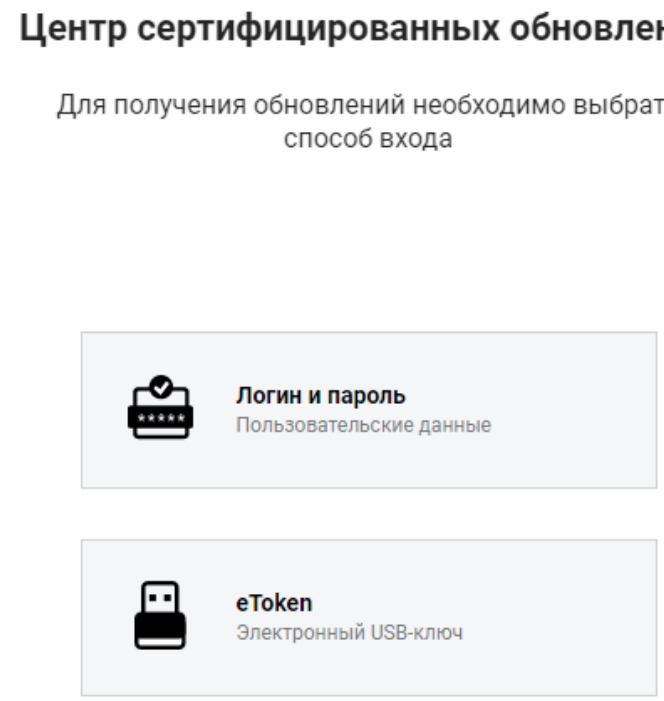


Директория может находиться в произвольном месте в инфраструктуре сети и должна быть доступна для чтения хостом, на котором установлена служба синхронизации. В случае сетевой папки указывается учетная запись RedCheck,

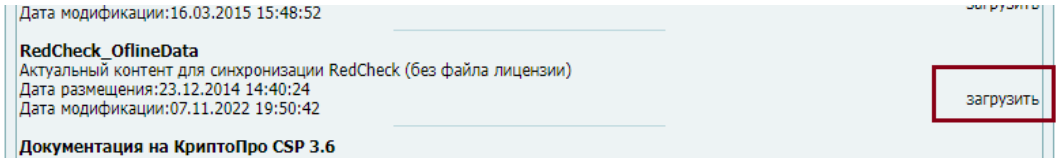
пользователь которой имеет разрешение на чтение.

Шаг 3. Авторизуйтесь в Центре сертифицированных обновлений с помощью логина и пароля;

Логин/пароль поставляется всем коммерческим клиентам на последней странице формуляра (начиная с 18.05.2022).

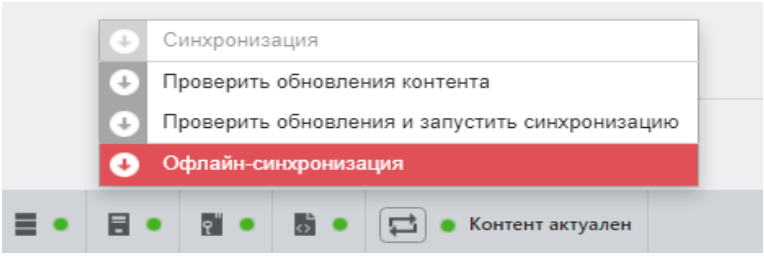


Шаг 4. Раскройте **Файлы** → скачайте архив **RedCheck_OfflineData**, нажав **Загрузить**;



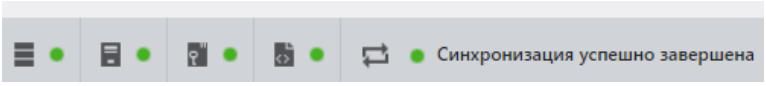
Шаг 5. Распакуйте архив в директорию для офлайн-синхронизации, указанную в настройках консоли управления RedCheck;

Шаг 6. Откройте консоль управления RedCheck → нажмите на статусной панели кнопку синхронизации → **Офлайн-синхронизация**;



После завершения процесса синхронизации директория с контентом будет очищена. Не рекомендуется хранить в ней важные файлы.

Статус синхронизации отображается на статусной панели. Для создания новых заданий необходимо дождаться завершения процесса.

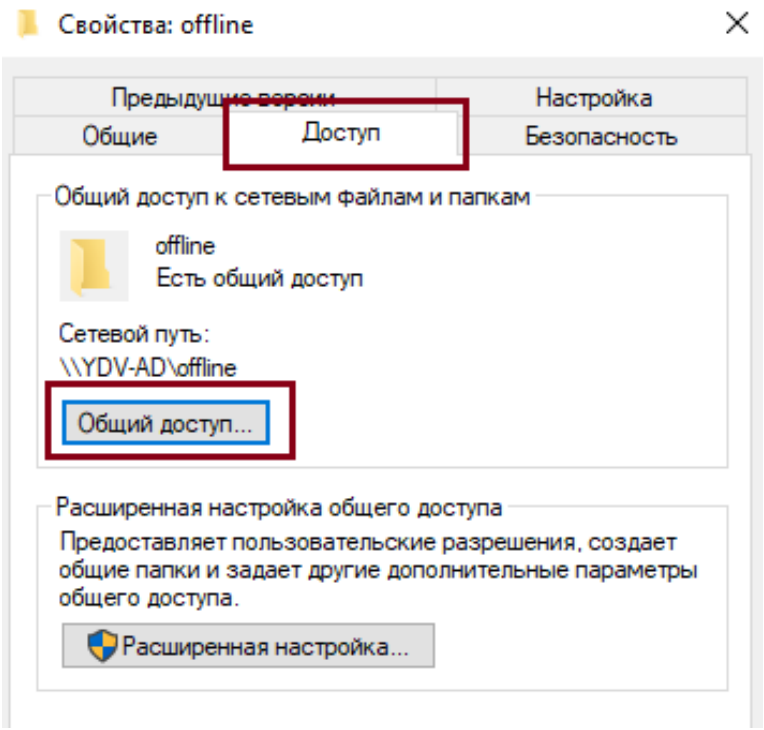


5.3.3 Синхронизация через RedCheck Update Server

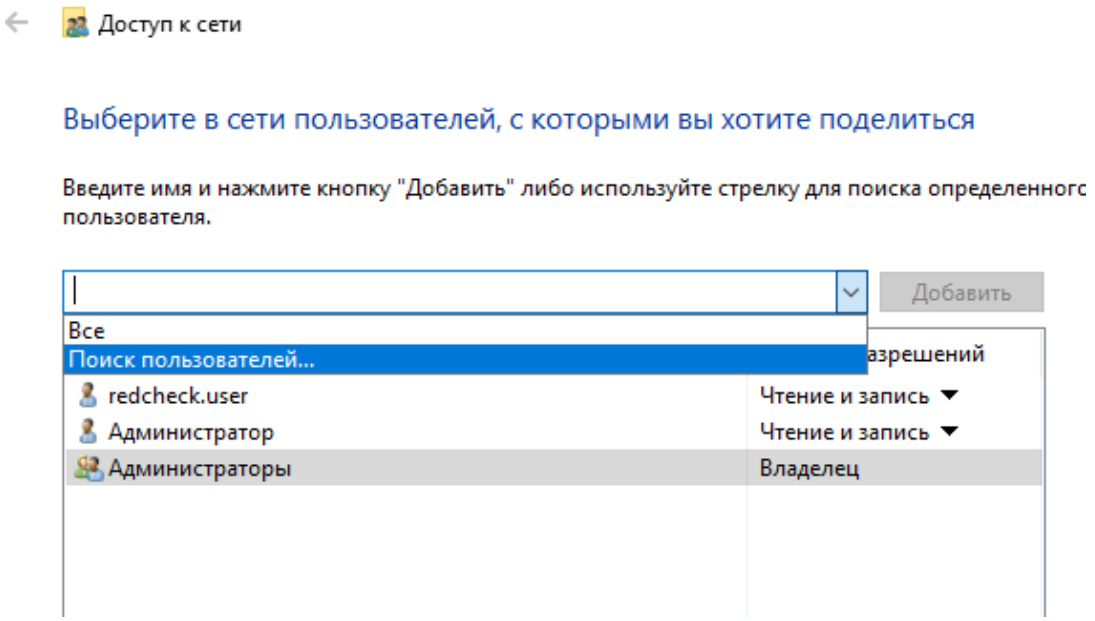
Более подробная инструкция по работе с компонентов находится в отдельном Руководстве.

Шаг 1. Создайте на хосте с установленным RedCheck Update Server в DMZ-сегменте директорию с произвольным названием и местоположением. В данной инструкции создается директория **offline** (C:\offline);

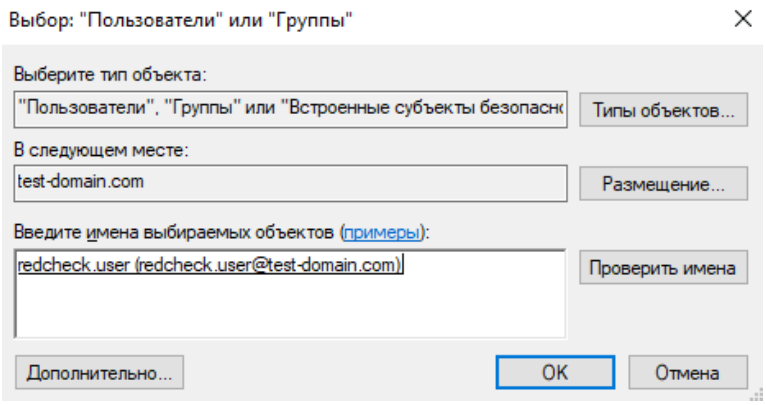
Шаг 2. ПКМ по созданной директории→ **Свойства** → **Доступ** → **Общий доступ**;



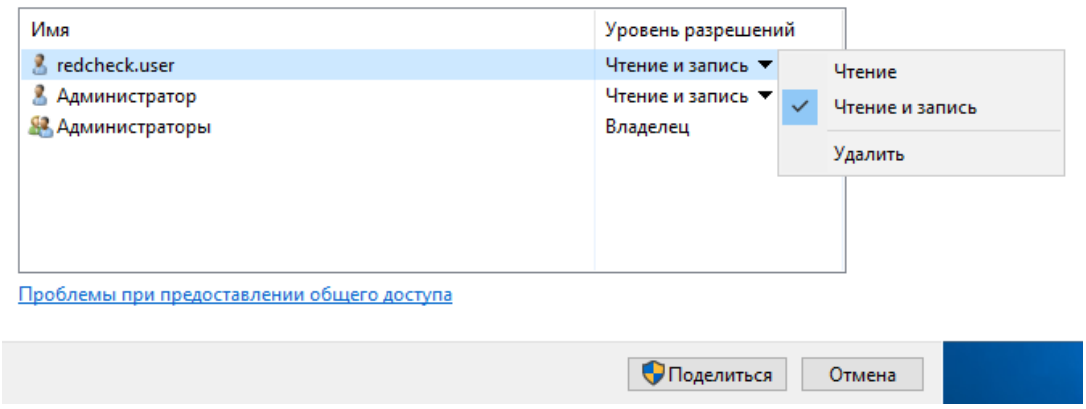
Раскройте список → **Поиск пользователей**;



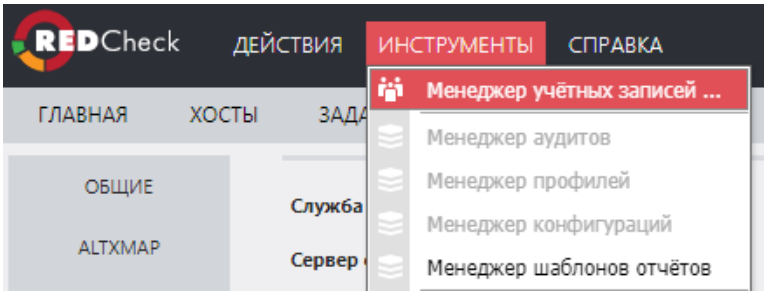
Укажите имя пользователя, который будет иметь доступ к созданной директории с контентом → **ОК**;



Предоставьте разрешения на **Чтение и запись** → **Поделиться;**

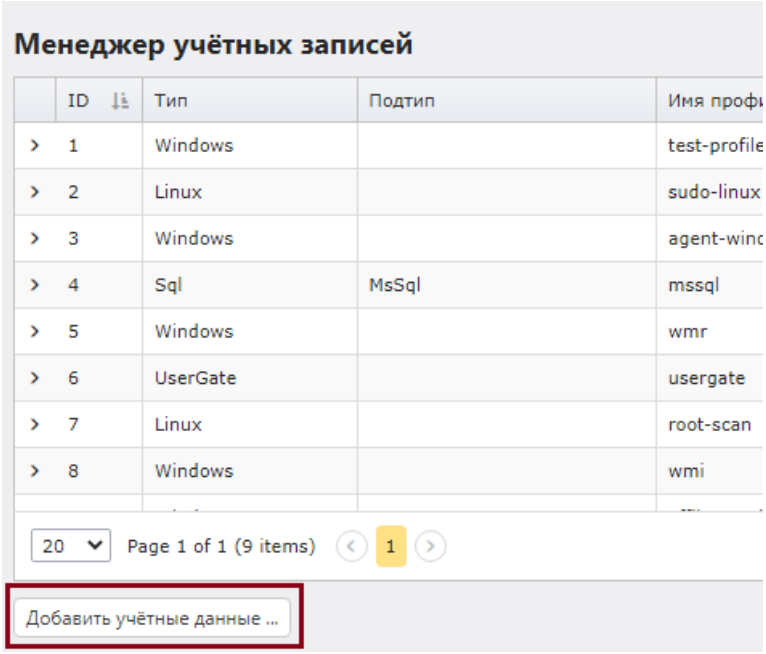


Шаг 3. Откройте консоль управления RedCheck → на панели навигации выберите **ИНСТРУМЕНТЫ** → **Менеджер учетных записей**;

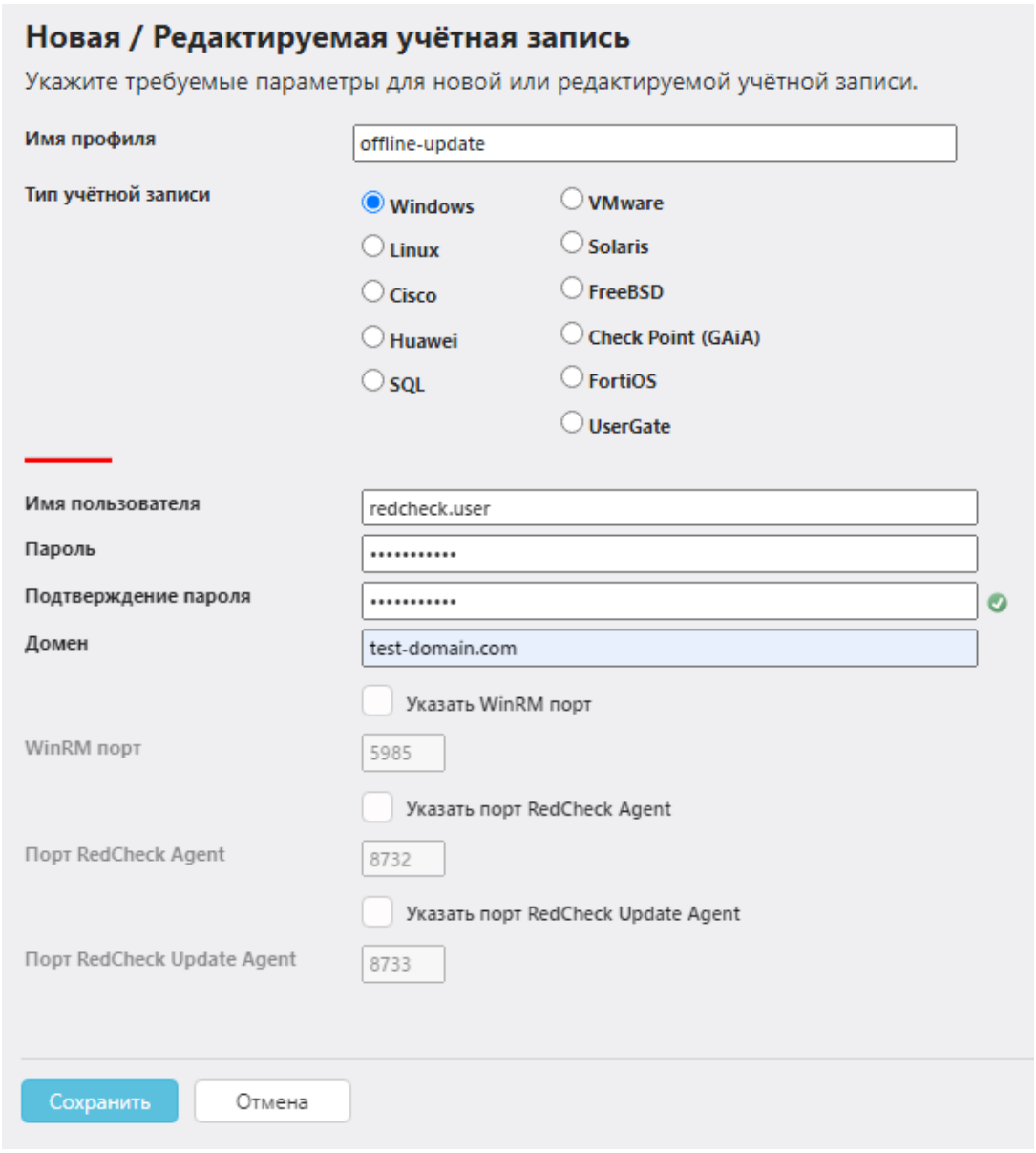


Для изменения настроек RedCheck авторизуйтесь под УЗ с ролью **REDCHECK_SYSTEMS** или **REDCHECK_ADMINS**

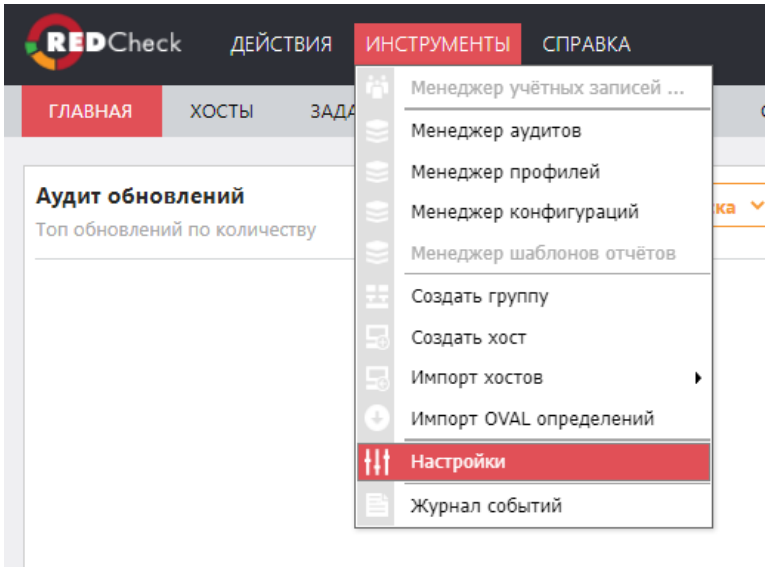
Нажмите **Добавить учетные данные;**



Выберите **Тип учетной записи** – **Windows.** Укажите учетные данные пользователя, у которого есть доступ к сетевой папке → **Сохранить**;

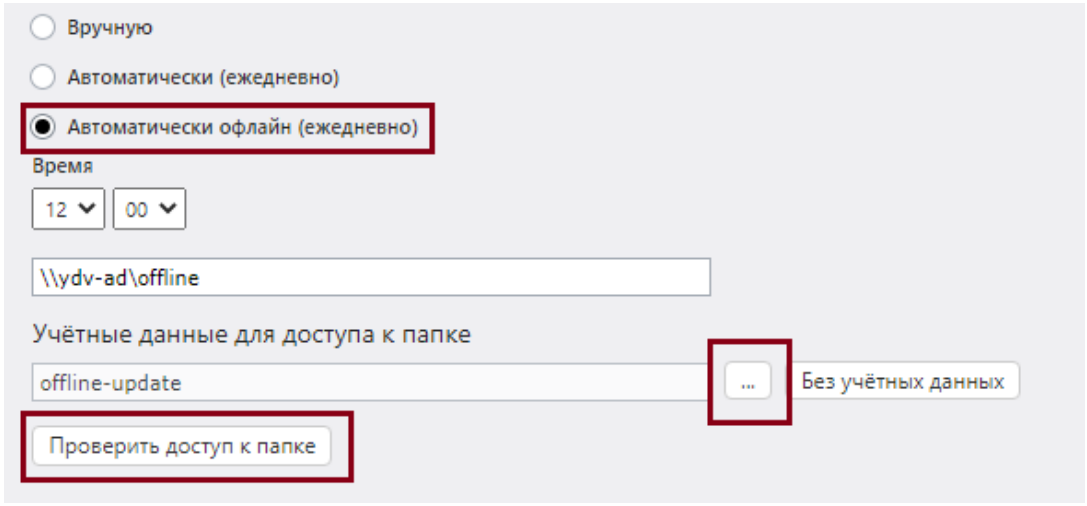


Шаг 4. На панели навигации выберите **ИНСТРУМЕНТЫ** → **Настройки**;

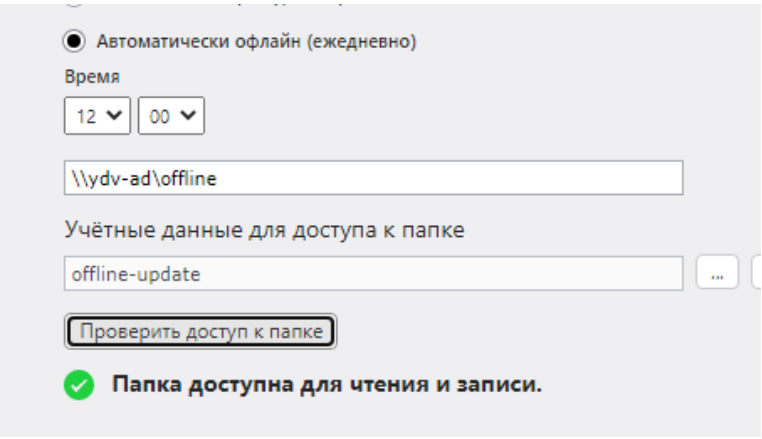


Перейдите в **СИНХРОНИЗАЦИЯ**:

- Отметьте **Автоматически офлайн (ежедневно)**. Измените по необходимости время;
- Укажите путь к сетевой папке;
- Выберите ранее созданную учетную запись;

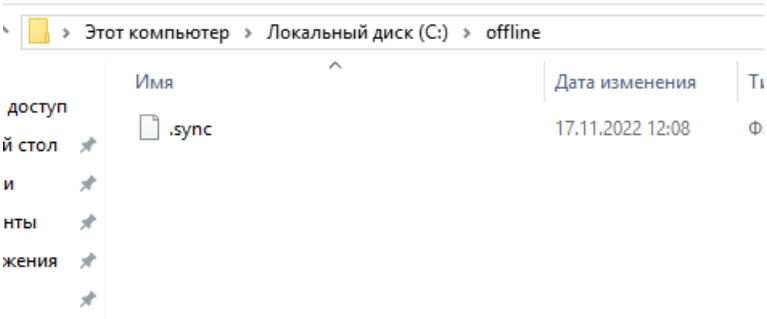


Нажмите **Проверить доступ к папке** и дождитесь положительного результата;

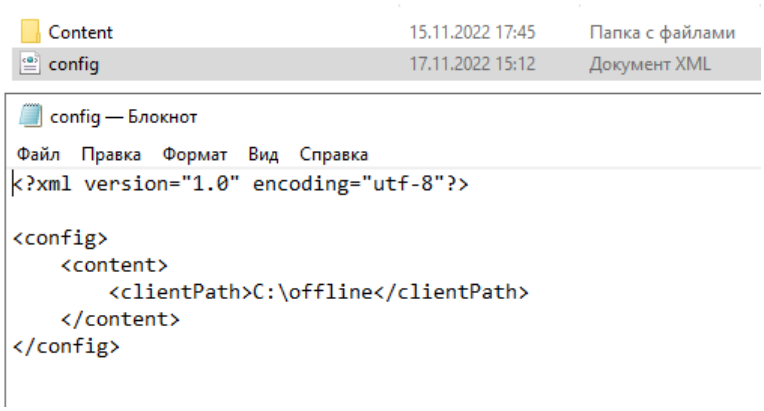


Шаг 5. Нажмите **Сохранить** для внесения изменений;

После сохранения и проверки доступа в сетевой папке в ней появится файл **.sync**;



Шаг 6. Перейдите в директорию C:\ProgramData\ALTEX-SOFT\RedCheckUpdateServer → отредактируйте файл **config.xml**, добавив строку **<clientPath>адрес_директории_для_синхронизации</clientPath>**

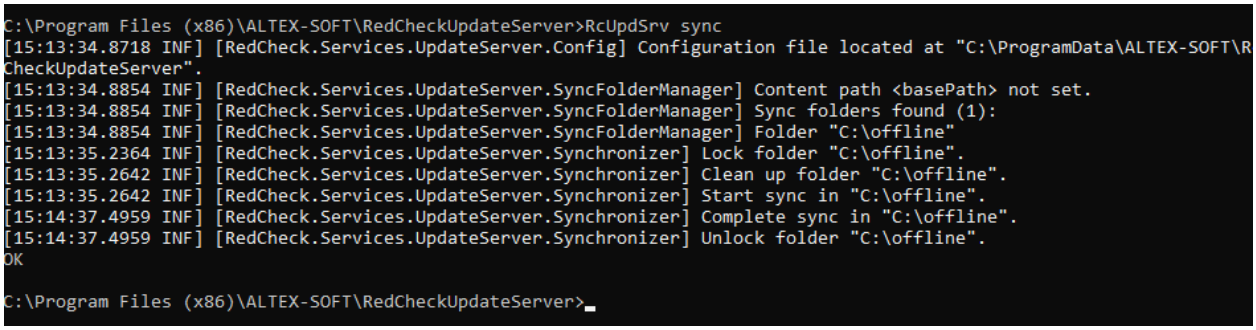


Шаг 7. Перейдите в директорию с установленным RedCheckUpdateServer (по умолчанию C:\ProgramFiles (x86)\ALTEX-SOFT\RedCheckUpdateServer) → введите в поле для адреса **cmd** → выполните команду:

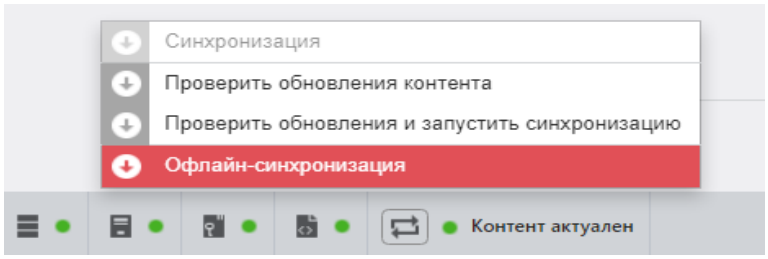
Код

```
RcUpdSrv sync
```

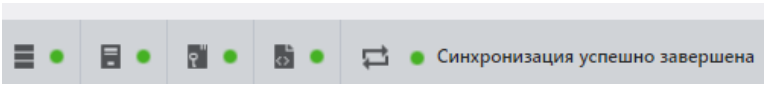
Начнется скачивание недостающего контента ИБ;



Шаг 8. Откройте консоль управления RedCheck → нажмите на статусной панели кнопку синхронизации → **Офлайн-синхронизация**;



Статус синхронизации отображается на статусной панели. Для создания новых заданий необходимо дождаться завершения процесса.



Возможно выполнять автоматическую синхронизацию, настроив ежедневный запуск RedCheck Update Server в определенное время посредством Планировщика заданий Windows.

5.4 Настройка учетных записей для сканирования

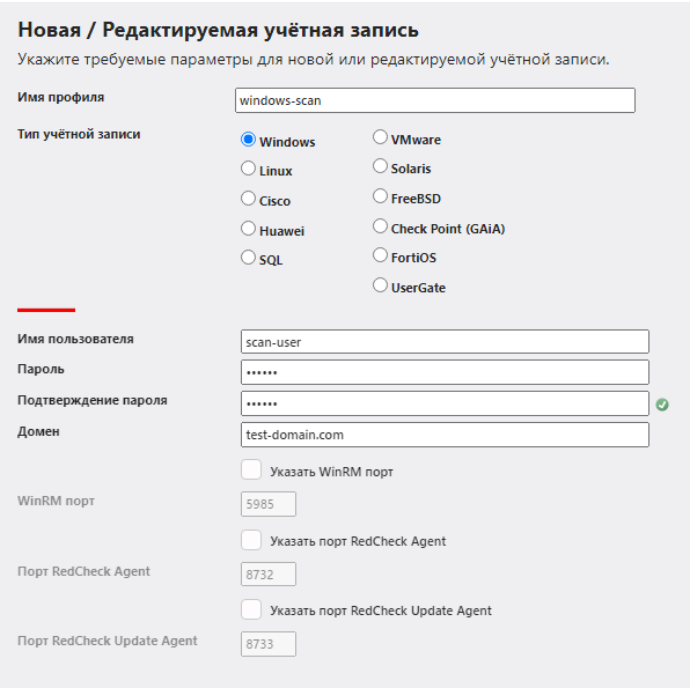
Рекомендуется:

- Не ограничивать срок действия пароля для сервисной учетной записи, если таких требований не предъявляет политика безопасности;
- Запретить учетной записи изменять свой пароль.

Содержание

5.4.1 Сканирование WIndows-систем

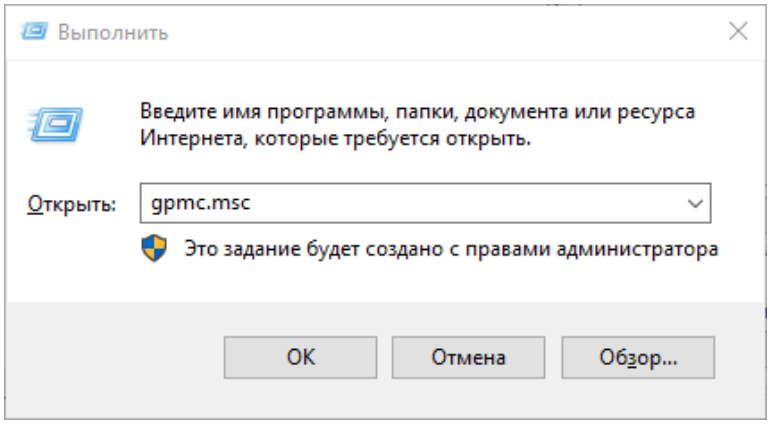
В Redcheck для сканирования удаленного хоста требуется создать учётную запись, **Тип учетной записи** – **Windows**.



Для сканирования удаленных хостов необходимо их заранее настроить. Это можно сделать как локально на каждом компьютере, так и через групповые политики, если хосты находятся в домене.

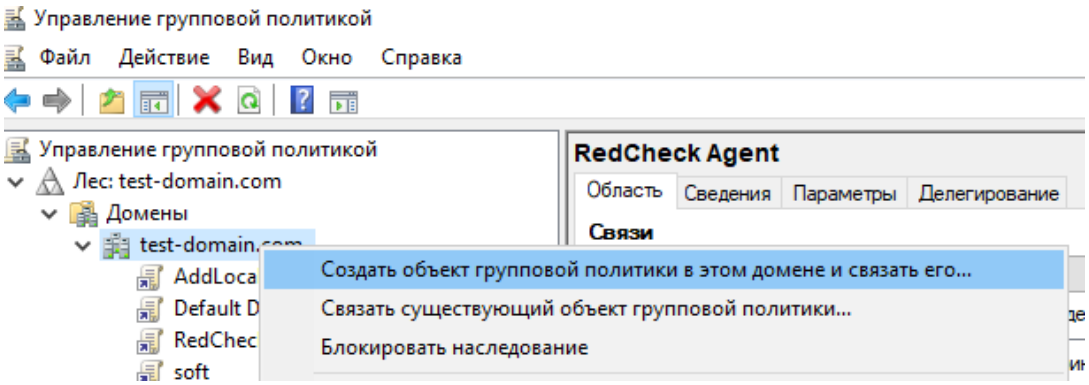
Создание групповой политики

Шаг 1. Нажмите **Win + R** → введите **gpmc.msc**;

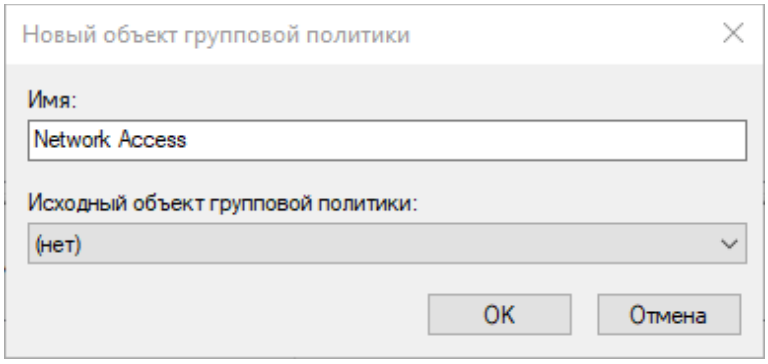


При локальной настройке нажмите **Win + R** → введите **gpedit.msc**;

Шаг 2. Раскройте **Домены** → ПКМ по **Создать объект групповой политики в этом домене...**

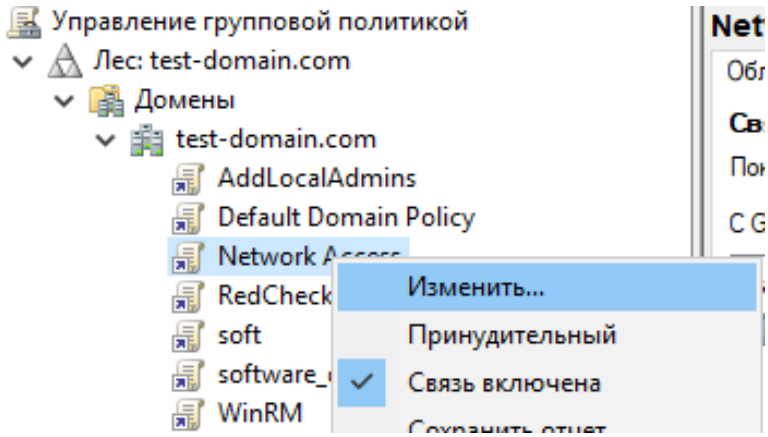


Введите название новой групповой политики;

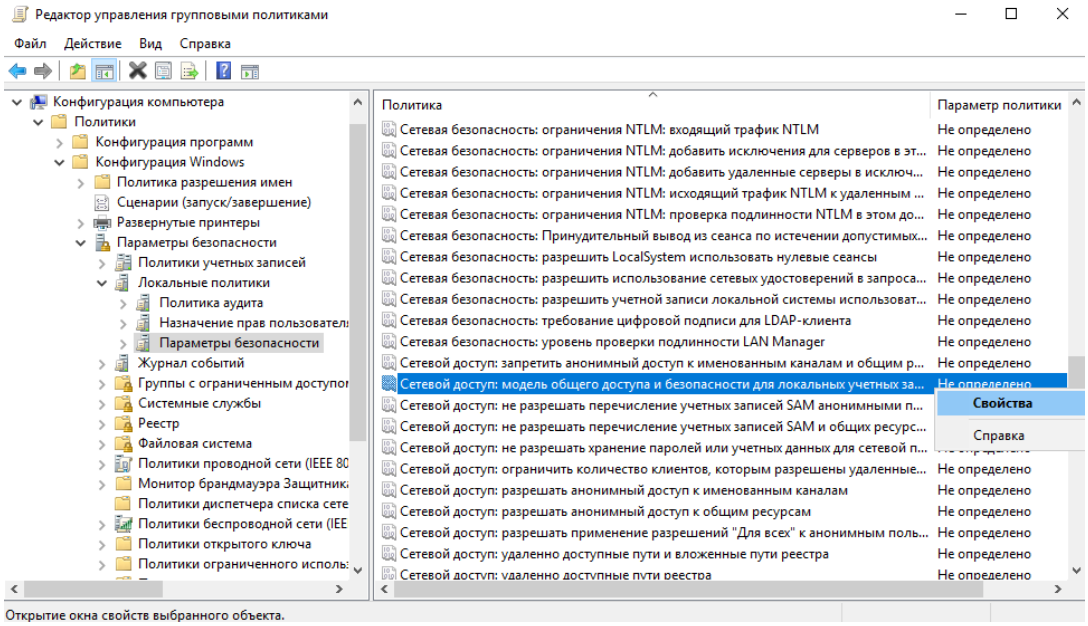


Настройка сетевого доступа

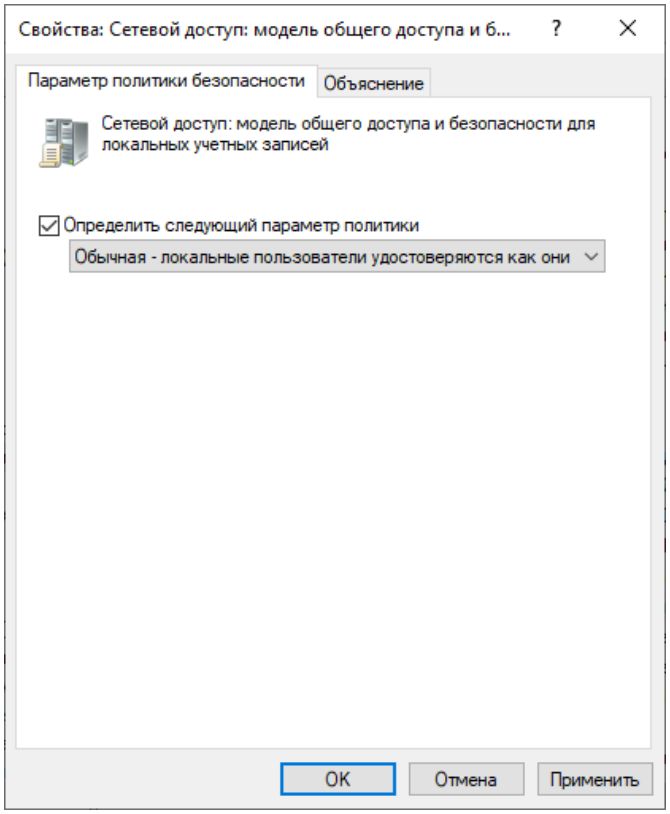
Шаг 3. ПКМ по созданной групповой политике → **Изменить**;



Шаг 4. Раскройте **Конфигурация компьютера → Политика → Конфигурация Windows → Параметры безопасности → Локальные политики → Параметры безопасности** → ПКМ по **Сетевой доступ: модель общего доступа и безопасности для локальных учетных записей → Свойства**;



Шаг 5. Отметьте **Определить следующий параметр политики** → выберите **Обычная – локальные пользователи...**

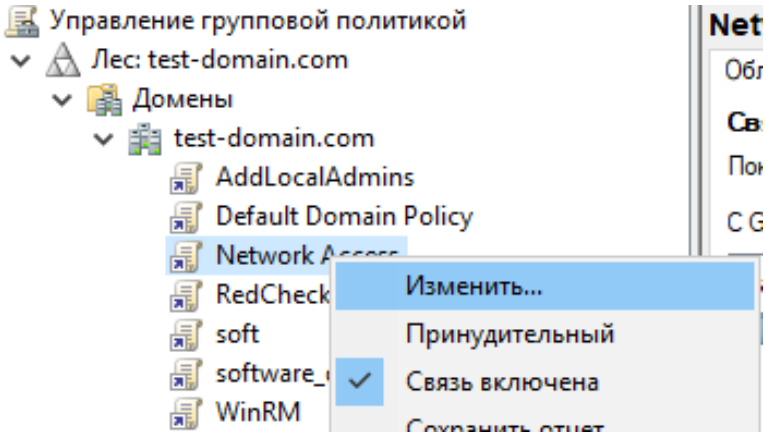


Настройка контроля учетных записей пользователей

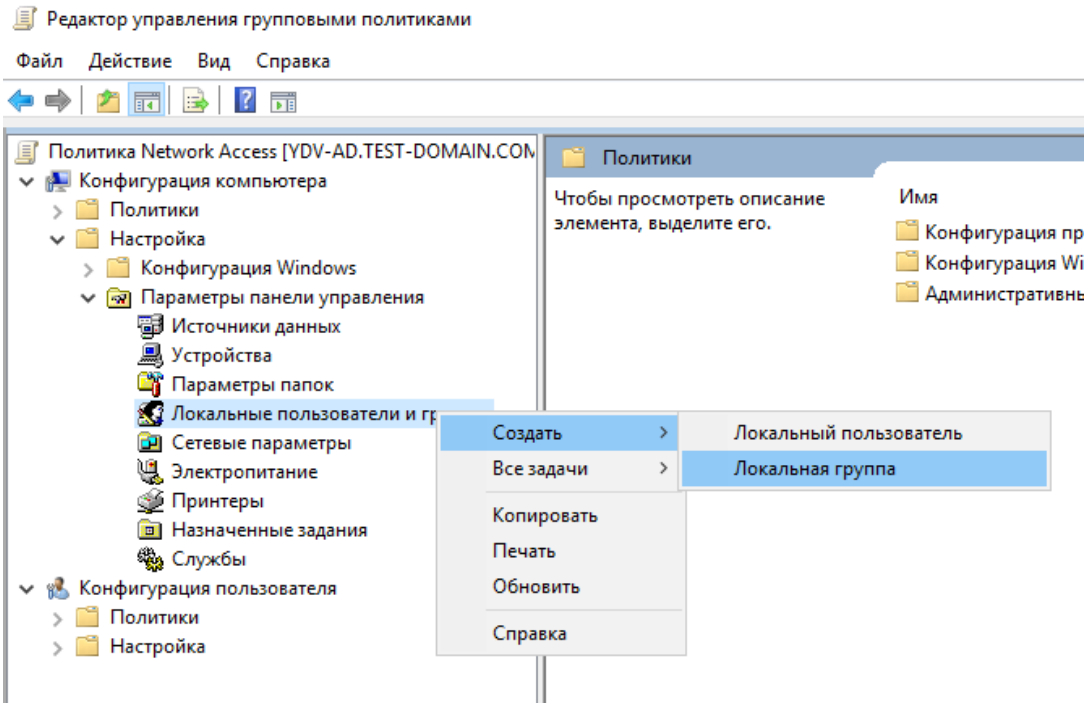
Рекомендуется использовать доменную УЗ для отключения функции UAC.

Шаг 1. Создайте доменную учетную запись, которая будет предназначена для сканирования;

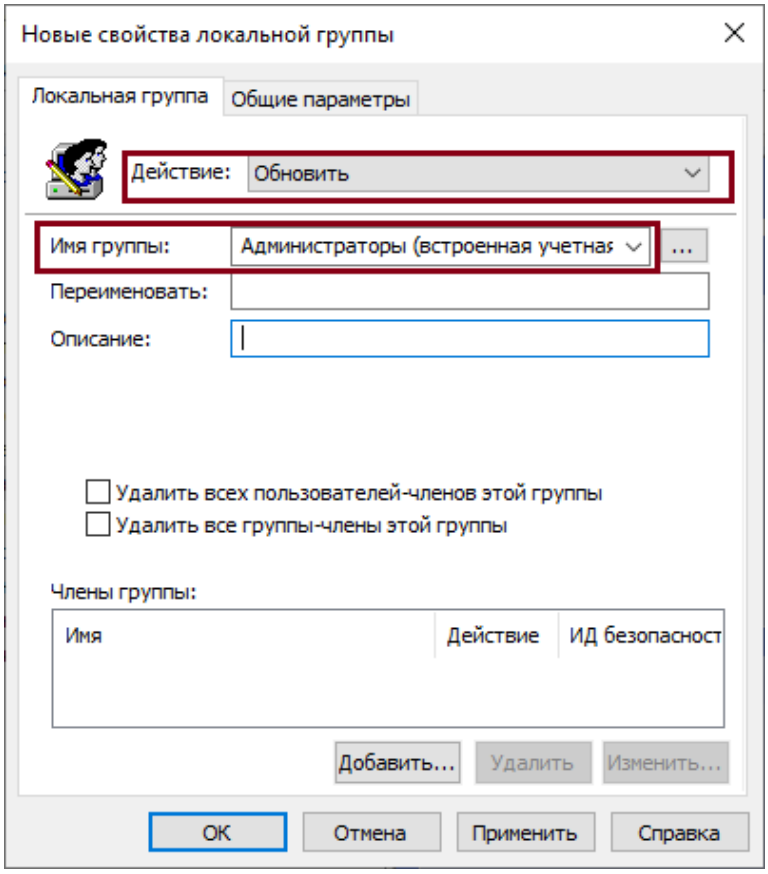
Шаг 2. ПКМ по необходимой групповой политике → **Изменить**;



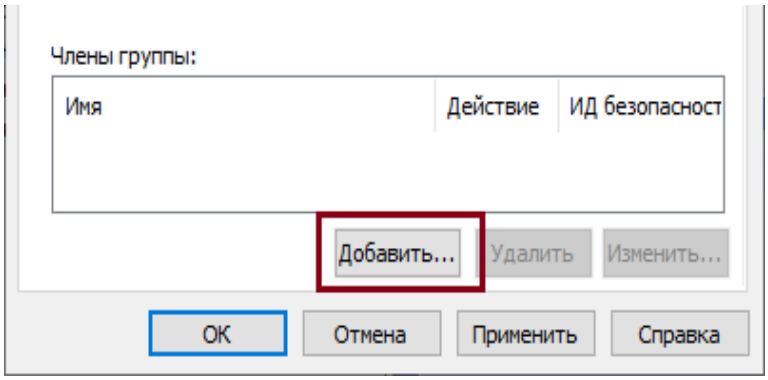
Шаг 3. Добавьте пользователя в группу локальных администраторов сканируемого хоста: **Конфигурация компьютера** → **Настройки** → **Параметры панели управления** → ПКМ по **Локальные пользователи и группы** → **Создать** → **Локальная группа**;



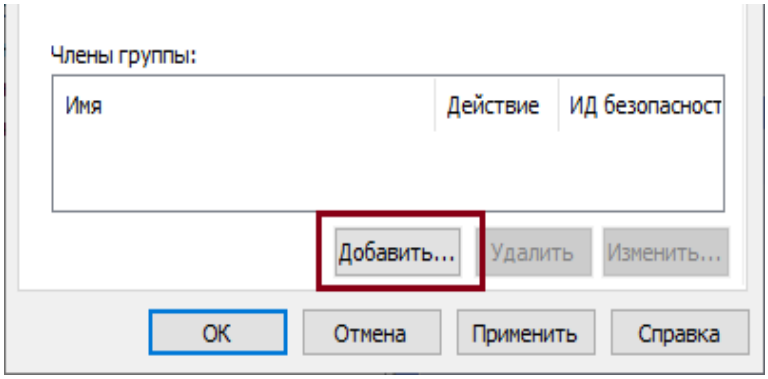
Шаг 4. В **Действие** выберите **Обновить** , в **Имя группы** – **Администраторы (встроенная учетная запись)**;



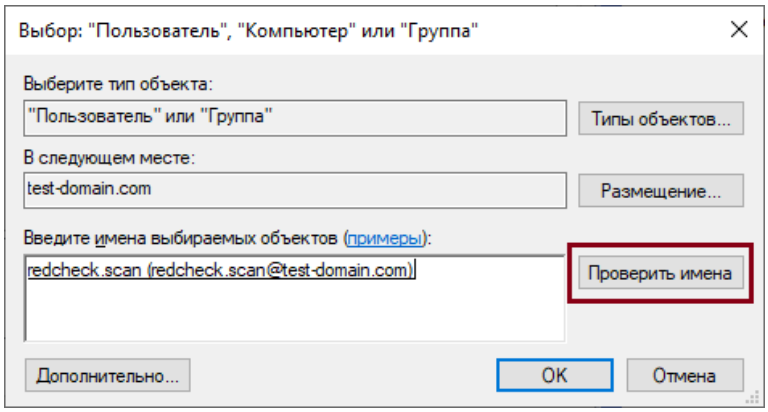
Нажмите **Добавить**;



Нажмите на троеточие справа от строки **Имя**;



Укажите имя созданного ранее пользователя → **Проверить имена** → **ОК**;



Шаг 5. Дождитесь обновления групповой политики на устройствах.

При использовании такой учётной записи настройки UAC не будут влиять на сканирование.

Дальнейшая настройка

- 5.4.1.1 Транспорт Агент RedCheck
- 5.4.1.2 Транспорт WinRM
- 5.4.1.3 Транспорт WMI

5.4.1.1 Транспорт Агент RedCheck

Для агентского сканирования на целевых хостах должен быть установлен компонент Microsoft .NET Framework 4.8.

- Должна быть запущена служба Агента, открыт порт для входящих соединений TCP (по умолчанию 8732) (4.5 Установка агента сканирования RedCheck);
- В одноранговой сети пользователь, от имени которого происходит обращение к агенту, должен находиться в локальной группе безопасности **REDCHECK_***. В случае доменной сети пользователь должен находиться в доменной группе безопасности **REDCHECK_*** (5.1.2 Создание групп безопасности для Windows аутентификации);

Для повышения безопасности в сети предприятия рекомендуется, чтобы пользователь имел роль с минимальными правами доступа в ролевой модели RedCheck (1..4 Ролевая модель RedCheck).

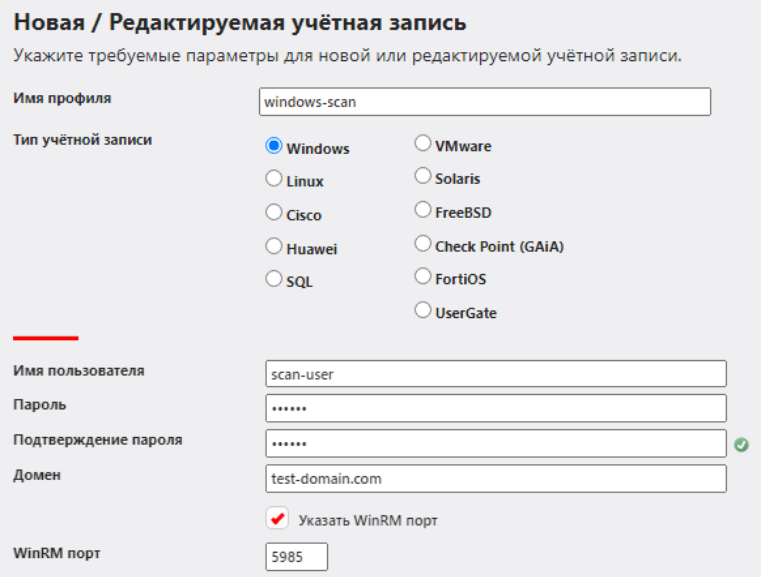
- Пропускная способность канала между Агентом и службой сканирования должна быть не менее 128 Кбит/с.

Привилегии учетной записи, необходимые для взаимодействия:

- Локальный пользователь сканируемого хоста или пользователь домена;
- Пользователь с правом удаленного подключения к хосту;
- Пользователь с правами **Вход в качестве службы**, **Доступ к компьютеру из сети**;
- Пользователь с правами на чтение списка состава групп REDCHECK_* и списка компьютеров в сети.

5.4.1.2 Транспорт WinRM

Для обеспечения сканирования хостов без применения агента сканирования RedCheck используется технология Remote Engine, которая осуществляется посредством службы удалённого управления Windows **Remote Management (WinRM)**.



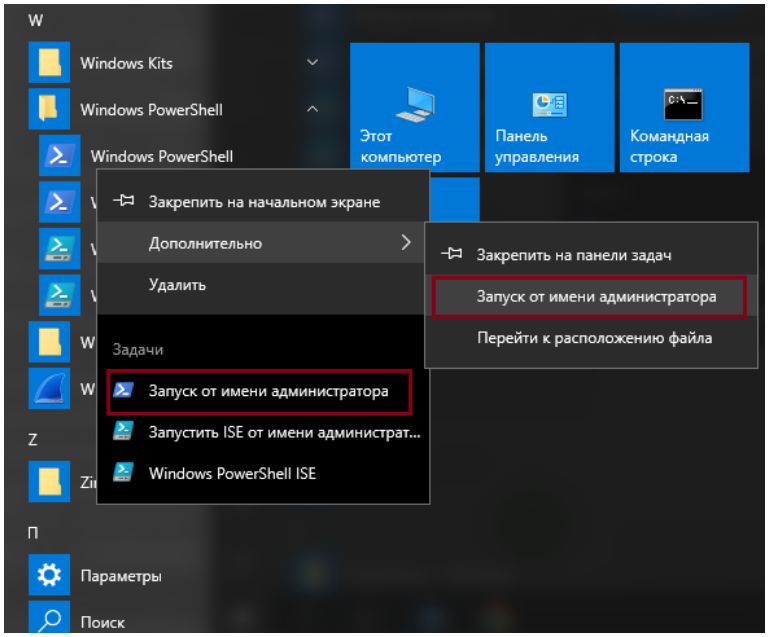
Для обеспечения сканирования в режиме Remote Engine необходимо настроить как хост, где находится служба сканирования RedCheck, так и сканируемые узлы. Все настройки производятся из консоли PowerShell от имени администратора.

Для сканирования транспортом WinRM на целевых хостах должен быть установлен компонент Microsoft .NET Framework 4.8.

Windows Remote Management присутствует в составе Windows Vista\Windows Server 2008 и более поздних версий Windows. Для более ранних версий Windows необходимо отдельно скачать и установить пакет Windows Management Framework.

Настройка хоста службы сканирования

Шаг 1. Откройте консоль **PowerShell**: **Пуск** → **Windows PowerShell** → ПКМ по **Windows PowerShell** → **Запуск от имени администратора**;



Шаг 2. Включите службу Windows Remote Management (WS-managment) командой:

```
winrm qc
```

Команда изменит тип запуска службы WinRM на автоматический, задаст стандартные настройки WinRM и добавит исключения для WinRM портов (HTTP – 5985, HTTPS - 5986) в брандмауэр Windows.

Шаг 3. Добавьте ip-адреса сканируемых хостов в список доверенных командой:

```
winrm set winrm/config/client '@{TrustedHosts="IP"}'
```

IP могут быть записаны следующими способами:

- "IP1,IP2,IP3" - перечисление;
- "192.168.100.*" - диапазон;
- “*” - все.

Настройка сканируемого узла

Шаг 4. Откройте PowerShell и выполните вышеприведенные команды. В доверенные хосты добавьте ip-адрес сервера сканирования;

Шаг 5. Для стабильной работы RedCheck в режиме Remote Engine необходимо расширить квоту по использованию памяти с 150 Мб (по умолчанию) до рекомендованных 2 Гб. Для этого в оболочке PowerShell введите команду:

```
Code

Set-Item wsman:localhost\Shell\MaxMemoryPerShellMB 2048
```

Проверка подключения

Для подключения сервера сканирования к хосту выполните команды:

Для HTTP

```
Code

Enter-PSSession -ComputerName <Host> -Port 5985 -Credential <User>
```

Для HTTPS

```
Code

Enter-PSSession -ComputerName <Host> -Port 5986 -Credential <User> -
UseSSL
```

<Host> - имя хоста;
<User> - имя пользователя для сканирования.

Если подключение не удалось, проверьте корректность настроенной вами конфигурации. Сделать это можно командой:

```
Code

winrm get winrm/config/client
```

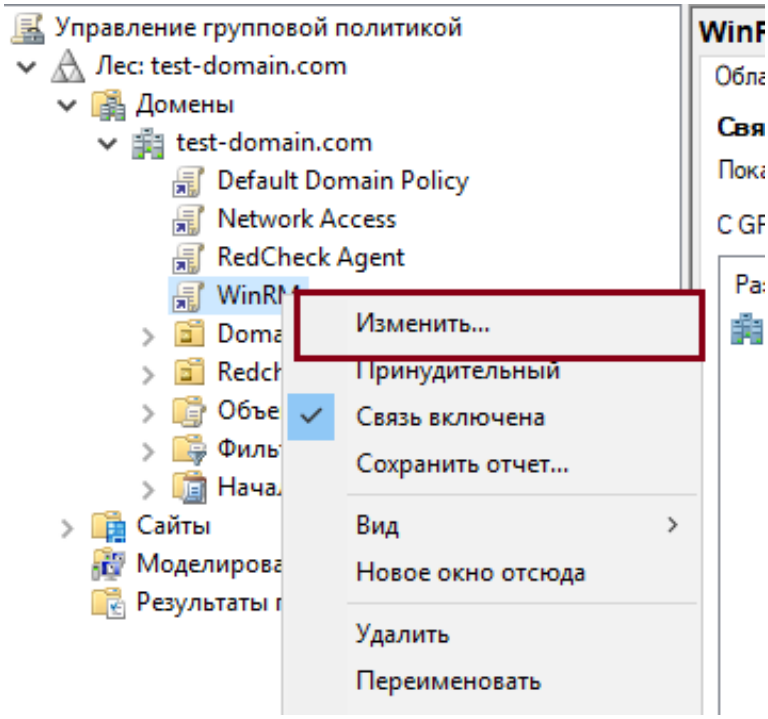
В случае возникновения проблем с подключением рекомендуется

следовать руководству.

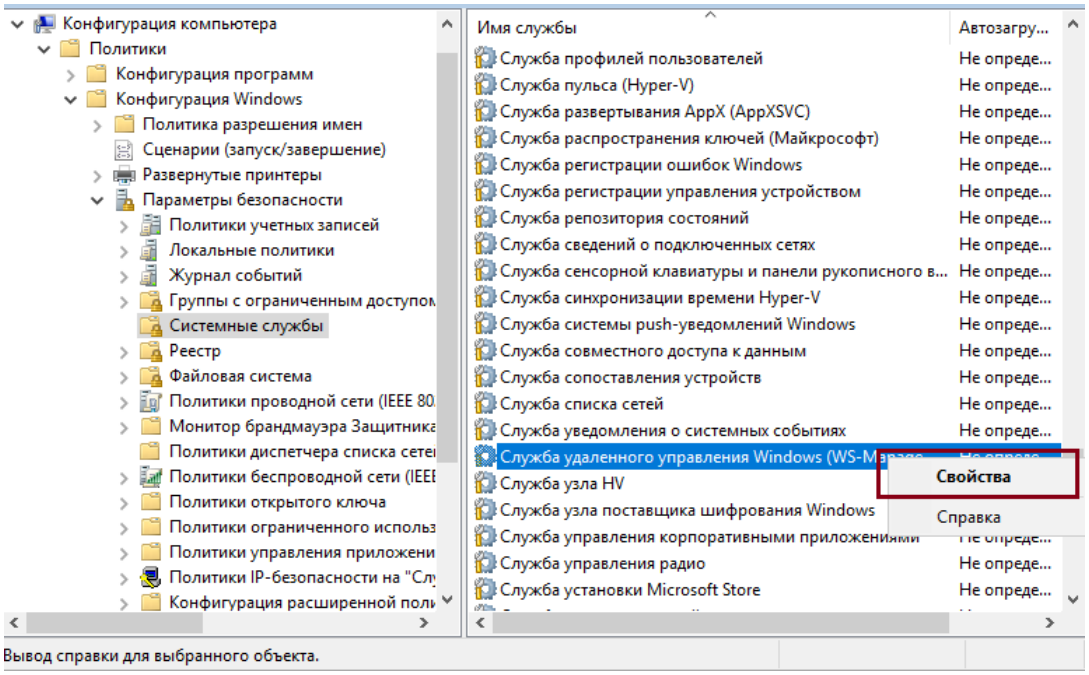
Настройка WinRM через групповые политики

Для настройки WinRM потребуется две групповые политики: одна для сервера сканирования, другая для сканируемых хостов. Их настройка идентична.

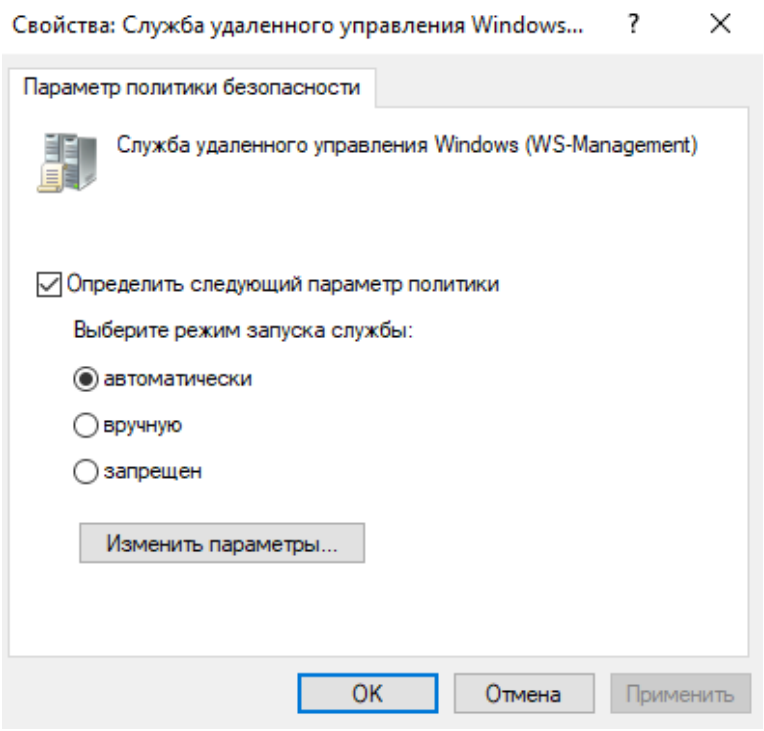
Шаг 1. ПКМ по групповой политике → **Изменить**;



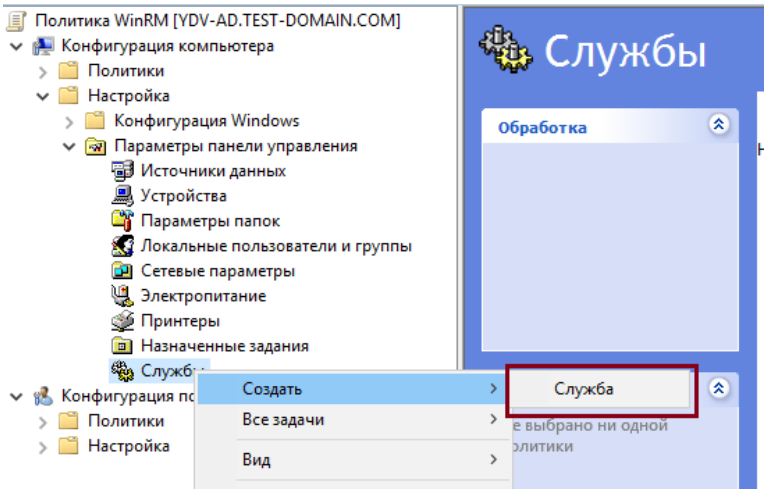
Шаг 2. Перейдите в **Конфигурация компьютера → Политики → Конфигурация Windows → Параметры безопасности → Системные службы** → ПКМ по **Служба удаленного управления Windows (WS-Management) → Свойства**;



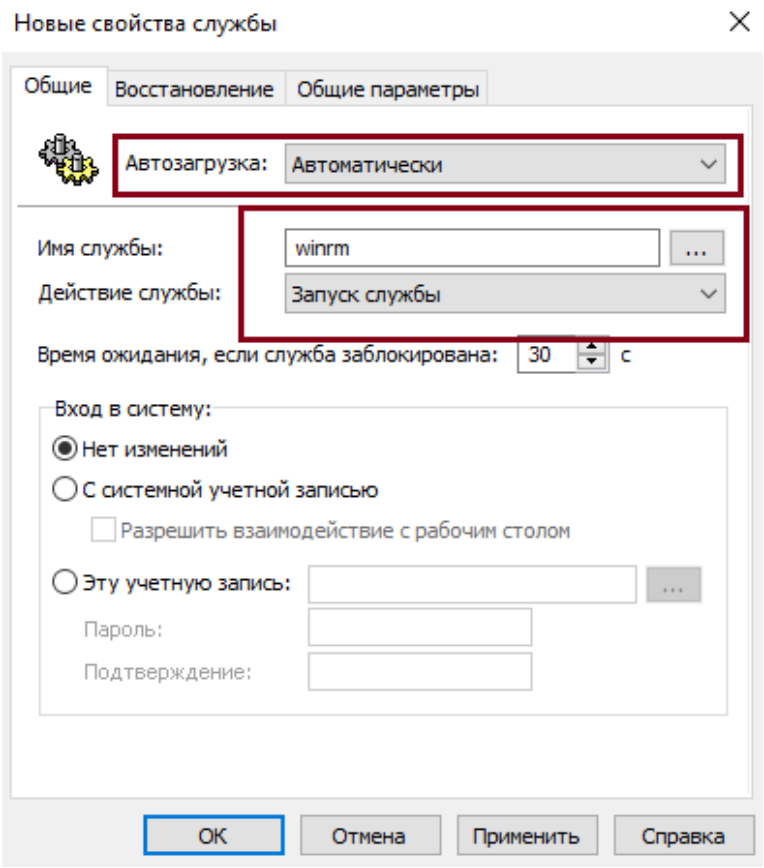
Отметьте **Определить следующий параметр политики**, режим запуска службы – **автоматически → ОК**;



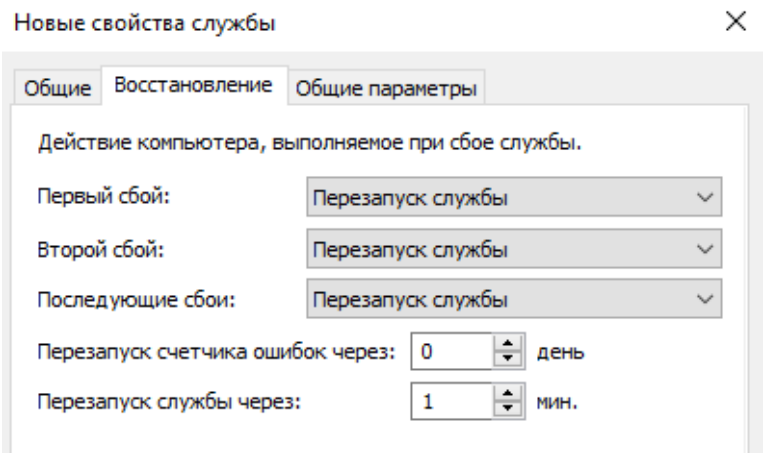
Шаг 3. Перейдите в **Конфигурация компьютера** → **Настройка** → **Параметры панели управления** →ПКМ по **Службы** → **Создать** → **Служба**;



Шаг 4. Имя службы – **winrm**. В **Действия** выберите **Запуск службы;**

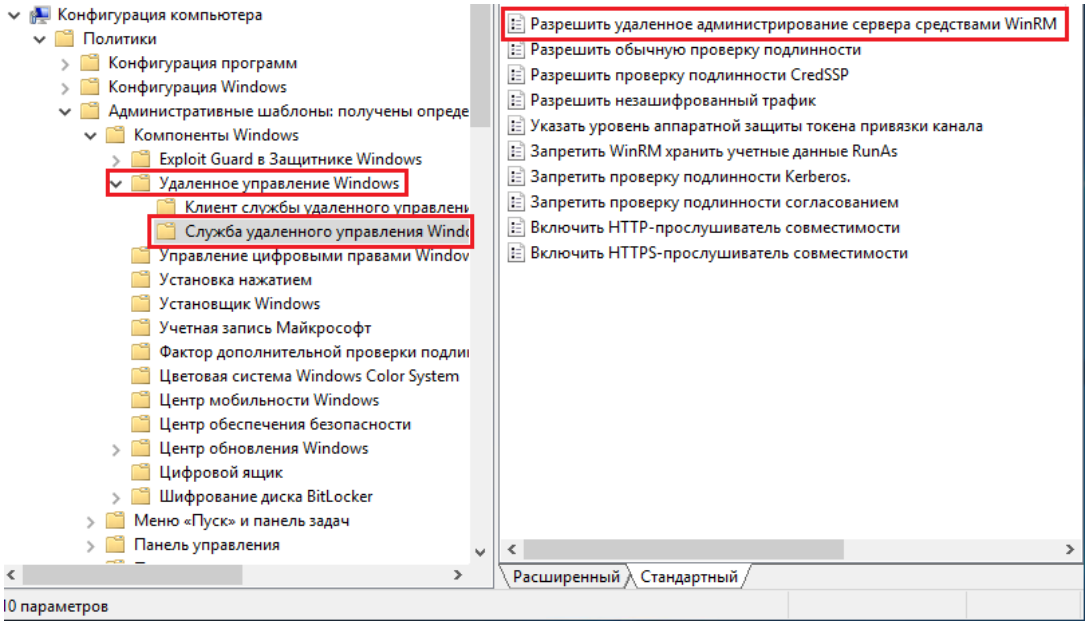


В разделе **Восстановление** укажите для трех параметров значение **Перезапуск службы**;



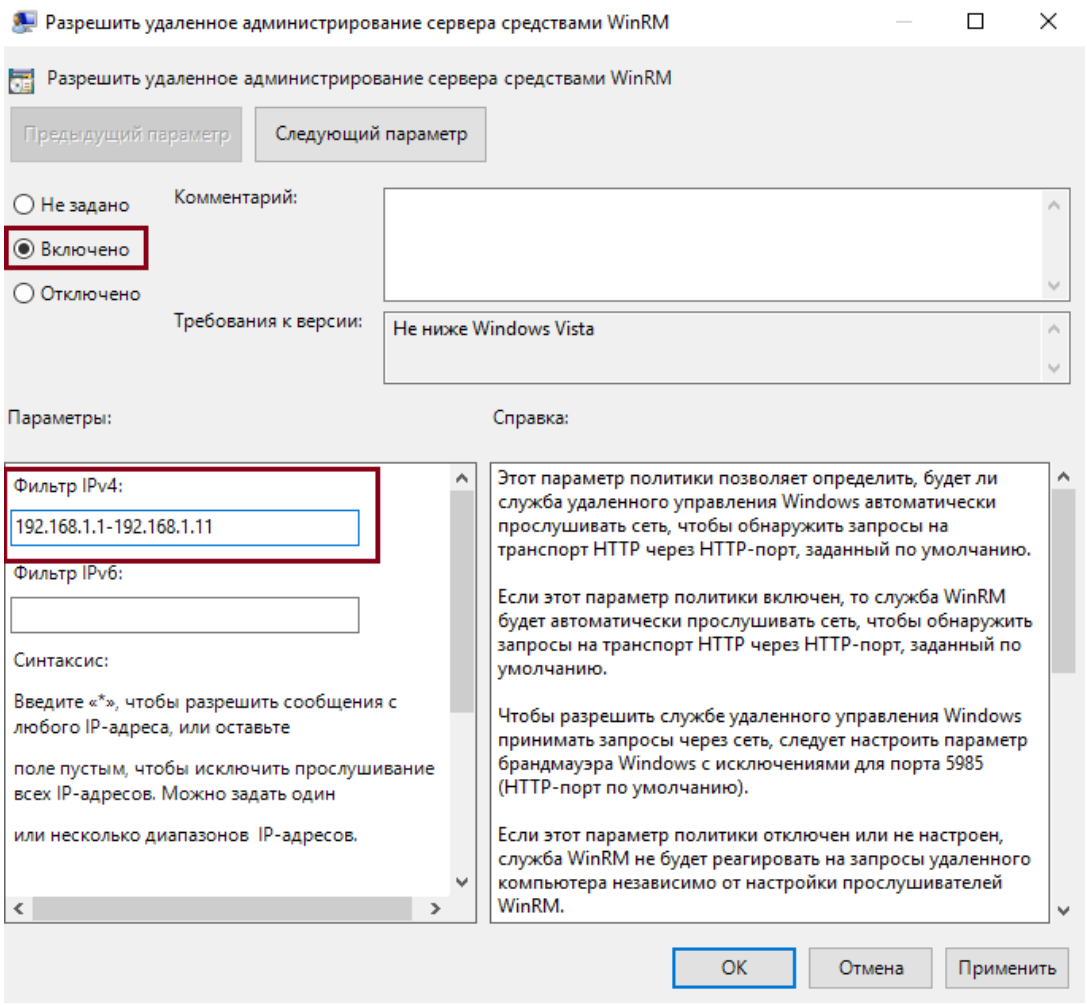
Шаг 5. Перейдите в **Конфигурация компьютера → Политики → Административные шаблоны... → Компоненты Windows → Удаленное**

управление Windows → Служба удаленного управления Windows → откройте **Разрешить удаленное администрирование сервера…**;

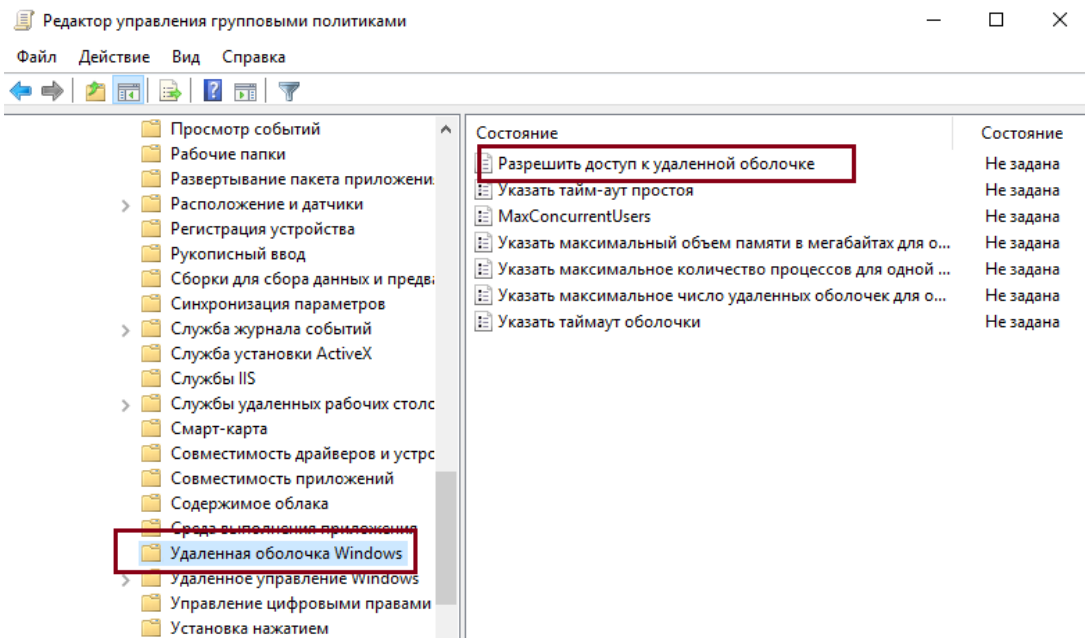


Укажите **Включено** → укажите в **Фильтр IPv4** IP-адреса:

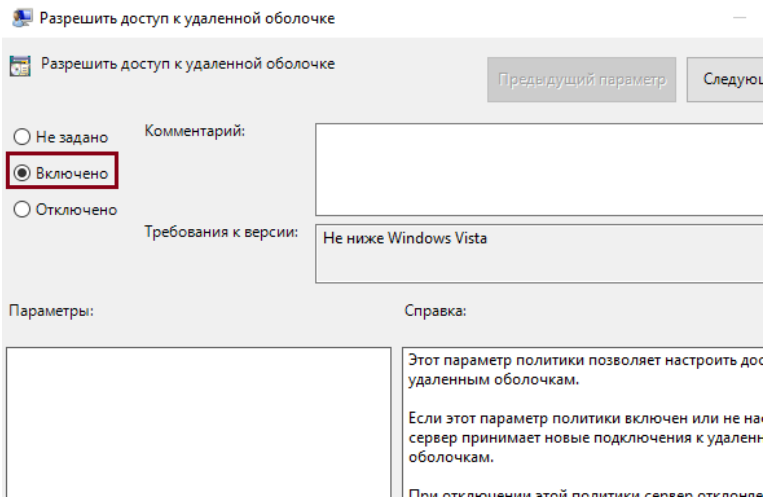
- **Для групповой политики для хоста службы сканирования:** ip-адрес хоста службы сканирования;
- **Для групповой политики для сканирумых узлов:** диапазон ip-адресов.



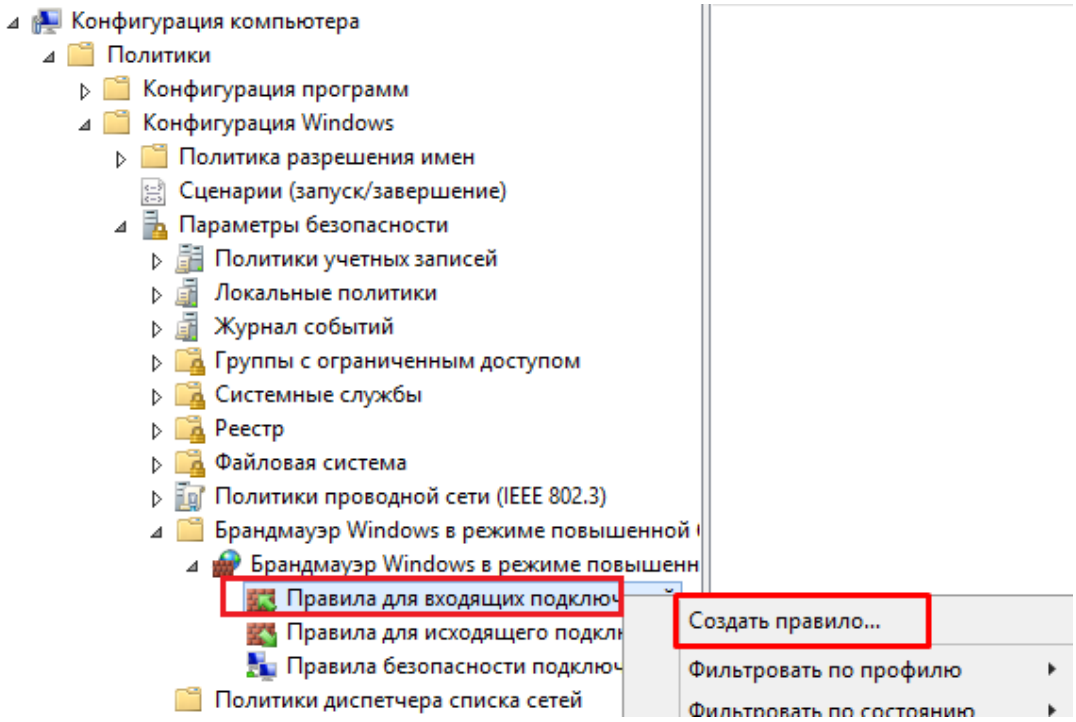
Шаг 6. Перейдите в **Компоненты Windows → Удаленная оболочка Windows** → откройте **Разрешить доступ к удаленной оболочке**;



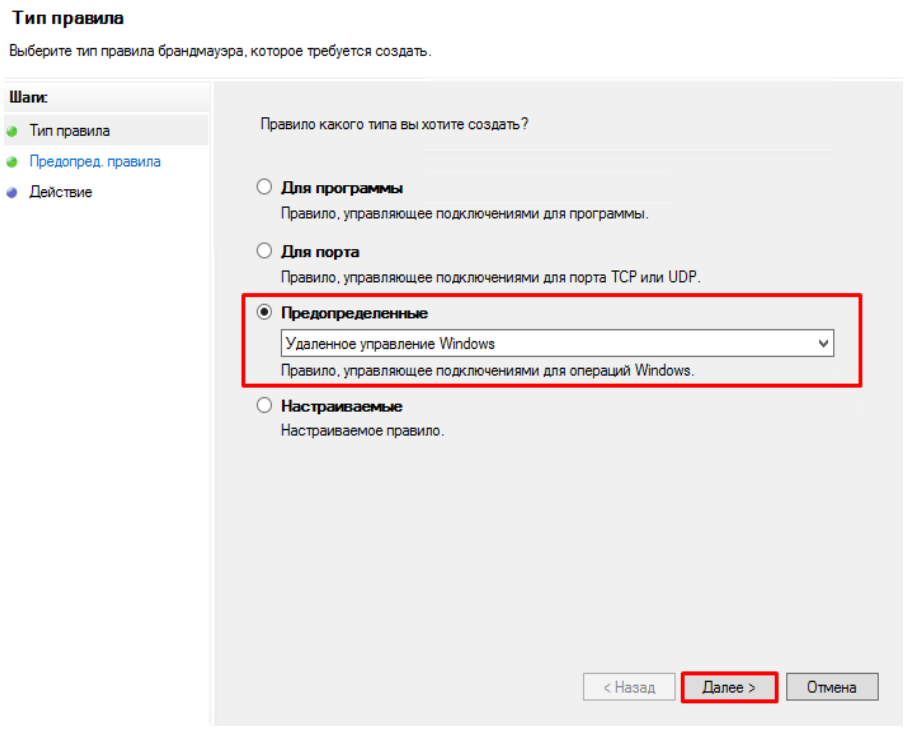
Укажите **Включено**;



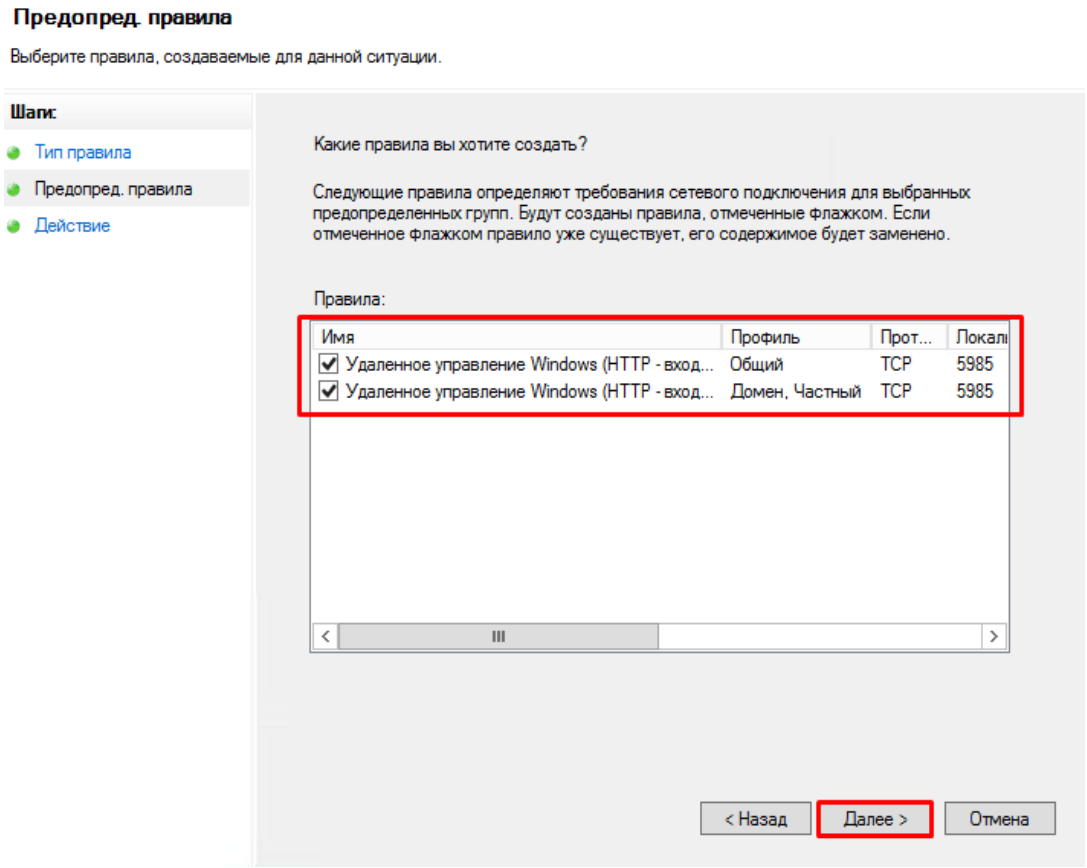
Шаг 7. Перейдите в **Конфигурация компьютера** → **Политики** → **Конфигурация Windows** → **Параметры безопасности** → **Монитор брандмауэра Защитника Windows** → ПКМ по **Правила для входящих подключений** → **Создать правило**;



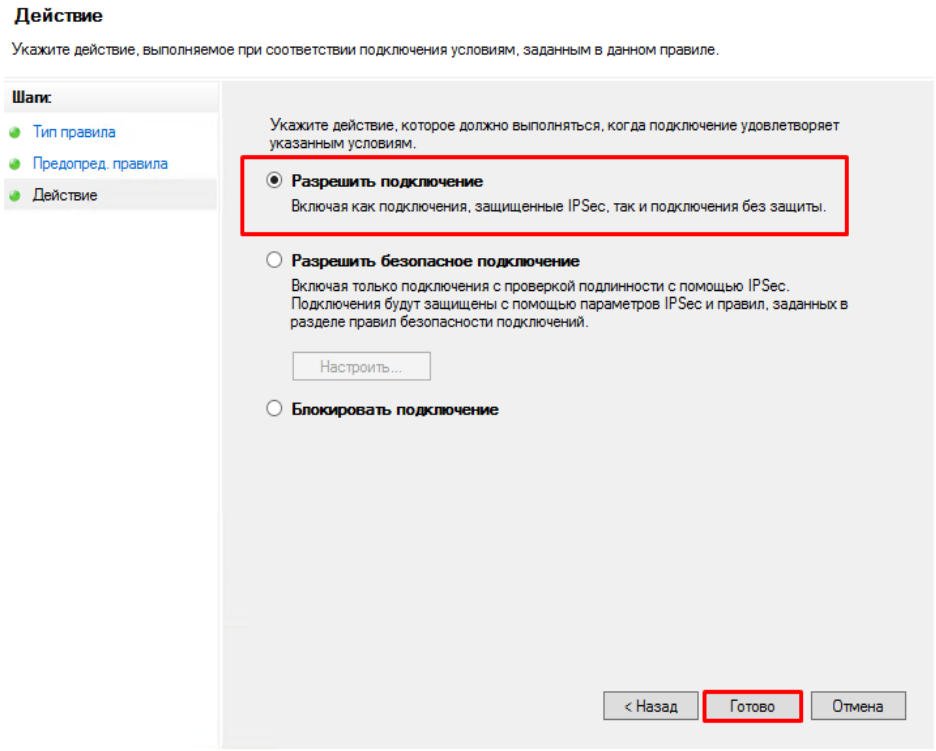
Шаг 8. Отметьте **Предопределенные** → выберите **Удаленное управление Windows** → **Далее**;



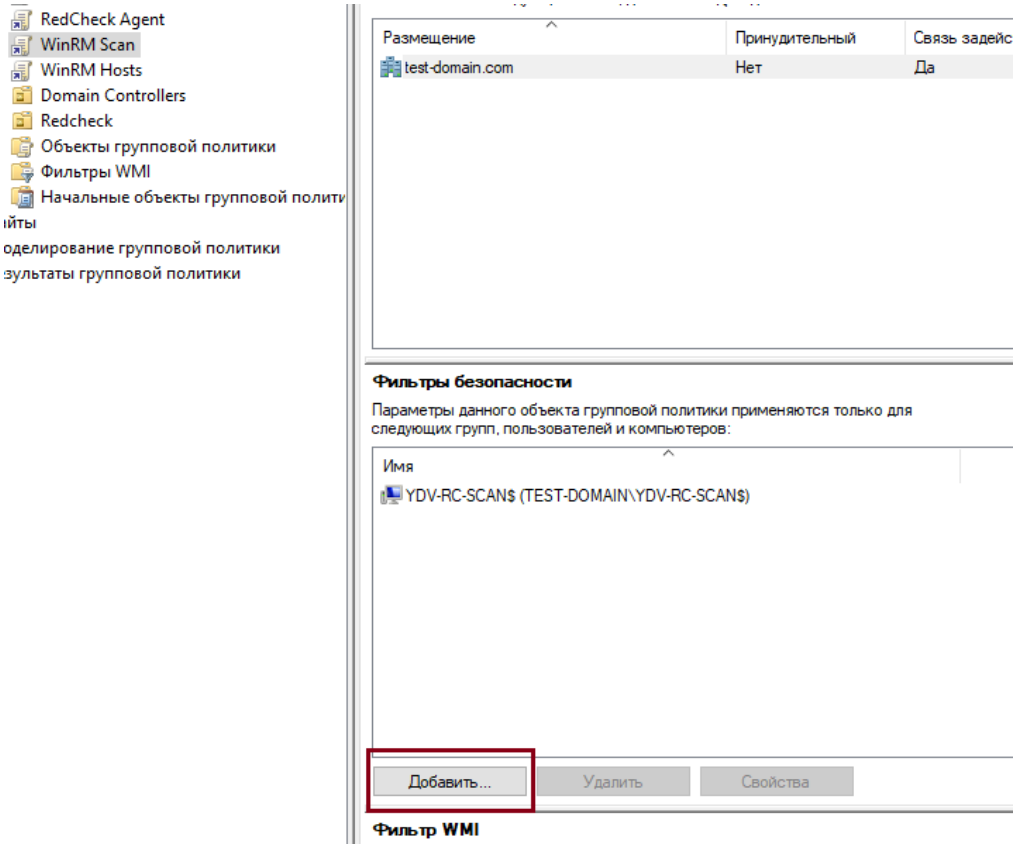
Отметьте два правила **Удаленное управление Windows...** → **Далее**;



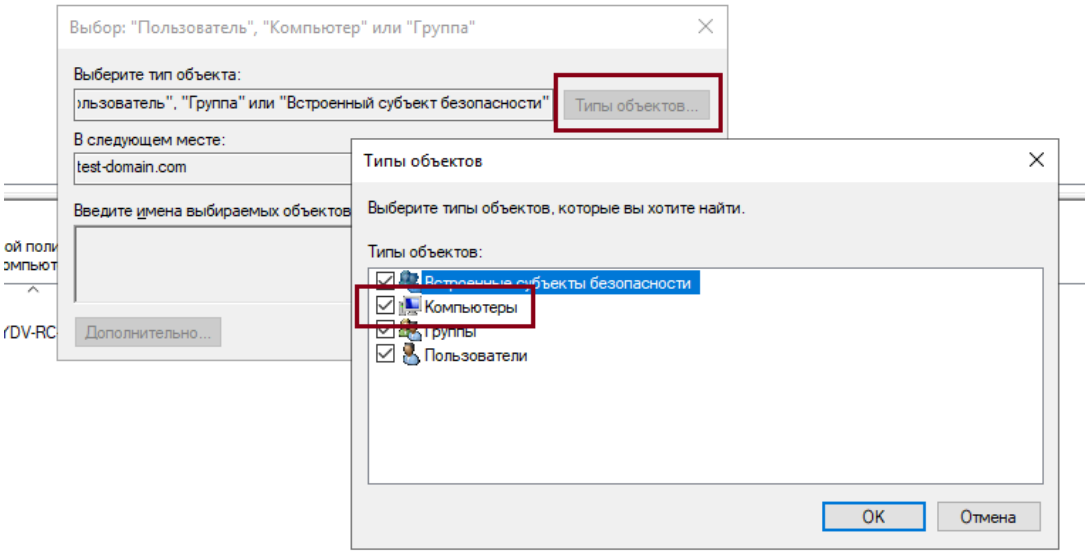
Укажите **Разрешить подключение** → **Готово**;



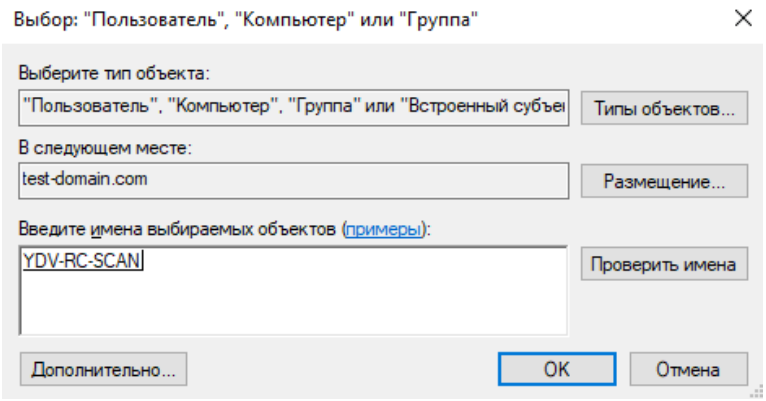
Шаг 9. Укажите каждой групповой политике хосты, для которых эти политики будут применяться. Для хоста службы сканирования удалите группу **Прошедшие проверку** → **Добавить**;



Нажмите **Типы объектов** → отметьте **Компьютеры**;



Укажите имя компьютера, на котором установлена служба сканирования → **OK**;

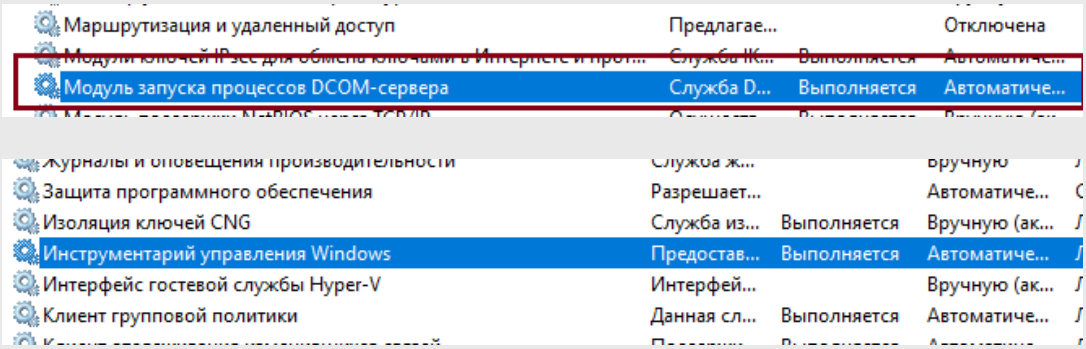


5.4.1.3 Транспорт WMI

Безагентскую технологию **Windows Management Instrumentation (WMI)** рекомендуется использовать только для выборочных проверок из-за больших нагрузок на сканируемую сеть.

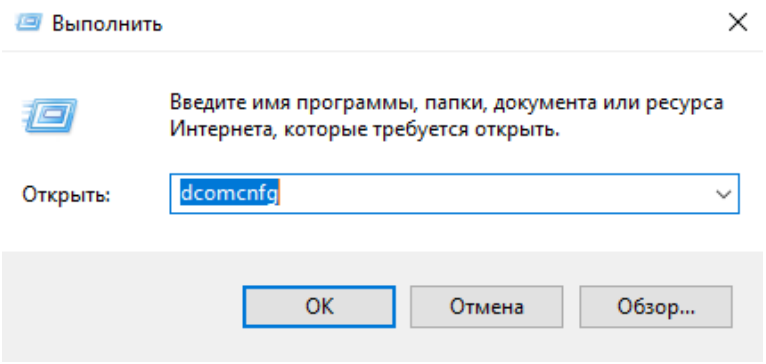
Для обеспечения сканирования данной технологией необходимо обеспечить подключение RedCheck к WMI сканируемого хоста, произвести настройки удаленного доступа и службы DCOM (при необходимости). Настройки могут быть произведены локально на узле или централизованно с помощью групповых политик Windows, а также другими средствами администрирования сети.

Убедитесь, что службы DCOM и WMI выполняются и имеют тип запуска **Автоматически**. По умолчанию служба DCOM включена.

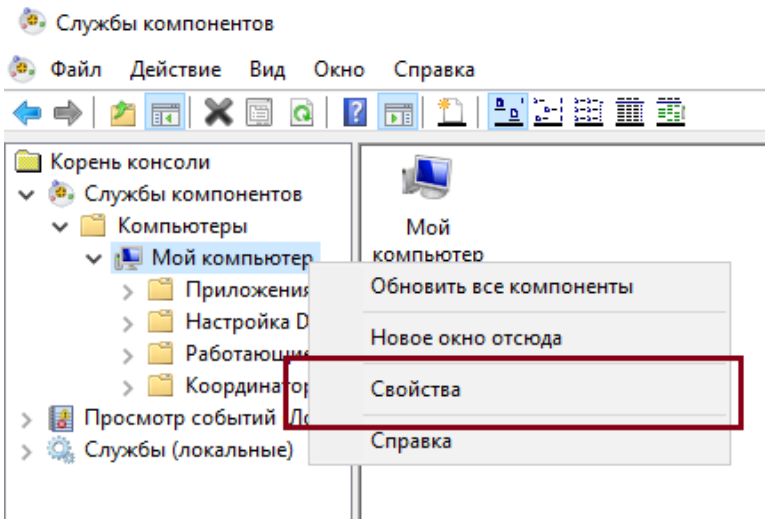


Локальная настройка службы DCOM на сканируемом хосте

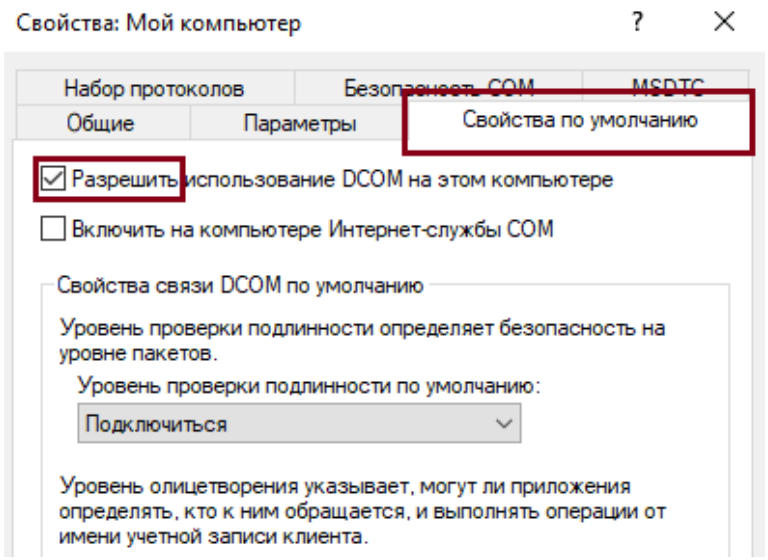
Шаг 1. Запустите **Службы компонентов** комбинацией **Win + R** → введите **dcomcnfg**;



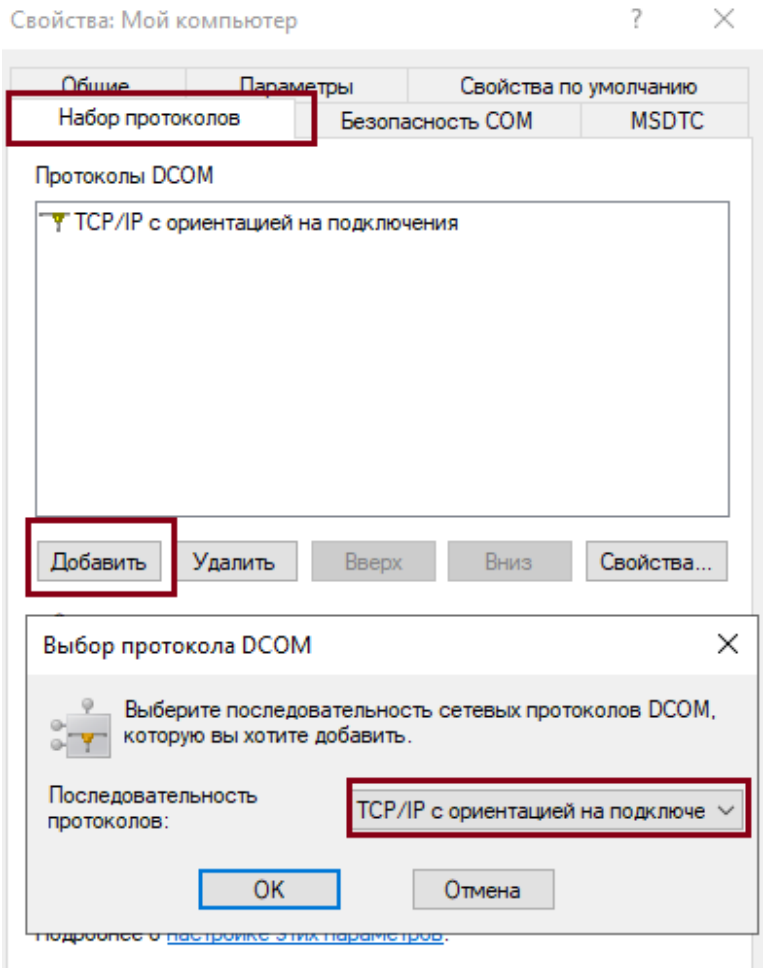
Шаг 2. Раскройте **Компьютеры** → ПКМ по **Мой компьютер** → **Свойства**;



Перейдите в **Свойства по умолчанию** → отметьте **Разрешить использование DCOM на этом компьютере**;

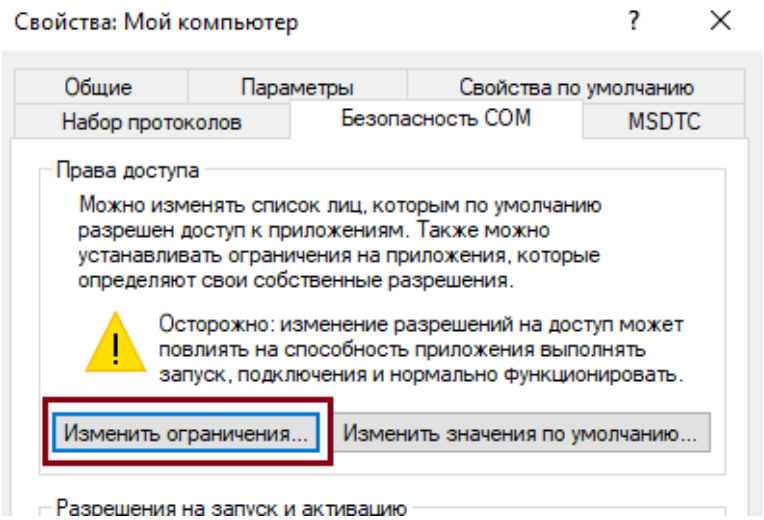


Перейдите в **Набор протоколов** → **Добавить** → выберите **TCP/IP с ориентацией на подключения** → **OK**.

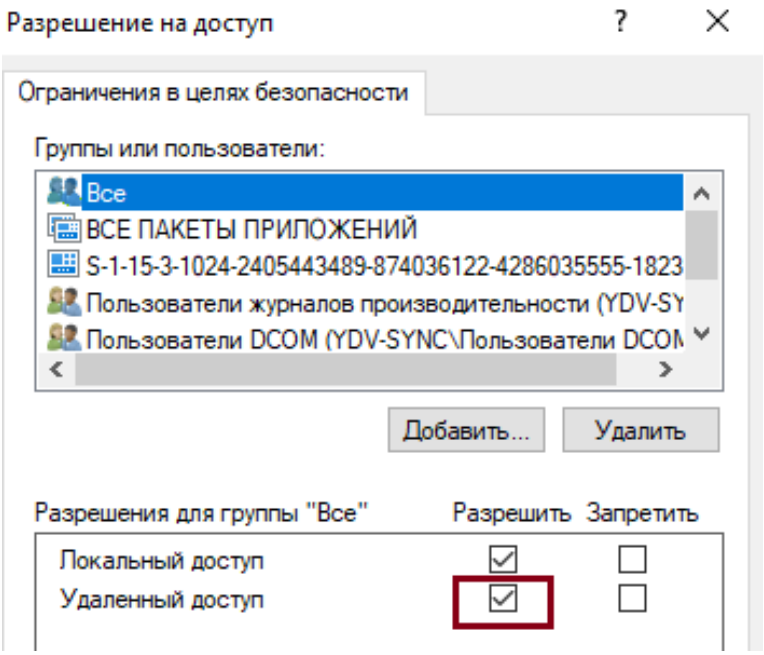


Настройка удалённого доступа для учётной записи, от имени которой производится сканирование

Шаг 3. Перейдите в **Безопасность COM** → **Изменить ограничения**;



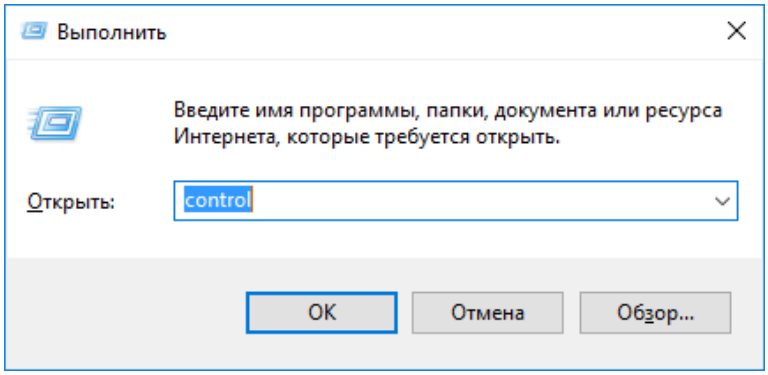
Предоставьте группе **Все** разрешение **Удаленный доступ**;



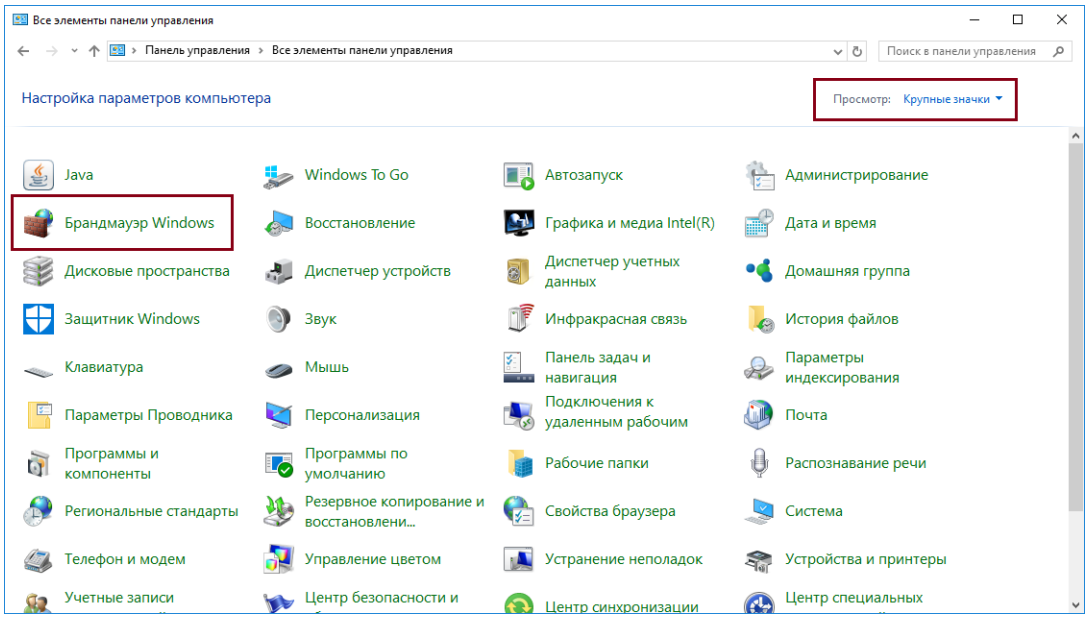
Шаг 4. Перезагрузите устройство.

Разрешение WMI (локальная настройка)

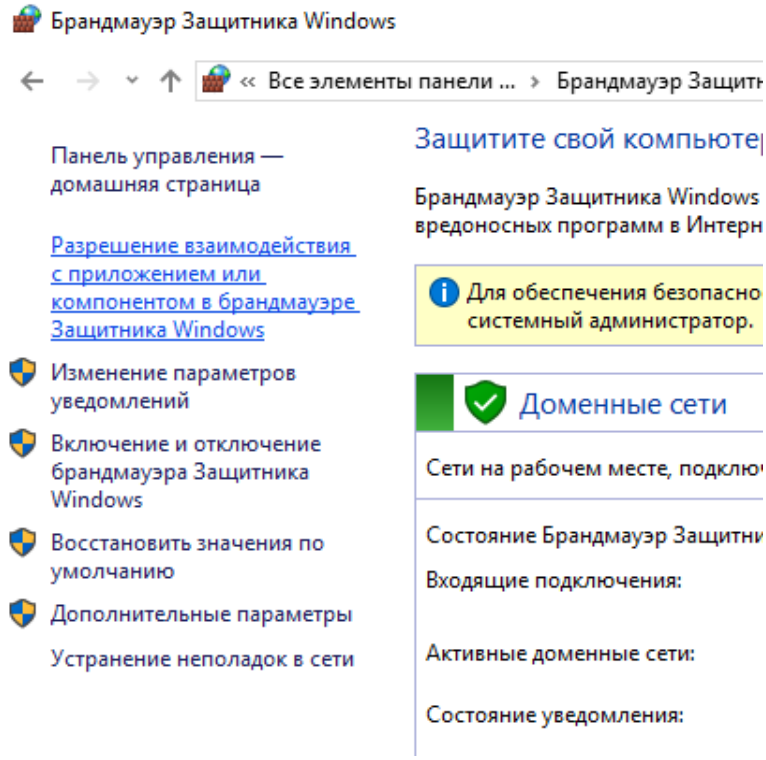
Шаг 1. Нажмите **Win + R** → введите **control**;



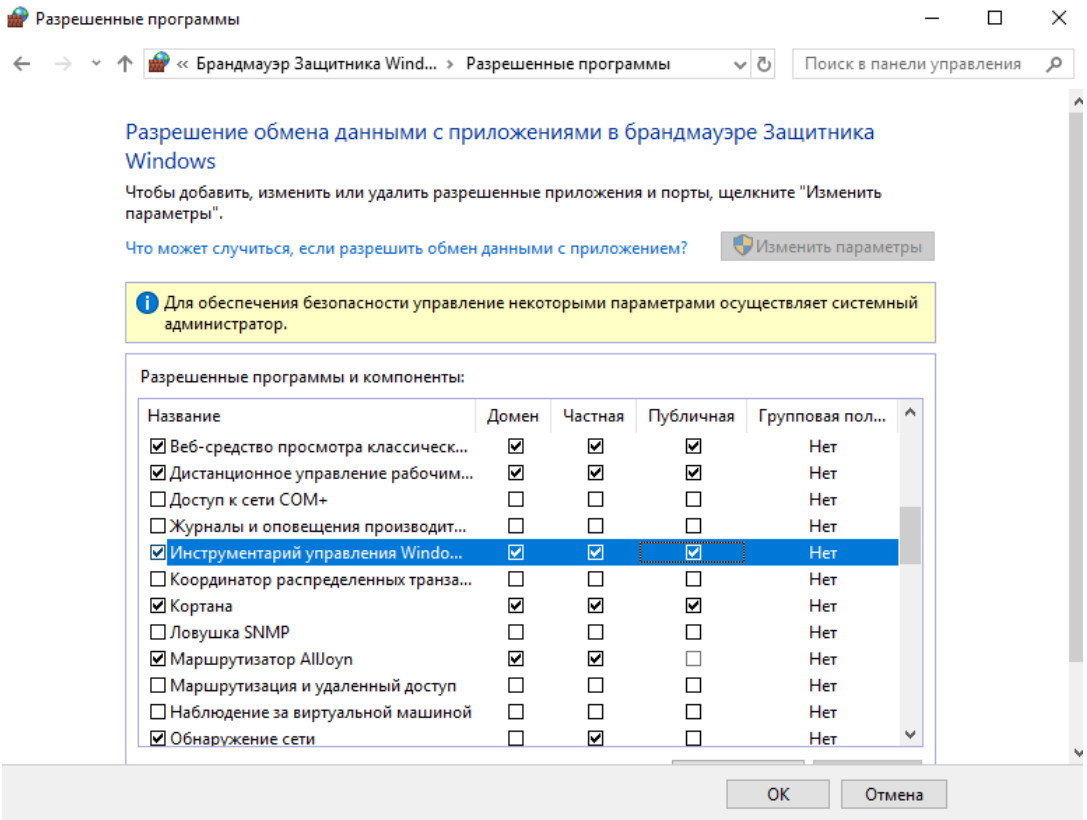
Измените способ отображение на **Крупные значки → Брандмауэр Защитника Window**;



Шаг 2. Выберите **Разрешение взаимодействия с приложением или компонентом в брандмауэре Защитника Windows**;

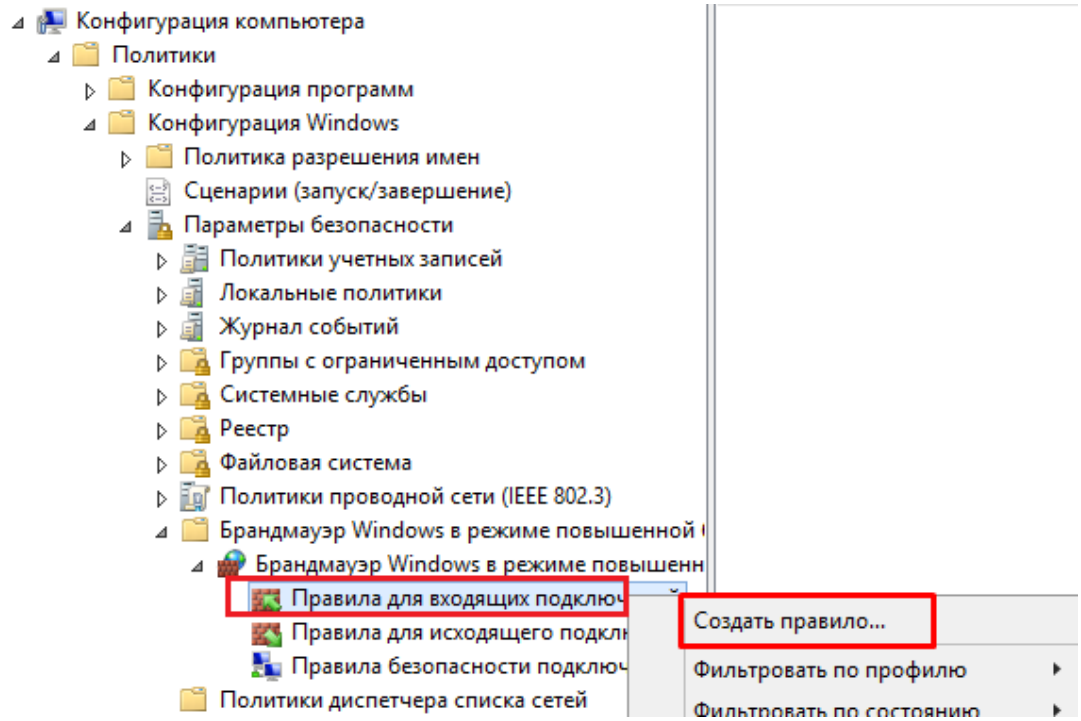


Шаг 3. Отметьте **Инструментарий управления Windows (WMI)** → выберите метод организации сети.

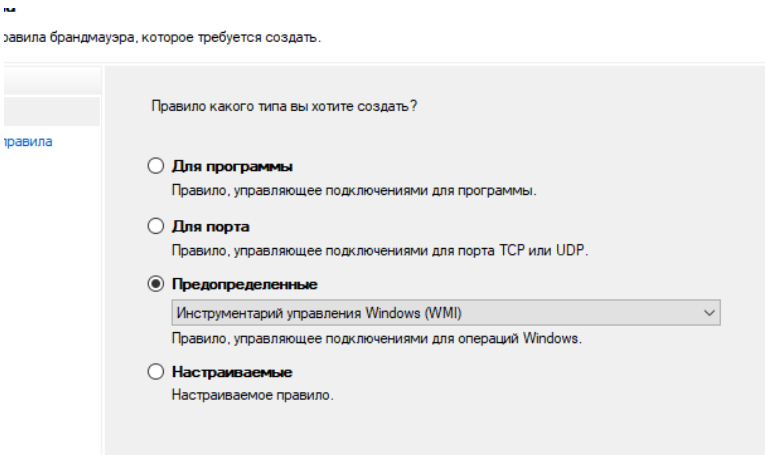


Разрешение WMI (через групповую политику)

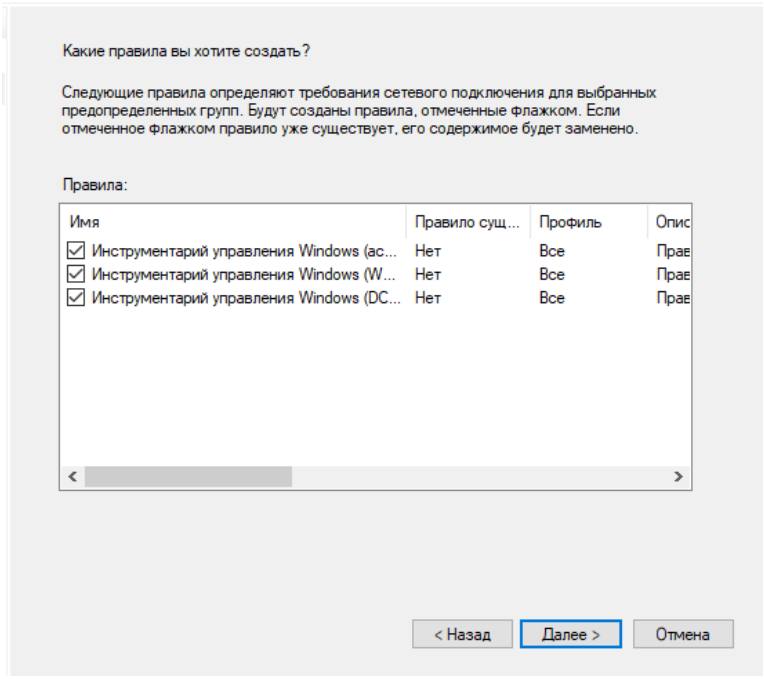
Шаг 1. Перейдите в **Конфигурация компьютера** → **Политики** → **Конфигурация Windows** → **Параметры безопасности** → **Монитор брандмауэра Защитника Windows** → ПКМ по **Правила для входящих подключений** → **Создать правило**;



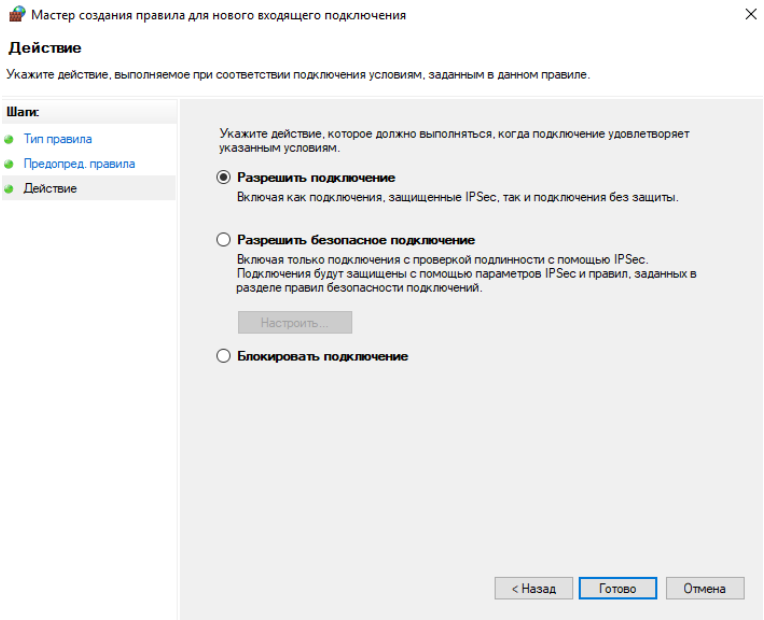
Шаг 2. Укажите **Предопределенные** → выберите **Инструментарий управления Windows (WMI)** → **Далее**;



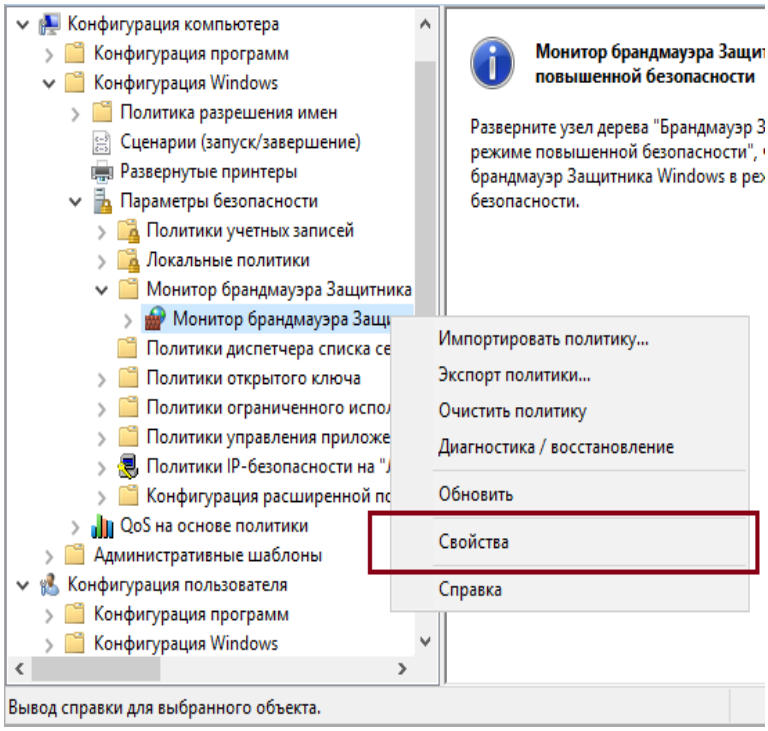
Отметьте три поля **Инструментарий управления Windows** → **Далее**;



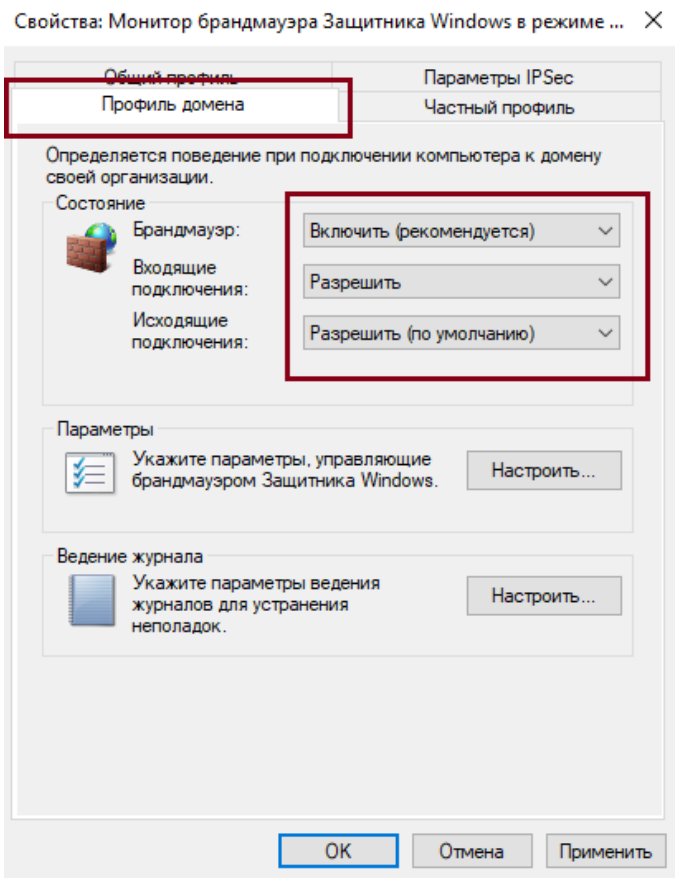
Укажите **Разрешить подключение** → **Готово**;



Шаг 3. ПМК по **Монитор брандмауэра Защитника Windows → Свойства**;



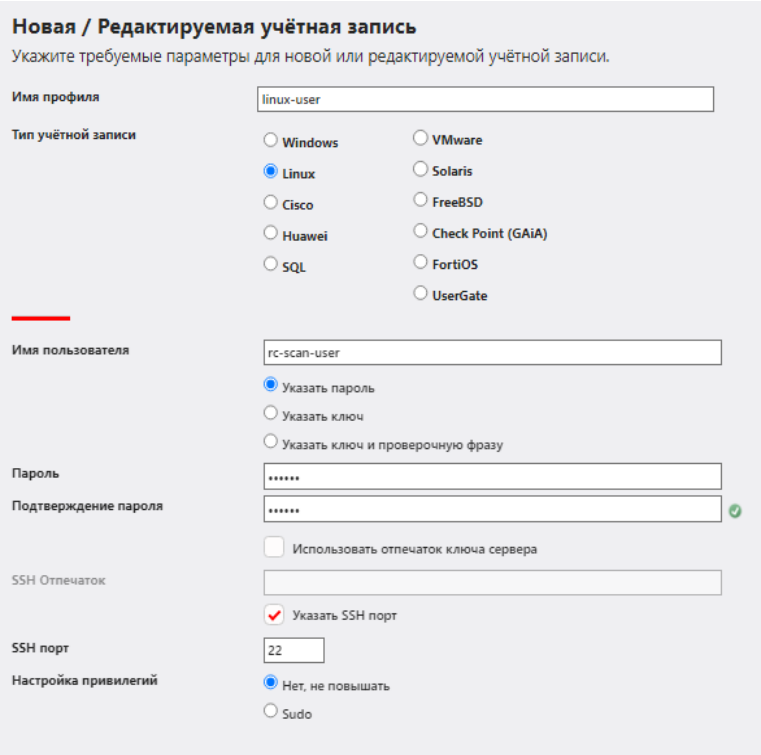
В **Профиль домена** включите брандмауэр и разрешите входящие и исходящие подключения.



5.4.2 Сканирование Linux-систем

При сканировании Linux-систем (сканирование осуществляется по безагентской технологии) в качестве транспорта используется SSH-протокол не ниже версии 2.0 с включенным модулем поддержки протокола SFTP. Для сканирования удаленного хоста требуется создать учётную запись с возможностью подключения к удалённой системе по протоколу SSH. Осуществить проверку подключения можно с помощью любого удобного SSH-клиента.

В RedCheck для сканирования удаленного хоста требуется создать учётную запись, **Тип учетной записи** – **Linux**.



Для сканирования удалённой системы могут использоваться следующие типы учётных записей:

- 5.4.2.1 Учетная запись суперпользователя (root)
- 5.4.2.2 Учетная записи привилегированного пользователя (sudo)
- 5.4.2.3 Учётная запись непривилегированного пользователя

Установка openssh-server и sftp

Перед настройкой учетных записей необходимо установить пакет openssh-server, если его нет в системе по умолчанию.

Шаг 1. Выполните команду:

```
Bash (Unix Shell)

apt-get -y install openssh-server
```

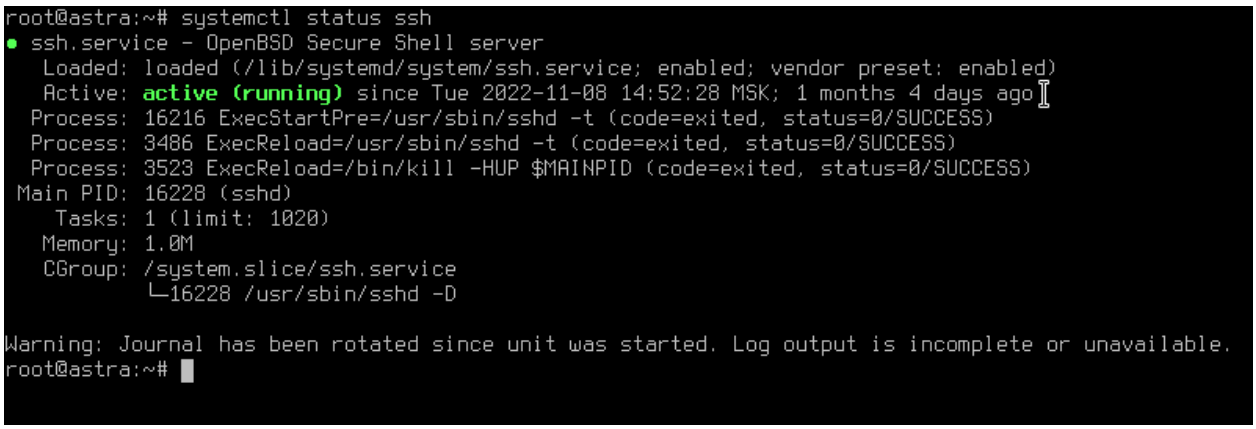
Шаг 2. Запустите сервис:

```
Bash (Unix Shell)

/etc/init.d/ssh start
```

или

```
Bash (Unix Shell)

/etc/init.d/sshd start
```

Для проверки статуса работы сервиса введите команду: **systemctl status sshd** (или **systemctl status ssh**).



Шаг 3. Протокол sftp включается добавлением специальной строки в файл **/etc/ssh/sshd_config** (или **/etc/openssh/sshd_config**). Проверьте наличие необходимой строки командой:

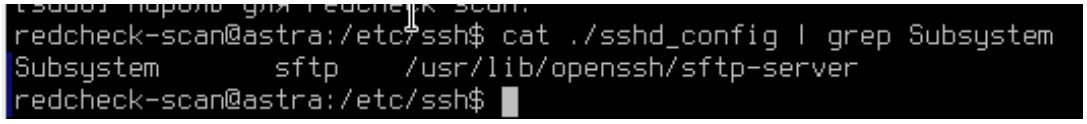
Bash (Unix Shell)

```
cat /etc/ssh/sshd_config | grep Subsystem
```

или

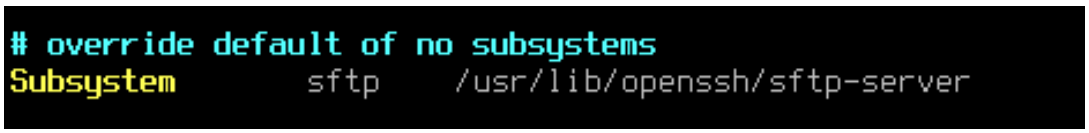
Bash (Unix Shell)

```
cat /etc/openssh/sshd_config | grep Subsystem
```



Если результат команды оказался пустым, откройте файл любым текстовым редактором и добавьте следующую строку:

Subsystem sftp /usr/lib/openssh/sftp-server



Необходимо отключить SELinux для корректного сканирования с использованием привилегированной учетной записи (sudo).

Требования к ключам шифрования:

- Минимальная длина ключа RSA - 1024;
- Минимальная длина ключа DiffieHellman - 1024;

Поддерживаемые алгоритмы обмена ключами:

- Diffie-Hellman (Oakley Group 2) with SHA-1
- Diffie-Hellman (Oakley Group 14) with SHA-1
- Diffie-Hellman (Group Exchange) with SHA-1
- Diffie-Hellman (Group Exchange) with SHA-256
- Diffie-Hellman (Oakley Group 14) with SHA-256
- Diffie-Hellman (Oakley Group 15 or 16) with SHA-512

Поддерживаемые алгоритмы шифрования:

- aes256-gcm@openssh.com
- aes128-gcm@openssh.com
- chacha20-poly1305@openssh.com
- aes256-ctr
- aes192-ctr
- aes128-ctr
- aes256-cbc
- aes192-cbc
- aes128-cbc
- 3des-ctr
- 3des-cbc
- twofish256-ctr
- twofish192-ctr
- twofish128-ctr
- twofish256-cbc
- twofish192-cbc
- twofish128-cbc
- twofish-cbc

Поддерживаемые алгоритмы имитовставки:

- MD5
- SHA1
- SHA256
- SHA512

Поддерживаемые методы аутентификации:

- Password
- KeyboardInteractive
- PublicKey

Поддерживаемые форматы закрытого ключа:

- PKCS #8 (RFC 5208)
- PuTTY .ppk
- OpenSSH/OpenSSL (SSLeay) for RSA/DSA
- New OpenSSH for EcDSA

Поддерживаемые алгоритмы открытого ключа и ключа хоста:

- RSA
- DSS

- ECDsaNistP256
- ECDsaNistP384
- ECDsaNistP521

Список используемых команд при сканировании динамичен и зависит от конфигурации конкретного хоста.

5.4.2.1 Учетная запись суперпользователя (root)

Данный тип учётной записи используется, чтобы получить все доступные данные и провести глубокий анализ параметров безопасности удалённой системы, и/или в случаях, когда невозможно использовать другие типы учётных записей.

По умолчанию в Linux-системах учётная запись суперпользователя имеет имя root.

RedCheck не накладывает ограничений на использование в качестве учетной записи суперпользователя root. Допустимо использовать любую другую учётную запись суперпользователя с отличным от root именем, если таковые существуют на удалённой системе.

По умолчанию на некоторых Linux-системах учетная запись суперпользователя root может быть неактивна. Чтобы активировать учетную запись суперпользователя root, выполните команду смены пароля:

Bash (Unix Shell)

```
passwd root
```

На некоторых Linux-системах для учетной записи суперпользователя root запрещен удаленный вход по протоколу SSH. Чтобы разрешить учетной записи суперпользователя root выполнять вход по протоколу SSH, выполните настройку SSH-сервера:

Шаг 1. Откройте текстовым редактором файл **/etc/ssh/sshd_config** или **/etc/openssh/sshd_config**

Шаг 2. Добавьте строку

Code

```
PermitRootLogin yes
```

Шаг 3. Перезапустите сервис **ssh** командой:

Bash (Unix Shell)

```
/etc/init.d/ssh restart
```

или

Bash (Unix Shell)

```
/etc/init.d/sshd restart
```

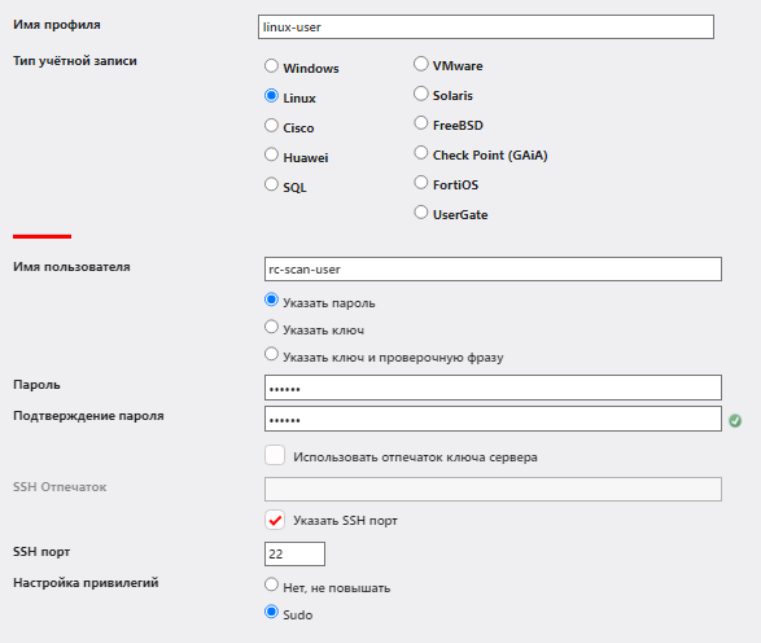
Конфигурационный файл SSH-сервера уже может содержать директиву **PermitRootLogin**. В таком случае измените значение директивы на **yes** с помощью текстового редактора.

Проверьте, что порт 22 открыт для входящих подключений.

5.4.2.2 Учетная записи привилегированного пользователя (sudo)

Рекомендуется использовать учетную запись суперпользователя (root) вместо повышения прав с использованием sudo. В противном случае возможны проблемы с производительностью при сканировании.

Для сканирования удалённой системы с помощью данного типа учётной записи у пользователя требуется наличие прав для выполнения sudo на удалённой системе. При создании учетной записи RedCheck необходимо указать **Sudo** для параметра **Настройка привилегий**.



По умолчанию на большинстве Linux-систем уже установлена программа sudo. Для проверки наличия программы sudo на удалённой системе выполните команду: **sudo –V**
Если программа sudo отсутствует на удалённой машине, необходимо выполнить её установку или воспользоваться другими типами учётных записей.

Шаг 1. Создайте учётную запись привилегированного пользователя (в примере ниже указано имя rc-scan-user) на удалённой системе:

Bash (Unix Shell)

```
adduser rc-scan-user
```

Шаг 2. Задайте пароль для созданной учётной записи пользователя:

Bash (Unix Shell)

```
passwd rc-scan-user
```

Шаг 3. Наделите пользователя правами для выполнения sudo, выполнив команду:

Bash (Unix Shell)

```
usermod -aG sudo rc-scan-user
```

Или отредактируйте конфигурацию sudo:

Код

```
echo "rc-scan-user ALL=(root)NOPASSWD:ALL" >> /etc/sudoers
```

При использовании команды **usermod** для учетной записи будет необходимо дополнительно указать пароль для sudo в соответствующем поле в Менеджере учетных записей.
При редактировании конфигурации sudo указывать дополнительные пароли для учетной записи не нужно.

5.4.2.3 Учётная запись непривилегированного пользователя

Рекомендуется использовать учетную запись суперпользователя (root) вместо повышения прав с использованием sudo. В противном случае возможны проблемы с производительностью при сканировании.

Данный тип учётной записи предназначен для получения данных, не требующих для своего доступа повышения прав, и не может применяться для полной оценки защищенности удалённой системы.

Шаг 1. Создайте учётную запись непривилегированного пользователя (в примере ниже указано имя rc-scan-user) на удалённой системе:

Bash (Unix Shell)

```
adduser rc-scan-user
```

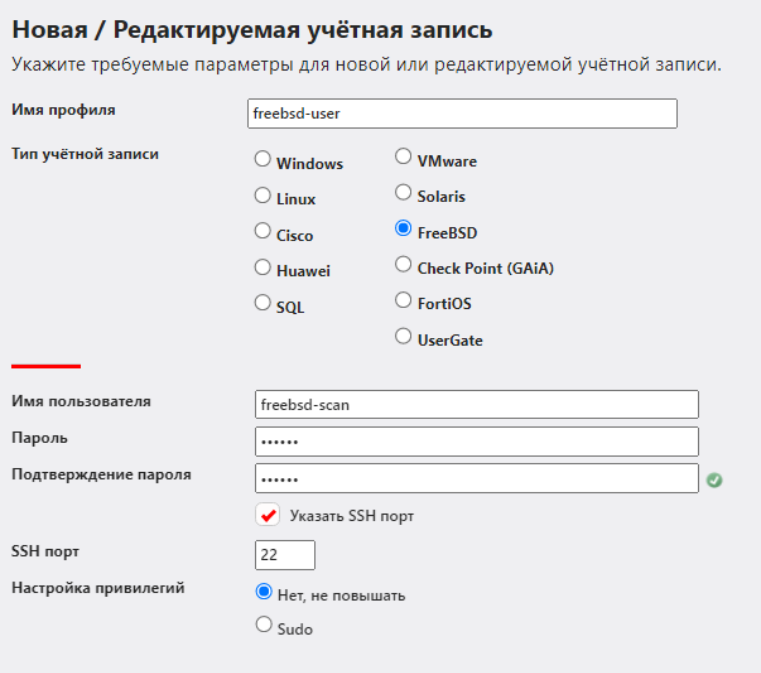
Шаг 2. Задайте пароль для созданной учётной записи пользователя:

Bash (Unix Shell)

```
passwd rc-scan-user
```

5.4.3 Сканирование FreeBSD

Для сканирования удалённого хоста требуется создать учётную запись, **Тип** – **FreeBSD**.



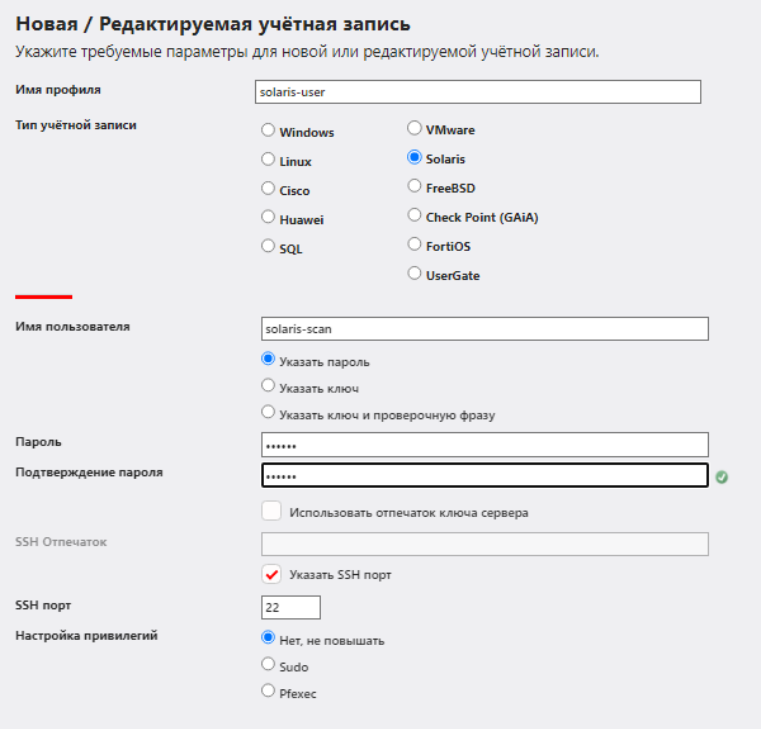
Для сканирования FreeBSD (сканирование осуществляется по безагентской технологии) в качестве транспорта для сканирования используется SSH-протокол (по умолчанию используется порт 22) с включенным модулем поддержки протокола SFTP.

Перечень выполняемых команд в момент сканирования:

- sudo
- echo
- bind
- printf
- grep
- test
- file
- mktemp
- rm
- basename
- dirname
- which
- command
- cat
- find
- getfacl
- stat
- uname
- chmod
- base64
- openssl
- ls
- pkg

5.4.4 Сканирование Solaris

Для сканирования удалённого хоста требуется создать учётную запись, **Тип** – **Solaris.**

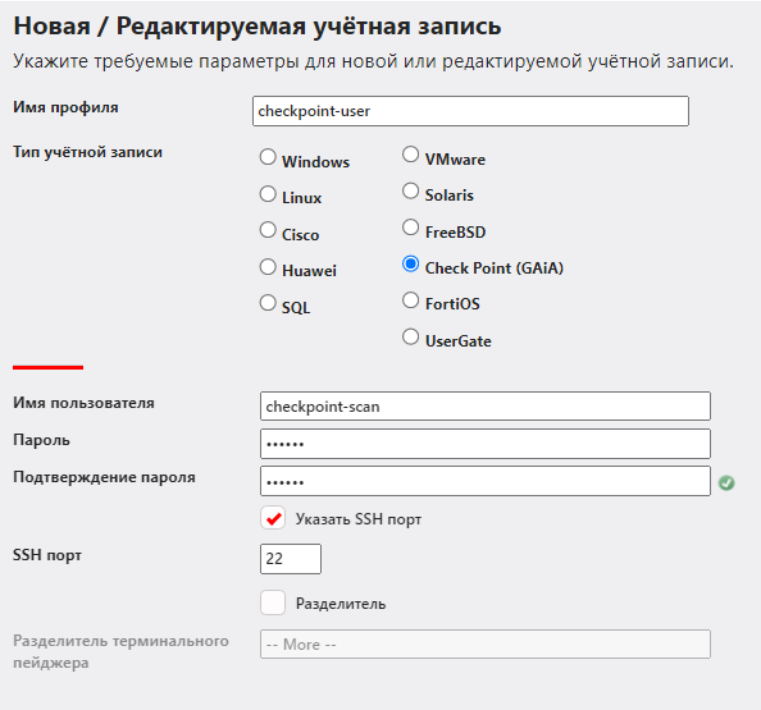


Для сканирования удалённой системы в качестве основного транспорта используется протокол SSH. Убедитесь, что SSH-сервер установлен и настроен, а выбранная учётная запись пользователя имеет возможность подключения к удалённой системе по протоколу SSH. Осуществить проверку подключения можно с помощью любого удобного SSH-клиента.

Для сканирования удалённой системы, допускается использовать существующую учётную запись пользователя Solaris (привилегированного - sudo и pfexec; непривилегированного), или создать отдельную.

5.4.5 Сканирование Check Point

Для сканирования удалённого хоста требуется создать учетную запись, **Тип** – **Check Point**.



Для сканирования Check Point (сканирование осуществляется по безагентской технологии) в качестве транспорта для сканирования используется SSH-протокол (по умолчанию используется порт 22).

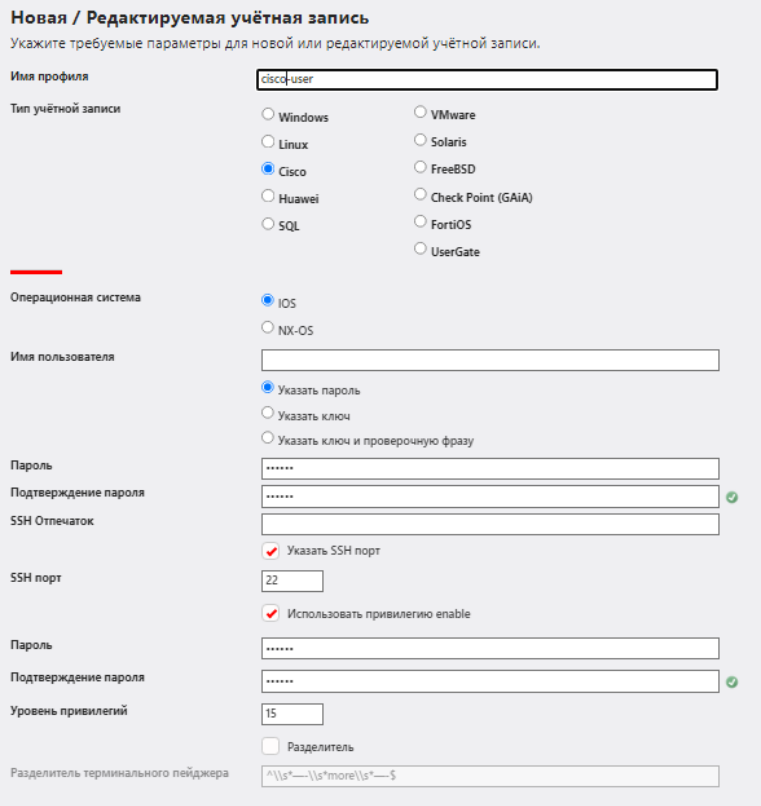
Перечень выполняемых команд в момент сканирования:

- show version all
- show software-version
- show interfaces
- show asset all
- cpinfo -y all
- cpstat os

5.4.6 Сканирование Cisco IOS

Для сканирования Cisco IOS (сканирование осуществляется по безагентской технологии) в качестве транспорта для сканирования используется SSH-протокол (по умолчанию используется порт 22). Перед проведением сканирования необходимо убедиться, что служба SSH включена и настроена, а выбранная учётная запись пользователя имеет возможность подключения к удалённой системе по протоколу SSH. Осуществить проверку подключения можно с помощью любого удобного SSH-клиента.

Для сканирования удалённого хоста требуется создать учётную запись, **Тип** – **Cisco**.



Для сканирования должна использоваться учётная запись пользователя с возможностью входа в привилегированный режим с использованием команды **enable**

Требования к ключам и алгоритмам шифрования:

- Минимальная длина ключа RSA - 1024
- Минимальная длина ключа DiffieHellman - 1024

Поддерживаемые алгоритмы обмена ключами:

- DiffieHellmanGroup1SHA1
- DiffieHellmanGroup14SHA1
- DiffieHellmanGroupExchangeSHA1
- DiffieHellmanGroupExchangeSHA256
- ECDiffieHellmanNistP256
- ECDiffieHellmanNistP384
- ECDiffieHellmanNistP521
- Curve25519
- DiffieHellmanOakleyGroupSHA256
- DiffieHellmanOakleyGroupSHA512

Поддерживаемые алгоритмы шифрования:

- RC4
- TripleDES
- AES
- Blowfish
- Twofish

Поддерживаемые алгоритмы ключа хоста:

- RSA
- DSS
- ED25519
- ECDsaNistP256
- ECDsaNistP384
- ECDsaNistP521

Поддерживаемые алгоритмы имитовставки:

- MD5
- SHA1
- SHA256
- SHA512

Поддерживаемые методы аутентификации:

- Password
- KeyboardInteractive
- PublicKey

Поддерживаемые форматы закрытого ключа:

- PKCS #8 (RFC 5208)
- PuTTY .ppk
- OpenSSH/OpenSSL (SSLeay) for RSA/DSA
- New OpenSSH for EcDSA/Ed25519

Поддерживаемые алгоритмы открытого ключа:

- RSA
- DSS
- ED25519
- ECDsaNistP256
- ECDsaNistP384
- ECDsaNistP521

Для сканирования оборудования Cisco существует возможность использовать учётную запись без возможности перехода в привилегированный режим. Для реализации такого типа сканирования необходимо дополнительно настроить разрешающие правила для учётной записи.

Для такой учётной записи необходимо добавить разрешение на выполнение команд, указанных ниже:

- terminal length 0
- show
- show access-lists
- show arp
- show cdp
- show clock
- show file systems
- show interfaces
- show inventory
- show ip interface brief
- show ip ssh
- show privilege
- show snmp user
- show version
- more
- dir
- tclsh
- exit

Указанные ниже команды выполняются в привилегированном режиме:

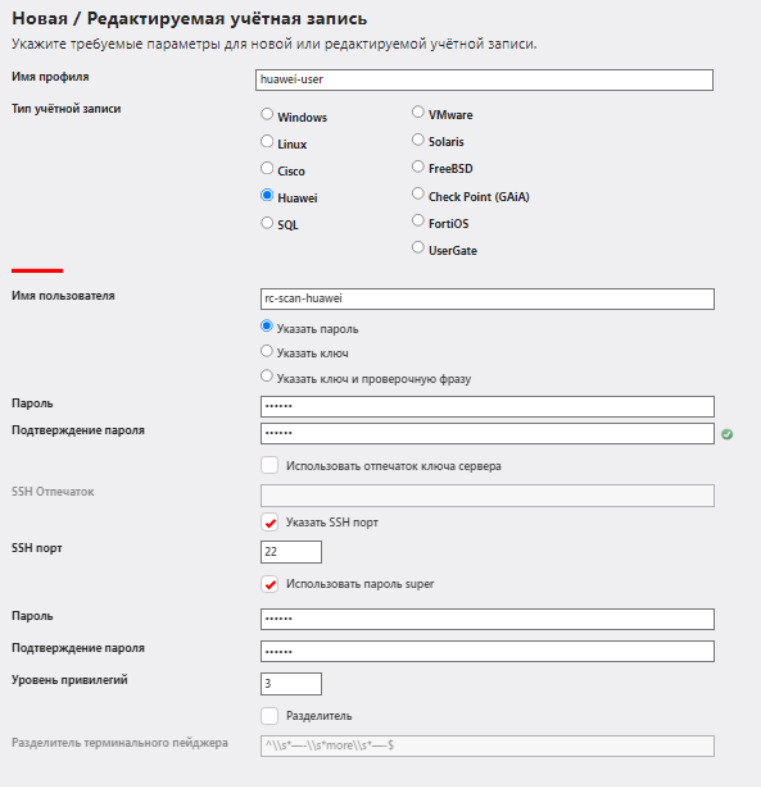
- show file information
- show running-config all
- show logging
- show snmp group
- show startup-config

5.4.7 Сканирование Huawei

Для сканирования Huawei VRP (сканирование осуществляется по безагентской технологии) в качестве транспорта для сканирования используется протокол SSH (по умолчанию используется порт 22). Для сканирования необходима учётная запись пользователя с возможностью перехода в привилегированный режим с вводом пароля «super» и указанием уровня доступа данного пользователя, используемого для конкретного типа оборудования (не ниже 3-го).

Перед проведением сканирования необходимо убедиться, что служба SSH включена и настроена, а выбранная учётная запись пользователя имеет возможность подключения к удалённой системе по протоколу SSH. Осуществить проверку подключения можно с помощью любого удобного SSH-клиента.

Для сканирования удаленного хоста требуется создать учётную запись, **Тип** – **Huawei**.



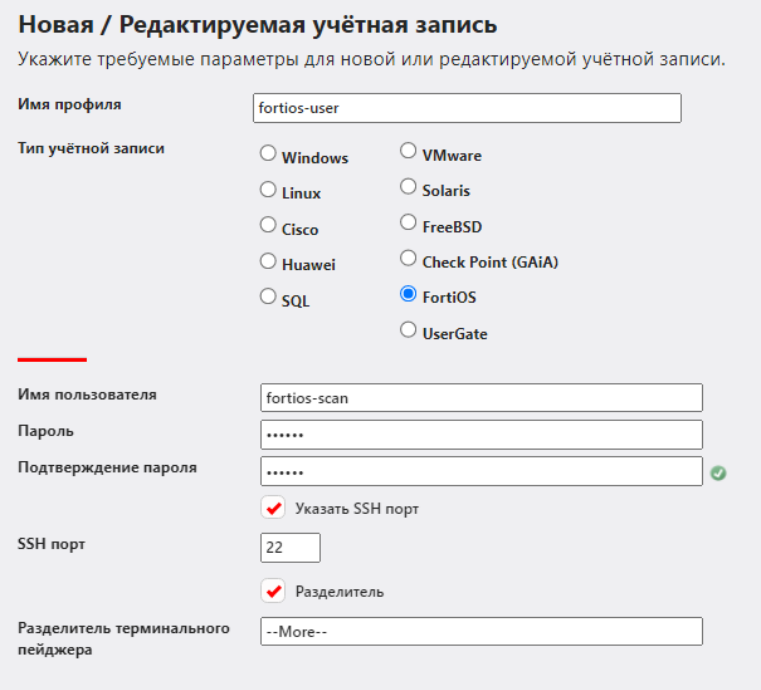
Аналогичные настройки учётных записей производятся и для сетевого оборудования «Булат».

Перечень команд, выполняемых при сканировании Huawei:

- screen-length 0 temporary
- display version
- display current-configuration
- display patch-information
- display authentication-scheme
- display aaa authentication-scheme
- display authorization-scheme
- display aaa authorization-scheme
- display accounting-scheme
- display aaa accounting-scheme
- display domain name
- display aaa domain
- display domain
- display elabel backplane
- display interface

5.4.8 Сканирование FortiOS

Для сканирования удаленного хоста требуется создать учётную запись, **Тип** – **FortiOS**.



При сканировании FortiOS (сканирование осуществляется по безагентской технологии) в качестве транспорта используется SSH-протокол не ниже версии 2.0 с включенным модулем поддержки протокола SFTP.

Требования к УЗ:

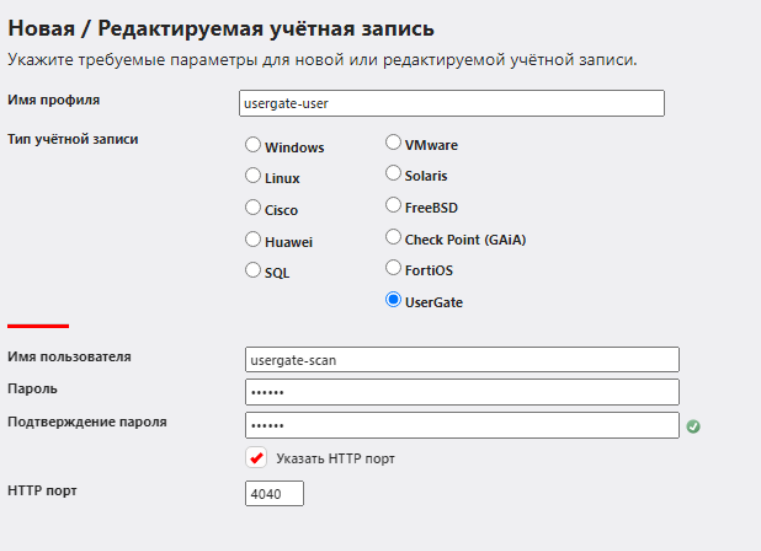
- Разделитель по умолчанию: **"--More-- "**, без пробела внутри, пробел в конце строки;

Настройки сканирования на стороне инфраструктуры:

- Создать профиль администрирования (System → Admin Profiles) с правами Read (Access Control);
- Создать УЗ администратора (System → Administrators);
- Привязать созданный профиль к УЗ;
- Отключить баннеры входа (pre-login-banner/post-login-banner).

5.4.9 Сканирование UserGate

Для сканирования удаленного хоста требуется создать учётную запись, **Тип** – **UserGate**.



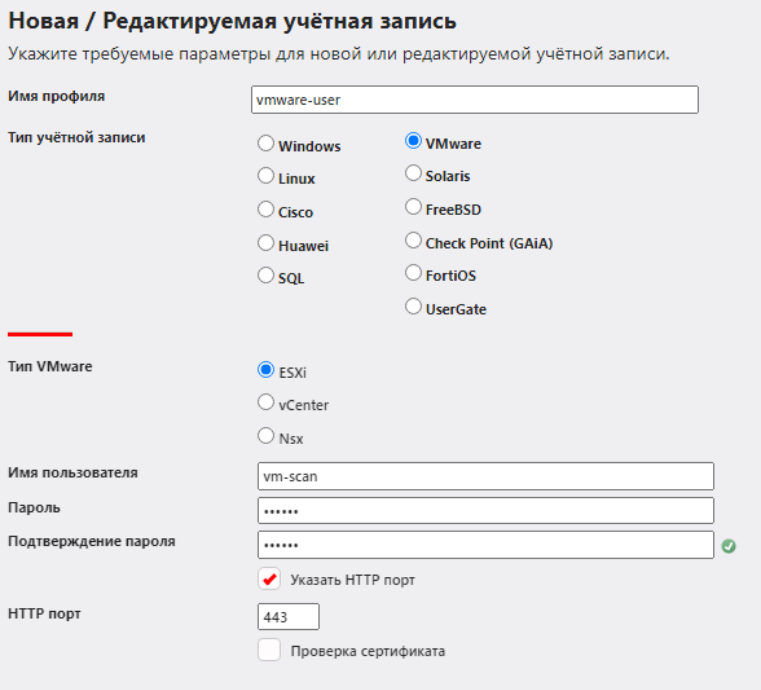
При сканировании UserGate (сканирование осуществляется по безагентской технологии) в качестве транспорта используется HTTP-протокол**,** номер порта 4040.

Настройки сканирования на стороне инфраструктуры

- Создать профиль администрирования (Настройки → UserGate → Администраторы → Профили администраторов);
- Указать для созданного профиля разрешения на чтение для всех объектов API (Настройки профиля → Разрешения для API);
- Создать УЗ администратора (Настройки → UserGate → Администраторы → Администраторы);
- Привязать созданный профиль к УЗ (Свойства администратора → Профиль администратора).

5.4.10 Сканирование VMware

Для сканирования удалённого хоста требуется создать учетную запись, **Тип** – **VMware**.



Поддерживаются все редакции, указанные в 1.8 Перечень поддерживаемых платформ, лицензии для которых активируют feature vSphere API.

При сканировании VMware ESXi Server и VMware vCenter Server (кроме задания типа **Фиксация**) в качестве транспорта используются протоколы SOAP+HTTPS. При сканировании VMware ESXi Server и VMware vCenter Server заданием типа **Фиксация** в качестве транспорта используется SSH-протокол не ниже версии 2.0 с включенным модулем поддержки протокола SFTP.

Используемая технология доступа к данным – VMware Infrastructure Management (VIM).

Общий перечень команд, выполняемых при сканировании VMware ESXi Server и vCenter Server:

- Login
- Logout
- RetrieveServiceContent
- ContinueRetrievePropertiesEx
- RetrievePropertiesEx
- CreateContainerView

- DestroyView
- HostImageConfigGetAcceptance
- HostImageConfigGetProfile
- QueryLockdownExceptions
- RetrieveHostAccessControlEntries

Команда, выполняемая при сканировании VMware ESXi Server:

- VimEsxCLIsoftwareviblist

Содержание

5.4.10.1 Настройка VMware ESXi Server

Для выполнения всех типов заданий RedCheck, кроме Фиксации, требуются:

- активированная лицензия на продукт с включенной в нее feature vSphere API;
- наличие учётной записи root;
- присутствие учётной записи пользователя, состоящей в группе Администраторы, а также добавленный в список исключений Lockdown Mode;
- редакция RedCheck Professional или Enterprise.

Для выполнения задания Фиксации, помимо обозначенных выше требований, необходимо:

- включенная служба SSH;
- включенная служба ESXi Shell;
- настроенные правила брандмауэра для доступа к SSH серверу;
- наличие параметра **PermitRootLogin yes** в настройках SSH сервера;
- наличие параметра **MaxSession 10** в настройках SSH сервера;

Для сканирования VMware ESXi Server заданиями типа **Аудит обновлений**, **Аудит уязвимостей**, **Аудит конфигураций** и **Инвентаризация** необходимо использовать учётную запись пользователя VMware ESXi Server.

Для сканирования VMware ESXi Server заданием типа **Фиксация** необходимо использовать учётную запись пользователя Linux.

При использовании авторизации по ключам для выполнения задания типа **Фиксация** необходим ключ, сгенерированный утилитой **ssh-keygen**. Ключ, сгенерированный утилитой **puttygen**, не применим для данного задания.

По умолчанию на серверах ESXi доступ по протоколу SSH отключен. Включить доступ по SSH можно следующими способами:

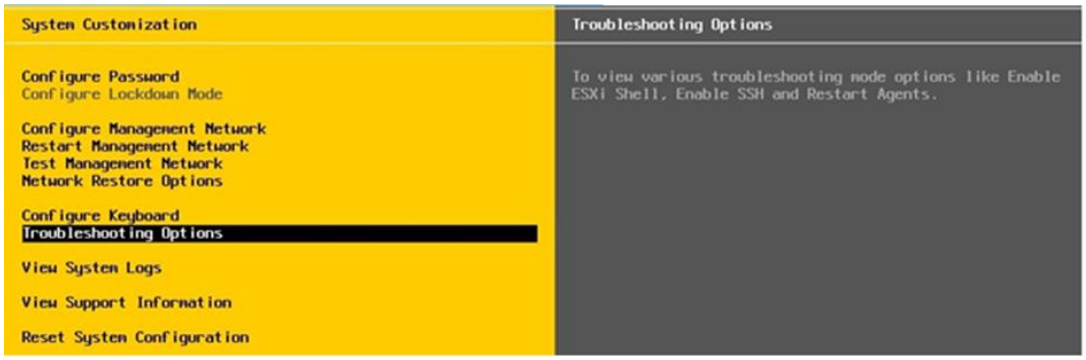
- Включение SSH через DCUI;
- Включение SSH при помощи Web-клиента vSphere.

Включение SSH через DCUI

Direct Console User Interface (DCUI) – это интерфейс сервера ESXi, который выводится на монитор при прямом подключении к серверу.

Шаг 1. На сервере ESXi нажмите **F2** и авторизуйтесь при помощи учётной записи root;

Шаг 2. В меню **System Customization** выберите **Troubleshooting Options**;



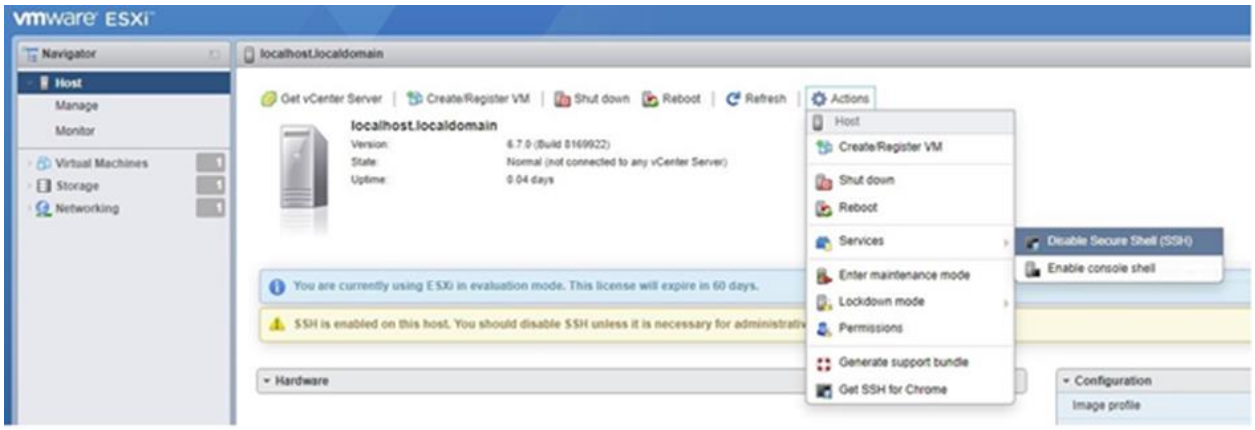
Шаг 3. В **Troubleshooting Mode Options** включите **Enable SSH**;

Для возврата в основное меню нажмите ESC.

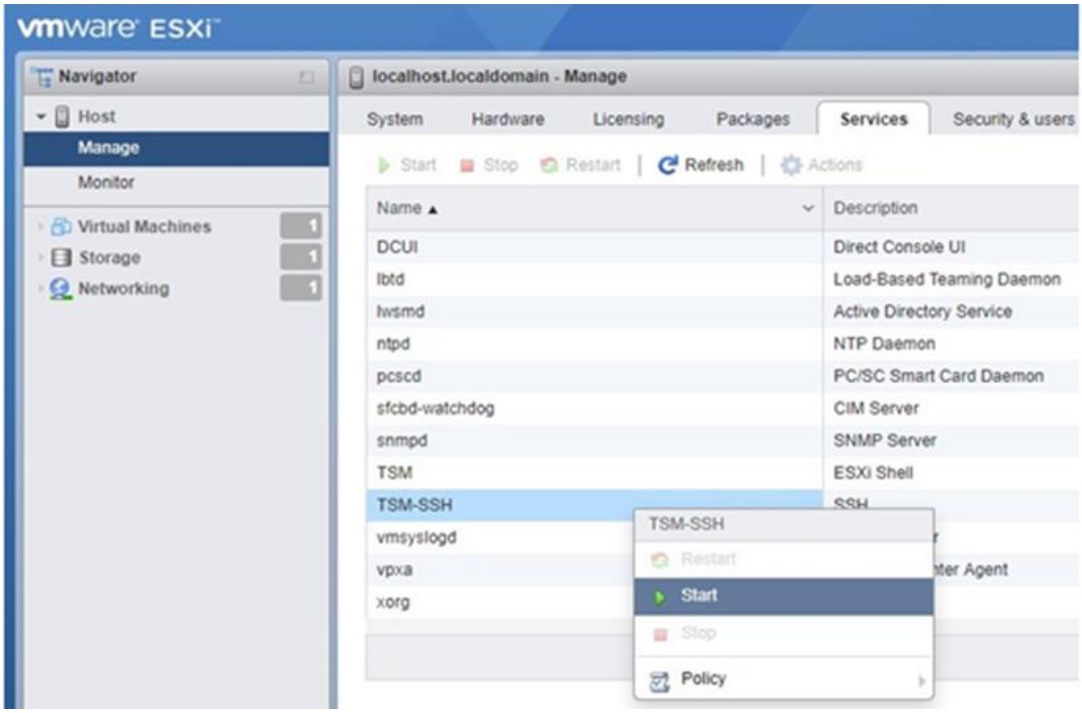
Включение SSH при помощи Web-клиента vSphere

Шаг 1. Запустите браузер → введите в адресной строке адрес VMware сервера → авторизуйтесь на сервере ESXi через интерфейс vSphere Web Client;

Шаг 2. Выберите **Actions** → **Services** → **Enable Secure Shell (SSH);**



Также активировать SSH можно в разделе **Manage** → **Services** → ПКМ по службе **TSM-SSH** → **Start**



Настройка SSH-туннеля завершена.

5.4.10.2 Настройка VMware vCenter Server

Для выполнения всех типов заданий RedCheck, кроме Фиксации, требуются:

- активированная лицензия на продукт с включенной в нее feature vSphere API;
- наличие учётной записи администратора (администратора или root для задания типа **Фиксация**);
- редакция RedCheck Professional или Enterprise.

Для выполнения задания Фиксации, помимо обозначенных выше требований, необходимо:

- включенная служба SSH;
- включенная служба ESXi Shell;
- настроенные правила брандмауэра для доступа к SSH серверу;
- наличие параметра **PermitRootLogin yes** в настройках SSH сервера;
- наличие параметра **MaxSession 10** в настройках SSH сервера;
- наличие BASH в качестве shell по умолчанию;

Для сканирования VMware vCenter Server в режимах **Аудит обновлений**, **Аудит уязвимостей**, **Аудит конфигураций** и **Инвентаризация** необходимо использовать учётную запись пользователя VMware vCenter Server.

Для сканирования VMware vCenter Server заданием типа **Фиксация** необходимо использовать учётную запись пользователя Linux.

5.4.10.3 Настройка VMware NSX Data Center for vSphere

При сканировании VMware NSX Data Center for vSphere в качестве транспорта используется протокол HTTPS.

Для выполнения всех типов заданий RedCheck, кроме Фиксации, требуются:

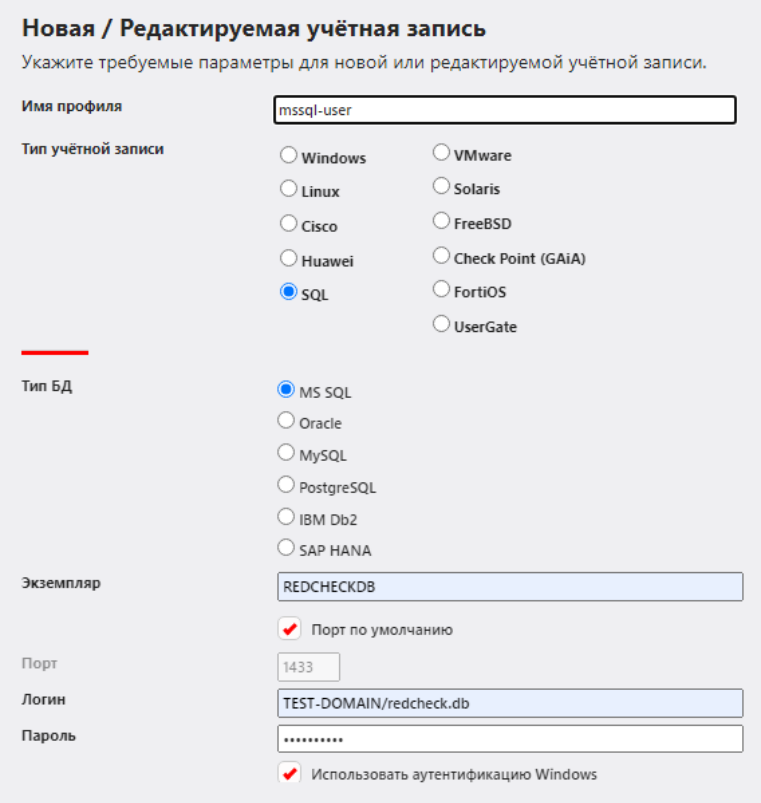
- наличие включенной учётной записи Auditor;
- проверка доступности транспорта внешними средствами (например, Postman);
- редакция RedCheck Professional или Enterprise.

Перечень команд, выполняемых при сканировании VMware NSX Data Center for vSphere:

- api/1.0/appliance-management/backuprestore/backupsettings
- api/1.0/appliance-management/system/network
- api/1.0/appliance-management/components
- api/1.0/appliance-management/system/timesettings
- api/1.0/appliance-management/system/syslogserver
- api/2.0/vdn/controller/node

5.4.11 Сканирование Microsoft SQL Server

Для сканирования БД Microsoft SQL Server требуется создать учётную запись, **Тип** – **SQL**, **Тип БД** – **MS SQL**.



Для сканирования СУБД Microsoft SQL Server в экземпляре СУБД может использовать режим доменной и смешанной авторизации.

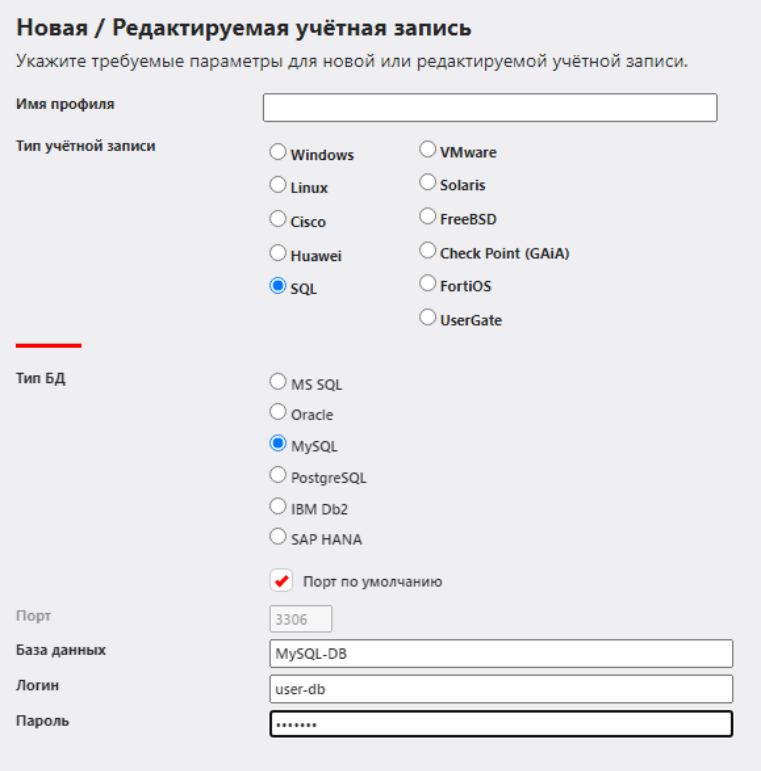
По умолчанию, для сканирования СУБД MS SQL используется порт 1433. В случае использования в инфраструктуре сети другого порта его необходимо явно указать.

Минимальные требования для учётной записи

- роль сервера – **public**;
- учётная запись должна быть включена для базы данных **master**.

5.4.12 Сканирование MySQL

Для сканирования БД MySQL требуется создать учётную запись, **Тип** – **SQL**, **Тип БД** – **MySQL**.



Для сканирования СУБД MySQL в экземпляре СУБД должен использоваться смешанный тип аутентификации (проверка подлинности MySQL).

По умолчанию, для сканирования СУБД MySQL используется порт 3306. В случае использования в инфраструктуре сети другого порта его необходимо явно указать.

Минимальные требования для учётной записи

1. **Учетная запись должна иметь права на выполнение SELECT-запросов к перечисленным таблицам:**

- information_schema.plugins
- mysql.user
- mysql.slave_master_info (если есть)

2. **Права на чтение объектов файловой системы:**

Windows

- C:\ProgramData\MySQL\MySQL Server x.x\
- C:\Program Files\MySQL\MySQL Server x.x\

Linux

- /etc/mysql
- /etc/passwd
- /etc/group
- /home/
- /proc/
- /var/lib/mysql/
- /var/log/mysql/

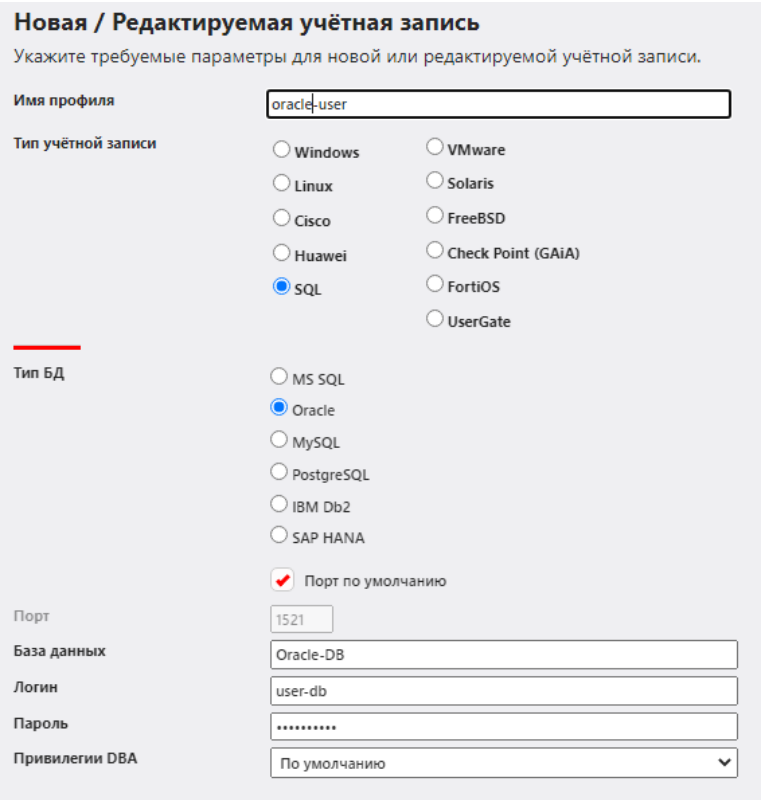
3. **Права на выполнение:**

Linux

- /usr/sbin/mysqld

5.4.13 Сканирование Oracle

Для сканирования БД Oracle требуется создать учётную запись, **Тип** – **SQL**, **Тип БД** – **Oracle**.



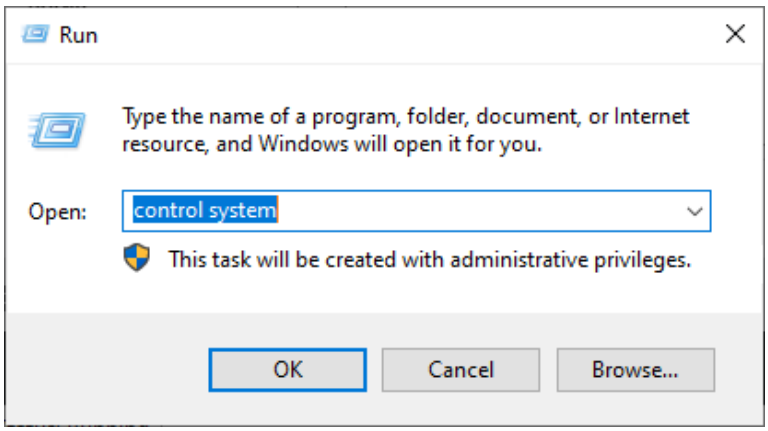
В экземпляре СУБД должен использоваться смешанный тип аутентификации (проверка подлинности Oracle).

По умолчанию для сканирования СУБД Oracle используется порт 1521. В случае использования в инфраструктуре сети другого порта его необходимо явно указать.

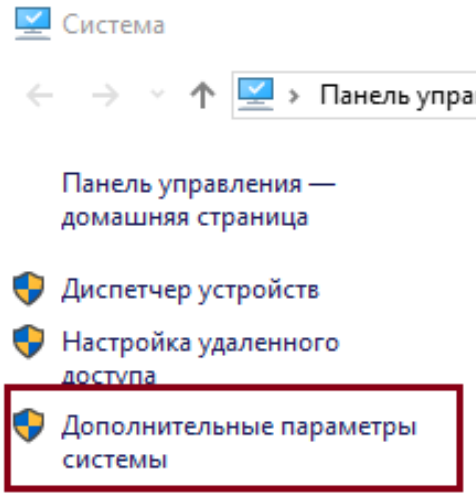
Добавление переменной среды ORACLE_HOME

Для проведения задания **Аудит БД Oracle** на сервере с установленной СУБД необходимо добавить переменную среды ORACLE_HOME.

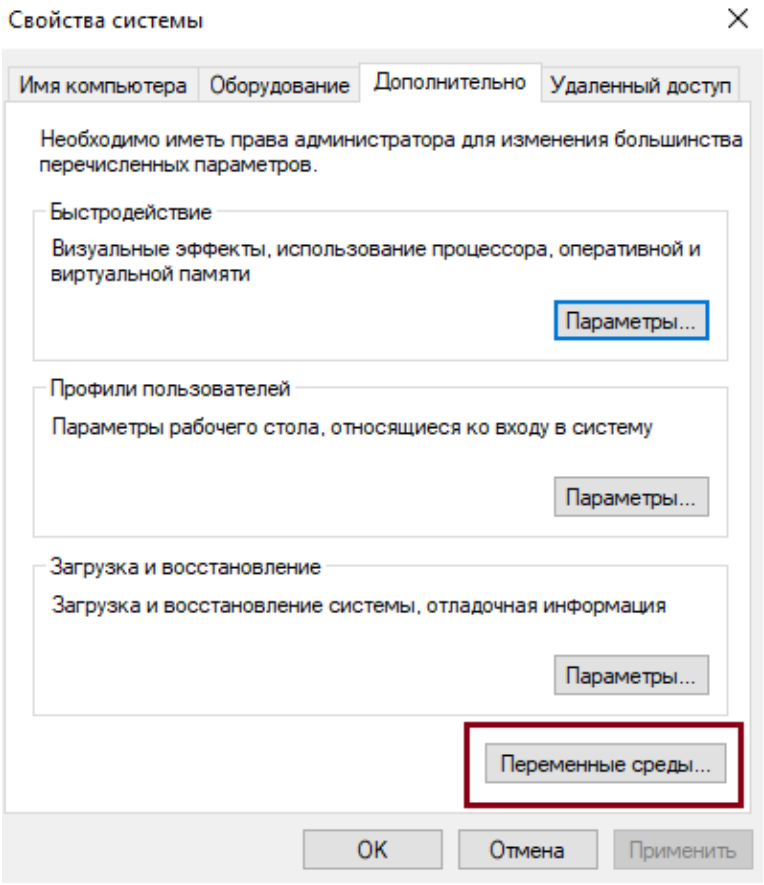
Шаг 1. Нажмите **Win + R** и введите **control system**;



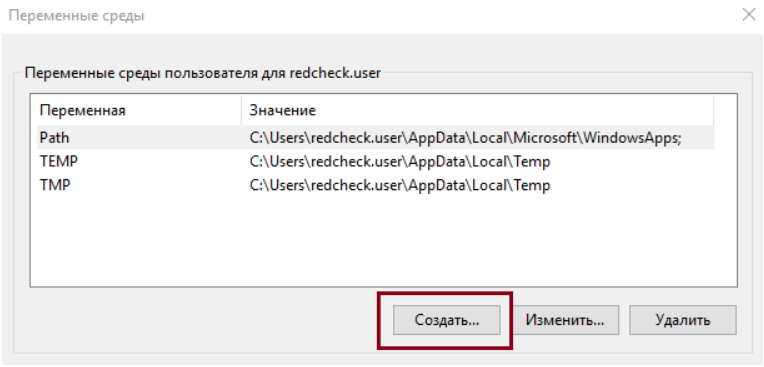
Шаг 2. Перейдите в **Дополнительные параметры системы**;



Перейдите в **Переменные среды**;



Нажмите **Создать**;



Шаг 3. В **Значение переменной** укажите каталог с ПО (по умолчанию каталог расположен по следующему
пути: **C:\app\Имя_пользователя\virtual\product\Версия\Имя_БД)**

Необходимые разрешения на выполнение команд

Для сканирования СУБД допускается использование непривилегированной учетной записи. Ей потребуется добавить роль и предоставить необходимые разрешения, выполнив указанные ниже команды от имени привилегированного пользователя СУБД:

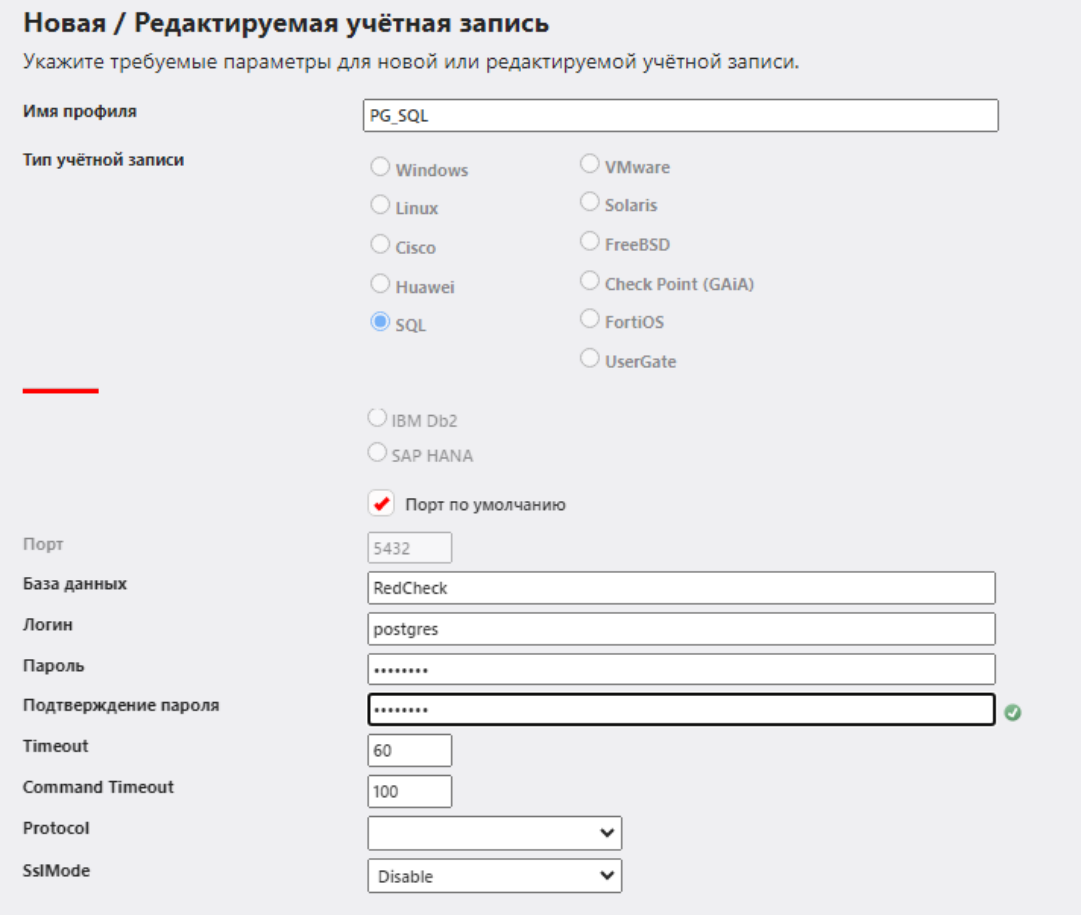
PL/SQL

```
GRANT CONNECT TO <USER NAME>;
GRANT SELECT ON DBA_USERS TO <USER NAME>;
GRANT SELECT ON DBA_USERS_WITH_DEFPWD TO <USER NAME>;
GRANT SELECT ON DBA_TAB_PRIVS TO <USER NAME>;
GRANT SELECT ON DBA_PROFILES TO <USER NAME>;
GRANT SELECT ON DBA_TS_QUOTAS TO <USER NAME>;
GRANT SELECT ON DBA_ROLE_PRIVS TO <USER NAME>;
GRANT SELECT ON DBA_SYS_PRIVS TO <USER NAME>;
GRANT SELECT ON DBA_ROLES TO <USER NAME>;
GRANT SELECT ON DBA_PRIV_AUDIT_OPTS TO <USER NAME>;
GRANT SELECT ON DBA_OBJ_AUDIT_OPTS TO <USER NAME>;
GRANT SELECT ON DBA_STMT_AUDIT_OPTS TO <USER NAME>;
GRANT SELECT ON ALL_SYNONYMS TO <USER NAME>;
GRANT SELECT ON V_$PARAMETER TO <USER NAME>;
GRANT SELECT ON V_$DATABASE TO <USER NAME>;
GRANT SELECT ON V_$INSTANCE TO <USER NAME>;
GRANT SELECT ON V_$SESSION TO <USER NAME>;
```

<USER NAME> – имя непривилегированной учетной записи.

5.4.14 Сканирование PostgreSQL

Для сканирования БД требуется создать учётную запись **Тип** – **SQL**, **Тип БД** – **PostgreSQL**.



По умолчанию для сканирования СУБД PostgreSQL используется порт 5432. В случае использования в инфраструктуре сети другого порта его необходимо явно указать.

Настройка учетной записи СУБД

Для СУБД необходимо создать учётную запись (например, rc_scan_pg) с правами, достаточными для выполнения запросов.

Шаг 1. Выполните минимальную настройку прав следующими командами (выполняются от привилегированного пользователя в СУБД):

PL/SQL

```
GRANT SELECT ON pg_settings TO rc_scan_pg;
GRANT SELECT ON pg_roles TO rc_scan_pg;
```

```
GRANT SELECT ON pg_database TO rc_scan_pg;
GRANT SELECT ON pg_user TO rc_scan_pg;
GRANT SELECT ON pg_class TO rc_scan_pg;
GRANT SELECT ON pg_authid TO rc_scan_pg;
GRANT SELECT ON pg_shadow TO rc_scan_pg;
GRANT EXECUTE ON has_schema_privilege('public','public','create') TO
rc_scan_pg;
```

Шаг 2. В файле **pg_hba.conf** необходимо разрешить подключение к СУБД. Выполните для этого команды:

Для Windows-систем

Code

```
echo host all rc_scan_pg <имя_сети/маска> md5 >> C:\Program
Files\PostgreSQL\версия\data\pg_hba.conf
```

<имя_сети/маска> - сеть или один адрес, которым разрешается доступ к СУБД. К примеру, 192.168.100.0/24 или 192.168.100.15/32;

Для Astra Linux

Bash (Unix Shell)

```
echo host all rc_scan_pg <имя_сети/маска> md5 >>
/etc/postgresql/версия/main/pg_hba.conf
```

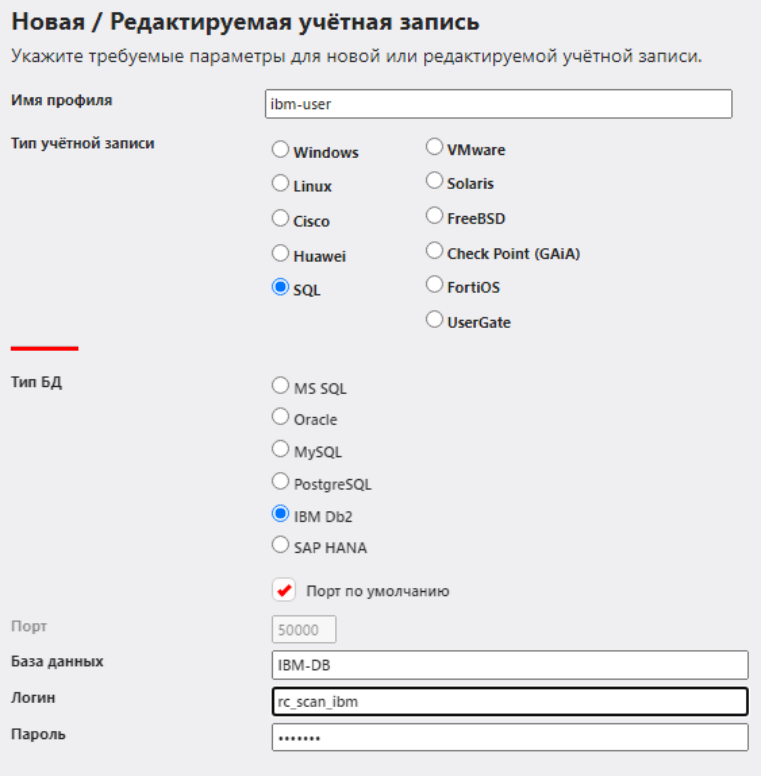
Для BaseAlt

Bash (Unix Shell)

```
echo host all rc_scan_pg <имя_сети/маска> md5 >>
/var/lib/pgsql/data/pg_hba.conf
```

5.4.15 Сканирование IBM Db2

Для сканирования БД требуется создать учётную запись, **Тип** – **SQL**, **Тип БД** – **IBM Db2**.

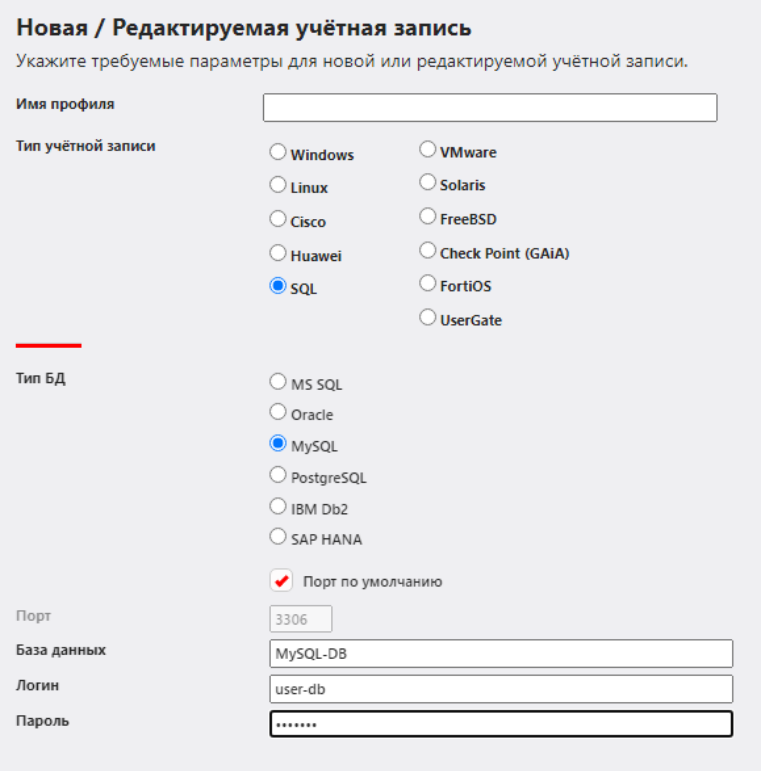


По умолчанию для сканирования СУБД IBM Db2 используется порт 50000. В случае использования в инфраструктуре сети другого порта его необходимо явно указать.

Для сканирования СУБД на хосте с серверным компонентом RedCheck необходимо установить IBM Data Server Client.

5.4.16 Сканирование SAP HANA

Для сканирования БД MySQL требуется создать учётную запись, **Тип** – **SQL**, **Тип БД** – **MySQL**.



Для сканирования СУБД MySQL в экземпляре СУБД должен использоваться смешанный тип аутентификации (проверка подлинности MySQL).

По умолчанию, для сканирования СУБД MySQL используется порт 3306. В случае использования в инфраструктуре сети другого порта его необходимо явно указать.

Минимальные требования для учётной записи

Учетная запись должна иметь права на выполнение SELECT-запросов к перечисленным таблицам и view-ам:

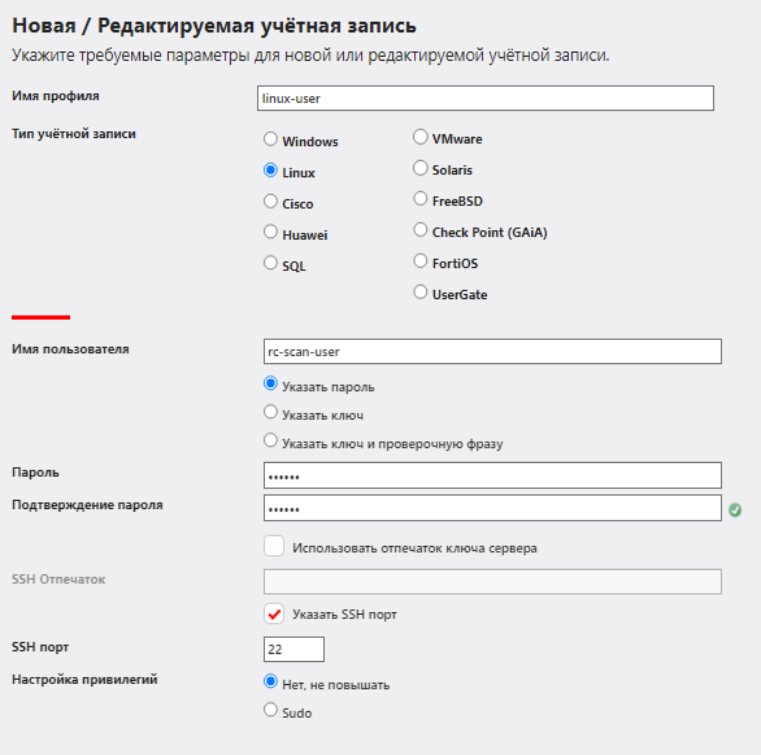
- SYS.M_PASSWORD_POLICY (View)
- SYS.AUDIT_POLICIES (View)
- SYS.USERS (View)
- SYS.M_INIFILE_CONTENTS (View)
- _SYS_SECURITY._SYS_PASSWORD_BLACKLIST (Table)

5.4.17 Сканирование Docker

При сканировании образов под управлением Docker выполняется подключение к хосту с клиентом и демоном Docker. В качестве транспорта используется SSH-протокол не ниже версии 2.0 с включенным модулем поддержки протокола SFTP.

Для проведения сканирования требуется, чтобы пользователь, от имени которого выполняется сканирование, имел права root или возможность использовать sudo для повышения привилегий.

В RedCheck для сканирования Docker требуется создать учётную запись, **Тип учетной записи** – **Linux**.



Рекомендуется использовать учетную запись суперпользователя (root) вместо повышения прав с использованием sudo. В противном случае возможны проблемы с производительностью при сканировании.

На целевом хосте требуется установка следующего ПО:

- Bash shell;
- Утилита rc-rpm (ссылка ниже).

Утилиту rc-rpm необходимо установить в папку /usr/local/bin и дать права на чтение и исполнение тому пользователю, от имени которого будет выполняться сканирование.

Ссылка на скачивание: скачать

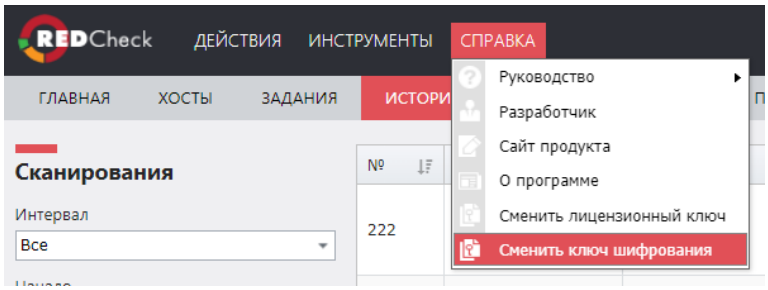
Контрольные суммы:

MD5: E522F13371499143F948EDB79194BB8E

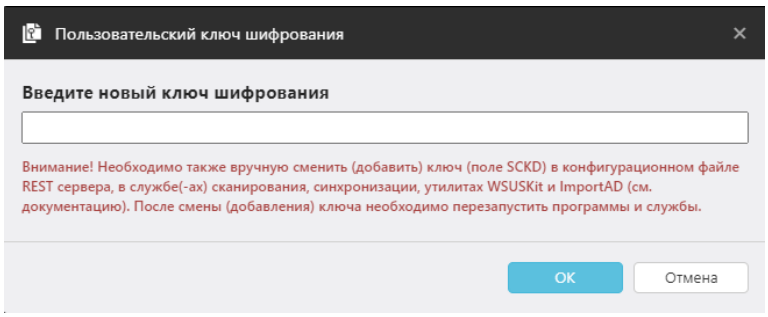
SHA256: FF94E2F4A9E8480D568BF3CD920AB676C884C315338247727B7C78406C89ADC6

5.5 Смена ключа шифрования

Шаг 1. Раскройте **Справка → Сменить ключ шифрования**;

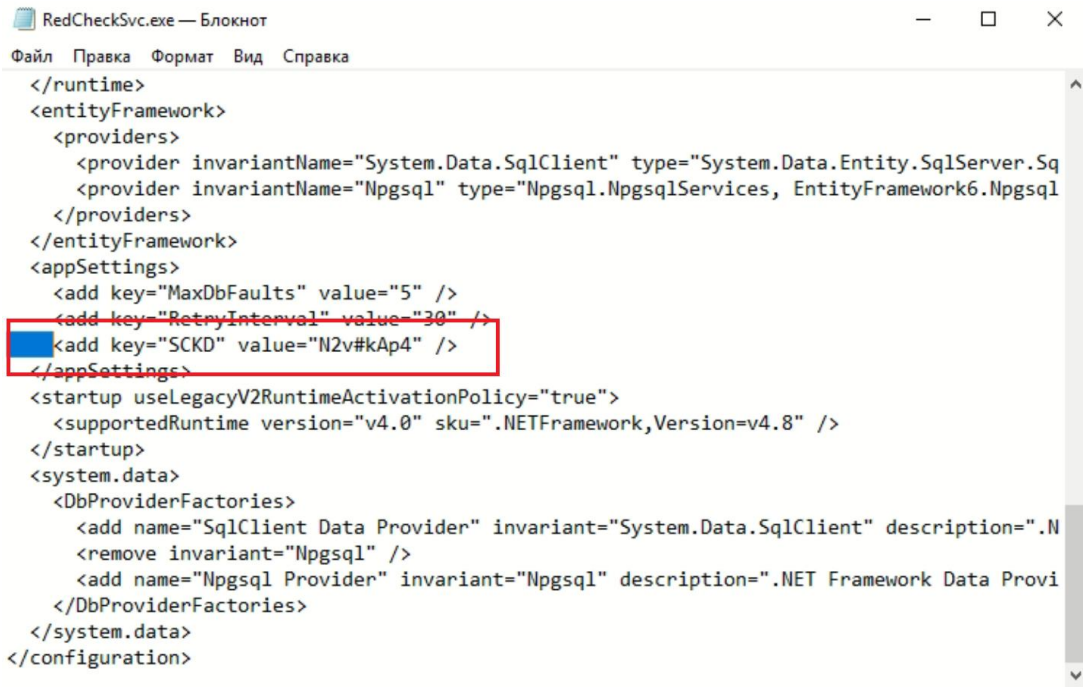


Шаг 2. Введите новый ключ шифрования → **OK**;

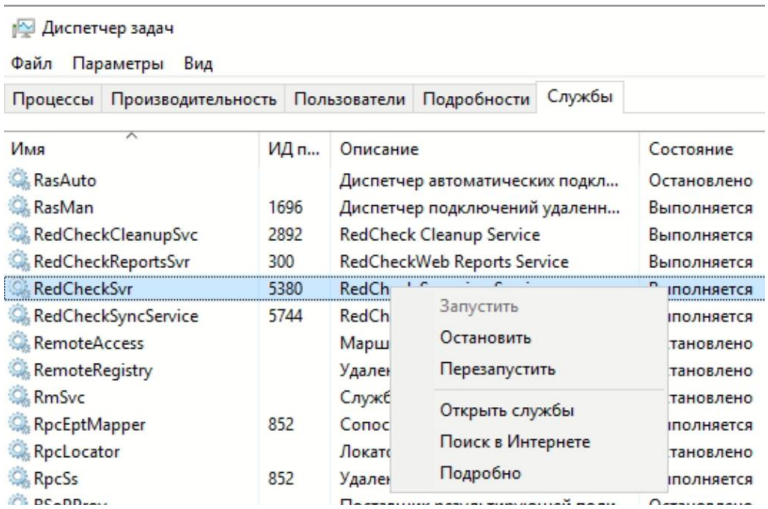


Шаг 3. Вручную смените ключ шифрования для серверного компонента. На хосте с установленным серверным компонентом необходимо открыть файл **appsettings.json** (расположение по умолчанию **C:\Program Files\ALTEX-SOFT\RedCheckWeb.Rest**) → замените старый ключ шифрования на новый для ключа **SCKD**;

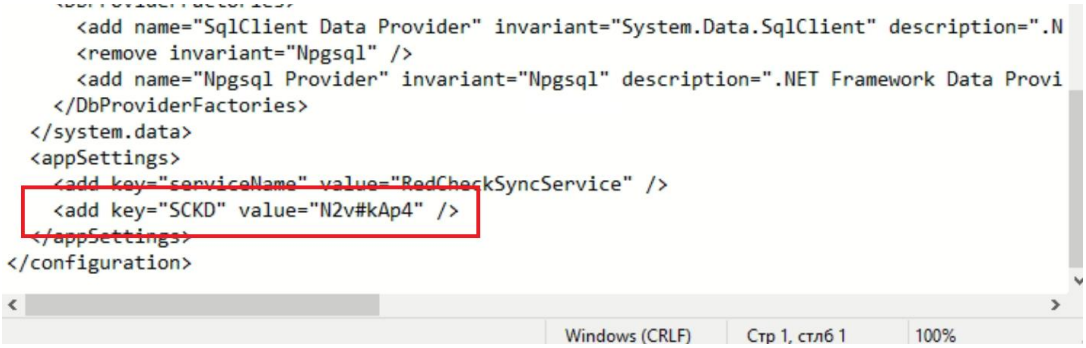
Шаг 4. Смените ключ шифрования для службы сканирования. На хосте с установленной службой сканирования необходимо открыть файл **RedCheckSvc.exe.config** (расположение по умолчанию **C:\Program Files\ALTEX-SOFT\RedCheckScanService**) → замените старый ключ шифрования на новый для параметра **SCKD**;



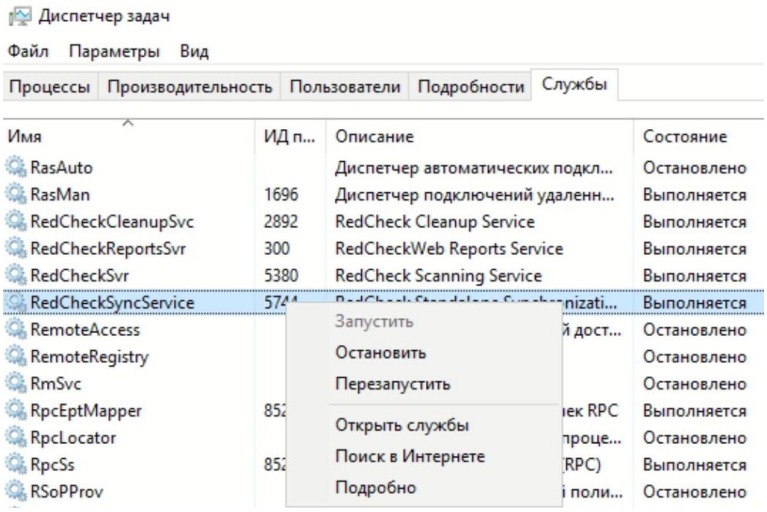
Шаг 5. Нажмите **Ctrl + Alt + Delete** → **Диспетчер задач**. Перейдите в **Службы** → ПКМ по **RedCheckSvr** → **Перезапустить**;



Шаг 6. Смените ключ шифрования для службы синхронизации. На хосте с установленной службой синхронизации необходимо открыть файл **RedCheckSnc.exe.config** (расположение по умолчанию **C:\Program Files\ALTEX-SOFT\RedCheckSyncService**) → замените старый ключ шифрования на новый для параметра **SCKD**;

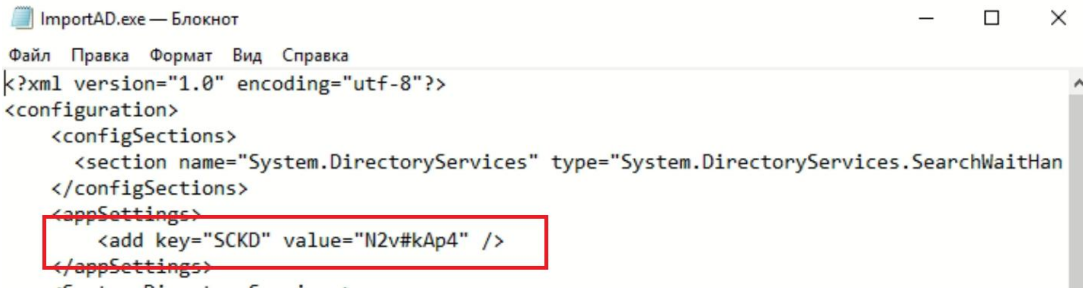


Шаг 7. Нажмите **Ctrl + Alt + Delete** → **Диспетчер задач**. Перейдите в **Службы** → ПКМ по **RedCheckSyncService** → **Перезапустить**;



При использовании утилит ImportAD и WSUSkit необходимо также сменить ключ шифрования в их файлах конфигурации.

Смените ключ шифрования для ImportAD. На хосте с установленным серверным компонентом необходимо открыть файл **ImportAD.exe.config** (расположение по умолчанию **C:\Program Files\ALTEX-SOFT\RedCheckWeb.Rest\ImportAD**) → замените старый ключ шифрования на новый для параметра **SCKD**.



5.6 Исключения для средств защиты (СЗИ, САЗ)

Не рекомендуется устанавливать RedCheck на один сервер с другими средствами защиты в противном случае, могут быть внесены изменения в библиотеки среды функционирования, что нарушит работу RedCheck.

Общий перечень папок и исполняемых файлов, подлежащих добавлению в списки исключений средств защиты, используемых в сети предприятия:

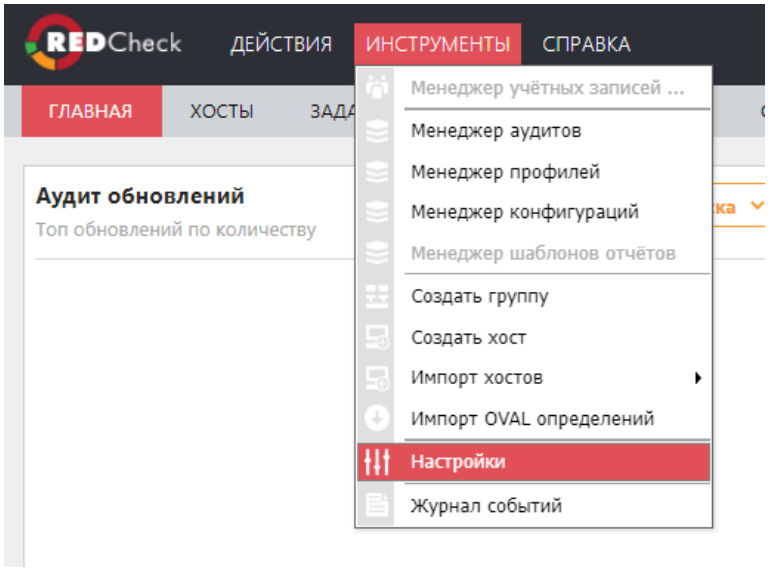
Список директорий установки	Исполняемый файл
Desktop-версия RedCheck	
C:\Program Files\ALTEX-SOFT\RedCheck	\RedCheck.exe \RedCheckSnc.exe \RedCheckSvc.exe
Web-версия RedCheck	
Серверный компонент (RestAPI): C:\Program Files\ALTEX-SOFT\RedCheckWeb.Rest	–
Web-консоль управления: C:\Program Files\ALTEX-SOFT\RedCheckWebClient C:\Program Files\ALTEX-SOFT\RedCheckWebClientReportsSvc	–
Служба сканирования: C:\Program Files\ALTEX-SOFT\RedCheckScanService C:\Program Files\ALTEX-SOFT\ALTXmap	\RedCheckSvc.exe \nmap.exe

Служба синхронизации: C:\Program Files\ALTEX-SOFT\RedCheckSyncService	\RedCheckSnc.exe
Дополнительные компоненты	
Сервер обновлений: C:\Program Files (x86)\ALTEX-SOFT\RedCheckUpdateServer	\RcUpdSrv.exe
Агент сканирования: C:\Program Files\ALTEX-SOFT\RedCheckAgent C:\Program Files (x86)\ALTEX-SOFT\RedCheckAgent	\RedCheckAgent.exe
Агент обновлений: C:\Program Files\ALTEX-SOFT\RedCheckUpdateAgent C:\Program Files (x86)\ALTEX-SOFT\RedCheckUpdateAgent	\RedCheckUpdateAgent.exe
Модуль взаимодействия со WSUS-сервером: C:\Program Files\ALTEX-SOFT\WsusKit	\WsusClientUi.exe

Содержание

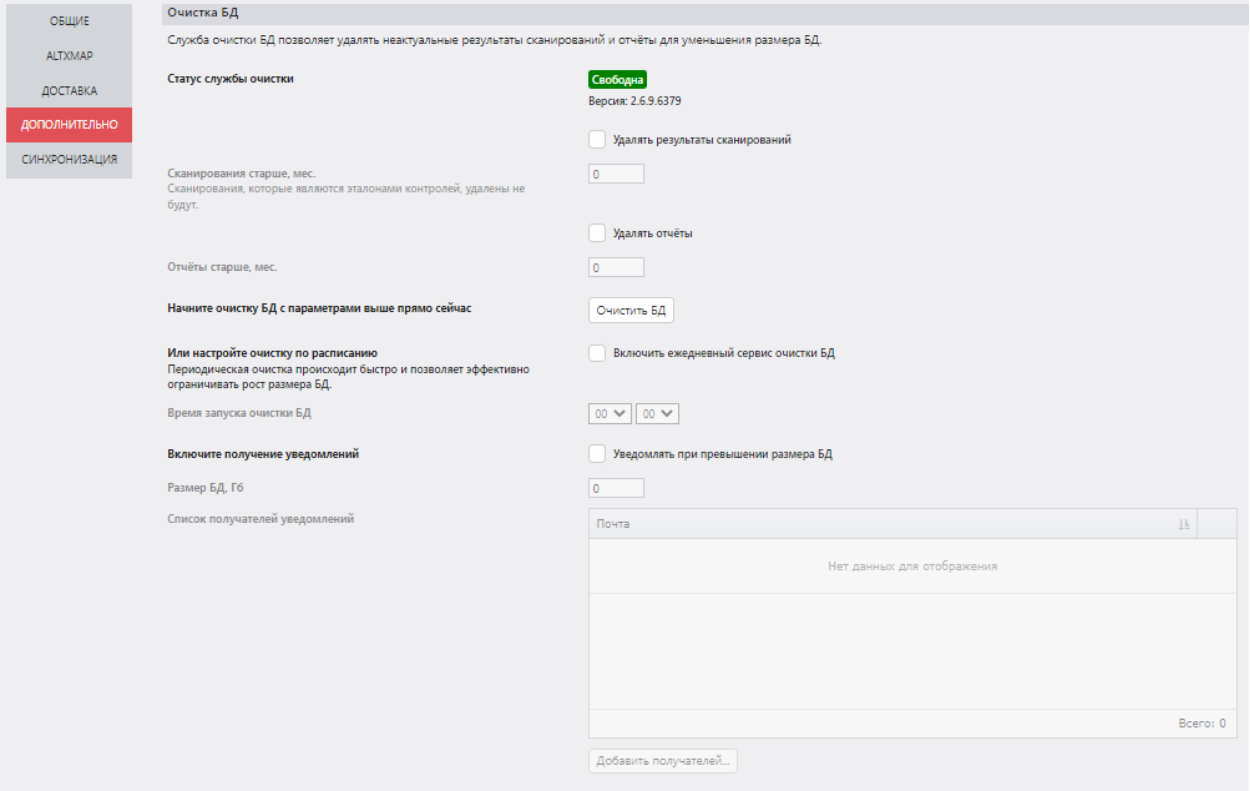
5.7.1 Автоматическая очистка БД

Шаг 1. Откройте консоль управления RedCheck → на панели навигации выберите **ИНСТРУМЕНТЫ** → **Настройки**;

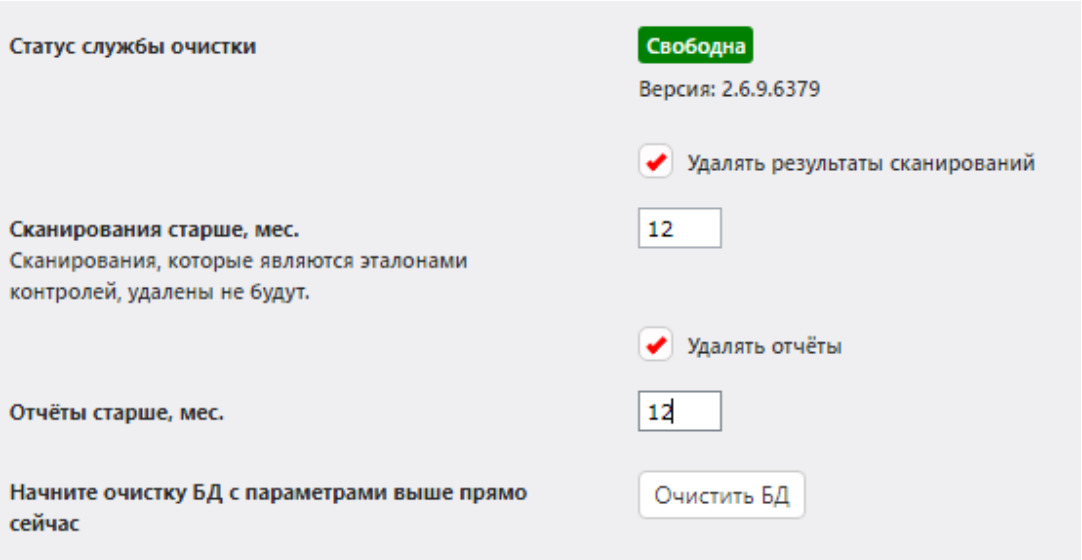


Для изменения настроек RedCheck авторизуйтесь под УЗ с ролью **REDCHECK_SYSTEMS** или **REDCHECK_ADMINS**

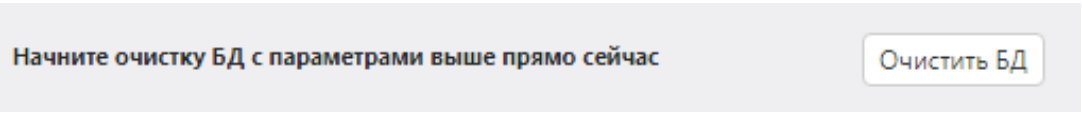
Шаг 2. Перейдите в **ДОПОЛНИТЕЛЬНО** и дождитесь подключения к службе очистки БД;



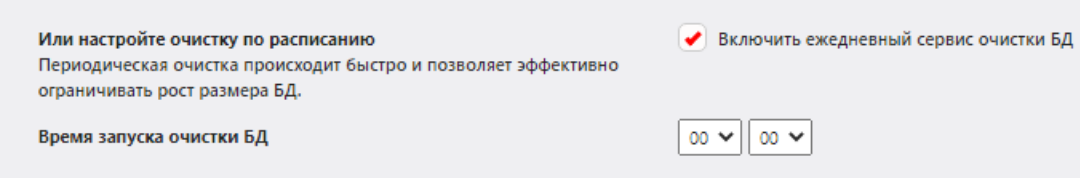
Шаг 3. Отметьте **Удалять отчеты** и **Удалять результаты сканирований.** Укажите нужный срок давности отчетов для очистки;



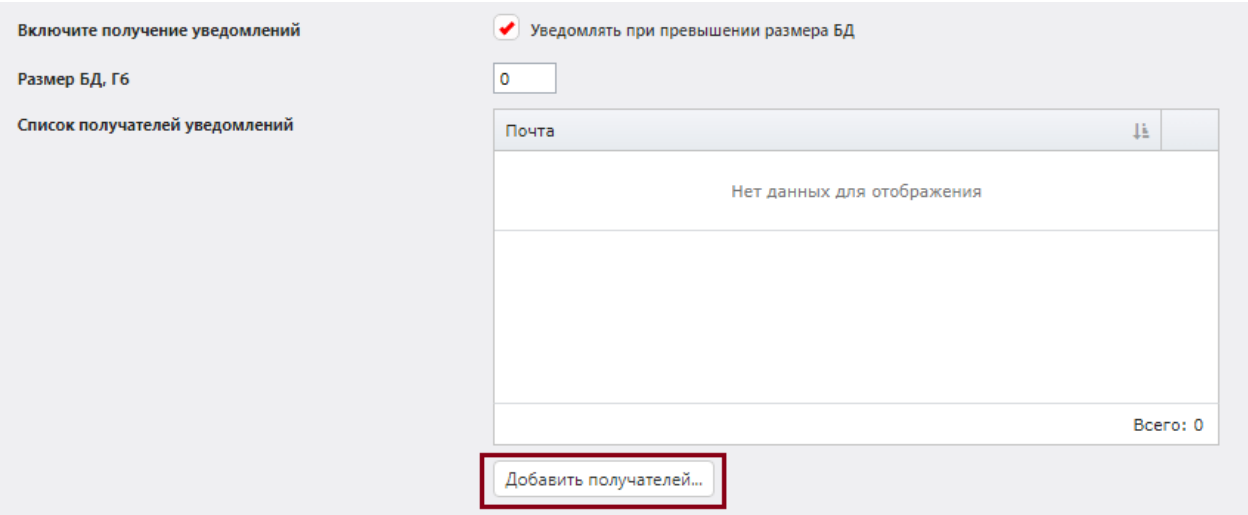
Шаг 4. Нажмите **Очистить БД**;



Шаг 5. Для автоматической очистки БД отметьте **Включить ежедневный сервис очистки БД** → выберите время запуска службы очистки;



Шаг 6. При необходимости включите оповещение о превышении БД указанного размера, отметив **Уведомлять при превышении размера БД** и указав почтовые адреса получателей;



5.7.2 Обслуживание БД при помощи Microsoft SQL Server Management Studio

В процессе работы RedCheck происходит естественное увеличение данных, хранимых в БД. В целях обеспечения стабильной и бесперебойной работы СУБД рекомендуется выполнять её обслуживание.

Под обслуживанием подразумевается три основных действия:

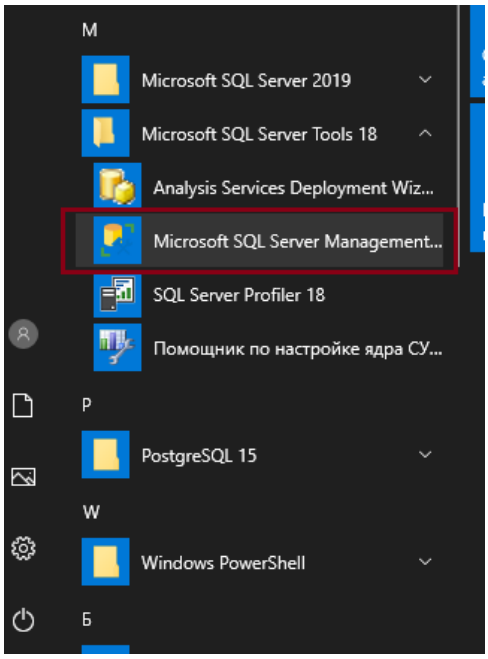
- Систематическое резервное копирование БД Системы;
- Сжатие журнала транзакций;
- Сжатие данных в СУБД с целью уменьшения занимаемого ими объёма на диске.

Систематическое резервное копирование БД Системы

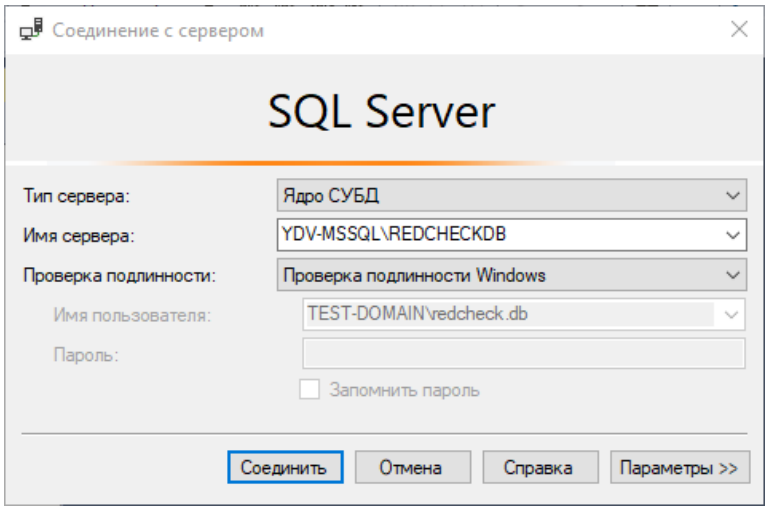
Резервное копирование БД можно произвести одним из способов, описанных в 5.7.1.1 Резервирование Microsoft SQL Server.

Сжатие журнала транзакций

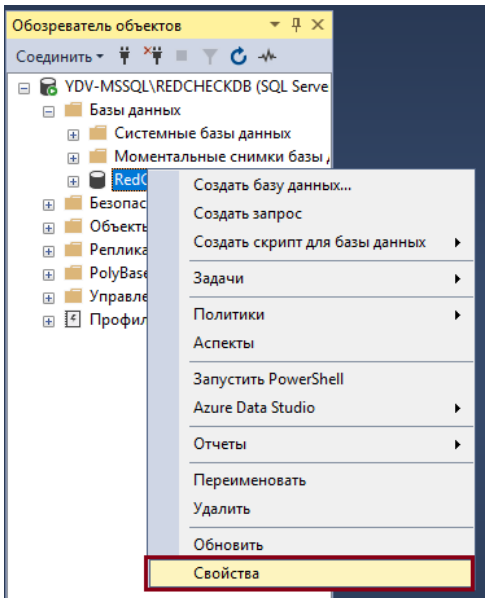
Шаг 1. Запустите Microsoft SQL Server Management Studio: **Пуск** → **Microsoft SQL Server Tools** → **Microsoft SQL Server Management**;



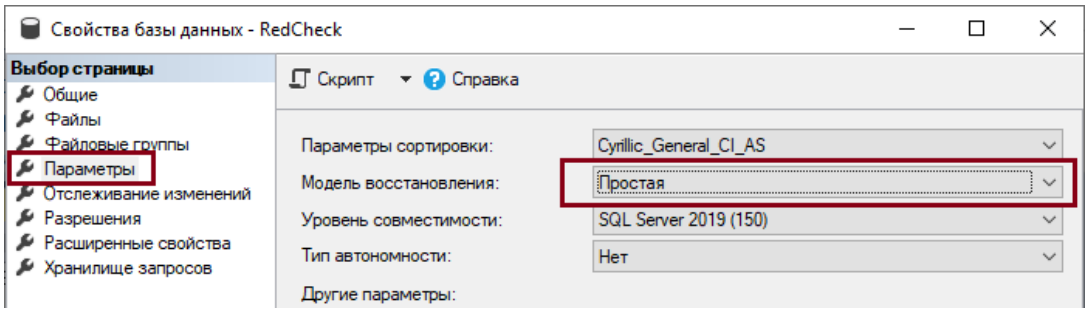
Введите необходимые данные для подключения к серверу СУБД → **Соединить**;



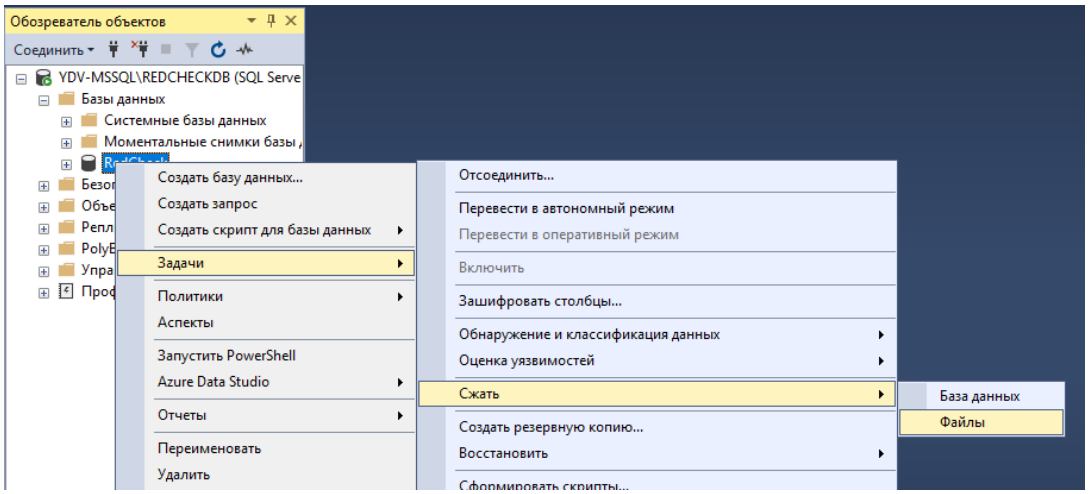
Шаг 2. ПКМ по БД RedCheck → **Свойства**;



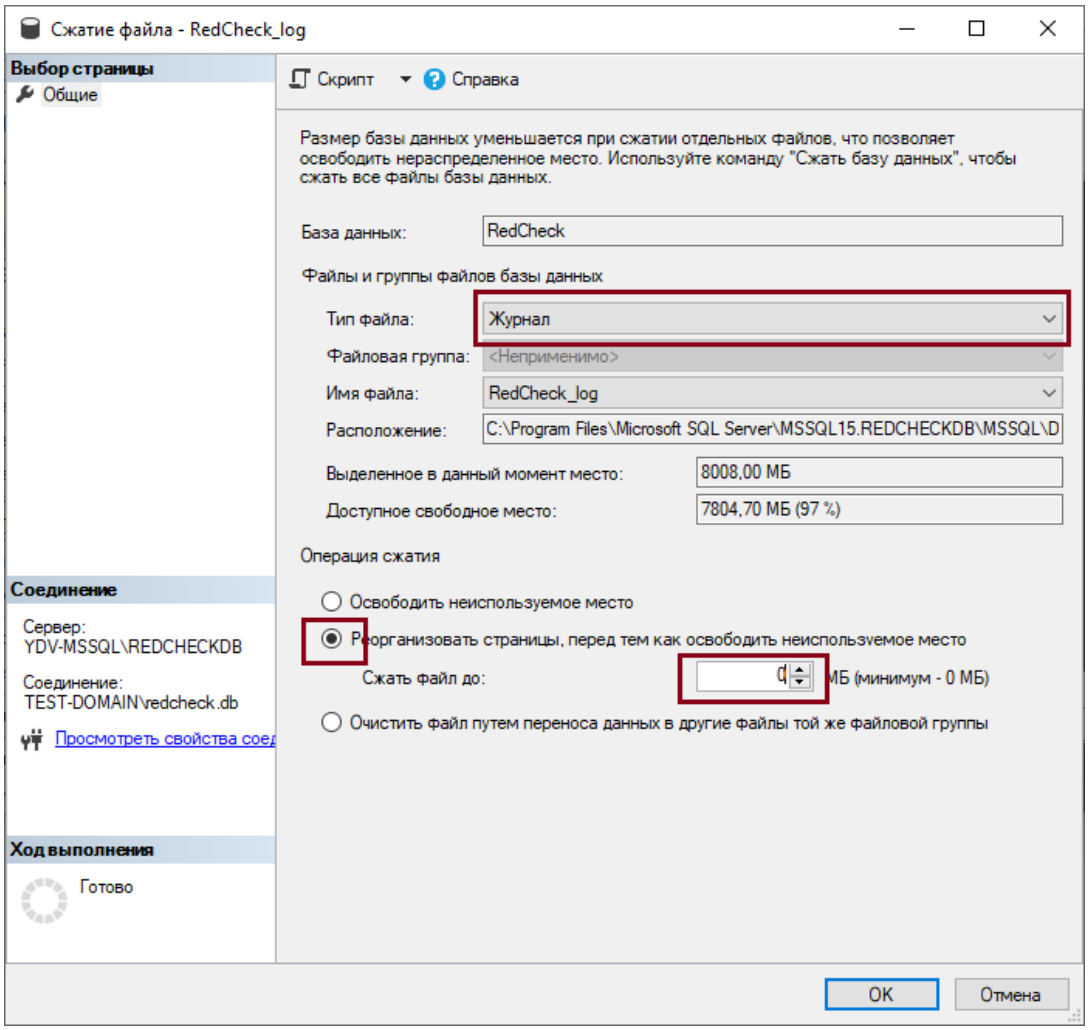
Шаг 3. Перейдите в **Параметры** → в **Модель восстановления** выберите **Простая** → **ОК**;



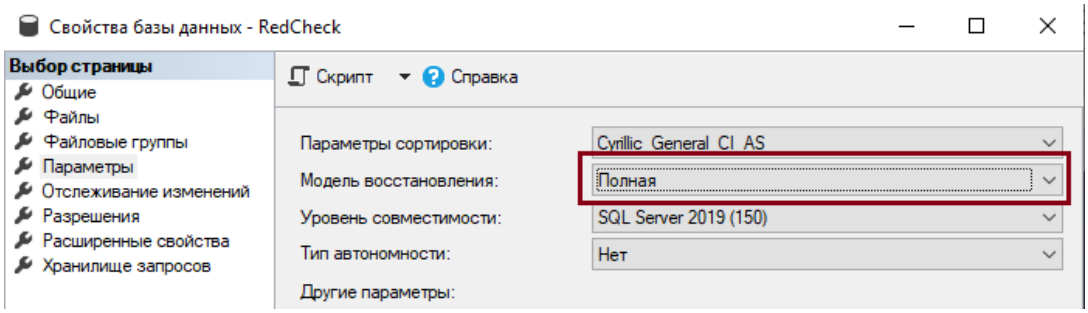
Шаг 4. ПКМ по БД RedCheck → **Задачи** → **Сжать** → **Файлы**;



Шаг 5. В **Тип Файла** выберите **Журнал** → укажите операцию сжатия **Реорганизовать страницы, перед тем как освободить неиспользуемое место** → в **Сжать файл до** установите желаемый размер журнала → **ОК**;



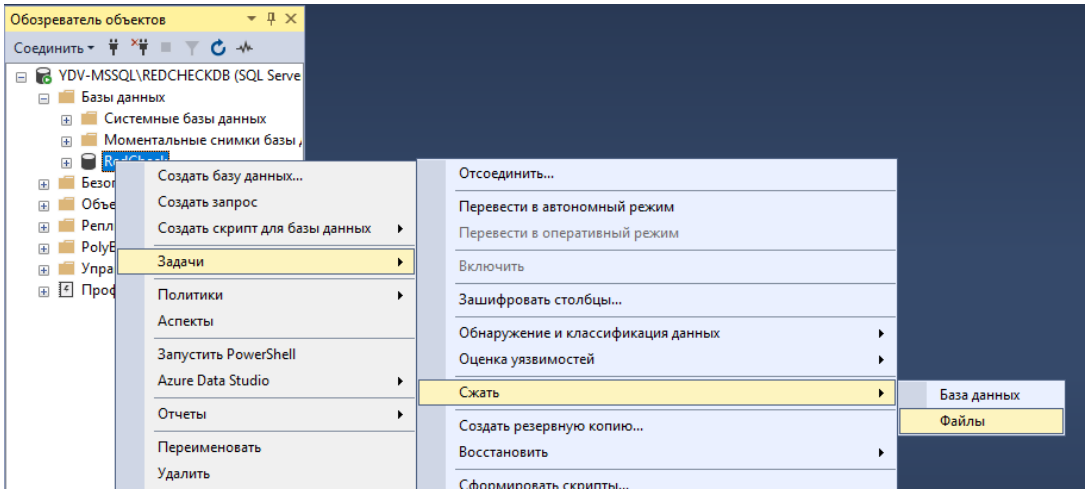
Шаг 6. Вернитесь в свойства БД RedCheck → перейдите в **Параметры** → в **Модель восстановления** выберите **Полная** → **ОК**.



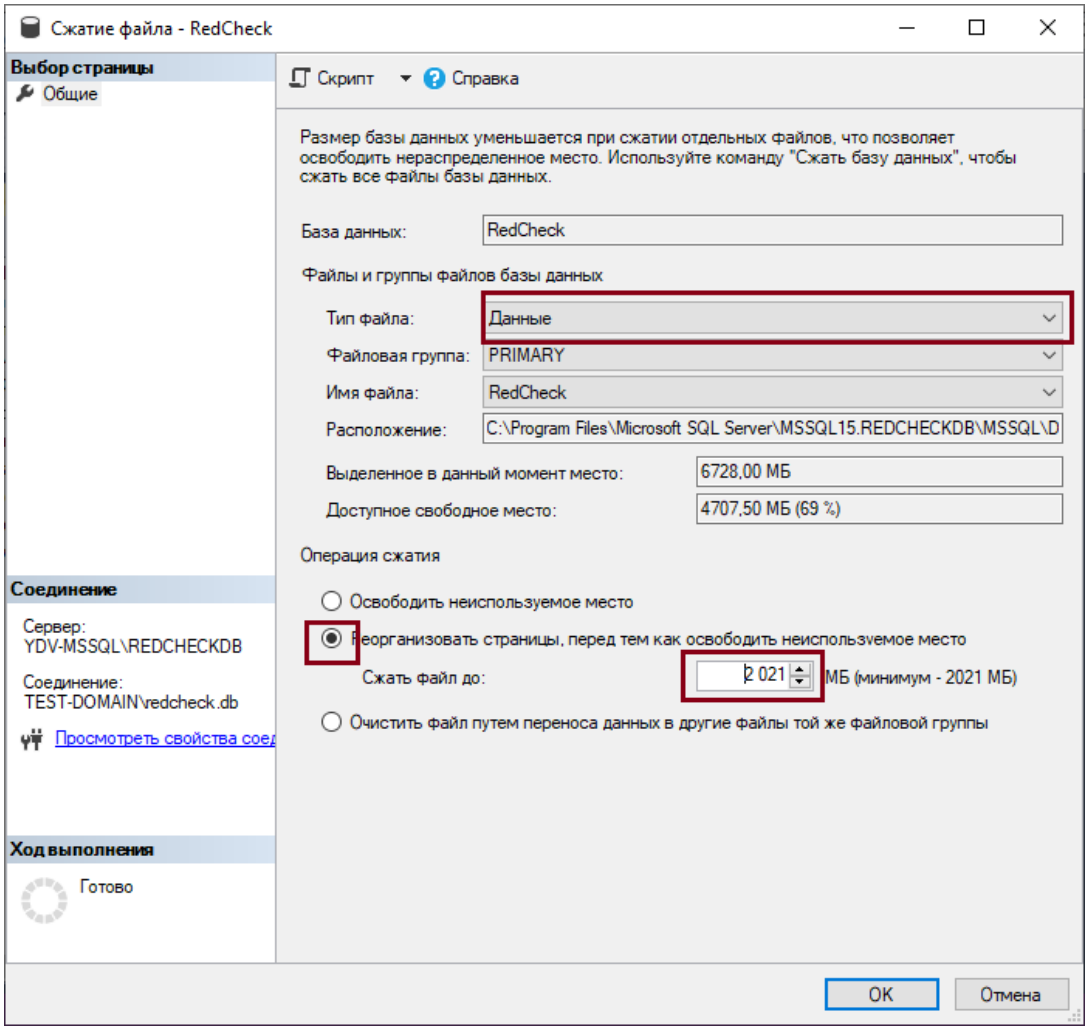
Сжатие данных в СУБД с целью уменьшения занимаемого ими объёма на диске

Рекомендуется выполнять сжатие данных в нерабочее время, когда нагрузка на БД минимальна или вовсе отсутствует.

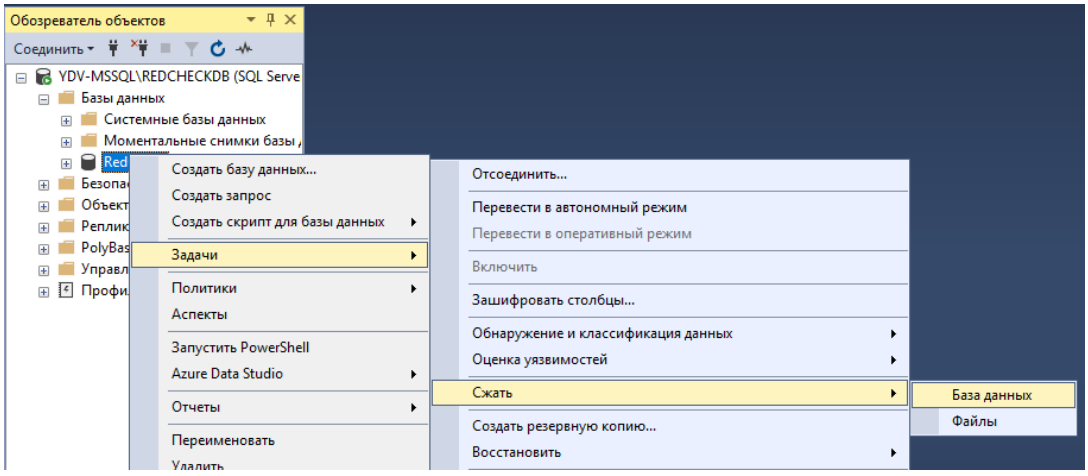
Шаг 1. ПКМ по БД RedCheck → **Задачи** → **Сжать** → **Файлы**;



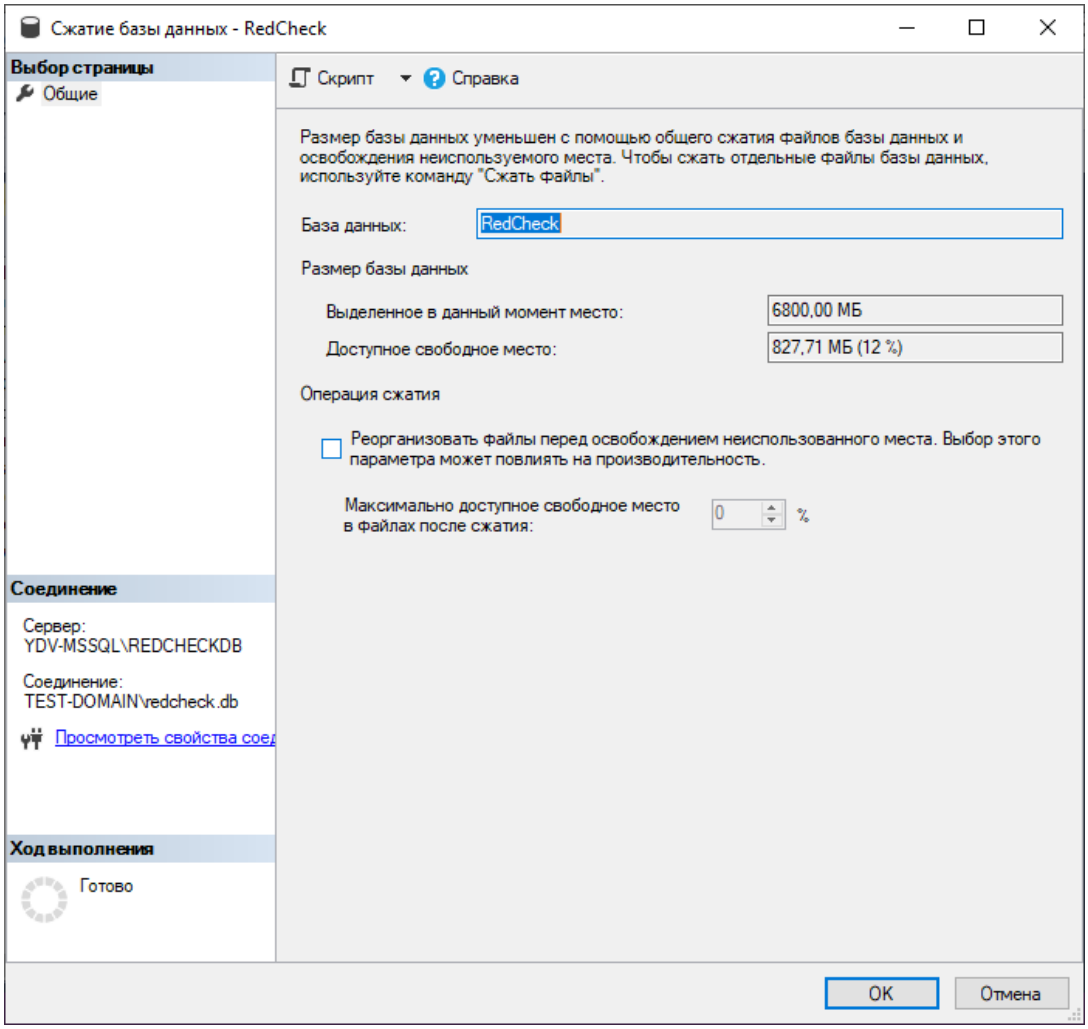
Шаг 2. В **Тип Файла** выберите **Данные** → укажите операцию сжатия **Реорганизовать страницы, перед тем как освободить неиспользуемое место** → в **Сжать файл до** установите желаемый размер журнала → **ОК**;



Шаг 3. ПКМ по БД RedCheck → **Задачи** → **Сжать** → **База данных**;



Шаг 4. В **Доступное свободное место** будет указано насколько возможно уменьшить БД → **ОК**.



5.8 Резервное копирование и восстановление

Все данные о хостах, результаты сканирования и настройки RedCheck хранятся в базе данных. Для планового резервного копирования достаточно поддерживать актуальную резервную копию БД.

В системах виртуализации допускается резервное копирование и восстановление виртуальных машин целиком.

Содержание

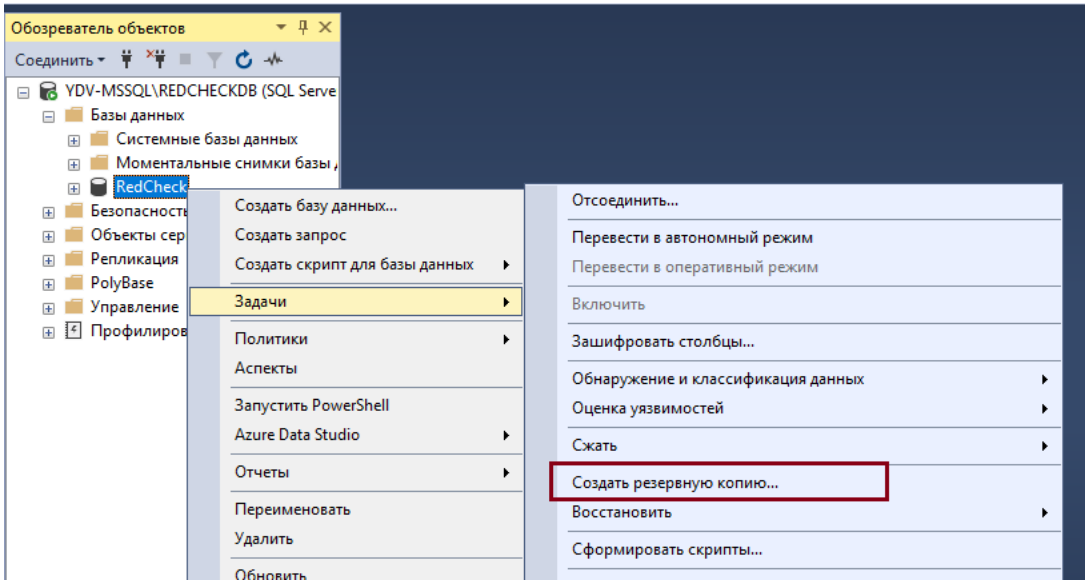
5.8.1 Рекомендации по резервному копированию

Содержание

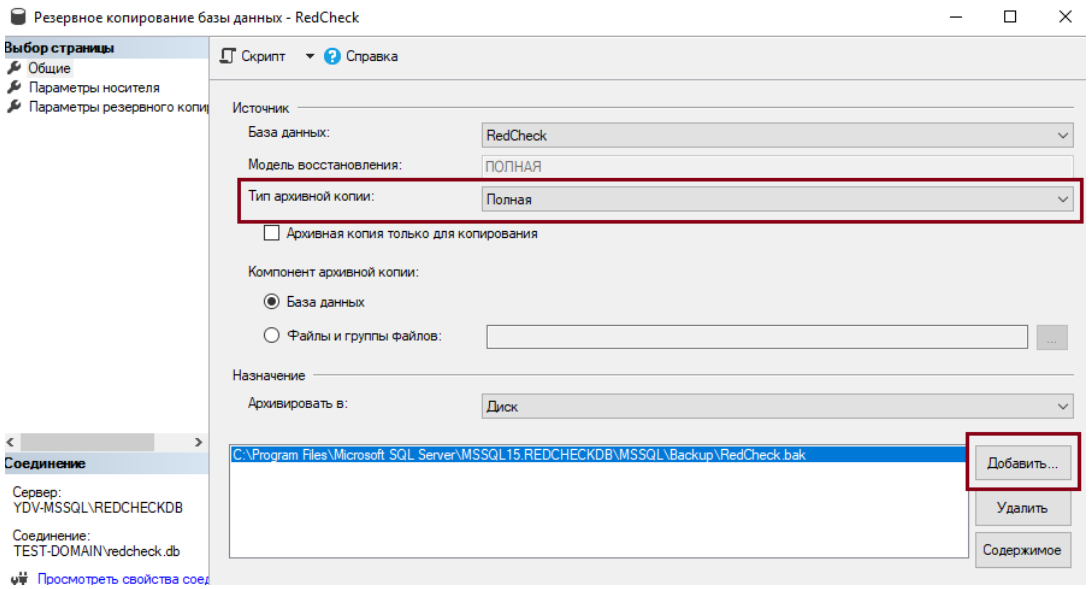
5.8.1.1 Резервирование Microsoft SQL Server

Резервирование с помощью SSMS

Шаг 1. Раскройте **Базы Данных** →ПКМ по необходимой БД → **Задачи** → **Создать резервную копию**;



Шаг 2. Измените при необходимости **Тип архивной копии** и расположение резервной копии → **ОК**.



Тип архивной копии:
Полная: резервируется вся БД, из-за чего требуется больше дискового пространства и времени;
Разностная: резервируются данные, появившиеся с момента последней резервной копии.

При выборе параметра **Разностная** убедитесь в том, что флажок **Архивная копия только для копирования** снят.

Резервирование через PowerShell

Для архивации необходим модуль **SqlServer**. Проверить его наличие можно командой:

Code

```
Get-Module -Name SqlServer
```

Установите модуль:

Code

```
Install-Module -Name SqlServer
```

Команда для создания полной резервной копии (расположение архивной копии в директории по умолчанию):

Code

```
Backup-SqlDatabase -ServerInstance Computer[\Instance] -Database
<myDatabase> -BackupAction Database
```

Подробная информация доступна на [странице](#) официальной документации Microsoft SQL Server.

5.8.1.2 Резервирование PostgreSQL

Резервное копирование через терминал

Шаг 1. Создайте резервную копию с помощью утилиты pg_dump;

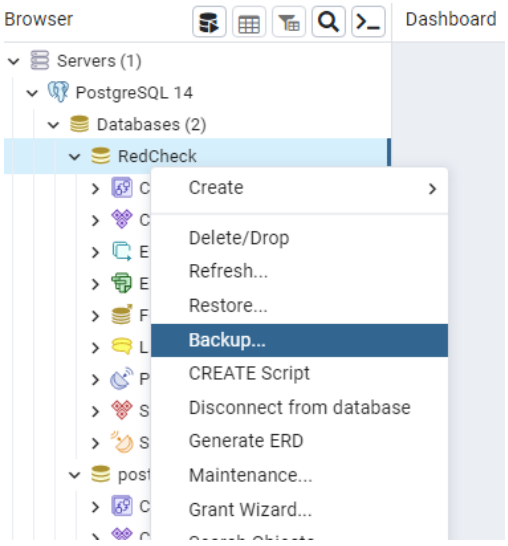
Bash (оболочка Unix)

```
pg_dump -Fc -h 127.0.0.1 -U redcheck RedCheck -f db_dd_mm_yyyy.dump
```

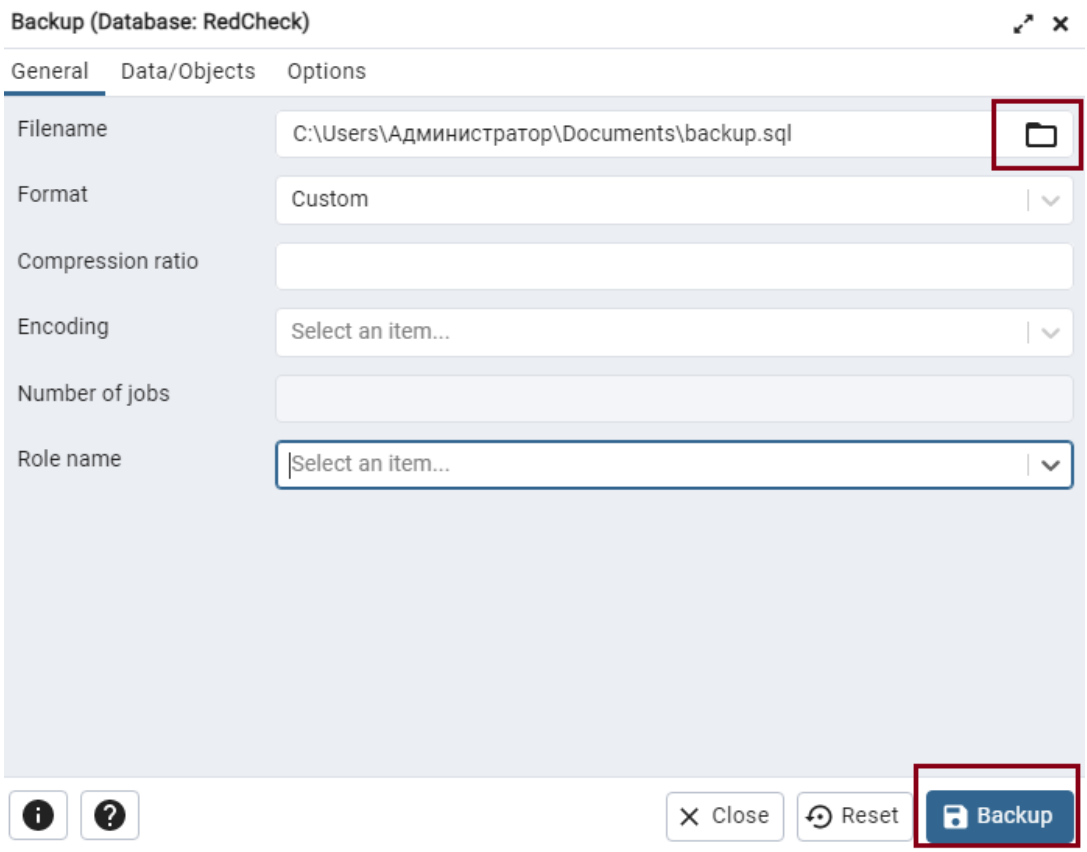
-Fc = пользовательский архивный формат результирующего файла;
-h = listen_address, на котором работает СУБД;
-U = имя пользователя, имеющего права для выполнения операции;
RedCheck = имя БД;
-f = путь для результирующего файла.

Резервное копирование через pgAdmin

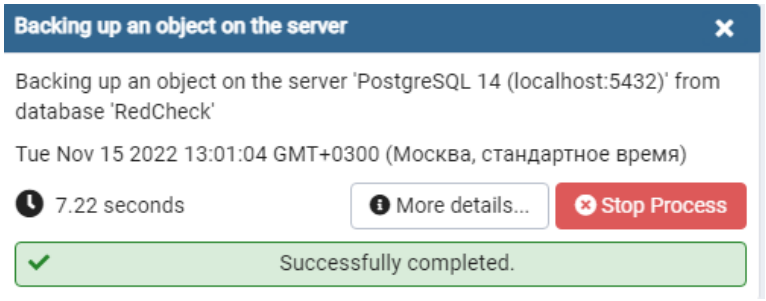
Шаг 1. ПКМ по необходимой БД → **Backup**;



Шаг 2. В **Filename** укажите расположение резервной копии → **Backup**;



Архивация завершится оповещением.



5.8.2 Восстановление БД

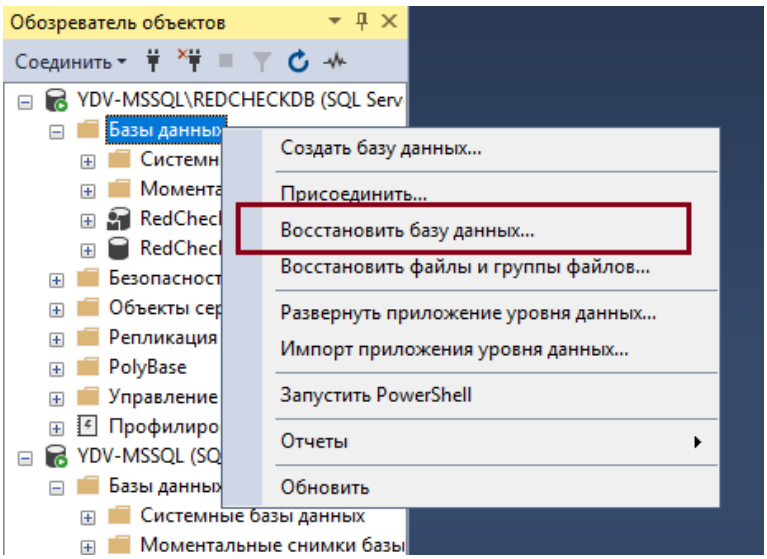
Содержание

5.8.2.1 Восстановление Microsoft SQL Server

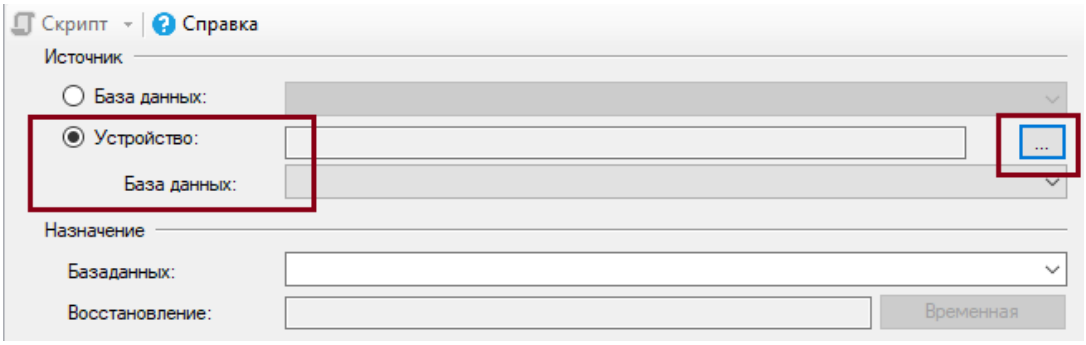
Если у вас имеется только файл резервного копирования, необходимо сперва установить СУБД Microsoft SQL Server (4.1.1 Установка СУБД Microsoft SQL Server)

Восстановление через SSMS

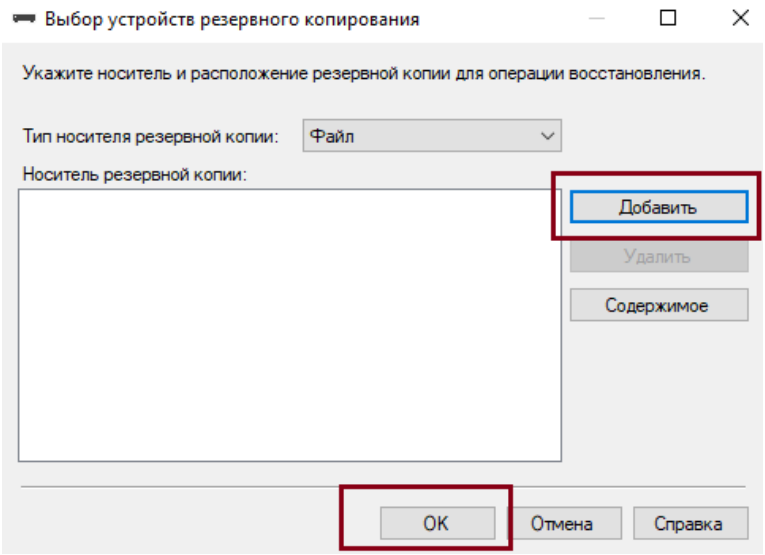
Шаг 1. В контекстном меню каталога **Базы данных** выберите **Восстановить базу данных**;



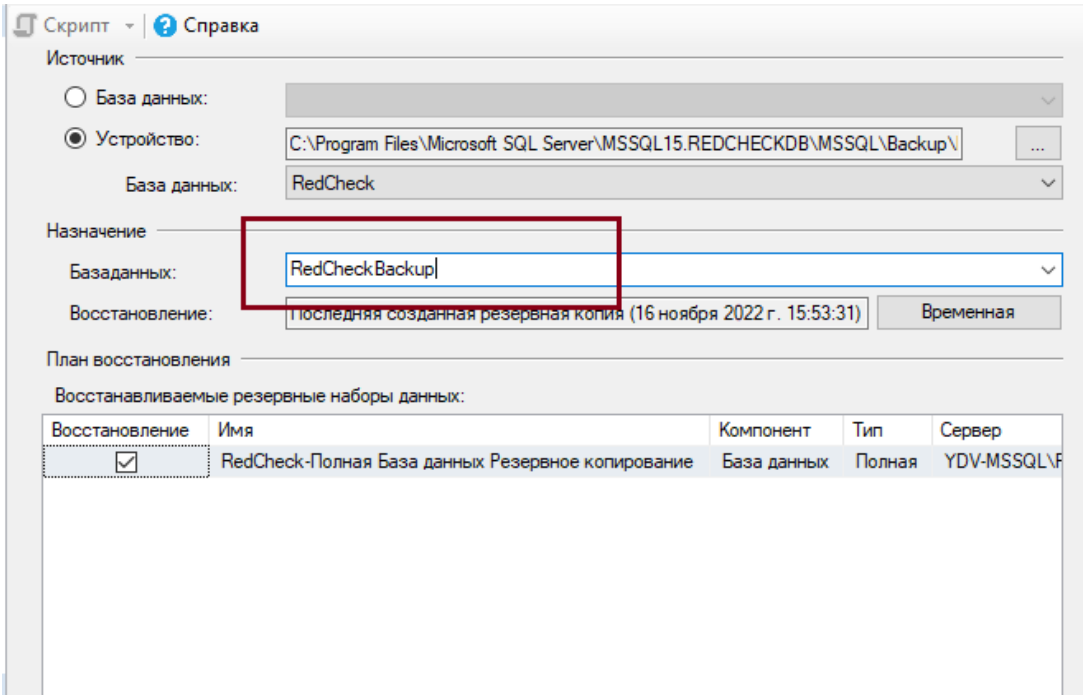
Шаг 2. Отметьте поле **Устройство** → нажмите на кнопку справа для выбора файла резервного копирования;



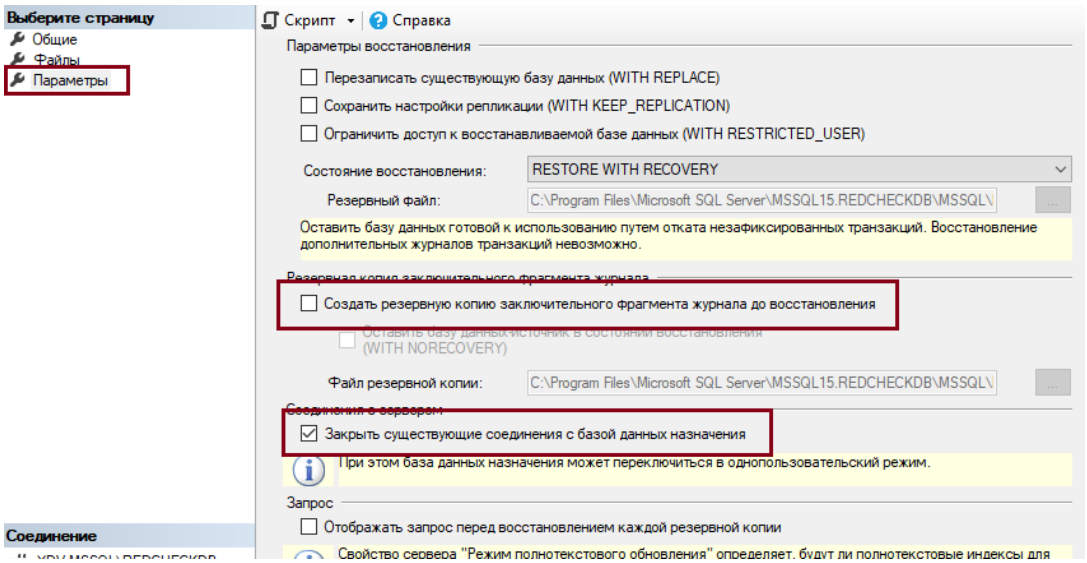
Нажмите **Добавить** → выберите необходимый файл → нажмите **ОК**;



Укажите название для БД;



Шаг 3. Перейдите на страницу **Параметры** и снимите отметку с поля **Создать резервную копию заключительного фрагмента журнала до восстановления**;
отметьте поле **Закрыть существующие соединения с базой данных назначения** → нажмите **ОК**;



После успешного восстановления новая база данных появится в каталоге **Базы данных**.

5.8.2.2 Восстановление PostgreSQL

Если у вас имеется только файл резервного копирования, необходимо сперва установить СУБД PostgreSQL (4.1.2 Установка СУБД PostgreSQL на Windows, 4.1.3 Установка СУБД PostgreSQL на Linux)

Восстановление через терминал

Шаг 1. Войдите под пользователем postgres;

Bash (оболочка Unix)

```
sudo su postgres
```

Шаг 2. Удалите текущую базу данных;

```
Bash (оболочка Unix)
dropdb -U redcheck -f RedCheck
```

-U = имя пользователя, имеющего права для выполнения операции;
-f = принудительный режим удаления БД.

Шаг 3. Создайте новую базу данных;

```
Bash (оболочка Unix)
createdb RedCheck -h 127.0.0.1 -O redcheck -U redcheck
```

-h = listen_address, на котором работает СУБД;
-O = имя владельца БД;
-U = имя пользователя, имеющего права для выполнения операции.

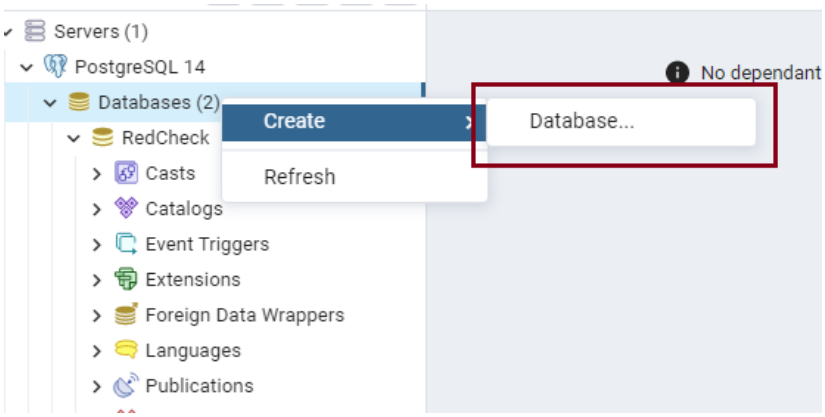
Шаг 4. Восстановите данные;

```
Bash (оболочка Unix)
pg_restore -d RedCheck -h 127.0.0.1 -U redcheck db_dd_mm_yyyy.dump
```

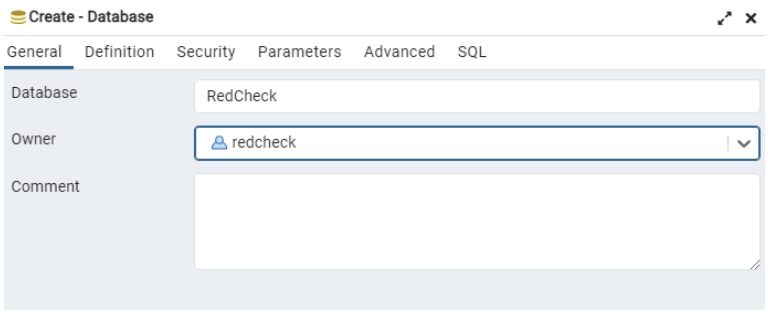
-d = имя базы данных;
-h = listen_address, на котором работает СУБД;
-U = имя пользователя, имеющего права для выполнения операции;
путь к файлу резервной копии.

Восстановление через pgAdmin

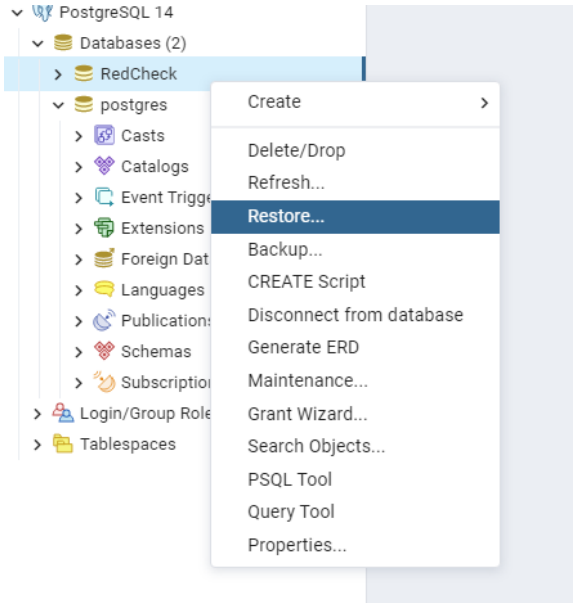
Шаг 1. Создайте новую базу данных. В контекстном меню в директории **Databases** выберите **Create** и нажмите **Database**;



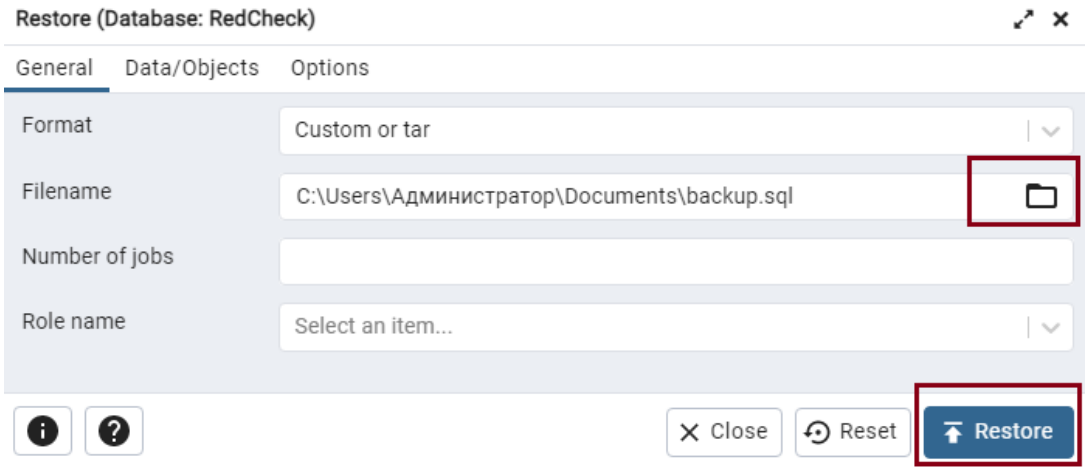
Введите имя и укажите владельца;



Шаг 2. В контекстном меню новой базы данных выберите **Restore**;



Укажите файл резервного копирования и нажмите **Restore**.



5.8.3 Восстановление RedCheck

Перед восстановлением RedCheck на новый сервер убедитесь, что установлены все необходимые компоненты:

- Microsoft .NET Framework 4.8 (4.2.1 Установка Microsoft .NET Framework),

Для Web-версии:

- Web-сервер IIS (4.3.1 Установка Web-сервера IIS),
- Microsoft ASP.NET Core Runtime (4.3.3 Установка Microsoft .NET Core).

Восстановление RedCheck подразумевает под собой подключение к восстановленной из резервной копии БД.

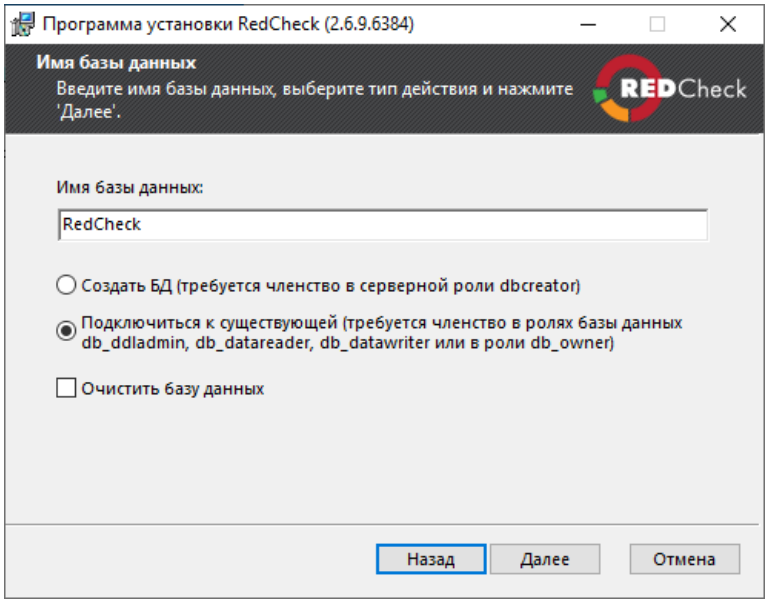
База данных RedCheck для разных версий продукта имеет свою индивидуальную структуру. Резервные копии версий RedCheck ниже 2.6.9 необходимо подключать к соответствующим версиям Системы. При обновлении RedCheck структура базы данных будет изменена до версии дистрибутива. Понижение версии базы данных не поддерживается.

Шаг 1. Произведите установку необходимой версии в следующей последовательности:

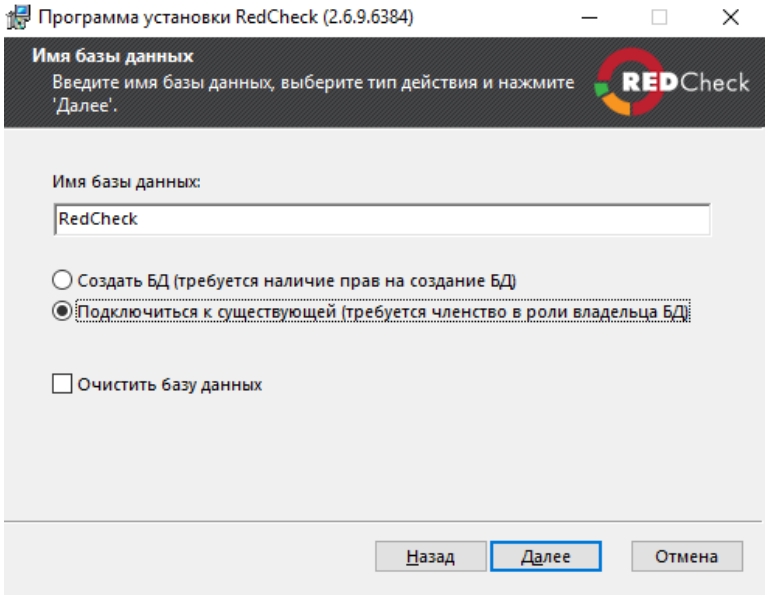
- Для Desktop-версии: 4.2.2 Установка Desktop-версии;
- Для Web-версии: 4.3.4 Установка серверного компонента, 4.3.5 Установка консоли управления, 4.3.8 Установка службы сканирования, 4.3.9 Установка службы синхронизации.

Шаг 2. На шаге **Имя базы данных** укажите **Подключиться к существующей...** → **Далее**;

Microsoft SQL Server



PostgreSQL



5.9 Обновление RedCheck

Начиная с версии RedCheck 2.6.9 возможна установка только одной консоли: или Desktop (монолитный клиент, один пользователь), или Web (клиент-серверная архитектура, несколько пользователей).

Шаг 1. Сделайте резервное копирование БД RedCheck (5.7 Резервное копирование и восстановление);

База данных RedCheck для разных версий продукта имеет свою индивидуальную структуру. Резервные копии версий RedCheck ниже 2.6.9 необходимо подключать к соответствующим версиям Системы. При обновлении RedCheck структура БД будет изменена до версии дистрибутива. Понижение версии базы данных не поддерживается.

Шаг 2. Скачайте с официального сайта разработчика инсталляционные пакеты, исходя из требуемой версии консоли:

- Для Desktop-версии: **RedCheck-X.X.X.XXXX.msi**;
- Для Web-версии: **RedCheckWeb.Rest.Setup-X.X.X.XXXX.msi**, **RedCheckWeb.Client.Setup-X.X.X.XXXX.msi**, **RedCheckSyncService-X.X.X.XXXX.msi**, **RedCheckScanService-X.X.X.XXXX.msi**;

Шаг 3. Удалите компоненты прошлой версии RedCheck:

- Для Desktop-версии: 5.12.1 Удаление Desktop-версии;
- Для Web-версии: 5.12.2.1 Удаление серверного компонента, 5.12.2.2 Удаление консоли управления, 5.12.2.3 Удаление службы сканирования, 5.12.2.4 Удаление службы синхронизации.

Шаг 4. Произведите установку необходимой версии в следующей последовательности:

- Для Desktop-версии: 4.2.2.1 Установка Desktop-версии;
- Для Web-версии: 4.3.4.1 Установка серверного компонента, 4.3.5 Установка консоли управления, 4.3.8.1 Установка службы синхронизации, 4.3.9.1 Установка службы сканирования.

При использовании заданий **Аудит в режиме «Пентест»**, **Обнаружение хостов** обновление ALTXmap для службы сканирования выполняется обязательно.
Рекомендуется обновить агенты сканирования на сканируемых хостах

5.10 Изменение учётной записи для подключения к БД

Содержание

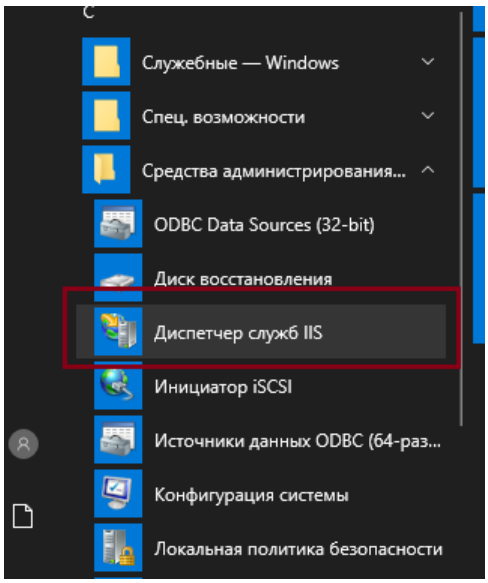
5.10.1 Смена учетной записи для серверного компонента RedCheck

Данная инструкция актуальна только для СУБД Microsoft SQL Server. Если используется авторизация средствами СУБД Microsoft SQL Server / СУБД PostgreSQL, сменить пользователя для подключения к БД возможно только путем переустановки серверного компонента.

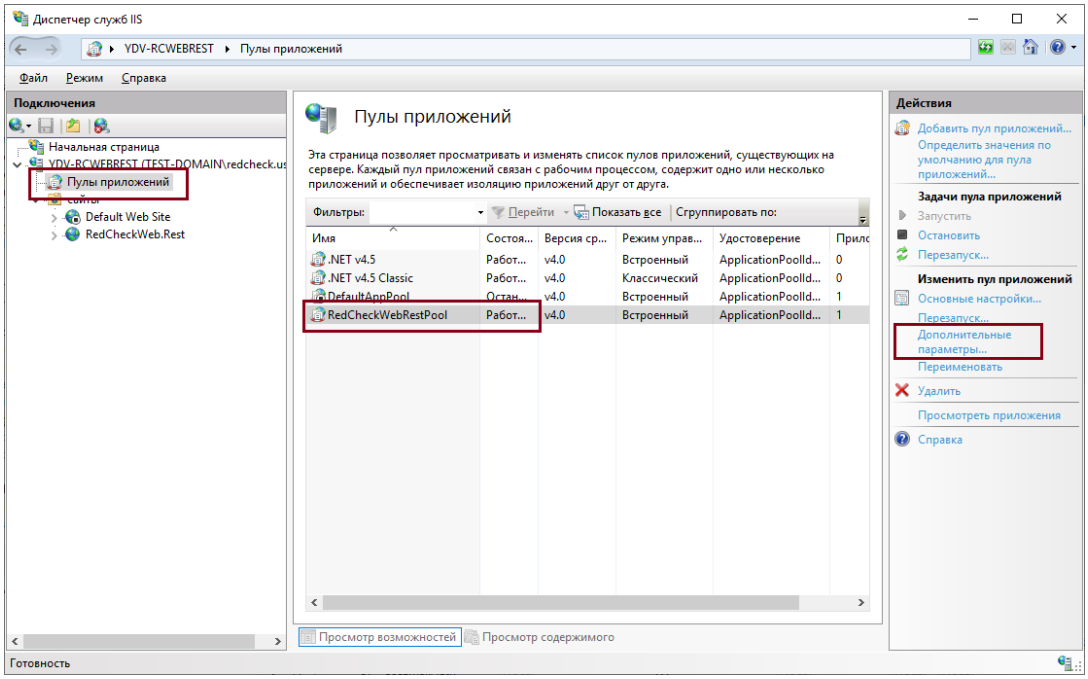
При изменении учетной записи, используемой серверным компонентов для подключения к БД, необходимо указать новые данные для подключения к БД в настройках веб-сервера IIS.

Чтобы сменить учетную запись, выполните следующие шаги:

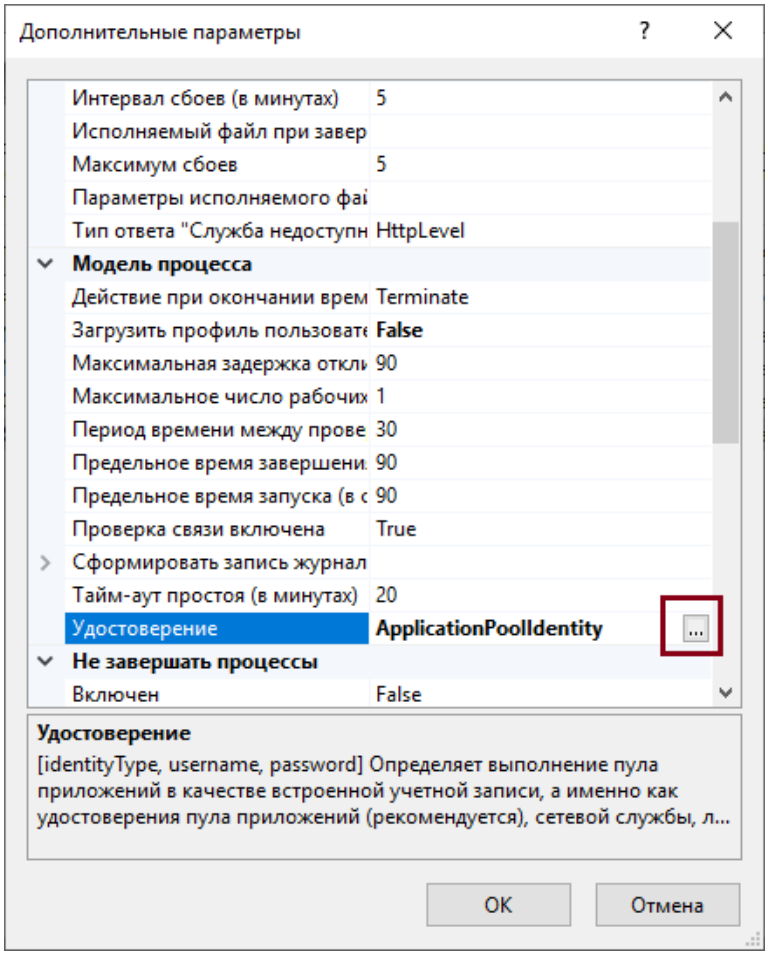
Шаг 1. Откройте Диспетчер служб IIS: **Пуск** → **Средства администрирования Windows** → **Диспетчер служб IIS**;



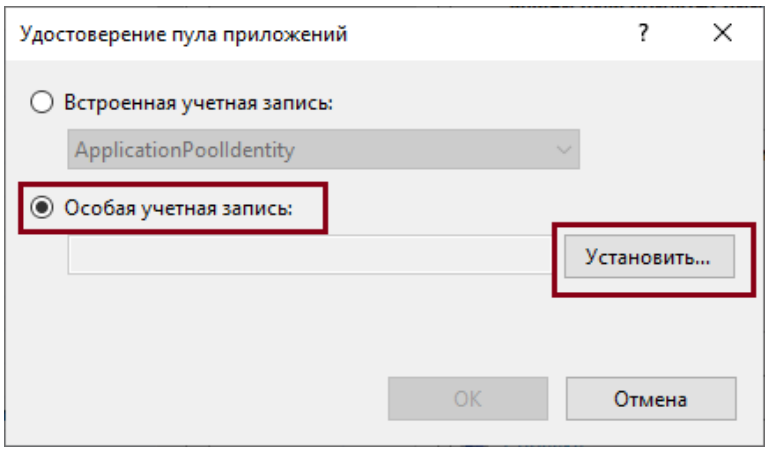
Шаг 2. Перейдите в **Пулы приложений** → **RedCheckWebRestPool** → в меню действий нажмите **Дополнительные параметры**;



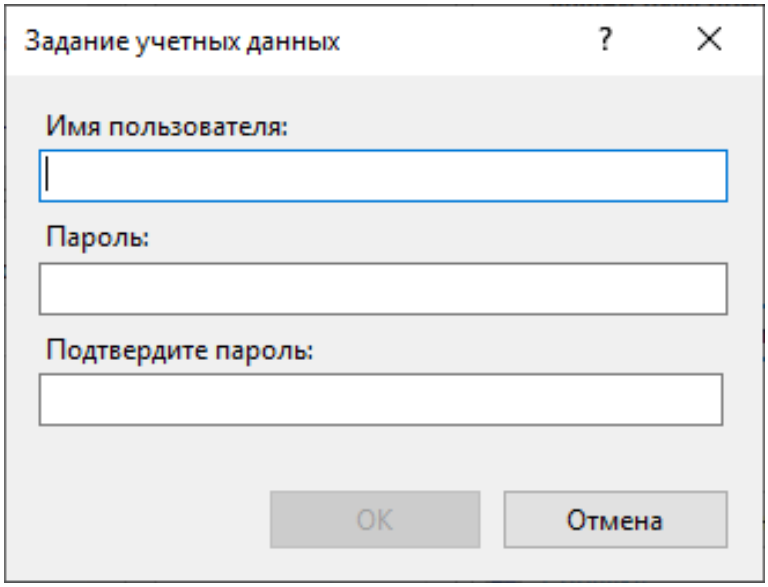
Шаг 3. В **Модель процесса** выберите **Удостоверение** и нажмите на появившуюся кнопку справа;



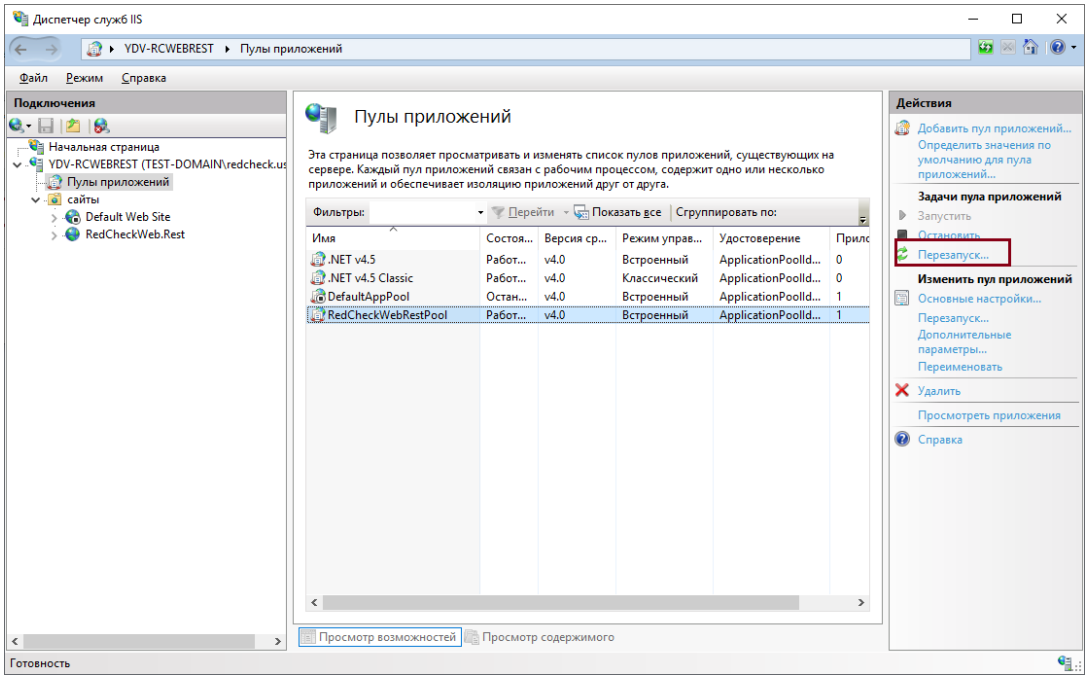
Укажите **Особая учетная запись** → **Установить**;



Введите имя пользователя и новый пароль владельца БД → **ОК**;



Шаг 4. Закройте окно **Доп. параметры** → в меню действий нажмите **Перезапустить**.



5.10.2 Смена данных учетной записи для службы синхронизации RedCheck

При изменении учетных данных пользователя, который имеет доступ к БД, необходимо изменить строку подключения для службы синхронизации.

Чтобы изменить данные в строке подключения, выполните следующие шаги.

Шаг 1. Откройте PowerShell от имени администратора → перейдите в каталог службы синхронизации (по умолчанию **C:\Program Files\ALTEX-SOFT\RedCheckSyncService**)

Шаг 2. С помощью команды **redchecksnc** задайте новую строку подключения к БД:

Для Microsoft SQL Server

Код

```
.\RedCheckSnc configure -c "Data Source=HOSTNAME;Initial
Catalog=DATABASENAME;Integrated Security=True;User
ID=DOMAIN\USERNAME;Password=PASSWORD;MultipleActiveResultSets=True"
```

- Data Source – адрес сервера СУБД;
- Initial Catalog – имя базы данных;
- Integrated Security – использование Windows-аутентификации;
- User ID – (указывается при **Integrated Security=True**) домен\имя пользователя ;
- Password – (указывается при **Integrated Security=True**) пароль;
- MultipleActiveResultSets – включение многопоточного соединения с СУБД;

Для PostgreSQL

Код

```
.\RedCheckSnc configure -c
"Host=localhost;Database=RedCheck;Username=postgres;Password=Password
;Port=5432;Timeout=5"
```

- Host – адрес сервера СУБД;
- Database – имя базы данных;
- Port – (необязательный параметр) порт СУБД;
- Username – имя пользователя;
- Password – пароль;
- Timeout – (необязательный параметр) таймаут для попытки установить соединение;

5.10.3 Смена данных учетной записи для службы сканирования RedCheck

При изменении учетных данных пользователя, который имеет доступ к БД, необходимо изменить строку подключения для службы синхронизации.

Чтобы изменить данные в строке подключения, выполните следующие шаги.

Шаг 1. Откройте PowerShell от имени администратора → перейдите в каталог службы сканирования (по умолчанию **C:\Program Files\ALTEX-SOFT\RedCheckScanService**)

Шаг 2. С помощью команды **redchecksvc** задайте новую строку подключения к БД:

Для Microsoft SQL Server

Код

```
.\RedCheckSnc configure -c "Data Source=HOSTNAME;Initial
Catalog=DATABASENAME;Integrated Security=True;User
ID=DOMAIN\USERNAME;Password=PASSWORD;MultipleActiveResultSets=True"
```

- Data Source – адрес сервера СУБД;
- Initial Catalog – имя базы данных;
- Integrated Security – использование Windows-аутентификации;
- User ID – (указывается при **Integrated Security=True**) домен\имя пользователя;
- Password – (указывается при **Integrated Security=True**) пароль;
- MultipleActiveResultSets – включение многопоточного соединения с СУБД;

Для PostgreSQL

Код

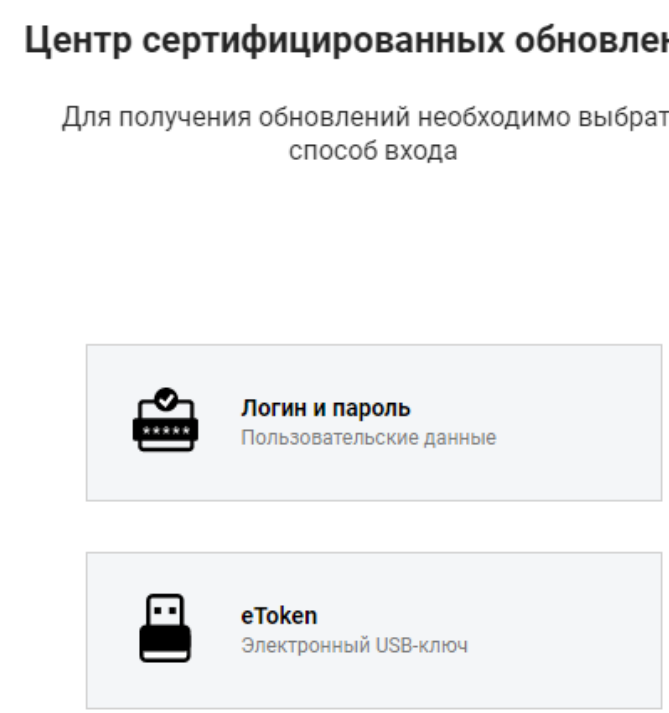
```
.\RedCheckSvc configure -c
"Host=localhost;Database=RedCheck;Username=postgres;Password=Password
;Port=5432;Timeout=5"
```

- Host – адрес сервера СУБД;
- Database – имя базы данных;
- Port – (необязательный параметр) порт СУБД;
- Username – имя пользователя;
- Password – пароль;
- Timeout – (необязательный параметр) таймаут для попытки установить соединение;

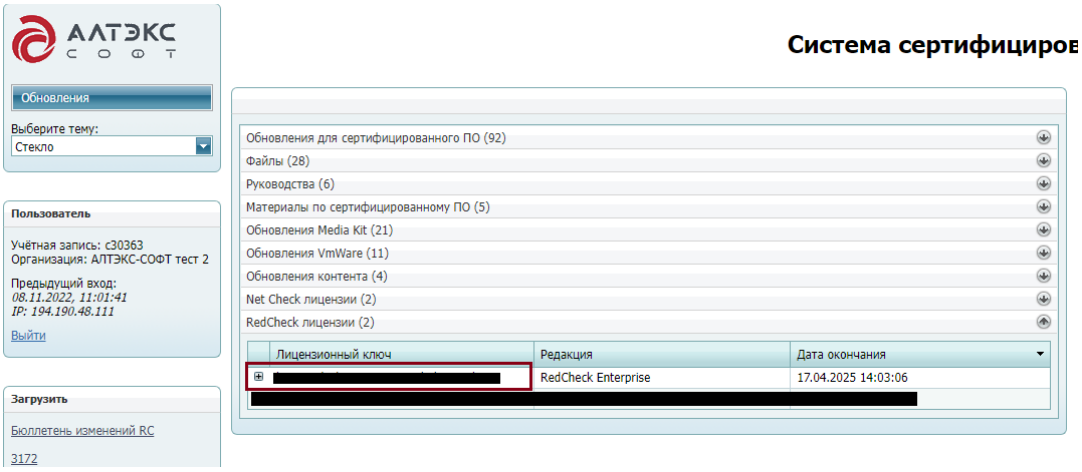
5.11 Сброс привязки лицензии

Шаг 1. Авторизуйтесь в Центре сертифицированных обновлений с помощью логина и пароля;

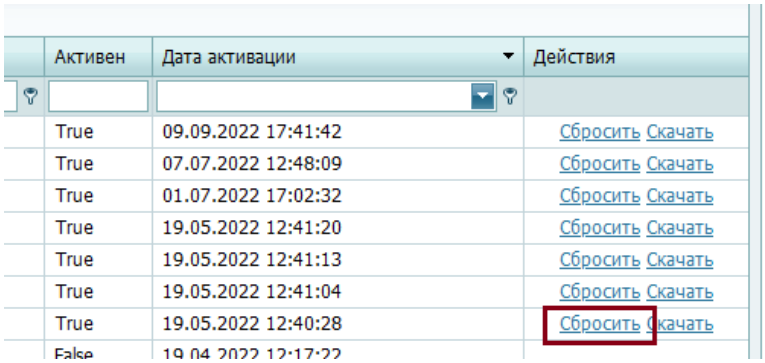
Логин/пароль поставляется всем коммерческим клиентам на последней странице формуляра (начиная с 18.05.2022).



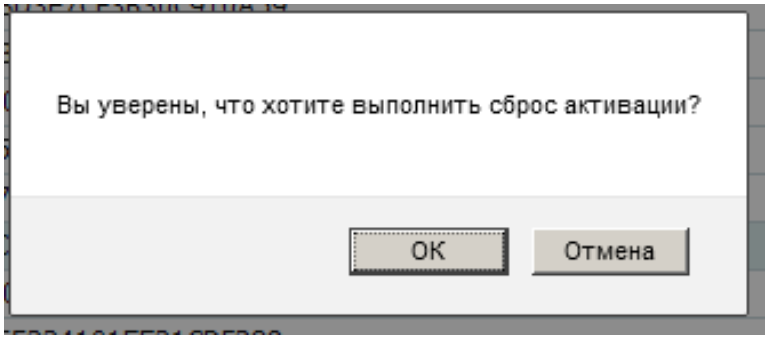
Шаг 2. Раскройте **RedCheck лицензии** → нажмите на интересующий Вас номер ключа RedCheck;



Шаг 3. Нажмите **Сбросить** в столбце **Действия**;

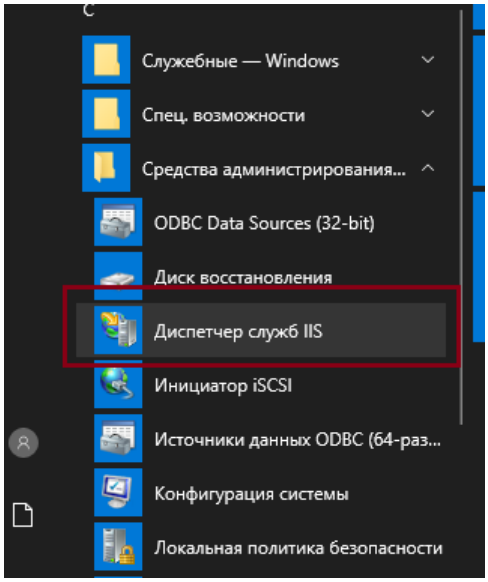


Шаг 4. Нажмите **ОК**.

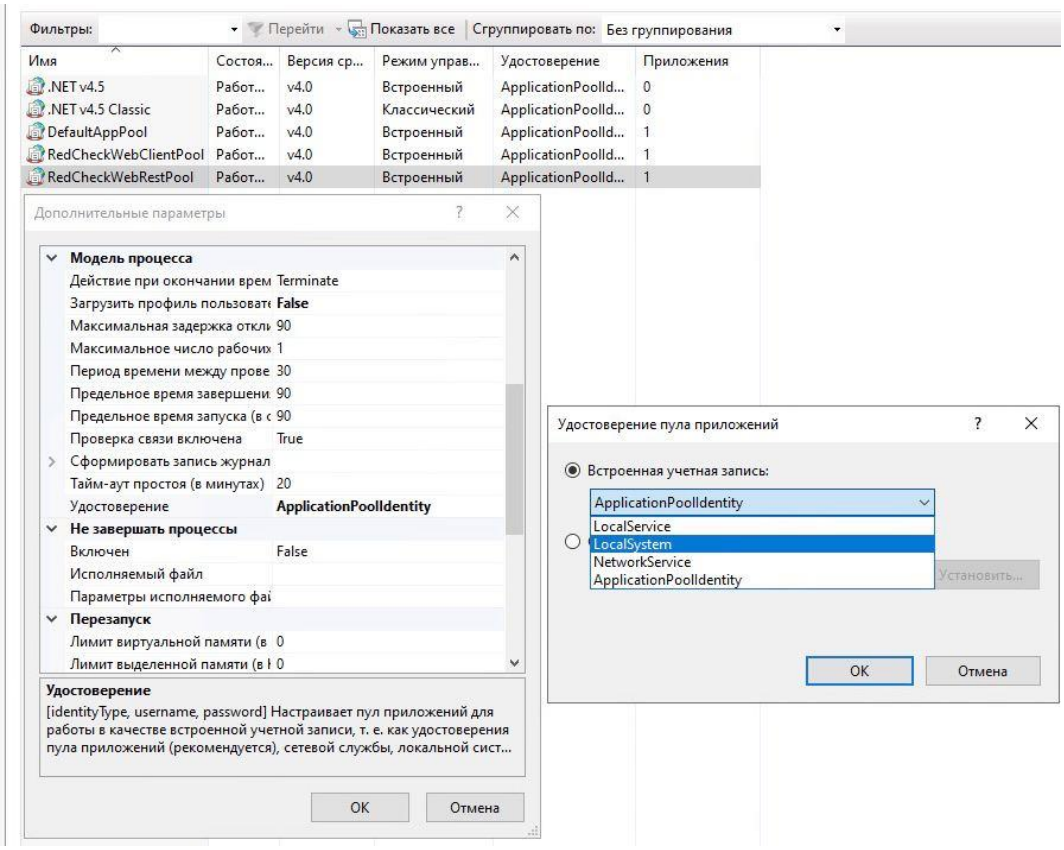


5.12 Смена лицензионного ключа

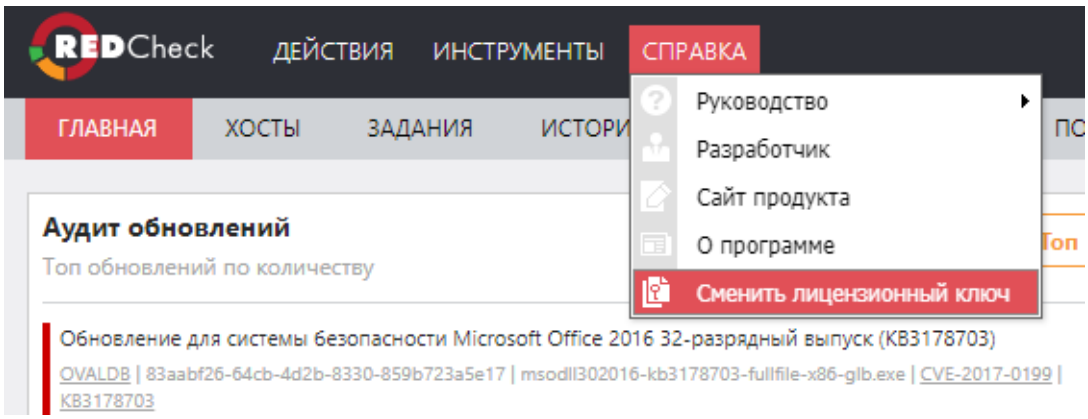
Шаг 1. Откройте Диспетчер служб IIS: **Пуск → Средства администрирования Windows → Диспетчер служб IIS**;



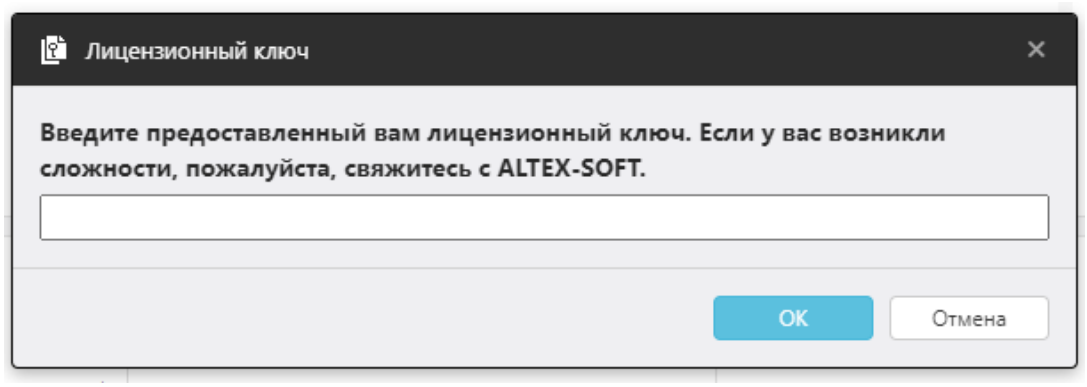
Шаг 2. Перейдите в **Пулы приложений → RedCheckWebRestPool →** в меню действий нажмите **Дополнительные параметры → Удостоверение → Удостоверение пула приложений → Встроенная учетная запись →** выберите **LocalSystem**;



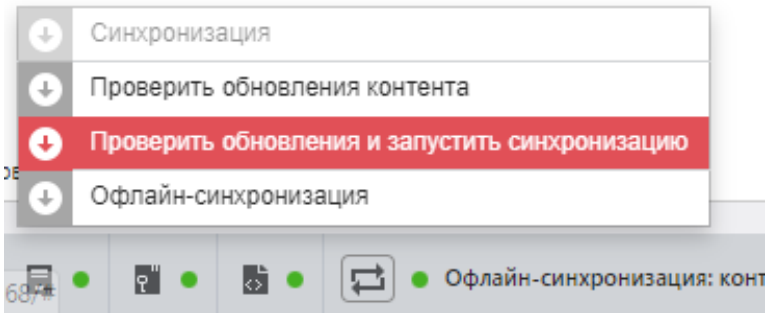
Шаг 3. Откройте консоль управления RedCheck, авторизовавших под учетной записью с ролью RedCheck_Admins → **Справка** → **Сменить лицензионный ключ**;



Шаг 4. Введите новый лицензионный ключ → **ОК**;



Шаг 5. Выполните синхронизацию (5.3 Обновление контента информационной безопасности).



Шаг 6. Верните прежние настройки для пула **RedCheckWebRestPool**;

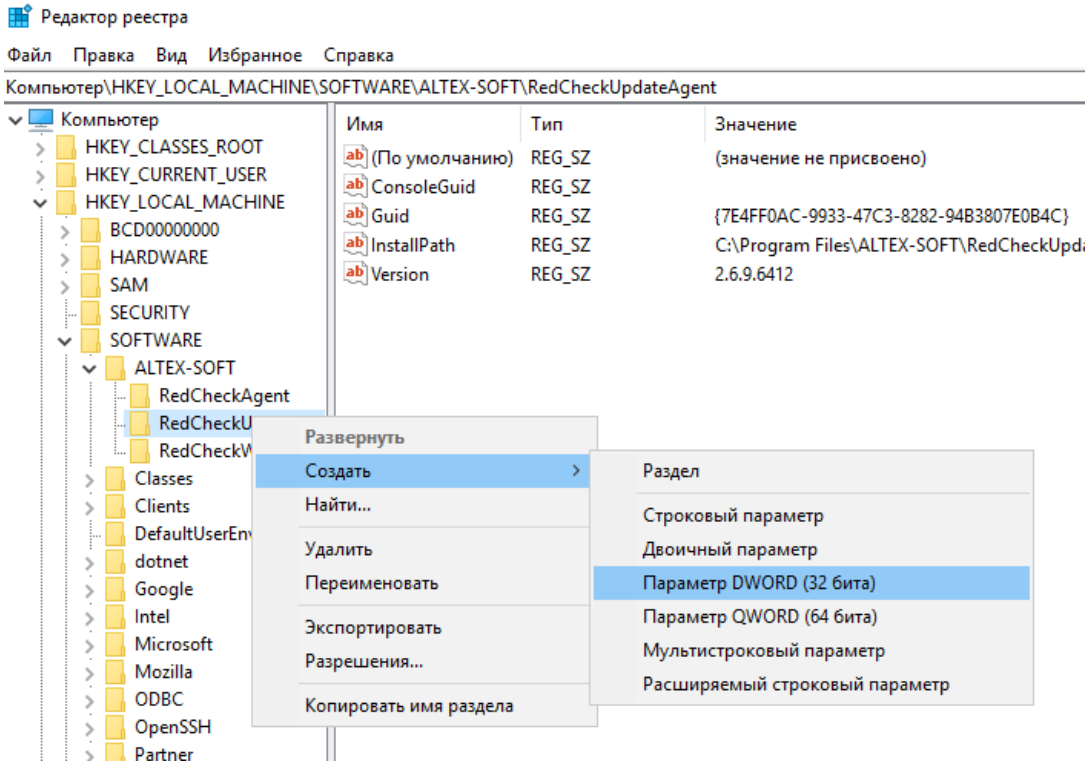
Содержание

5.13.1 Агент обновления

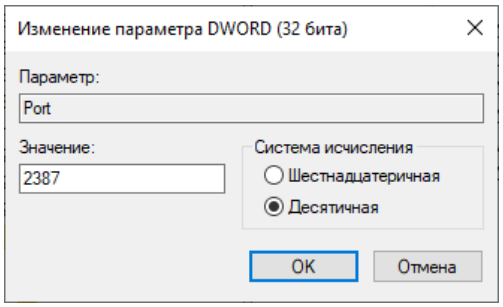
Стандартный порт Update Агента **TCP/IP 8733**.

Шаг 1. Зайдите в реестр хоста с установленным агентом и создайте новый параметр **DWORD** с именем **Port**;

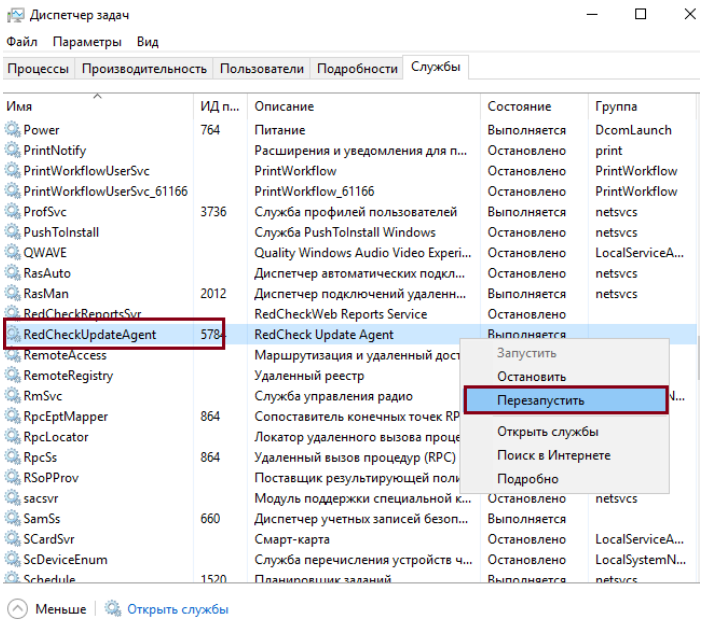
Для x-86 разрядных систем: **HKEY_LOCAL_MACHINE\ SOFTWARE\ Wow6432Node\ ALTEX-SOFT\ RedCheckUpdateAgent\ Port (DWORD)**
Для x-64 разрядных систем: **HKEY_LOCAL_MACHINE\ SOFTWARE\ ALTEX-SOFT\ RedCheckUpdateAgent\ Port (DWORD)**



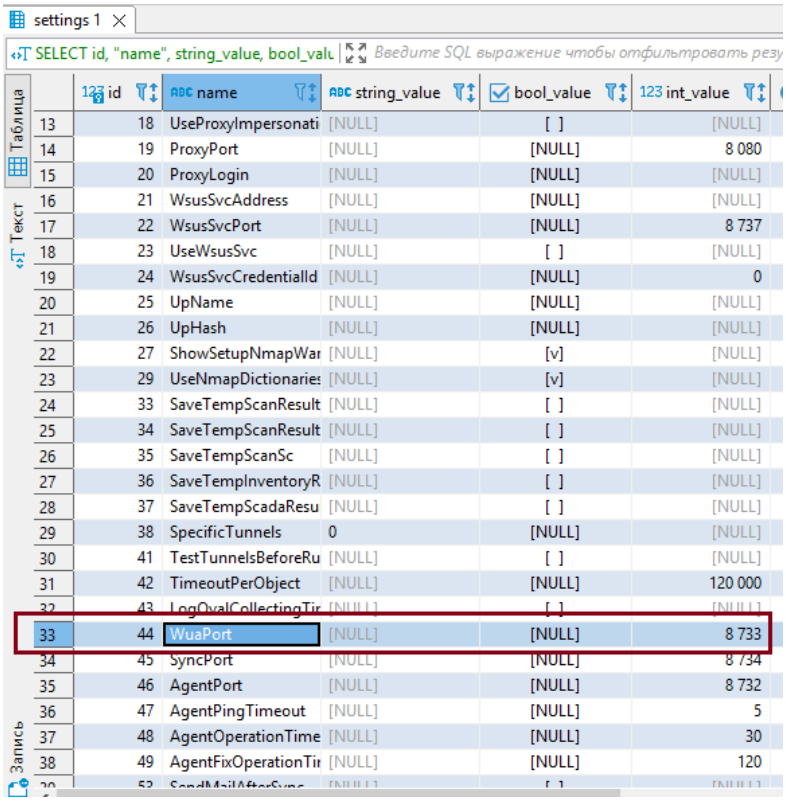
Присвойте ему необходимое значение → **OK**;



Шаг 2. Нажмите **Ctrl + Alt + Delete** → **Диспетчер задач**. Перейдите в **Службы** → ПКМ по **RedCheckUpdateAgent** → **Перезапустить**;



Шаг 3. В БД RedCheck найдите таблицу **settings** → в столбце **name** найдите поле **WuaPort** и внесите новое значение порта;



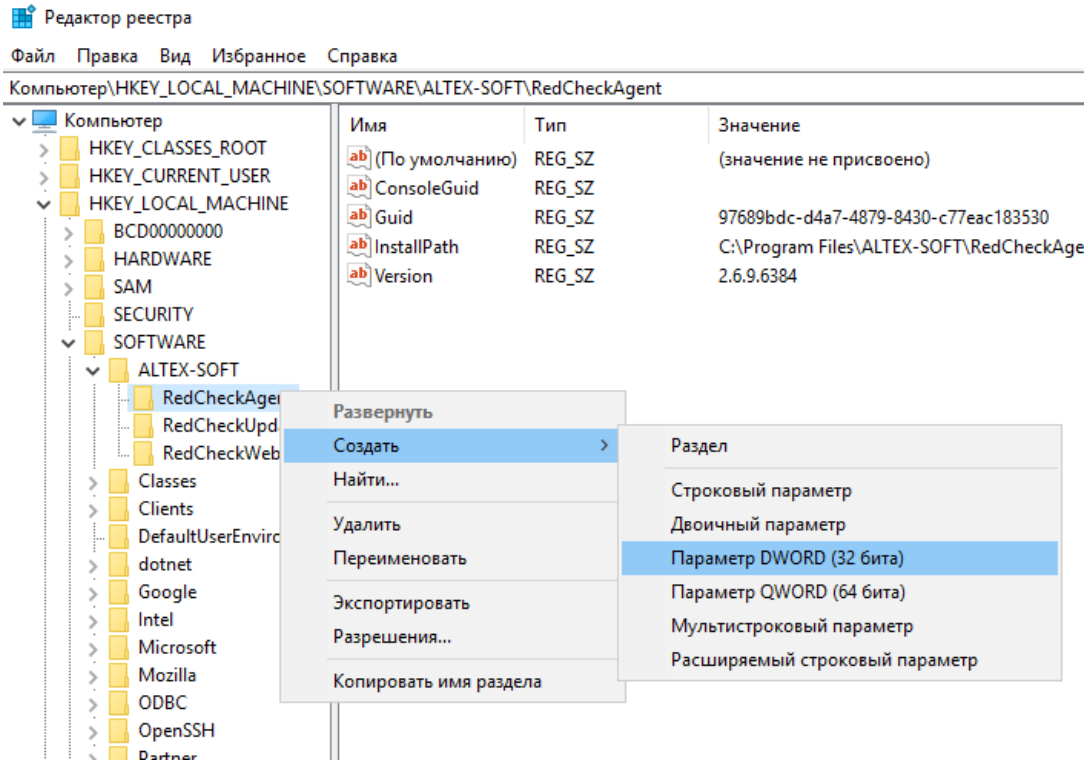
Шаг 4. Перезагрузите службу агента обновления, выполнив аналогичные действия из шага 2.

5.13.2 Агент сканирования

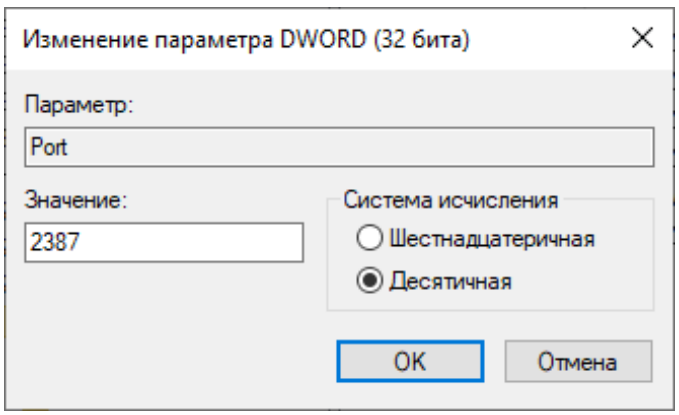
Стандартный порт Агента **TCP/IP 8732**.

Шаг 1. Зайдите в реестр хоста с установленным агентом и создайте новый параметр **DWORD** с именем **Port**;

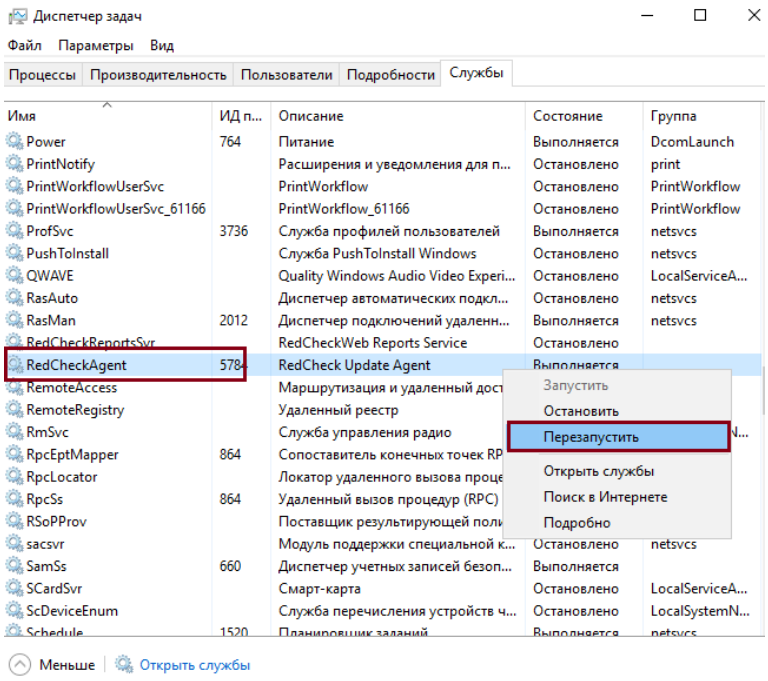
Для x-86 разрядных систем: **HKEY_LOCAL_MACHINE\ SOFTWARE\ Wow6432Node\ ALTEX-SOFT\ RedCheckAgent\ Port (DWORD)**
Для x-64 разрядных систем: **HKEY_LOCAL_MACHINE\ SOFTWARE\ ALTEX-SOFT\ RedCheckAgent\ Port (DWORD) D)**



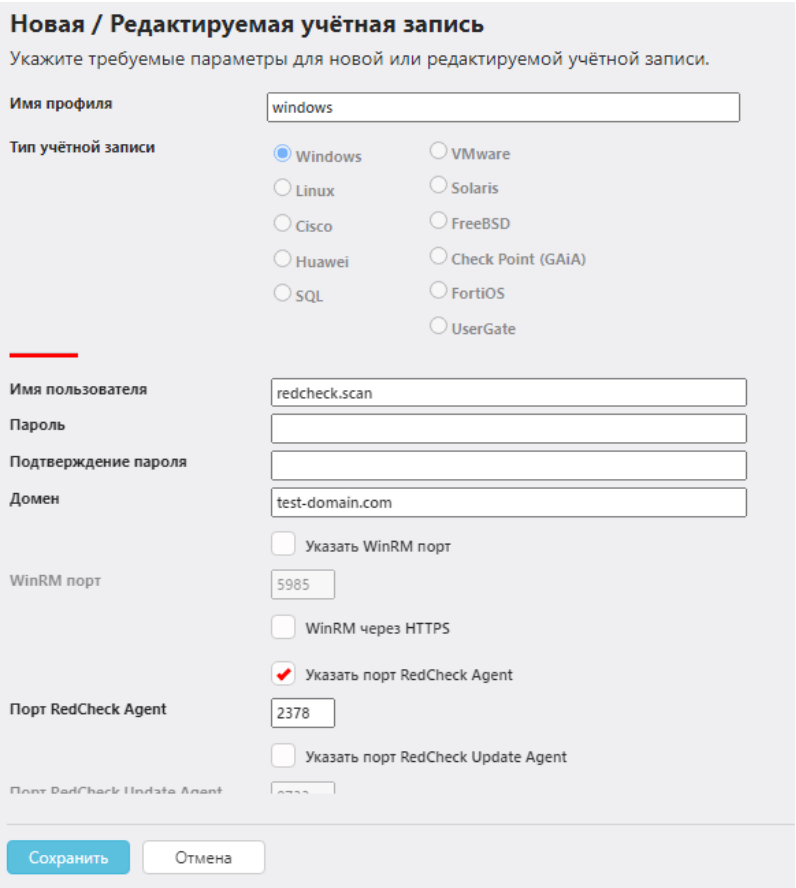
Присвойте ему необходимое значение → **OK**;



Шаг 2. Нажмите **Ctrl + Alt + Delete** → **Диспетчер задач**. Перейдите в **Службы** → ПКМ по **RedCheckAgent** → **Перезапустить**;



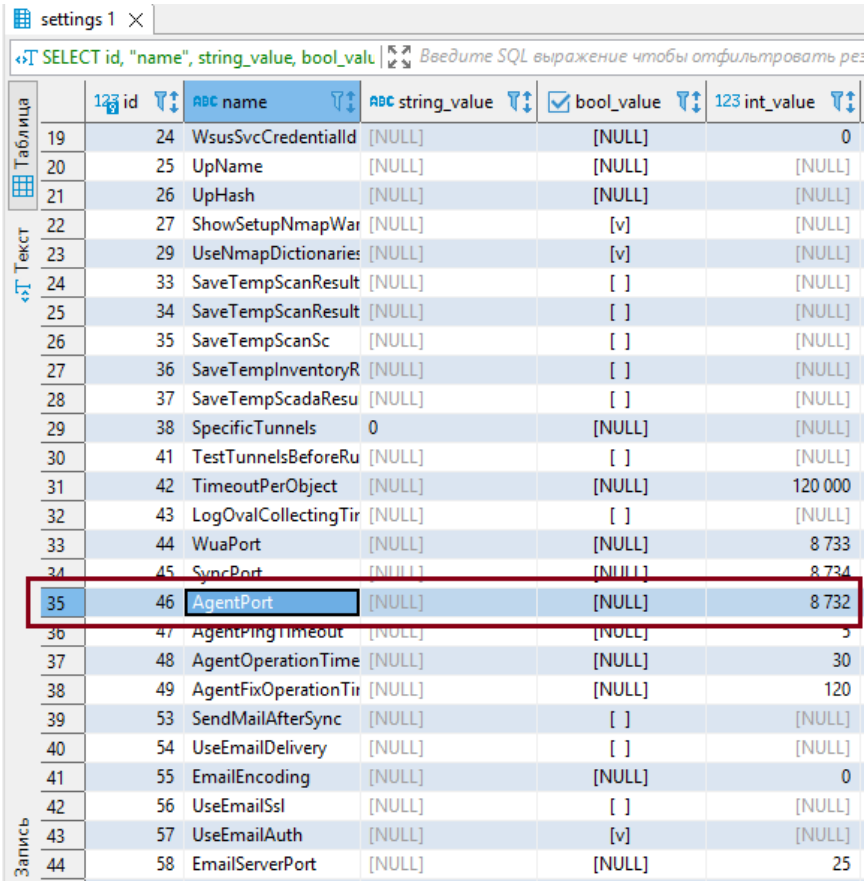
Для сканирования сегмента сети, в которой для Агента установлен альтернативный порт, используется учетная запись RedCheck с указанием переопределенного порта по умолчанию.



Изменение порта по умолчанию

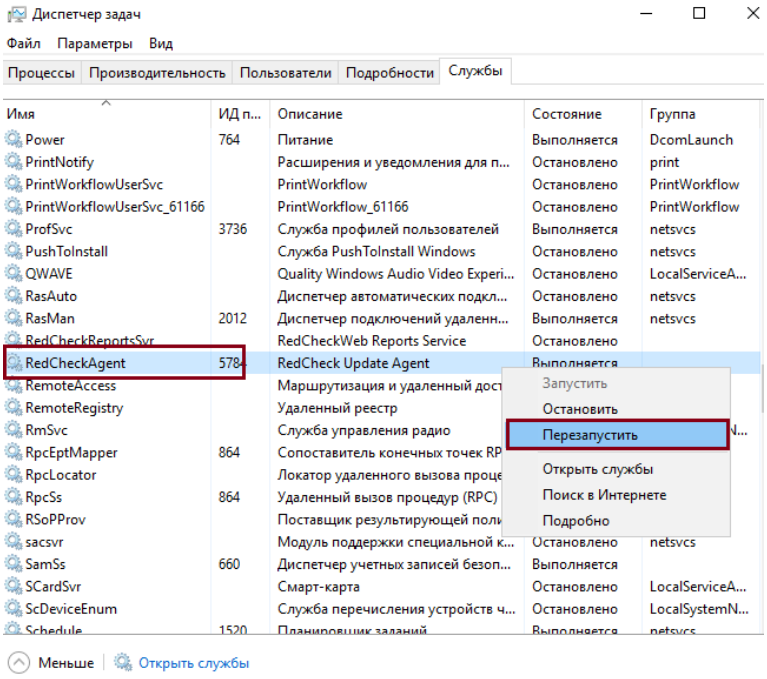
Порт по умолчанию используется для сканирования в тех случаях, когда не указано альтернативное значение в УЗ RedCheck.

Шаг 1. В БД RedCheck найдите таблицу **settings** → в столбце **name** найдите поле **AgentPort** и внесите новое значение порта;



	id	name	string_value	bool_value	int_value
19	24	WsusSvcCredentialId	[NULL]	[NULL]	0
20	25	UpName	[NULL]	[NULL]	[NULL]
21	26	UpHash	[NULL]	[NULL]	[NULL]
22	27	ShowSetupNmapWar	[NULL]	[v]	[NULL]
23	29	UseNmapDictionaries	[NULL]	[v]	[NULL]
24	33	SaveTempScanResult	[NULL]	[ ]	[NULL]
25	34	SaveTempScanResult	[NULL]	[ ]	[NULL]
26	35	SaveTempScanSc	[NULL]	[ ]	[NULL]
27	36	SaveTempInventoryR	[NULL]	[ ]	[NULL]
28	37	SaveTempScadaResu	[NULL]	[ ]	[NULL]
29	38	SpecificTunnels	0	[NULL]	[NULL]
30	41	TestTunnelsBeforeRu	[NULL]	[ ]	[NULL]
31	42	TimeoutPerObject	[NULL]	[NULL]	120 000
32	43	LogOvalCollectingTir	[NULL]	[ ]	[NULL]
33	44	WuaPort	[NULL]	[NULL]	8 733
34	45	SyncPort	[NULL]	[NULL]	8 734
35	46	AgentPort	[NULL]	[NULL]	8 732
36	47	AgentPingTimeout	[NULL]	[NULL]	5
37	48	AgentOperationTime	[NULL]	[NULL]	30
38	49	AgentFixOperationTir	[NULL]	[NULL]	120
39	53	SendMailAfterSync	[NULL]	[ ]	[NULL]
40	54	UseEmailDelivery	[NULL]	[ ]	[NULL]
41	55	EmailEncoding	[NULL]	[NULL]	0
42	56	UseEmailSsl	[NULL]	[ ]	[NULL]
43	57	UseEmailAuth	[NULL]	[v]	[NULL]
44	58	EmailServerPort	[NULL]	[NULL]	25

Шаг 2. Нажмите **Ctrl + Alt + Delete** → **Диспетчер задач**. Перейдите в **Службы** → ПКМ по **RedCheckAgent** → **Перезапустить**;

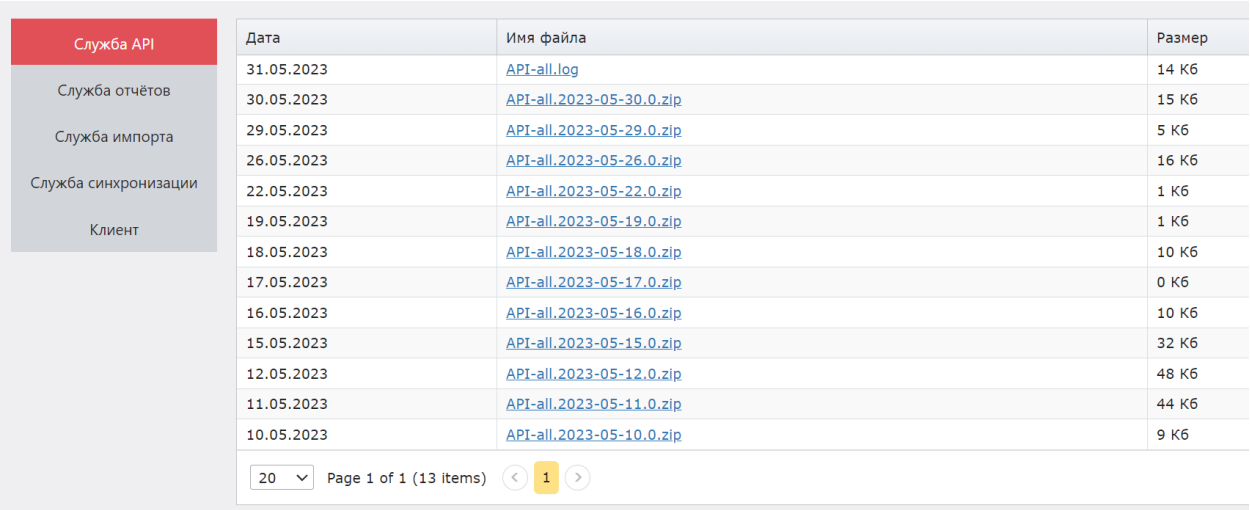


5.14 Журнал событий (логи)

Раскройте **Инструменты → Журнал событий**;

Из консоли управления можно скачать логи следующих основных компонентов RedCheck:

- Серверный компонент REST API (Служба API);
- Служба синхронизации;
- Консоль управления (Клиент).

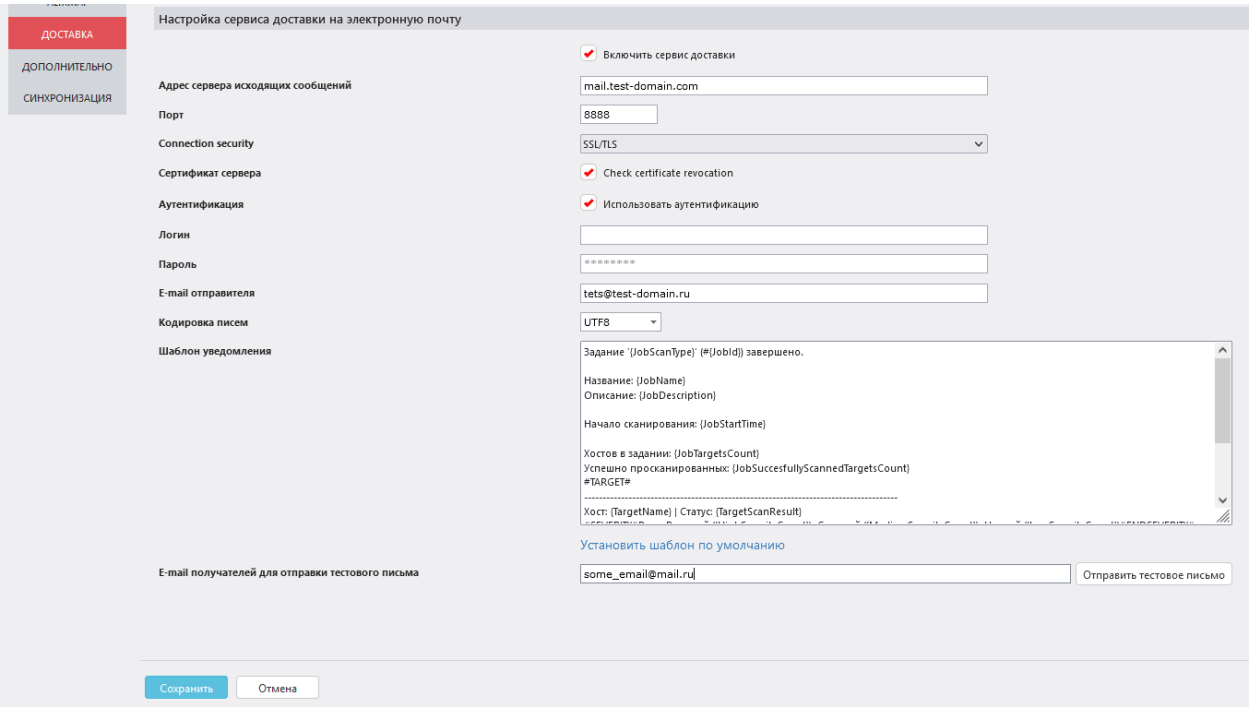


Логи службы сканирования находятся на сервере, где установлена служба, по следующему пути: C:\ProgramData\ALTEX-SOFT\RedCheck\Logs\SVC.

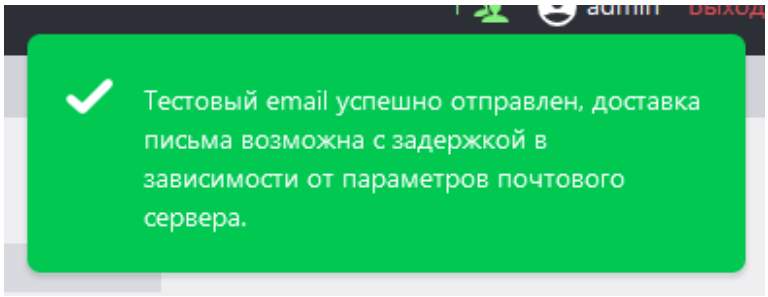
Для сбора расширенных журналов событий воспользуйтесь следующей инструкцией.

5.15 Настройка сервиса доставки отчетов

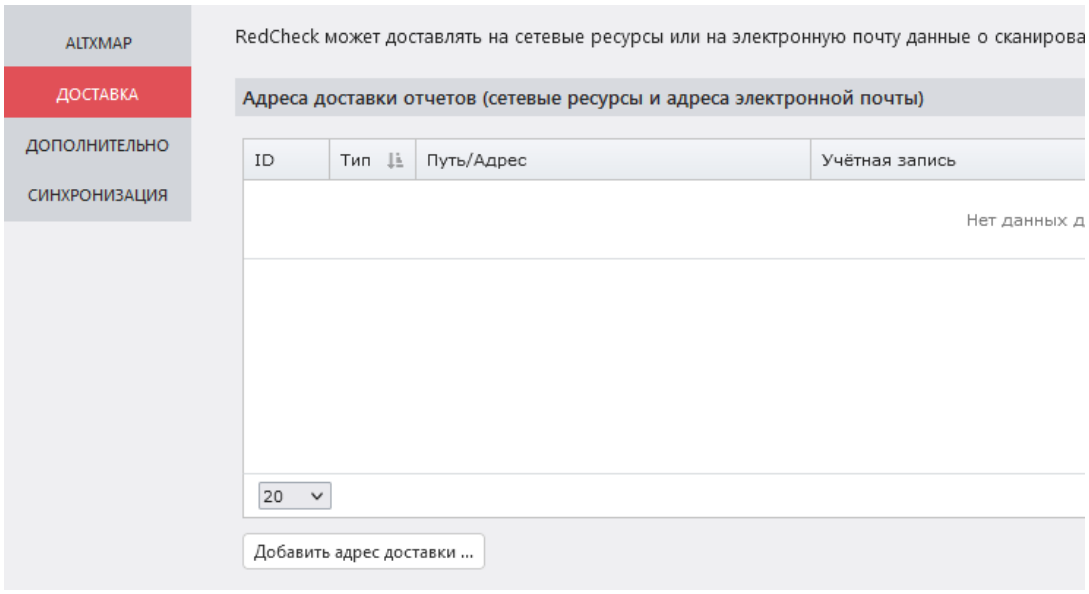
Шаг 1. Раскройте **Инструменты** → **Настройки** → перейдите в **Доставка** → в разделе **Настройка сервиса доставки на электронную почту** отметьте **Включить сервис доставки**;



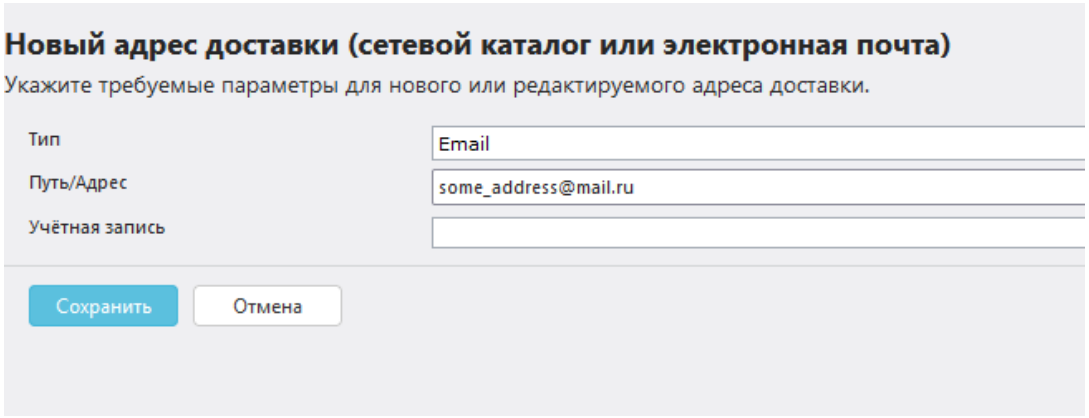
Шаг 2. Укажите необходимые данные для отправки писем → нажмите **Отправить тестовое письмо** для проверки;



Шаг 3. Чтобы добавить email, нажмите **Добавить адрес доставки**;



Шаг 4. Укажите **Тип** адреса доставки **Email** и адрес почты в поле **Путь/Адрес**→ **Сохранить**;



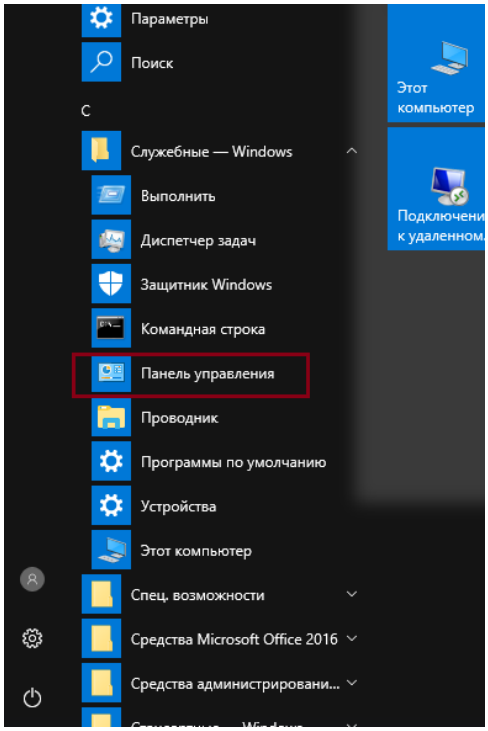
Для отправки отчетов на почту после завершения задания необходимо создать шаблон отчетов.

Содержание

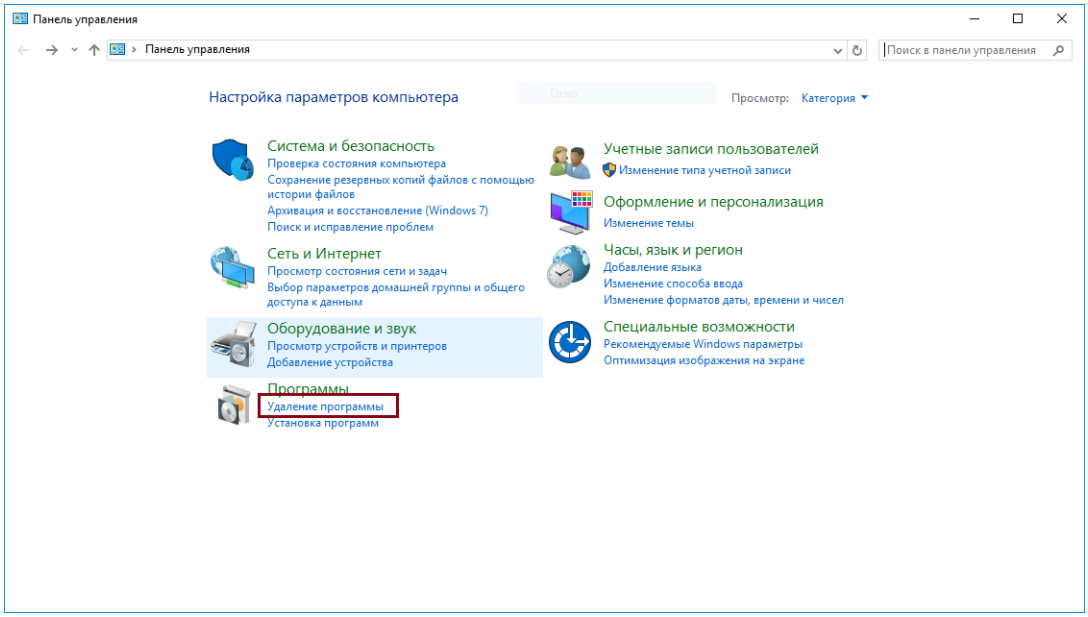
5.16.1 Удаление Desktop-версии

Удаление RedCheck стандартными средствами Microsoft Windows

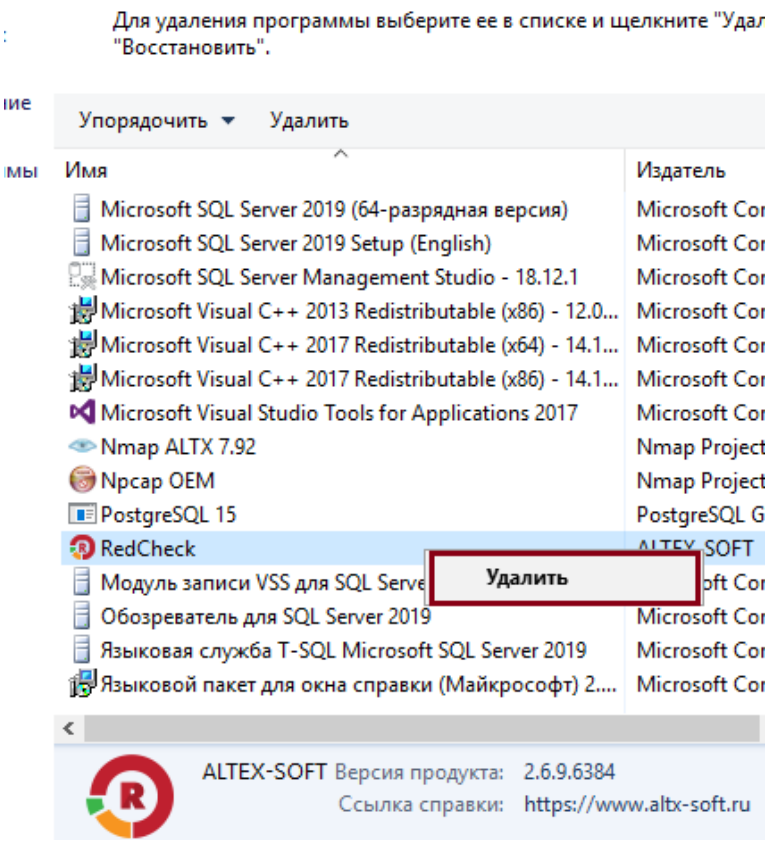
Шаг 1. Пуск → Служебные - Windows → Панель управления;



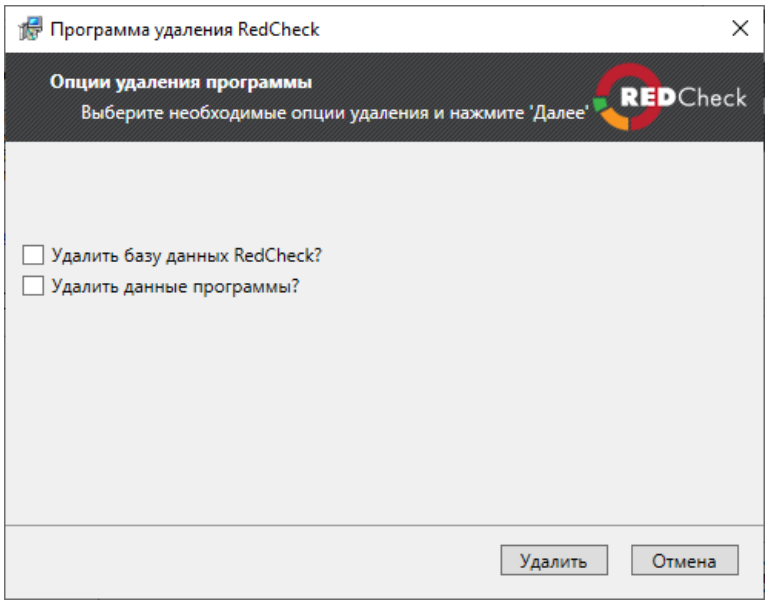
Шаг 2. Откройте утилиту **Удаление программ**;



Шаг 3. ПКМ по **RedCheck** → **Удалить**;

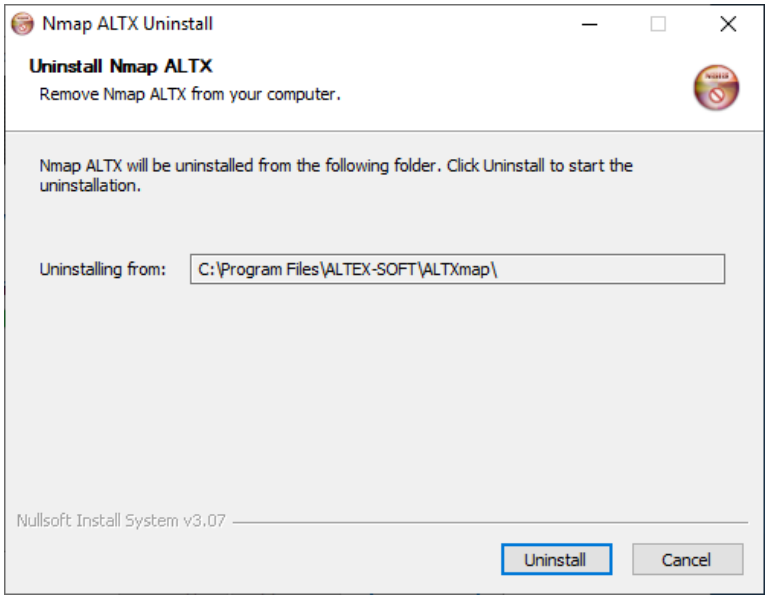


Шаг 4. Отметьте необходимые для удаления данные → **Удалить**;



Под данными программы подразумеваются логи работы RedCheck.msi

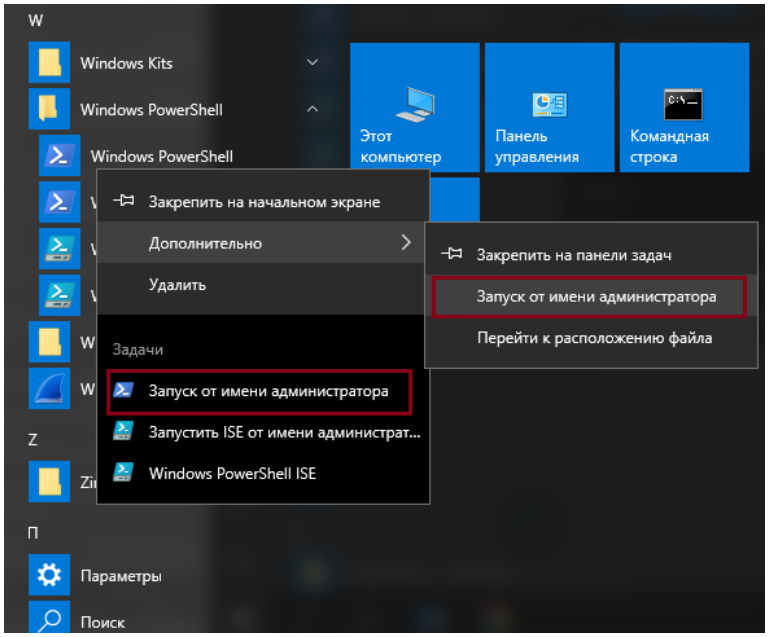
Нажмите **Uninstall** в окне деинсталлятора **Nmap ALTX**.



Удаление RedCheck через командную строку

Для данного способа деинсталляции необходим установочный пакет RedCheck.

Шаг 1. Пуск → Windows PowerShell → ПКМ по **Windows PowerShell** → **Запуск от имени администратора**;



Шаг 2. Введите команду для удаления:

Код

```
msiexec /x "<путь_к_установщику.msi>" /qn NEED_REMOVE_DATABASE=0
```

Параметр **NEED_REMOVE_DATABASE** определяет, будет удалена база данных RedCheck или нет (Значение 0 - Нет, 1 - Да).

/q[n, b, f] – параметр отображения пользовательского интерфейса:
n – без интерфейса;
b – основной интерфейс (индикатор удаления);
f – полный интерфейс (по умолчанию);

Шаг 3. Проверьте работу деинсталлятора. При успешном удалении директория RedCheck будет отсутствовать (по умолчанию Система находится по адресу C:\Program Files\ALTEX-SOFT).

5.16.2 Удаление Web-версии

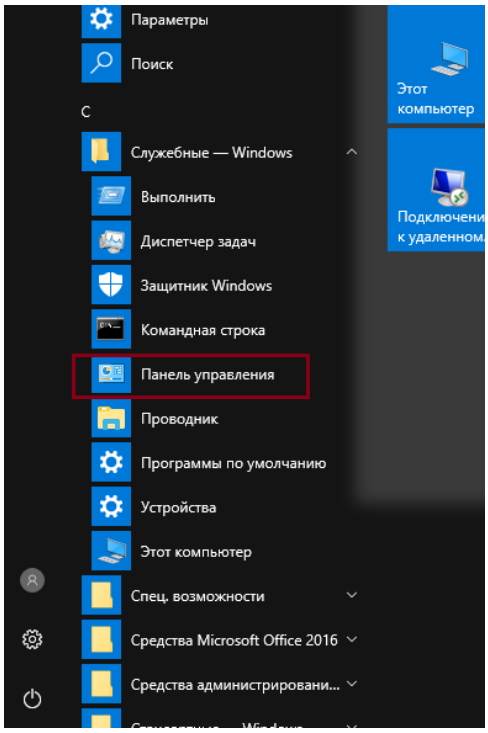
Для полного удаления Web-версии RedCheck необходимо деинсталлировать каждый компонент отдельно.

Содержание

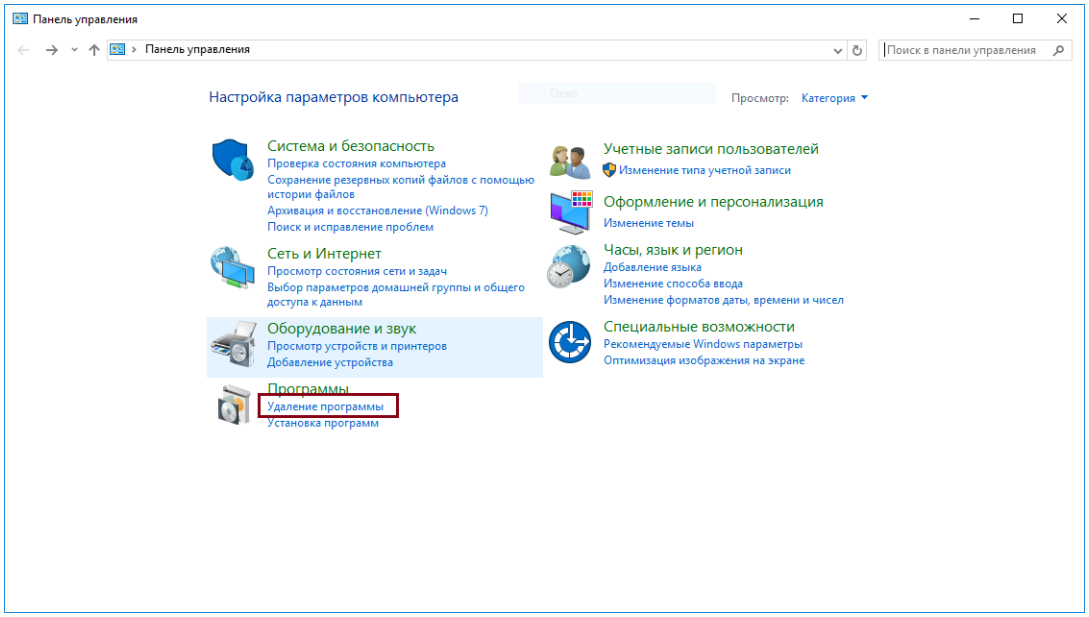
5.16.2.1 Удаление серверного компонента

Удаление серверного компонента RedCheck стандартными средствами Microsoft Windows

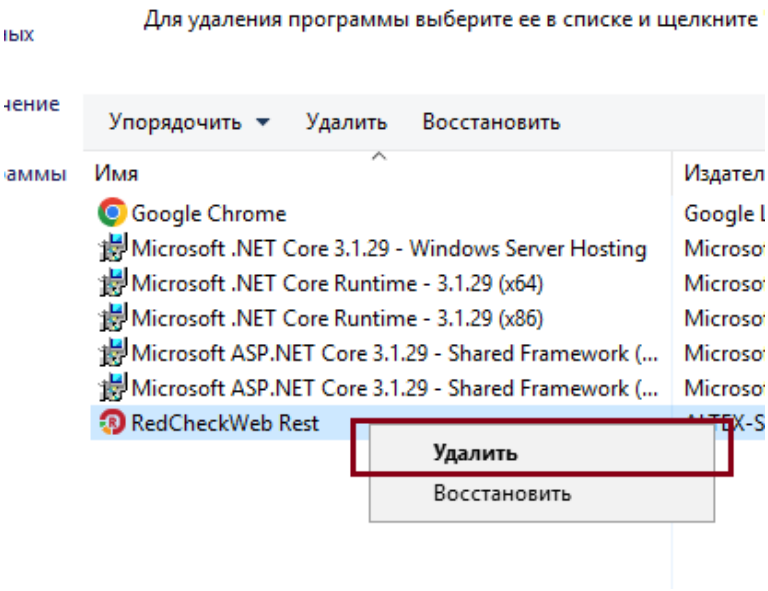
Шаг 1. Пуск → Служебные - Windows → Панель управления;



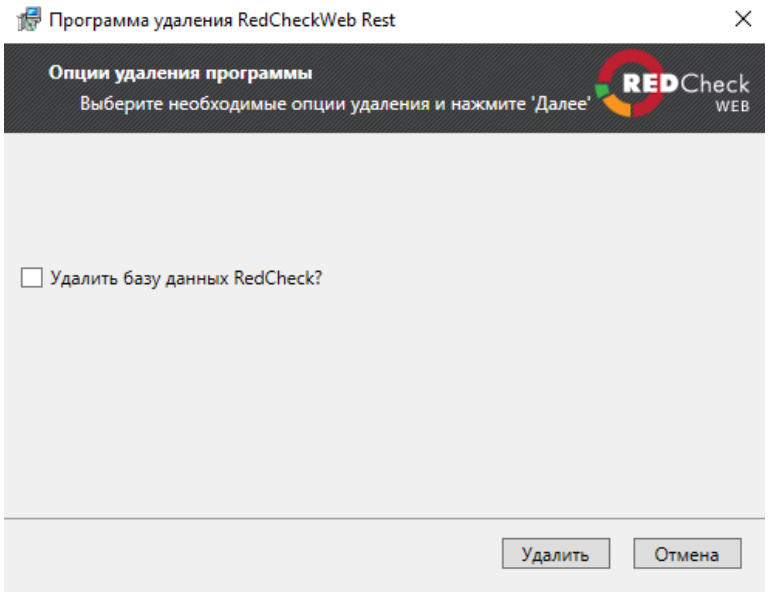
Шаг 2. Откройте утилиту **Удаление программ**;



Шаг 3. ПКМ по **RedCheckWeb Rest** → **Удалить**;



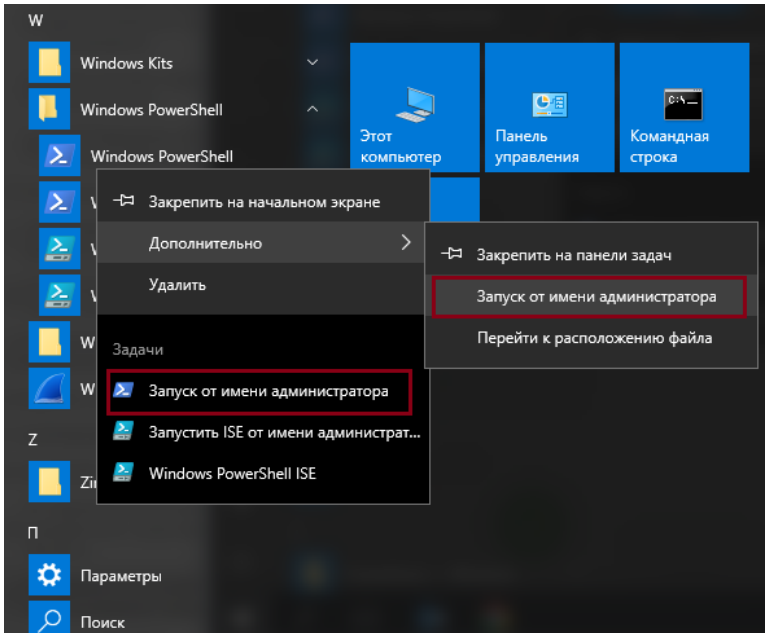
Шаг 4. Отметьте по необходимости **Удалить базу данных RedCheck → Удалить**;



Удаление серверного компонента RedCheck через командную строку

Для данного способа деинсталляции необходим установочный пакет RedCheckWeb.Rest.msi

Шаг 1. Пуск → Windows PowerShell → ПКМ по **Windows PowerShell → Запуск от имени администратора**;



Шаг 2. Введите команду для удаления:

Код

```
msiexec /x "<путь_к_установщику.msi>" /qn NEED_REMOVE_DATABASE=0
```

Параметр **NEED_REMOVE_DATABASE** определяет, будет удалена база данных RedCheck или нет (Значение 0 - Нет, 1 - Да).

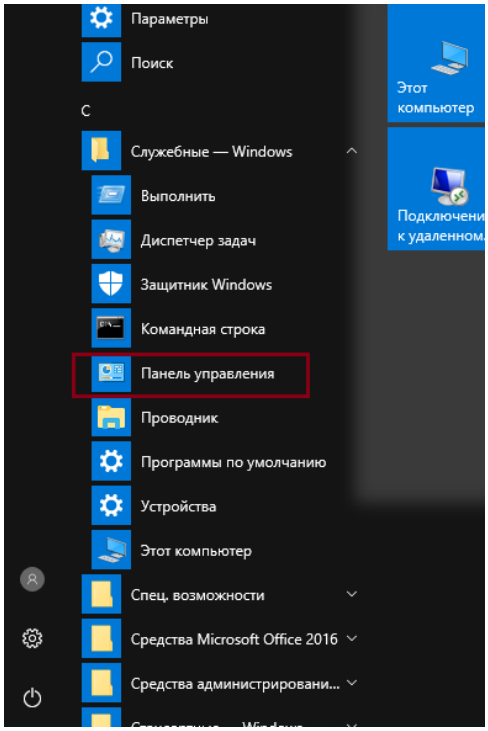
/q[n, b, f] – параметр отображения пользовательского интерфейса:
n – без интерфейса;
b – основной интерфейс (индикатор удаления);
f – полный интерфейс (по умолчанию);

Шаг 3. Проверьте работу деинсталлятора. При успешном удалении директория соответствующего компонента будет отсутствовать (по умолчанию все компоненты находятся по адресу C:\Program Files\ALTEX-SOFT).

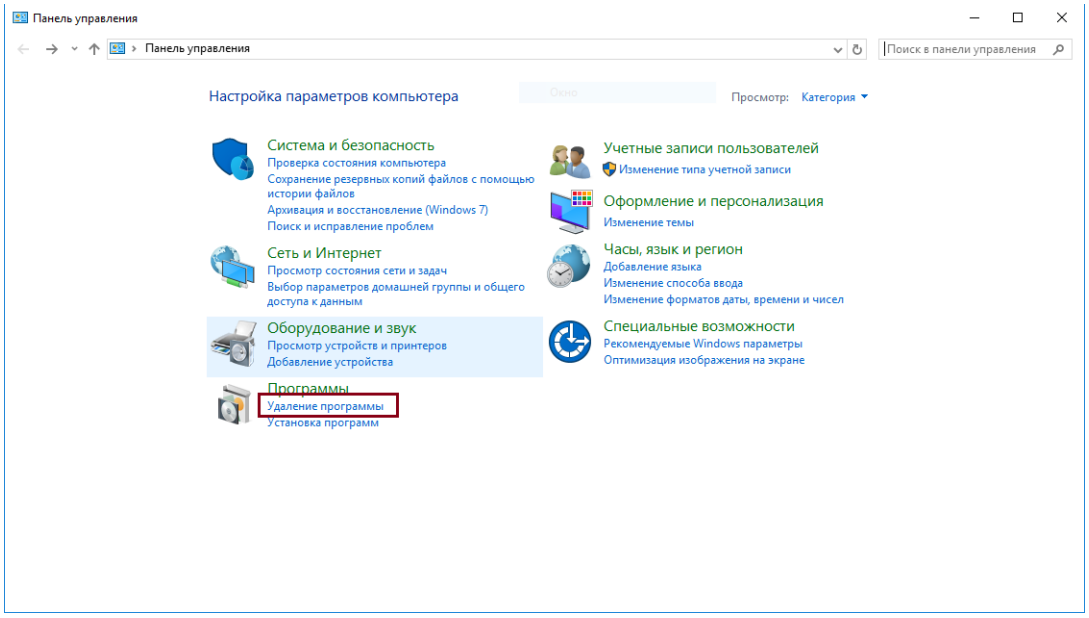
5.16.2.2 Удаление консоли управления

Удаление консоли управления RedCheck стандартными средствами Microsoft Windows

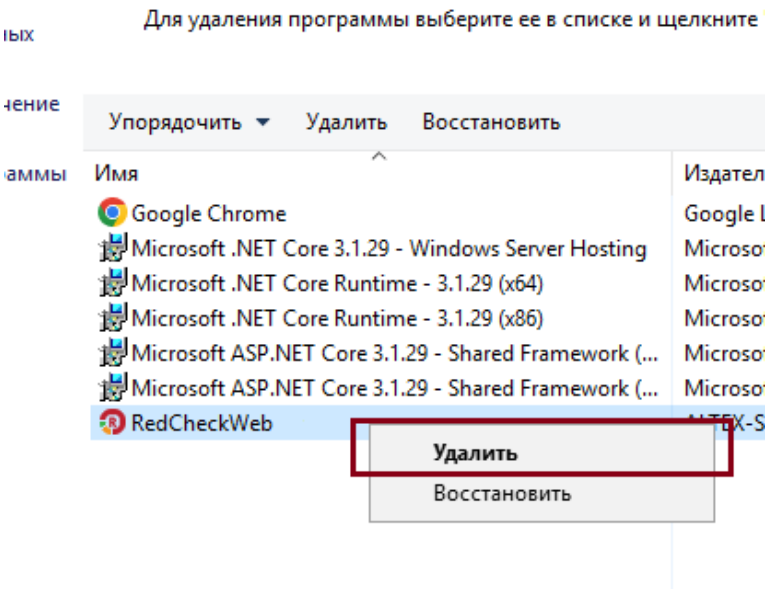
Шаг 1. Пуск → Служебные - Windows → Панель управления;



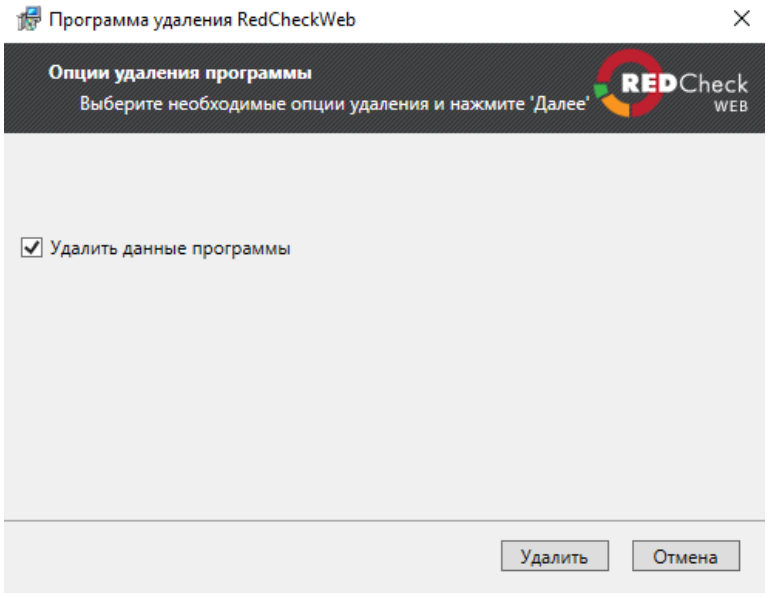
Шаг 2. Откройте утилиту **Удаление программ**;



Шаг 3. ПКМ по **RedCheckWeb** → **Удалить**;



Шаг 4. Отметьте по необходимости **Удалить данные программы** → **Удалить**;

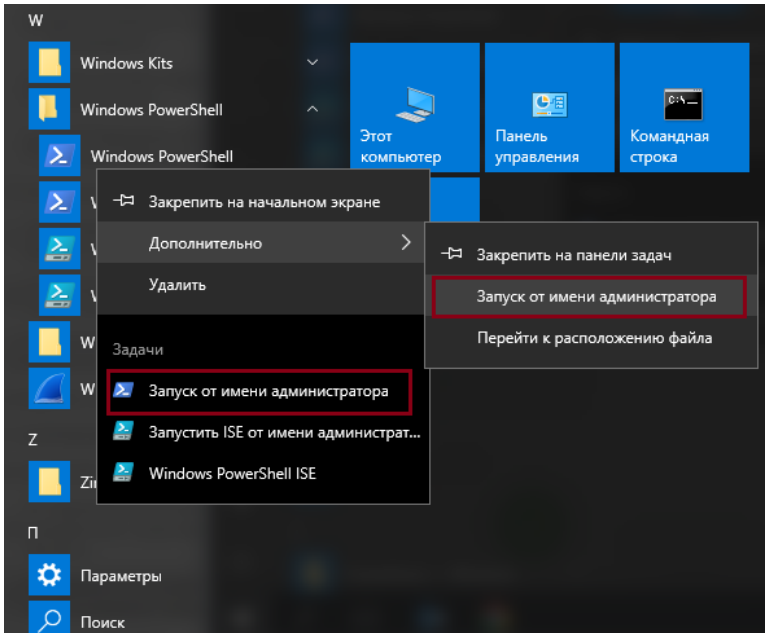


Под данными программы подразумеваются логи работы RedCheck.

Удаление консоли управления RedCheck через командную строку

Для данного способа деинсталляции необходим установочный пакет RedCheckWeb.Client.msi

Шаг 1. Пуск → Windows PowerShell → ПКМ по **Windows PowerShell → Запуск от имени администратора**;



Шаг 2. Введите команду для удаления:

Код

```
msiexec /x "<путь_к_установщику.msi>" /qn
```

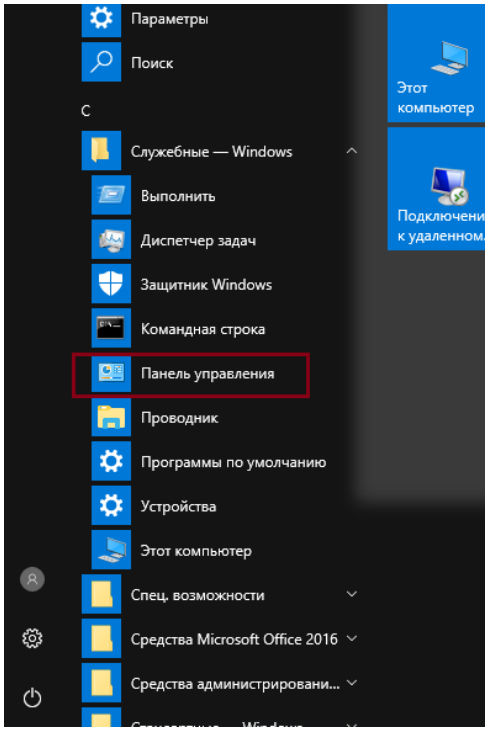
/q[n, b, f] – параметр отображения пользовательского интерфейса:
n – без интерфейса;
b – основной интерфейс (индикатор удаления);
f – полный интерфейс (по умолчанию);

Шаг 3. Проверьте работу деинсталлятора. При успешном удалении директория соответствующего компонента будет отсутствовать (по умолчанию все компоненты находятся по адресу C:\Program Files\ALTEX-SOFT).

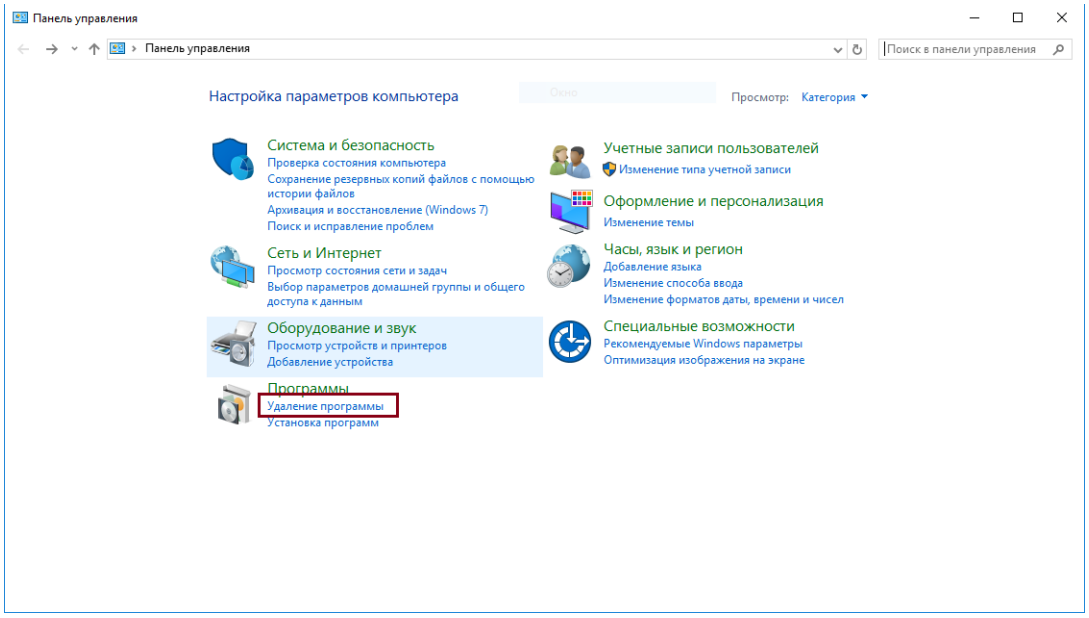
5.16.2.3 Удаление службы сканирования

Удаление службы сканирования RedCheck стандартными средствами Microsoft Windows

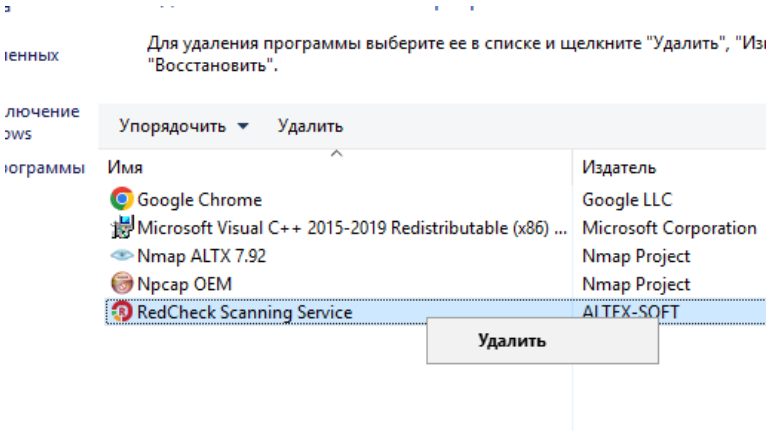
Шаг 1. Пуск → Служебные - Windows → Панель управления;



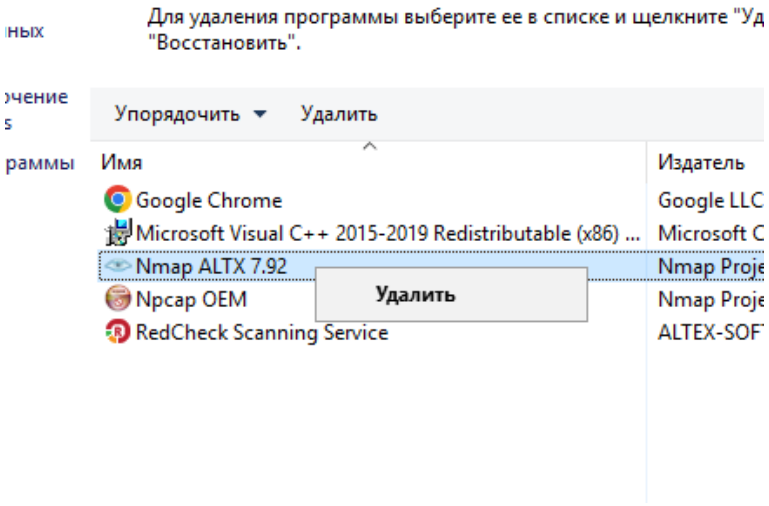
Шаг 2. Откройте утилиту **Удаление программ**;



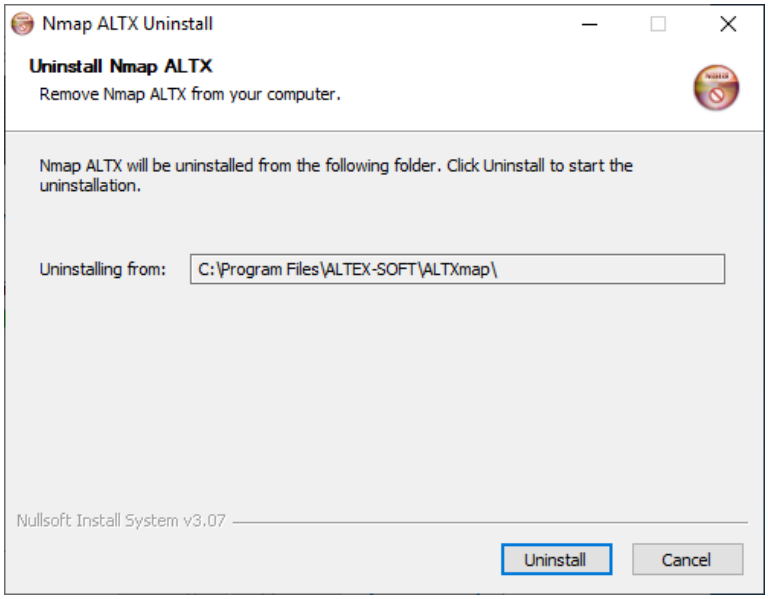
Шаг 3. ПКМ по **RedCheck Scanning Service** → **Удалить**;



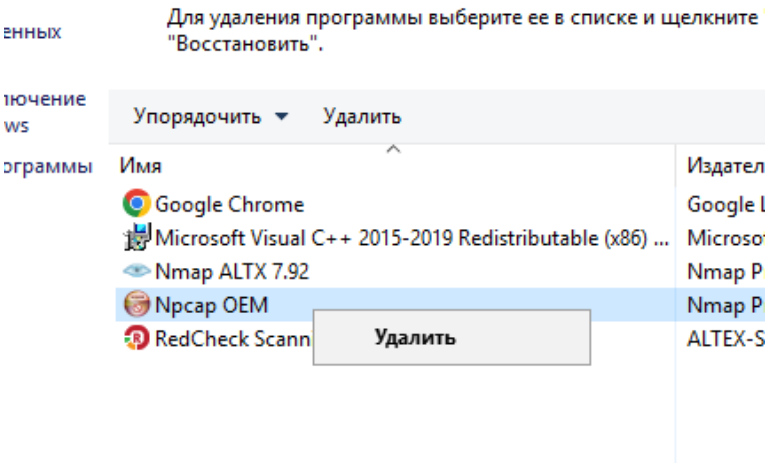
Шаг 4. После деинсталляции службы сканера необходимо удалить **Nmap ALTX 7.92**;



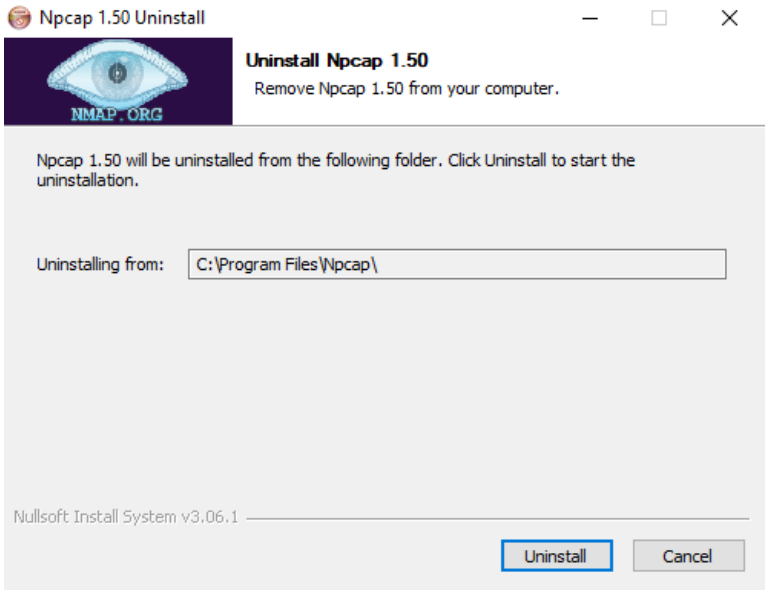
Шаг 5. Нажмите **Uninstall** в окне деинсталлятора **ALTXmap**;



Шаг 6. Последний компонент – **Npcap OEM**;



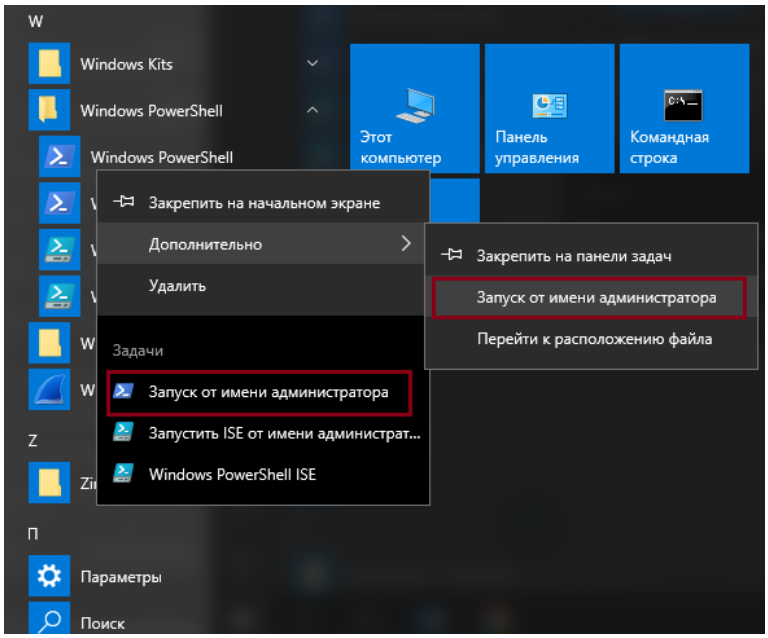
Шаг 7. Нажмите **Uninstall** в окне деинсталлятора **Npcap OEM**.



Удаление службы сканирования RedCheck через командную строку

Для данного способа деинсталляции необходим установочный пакет RedCheckScanService.msi

Шаг 1. Пуск → Windows PowerShell → ПКМ по **Windows PowerShell → Запуск от имени администратора**;



Шаг 2. Введите команду для удаления:

Код

```
msiexec /x "<путь_к_установщику.msi>" /qn
```

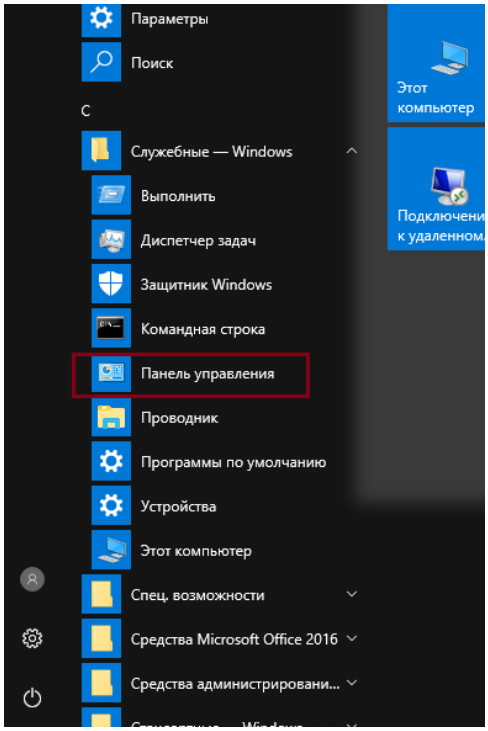
/q[n, b, f] – параметр отображения пользовательского интерфейса:
n – без интерфейса;
b – основной интерфейс (индикатор удаления);
f – полный интерфейс (по умолчанию);

Шаг 3. Проверьте работу деинсталлятора. При успешном удалении директория соответствующего компонента будет отсутствовать (по умолчанию все компоненты находятся по адресу C:\Program Files\ALTEX-SOFT).

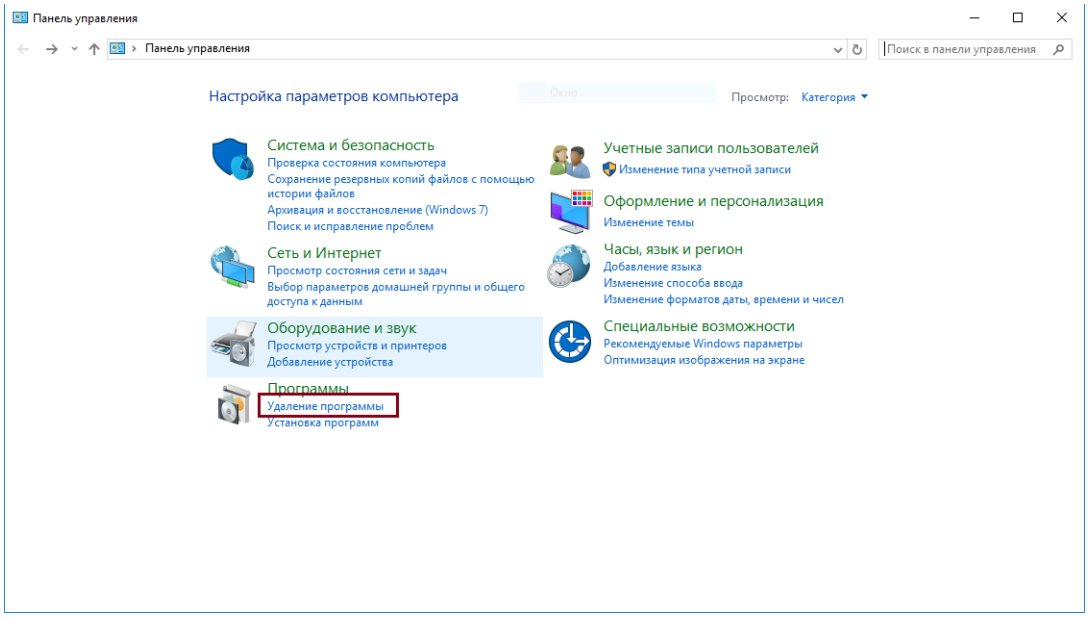
5.16.2.4 Удаление службы синхронизации

Удаление службы синхронизации RedCheck стандартными средствами Microsoft Windows

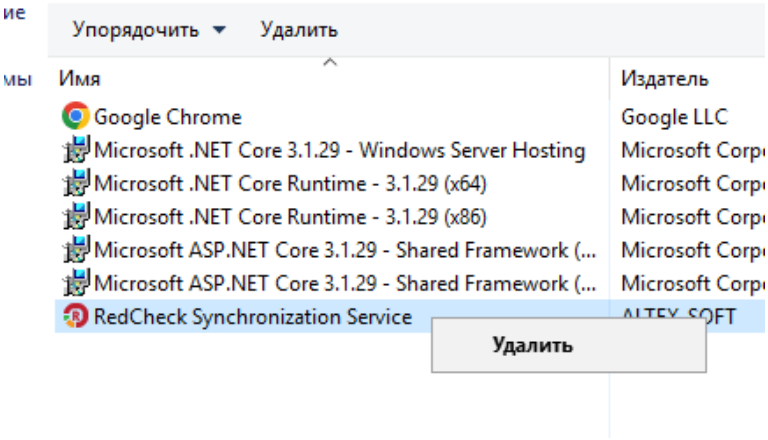
Шаг 1. Пуск → Служебные - Windows → Панель управления;



Шаг 2. Откройте утилиту **Удаление программ**;



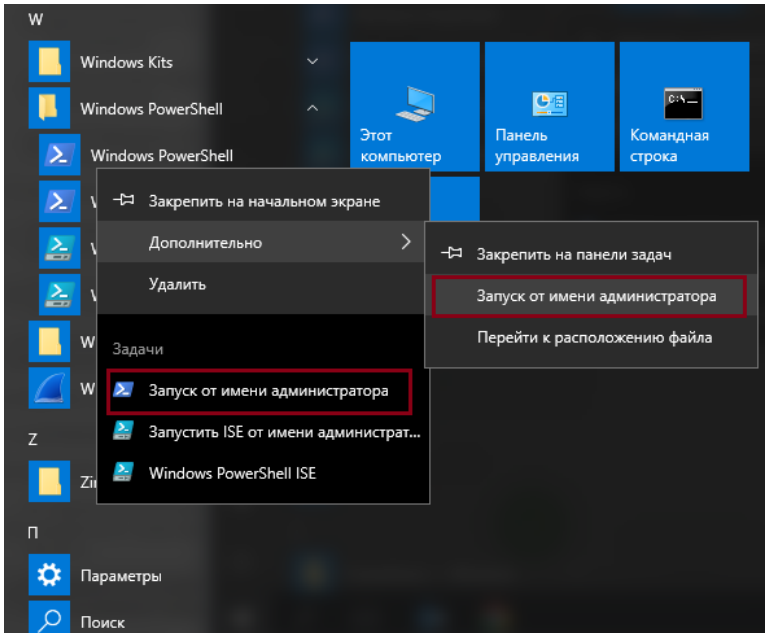
Шаг 3. ПКМ по **RedCheck Synchronization Service** → **Удалить**;



Удаление службы синхронизации RedCheck через командную строку

Для данного способа деинсталляции необходим установочный пакет RedCheckSyncService.msi

Шаг 1. Пуск → **Windows PowerShell** → ПКМ по **Windows PowerShell** → **Запуск от имени администратора**;



Шаг 2. Введите команду для удаления:

Код

```
msiexec /x "<путь_к_установщику.msi>" /qn
```

/q[n, b, f] – параметр отображения пользовательского интерфейса:
n – без интерфейса;
b – основной интерфейс (индикатор удаления);
f – полный интерфейс (по умолчанию);

Шаг 3. Проверьте работу деинсталлятора. При успешном удалении директория соответствующего компонента будет отсутствовать (по умолчанию все компоненты находятся по адресу C:\Program Files\ALTEX-SOFT).

6 Решение проблем

В данном разделе отображены проблемы, которые могут возникнуть при установке, настройке и эксплуатации RedCheck.

Содержание

6.1.1 Лицензионный ключ уже активирован на другом ПК

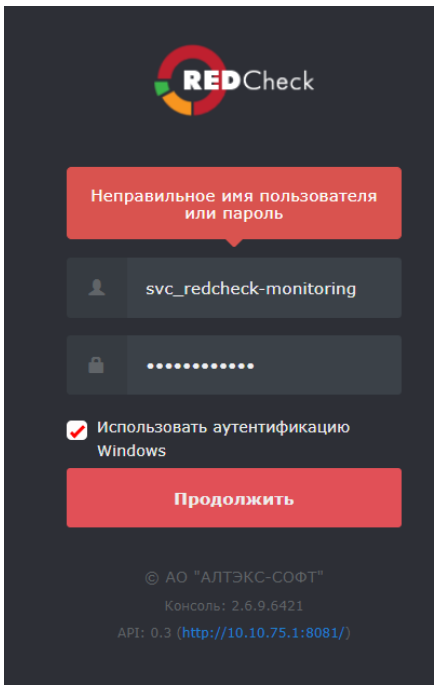
Ошибка актуальна при работе без доступа к сети Интернет. В таком случае RedChek не может удалить активацию при деинсталляции.

Во время установки происходит «привязка» к хосту. Это выполняется с целью регистрации факта установки. Поэтому в случае появления данной проблемы становится невозможным выполнить установку на другом хосте.

Для решения проблемы необходимо в личном кабинете **Центра сертифицированных обновлений** сбросить привязку (5.10 Сброс привязки лицензии). После этого инсталлятор проверит её и разрешит произвести установку на другом устройстве.

Содержание

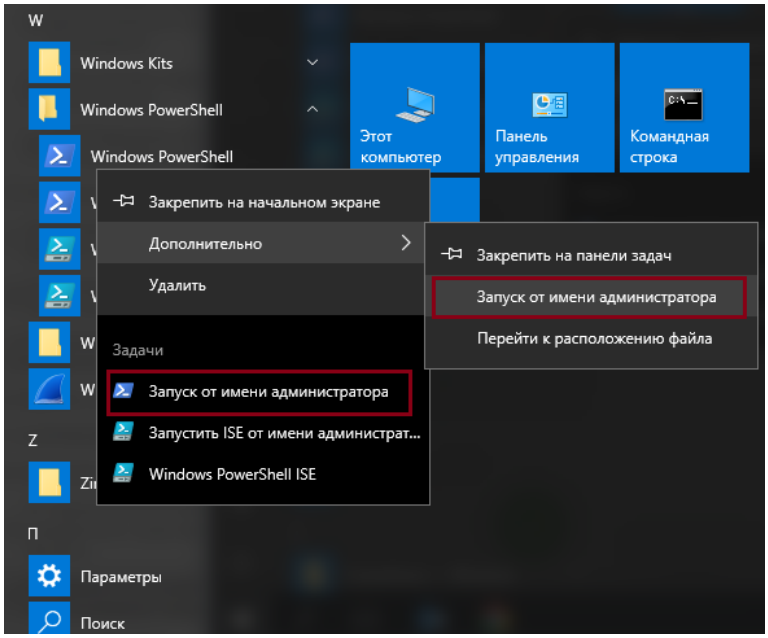
6.2.1 Невозможно войти с помощью Windows-авторизации



Данные учетной записи вводятся верные, но в RedCheck авторизоваться не удается.

Решение

Шаг 1. Откройте консоль PowerShell с правами администратора: **Пуск** → **Windows PowerShell** → в контекстном меню **Windows PowerShell** выберите **Запуск от имени администратора**;



Шаг 2. Введите команды **klist purge** и **gpupdate /force**

6.2.2 Не удалось подключиться к серверу синхронизации

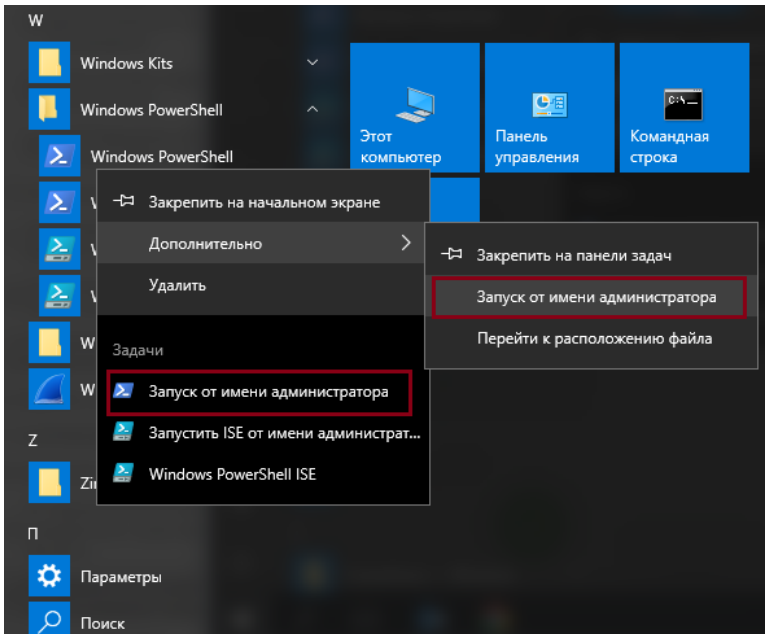
Необходимо на пограничном брандмауэре отрыть доступ к серверу обновлений, который расположен по адресу https://sync.altx-soft.ru (443/TCP), либо, если в сети используется прокси сервер, указать его настройки на вкладке **Настройки** → **Дополнительно** → **Прокси-сервер**.

6.2.3 Нет связи с агентом сканирования

При проверке хостов с использованием Агента, удаленный хост не доступен.

Проверьте наличие разрешающего входящего и исходящего правила для протокола **TCP/IP** порт **8732**; Если разрешения нет, добавьте его:

Шаг 1. Пуск → **Windows PowerShell** → в контекстном меню **Windows PowerShell** выберите **Запуск от имени администратора**;



Шаг 2. Выполните следующую команду:

Код

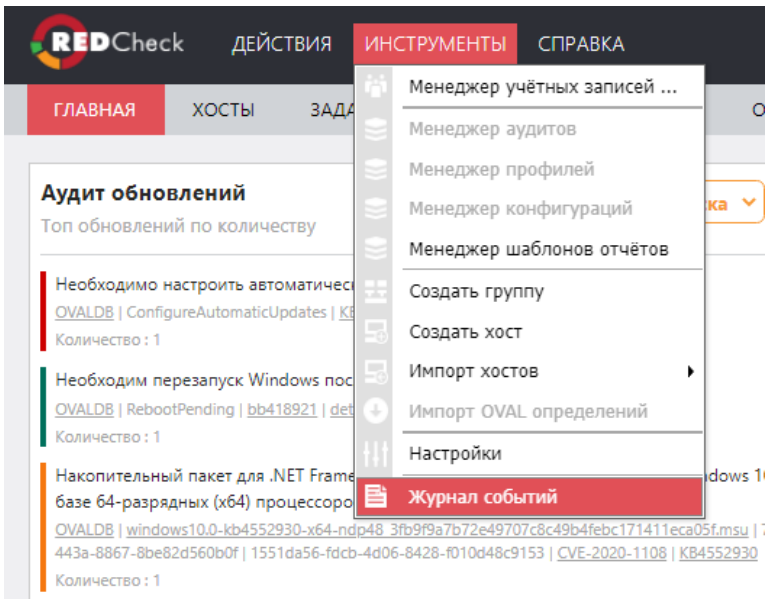
```
netsh advfirewall firewall add rule name="RedCheck Agent port" dir=in
action=allow protocol=TCP localport=8732
```

В одноранговой сети пользователь, от имени которого происходит обращение к агенту, должен находиться в локальной группе безопасности **REDCHECK_*.** В случае доменной сети пользователь должен находиться в доменной группе безопасности **REDCHECK_*** (5.1.2 Создание групп безопасности для Windows аутентификации).

Для повышения безопасности в сети предприятия рекомендуется, чтобы пользователь имел роль с минимальными правами доступа в ролевой модели RedCheck (1..4 Ролевая модель RedCheck).

6.2.4 Ошибка в рассылке отчётов по электронной почте

Ошибка возникает в результате некорректной настройки взаимодействия с сервером почты, который должен отправлять сообщения о результатах задания. Подробная информация об ошибке будет указана в журнале событий.



Содержание

6.3.1 Сбор расширенных журналов событий при сканировании

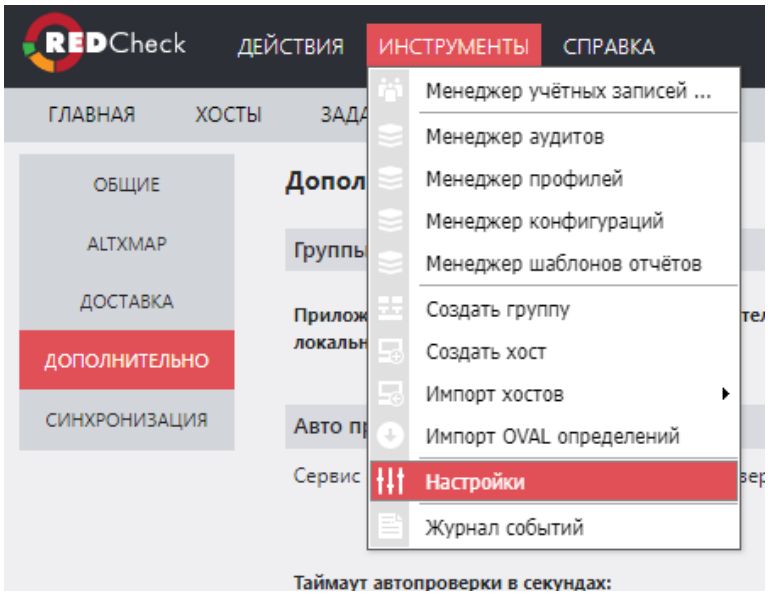
При возникновении ошибок во время сканирования технической поддержке может понадобиться файл с логами работы служб Системы. RedCheck позволяет сохранять два типа логов: обычные и расширенные. По умолчанию расширенные логи отключены.

Обычные логи располагаются в директории: C:\ProgramData\ALTEX-SOFT\RedCheck\Logs

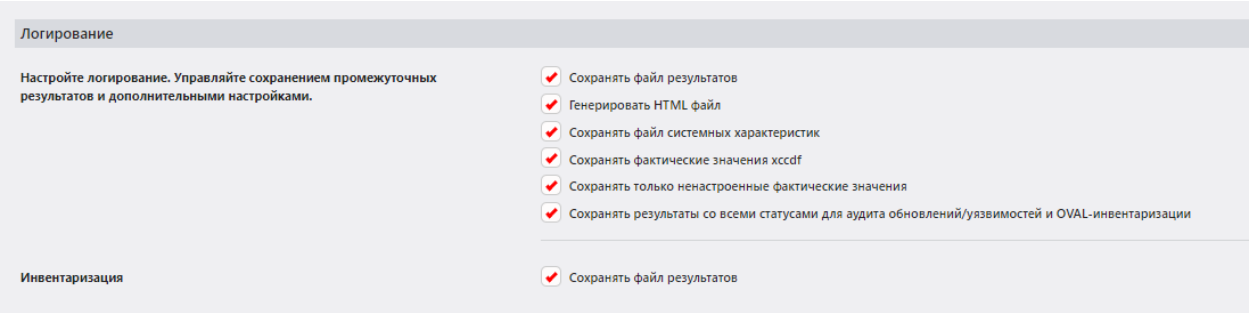
- \API – серверный компонент;
- \SVC – служба сканирования;
- \RedCheckSyncService – служба синхронизации;
- \WebClient – консоль управления;
- \Agent – агент сканирования:

Расширенные логи

Шаг 1. Откройте консоль управления RedCheck → **Инструменты** → **Настройки**;



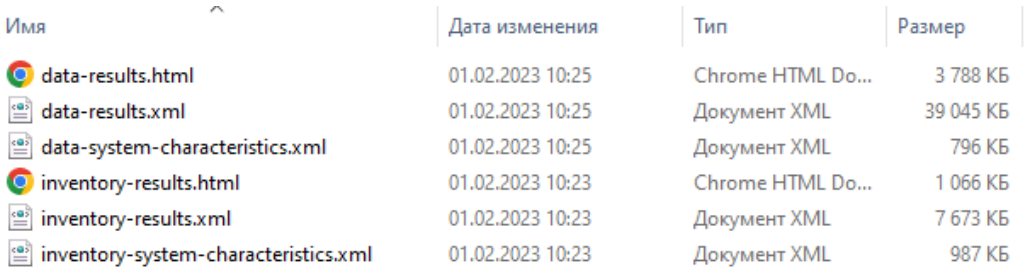
Шаг 2. Перейдите в **Дополнительно** → отметьте все параметры в разделе **Логирование** (для сохранения подробной информации по каждому из сканирований);



Шаг 3. Перезапустите задание, в котором произошла ошибка;

Шаг 4. Расширенные логи находятся в директории: C:\ProgramData\ALTEX-SOFT\RedCheck\Temp\OutputSchemes\[UID_Задания]\[IP_или_имя_хоста]\[uniqueId]

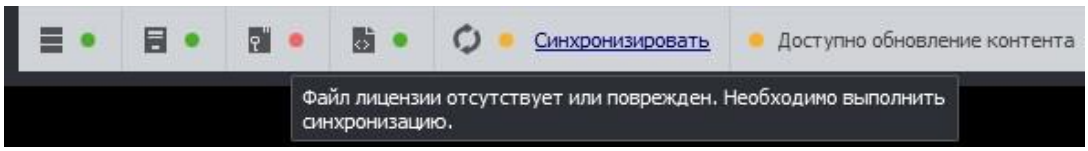
- UID_Задания: **История** → ⚙ → **Свойства** → **поле UID**;
- uniqueId: UUID хоста;



После отправки в службу поддержки расширенных логов рекомендуется снять флажки с параметров логирования, отмеченных ранее.

Содержание

6.4.1 Файл лицензии отсутствует или поврежден



На статусной панели индикатор лицензионного ключа показывает наличие ошибки – **Файл лицензии отсутствует или поврежден**.

Решение

Выполните синхронизацию. Лицензионный ключ будет обновлен после синхронизации с сервером обновлений.

7 Термины и сокращения

Термин	Определение
Администратор	Должностное лицо организации, участвующее в функционировании Системы и имеющее полные права ко всем функциям Системы
Гипервизор	ПО, которое дает базовому оборудованию хостов возможность автономного запуска и управления виртуальными машинами (имеющими права гостевых) изолированно от аппаратной части
Интернет	Информационно-телекоммуникационная сеть Интернет
Пользователь	Лицо, участвующее в функционировании Системы или использующее результаты её функционирования
Руководство	Руководство администратора
Хост	Любое устройство, которое подвергается сканированию Системой

Сокращение	Расшифровка
АО «АЛТЭКС-СОФТ»	Организация-разработчик Системы
АСУ ТП	Автоматизированная система управления технологическими процессами
БД	База данных
ИБ	Информационная безопасность
ИС	Информационная система
ОС	Операционная система

ПО	Программное обеспечение
Репозиторий OVALdb	БД определений проблем безопасности
СЗИ	Средства защиты информации
Система	Программное средство анализа защищенности RedCheck
СУБД	Система управления базами данных
УЗ	Учётная запись
ФСТЭК России	Федеральная служба по техническому и экспортному контролю
CPE	Common Platform Enumeration – перечисление общих платформ. Структурированная схема именования систем, ПО и пакетов информационных технологий. Включает в себя формальный формат имени, метод проверки имен в системе и формат описания для привязки текста и тестов к имени
CSV	Импорт хостов из CSV-файла
CVSS	Common Vulnerability Scoring System – общая оценка уязвимостей. Открытый стандарт, используемый для расчета количественных оценок уязвимости в безопасности компьютерной системы, обычно с целью принять ее приоритет
DMZ	DeMilitarized Zone – демилитаризованная зона, ДМЗ. Сегмент сети, содержащий и предоставляющий организации общедоступные сервисы, а также отделяющих их от остальных участков локальной сети, что позволяет обеспечить внутреннему информационному пространству дополнительную защиту от внешних атак
DNS	Domain Name System – система доменных имен. Технология, которая отвечает за хранение и обработку информации о доменных адресах. Инструмент используется для преобразования доменных имен в IP-адреса в момент отправки пользователем запроса на сервер

Docker	Открытая платформа для разработки, доставки и эксплуатации приложений
FQDN	Full Qualified Domain Name – полностью определенное имя домена. Доменное имя, однозначно определяющее узел в сети Интернет. Включает в себя имена всех родительских доменов
HTML	HyperText Markup Language – язык разметки гипертекста. Стандартизированный язык разметки Web-страниц
Hyper-V	Платформа виртуализации от Microsoft, которая распределяет ресурсы одного физического сервера между набором виртуальных серверов
IP	Internet Protocol – «Интернет-протокол». Набор правил, регулирующих формат данных, отправляемых через интернет или локальную сеть
IP-адрес	Уникальный адрес, идентифицирующее устройство в интернете или локальной сети
Kubernetes	Портативная расширяемая платформа с открытым исходным кодом для управления контейнеризованными рабочими нагрузками и сервисами
LAN	Local Area Network – локальная вычислительная сеть (ЛВС)
LAN-сегмент	Часть ЛВС, отделенная от других частей ЛВС с помощью одного или нескольких мостов, маршрутизаторов, повторителей или коммутаторов
PDF	Portable Document Format – межплатформенный открытый формат электронных документов
RDP	Remote Desktop Protocol – протокол удаленного стола. Протокол предоставляет возможность удаленного отображения и ввода через сетевые соединения для приложений на базе Microsoft Windows, работающих на сервере
SCAP	Security Content Automation Protocol – протокол автоматизации управления данными безопасности. Набор открытых стандартов,

	определяющих технические спецификации для представления и обмена данными безопасности
SOAP	Simple Object Access Protocol – упрощенный протокол обмена информацией в распределенной среде без централизованного управления
SSH	Secure Shell – «безопасная оболочка». Сетевой протокол для удаленного управления операционной системой с помощью командной строки и передачи данных в зашифрованном виде
TCP	Transmission Control Protocol/Internet Protocol – протокол передачи данных в сети Интернет
UAC	User Account Control – средство контроля пользовательских учётных записей
UUID	Universally Unique identifier – универсальный уникальный идентификатор. Уникальный идентификатор, сгенерированный машиной в определенном диапазоне
VMware	Технология виртуализации сервера, созданная для консолидации серверов уровня предприятия, организации их непрерывной работы, а также для разработчиков. Виртуализация требуется для того, чтобы разделить сервер на множество изолированных друг от друга виртуальных выделенных серверов
WinRM	Windows Remote Management – удаленное управление Windows. Служба удаленного управления для операционных систем Windows
WMI	Windows Management Instrumentation – инструментарий управления Windows. Одна из базовых технологий для централизованного управления и слежения за работой различных частей компьютерной части под управлением платформы Windows
WSUS	Windows Server Update Services – сервис обновлений операционных систем и продуктов Microsoft
XML	eXtensible Markup Language – расширяемый язык разметки