

# RedCheck

СРЕДСТВО АНАЛИЗА  
ЗАЩИЩЕННОСТИ

Руководство  
администратора

---

АЛМЮ.501410.RC02-01.РА



Версия документа 2.7.0.ru



## Содержание

---

Аннотация.....	5
1 Знакомство с RedCheck.....	7
1.1 Основные сведения.....	8
1.2 Репозиторий OVALdb.....	14
1.3 Архитектура RedCheck.....	15
1.4 Функциональные возможности.....	16
1.5 Ролевая модель RedCheck.....	22
1.6 Редакции RedCheck.....	24
1.7 Лицензирование.....	27
1.8 Как получить тестовую версию?.....	28
1.9 Перечень поддерживаемых платформ.....	30
1.10 Перечень интегрируемых систем.....	35
1.11 Служба технической поддержки.....	36
2 Системные требования.....	37
2.1 Требования к аппаратному обеспечению.....	38
2.2 Требования к программному обеспечению.....	42
2.3 Требования к сетевой инфраструктуре.....	43
3 Установка RedCheck Nix.....	47
3.1 Astra Linux.....	48
Установка СУБД.....	48
Инсталляция RedCheck.....	52
Конфигурация RedCheck.....	54
Подключение репозитория Astra Linux без доступа к сети Интернет.....	60
3.2 Debian.....	63
Установка СУБД.....	63
Инсталляция RedCheck.....	67
Конфигурация RedCheck.....	69
3.3 РЕД ОС.....	72
Установка СУБД.....	73
Инсталляция RedCheck.....	77
Конфигурация RedCheck.....	80

3.4 SberLinux.....	85
Инсталляция RedCheck .....	86
Конфигурация RedCheck.....	89
3.5 Установка RedCheck Update Server (Windows).....	94
3.6 Установка агента RedCheck (Windows).....	96
3.6.1 Установка на сканируемом хосте в ручном режиме .....	97
3.6.2 Установка через групповые политики домена.....	102
3.7 Раздельная установка компонентов.....	124
4 Сопровождение Системы.....	126
4.1 Создание локальных пользователей RedCheck .....	127
4.2 Активация лицензии.....	128
4.3 Обновление контента информационной безопасности .....	132
4.3.1 Синхронизация через сеть Интернет .....	133
4.3.2 Офлайн-синхронизация .....	134
4.3.3 Синхронизация через RedCheck Update Server.....	137
4.3.4 Синхронизация через прокси-сервер .....	143
4.4 Настройка учетных записей для сканирования.....	144
4.4.1 Сканирование Windows-систем.....	145
Транспорт Агент RedCheck .....	152
Транспорт WinRM.....	153
Транспорт WinRM (Kerberos).....	168
4.4.2 Сканирование Unix-систем (SSH) .....	170
Учетная запись суперпользователя (root) .....	174
Учетная запись привилегированного пользователя (sudo).....	176
Учетная запись непривилегированного пользователя .....	177
4.4.3 Сканирование FreeBSD.....	179
4.4.4 Сканирование Solaris.....	181
4.4.5 Сканирование Check Point.....	182
4.4.6 Сканирование Cisco IOS / NX-OS.....	183
4.4.7 Сканирование Huawei .....	187
4.4.8 Сканирование FortiOS.....	189
4.4.9 Сканирование UserGate .....	190

4.4.10 Сканирование VMware .....	191
Настройка VMware ESXi Server .....	192
Настройка VMware vCenter Server .....	196
Настройка VMware NSX Data Center .....	197
4.4.11 Сканирование Microsoft SQL Server .....	199
4.4.12 Сканирование MySQL .....	201
4.4.13 Сканирование PostgreSQL .....	203
4.4.14 Сканирование Oracle .....	205
4.5 Смена ключа шифрования .....	209
4.6 Обслуживание БД .....	211
4.7 Резервное копирование и восстановление БД .....	214
4.7.1 Резервное копирование PostgreSQL .....	215
4.7.2 Восстановление PostgreSQL .....	216
4.8 Обновление RedCheck Nix .....	217
4.9 Сброс привязки лицензии .....	221
4.10 Смена лицензионного ключа .....	223
4.11 Изменение портов для компонентов RedCheck .....	225
4.11.1 Агент обновления .....	226
4.11.2 Агент сканирования .....	229
4.12 Журнал событий (логи) .....	233
4.13 Настройка сервиса доставки отчетов .....	234
4.14 Исключения для средств защиты (САЗ, СЗИ) .....	236
5 Термины и сокращения .....	238

## Аннотация

---

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

Для пользователей RedCheck рекомендуется ознакомиться с [Руководством Пользователя RedCheck Nix](#).

Для взаимодействия с RedCheck посредством RestAPI рекомендуется ознакомиться с [Документацией API RedCheck](#).

Руководство состоит из следующих разделов:

- [1 Знакомство с RedCheck](#)
- [2 Системные требования](#)
- [3 Установка RedCheck Nix](#)
- [4 Сопровождение Системы](#)
- [5 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., 141090
Электронная почта:	<a href="mailto:info@altx-soft.ru">info@altx-soft.ru</a> / <a href="mailto:support@altx-soft.ru">support@altx-soft.ru</a>
Телефон:	+7(495) 543-31-01

Адрес сайта  
производителя:

[altx-soft.ru](http://altx-soft.ru)

Адрес сайта товара:

[redcheck.ru](http://redcheck.ru)

# 1 Знакомство с RedCheck

---

RedCheck NIX на данный момент имеет несколько ограничений:

- отсутствует возможность Windows-аутентификации (используя доменную учетную запись) для входа в консоль управления. Для аутентификации используются локальные пользователи RedCheck;
- отсутствует возможность выполнения задания Аудит уязвимостей образов Docker.

Отсутствующий функционал находится в разработке и появится в следующих версиях.

## Содержание

- [1.1 Основные сведения](#)
- [1.2 Репозиторий OVALdb](#)
- [1.3 Архитектура RedCheck](#)
- [1.4 Функциональные возможности](#)
- [1.5 Ролевая модель RedCheck](#)
- [1.6 Редакции RedCheck](#)
- [1.7 Лицензирование](#)
- [1.8 Как получить тестовую версию?](#)
- [1.9 Перечень поддерживаемых платформ](#)
- [1.10 Перечень интегрируемых систем](#)
- [1.11 Служба технической поддержки](#)

## 1.1 Основные сведения

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 в реестре – 765



# 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 «АЛТЭК-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 № СИЗ 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 № СИЗ 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 «АЛТЭК-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 № ВУ/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 № ВУ/112 036.01, дата регистрации 15.10.1997 г.)

## СЕРТИФИКАТ СООТВЕТСТВИЯ



Зарегистрирован в реестре № ВУ/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/ВУ (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 ВУ/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 ВУ/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://ovaldb.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).

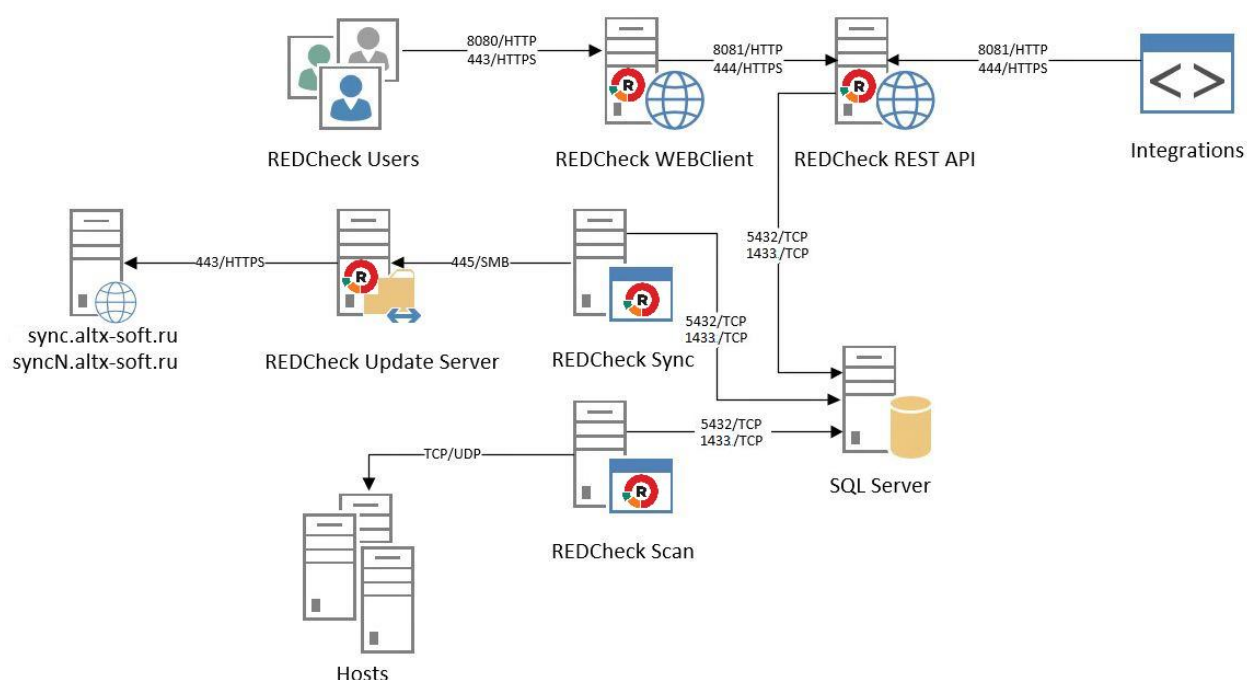
Кроме контента, разработанного компанией АЛТЭКС-СОФТ, его содержание синхронизировано с экспертными ресурсами, такими как БДУ ФСТЭК России, НКЦКИ, бюллетени производителей и ряд других международных экспертных справочников. Периодичность публикации новых определений составляет 2-3 дня в соответствии 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.

### 1.3 Архитектура RedCheck

RedCheck состоит из перечня компонентов, разработанных АО «АЛТЭК-СОФТ» в рамках единой платформы, способных функционировать на выделенных серверах и в соответствии с используемой лицензией. Поддерживается установка всех основных компонентов на один сервер при сканировании малых сетей. Пример распределенного расположения компонентов приведен на рисунке ниже.

RedCheck Update Server является необязательным компонентом и лицензируется отдельно. Установка RedCheck Update Server производится в DMZ-сегменте сети для обновления контента безопасности без доступа к сети Интернет со стороны компонента RedCheck Sync.



RedCheck может использовать несколько служб сканирования (RedCheck Scan), в соответствии с используемой лицензией.

## 1.4 Функциональные возможности

В процессе выполнения всех типов заданий не требуется остановка или перезапуск сервисов на конечных хостах.

### 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 либо с использованием агента RedCheck, либо на основе безагентной технологии с использованием привилегированных учетных записей (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, Аудит конфигураций, Инвентаризация и Фиксация. Сравнение новых отчетов с эталоном позволяет увидеть произошедшие изменения на хосте.

## 1.5 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 ([4.1 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

Управление – возможность создавать, просматривать, изменять и удалять

Название роли	Перечень возможностей
Суперпользователь	<ul style="list-style-type: none"><li>▪ Обладает всеми возможностями в рамках работы с консолью управления RedCheck</li></ul>
Администратор ИБ	<ul style="list-style-type: none"><li>▪ Управление хостами (+импорт / экспорт);</li><li>▪ Управление группами;</li><li>▪ Просмотр учетных записей;</li><li>▪ Управление заданиями;</li><li>▪ Просмотр и удаление результатов сканирования;</li><li>▪ Управление функцией Контроль для выполненного задания</li><li>▪ Управление отчетами;</li><li>▪ Управление профилями для Аудита уязвимостей / конфигураций;</li><li>▪ Управление пользователями для работы с</li></ul>

	<p>RedCheck</p> <ul style="list-style-type: none"> <li>▪ Запуск синхронизации и импортирование OVAL-сигнатур;</li> <li>▪ Просмотр журнала событий и справки о программе;</li> </ul>
<p>Системный администратор</p>	<ul style="list-style-type: none"> <li>▪ Управление хостами (+импорт / экспорт);</li> <li>▪ Управление группами;</li> <li>▪ Управление учетными записями;</li> <li>▪ Просмотр свойств заданий;</li> <li>▪ Управление профилями для Аудита уязвимостей / конфигураций;</li> <li>▪ Изменять настройки RedCheck (+смена лицензионного ключа);</li> <li>▪ Запуск и настройка синхронизации контента безопасности;</li> <li>▪ Просмотр журнала событий и справки о программе;</li> </ul>
<p>Пользователь ИБ</p>	<ul style="list-style-type: none"> <li>▪ Просмотр свойств хостов;</li> <li>▪ Просмотр свойств групп;</li> <li>▪ Просмотр учетных записей;</li> <li>▪ Просмотр свойств заданий;</li> <li>▪ Просмотр результатов сканирования;</li> <li>▪ Просмотр работы функции Контроль для отчета выполненного задания</li> <li>▪ Просмотр отчетов;</li> <li>▪ Просмотр профилей для Аудита уязвимостей / конфигураций;</li> <li>▪ Запуск синхронизации контента безопасности;</li> <li>▪ Просмотр справки о программе;</li> </ul>

## 1.6 Редакции RedCheck

RedCheck доступен в четырех редакциях:

**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	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 (по количеству хостов)		
Аудит уязвимостей образов Docker	–	+	+
Проверка доступности	+	+	+
Отчеты по результатам аудитов	+	+	+
<b>ОБЪЕКТЫ СКАНИРОВАНИЯ</b>			
ОС Windows и Linux	+	+	+
Сетевое оборудование	+	+	+
Протоколы АСУ ТП	за дополнительную плату (по количеству хостов)		
Средства виртуализации	+	+	+
Средства контейнеризации и оркестрации	–	+	+
СУБД	+	+	+
<b>ДОПОЛНИТЕЛЬНЫЙ СЕРВИС</b>			
Сертифицированная версия Системы	+	+	+
Адаптация конфигураций	за дополнительную плату		+
Разработка индивидуальных конфигураций безопасности	за дополнительную плату		

Расширенная поддержка	за дополнительную плату		+
<b>АРХИТЕКТУРА И МАСШТАБИРУЕМОСТЬ</b>			
Подключение дополнительных служб сканирования (лицензируются отдельно)	–	+	+
Многопоточное сканирование Белым ящиком	+	+	+
Многопоточное сканирование Черным ящиком («Пентест»)	+	+	+
Возможность интеграции с помощью RestAPI	+	+	+
Web-консоль управления	+	+	+

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

## 1.7 Лицензирование

Система лицензируется согласно редакциям, указанным в [1.6 Редакции RedCheck](#)

Система лицензирования не накладывает ограничений на количество проводимых аудитов, их повтор, а также количество сканируемых хостов в каждом аудите в пределах используемой лицензии.

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 САЗ 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 «АЛТЭК-СОФТ» в свободной форме – [sales@altx-soft.ru](mailto:sales@altx-soft.ru) или к партнерам в вашем регионе - [https://www.altx-soft.ru/company/partner\\_net/](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<sup>1</sup> / XP Embedded / Vista / 7 / 8 / 8.1 / 10 / 11
- Server 2003<sup>2</sup> / 2008 / 2008 R2 / 2012 / 2012 R2 / 2016 / 2019<sup>3</sup> / 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/kFreeBSD 6 / 7
- 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 / 24.04

## 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
- SberLinux OS Server

## 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<sup>4</sup>
- 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
- Jatoba
- 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
- Pangolin
- SAP HANA

## АСУ ТП

- Codesys V2 / V3
- 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 Агава
- ПЛК Кастом
- ПЛК Овен
- ПЛК Элси
- ПЛК Advantech APAX-xxxxKW, ADAM-xxxxKW
- ПЛК Ergon
- ПЛК Fastwel
- ПЛК Omron
- ПЛК RealLab!
- 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

<sup>1</sup>RedCheck не поддерживает сканирование Windows XP при помощи WinRm-туннеля;

<sup>2</sup>RedCheck не поддерживает сканирование Windows Server 2003 при помощи агента;

<sup>3</sup>Для Windows Server 2019 не применим функционал PatchManagement;

<sup>4</sup>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
Аудит в режиме 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	AL	NA
Аудит в режиме Пентест	BB	BB

**Условные обозначения**

«А» – 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 ([официальный сайт](#));
- 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](http://portal.altx-soft.ru)
- Электронная почта: [support@altx-soft.ru](mailto:support@altx-soft.ru)
- Web-сайт продукта: [redcheck.ru](http://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.

## 2 Системные требования

---

### Содержание

- [2.1 Требования к аппаратному обеспечению](#)
- [2.2 Требования к программному обеспечению](#)
- [2.3 Требования к сетевой инфраструктуре](#)

## 2.1 Требования к аппаратному обеспечению

Допускается установка компонентов RedCheck на виртуальные машины. При этом система виртуализации должна быть совместима с ОС, представленными в пункте [2.2 Требования к программному обеспечению](#)

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

Компоненты	Аппаратные требования
Совместная установка	
Серверный компонент (redcheck-api) Консоль управления (redcheck-client) Служба сканирования (redcheck-scan-service) Служба синхронизации (redcheck-sync-service)	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 (redcheck-api) Консоль управления (redcheck-client)	ЦП Xeon, частота не ниже 1,86 ГГц, не менее 2 ядер ОЗУ не менее 6 ГБ ПЗУ не менее 1 ГБ
Служба сканирования (redcheck-scan-service)	ЦП Xeon, частота не ниже 1,86 ГГц, не менее 2 ядер ОЗУ не менее 6 ГБ ПЗУ не менее 1 ГБ

Служба синхронизации (redcheck-sync-service)	ЦП Xeon, частота не ниже 1,86 ГГц, не менее 2 ядер ОЗУ не менее 4 ГБ ПЗУ не менее 1 ГБ
Сервер СУБД <sup>1</sup>	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)
<b>Дополнительные компоненты</b>	
Дополнительный модуль сканирования	ЦП Xeon, частота не ниже 1,86 ГГц, не менее 2 ядер ОЗУ не менее 6 ГБ ПЗУ не менее 1 ГБ

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

<sup>1</sup> - 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:

$$V_{HDD} \approx V_{ср} NT$$

где  $V_{HDD}$  – необходимый объем HDD, ГБ;  $V_{ср}$  – средний объем результатов сканирования одного хоста,

$V_{ср} \approx 2$  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  $0,002 \cdot 100 \cdot 26 = 5,2$  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.

## 2.2 Требования к программному обеспечению

Требования к ПО для корректного функционирования основных компонентов RedCheck:

- ОС:
  - Astra Linux 1.7 SE (Смоленск/Воронеж/Орел);
  - Debian 10;
  - РЕД ОС 7.3;
  - SberLinux OS Server 8.8 и выше;
- СУБД:
  - [PostgreSQL](#) версия 12.5 – 16;
  - [Postgres Pro](#) версия 14 / 15;
  - Rangolin версии 6.1.2 и выше;
- Браузер на основе ядра Chromium;
- Командная оболочка Bash.

## 2.3 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.

Все порты назначения могут быть переопределены, кроме получения обновлений с официального репозитория производителя (Сервис синхронизации - <https://syncn.altx-soft.ru>).

**Таблица 1** – перечень сетевых портов взаимодействия компонентов RedCheck

Источник	Назначение	Порт назначения	Прикладной протокол/комментарий
Веб-консоль RedCheck	Веб-консоль RedCheck	8080/TCP	HTTP/Взаимодействие с веб-консолью (рекомендуется установить SSL-сертификат и переопределить порт)
Служба REST 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
Служба REST RedCheck	База данных	5432/TCP	Взаимодействие с базой данных
Служба REST RedCheck	Сервис DNS	53/TCP	DNS/Запросы в службу разрешения имен

Служба сканирования RedCheck	База данных	5432/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	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 сообщений, e-mail	25/TCP	SMTP/Отправка почтовых уведомлений о результатах работы службы
Служба сканирования RedCheck	Сервис DNS	53/TCP	DNS/Запросы в службу разрешения имен
Служба синхронизации RedCheck	База данных	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 <a href="https://syncn.altx-soft.ru">https://syncn.altx-soft.ru</a>
Служба синхронизации RedCheck	Сервис синхронизации ( <a href="https://syncn.altx-soft.ru">https://syncn.altx-soft.ru</a> )	443/TCP	HTTPS/Доступ к сервису синхронизации производителя <a href="https://syncn.altx-soft.ru">https://syncn.altx-soft.ru</a>

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

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

	Сканирование посредством SSH	Сканирование посредством Агента сканирования
Скорость передачи данных, Кбит/с	160	121
Суммарный объем трафика на узел, КБ	5 000	8 400

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

## 3 Установка RedCheck Nix

---

### Содержание

- [3.1 Astra Linux](#)
- [3.2 Debian](#)
- [3.3 РЕД ОС](#)
- [3.4 SberLinux](#)
- [3.5 Установка RedCheck Update Server \(Windows\)](#)
- [3.6 Установка агента RedCheck \(Windows\)](#)

## 3.1 Astra Linux

- [Установка СУБД](#)
- [Инсталляция RedCheck](#)
- [Конфигурация RedCheck](#)
- [Подключение репозитория Astra Linux](#)

### Установка СУБД

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

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

**Шаг 2.** Войдите под root пользователем;

Bash (оболочка Unix)

```
sudo su -
```

Если хост без подключения к сети Интернет, скачайте репозитории в личном кабинете Astra Linux – [Подключение репозитория Astra Linux без доступа к сети Интернет](#)

**Шаг 3.** Добавьте адреса репозитория в файл `/etc/apt/sources.list`:



Bash (оболочка Unix)

```
deb https://dl.astralinux.ru/astra/stable/1.7_x86-64/repository-extended/ 1.7_x86-64 astra-ce main contrib non-free
deb https://dl.astralinux.ru/astra/stable/1.7_x86-64/repository-base/1.7_x86-64 main contrib non-free
deb https://dl.astralinux.ru/astra/stable/1.7_x86-64/repository-update/ 1.7_x86-64 main contrib non-free
deb https://dl.astralinux.ru/astra/stable/1.7_x86-64/repository-main/1.7_x86-64 main contrib non-free
```

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

**Шаг 1.** Откройте файл с помощью команды (sudo);

Bash (оболочка Unix)

```
nano /etc/apt/sources.list
```

**Шаг 2.** Переместите курсор в конец документа с помощью стрелки вниз. Для перехода на новую строку используйте клавишу **Enter**;

**Шаг 3.** Скопируйте репозитории и вставьте их с помощью комбинации **Ctrl + U**;

**Шаг 4.** Сохраните файл с помощью комбинации **Ctrl + O**; Для выхода используйте **Ctrl + X**;

**Шаг 4.** Обновите пакеты;

Bash (оболочка Unix)

```
apt -y update
```

**Шаг 5.** Установите PostgreSQL;

Bash (оболочка Unix)

```
apt -y install postgresql
```

## Настройка PostgreSQL

**Шаг 6.** 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 7.** Создайте пользователя для администрирования СУБД;

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

Bash (оболочка Unix)

```
sudo su postgres
```

Bash (оболочка Unix)

```
psql -U postgres
```

Bash (оболочка Unix)

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

```
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# █
```

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

**Шаг 8.** Завершите сессию командой **exit**

**Шаг 9.** 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 10.** 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
```

## Инсталляция RedCheck

Все команды в инструкции выполняются под root-пользователем. При необходимости используйте повышение прав (sudo).

Для обновления RedCheck – [4.8 Обновление RedCheck Nix](#)

## Установка компонентов

Для перемещения по каталогам используйте команду **cd**. Например, чтобы перейти в каталог /mnt, напишите **cd /mnt**  
Чтобы автоматически дополнить название каталога или файла, используйте **Tab**

**Шаг 1.** Смонтируйте установочный диск и добавьте репозиторий в **/etc/apt/sources.list**;

Bash (оболочка Unix)

```
deb cdrom:[OS Astra Linux 1.7.5 1.7_x86-64 DVD ]/ 1.7_x86-64 contrib  
main non-free
```

**Шаг 2.** Переместите скачанный архив `redcheck-repo-2.7.0.8862.tar.gz` в директорию, отличную от пользовательского каталога. В инструкции архив перемещается в `/mnt`;

Bash (оболочка Unix)

```
mv /home/имя_пользователя/Загрузки/redcheck-repo-2.7.0.8862.tar.gz  
/mnt/
```

**Шаг 3.** Перейдите в каталог и разархивируйте дистрибутив;

Bash (оболочка Unix)

```
cd /mnt
```

Bash (оболочка Unix)

```
tar -xf redcheck-repo-2.7.0.8862.tar.gz
```

**Шаг 4.** Добавьте GPG-ключ, который находится в только что разархивированном каталоге;

Bash (оболочка Unix)

```
apt-key add redcheck-repo/PUBLIC-GPG-KEY-redcheck
```

**Шаг 5.** Создайте файл `redcheck.list` и добавьте в него запись репозитория;

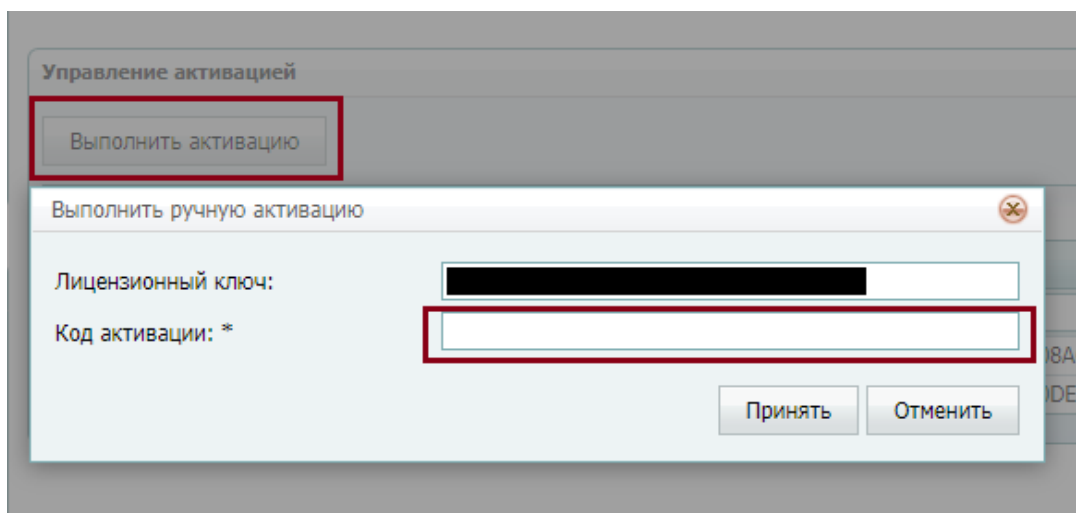
Bash (оболочка Unix)

```
touch /etc/apt/sources.list.d/redcheck.list  
echo "deb file:/mnt/redcheck-repo/ 1.7_x86-64 non-free dotnet" >  
/etc/apt/sources.list.d/redcheck.list
```

**Шаг 6.** Обновите пакеты;







**Шаг 4.** Нажмите **Скачать**;

	Активен	Дата активации	Действия
	False	10.12.2021 09:54:44	<a href="#">Скачать</a>
	True	24.09.2020 11:09:35	<a href="#">Скачать</a>

**Шаг 5.** Сохраните файл **license.xml**;

**Шаг 6.** Настройте компоненты RedCheck;

Перед повторной конфигурацией **рекомендуем** [сделать резервную копию](#) базы данных.

Bash (оболочка Unix)

```
redcheck-bootstrap configure -c=all
```

Будет запущен процесс конфигурации компонентов, который потребует ввода данных для доступа к СУБД, лицензионного ключа и других параметров для корректной работы Системы. Данной командой будут сконфигурированы все основные компоненты RedCheck на одном сервере.

На этапе генерации сертификата для протокола HTTPS необходимо ввести



названия: **области (страны), города, организации, отдела, электронной почты.**

```
Генерация сертификата..
Введите область
moscow
Введите город
korolev
Введите название организации
altx
Введите отдел
market
Введите адрес электронной почты
info
```

**Шаг 7.** Если хост не подключен к сети Интернет, выберите способ активации файлом и укажите путь к файлу **license.xml**. Если подключен, укажите ключ лицензии:

```
ТЕКУЩИЙ этап: Ввод лицензии (проверка лицензии, активация продукта)
=====
Выберите тип работы с лицензией - ключ лицензии или файл лицензии? (К/Ф): ф
Введите путь к файлу лицензии: /home/astra/Загрузки/license.xml
```

**Шаг 8.** Настройте службу очистки БД:

Bash (оболочка Unix)

```
redcheck-bootstrap configure -c=redcheck-cleanup-service
```

В процессе настройки службы вам нужно ввести URL redcheck-api в формате `http://ip:port`, а также учетные данные пользователя с ролью RedCheck\_Admins

**Шаг 9.** Укажите в конфигурационном файле redcheck-client строку подключения к службе очистки (`http://ip_rest_api:8740`);

Bash (оболочка Unix)

```
nano /var/opt/redcheck-client/conf/redcheck-web.dll.config
```

Пример конфигурационного файла после редактирования.

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <appSettings>
    <add key="RestUrl" value="192.168.80.169" />
    <add key="RestPort" value="8081" />
    <add key="RestApiVersion" value="0.3" />
    <add key="RestProtocol" value="http" />
    <add key="RestExtendedConnectionTimeout" value="100" />
    <add key="SessionTimeout" value="151" />
    <add key="CleanupServiceUrl" value="http://192.168.80.169:8740" />
  </appSettings>
</configuration>
```

**Шаг 10.** Перезапустите компонент redcheck-client;

Bash (оболочка Unix)

```
systemctl restart redcheck-client
```

Логи инсталлятора располагаются в **/var/opt/redcheck-common/log/configuration.log**

## Установка компонентов

Для перемещения по каталогам используйте команду **cd**. Например, чтобы перейти в каталог /mnt, напишите **cd /mnt**  
Чтобы автоматически дополнить название каталога или файла, используйте **Tab**

**Шаг 1.** Переместите скачанный архив redcheck-repo-2.7.0.8862.tar.gz в директорию, отличную от пользовательского каталога. В инструкции архив перемещается в /mnt;

Bash (оболочка Unix)

```
mv /home/имя_пользователя/Загрузки/redcheck-repo-2.7.0.8862.tar.gz /mnt/
```

**Шаг 2.** Перейдите в каталог и разархивируйте дистрибутив;

Bash (оболочка Unix)

```
cd /mnt
```

Bash (оболочка Unix)

```
tar -xf redcheck-repo-2.7.0.8862.tar.gz
```

**Шаг 3.** Добавьте GPG-ключ, который находится в только что разархивированном каталоге;

Bash (оболочка Unix)

```
apt-key add redcheck-repo/PUBLIC-GPG-KEY-redcheck
```

**Шаг 4.** Создайте файл **redcheck.list** и добавьте в него запись репозитория;

Bash (оболочка Unix)

```
touch /etc/apt/sources.list.d/redcheck.list  
echo "deb file:/mnt/redcheck-repo/ 1.7_x86-64 non-free dotnet" >  
/etc/apt/sources.list.d/redcheck.list
```

**Шаг 5.** Обновите пакеты;

Bash (оболочка Unix)

```
apt -y update
```

**Шаг 6.** Установите компоненты RedCheck;

Bash (оболочка Unix)

```
apt -y install redcheck-dotnet-runtime redcheck-aspnetcore-runtime  
redcheck-api redcheck-client redcheck-scan-service redcheck-sync-  
service redcheck-cleanup-service
```

Если на хосте ранее уже был установлен dotnet, перед инсталляцией необходимо его деинсталлировать:

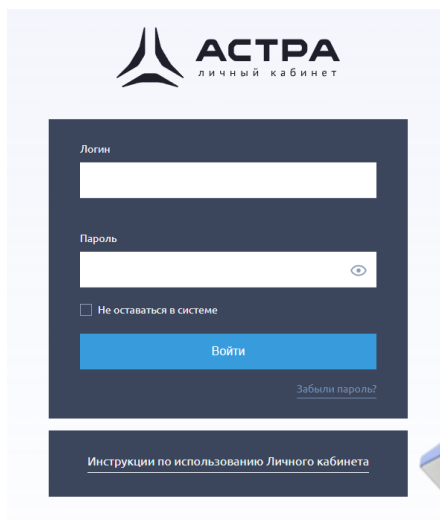
Bash (оболочка Unix)

```
apt -y remove dotnet-runtime-6.0 aspnetcore-runtime-6.0 dotnet-host-6.0 dotnet-hostfxr-6.0
```

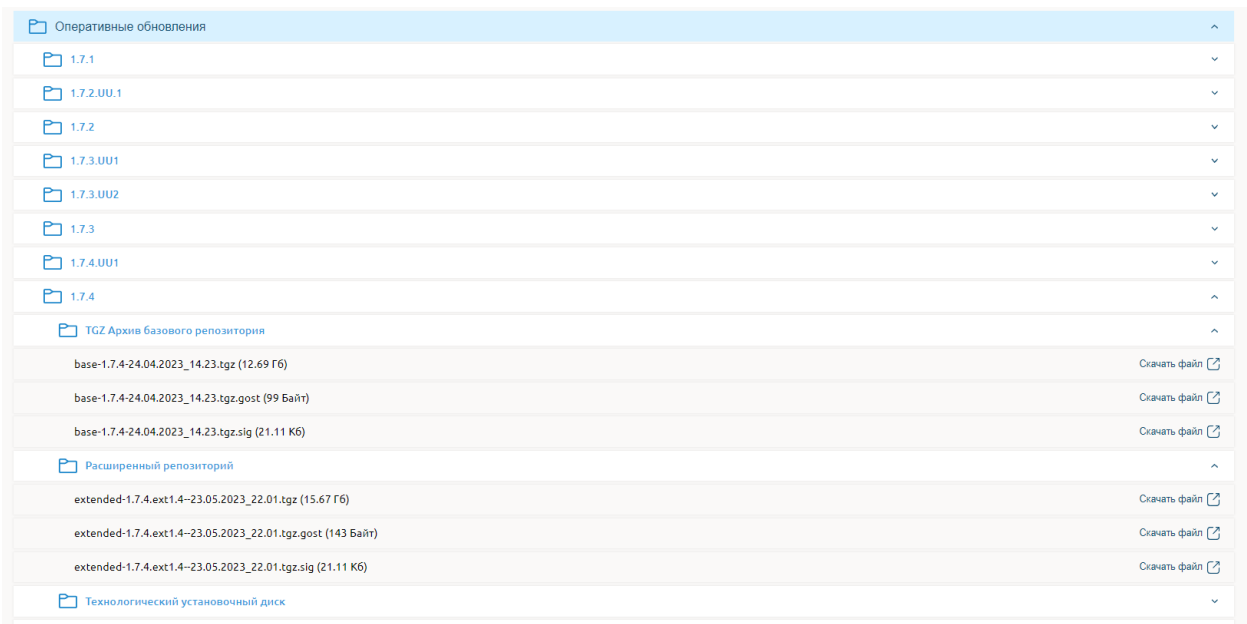
Логи инсталлятора располагаются в **`/var/opt/redcheck-common/log/configuration.log`**

## Подключение репозитория Astra Linux без доступа к сети Интернет

**Шаг 1.** Войдите в личный кабинет Astra Linux, используя логин (e-mail) и пароль:



**Шаг 2.** Перейдите в раздел **Лицензии и сертификаты** → выберите необходимую лицензию → перейдите подраздел **Обновления** → раскройте список **Оперативные обновления** → **1.7.5** → скачайте .iso файлы для **TGZ Архив базового репозитория** и **Расширенный репозиторий**;



**Шаг 3.** Разархивируйте скачанные файлы с расширением .tar → переименуйте появившиеся файлы, добавив в конце расширение .iso → разархивируйте .iso файл и переместите получившийся каталог на хост;

conf	20.10.2023 10:31	Папка с файлами
db	20.10.2023 10:31	Папка с файлами
dists	20.10.2023 10:31	Папка с файлами
pool	20.10.2023 10:35	Папка с файлами
extended-1.7.4.ext1.4--23.05.2023_22.01.iso	15.2023 22:29	Файл "01" 16 488 040 ...

Репозиторий обязательно должен состоять из каталогов **dists** и **pool**

**Шаг 4.** Переместите каталоги в директорию, отличную от пользовательского каталога. В инструкции репозитории перемещаются в /mnt;

```
Bash (оболочка Unix)

mv /home/имя_пользователя/Загрузки/astra-base /mnt/
mv /home/имя_пользователя/Загрузки/astra-main /mnt/
mv /home/имя_пользователя/Загрузки/astra-update /mnt/
mv /home/имя_пользователя/Загрузки/astra-extended /mnt/
```

В инструкции репозитории имеют имена: **astra-base, astra-main, astra-update, astra-extended**

**Шаг 5.** Добавьте репозитории в файл `/etc/apt/sources.list`:

Bash (оболочка Unix)

```
deb file:/mnt/astra-base/ 1.7_x86-64 main contrib non-free
deb file:/mnt/astra-main/ 1.7_x86-64 main contrib non-free
deb file:/mnt/astra-update/ 1.7_x86-64 main contrib non-free
deb file:/mnt/astra-extended/ 1.7_x86-64 astra-ce main contrib non-free
```

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

**Шаг 1.** Откройте файл с помощью команды (`sudo`):

Bash (оболочка Unix)

```
nano /etc/apt/sources.list
```

**Шаг 2.** Переместите курсор в конец документа с помощью стрелки вниз. Для перехода на новую строку используйте клавишу **Enter**;

**Шаг 3.** Скопируйте репозитории и вставьте их с помощью комбинации **Ctrl + U**;

**Шаг 4.** Сохраните файл с помощью комбинации **Ctrl + O**; Для выхода используйте **Ctrl + X**;

## 3.2 Debian

- [Установка СУБД](#)
- [Инсталляция RedCheck](#)
- [Конфигурация RedCheck](#)

### Установка СУБД

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 5.** 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 6.** 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;
```

```
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#
```

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

**Шаг 7.** Завершите сессию командой **exit**

**Шаг 8.** 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 9.** 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# █
```

## Инсталляция RedCheck

Все команды в инструкции выполняются под root-пользователем.

Для обновления RedCheck – [4.8 Обновление RedCheck Nix](#)

## Установка компонентов

Для перемещения по каталогам используйте команду **cd**. Например, чтобы перейти в каталог `/mnt`, напишите **cd /mnt**  
Чтобы автоматически дополнить название каталога или файла, используйте **Tab**

**Шаг 1.** Переместите скачанный архив `redcheck-repo-2.7.0.8862.tar.gz` в директорию, отличную от пользовательского каталога. В инструкции архив перемещается в `/mnt`;

Bash (оболочка Unix)

```
mv /home/имя_пользователя/Загрузки/redcheck-repo-2.7.0.8862.tar.gz
/mnt/
```

**Шаг 3.** Перейдите в каталог и разархивируйте дистрибутив;

Bash (оболочка Unix)

```
cd /mnt
```

Bash (оболочка Unix)

```
tar -xf redcheck-repo-2.7.0.8862.tar.gz
```

**Шаг 4.** Добавьте GPG-ключ, который находится в только что разархивированном каталоге;

Bash (оболочка Unix)

```
apt-key add redcheck-repo/PUBLIC-GPG-KEY-redcheck
```

**Шаг 5.** Создайте файл **redcheck.list** и добавьте в него запись репозитория;

Bash (оболочка Unix)

```
touch /etc/apt/sources.list.d/redcheck.list  
echo "deb file:/mnt/redcheck-repo/ 1.7_x86-64 non-free dotnet" >  
/etc/apt/sources.list.d/redcheck.list
```

**Шаг 6.** Обновите пакеты;

Bash (оболочка Unix)

```
apt -y update
```

**Шаг 7.** Установите компоненты RedCheck;

Bash (оболочка Unix)

```
apt install -y icu-devtools=63.1-6+deb10u2 libicu63.1-6+deb10u2 libicu-  
dev=63.1-6+deb10u2 -allow-downgrades
```

Bash (оболочка Unix)

```
apt -y install redcheck-dotnet-runtime redcheck-aspnetcore-runtime  
redcheck-api redcheck-client redcheck-scan-service redcheck-sync-  
service redcheck-cleanup-service
```

Логи инсталлятора располагаются в **`/var/opt/redcheck-common/log/configuration.log`**

## Конфигурация RedCheck

**Шаг 1.** Настройте компоненты RedCheck;

Перед повторной конфигурацией **рекомендуем [сделать резервную копию](#)** базы данных.

Bash (оболочка Unix)

```
redcheck-bootstrap configure -c=all
```

Будет запущен процесс конфигурации компонентов, который потребует ввода данных для доступа к СУБД, лицензионного ключа и других параметров для корректной работы Системы. Данной командой будут сконфигурированы все основные компоненты RedCheck на одном сервере.

На этапе генерации сертификата для протокола HTTPS необходимо ввести названия: **области (страны), города, организации, отдела, электронной почты.**

```
Генерация сертификата..
Введите область
moscow
Введите город
korolev
Введите название организации
altx
Введите отдел
market
Введите адрес электронной почты
info
```

**Шаг 2.** Настройте службу очистки БД:

Bash (оболочка Unix)

```
redcheck-bootstrap configure -c=redcheck-cleanup-service
```

В процессе настройки службы вам нужно ввести URL redcheck-api в формате `http://ip:port`, а также учетные данные пользователя с ролью `RedCheck_Admins`

**Шаг 3.** Укажите в конфигурационном файле `redcheck-client` строку подключения к службе очистки (`http://ip_rest_api:8740`);

Bash (оболочка Unix)

```
nano /var/opt/redcheck-client/conf/redcheck-web.dll.config
```

Пример конфигурационного файла после редактирования.

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <appSettings>
    <add key="RestUrl" value="192.168.80.169" />
    <add key="RestPort" value="8081" />
    <add key="RestApiVersion" value="0.3" />
    <add key="RestProtocol" value="http" />
    <add key="RestExtendedConnectionTimeout" value="100" />
    <add key="SessionTimeout" value="151" />
    <add key="CleanupServiceUrl" value="http://192.168.80.169:8740" />
  </appSettings>
</configuration>
```

**Шаг 4.** Перезапустите компонент redcheck-client;

Bash (оболочка Unix)

```
systemctl restart redcheck-client
```

### 3.3 РЕД ОС

- Установка СУБД
- Инсталляция RedCheck
- Конфигурация RedCheck



## Установка СУБД

### Содержание

- [Установка СУБД PostgreSQL с репозитория РЕД ОС](#)
- [Настройка СУБД](#)

## Установка СУБД PostgreSQL с репозитория РЕД ОС

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

**Шаг 2.** Войдите под root пользователем с помощью команды **su**;

**Шаг 3.** Установите PostgreSQL следующей командой;

Устанавливать можно любую версию postgresql, имеющуюся в репозиториях РЕД ОС;

Bash (оболочка Unix)

```
dnf -y install postgresql15-server postgresql15-contrib
```

**Шаг 4.** Произведите инициализацию базы данных postgresql;

Bash (оболочка Unix)

```
postgresql-15-setup initdb
```

**Шаг 5.** Запустите службу postgresql и добавьте ее в автозагрузку;

Bash (оболочка Unix)

```
systemctl enable postgresql-15 --now
```

Для проверки статуса службы используйте команду **systemctl status postgresql-15**

## Настройка СУБД

**Шаг 6.** Создайте пользователя для администрирования СУБД;

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

Bash (оболочка Unix)

```
sudo 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 7.** Завершите сессию командой **exit**

**Шаг 8.** Откройте доступ по сети для серверов, на которых планируется установка серверного-компонента и служб сканирования и синхронизации RedCheck;

Bash (оболочка Unix)

```
echo "listen_addresses = 'ip_СУБД'" >>  
/var/lib/pgsql/15/data/postgresql.conf
```

Bash (оболочка Unix)

```
echo host all имя_пользователя_СУБД имя_сети/маска md5 >>  
/var/lib/pgsql/15/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 a**

**Шаг 9.** Перезапустите PostgreSQL.

Bash (оболочка Unix)

```
systemctl restart postgresql-15
```

Для установки firewall используйте команду:

Bash (оболочка Unix)

```
dnf -y install firewalld
```

Запустите firewall:

Bash (оболочка Unix)

```
systemctl start firewalld
```

Добавьте исключение для порта, на котором работает postgresql:

Bash (оболочка Unix)

```
firewall-cmd --permanent --add-port=5432/tcp
```

```
firewall-cmd --reload
```

## Инсталляция RedCheck

Для перемещения по каталогам используйте команду **cd**. Например, чтобы перейти в каталог /mnt, напишите **cd /mnt**  
Чтобы автоматически дополнить название каталога или файла, используйте **Tab**

Для обновления RedCheck – [4.8 Обновление RedCheck Nix](#)

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

**Шаг 2.** Войдите под root пользователем с помощью команды **su**;

**Шаг 3.** Смонтируйте установочный диск и создайте файл cd.repo;

Bash (оболочка Unix)

```
touch /etc/yum.repos.d/cd.repo
```

**Bash (оболочка Unix)**

```
echo -e "[cd]
name=CD
baseurl=file:///run/media/user/redos-DVD-x86_64-MUROM-7.3
enabled=1
gpgcheck=0" > /etc/yum.repos.d/cd.repo
```

**Шаг 4.** Переместите скачанный архив redcheck-redos-repo-2.7.0.28053.tar.gz в директорию, отличную от пользовательского каталога. В инструкции архив перемещается в /mnt;

Bash (оболочка Unix)

```
mv /home/имя_пользователя/Загрузки/redcheck-redos-repo-
2.7.0.28053.tar.gz /mnt/
```

**Шаг 5.** Перейдите в каталог и разархивируйте дистрибутив;

Bash (оболочка Unix)

```
cd /mnt
```

Bash (оболочка Unix)

```
tar -xf redcheck-redos-repo-2.7.0.28053.tar.gz
```

**Шаг 6.** Создайте файл `redcheck.repo` и добавьте в него запись репозитория;

Bash (оболочка Unix)

```
touch /etc/yum.repos.d/redcheck.repo
```

Bash (оболочка Unix)

```
echo -e "[redcheck-repo]
name=RedCheck 2.7.0
baseurl=file:/mnt/redcheck-redos-repo/redcheck-base
enabled=1
gpgcheck=0
gpgkey=file:/mnt/redcheck-redos-repo/redcheck-base/PUBLIC-GPG-KEY-
redcheck" > /etc/yum.repos.d/redcheck.repo
```

**Шаг 7.** Создайте файл `redcheck-dotnet.repo` и добавьте в него запись репозитория;

Bash (оболочка Unix)

```
touch /etc/yum.repos.d/redcheck-dotnet.repo
```

**Bash (оболочка Unix)**

```
echo -e "[redcheck-dotnet-repo]
name=ALTX .NET 6.0.26
baseurl=file:/mnt/redcheck-redos-repo/redcheck-dotnet
enabled=1
gpgcheck=0
gpgkey=file:/mnt/redcheck-redos-repo/redcheck-base/PUBLIC-GPG-KEY-
redcheck" > /etc/yum.repos.d/redcheck-dotnet.repo
```

**Шаг 8.** Обновите пакеты;

Bash (оболочка Unix)

```
dnf check-update
```

### Шаг 9. Установите компоненты RedCheck;

Bash (оболочка Unix)

```
dnf -y install redcheck-dotnet-runtime redcheck-aspnetcore-runtime  
redcheck-api redcheck-client redcheck-scan-service redcheck-sync-  
service redcheck-cleanup-service
```

Логи инсталлятора располагаются в **/var/opt/redcheck-common/log/configuration.log**





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

**Система сертификации**

Обновления для сертифицированного ПО (92)

- Файлы (28)
- Руководства (6)
- Материалы по сертифицированному ПО (5)
- Обновления Media Kit (21)
- Обновления VmWare (11)
- Обновления контента (4)
- Net Check лицензии (2)
- RedCheck лицензии (2)

Лицензионный ключ	Редакция	Дата окончания
[Redacted]	RedCheck Enterprise	17.04.2025 14:03:06

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

**Управление активацией**

Выполнить активацию

Выполнить ручную активацию

Лицензионный ключ: [Redacted]

Код активации: \* [Redacted]

Принять Отменить

**Шаг 4.** Нажмите **Скачать**;

	Активен	Дата активации	Действия
	False	10.12.2021 09:54:44	<a href="#">Скачать</a>
	True	24.09.2020 11:09:35	<a href="#">Скачать</a>

**Шаг 5.** Сохраните файл license.xml;

## Конфигурация RedCheck

**Шаг 1.** Настройте компоненты RedCheck;

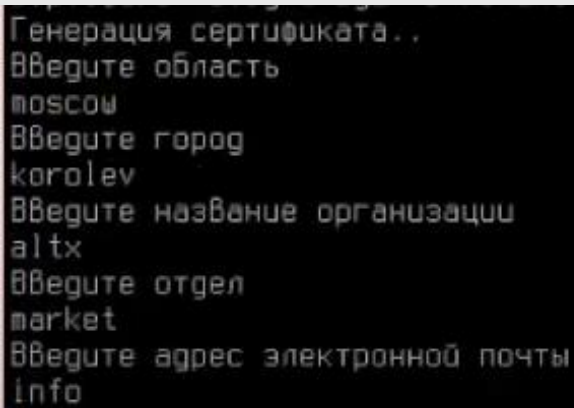
Перед повторной конфигурацией **рекомендуем** [сделать резервную копию](#) базы данных.

Bash (оболочка Unix)

```
redcheck-bootstrap configure -c=all
```

Будет запущен процесс конфигурации компонентов, который потребует ввода данных для доступа к СУБД, лицензионного ключа и других параметров для корректной работы Системы. Данной командой будут сконфигурированы все основные компоненты RedCheck на одном сервере.

На этапе генерации сертификата для протокола HTTPS \необходимо ввести названия: **области (страны), города, организации, отдела, электронной почты.**



```
Генерация сертификата..  
Введите область  
moscow  
Введите город  
korolev  
Введите название организации  
altx  
Введите отдел  
market  
Введите адрес электронной почты  
info
```

Для установки firewall используйте команду:

Bash (оболочка Unix)

```
dnf -y install firewalld
```

Запустите firewall:

Bash (оболочка Unix)

```
systemctl start firewalld
```

Добавьте исключения для портов, на которых работают компоненты RedCheck:

Bash (оболочка Unix)

```
firewall-cmd --permanent --add-port=5432/tcp
```

```
firewall-cmd --reload
```

**Шаг 2.** Настройте службу очистки БД:

Bash (оболочка Unix)

```
redcheck-bootstrap configure -c=redcheck-cleanup-service
```

В процессе настройки службы вам нужно ввести URL redcheck-аpi в формате `http://ip:port`

**Шаг 3.** Укажите в конфигурационном файле redcheck-client строку подключения к службе очистки (`http://ip_rest_api:8740`);

Bash (оболочка Unix)

```
nano /var/opt/redcheck-client/conf/redcheck-web.dll.config
```

Пример конфигурационного файла после редактирования.

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <appSettings>
    <add key="RestUrl" value="192.168.80.169" />
    <add key="RestPort" value="8081" />
    <add key="RestApiVersion" value="0.3" />
    <add key="RestProtocol" value="http" />
    <add key="RestExtendedConnectionTimeout" value="100" />
    <add key="SessionTimeout" value="151" />
    <add key="CleanupServiceUrl" value="http://192.168.80.169:8740" />
  </appSettings>
</configuration>
```

**Шаг 4.** Перезапустите компонент redcheck-client;

Bash (оболочка Unix)

```
systemctl restart redcheck-client
```

## 3.4 SberLinux

- Инсталляция RedCheck
- Конфигурация RedCheck

## Инсталляция RedCheck

В качестве СУБД для RedCheck на SberLinux может использоваться Pangolin. Рекомендуется использовать инструкцию по установке от вендора.

Для обновления RedCheck – [4.8 Обновление RedCheck Nix](#)

Для установки RedCheck необходимо два репозитория: BaseOS и AppStream.

**Шаг 1.** Откройте терминал и войдите под root пользователем с помощью команды **sudo su**;

**Шаг 2.** Переместите скачанный архив `redcheck-sber-repo-2.7.0.92.tar.gz` в директорию, отличную от пользовательского каталога. В инструкции архив перемещается в `/mnt`;

Bash (оболочка Unix)

```
mv /home/имя_пользователя/Загрузки/redcheck-sber-repo-2.7.0.92.tar.gz /mnt/
```

**Шаг 3.** Перейдите в директорию и разархивируйте дистрибутив;

Bash (оболочка Unix)

```
cd /mnt
```

Bash (оболочка Unix)

```
tar -xf redcheck-sber-repo-2.7.0.92.tar.gz
```

**Шаг 4.** Создайте файл `redcheck.repo` и добавьте в него запись репозитория;

Bash (оболочка Unix)

```
touch /etc/yum.repos.d/redcheck.repo
```

Bash (оболочка Unix)

```
echo -e "[redcheck-repo]
name=RedCheck 2.7.0
baseurl=file:/mnt/redcheck-sber-repo/redcheck-base
enabled=1
gpgcheck=0
gpgkey=file:/mnt/redcheck-sber-repo/redcheck-base/PUBLIC-GPG-KEY-
redcheck" > /etc/yum.repos.d/redcheck.repo
```

**Шаг 5.** Создайте файл `redcheck-dotnet.repo` и добавьте в него запись репозитория;

Bash (оболочка Unix)

```
touch /etc/yum.repos.d/redcheck-dotnet.repo
```

Bash (оболочка Unix)

```
echo -e "[redcheck-dotnet-repo]
name=ALTX .NET 6.0.26
baseurl=file:/mnt/redcheck-sber-repo/redcheck-dotnet
enabled=1
gpgcheck=0
gpgkey=file:/mnt/redcheck-sber-repo/redcheck-base/PUBLIC-GPG-KEY-
redcheck" > /etc/yum.repos.d/redcheck-dotnet.repo
```

**Шаг 6.** Обновите пакеты;

Bash (оболочка Unix)

```
dnf check-update
```

**Шаг 7.** Установите компоненты RedCheck;

Bash (оболочка Unix)

```
dnf -y install redcheck-dotnet-runtime redcheck-aspnetcore-runtime
redcheck-api redcheck-client redcheck-scan-service redcheck-sync-
service redcheck-cleanup-service
```

Логи инсталлятора располагаются в `/var/opt/redcheck-`

**common/log/configuration.log**





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

**Система сертификации**

Обновления для сертифицированного ПО (92)

- Файлы (28)
- Руководства (6)
- Материалы по сертифицированному ПО (5)
- Обновления Media Kit (21)
- Обновления VmWare (11)
- Обновления контента (4)
- Net Check лицензии (2)
- RedCheck лицензии (2)

Лицензионный ключ	Редакция	Дата окончания
[Redacted]	RedCheck Enterprise	17.04.2025 14:03:06

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

**Управление активацией**

Выполнить активацию

Выполнить ручную активацию

Лицензионный ключ: [Redacted]

Код активации: \* [Redacted]

Принять Отменить

**Шаг 4.** Нажмите **Скачать**;

	Активен	Дата активации	Действия
	False	10.12.2021 09:54:44	<a href="#">Скачать</a>
	True	24.09.2020 11:09:35	<a href="#">Скачать</a>

**Шаг 5.** Сохраните файл license.xml;

## Конфигурация RedCheck

**Шаг 1.** Настройте компоненты RedCheck;

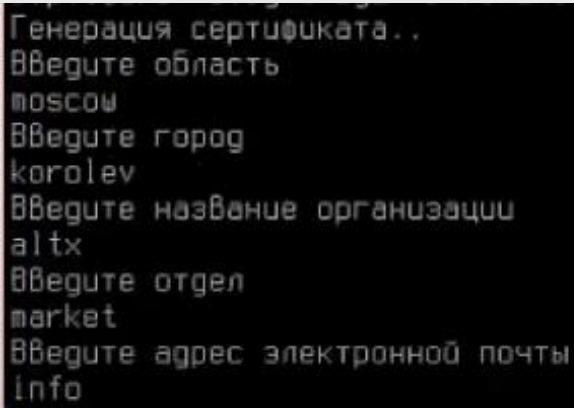
Перед повторной конфигурацией **рекомендуем** [сделать резервную копию](#) базы данных.

Bash (оболочка Unix)

```
redcheck-bootstrap configure -c=all
```

Будет запущен процесс конфигурации компонентов, который потребует ввода данных для доступа к СУБД, лицензионного ключа и других параметров для корректной работы Системы. Данной командой будут сконфигурированы все основные компоненты RedCheck на одном сервере.

На этапе генерации сертификата для протокола HTTPS необходимо ввести названия: **области (страны), города, организации, отдела, электронной почты.**



```
Генерация сертификата..  
Введите область  
moscow  
Введите город  
korolev  
Введите название организации  
altx  
Введите отдел  
market  
Введите адрес электронной почты  
info
```

Для установки firewall используйте команду:

Bash (оболочка Unix)

```
dnf -y install firewalld
```

Запустите firewall:

Bash (оболочка Unix)

```
systemctl start firewalld
```

Добавьте исключения для портов, на которых работают компоненты RedCheck:

Bash (оболочка Unix)

```
firewall-cmd --permanent --add-port=5432/tcp
```

```
firewall-cmd --reload
```

**Шаг 2.** Настройте службу очистки БД:

Bash (оболочка Unix)

```
redcheck-bootstrap configure -c=redcheck-cleanup-service
```

В процессе настройки службы вам нужно ввести URL redcheck-аpi в формате `http://ip:port`

**Шаг 3.** Укажите в конфигурационном файле redcheck-client строку подключения к службе очистки (`http://ip_rest_api:8740`);

Bash (оболочка Unix)

```
nano /var/opt/redcheck-client/conf/redcheck-web.dll.config
```

Пример конфигурационного файла после редактирования.

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <appSettings>
    <add key="RestUrl" value="192.168.80.169" />
    <add key="RestPort" value="8081" />
    <add key="RestApiVersion" value="0.3" />
    <add key="RestProtocol" value="http" />
    <add key="RestExtendedConnectionTimeout" value="100" />
    <add key="SessionTimeout" value="151" />
    <add key="CleanupServiceUrl" value="http://192.168.80.169:8740" />
  </appSettings>
</configuration>
```

**Шаг 4.** Перезапустите компонент redcheck-client;

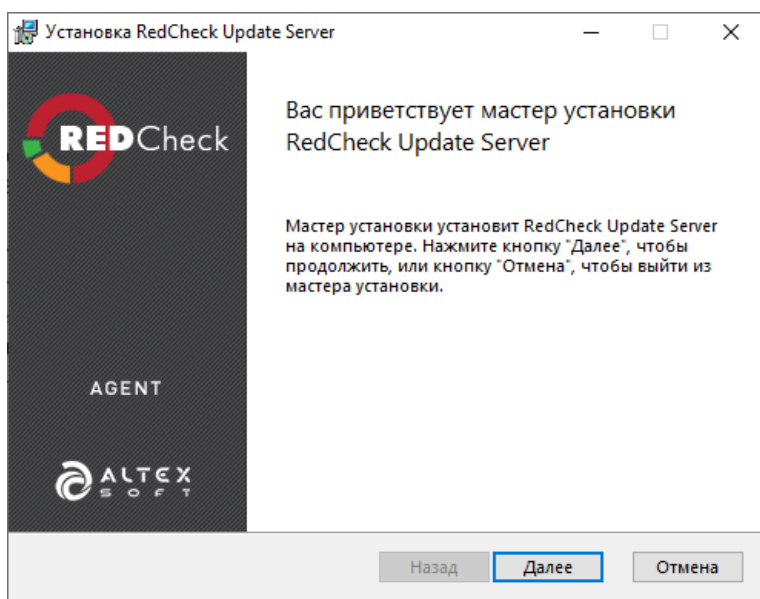
Bash (оболочка Unix)

```
systemctl restart redcheck-client
```

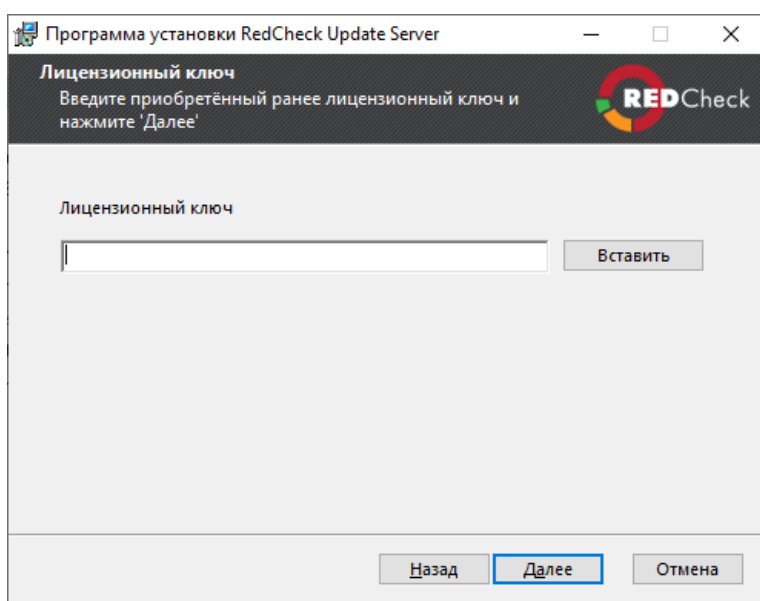
### 3.5 Установка RedCheck Update Server (Windows)

Компонент не является обязательным и лицензируется отдельно. Установка RedCheck Update Server производится в DMZ-сегменте сети для обновления контента безопасности без доступа к сети Интернет со стороны службы синхронизации (RedCheck Sync).

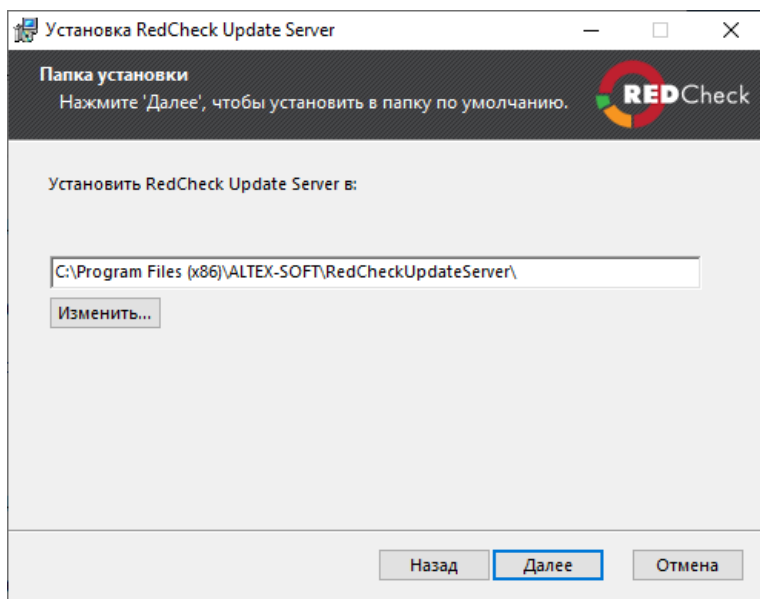
**Шаг 1.** Запустите инсталляционный пакет **RedCheckUpdateServer.msi**;



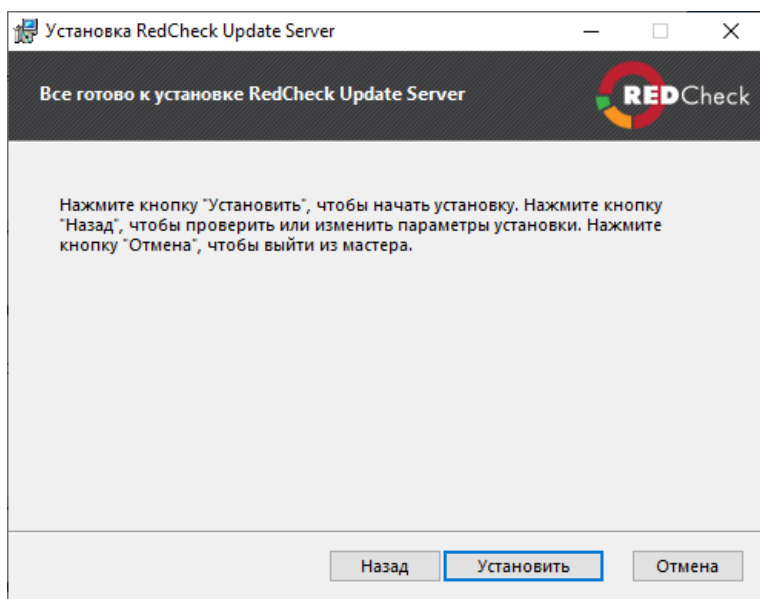
**Шаг 2.** Введите лицензионный ключ → **Далее**;



**Шаг 3.** Укажите директорию для установки;



**Шаг 4.** Нажмите **Установить**.



После установки необходимо произвести настройку ([4.3.3 Синхронизация через RedCheck Update Server](#)).

## 3.6 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

- [3.6.1 Установка на сканируемом хосте в ручном режиме](#)
- [3.6.2 Установка через групповые политики домена](#)



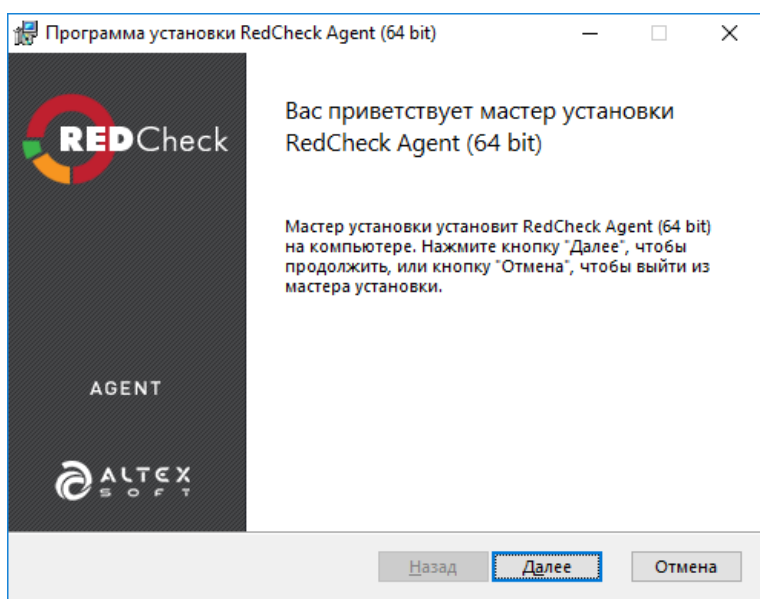
### 3.6.1 Установка на сканируемом хосте в ручном режиме

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

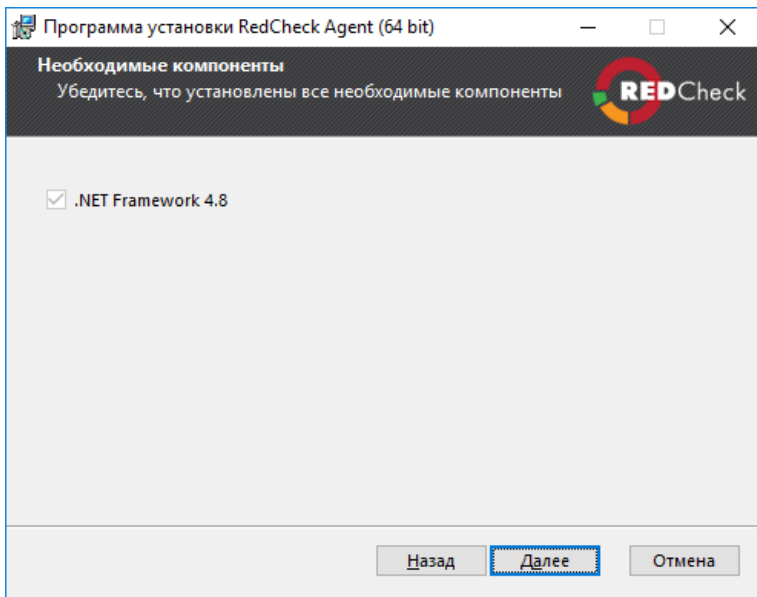
- Microsoft .NET Framework 4.8 ([4.3.2 Установка Microsoft .NET Framework](#)).

Возможна автоматическая установка через командную строку ([4.6.3 Агент RedCheck](#))

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

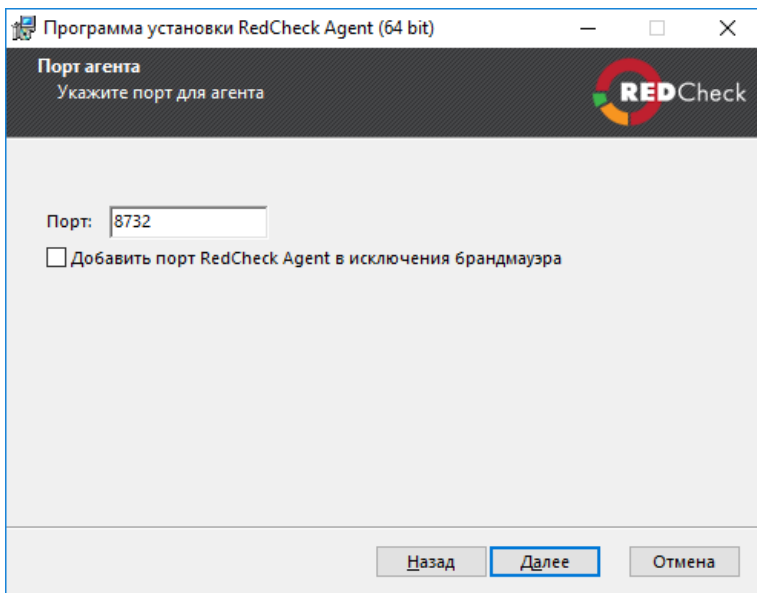


**Шаг 2.** Инсталлятор проверит наличие всех необходимых компонентов → **Далее;**

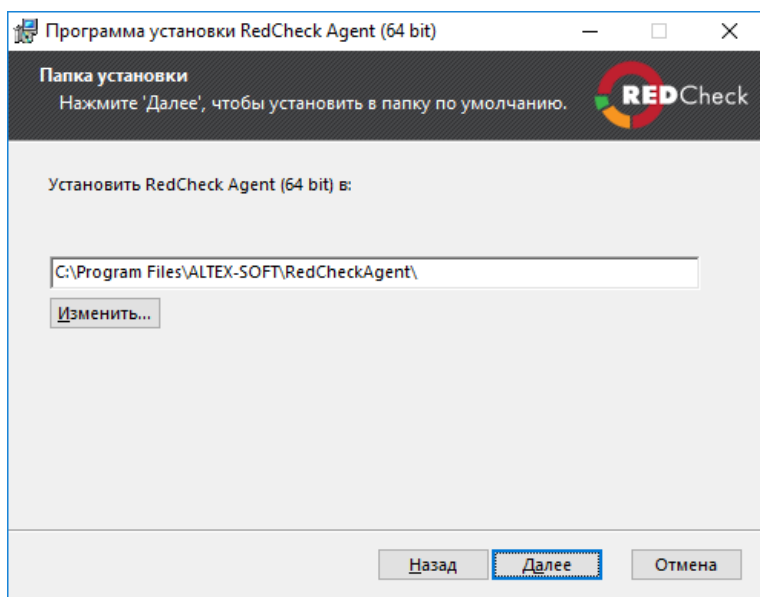


**Шаг 3.** Задайте порт агента (по умолчанию 8732) и отметьте поле **Добавить порт... в исключение брандмауэра** → **Далее**;

Изменить порт можно после установки ([4.11.2 Изменение порта для агента RedCheck](#)).

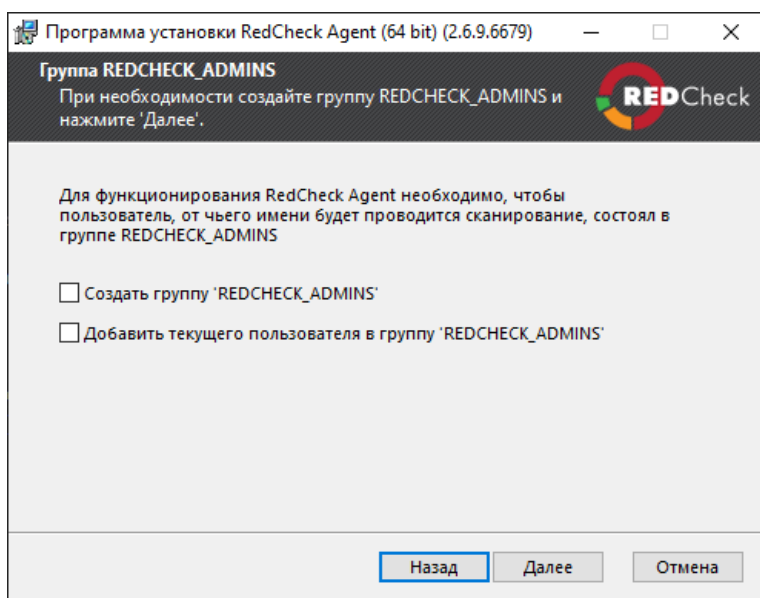


**Шаг 4.** Укажите директорию для установки агента → **Далее**;



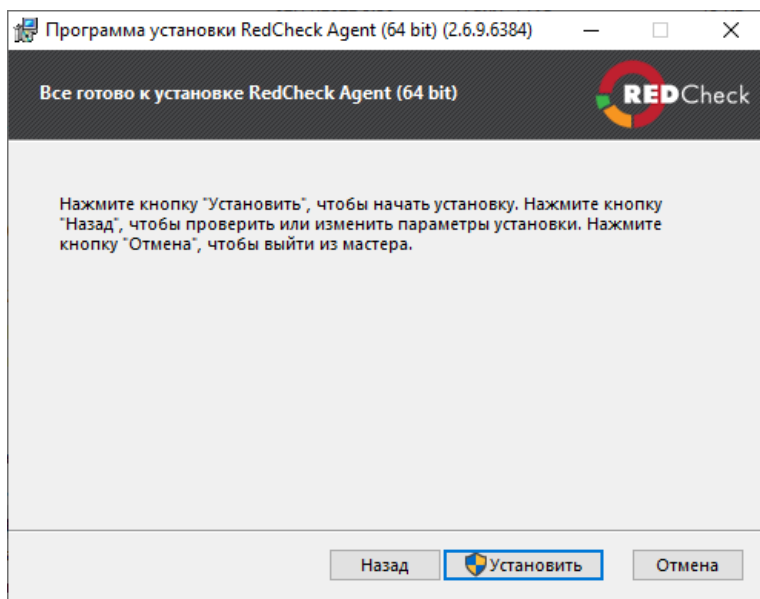
**Шаг 5.** По необходимости отметьте создание локальной группы безопасности REDCHECK\_ADMINS и добавление в нее пользователя, из под которого производится установка агента → **Далее;**

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.

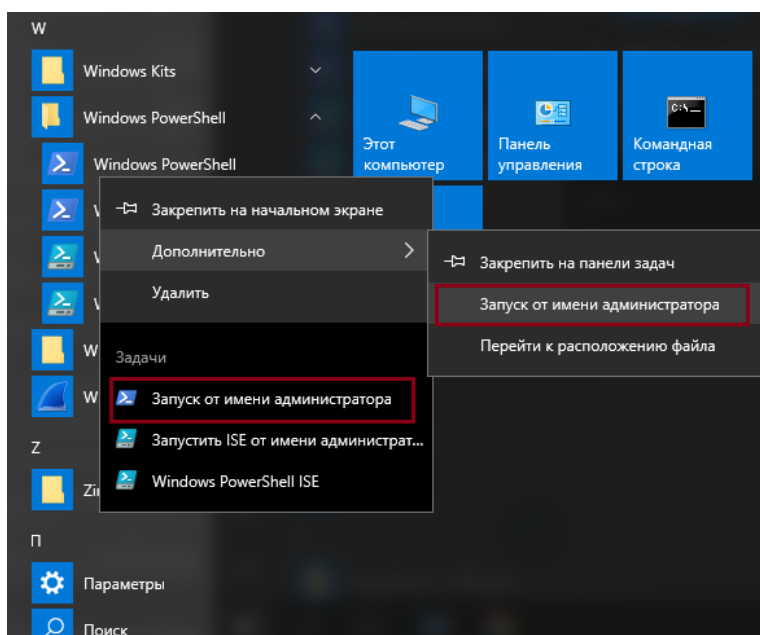
## Шаг 6. Нажмите **Установить**;



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
```

## 3.6.2 Установка через групповые политики домена

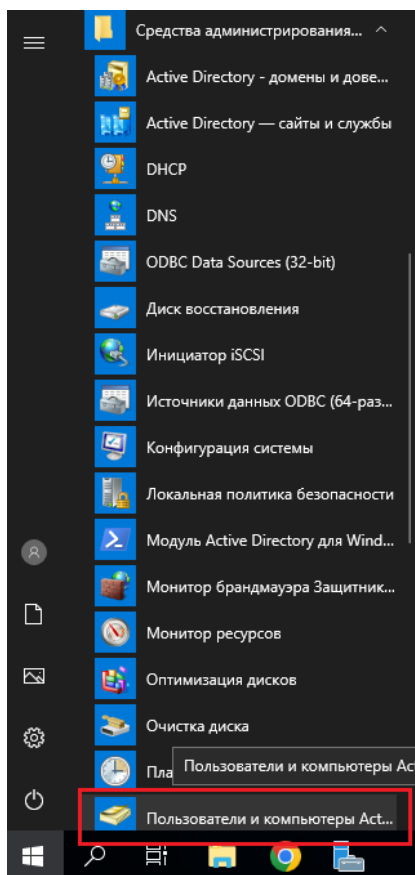
Инсталляция агента сканирования RedCheck в доменном окружении осуществляется посредством групповых политик в несколько этапов:

- [Создание и настройка группы безопасности](#)
- [Создание и настройка сетевой папки](#)
- [Настройка групповой политики](#)

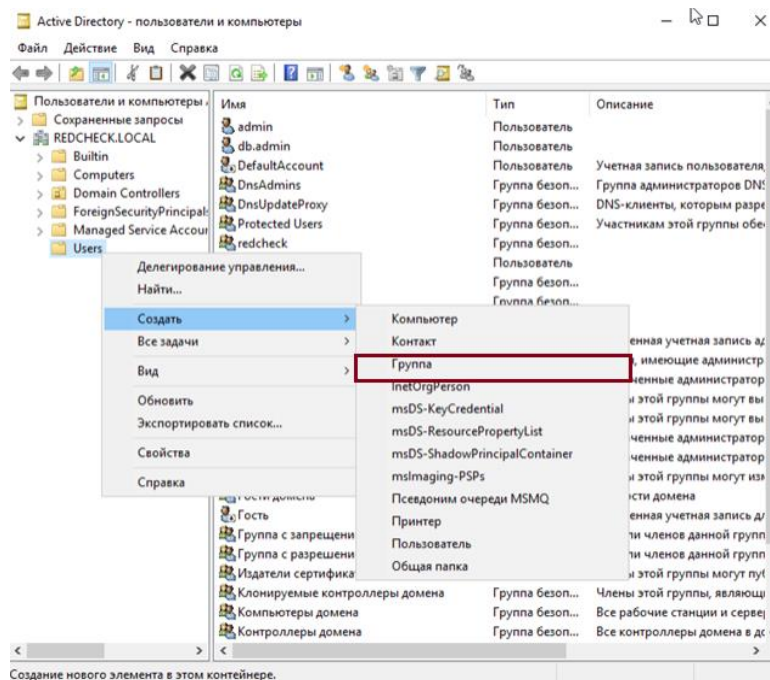
Для обеспечения большей безопасности и контроля за установкой Агента, создайте группу безопасности, в которой определите, какие устройства подлежат установке, а какие нет. Если такой ГБ не требуется, начните с шага 8.

### Создание и настройка группы безопасности

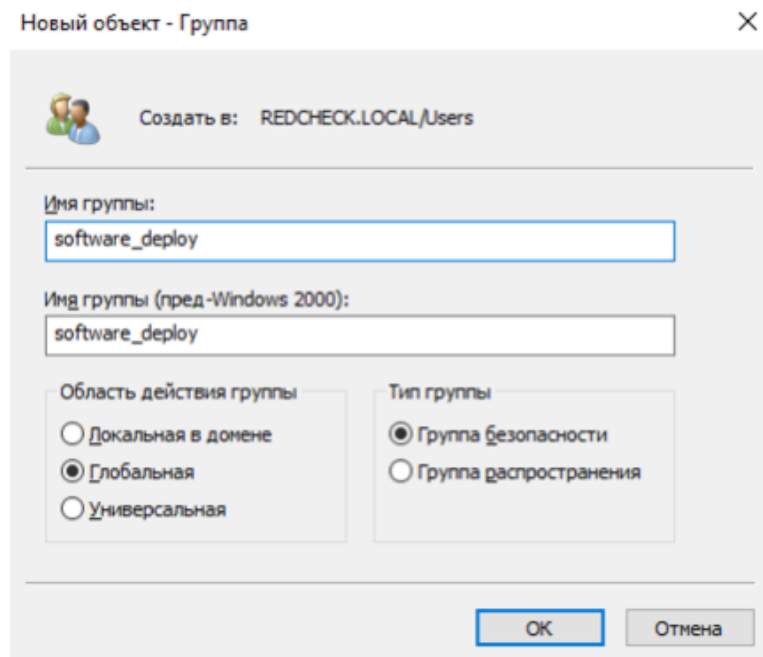
**Шаг 1. Пуск → Средства администрирования Windows → Пользователи и компьютеры Active Directory;**



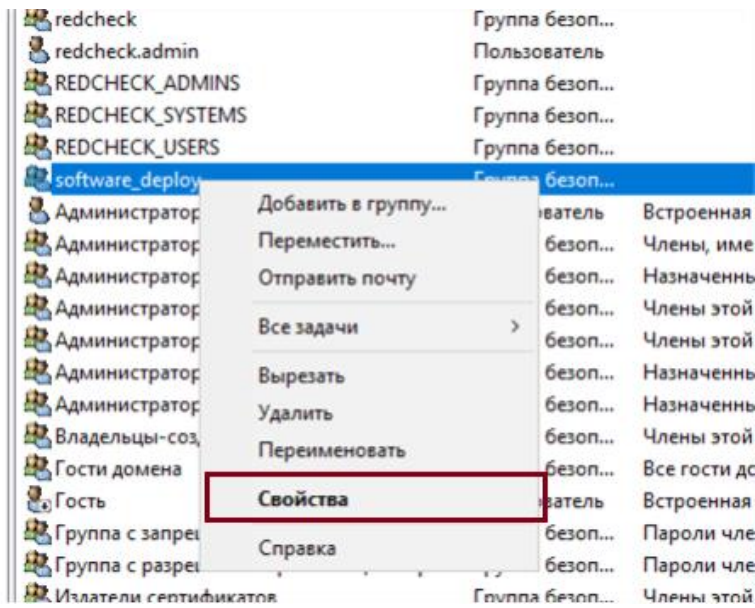
**Шаг 2.** ПКМ по **Users** → **Создать** → **Группа**;



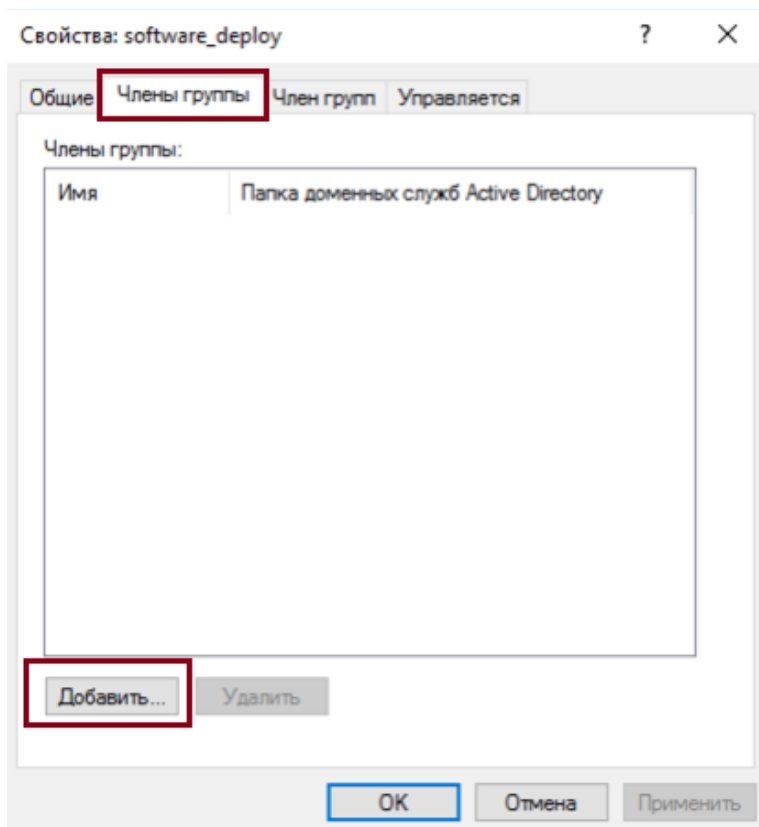
**Шаг 3.** В поле **Имя группы** укажите название группы (в примере **software\_deploy**). Область действия группы **Глобальная**; тип группы **Группа безопасности** → **ОК**.



**Шаг 4.** ПКМ по **software\_deploy** → **Свойства**;



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



**Шаг 6.** Нажмите **Типы объектов**



Выбор: "Пользователи", "Контакты", "Компьютеры", "Учетные записи служ... X

Выберите тип объекта:  
"Пользователи", "Компьютеры", "Учетные записи служб", "Группы" **Типы объектов...**

В следующем месте:  
REDCHECK.LOCAL **Размещение...**

Введите имена выбираемых объектов (примеры):  
 **Проверить имена**

**Дополнительно...** **OK** **Отмена**

Отметьте **Компьютеры**;

Типы объектов X

Выберите типы объектов, которые вы хотите найти.

Типы объектов:

- Другие объекты
- Контакты
- Учетные записи служб
- Компьютеры**
- Группы
- Пользователи

**OK** **Отмена**

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

Выбор: "Пользователи", "Контакты", "Компьютеры", "Учетные записи служ... X

Выберите тип объекта:  
"Пользователи", "Компьютеры", "Учетные записи служб", "Группы" **Типы объектов...**

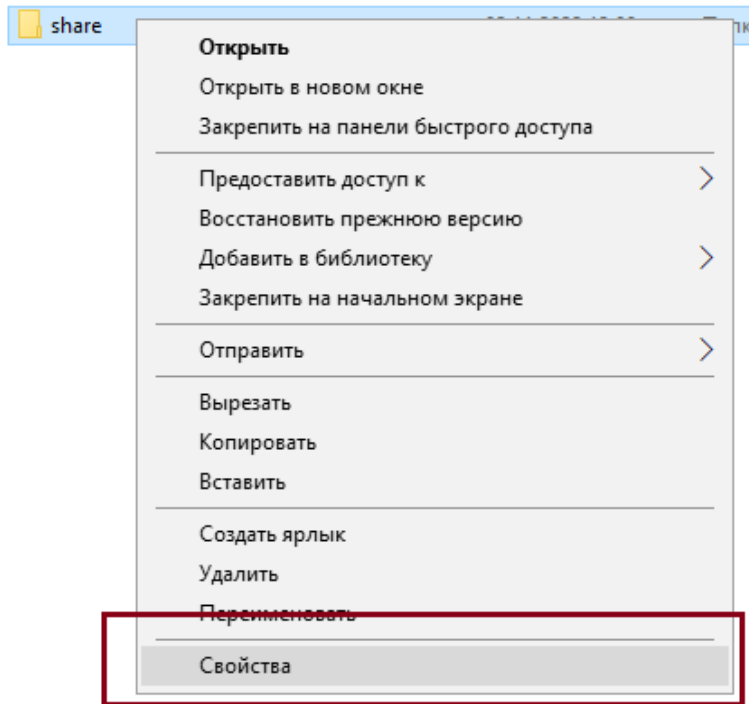
В следующем месте:  
REDCHECK.LOCAL **Размещение...**

Введите имена выбираемых объектов (примеры):  
ARM **Проверить имена**

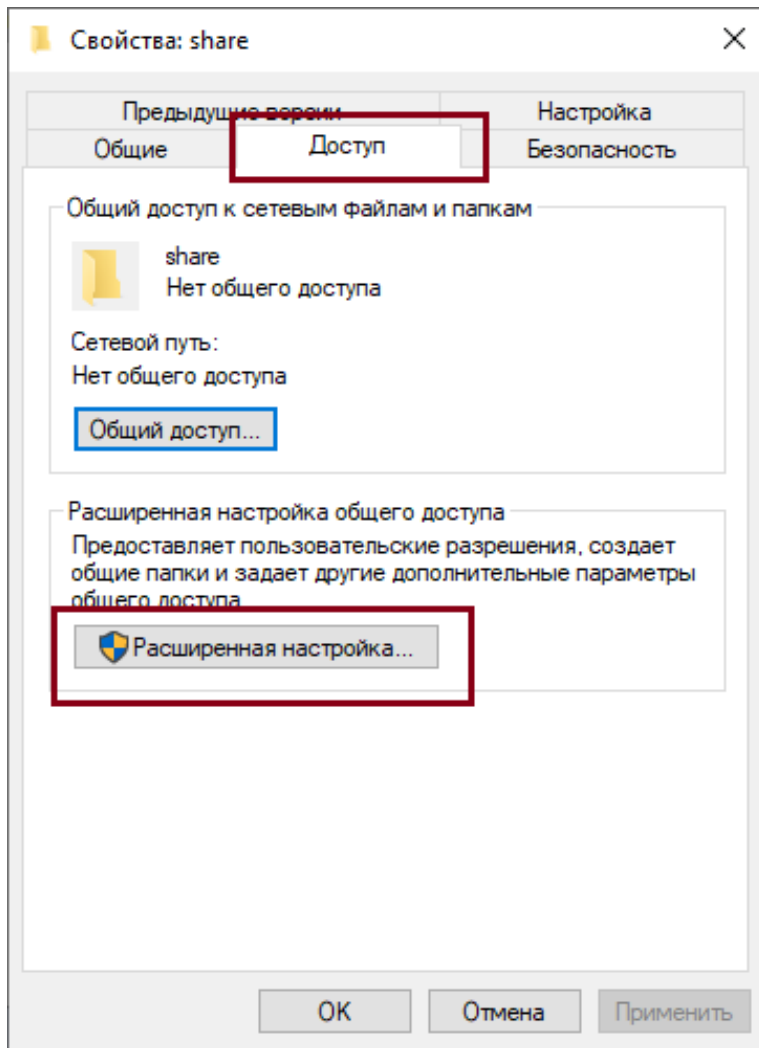
**Дополнительно...** **OK** **Отмена**

## Создание и настройка сетевой папки

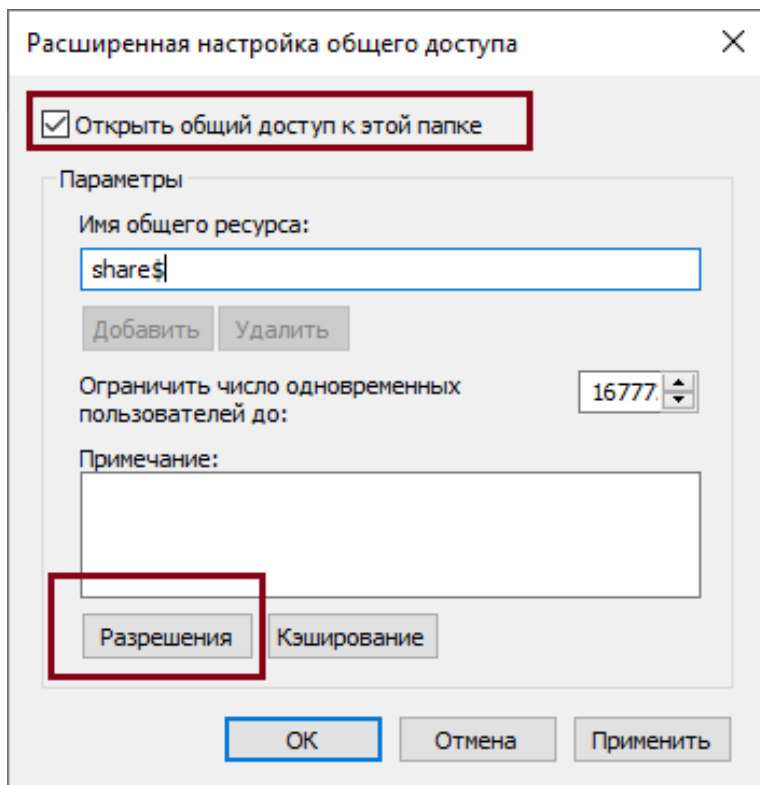
**Шаг 8.** Создайте директорию с произвольным названием (например, C:\share) → ПКМ по созданной директории → **Свойства**;



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

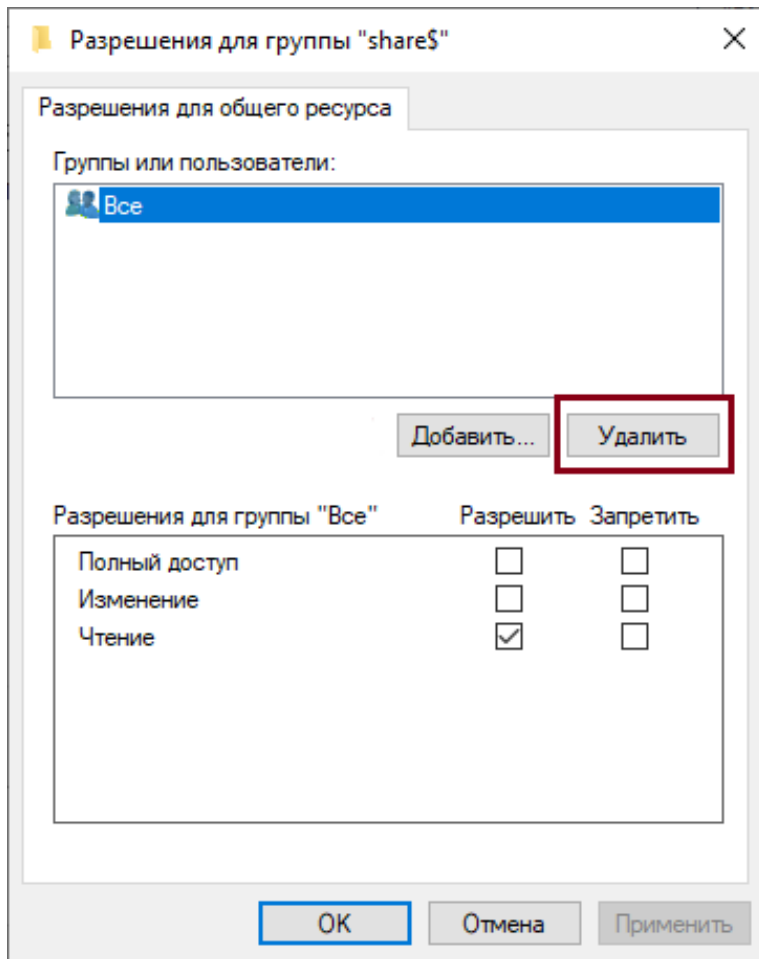


**Шаг 10.** Отметьте **Открыть общий доступ** → **Разрешения**;

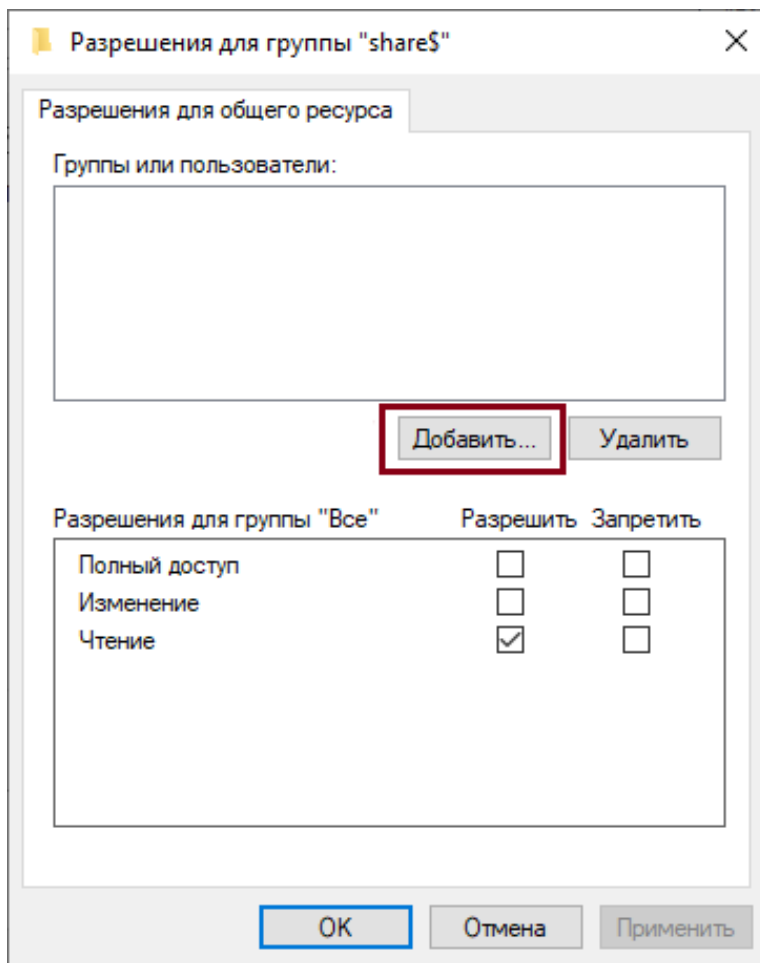


Символ \$ на конце имени папки позволяет скрыть её из сетевого окружения пользователей.

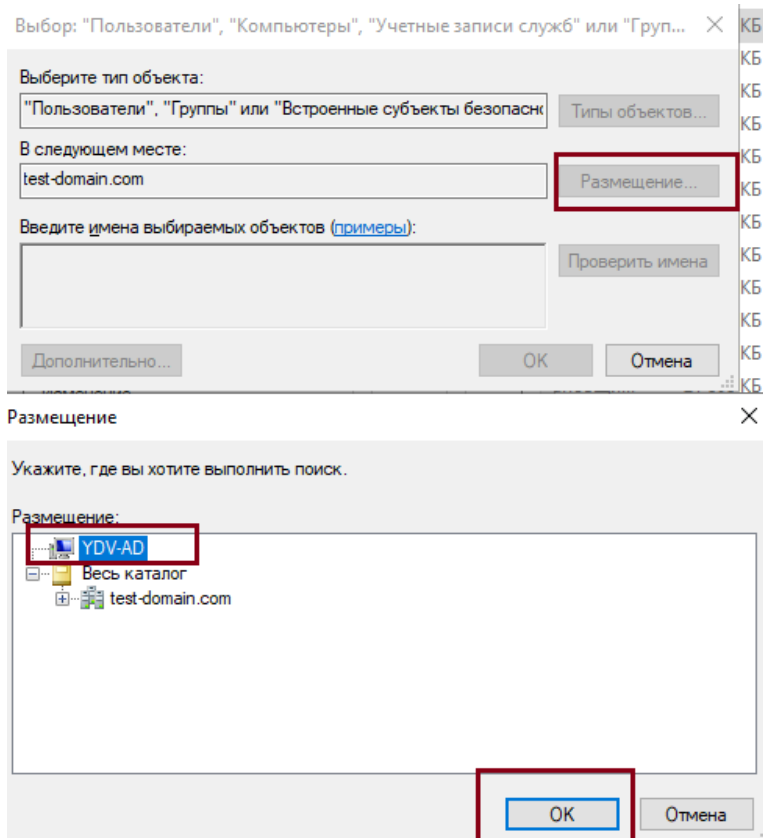
**Шаг 11.** Удалите группу **Все**;



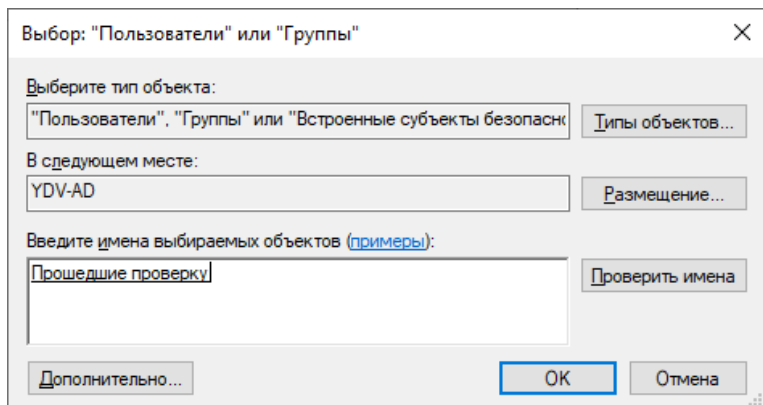
Нажмите **Добавить**;



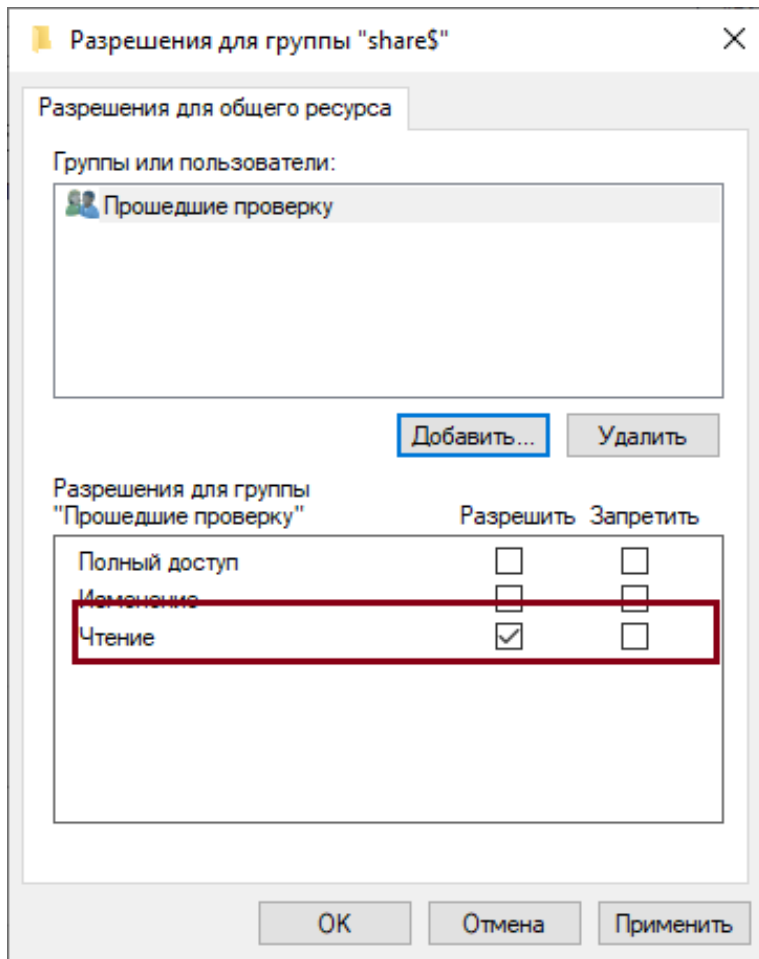
**Шаг 12.** Нажмите **Размещение** → выберите локальный компьютер → **ОК**;



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

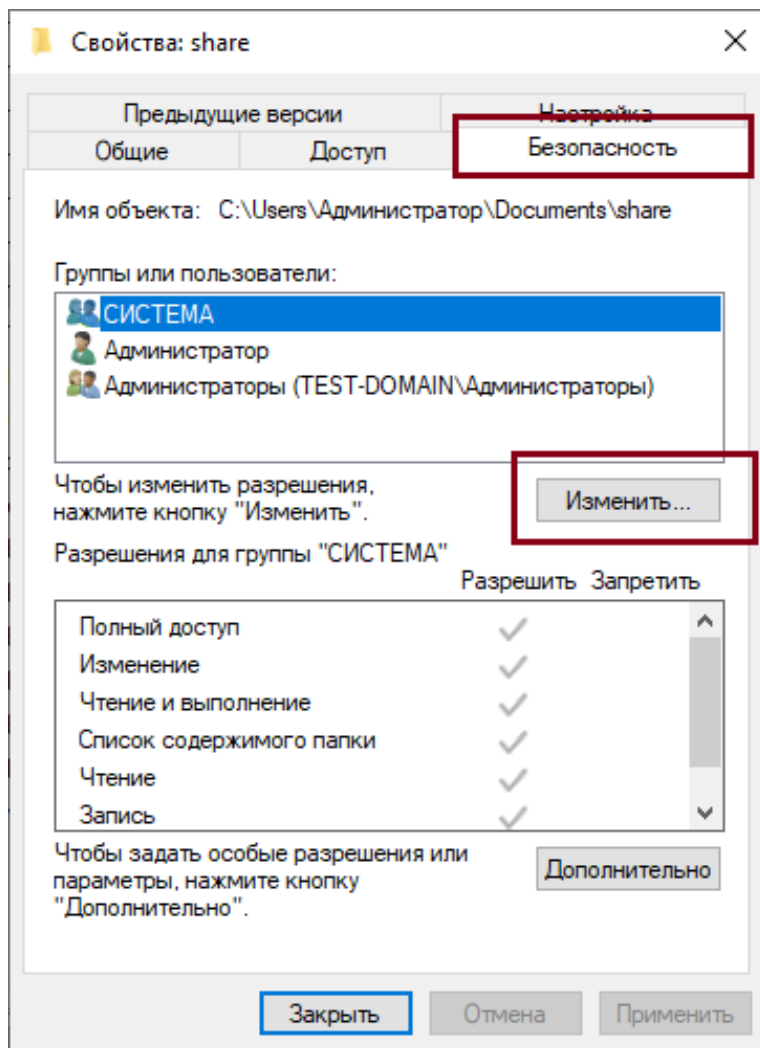


Предоставьте разрешение на **Чтение**;

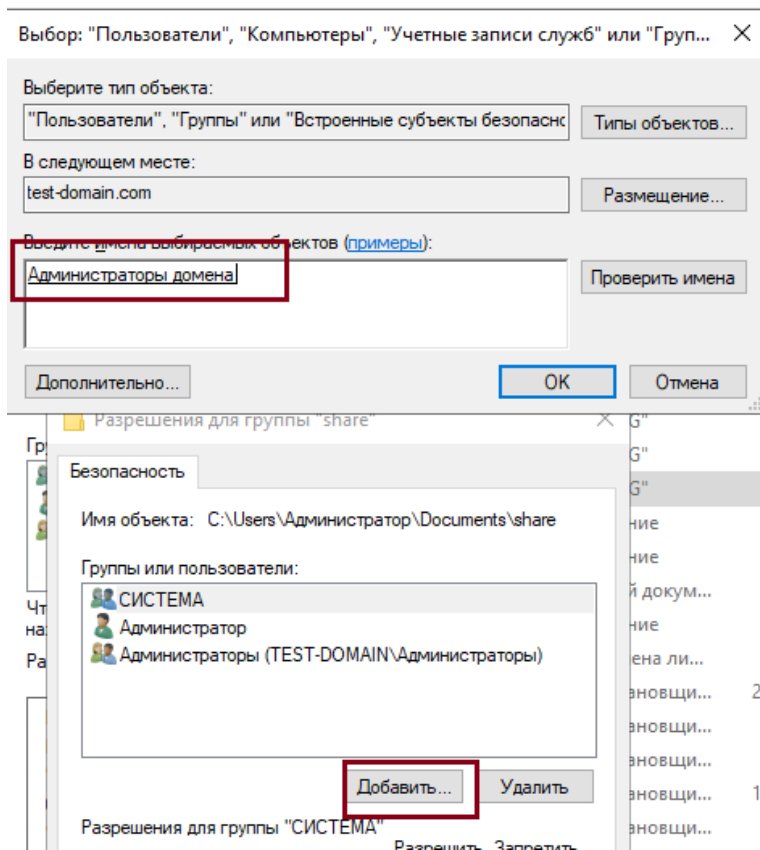


**Шаг 14.** В свойствах директории перейдите в **Безопасность** → **Изменить**;

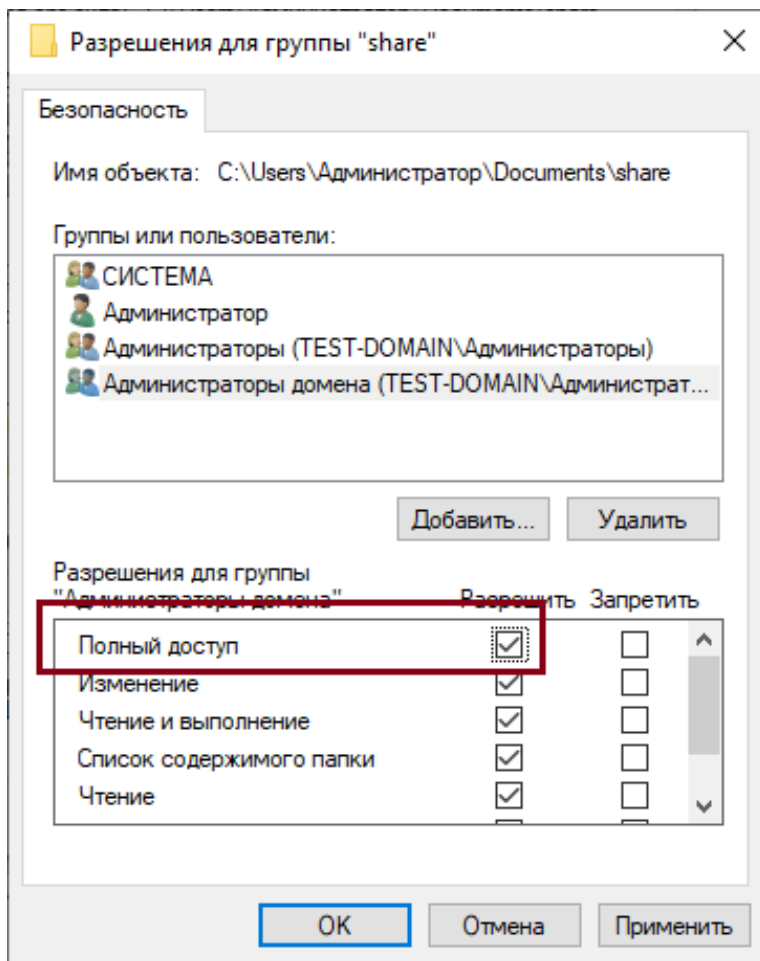




**Шаг 15.** Нажмите **Добавить** → введите **Администраторы домена** → **ОК**;



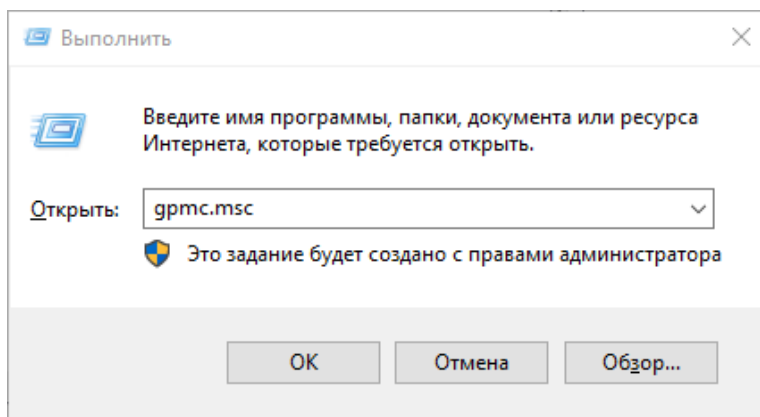
**Шаг 16.** Для **Администраторы домена** отметьте **Полный доступ** → **ОК**;



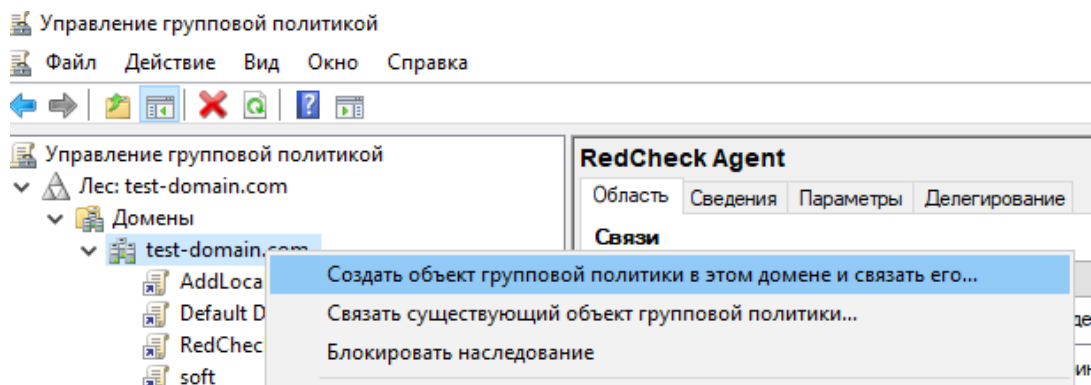
**Шаг 17.** Скопируйте в созданную директорию установочный файл Агента.

## Настройка групповой политики

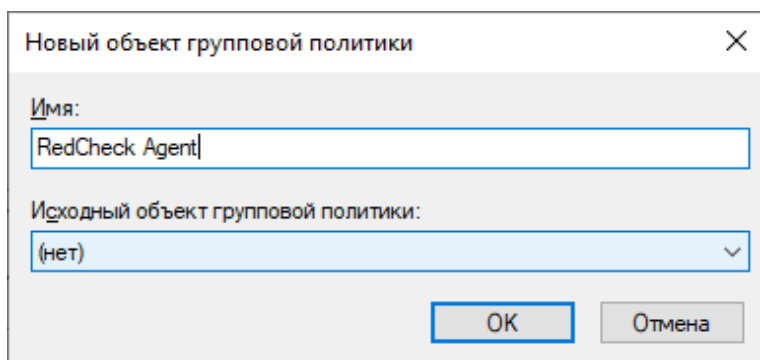
**Шаг 18.** Нажмите **Win + R** → введите **gpmsc.msc**;



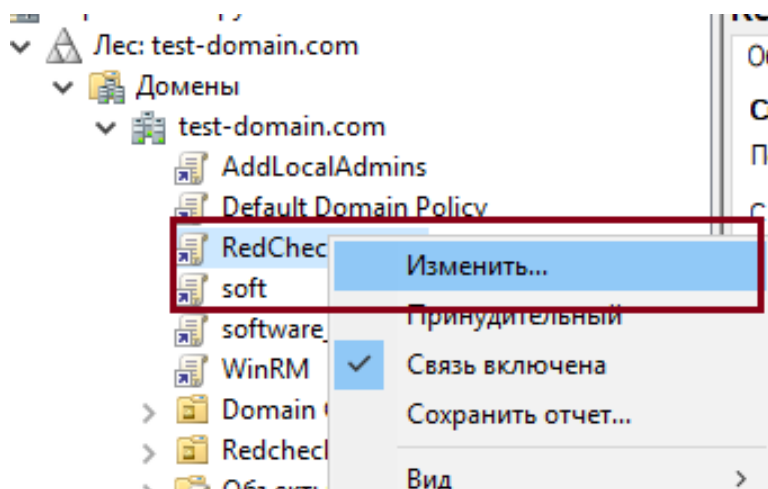
**Шаг 19.** Раскройте **Домены** → ПКМ по домену → **Создать объект групповой политики в этом домене...**;



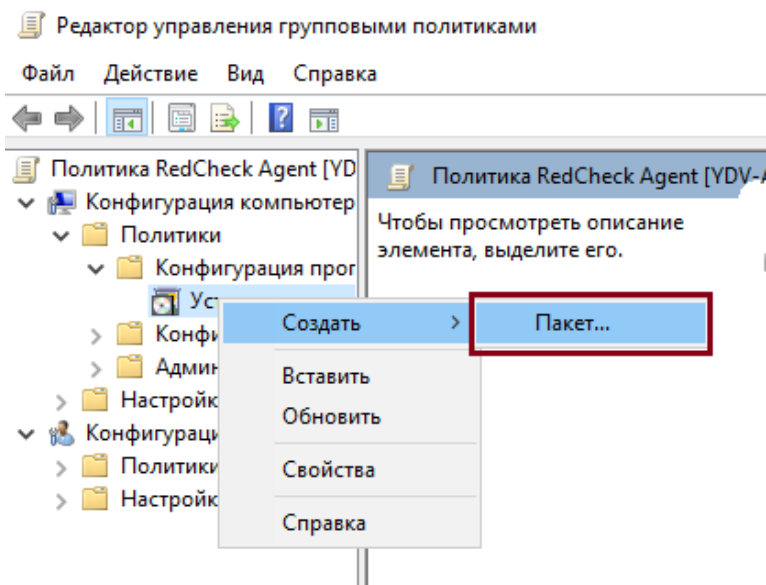
Введите имя для групповой политики → **ОК**;



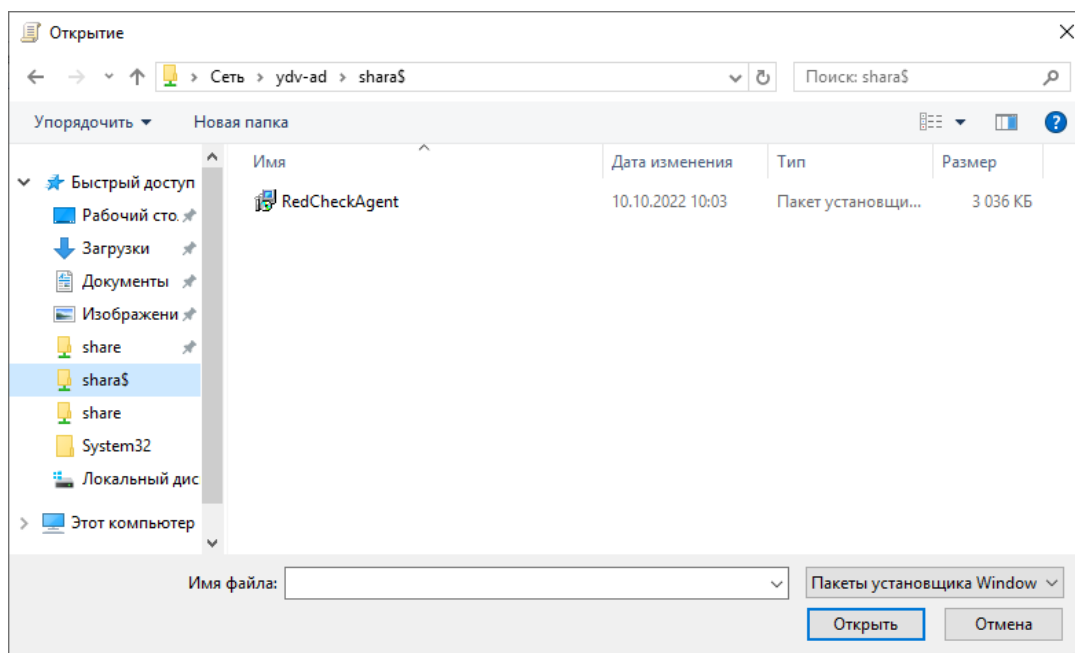
**Шаг 20.** ПКМ по созданной политике → **Изменить**;



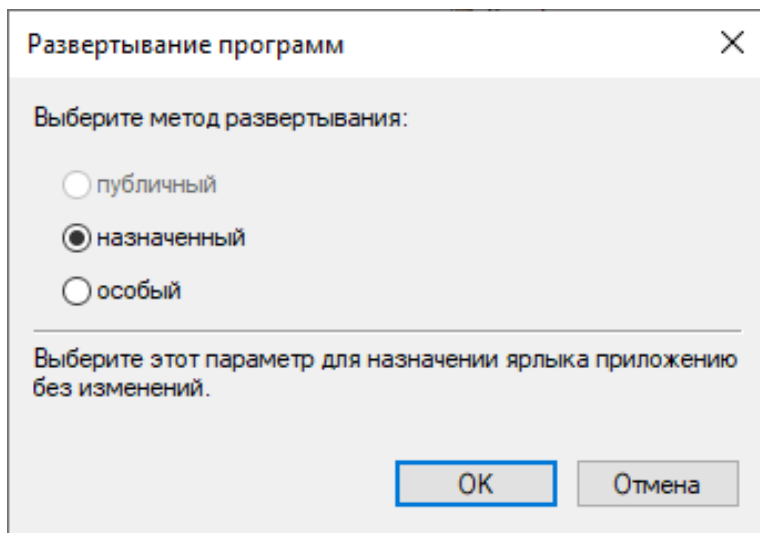
**Шаг 21.** Раскройте **Конфигурация компьютера** → **Политики** → **Конфигурация программ** → ПКМ по **Установка программ** → **Создать** → **Пакет**;



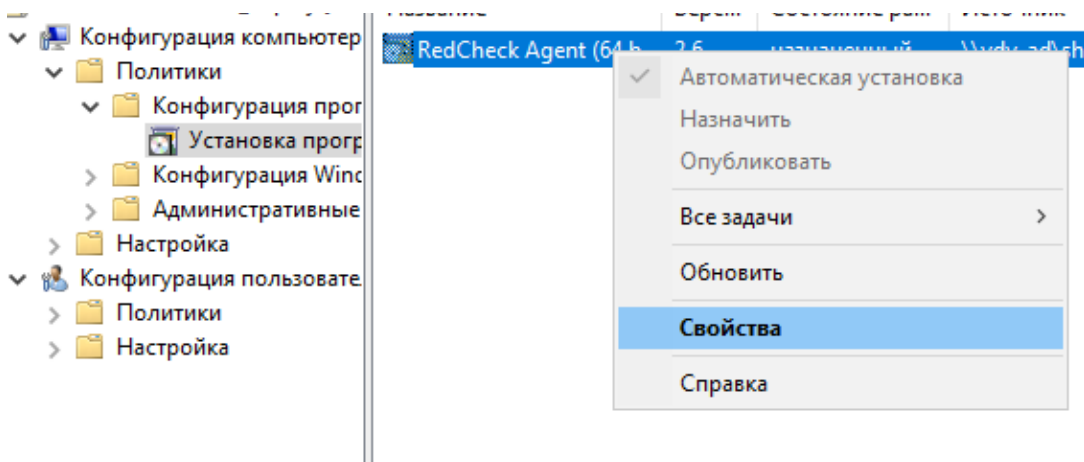
**Шаг 22.** Введите в адресной строке путь к сетевой папке: \\<имя\_компьютера>\<имя\_папки>\$ → выберите установочный файл Агента;



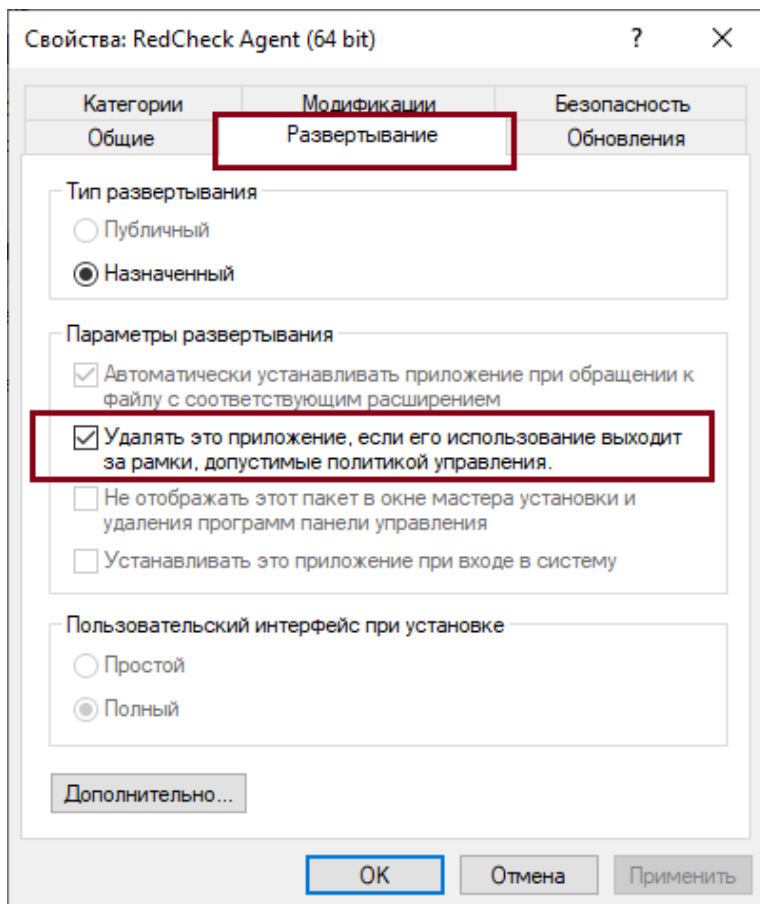
Метод развертывания – **назначенный**;



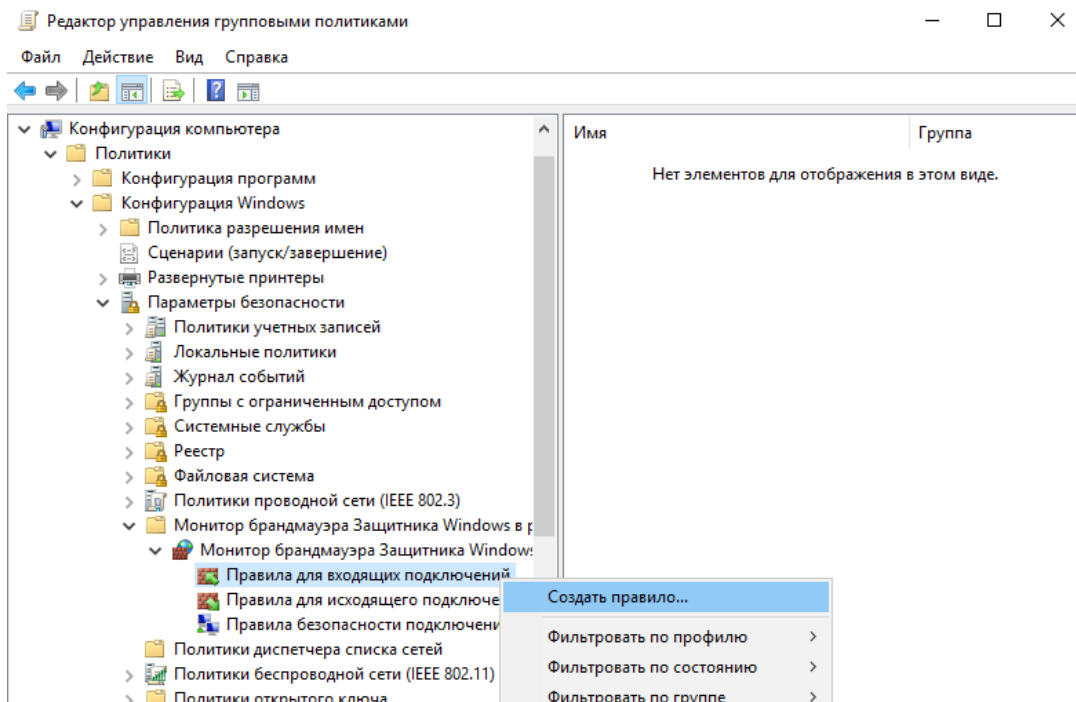
**Шаг 23.** ПКМ по появившемуся установочному файлу → **Свойства**;



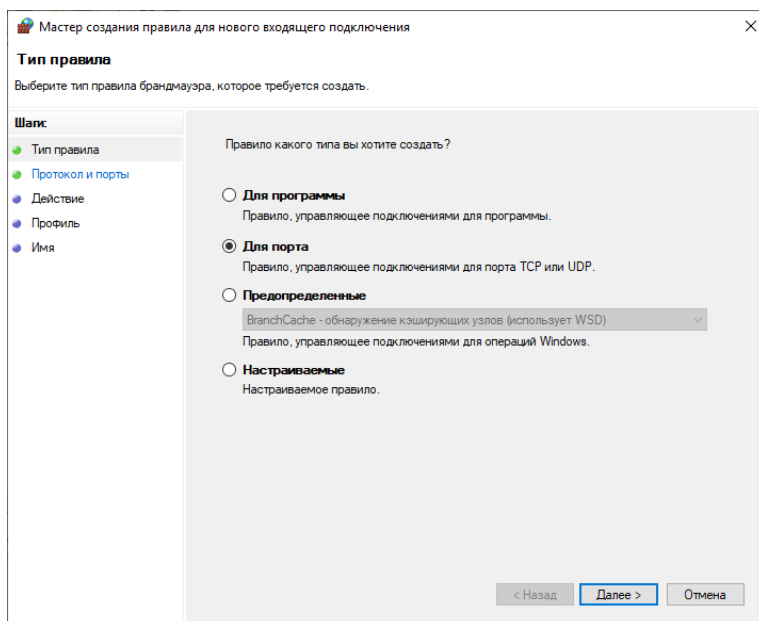
**Шаг 24.** В **Развертывание** отметьте **Удалить это приложение, если его использование...** → **ОК**;



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

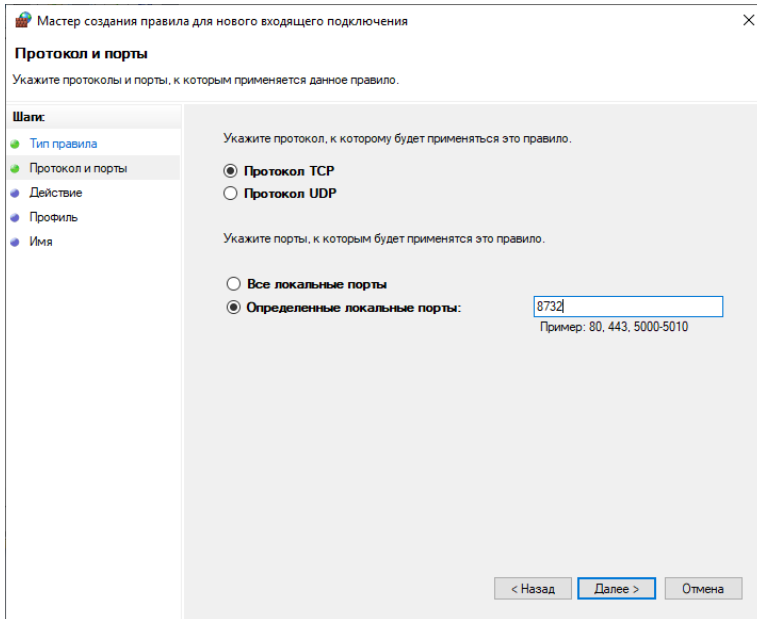


**Шаг 26.** Укажите тип правила **Для порта** → **Далее**;

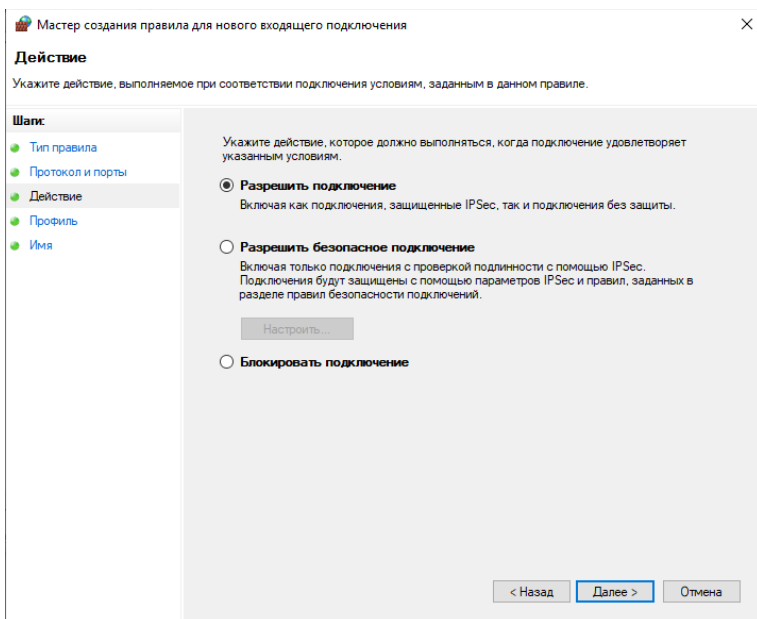


Отметьте **Протокол TCP** → укажите порт Агента (по умолчанию **8732**) → **Далее**;

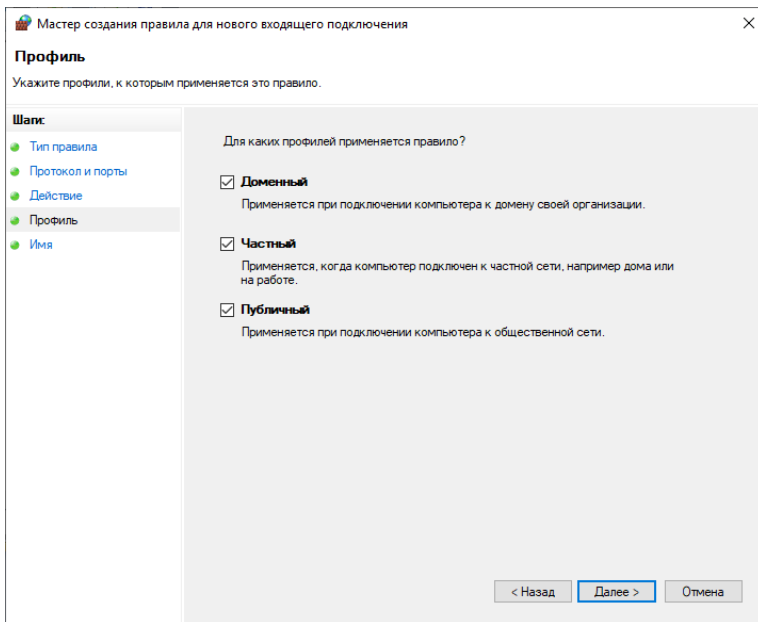




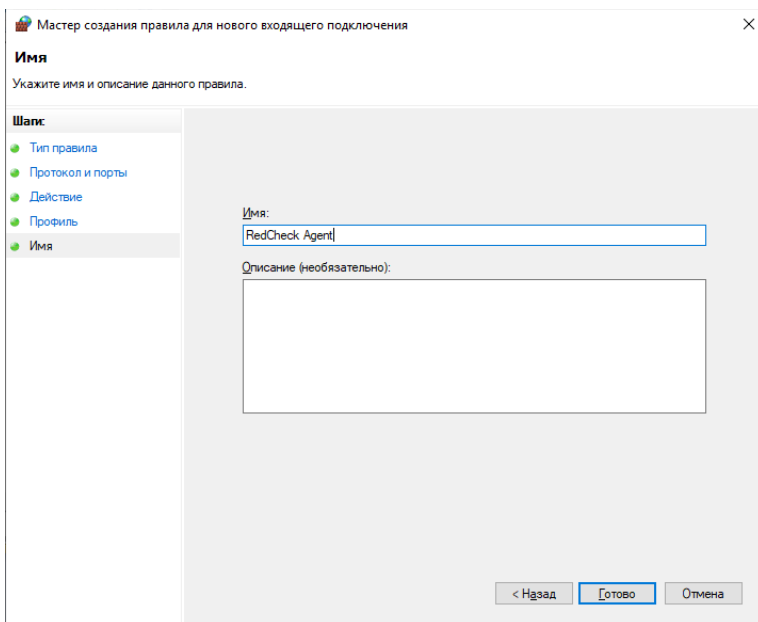
Выберите **Разрешить подключение** → **Далее**;



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**.

Имя	Состояние	39% ЦП	42% Память	1% Диск	0% Сеть
Application Frame Host		0%	4,3 МБ	0 МБ/с	0 Мбит/с
COM Surrogate		0%	1,9 МБ	0,1 МБ/с	0 Мбит/с
CTF-загрузчик		0%	3,1 МБ	0 МБ/с	0 Мбит/с
Microsoft Edge Update (32 бита)		0%	0,5 МБ	0 МБ/с	0 Мбит/с
Microsoft Network Realtime Ins...		0%	2,8 МБ	0 МБ/с	0 Мбит/с
Microsoft OneDrive		0%	15,4 МБ	0,1 МБ/с	0 Мбит/с
Microsoft Text Input Application		0%	5,4 МБ	0 МБ/с	0 Мбит/с
Microsoft Update Health Service		0%	0,9 МБ	0 МБ/с	0 Мбит/с
MoUSO Core Worker Process		0%	2,1 МБ	0 МБ/с	0 Мбит/с
RedCheck Agent		0%	9,5 МБ	0 МБ/с	0 Мбит/с
Runtime Broker		0%	1,1 МБ	0 МБ/с	0 Мбит/с
Runtime Broker		0%	2,3 МБ	0 МБ/с	0 Мбит/с
Runtime Broker		0%	2,3 МБ	0 МБ/с	0 Мбит/с

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.

## 3.7 Раздельная установка компонентов

Под раздельной установкой компонентов подразумевается инсталляция одного из компонентов отдельно от остальных. Это может быть необходимо, например, при установке дополнительной службы сканирования.

Для инсталляции компонента установите нужные пакеты. Например, если необходимо установить службу сканирования, то пакетами для инсталляции будут **redcheck-scan-service** и **redcheck-dotnet-runtime**

Bash (оболочка Unix)

```
sudo apt install redcheck-dotnet-runtime redcheck-scan-service
```

После чего проведите конфигурацию компонента:

Bash (оболочка Unix)

```
sudo redcheck-bootstrap configure -c=all
```

Инсталлятор предложит сконфигурировать только установленные в системе пакеты.

В случае инсталляции службы сканирования / синхронизации необходимо вручную заменить ключ шифрования в конфигурационном файле устанавливаемого компонента.

На хосте с установленной службой сканирования или службой синхронизации откройте файл **/var/opt/redcheck-scan-service/conf/appsettings.json** (для службы сканирования) или **/var/opt/redcheck-sync-service/conf/appsettings.json** (для службы синхронизации) и впишите ключ в параметр **Sckd**

```
{
  "ConnectionStrings": {
    "Default": "CfDJ8JN-D2R9
  },
  "DbOperationTimeout": 3000
  "Sckd": "",
  "Service": {
    "ServiceId": "3ba1f3f2-1
    "Language": "Ru"
  },
  "Polling": {
    "PollingIntervalSec": 1
  },
}
```

## 4 Сопровождение Системы

---

### Содержание

- [4.1 Создание локальных пользователей RedCheck](#)
- [4.2 Активация лицензии](#)
- [4.3 Обновление контента информационной безопасности](#)
- [4.4 Настройка учетных записей для сканирования](#)
- [4.5 Смена ключа шифрования](#)
- [4.6 Обслуживание БД](#)
- [4.7 Резервное копирование и восстановление БД](#)
- [4.8 Обновление RedCheck Nix](#)
- [4.9 Сброс привязки лицензии](#)
- [4.10 Смена лицензионного ключа](#)
- [4.11 Изменение портов для компонентов RedCheck](#)
- [4.12 Журнал событий \(логи\)](#)
- [4.13 Настройка сервиса доставки отчетов](#)
- [4.14 Исключения для средств защиты \(САЗ, СЗИ\)](#)

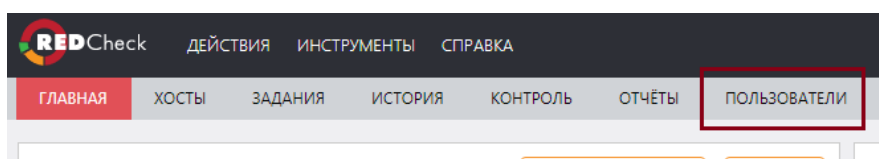
## 4.1 Создание локальных пользователей RedCheck

Для корректного распределения прав доступа ознакомьтесь с перечнем возможностей каждой из ролей ([1.4 Полевая модель RedCheck](#)).

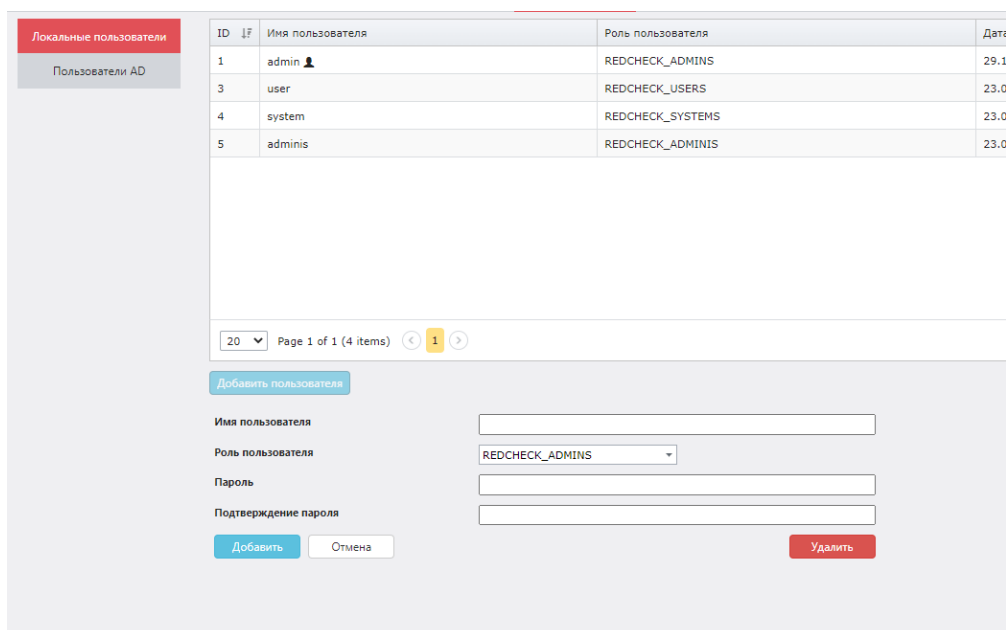
### Создание пользователя

Добавить пользователя может только пользователь с ролью Admins.

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



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



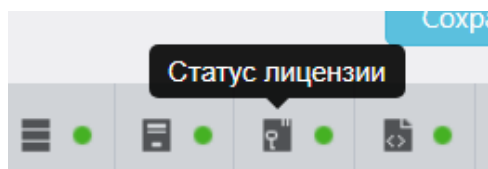
### Управление пользователя

**Редактирование:** нажмите  → **Редактировать**.

**Удаление:** нажмите  → **Удалить**;

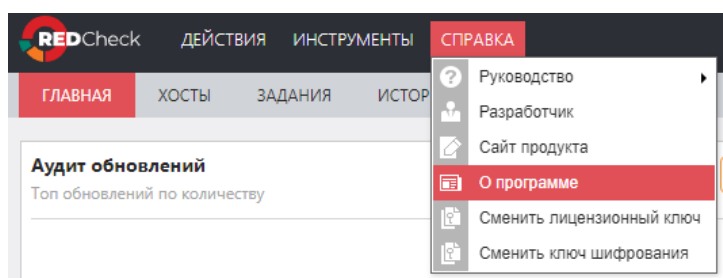
## 4.2 Активация лицензии

Статус лицензии отображается на статусной панели:



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;

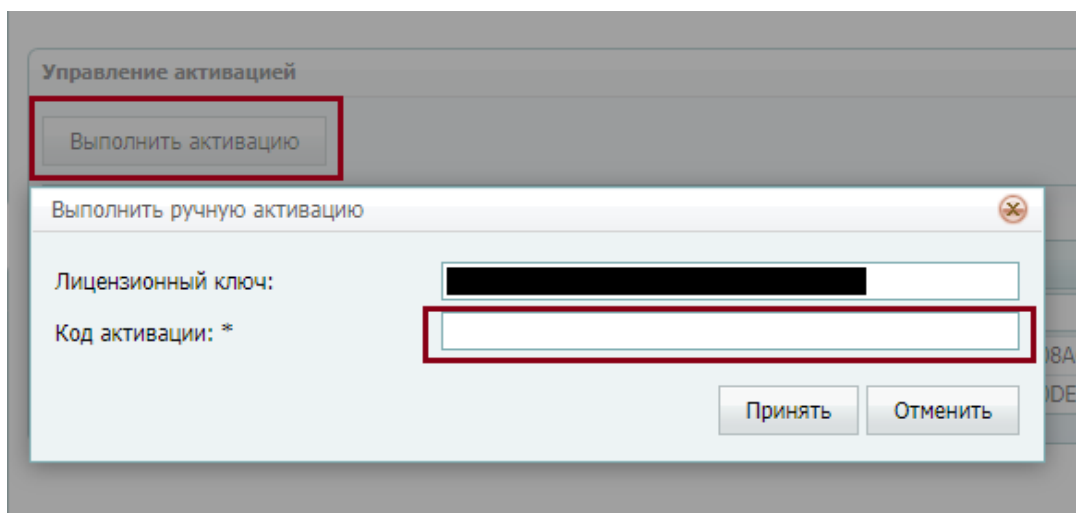
Средство анализа защищённости RedCheck	
Сведения о программе	
Параметр	Значение
Версия программы	
Версия сервера	
Версия REST	0.3
Версия базы данных	266
Версия контента	CVEFULL:1.10.5.9 NIXCOMPL:1.10.5.9 GLA:1.10.5.9 WINCOMPL:1.10.5.8
Уникальный ID программы	48660376-FB93-488F-A57B-0DD216E43211
Лицензионный ключ	
Код активации	<u>BED340FA43C07EE1983217D3FDC482D4C216B24E6B1E8EDAD58C42186CB114B5</u>

Код активации также можно получить во время установки ([Конфигурация RedCheck](#)).

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







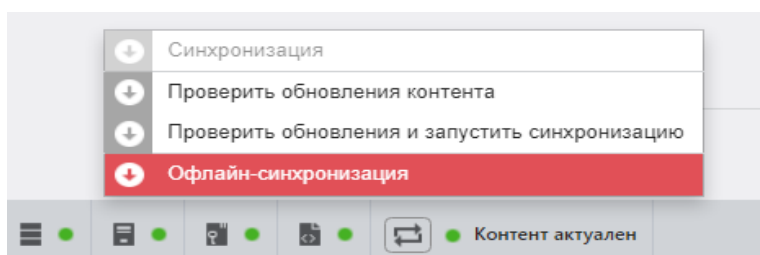
**Шаг 4.** Нажмите **Скачать**;

	Активен	Дата активации	Действия
	False	10.12.2021 09:54:44	<a href="#">Скачать</a>
	True	24.09.2020 11:09:35	<a href="#">Скачать</a>

**Шаг 5.** Сохраните файл **license.xml** в директорию для офлайн синхронизации (по-умолчанию **/var/opt/redcheck-sync-service/data**);

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.



Для изменения стандартного пути для оффлайн-синхронизации выполните следующие шаги:

**Шаг 1.** 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 оффлайн-синхронизации → **Сохранить**;

Синхронизация

Синхронизация по расписанию

Вручную

Автоматически (ежедневно)

Автоматически офлайн (ежедневно)

Время

12 00

Путь к папке офлайн-синхронизации

/var/opt/redcheck-sync-service/data

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.

## 4.3 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

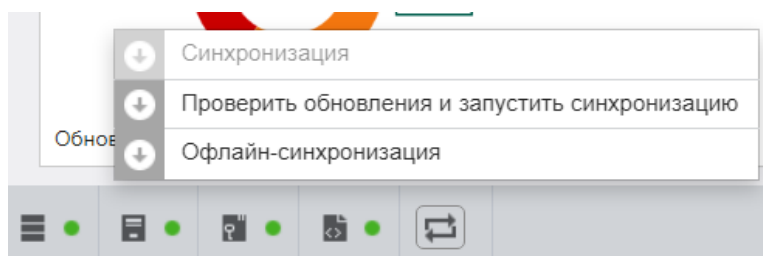
- [4.3.1 Синхронизация через сеть Интернет](#)
- [4.3.2 Офлайн-синхронизация](#)
- [4.3.3 Синхронизация через RedCheck Update Server](#)
- [4.3.4 Синхронизация через прокси-сервер](#)

### 4.3.1 Синхронизация через сеть Интернет

Данный способ является предпочтительным и осуществляется по умолчанию.

Адрес сервиса синхронизации - <https://syncn.altx-soft.ru>

**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.



## 4.3.2 Офлайн-синхронизация

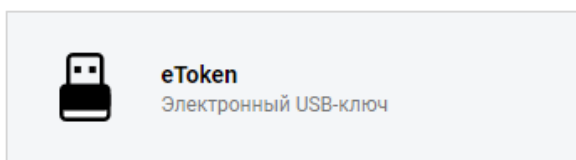
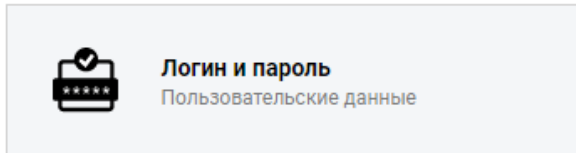
В случае отсутствия доступа к сети Интернет обновление контента ИБ осуществляется посредством архива с необходимым контентом.

**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).

### Центр сертифицированных обновлений

Для получения обновлений необходимо выбрать способ входа

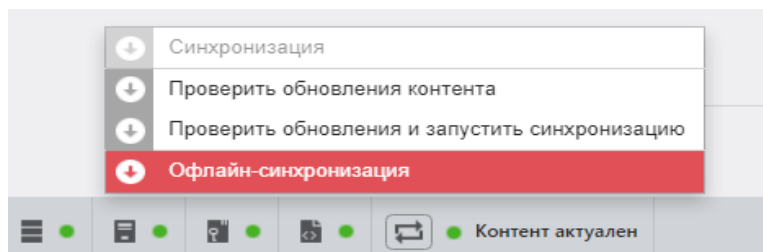


**Шаг 2.** Раскройте **Обновления** → **Файлы** → скачайте архив **RedCheck\_OfflineData (Актуальный контент для синхронизации RedCheck (без файла лицензии) для версии 2.7+)**, нажав **Скачать**;

<a href="#">Delete</a>		
<a href="#">Edit New Delete</a>	Документация на КриптоПро CSP 3.9	
<a href="#">Edit New Delete</a>	RedCheck_OfflineData	Актуальный контент для синхронизации RedCheck (без файла лицензии) для версии 2.7+
<a href="#">Edit New Delete</a>	КриптоПро CSP 3.9 KC1 x64	
<a href="#">Edit New</a>		

**Шаг 3.** Распакуйте архив в директорию для офлайн-синхронизации (по умолчанию `/var/opt/redcheck-sync-service/data`);

**Шаг 4.** 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.



Для изменения стандартного пути для оффлайн-синхронизации выполните следующие шаги:

**Шаг 1.** 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 → **Сохранить**;

ОБЩИЕ

СКАНИРОВАНИЕ

**СИНХРОНИЗАЦИЯ**

ДОСТАВКА

### Синхронизация

#### Синхронизация по расписанию

Вручную

Автоматически (ежедневно)

Автоматически офлайн (ежедневно)

Время

12 00

Путь к папке офлайн-синхронизации

`/var/opt/redcheck-sync-service/data`

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.

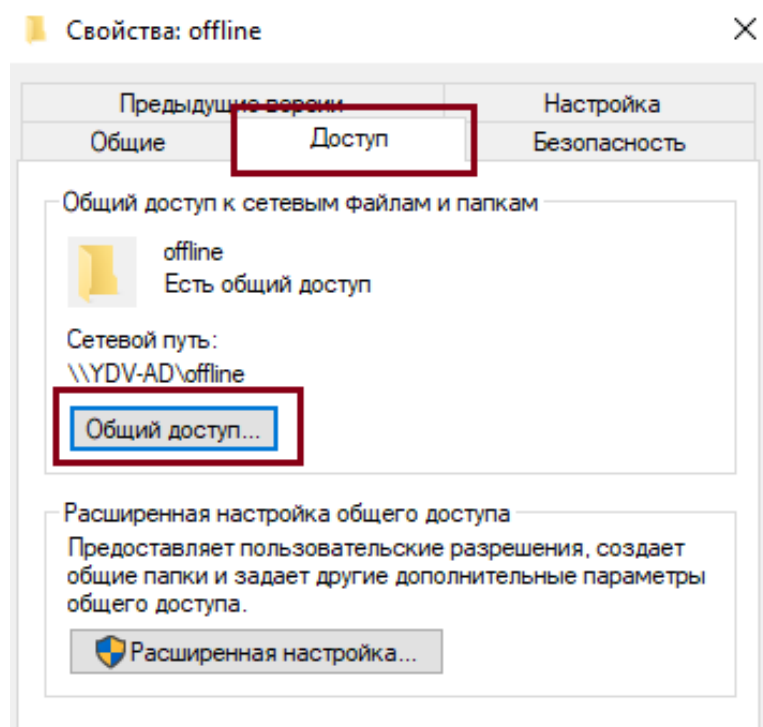


### 4.3.3 Синхронизация через RedCheck Update Server

Более подробная инструкция по работе с компонентами 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);

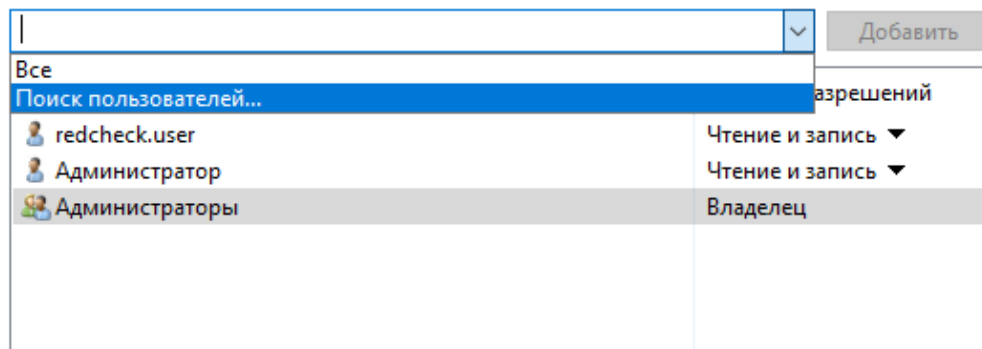
**Шаг 2.** ПКМ по созданной директории → **Свойства** → **Доступ** → **Общий доступ**;



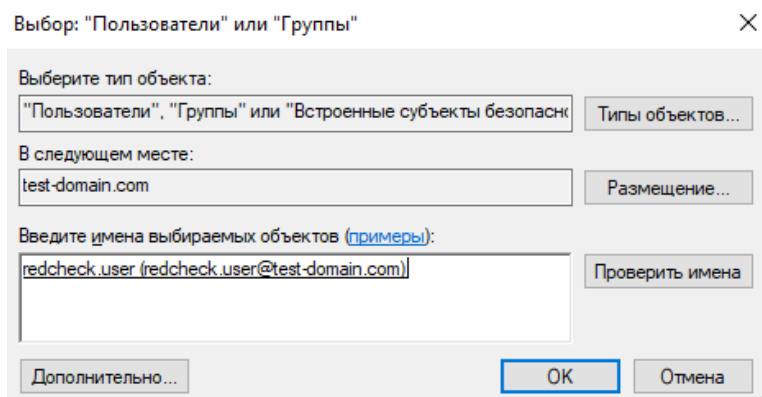
Раскройте список → **Поиск пользователей**;

### Выберите в сети пользователей, с которыми вы хотите поделиться

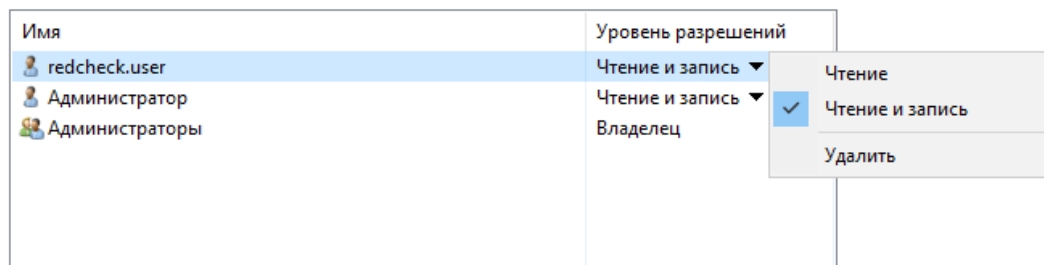
Введите имя и нажмите кнопку "Добавить" либо используйте стрелку для поиска определенного пользователя.



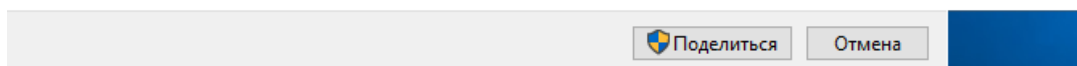
Укажите имя пользователя, который будет иметь доступ к созданной директории с контентом → **ОК**;



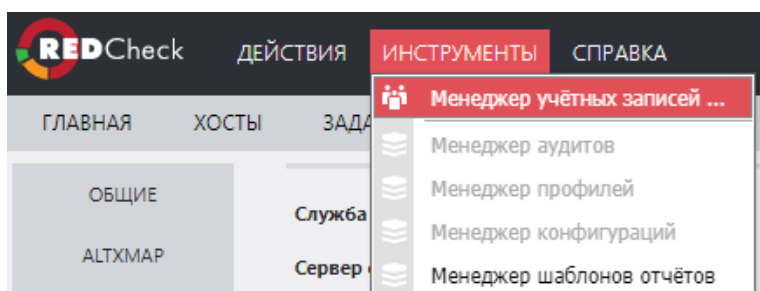
Предоставьте разрешения на **Чтение и запись** → **Поделиться**;



[Проблемы при предоставлении общего доступа](#)

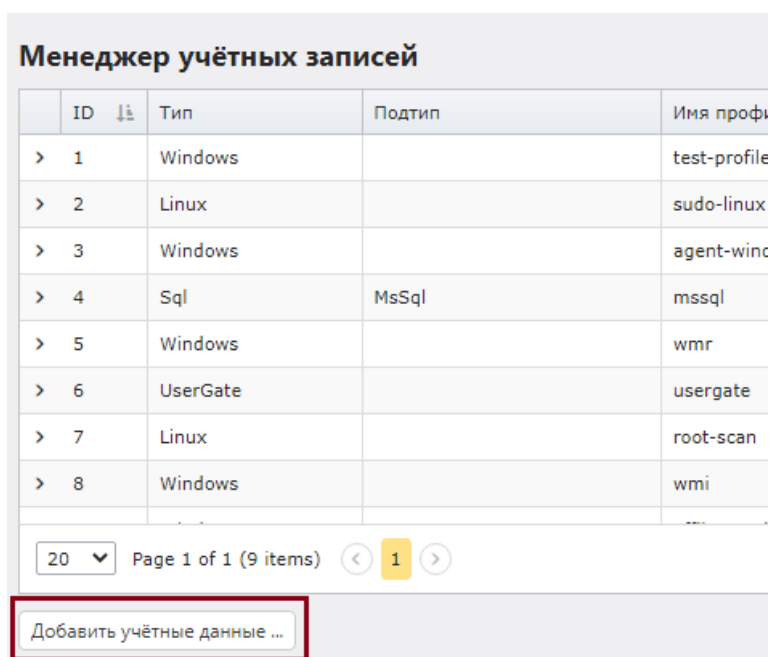


**Шаг 3.** Откройте консоль управления RedCheck → на панели навигации выберите **ИНСТРУМЕНТЫ** → **Менеджер учетных записей**;



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**;

### Новая / Редактируемая учётная запись

Укажите требуемые параметры для новой или редактируемой учётной записи.


Имя профиля:

Тип учётной записи:

---

Имя пользователя:

Пароль:

Подтверждение пароля:  

Домен:

Указать WinRM порт

WinRM порт:

WinRM через HTTPS

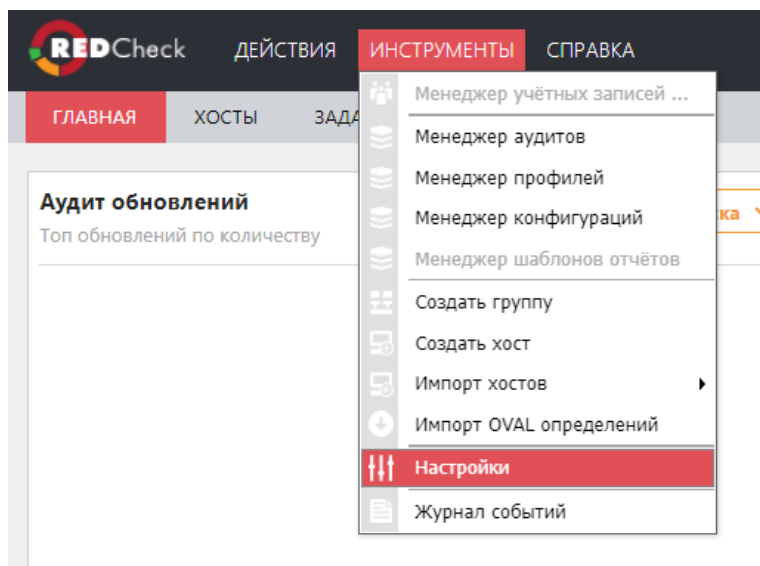
Указать порт RedCheck Agent

Порт RedCheck Agent:

Указать порт RedCheck Update Agent

Порт RedCheck Update Agent:

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



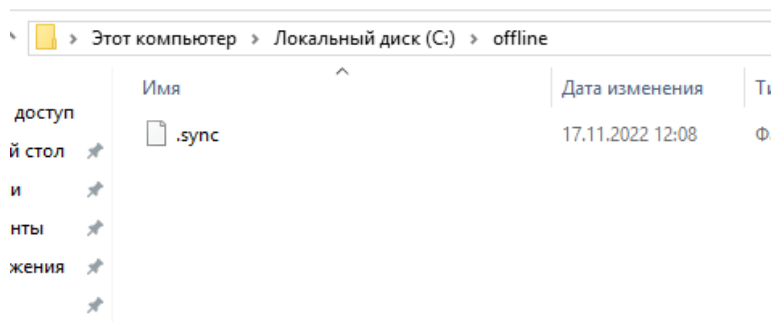
Перейдите в **СИНХРОНИЗАЦИЯ**:

- Отметьте **Автоматически онлайн (ежедневно)**. Измените по необходимости время;
- Укажите путь к сетевой папке;

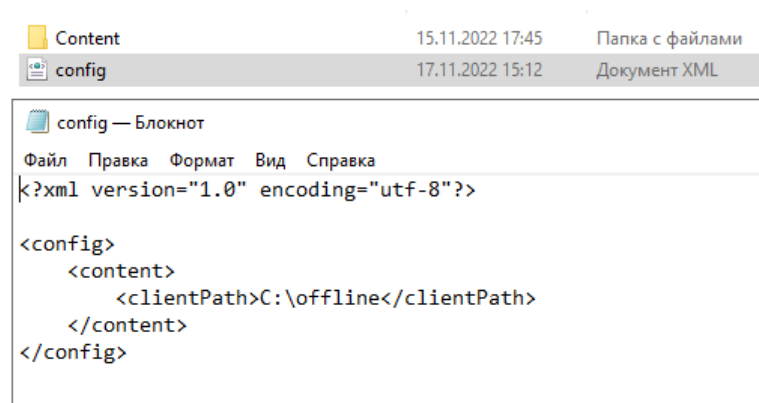
- Выберите ранее созданную учетную запись;

**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:

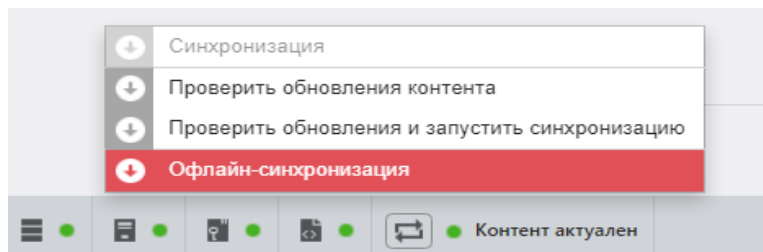
Код

```
RcUpdSrv sync
```

Начнется скачивание недостающего контента ИБ;

```
C:\Program Files (x86)\ALTEX-SOFT\RedCheckUpdateServer>RcUpdSrv sync
[15:13:34.8718 INF] [RedCheck.Services.UpdateServer.Config] Configuration file located at "C:\ProgramData\ALTEX-SOFT\RedCheckUpdateServer".
[15:13:34.8854 INF] [RedCheck.Services.UpdateServer.SyncFolderManager] Content path <basePath> not set.
[15:13:34.8854 INF] [RedCheck.Services.UpdateServer.SyncFolderManager] Sync folders found (1):
[15:13:34.8854 INF] [RedCheck.Services.UpdateServer.SyncFolderManager] Folder "C:\offline"
[15:13:35.2364 INF] [RedCheck.Services.UpdateServer.Synchronizer] Lock folder "C:\offline".
[15:13:35.2642 INF] [RedCheck.Services.UpdateServer.Synchronizer] Clean up folder "C:\offline".
[15:13:35.2642 INF] [RedCheck.Services.UpdateServer.Synchronizer] Start sync in "C:\offline".
[15:14:37.4959 INF] [RedCheck.Services.UpdateServer.Synchronizer] Complete sync in "C:\offline".
[15:14:37.4959 INF] [RedCheck.Services.UpdateServer.Synchronizer] Unlock folder "C:\offline".
OK
C:\Program Files (x86)\ALTEX-SOFT\RedCheckUpdateServer>_
```

**Шаг 7.** 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.

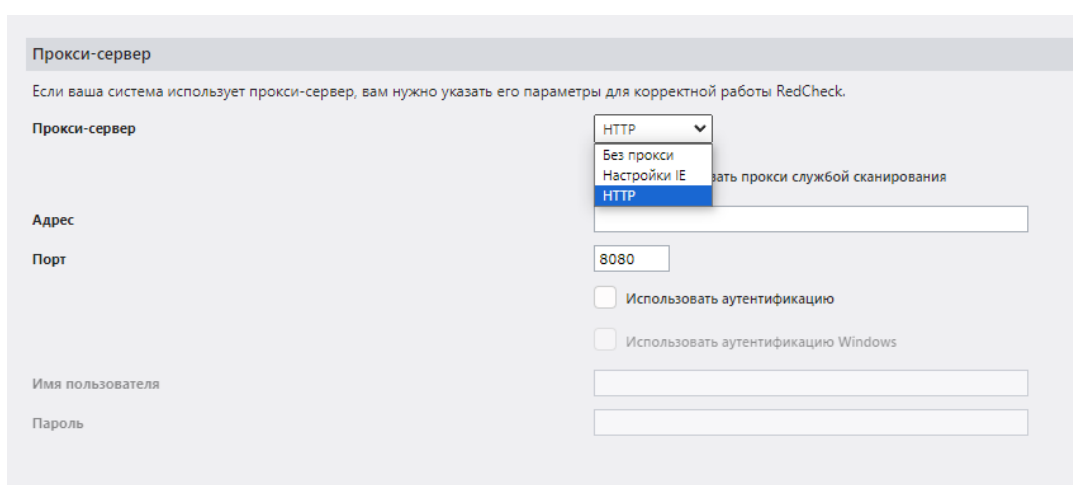


## 4.3.4 Синхронизация через прокси-сервер

Адрес сервиса синхронизации - <https://syncn.altx-soft.ru>

Для проведения синхронизации через прокси-сервер необходимо выполнить следующие шаги.

**Шаг 1.** Нажмите **Инструменты** → **Настройки** → **Общие** → в разделе **Прокси-сервер** выберите в соответствующем списке нужный параметр;



**Шаг 2.** Введите адрес и порт прокси-сервера, укажите при необходимости учетные данные для аутентификации;

Отметьте **Не использовать прокси службой сканирования**, если нет такой необходимости. По умолчанию функция включена.

**Шаг 3.** Нажмите **Сохранить**.

## 4.4 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

- [4.4.1 Сканирование Windows-систем](#)
- [4.4.2 Сканирование Unix-систем \(SSH\)](#)
- [4.4.3 Сканирование FreeBSD](#)
- [4.4.4 Сканирование Solaris](#)
- [4.4.5 Сканирование Check Point](#)
- [4.4.6 Сканирование Cisco IOS / NX-OS](#)
- [4.4.7 Сканирование Huawei](#)
- [4.4.8 Сканирование FortiOS](#)
- [4.4.9 Сканирование UserGate](#)
- [4.4.10 Сканирование VMware](#)
- [4.4.11 Сканирование Microsoft SQL Server](#)
- [4.4.12 Сканирование MySQL](#)
- [4.4.13 Сканирование PostgreSQL](#)
- [4.4.14 Сканирование Oracle](#)



## 4.4.1 Сканирование Windows-систем

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

### Новая / Редактируемая учётная запись

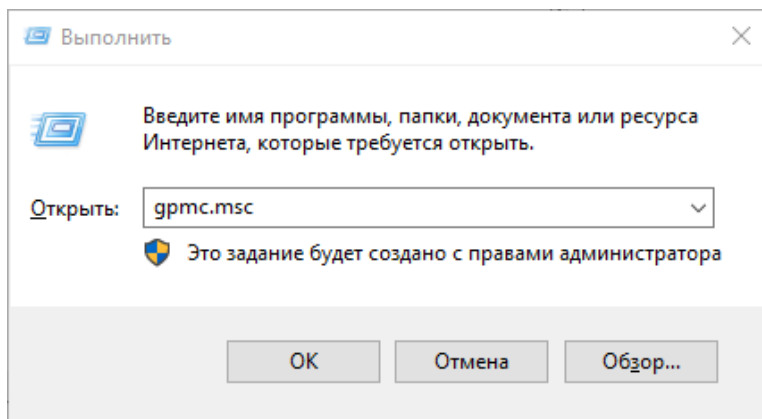
Укажите требуемые параметры для новой или редактируемой учётной записи.

Имя профиля	<input type="text" value="windows"/>
Тип учётной записи	<input type="text" value="Windows"/>
<hr/>	
Имя пользователя	<input type="text"/>
Пароль	<input type="password"/>
Подтверждение пароля	<input type="password"/>
Домен	<input type="text"/>
WinRM порт	<input type="checkbox"/> Указать WinRM порт <input type="text" value="5985"/>
	<input type="checkbox"/> WinRM через HTTPS
	<input type="checkbox"/> Указать порт RedCheck Agent
Порт RedCheck Agent	<input type="text" value="8732"/>
	<input type="checkbox"/> Указать порт RedCheck Update Agent
Порт RedCheck Update Agent	<input type="text" value="8733"/>

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.

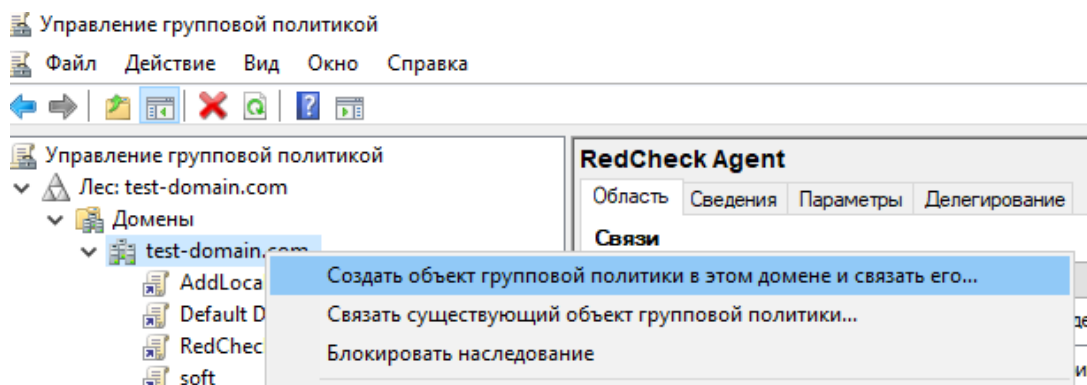
### Создание групповой политики

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

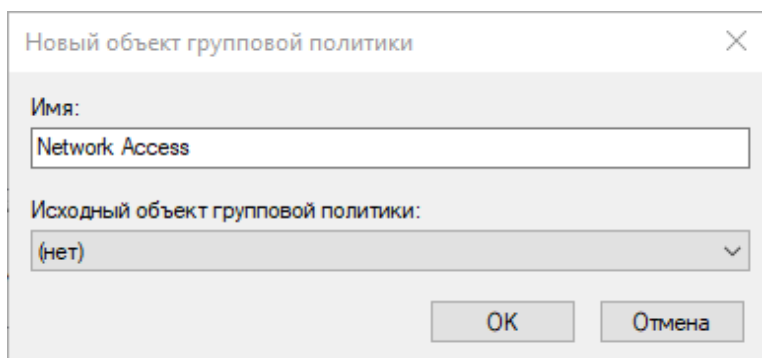


При локальной настройке нажмите **Win + R** → введите **gpedit.msc**;

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

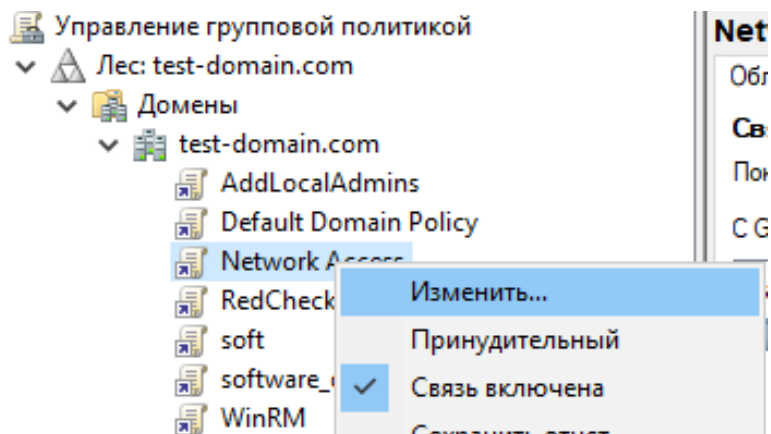


Введите название новой групповой политики;

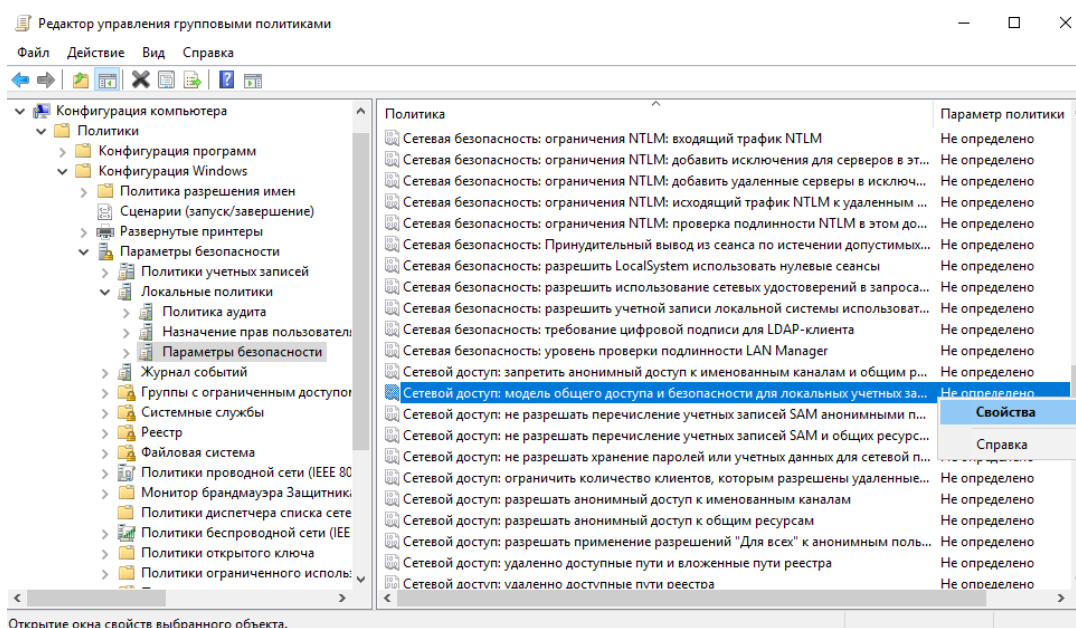


## Настройка сетевого доступа

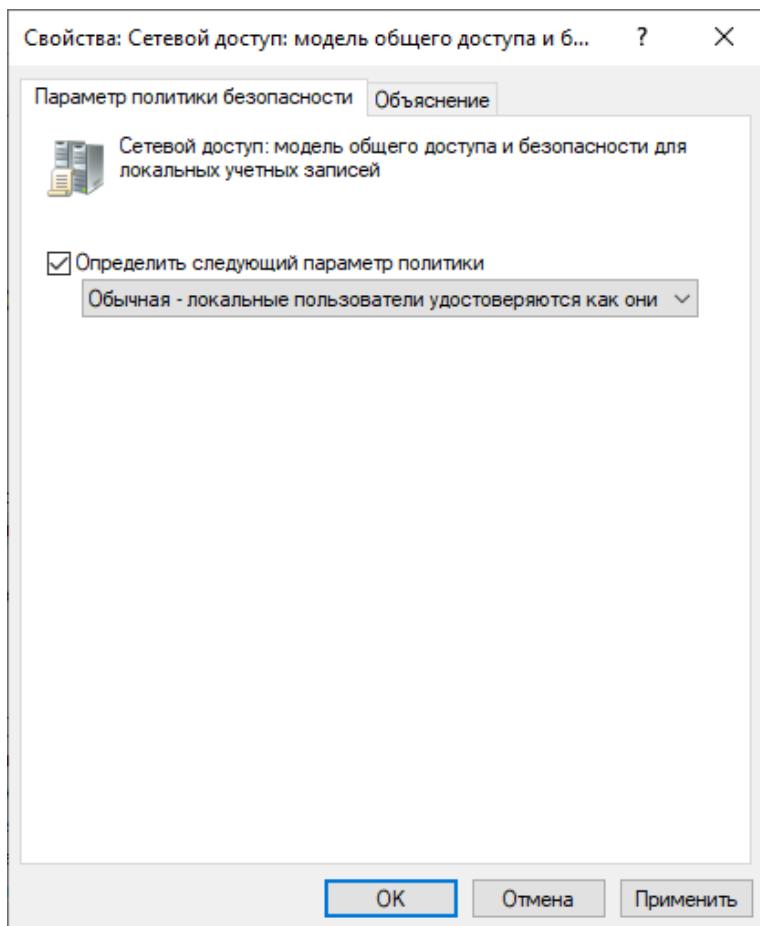
**Шаг 3.** ПКМ по созданной групповой политике → **Изменить**;



**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...**

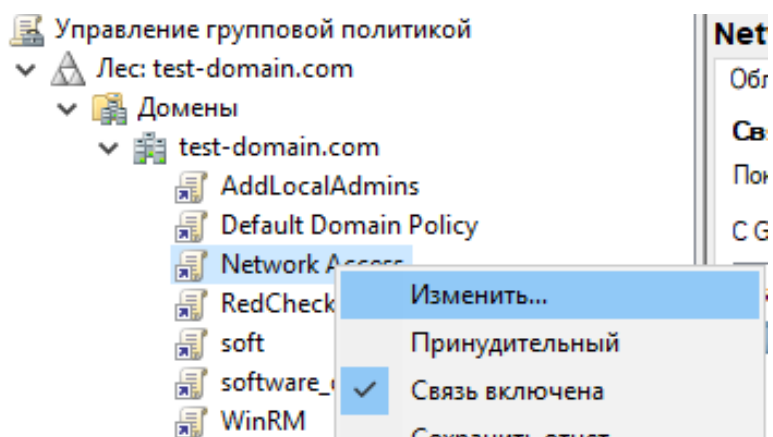


## Настройка контроля учетных записей пользователей

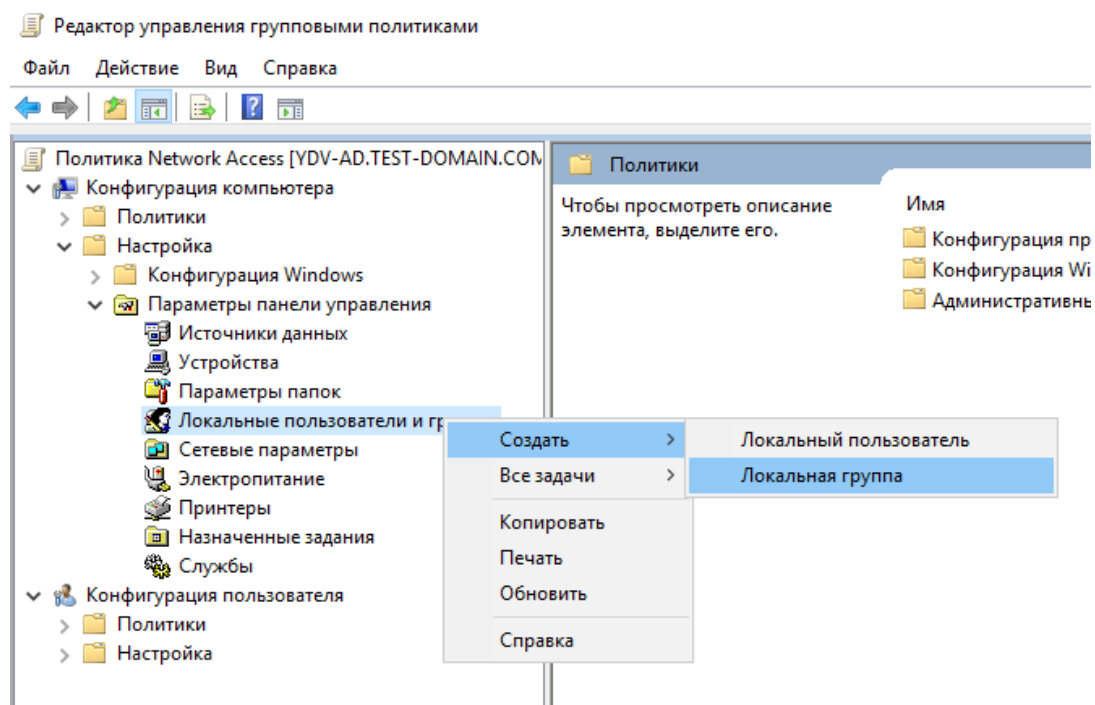
Рекомендуется использовать доменную УЗ для отключения функции UAC.

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

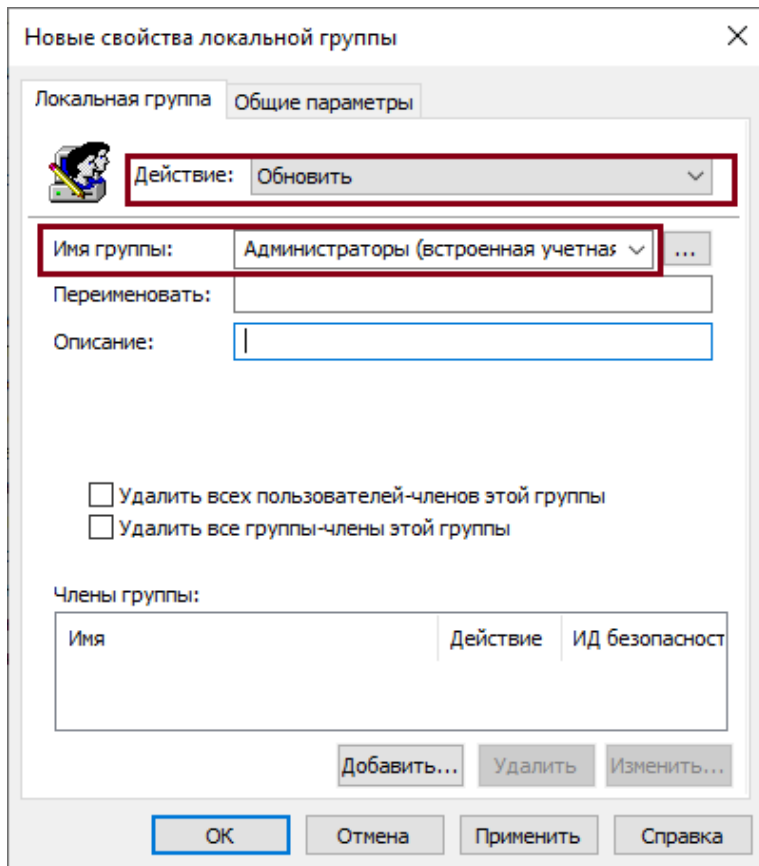
**Шаг 2.** ПКМ по необходимой групповой политике → **Изменить**;



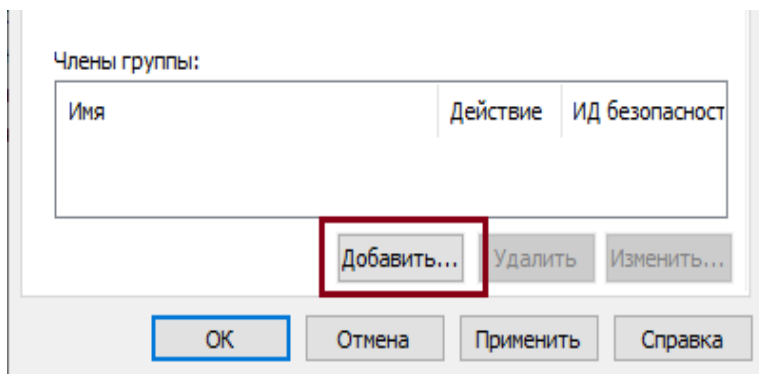
**Шаг 3.** Добавьте пользователя в группу локальных администраторов сканируемого хоста: **Конфигурация компьютера** → **Настройки** → **Параметры панели управления** → ПКМ по **Локальные пользователи и группы** → **Создать** → **Локальная группа**;



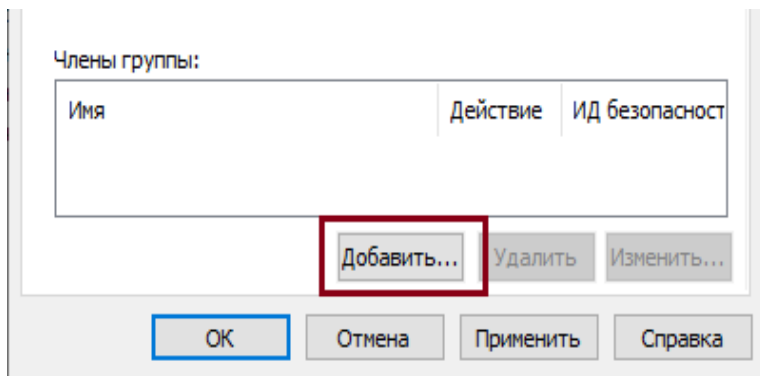
**Шаг 4.** В **Действие** выберите **Обновить** , в **Имя группы** – **Администраторы (встроенная учетная запись)**;



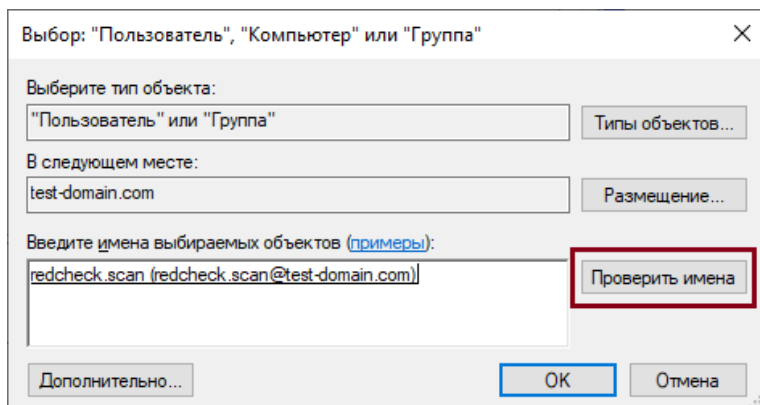
Нажмите **Добавить**;



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

- Транспорт Агент RedCheck
- Транспорт WinRM
- Транспорт WinRM (Kerberos)

## 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) ([3.4 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.



## 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)**. Данная служба для своей работы требует настройку службы сканирования и сканируемых узлов.

### Содержание

- [Настройка WinRM \(Astra Linux\)](#)
- [Настройка WinRM \(РЕД ОС\)](#)
- [Настройка сканируемого узла \(локально\)](#)
- [Настройка сканируемых хостов через групповые политики](#)

## Настройка транспорта WinRM на стороне службы сканирования (Astra Linux)

**Шаг 1.** Для настройки на хосте должны быть установлены пакеты **gcc python3-dev libkrb5-dev**

Bash (оболочка Unix)

```
sudo apt install gcc python3-dev libkrb5-dev
```

**Шаг 2.** Скачайте tar.gz архив ([ссылка на скачивание](#)) с необходимыми компонентами, поместите на хост с установленной службой сканирования (**/var/opt/redcheck-scan-service/pypsrp**) и разархивируйте;

Bash (оболочка Unix)

```
sudo tar -xf /var/opt/redcheck-scan-service/pypsrp/pypsrp-0.8.1-Astral.7.tar.gz
```

**Шаг 3.** Установите python-пакеты:

Bash (оболочка Unix)

```
sudo python3 /var/opt/redcheck-scan-service/pypsrp/pypsrp-0.8.1-Astral.7/pip-24.0-py3-none-any.whl/pip install --no-index -f /var/opt/redcheck-scan-service/pypsrp/pypsrp-0.8.1-Astral.7 setuptools wheel Cython
```

Bash (оболочка Unix)

```
sudo python3 /var/opt/redcheck-scan-service/pypsrp/pypsrp-0.8.1-Astral.7/pip-24.0-py3-none-any.whl/pip install --no-index -f /var/opt/redcheck-scan-service/pypsrp/pypsrp-0.8.1-Astral.7 pypsrp[kerberos]
```

**Шаг 4.** Внесите правки в конфигурационный файл службы сканирования **/var/opt/redcheck-scan-service/conf/appsettings.json**;

Bash (оболочка Unix)

```
sudo nano /var/opt/redcheck-scan-service/conf/appsettings.json
```

Для параметра **PythonDll** установите значение **/usr/lib/x86\_64-linux-gnu/libpython3.7m.so.1.0**



```
{
  "DbOperationTimeout": 3000,
  "Sckd": "",
  "Service": {
    "ServiceId": "a268e675-8442-4db3-940f-0005097cc829",
    "Language": "Ru"
  },
  "Polling": {
    "PollingIntervalSec": 1
  },
  "PythonRuntime": {
    "PythonDll": "/usr/lib/x86_64-linux-gnu/libpython3.7m.so.1.0"
  }
}
```

**Шаг 5.** Перезапустите службу сканирования;

Bash (оболочка Unix)

```
sudo systemctl restart redcheck-scan-service
```

Если в вашем домене настроена Kerberos-аутентификация, выполните [дополнительную настройку](#) на хосте с установленной службой сканирования.

## Настройка транспорта WinRM на стороне службы сканирования (РЕД ОС)

**Шаг 1.** Установите python-пакеты:

Bash (оболочка Unix)

```
sudo python3 /var/opt/redcheck-scan-service/pypsrp/pip-24.2-py3-none-any.whl/pip install --no-index -f /var/opt/redcheck-scan-service/pypsrp setuptools wheel Cython
```

Bash (оболочка Unix)

```
sudo python3 /var/opt/redcheck-scan-service/pypsrp/pip-24.2-py3-none-any.whl/pip install --no-index -f /var/opt/redcheck-scan-service/pypsrp pypsrp[kerberos]
```

**Шаг 2.** Внесите правки в конфигурационный файл службы сканирования **/var/opt/redcheck-scan-service/conf/appsettings.json**;

Bash (оболочка Unix)

```
sudo nano /var/opt/redcheck-scan-service/conf/appsettings.json
```

Для параметра **PythonDll** установите значение **/usr/lib64/libpython3.8.so.1.0**

```
    },
    "DbOperationTimeout": 3000,
    "Sckd": "",
    "Service": {
      "ServiceId": "48660376-fb93-488f-a57b-0dd216e43211",
      "Language": "Ru"
    },
  },
  "Polling": {
    "PollingIntervalSec": 1
  },
  "PythonRuntime": {
    "PythonDll": "/usr/lib64/libpython3.8.so.1.0"
  }
}
```

**Шаг 3.** Перезапустите службу сканирования;

Bash (оболочка Unix)

```
sudo systemctl restart redcheck-scan-service
```

Если в вашем домене настроена Kerberos-аутентификация, выполните [дополнительную настройку](#) на хосте с установленной службой сканирования.

## Настройка сканируемого узла

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.

Для сканирования транспортом WinRM на конечных хостах должен быть установлен .NET Framework 4.0 и выше

**Шаг 1.** Откройте PowerShell и включите службу Windows Remote Management (WS-managment) командой:

Code

```
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 2.** Добавьте в доверенные хосты ip-адрес службы сканирования:

Code

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

**Шаг 3.** 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
```

Для проверки подключения выполните задание **Проверка доступности**, выбрав вид транспорта WinRM и учетную запись Windows.

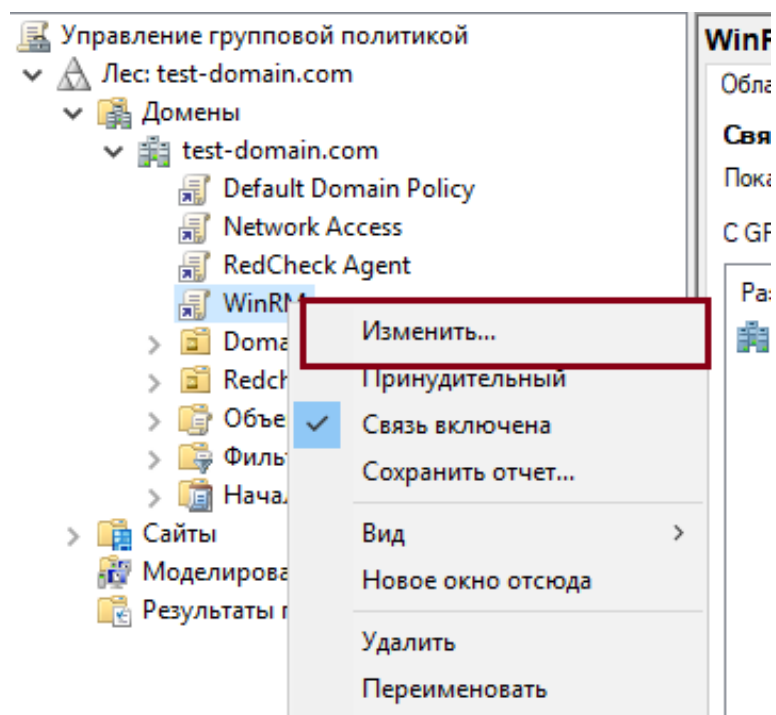
В случае возникновения проблем с подключением рекомендуется следовать [руководству](#).

## Настройка WinRM через групповые политики

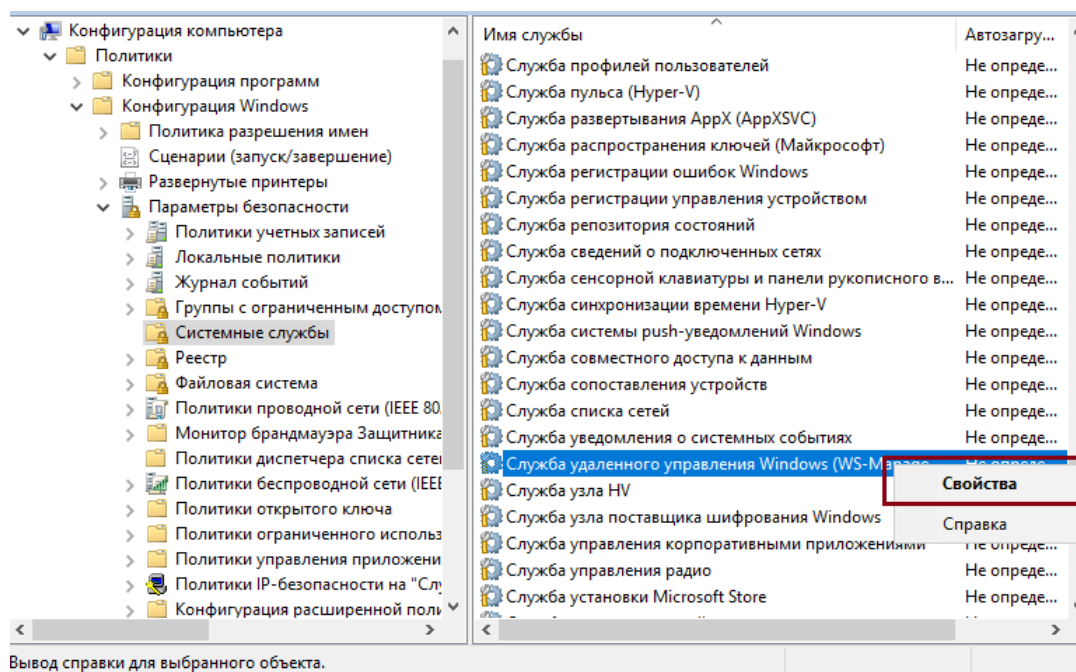
Для сканирования транспортом WinRM на конечных хостах должен быть установлен .NET Framework 4.0 и выше

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

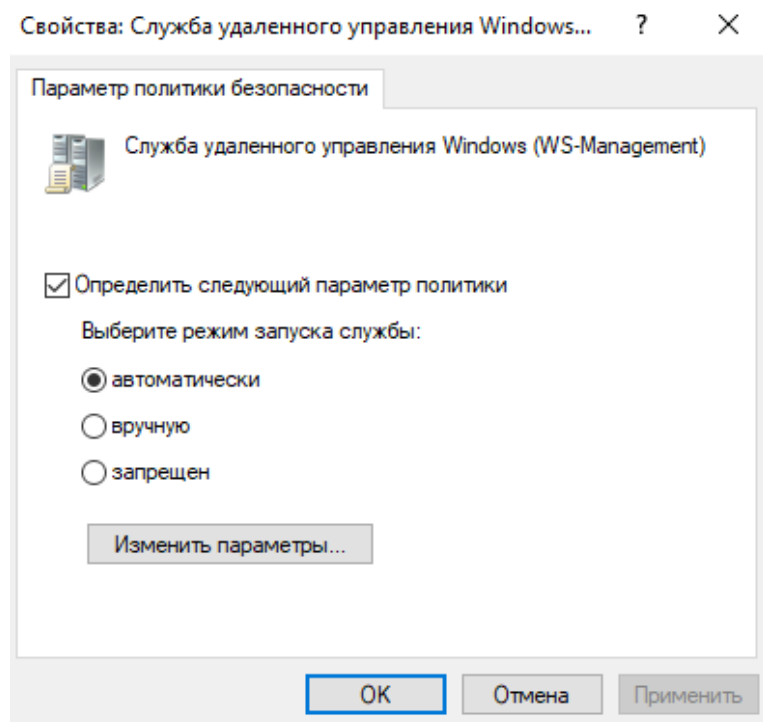
**Шаг 1.** ПКМ по групповой политике → **Изменить**;



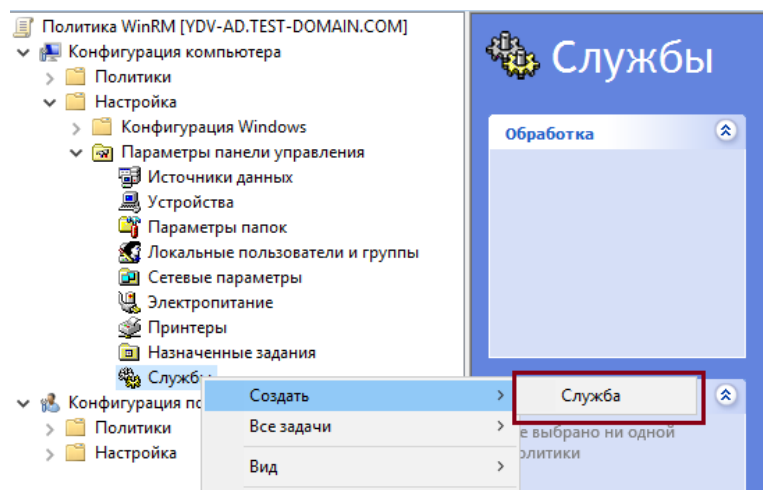
**Шаг 2.** Перейдите в **Конфигурация компьютера** → **Политики** → **Конфигурация Windows** → **Параметры безопасности** → **Системные службы** → ПКМ по **Служба удаленного управления Windows (WS-Management)** → **Свойства**;



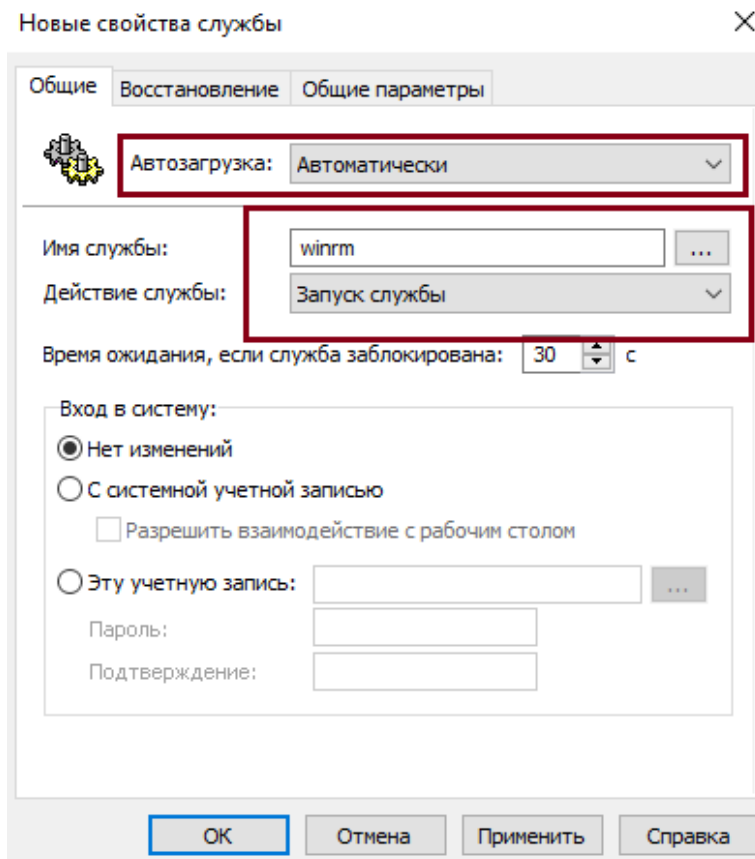
Отметьте **Определить следующий параметр политики**, режим запуска службы – **автоматически** → **ОК**;



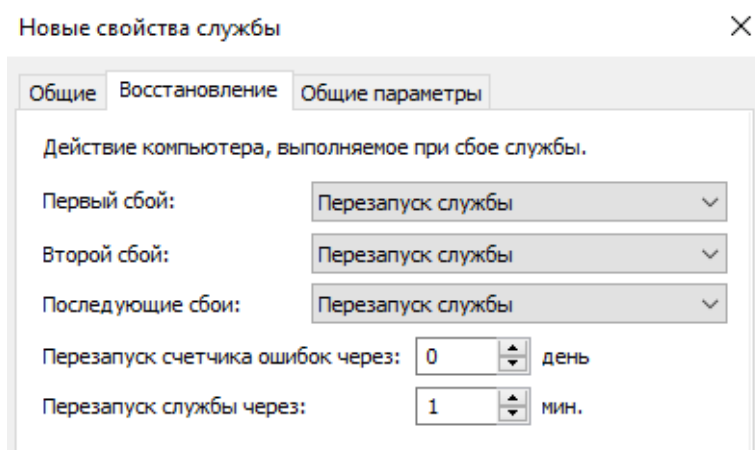
**Шаг 3.** Перейдите в **Конфигурация компьютера** → **Настройка** → **Параметры панели управления** → ПКМ по **Службы** → **Создать** → **Служба**;



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

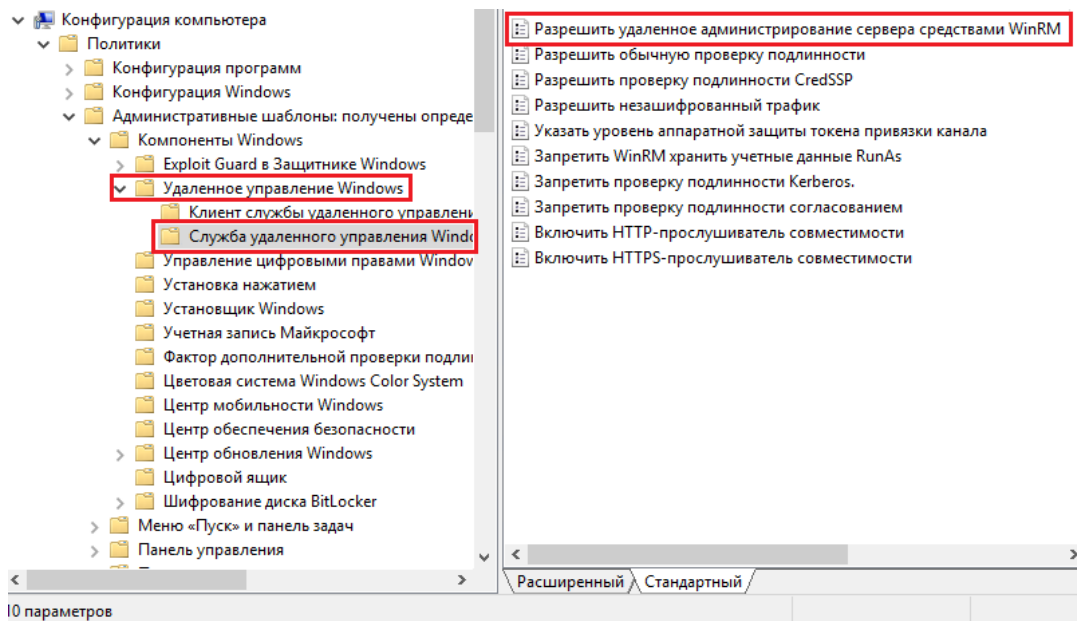


В разделе **Восстановление** укажите для трех параметров значение **Перезапуск службы**;



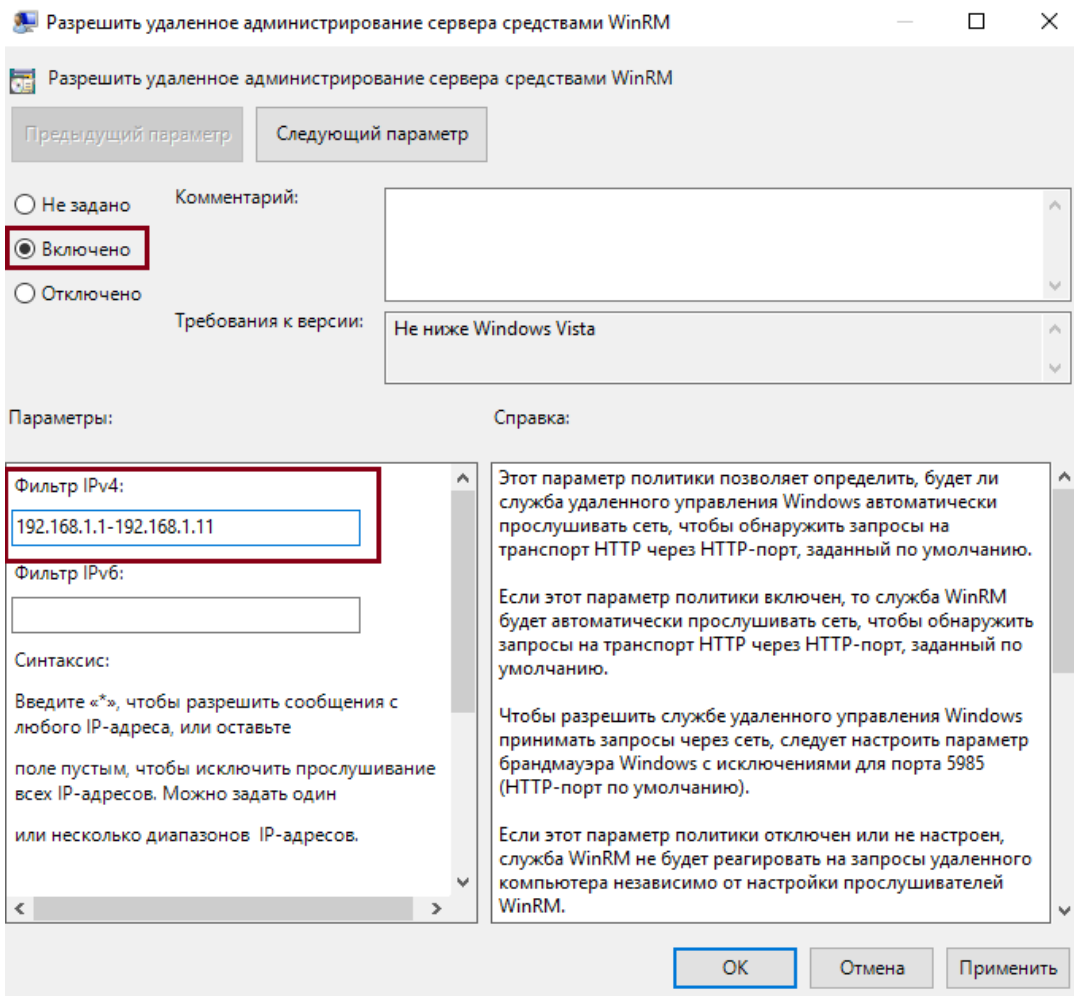
**Шаг 5.** Перейдите в **Конфигурация компьютера** → **Политики** → **Административные шаблоны...** → **Компоненты Windows** → **Удаленное управление Windows** → **Служба удаленного управления Windows** → откройте **Разрешить удаленное администрирование сервера...**;



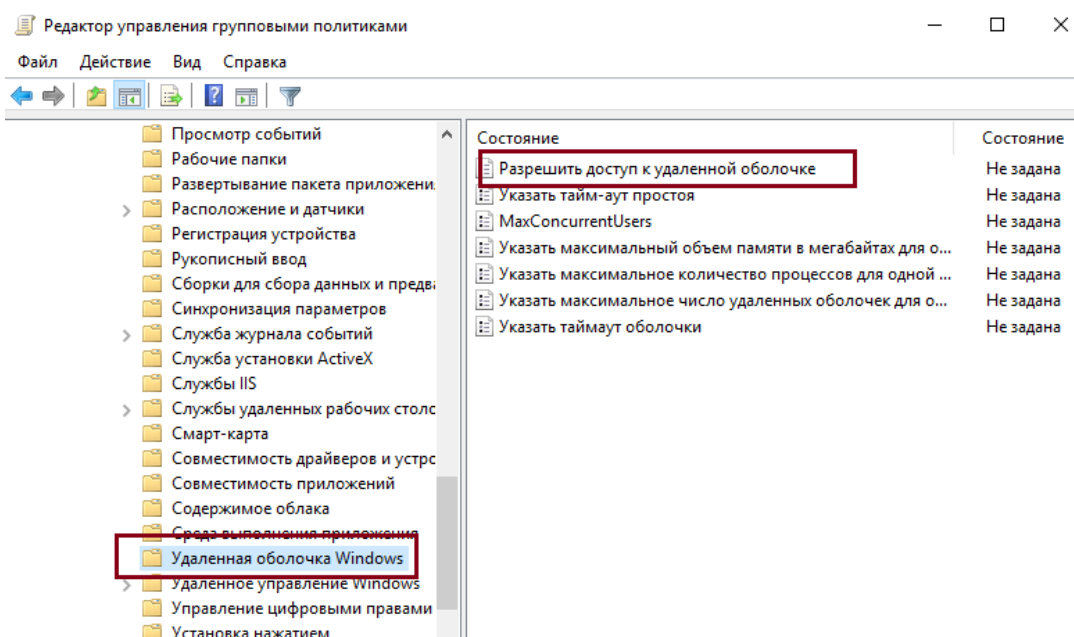


Укажите **Включено** → укажите в **Фильтр IPv4** IP-адреса:

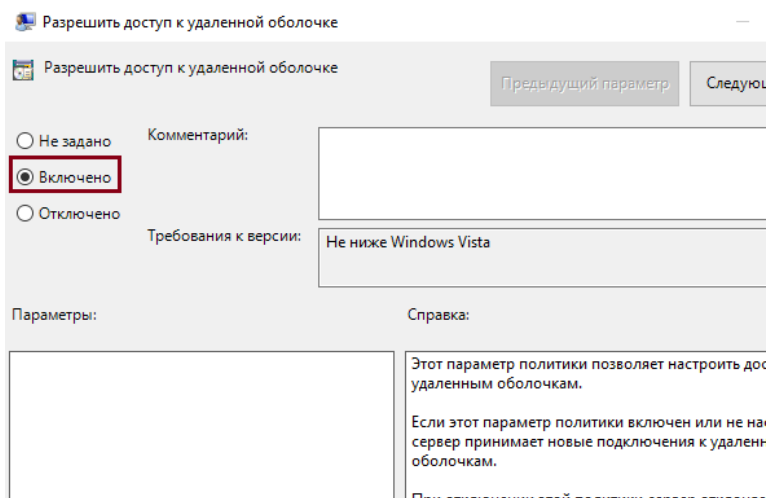
- **Для групповой политики для хоста службы сканирования:** ip-адрес хоста службы сканирования;
- **Для групповой политики для сканируемых узлов:** диапазон ip-адресов.



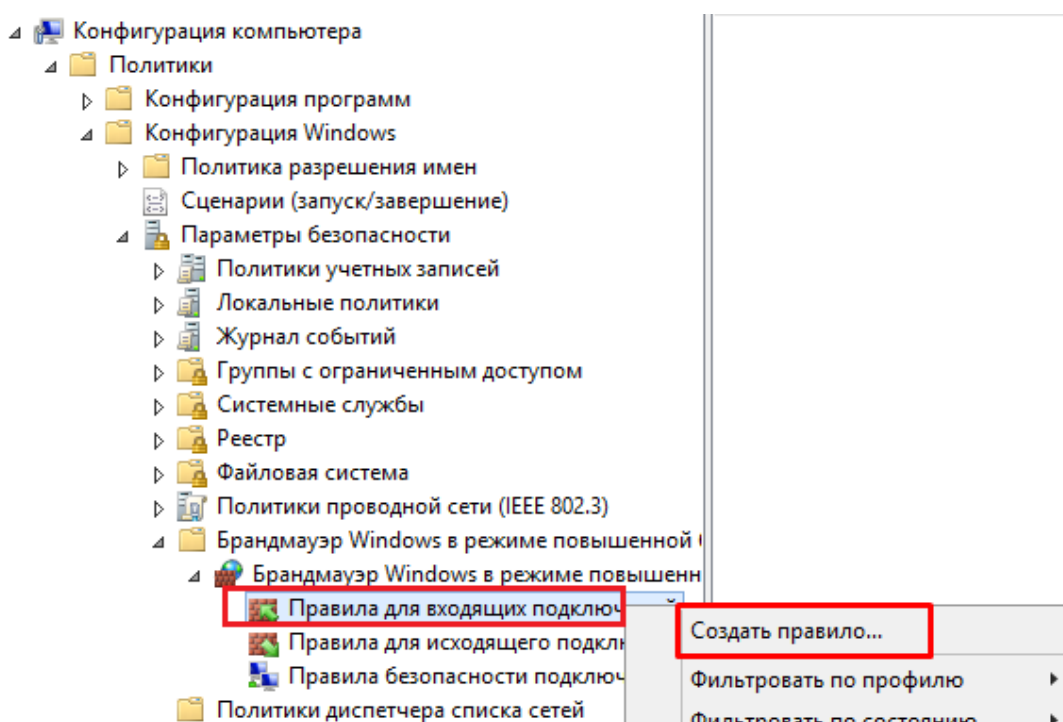
**Шаг 6.** Перейдите в **Компоненты Windows → Удаленная оболочка Windows** → откройте **Разрешить доступ к удаленной оболочке**;



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**;

## Тип правила

Выберите тип правила брандмауэра, которое требуется создать.

**Шаги:**

- Тип правила
- Предопред. правила
- Действие

Правило какого типа вы хотите создать?

**Для программы**  
Правило, управляющее подключениями для программы.

**Для порта**  
Правило, управляющее подключениями для порта TCP или UDP.

**Предопределенные**  
Удаленное управление Windows  
Правило, управляющее подключениями для операций Windows.

**Настраиваемые**  
Настраиваемое правило.

< Назад **Далее >** Отмена

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

## Предопред. правила

Выберите правила, создаваемые для данной ситуации.

### Шаги:

- Тип правила
- Предопред. правила
- Действие

Какие правила вы хотите создать?

Следующие правила определяют требования сетевого подключения для выбранных предопределенных групп. Будут созданы правила, отмеченные флажком. Если отмеченное флажком правило уже существует, его содержимое будет заменено.

Правила:

Имя	Профиль	Прот...	Локал
<input checked="" type="checkbox"/> Удаленное управление Windows (HTTP - вход...	Общий	TCP	5985
<input checked="" type="checkbox"/> Удаленное управление Windows (HTTP - вход...	Домен, Частный	TCP	5985

< Назад

Далее >

Отмена

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

## Действие

Укажите действие, выполняемое при соответствии подключения условиям, заданным в данном правиле.

**Шаги**

- Тип правила
- Предопред. правила
- Действие

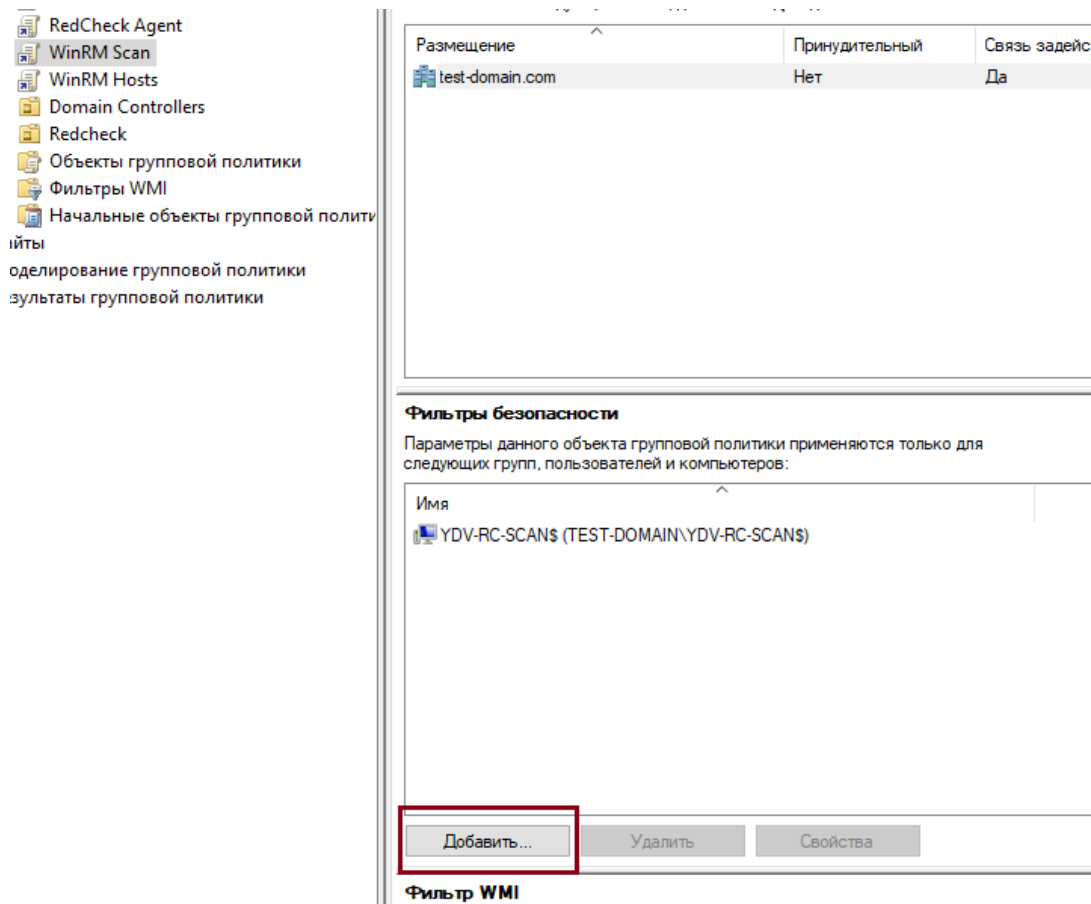
Укажите действие, которое должно выполняться, когда подключение удовлетворяет указанным условиям.

**Разрешить подключение**  
Включая как подключения, защищенные IPSec, так и подключения без защиты.

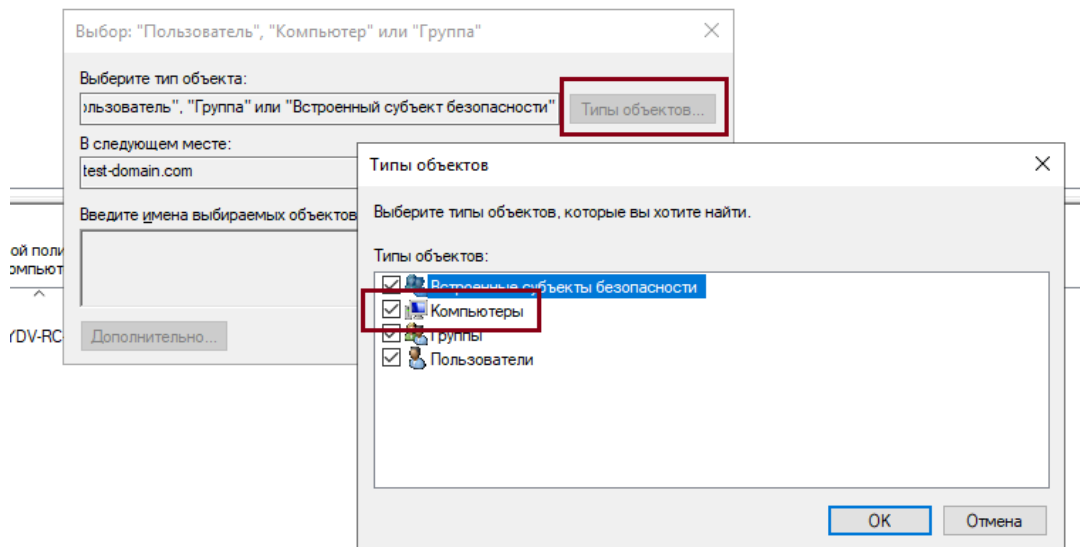
**Разрешить безопасное подключение**  
Включая только подключения с проверкой подлинности с помощью IPSec. Подключения будут защищены с помощью параметров IPSec и правил, заданных в разделе правил безопасности подключений.

**Блокировать подключение**

**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**;

Выбор: "Пользователь", "Компьютер" или "Группа" X

Выберите тип объекта:

В следующем месте:

Введите имена выбираемых объектов (примеры):

## Транспорт WinRM (Kerberos)

Для сканирования хостов по протоколу WinRM с использованием доменных учетных записей по протоколу аутентификации Kerberos необходимо настроить конфигурационный файл /etc/krb5.conf, находящийся на хосте с установленной службой сканирования.

Содержимое файла **регистрозависимо**

Свойства (файлы .properties)

```
includedir /etc/krb5.conf.d/

[logging]
default = FILE:/var/log/krb5libs.log
kdc = FILE:/var/log/krb5kdc.log
admin_server = FILE:/var/log/kadmind.log

[libdefaults]
dns_lookup_realm = false
dns_lookup_kdc = false
rdns = false
ticket_lifetime = 24h
renew_lifetime = 7d
pkinit_anchors = FILE:/etc/pki/tls/certs/ca-bundle.crt
spake_preauth_groups = edwards25519
default_ccache_name = KEYRING:persistent:%{uid}
permitted_encetypes = aes256-cts arcfour-hmac-md5 aes128-cts rc4-
hmac des3-cbc-sha1 des-cbc-md5 des-cbc-crc
default_tgs_encetypes = aes256-cts arcfour-hmac-md5 aes128-cts
rc4-hmac des3-cbc-sha1 des-cbc-md5 des-cbc-crc
default_tkt_encetypes = aes256-cts arcfour-hmac-md5 aes128-cts
rc4-hmac des3-cbc-sha1 des-cbc-md5 des-cbc-crc

[realms]
NAME-DOMAIN.COM = {
```



```
kdc = dnsname.name-domain.com
admin_server = dnsname.name-domain.com
}

[domain_realm]
.name-domain.com = NAME-DOMAIN.COM
name-domain.com = NAME-DOMAIN.COM
```

### [libdefaults]

- **rdns** – если этот флаг установлен, то обратный поиск по имени будет использоваться в дополнение к прямому поиску по имени для канонизации имен хостов для использования в именах участников службы;
- Параметры **permitted\_enctypes**, **default\_tgs\_enctypes**, **default\_tkt\_enctypes** необходимы для корректного определения алгоритма шифрования во время сканирования.

### [realms]

- **kdc** – имя или адрес хоста, на котором запущен KDC для этой области (может быть указано несколько адресов);
- **admin\_server** – определяет хост, на котором запущен сервер администрирования. Как правило, это главный сервер Kerberos;

Раздел **[domain\_realm]** предоставляет преобразование доменного имени или имени хоста в имя области Kerberos.

Подробную документацию по настройке конфигурационного файла можно найти по ссылке – [https://web.mit.edu/kerberos/krb5-1.16/doc/admin/conf\\_files/krb5\\_conf.html](https://web.mit.edu/kerberos/krb5-1.16/doc/admin/conf_files/krb5_conf.html)

## 4.4.2 Сканирование Unix-систем (SSH)

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 – SSH**.

**Новая / Редактируемая учётная запись**  
Укажите требуемые параметры для новой или редактируемой учётной записи.

Имя профиля

Тип учётной записи

---

Имя пользователя

Указать пароль  
 Указать ключ  
 Указать ключ и проверочную фразу

Пароль

Подтверждение пароля

SSH порт

Настройка привилегий

Указать пароль привилегий

Пароль привилегий

Подтверждение пароля привилегий

Разделитель

Разделитель терминального пейджера

Для сканирования удалённой системы могут использоваться следующие типы учётных записей:

- Учетная запись суперпользователя (root)
- Учетная запись привилегированного пользователя (sudo)

- Учетная 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**).

```
root@astra:~# systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2022-11-08 14:52:28 MSK; 1 months 4 days ago
     Process: 16216 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
     Process: 3486 ExecReload=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
     Process: 3523 ExecReload=/bin/kill -HUP $MAINPID (code=exited, status=0/SUCCESS)
    Main PID: 16228 (sshd)
      Tasks: 1 (limit: 1020)
     Memory: 1.0M
     CGroup: /system.slice/ssh.service
            └─16228 /usr/sbin/sshd -D

Warning: Journal has been rotated since unit was started. Log output is incomplete or unavailable.
root@astra:~# █
```

**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
```

```
redcheck-scan@astra:/etc/ssh$ cat ./sshd_config | grep Subsystem
Subsystem sftp /usr/lib/openssh/sftp-server
redcheck-scan@astra:/etc/ssh$
```

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

```
Subsystem sftp /usr/lib/openssh/sftp-server
```

```
# override default of no subsystems
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.

### **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.

## Учетная запись привилегированного пользователя (sudo)

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.

## Учетная 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
```

### 4.4.3 Сканирование FreeBSD

Для сканирования удалённого хоста требуется создать учётную запись, **Тип** – **FreeBSD**.

**Новая / Редактируемая учётная запись**  
Укажите требуемые параметры для новой или редактируемой учётной записи.

Имя профиля	<input type="text"/>
Тип учётной записи	FreeBSD <input type="button" value="v"/>
<hr/>	
Имя пользователя	<input type="text"/>
	<input checked="" type="radio"/> Указать пароль <input type="radio"/> Указать ключ <input type="radio"/> Указать ключ и проверочную фразу
Пароль	<input type="text"/>
Подтверждение пароля	<input type="text"/>
SSH порт	<input type="text" value="22"/>
Настройка привилегий	Sudo <input type="button" value="v"/> <input type="checkbox"/> Указать пароль привилегий
Пароль привилегий	<input type="text"/>
Подтверждение пароля привилегий	<input type="text"/>

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.

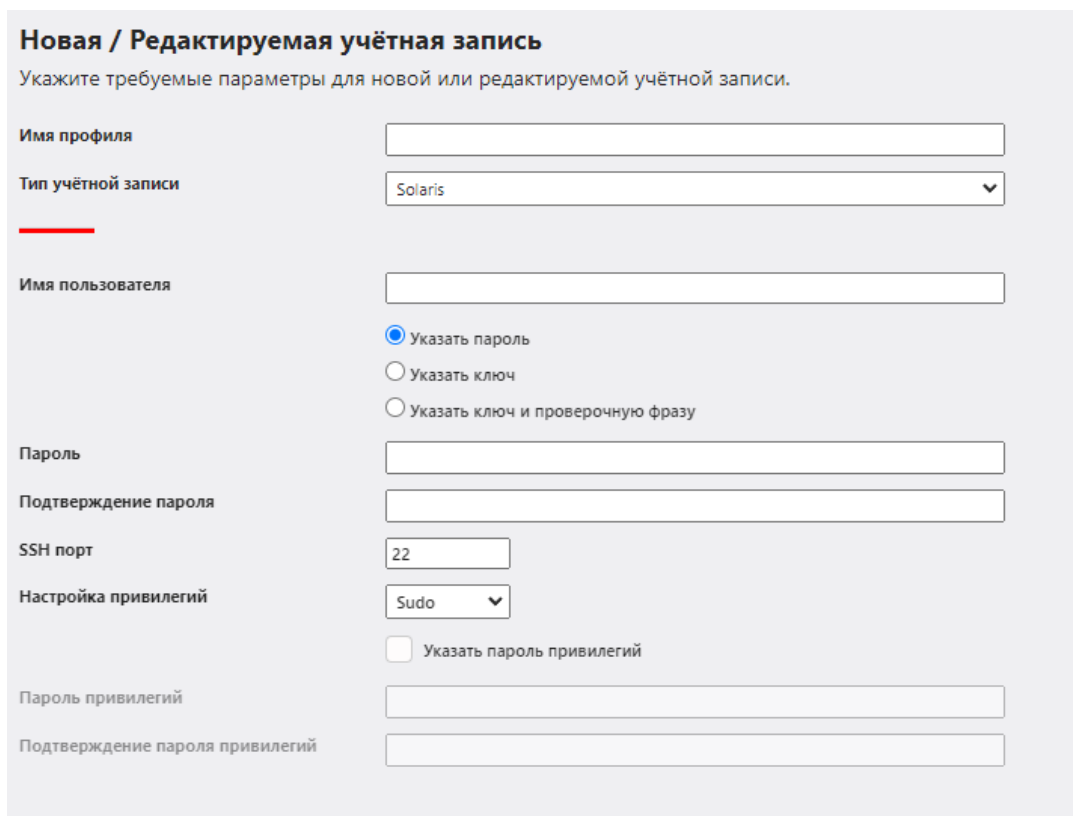
#### Перечень выполняемых команд в момент сканирования:

- sudo
- echo
- bind
- printf
- grep
- test
- file
- mktemp
- command
- cat
- find
- getfacl
- stat
- uname
- chmod
- base64

- rm
- basename
- dirname
- which
- openssl
- ls
- pkg

#### 4.4.4 Сканирование Solaris

Для сканирования удалённого хоста требуется создать учётную запись, **Тип – Solaris.**



**Новая / Редактируемая учётная запись**  
Укажите требуемые параметры для новой или редактируемой учётной записи.

Имя профиля

Тип учётной записи

---

Имя пользователя

Указать пароль  
 Указать ключ  
 Указать ключ и проверочную фразу

Пароль

Подтверждение пароля

SSH порт

Настройка привилегий

Указать пароль привилегий

Пароль привилегий

Подтверждение пароля привилегий

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 rfxes; непривилегированного), или создать отдельную.

## 4.4.5 Сканирование Check Point

Для сканирования удалённого хоста требуется создать учетную запись, **Тип** – **Check Point Gaia**.

**Новая / Редактируемая учётная запись**  
Укажите требуемые параметры для новой или редактируемой учётной записи.

Имя профиля	<input type="text"/>
Тип учётной записи	Check Point Gaia <input type="button" value="v"/>
<hr/>	
Имя пользователя	<input type="text"/>
	<input checked="" type="radio"/> Указать пароль <input type="radio"/> Указать ключ <input type="radio"/> Указать ключ и проверочную фразу
Пароль	<input type="text"/>
Подтверждение пароля	<input type="text"/>
SSH порт	<input type="text" value="22"/>
	<input type="checkbox"/> Разделитель
Разделитель терминального пейджера	<input type="text" value="-- More --"/>

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

## 4.4.6 Сканирование Cisco IOS / NX-OS

Для сканирования Cisco IOS / NX-OS (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 IOS / Cisco NX-OS**

### Новая / Редактируемая учётная запись

Укажите требуемые параметры для новой или редактируемой учётной записи.

Имя профиля	<input type="text"/>
Тип учётной записи	Cisco IOS <input type="button" value="v"/>
Имя пользователя	<input type="text"/>
Пароль	<input type="text"/>
Подтверждение пароля	<input type="text"/>
SSH порт	22 <input type="text"/>
Настройка привилегий	None <input type="button" value="v"/>
Разделитель терминального пейджера	<input type="text" value="^\s*--\s*more\s*--\s*\$"/>

Указать пароль  
 Указать ключ  
 Указать ключ и проверочную фразу  
 Разделитель

**Cisco IOS.** 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

## 4.4.7 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 VRP.**

### Новая / Редактируемая учётная запись

Укажите требуемые параметры для новой или редактируемой учётной записи.

Имя профиля	<input type="text"/>
Тип учётной записи	<input type="text" value="Huawei VRP"/>
<hr/>	
Имя пользователя	<input type="text"/>
	<input checked="" type="radio"/> Указать пароль <input type="radio"/> Указать ключ <input type="radio"/> Указать ключ и проверочную фразу
Пароль	<input type="text"/>
Подтверждение пароля	<input type="text"/>
SSH порт	<input type="text" value="22"/>
Настройка привилегий	<input type="text" value="None"/>
	<input type="checkbox"/> Разделитель
Разделитель терминального пейджера	<input type="text" value="^\s*--\s*more\s*--\s*\$"/>

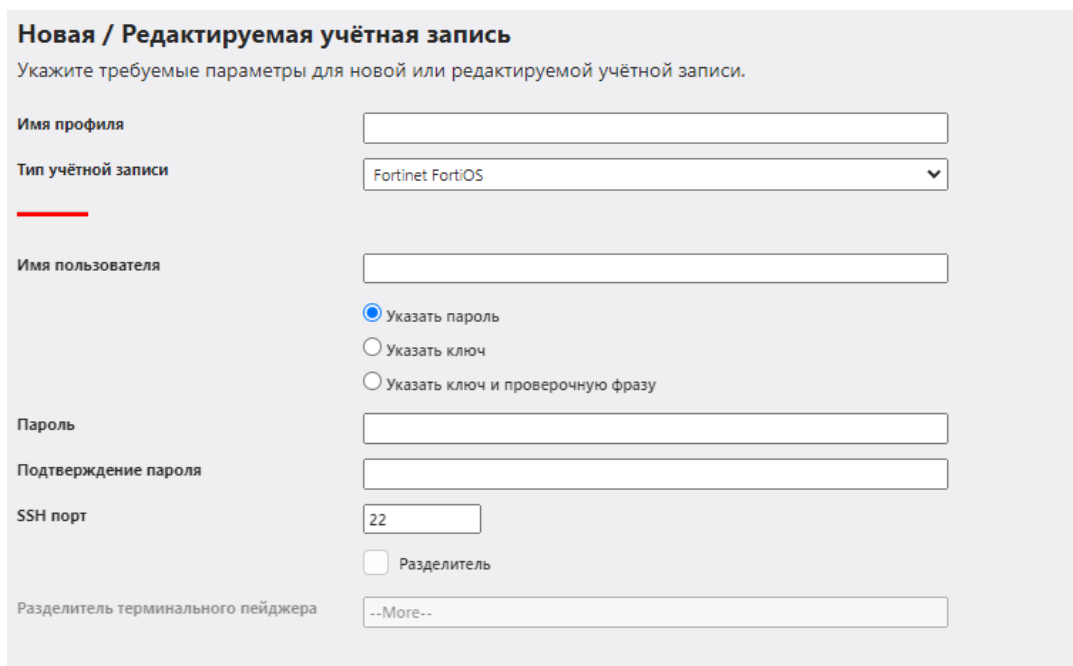
Аналогичные настройки учётных записей производятся и для сетевого оборудования «Булат».

**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

## 4.4.8 Сканирование FortiOS

Для сканирования удаленного хоста требуется создать учётную запись, **Тип – FortiOS**.



**Новая / Редактируемая учётная запись**  
Укажите требуемые параметры для новой или редактируемой учётной записи.

Имя профиля:

Тип учётной записи: Fortinet FortiOS

Имя пользователя:

Указать пароль:  Указать ключ:  Указать ключ и проверочную фразу:

Пароль:

Подтверждение пароля:

SSH порт: 22

Разделитель:

Разделитель терминального пейджера: --More--

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).

## 4.4.9 Сканирование UserGate

Для сканирования удаленного хоста требуется создать учётную запись, **Тип – UserGate**.

### Новая / Редактируемая учётная запись

Укажите требуемые параметры для новой или редактируемой учётной записи.

Имя профиля	<input type="text"/>
Тип учётной записи	UserGate NGFW
Имя пользователя	<input type="text"/>
Пароль	<input type="password"/>
Подтверждение пароля	<input type="password"/>
HTTP(S) порт	4040

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).

## 4.4.10 Сканирование 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:**

- VimEsxCLLsoftwareviblist

## **Содержание**

- [Настройка VMware ESXi Server](#)
- [Настройка VMware vCenter Server](#)
- [Настройка VMware NSX Data Center](#)

## Настройка VMware ESXi Server

Для сканирования удаленного хоста требуется создать учётную запись, **Тип – VMware ESXi**.

**Новая / Редактируемая учётная запись**

Укажите требуемые параметры для новой или редактируемой учётной записи.

Имя профиля	<input style="width: 90%;" type="text"/>
Тип учётной записи	<input style="width: 90%;" type="text" value="VMware ESXi"/>
<hr style="border: 1px solid red;"/>	
Имя пользователя	<input style="width: 90%;" type="text"/>
Пароль	<input style="width: 90%;" type="password"/>
Подтверждение пароля	<input style="width: 90%;" type="password"/>
HTTP(S) порт	<input style="width: 50%;" type="text" value="443"/>
	<input type="checkbox"/> Проверка сертификата

**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

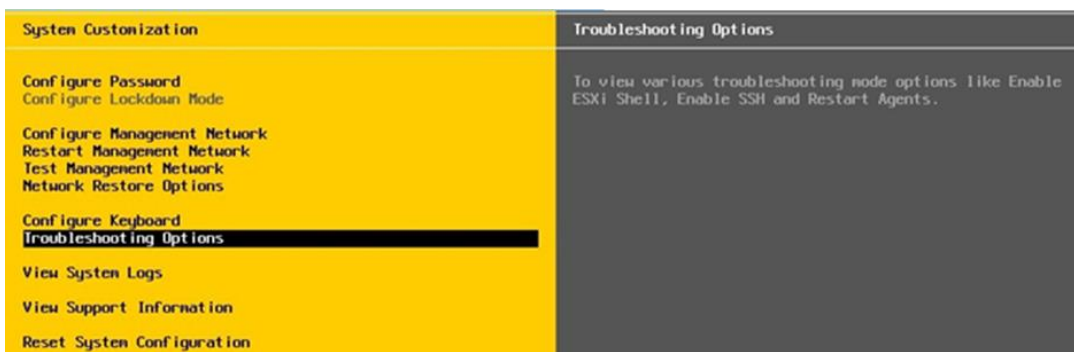
Direct Console User Interface (DCUI) – это интерфейс сервера ESXi, который выводится на монитор при прямом подключении к серверу.



**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**;



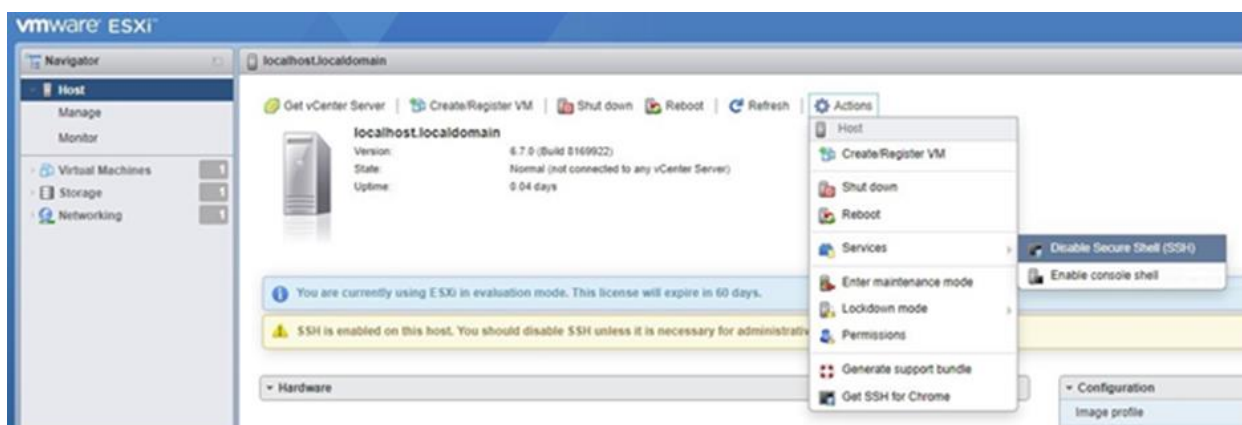
Для возврата в основное меню нажмите ESC.

## Включение SSH при помощи Web-клиента vSphere

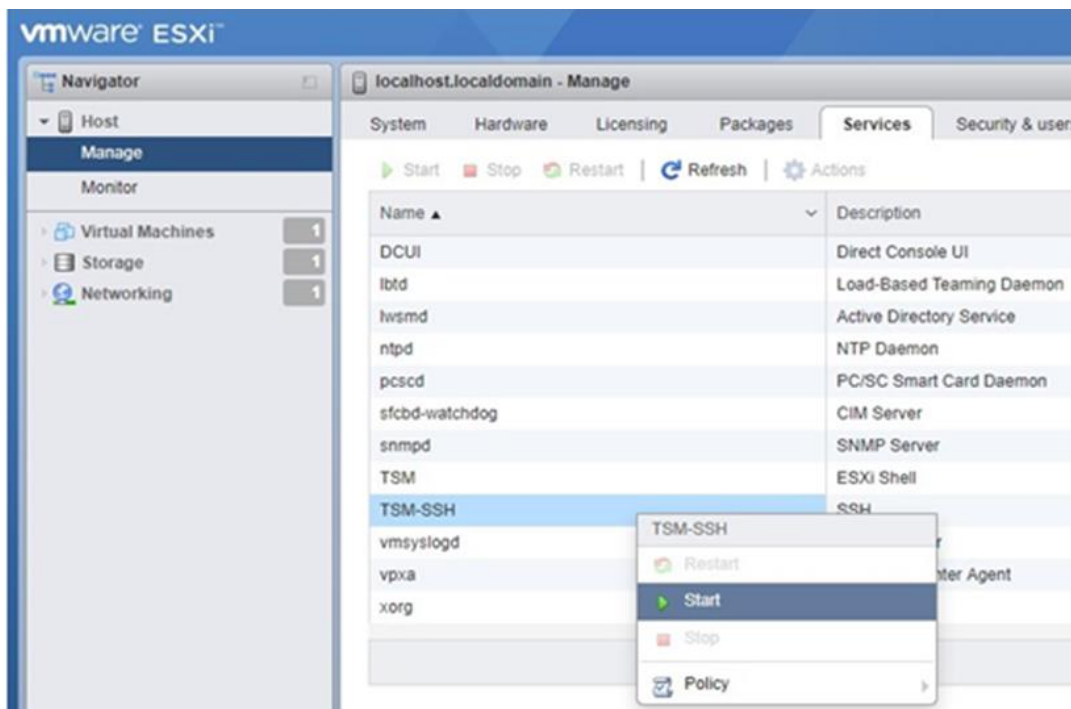
**Шаг 1.** Запустите браузер → введите в адресной строке адрес VMware сервера → авторизуйтесь на сервере ESXi через интерфейс vSphere Web Client;



**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.

## Настройка VMware vCenter Server

Для сканирования удаленного хоста требуется создать учётную запись, **Тип – VMware vCenter.**

**Новая / Редактируемая учётная запись**  
 Укажите требуемые параметры для новой или редактируемой учётной записи.

Имя профиля

Тип учётной записи

---

Имя пользователя

Пароль

Подтверждение пароля

HTTP(S) порт

Проверка сертификата

**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.

## **Настройка VMware NSX Data Center**

Для сканирования удаленного хоста требуется создать учётную запись, **Тип – VMware NSX.**

### Новая / Редактируемая учётная запись

Укажите требуемые параметры для новой или редактируемой учётной записи.

Имя профиля	<input type="text"/>
Тип учётной записи	VMware NSX <input type="button" value="v"/>
<hr/>	
Имя пользователя	<input type="text"/>
Пароль	<input type="password"/>
Подтверждение пароля	<input type="password"/>
HTTP(S) порт	<input type="text" value="443"/>
	<input type="checkbox"/> Проверка сертификата

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

## 4.4.11 Сканирование Microsoft SQL Server

Для сканирования БД Microsoft SQL Server требуется создать учётную запись, **Тип – SQL, Тип БД – MS SQL.**

### Новая / Редактируемая учётная запись

Укажите требуемые параметры для новой или редактируемой учётной записи.

Имя профиля	<input type="text"/>
Тип учётной записи	SQL <input type="button" value="v"/>
Тип БД	<input checked="" type="radio"/> MS SQL <input type="radio"/> Oracle <input type="radio"/> MySQL <input type="radio"/> PostgreSQL
Экземпляр	<input type="text"/>
Порт	<input checked="" type="checkbox"/> Порт по умолчанию <input type="text" value="1433"/>
Логин	<input type="text"/>
Пароль	<input type="text"/>
Подтверждение пароля	<input type="text"/>
	<input type="checkbox"/> Использовать аутентификацию Windows

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**.

Поддержка TLS 1.2 начинается с версии SQL Server 2016. Для сканирования Microsoft SQL Server ниже 2016 необходимо изменить версию протокола в `/etc/ssl/openssl.cnf` на стороне службы сканирования;

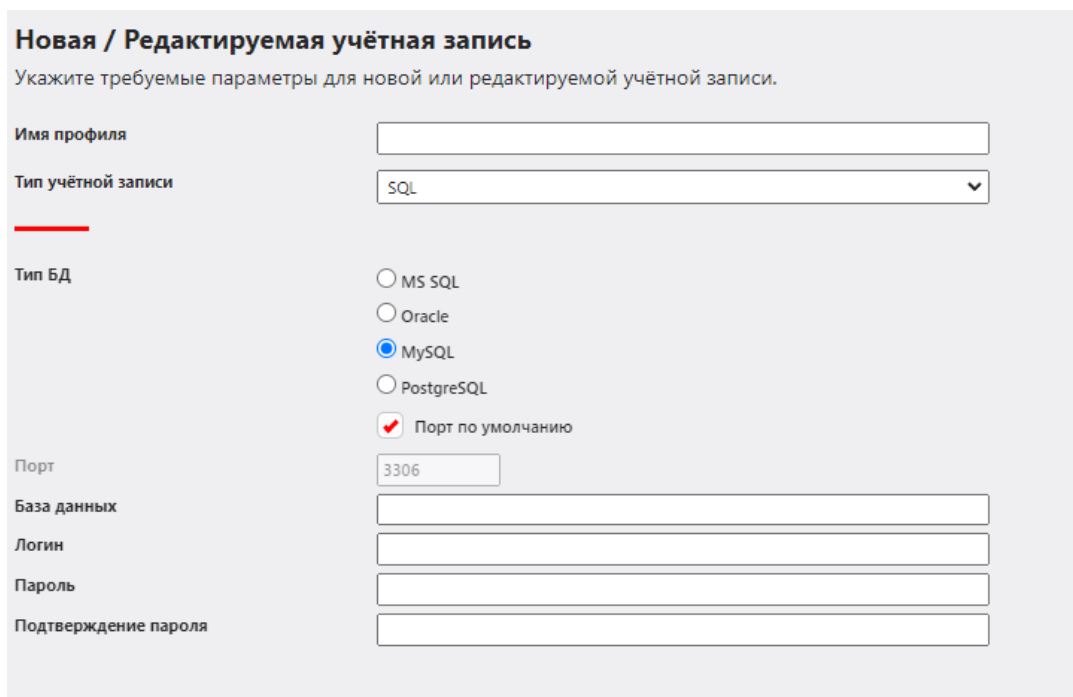
### Bash (оболочка Unix)

```
MinProtocol = TLSv1  
CipherString = DEFAULT@SECLEVEL=1
```



## 4.4.12 Сканирование MySQL

Для сканирования БД MySQL требуется создать учётную запись, **Тип – SQL, Тип БД – MySQL.**



The screenshot shows a web form titled "Новая / Редактируемая учётная запись" (New / Editable user profile). Below the title is a subtitle: "Укажите требуемые параметры для новой или редактируемой учётной записи." (Specify the required parameters for a new or editable user profile). The form contains several fields:

- Имя профиля** (Profile name): A text input field.
- Тип учётной записи** (User type): A dropdown menu with "SQL" selected.
- Тип БД** (Database type): Radio buttons for "MS SQL", "Oracle", "MySQL" (selected), and "PostgreSQL". There is also a checked checkbox for "Порт по умолчанию" (Default port).
- Порт** (Port): A text input field containing "3306".
- База данных** (Database): A text input field.
- Логин** (Login): A text input field.
- Пароль** (Password): A text input field.
- Подтверждение пароля** (Confirm password): A text input field.

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)



## 4.4.13 Сканирование PostgreSQL

Для сканирования БД требуется создать учётную запись **Тип – SQL, Тип БД – PostgreSQL**.

**Новая / Редактируемая учётная запись**  
Укажите требуемые параметры для новой или редактируемой учётной записи.

Имя профиля

Тип учётной записи

Тип БД

MS SQL  
 Oracle  
 MySQL  
 PostgreSQL  
 Порт по умолчанию

Порт

База данных

Логин

Пароль

Подтверждение пароля

Timeout

Command Timeout

Protocol

SslMode

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;
```

**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
```

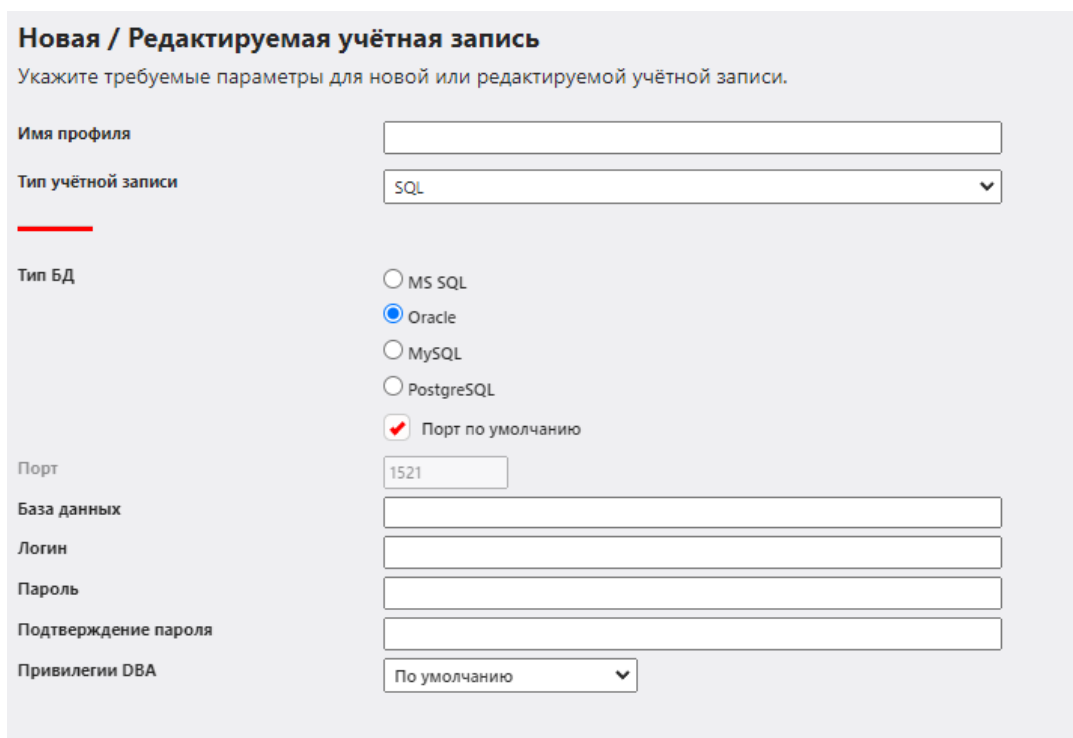
### Для BaseAlt

#### Bash (Unix Shell)

```
echo host all rc_scan_pg <имя_сети/маска> md5 >>  
/var/lib/pgsql/data/pg_hba.conf
```

## 4.4.14 Сканирование Oracle

Для сканирования БД Oracle требуется создать учётную запись, **Тип – SQL, Тип БД – Oracle.**



**Новая / Редактируемая учётная запись**  
Укажите требуемые параметры для новой или редактируемой учётной записи.

Имя профиля

Тип учётной записи

Тип БД

MS SQL

Oracle

MySQL

PostgreSQL

Порт по умолчанию

Порт

База данных

Логин

Пароль

Подтверждение пароля

Привилегии DBA

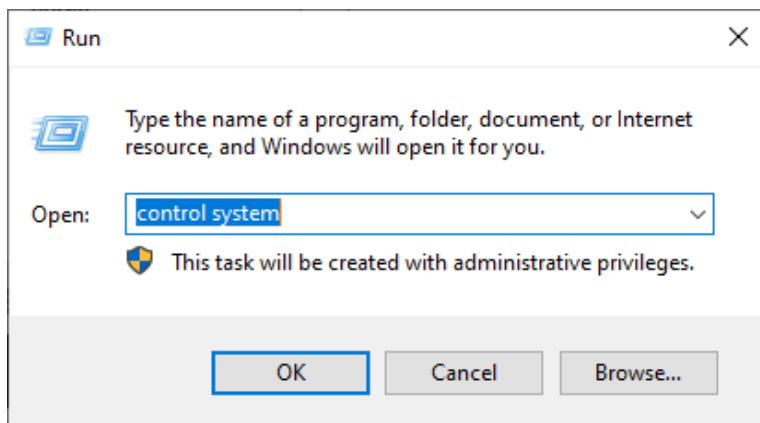
В экземпляре СУБД должен использоваться смешанный тип аутентификации (проверка подлинности Oracle).

По умолчанию для сканирования СУБД Oracle используется порт 1521. В случае использования в инфраструктуре сети другого порта его необходимо явно указать.

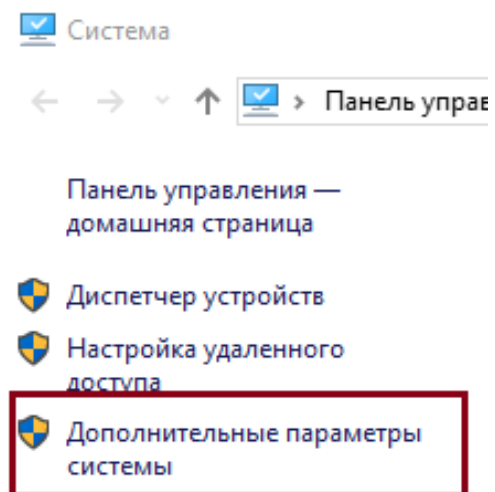
### Добавление переменной среды ORACLE\_HOME

Для проведения задания **Аудит БД Oracle** на сервере с установленной СУБД необходимо добавить переменную среды ORACLE\_HOME.

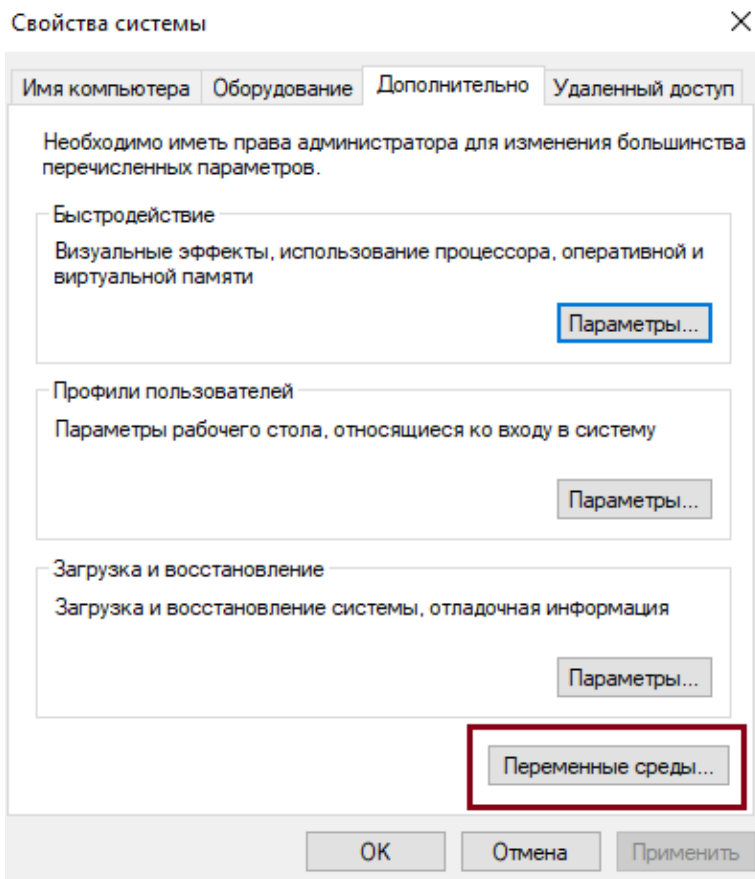
**Шаг 1.** Нажмите **Win + R** и введите **control system**;



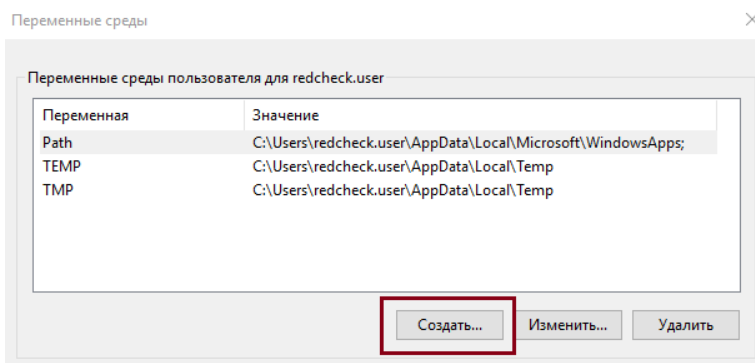
**Шаг 2.** Перейдите в **Дополнительные параметры системы;**



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

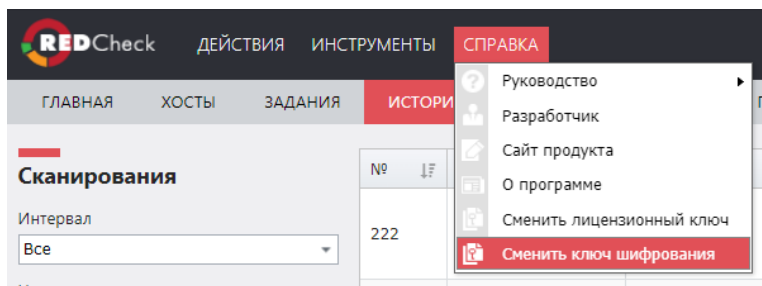
```
GRANT CONNECT TO <USER NAME>;
GRANT SELECT ON DBA_USERS TO <USER NAME>;
GRANT SELECT ON DBA_USERS_WITH_DEFPWD TO <USER NAME>;
GRANT SELECT ON DBA_TAB_PRIVS TO <USER NAME>;
GRANT SELECT ON DBA_PROFILES TO <USER NAME>;
GRANT SELECT ON DBA_TS_QUOTAS TO <USER NAME>;
GRANT SELECT ON DBA_ROLE_PRIVS TO <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.

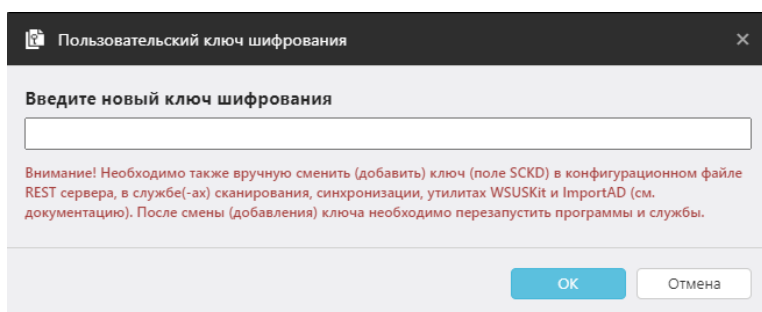


## 4.5 Смена ключа шифрования

**Шаг 1.** Раскройте **Справка** → **Сменить ключ шифрования**;



**Шаг 2.** Введите новый ключ шифрования → **ОК**;



**Шаг 3.** Вручную смените ключ шифрования для серверного компонента. На хосте с установленным серверным компонентом необходимо открыть файл **/var/opt/redcheck-api/conf/appsettings.json** и заменить старый ключ на новый для параметра **Sckd**

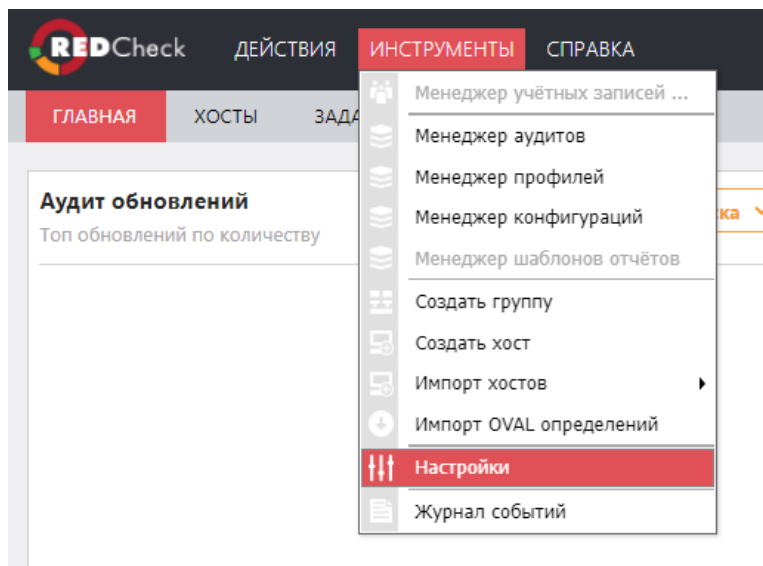
**Шаг 4.** На хосте для каждой установленной службы сканирования необходимо открыть файл **/var/opt/redcheck-scan-service/conf/appsettings.json** и заменить старый ключ на новый для параметра **Sckd**

```
{
  "ConnectionStrings": {
    "Default": "CfDJ8JN-D2R9
  },
  "DbOperationTimeout": 3000
  "Sckd": "",
  "Service": {
    "ServiceId": "3ba1f3f2-1
    "Language": "Ru"
  },
  "Polling": {
    "PollingIntervalSec": 1
  },
}
```

**Шаг 5.** На хосте с установленной службой синхронизации необходимо открыть файл `/var/opt/redcheck-sync-service/conf/appsettings.json` и заменить старый ключ на новый для параметра **Sckd**

## 4.6 Обслуживание 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;

**Очистка БД**  
Служба очистки БД позволяет удалять неактуальные результаты сканирований и отчёты для уменьшения размера БД.

**Статус службы очистки** Свободна

Удалять результаты сканирований  
0

Удалять отчёты  
0

Включить ежедневный сервис очистки БД  
00 00

Уведомлять при превышении размера БД  
0

Почта 11

Нет данных для отображения

Всего: 0

**Шаг 3.** Отметьте **Удалять отчеты** и **Удалять результаты сканирований**. Укажите нужный срок давности отчетов для очистки;

**Статус службы очистки** Свободна

Удалять результаты сканирований  
12

**Сканирования старше, мес.**  
Сканирования, которые являются эталонами контролей, удалены не будут.

Удалять отчёты  
12

**Отчёты старше, мес.**

**Начните очистку БД с параметрами выше прямо сейчас**

**Шаг 4.** Нажмите **Очистить БД**;

**Начните очистку БД с параметрами выше прямо сейчас**

**Шаг 5.** Для автоматической очистки БД отметьте **Включить ежедневный сервис очистки БД** → выберите время запуска службы очистки;

Или настройте очистку по расписанию  
Периодическая очистка происходит быстро и позволяет эффективно ограничивать рост размера БД.

Включить ежедневный сервис очистки БД

Время запуска очистки БД

**Шаг 6.** При необходимости включите оповещение о превышении БД указанного размера, отметив **Уведомлять при превышении размера БД** и указав почтовые адреса получателей;

Включите получение уведомлений  Уведомлять при превышении размера БД

Размер БД, Гб

Список получателей уведомлений

Почта	
Нет данных для отображения	
Всего: 0	

## 4.7 Резервное копирование и восстановление БД

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

- [4.7.1 Резервное копирование PostgreSQL](#)
- [4.7.2 Восстановление PostgreSQL](#)

## 4.7.1 Резервное копирование PostgreSQL

Для создания резервной копии базы данных выполните следующие шаги.

**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.

## 4.7.2 Восстановление PostgreSQL

**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.



## 4.8 Обновление RedCheck Nix

Обновлять службу сканирования необходимо только после окончания всех сканирований. В случае обновления службы, у которой есть не окончившиеся или принудительно остановленные задания, эти задания не смогут запуститься после обновления.

Для обновления RedCheck необходимо выполнить следующие шаги:

**Шаг 1.** Скачайте обновленный архив, переместите скачанный архив \*.tar.gz в директорию, отличную от пользовательского каталога. В инструкции архив перемещается в /mnt;

Bash (оболочка Unix)

```
mv /home/имя_пользователя/Загрузки/redcheck-repo-2.7.0.tar.gz /mnt/
```

**Шаг 2.** Перейдите в каталог, удалите текущий репозиторий и разархивируйте свежий дистрибутив;

Bash (оболочка Unix)

```
cd /mnt
```

Bash (оболочка Unix)

```
rm -R redcheck-repo
```

Bash (оболочка Unix)

```
tar -xf redcheck-repo-2.7.0.tar.gz
```

**Шаг 3.** Добавьте информацию в пакетный менеджер о новых .NET пакетах, если ранее это не выполнялось;

Astra Linux:

Bash (оболочка Unix)

```
echo "deb file:/mnt/redcheck-repo/ 1.7_x86-64 non-free dotnet" > /etc/apt/sources.list.d/redcheck.list
```

РЕД ОС / SberLinux:

Bash (оболочка Unix)

```
touch /etc/yum.repos.d/redcheck-dotnet.repo
```

Bash (оболочка Unix)

```
echo -e "[redcheck-dotnet-repo]
name=ALT.X .NET 6.0.35
baseurl=file:/mnt/redcheck-redos-repo/redcheck-dotnet
enabled=1
gpgcheck=0
gpgkey=file:/mnt/redcheck-redos-repo/redcheck-base/PUBLIC-GPG-KEY-
redcheck" > /etc/yum.repos.d/redcheck-dotnet.repo
```

**Шаг 4.** Обновите пакеты;

Astra Linux / Debian:

Bash (оболочка Unix)

```
apt -y update
```

РЕД ОС / SberLinux:

Bash (оболочка Unix)

```
dnf makecache
```

**Шаг 5.** Переустановите компоненты RedCheck;

Astra Linux:

Bash (оболочка Unix)

```
apt -y dist-upgrade redcheck-dotnet-runtime redcheck-aspnetcore-
```

```
runtime redcheck-api redcheck-client redcheck-scan-service redcheck-  
sync-service altxmap redcheck-cleanup-service
```

Debian:

Bash (оболочка Unix)

```
apt install -y icu-devtools=63.1-6+deb10u2 libicu63=63.1-6+deb10u2  
libicu-dev=63.1-6+deb10u2 --allow-downgrades
```

Bash (оболочка Unix)

```
apt -y dist-upgrade redcheck-dotnet-runtime redcheck-aspnetcore-  
runtime redcheck-api redcheck-client redcheck-scan-service redcheck-  
sync-service altxmap redcheck-cleanup-service
```

РЕД ОС / SberLinux:

Bash (оболочка Unix)

```
dnf -y upgrade redcheck-dotnet-runtime redcheck-aspnetcore-runtime  
redcheck-api redcheck-client redcheck-scan-service redcheck-sync-  
service altxmap redcheck-cleanup-service
```

На этапе обновления пакетов введите Y или I для обновления конфигурации:

```
Настраивается пакет redcheck-api (2.7.0-alpha484+build278) ...  
Файл настройки «/var/opt/redcheck-api/conf/appsettings.json»  
==> Изменён с момента установки (вами или сценарием).  
==> Автор пакета предоставил обновлённую версию.  
Что нужно сделать? Есть следующие варианты:  
Y или I : установить версию, предлагаемую сопровождающим пакета  
N или O : оставить установленную на данный момент версию  
D      : показать различия между версиями  
Z      : запустить оболочку командной строки для проверки ситуации  
По умолчанию сохраняется текущая версия файла настройки.  
*** appsettings.json (Y/I/N/O/D/Z) [по умолчанию N] ? █  
Ход выполнения: [ 79%] [#####.....]
```

**Шаг 6.** Заново проведите конфигурацию компонентов RedCheck.

Перед повторной конфигурацией **рекомендуем** [сделать резервную копию](#) базы данных.

Bash (оболочка Unix)

```
redcheck-bootstrap configure -c=all
```

В повторной конфигурации нуждается Web-консоль и служба сканирования / служба синхронизации. Этап с **настройкой подключения к БД** можно пропустить.

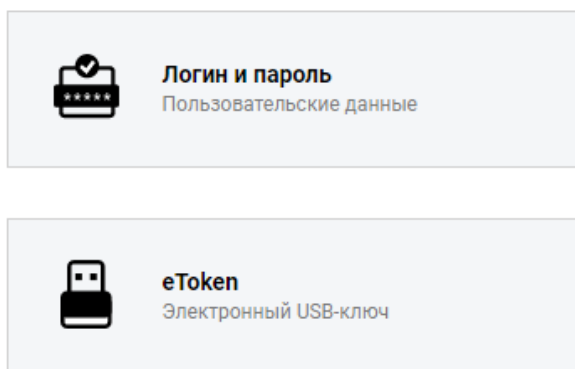
## 4.9 Сброс привязки лицензии

**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).

### Центр сертифицированных обновлений

Для получения обновлений необходимо выбрать способ входа



**Шаг 2.** Раскройте **RedCheck лицензии** → нажмите на интересующий Вас номер ключа RedCheck;

The screenshot shows the 'Система сертифицировое' (Certification System) interface. On the left, there is a sidebar with the 'АЛТЭК СОФТ' logo and navigation options like 'Обновления' (Updates), 'Пользователь' (User), and 'Загрузить' (Download). The main area displays a list of updates for certified software, including 'Обновления для сертифицированного ПО (92)', 'Файлы (28)', 'Руководства (6)', 'Материалы по сертифицированному ПО (5)', 'Обновления Media Kit (21)', 'Обновления VmWare (11)', 'Обновления контента (4)', 'Net Check лицензии (2)', and 'RedCheck лицензии (2)'. Below this list is a table with columns for 'Лицензионный ключ' (License key), 'Редакция' (Edition), and 'Дата окончания' (Expiration date). The table contains one entry for 'RedCheck Enterprise' with a license key highlighted by a red box and an expiration date of '17.04.2025 14:03:06'.

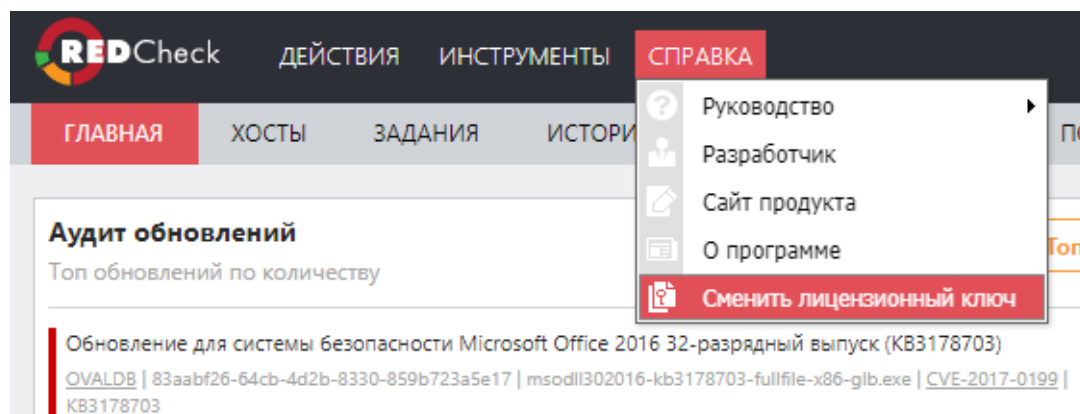
**Шаг 3.** Нажмите **Сбросить** в столбце **Действия**;

	Активен	Дата активации	Действия
	<input type="text"/>	<input type="text"/>	
	True	09.09.2022 17:41:42	<a href="#">Сбросить</a> <a href="#">Скачать</a>
	True	07.07.2022 12:48:09	<a href="#">Сбросить</a> <a href="#">Скачать</a>
	True	01.07.2022 17:02:32	<a href="#">Сбросить</a> <a href="#">Скачать</a>
	True	19.05.2022 12:41:20	<a href="#">Сбросить</a> <a href="#">Скачать</a>
	True	19.05.2022 12:41:13	<a href="#">Сбросить</a> <a href="#">Скачать</a>
	True	19.05.2022 12:41:04	<a href="#">Сбросить</a> <a href="#">Скачать</a>
	True	19.05.2022 12:40:28	<a href="#">Сбросить</a> <a href="#">Скачать</a>
	False	19.04.2022 12:17:22	

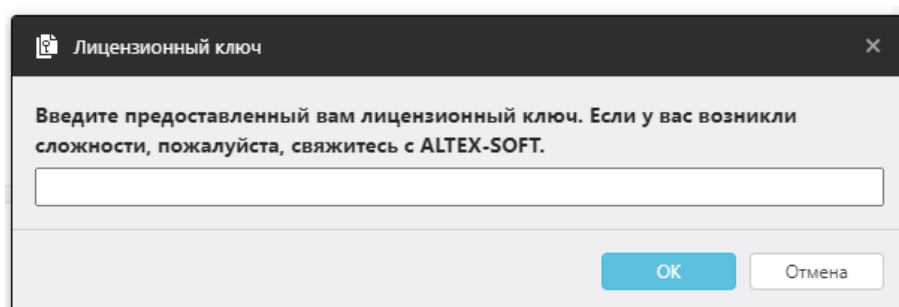
**Шаг 4.** Нажмите **ОК**.

## 4.10 Смена лицензионного ключа

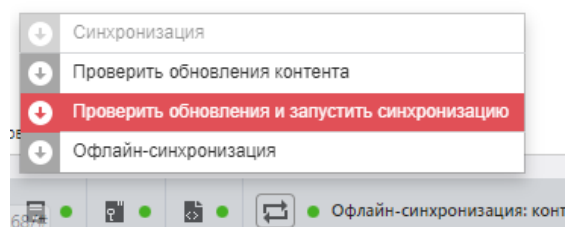
**Шаг 1.** Откройте консоль управления RedCheck, авторизовавшись под учетной записью с ролью RedCheck\_Admins → **Справка** → **Сменить лицензионный ключ**;



**Шаг 2.** Введите новый лицензионный ключ → **ОК**;



**Шаг 3.** Выполните синхронизацию ([4.3 Обновление контента информационной безопасности](#)).



Для офлайн-синхронизации необходимо получить License.xml файл ([4.2 Активация лицензии](#))

Смена ключа и его активация осуществляется после завершения синхронизации контента.



## 4.11 Изменение портов для компонентов RedCheck

### Содержание

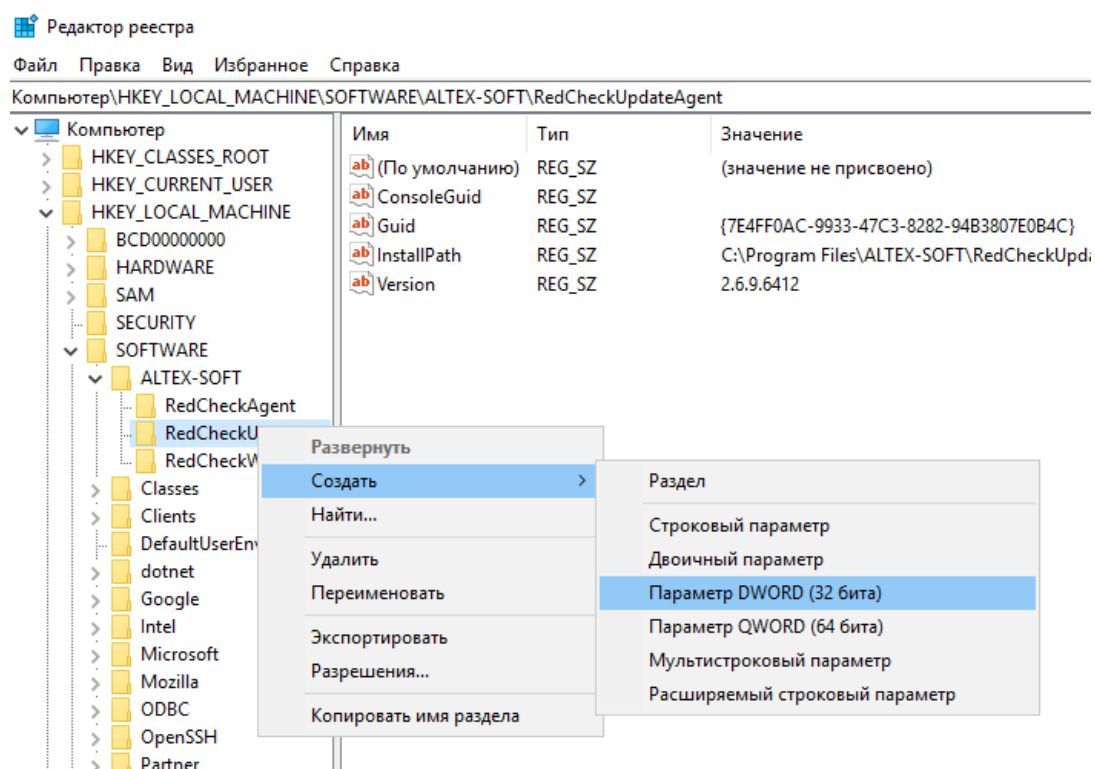
- [4.11.1 Агент обновления](#)
- [4.11.2 Агент сканирования](#)

## 4.11.1 Агент обновления

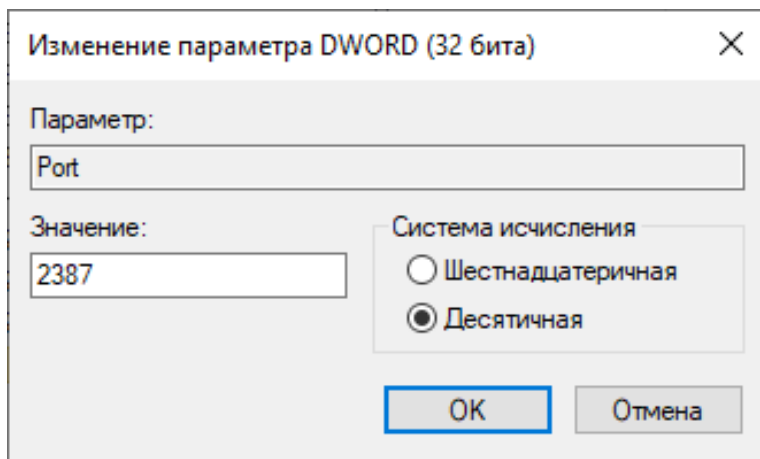
Стандартный порт Update Агента **TCP/IP 8733**.

**Шаг 1.** Зайдите в реестр хоста с установленным агентом и создайте новый параметр **DWORD** с именем **Port**;

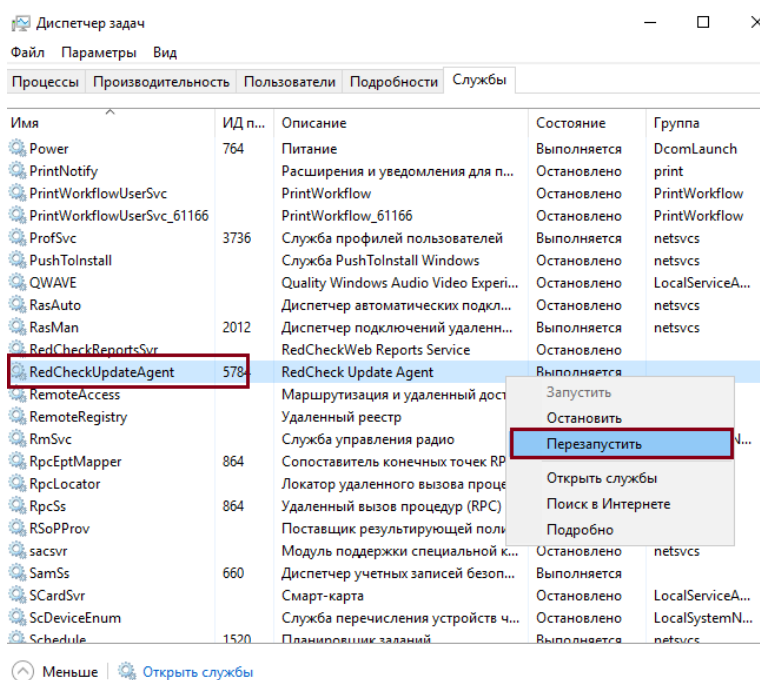
Для x-86 разрядных систем: **HKEY\_LOCAL\_MACHINE\ SOFTWARE\ Wow6432Node\ ALTEX-SOFT\ RedCheckUpdateAgent\ Port (DWORD)**  
Для x-64 разрядных систем: **HKEY\_LOCAL\_MACHINE\ SOFTWARE\ ALTEX-SOFT\ RedCheckUpdateAgent\ Port (DWORD)**



Присвойте ему необходимое значение → **ОК**;



**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;

settings 1 ×

SELECT id, "name", string\_value, bool\_valu | Введите SQL выражение чтобы отфильтровать резу

	123 id	ABC name	ABC string_value	<input checked="" type="checkbox"/> bool_value	123 int_value
13	18	UseProxyImpersonati	[NULL]	[ ]	[NULL]
14	19	ProxyPort	[NULL]	[NULL]	8 080
15	20	ProxyLogin	[NULL]	[NULL]	[NULL]
16	21	WsusSvcAddress	[NULL]	[NULL]	[NULL]
17	22	WsusSvcPort	[NULL]	[NULL]	8 737
18	23	UseWsusSvc	[NULL]	[ ]	[NULL]
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	52	SendMailAfterSuc	[NULL]	[ ]	[NULL]

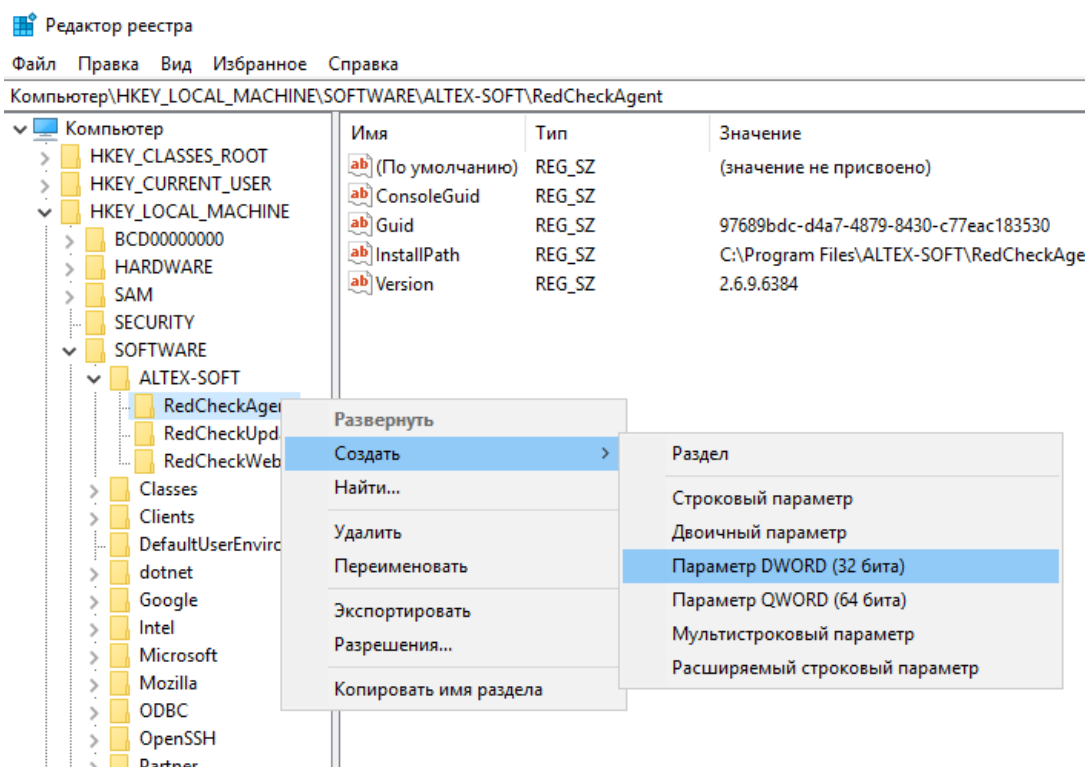
**Шаг 4.** Перезагрузите службу агента обновления, выполнив аналогичные действия из шага 2.

## 4.11.2 Агент сканирования

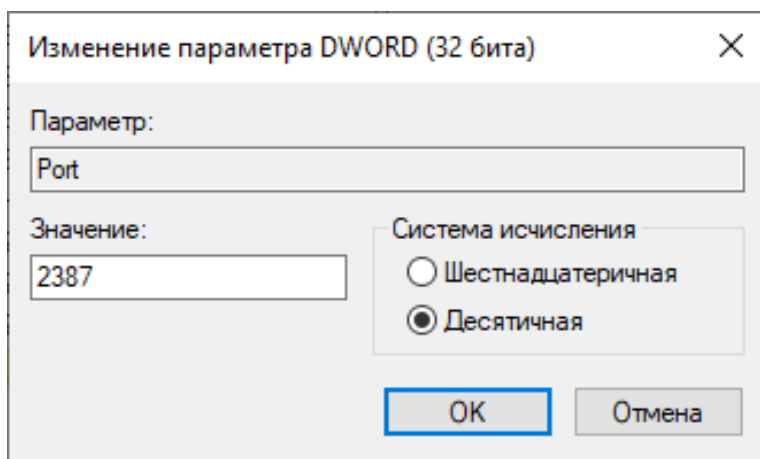
Стандартный порт Агента **TCP/IP 8732**.

**Шаг 1.** Зайдите в реестр хоста с установленным агентом и создайте новый параметр **DWORD** с именем **Port**;

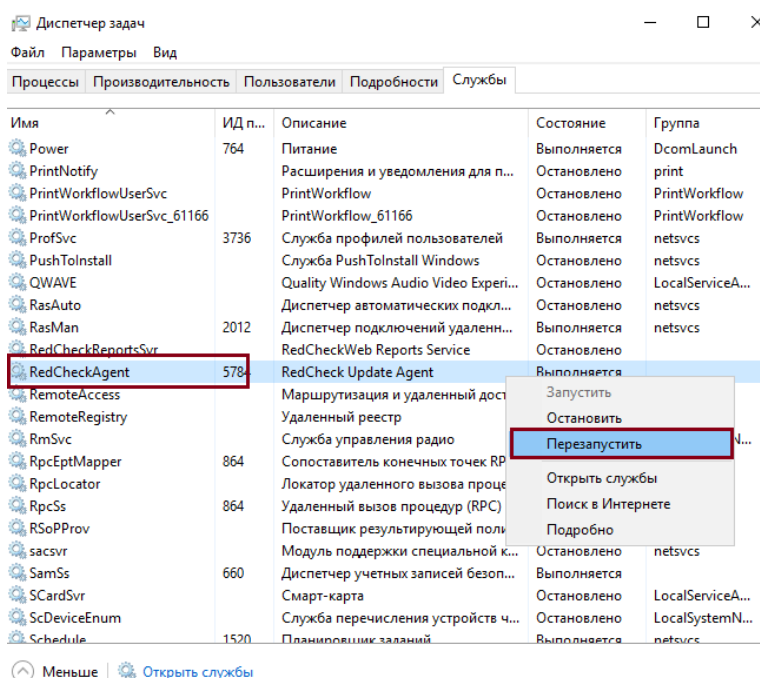
Для x-86 разрядных систем: **HKEY\_LOCAL\_MACHINE\ SOFTWARE\ Wow6432Node\ ALTEX-SOFT\ RedCheckAgent\ Port (DWORD)**  
Для x-64 разрядных систем: **HKEY\_LOCAL\_MACHINE\ SOFTWARE\ ALTEX-SOFT\ RedCheckAgent\ Port (DWORD) D)**



Присвойте ему необходимое значение → **ОК**;



**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;

settings 1 ×

SELECT id, "name", string\_value, bool\_valu | Введите SQL выражение чтобы отфильтровать рез

	123 id	ABC name	ABC string_value	<input checked="" type="checkbox"/> bool_value	123 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	SaveTemplInventoryR	[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**;

Диспетчер задач

Файл Параметры Вид

Процессы Производительность Пользователи Подробности **Службы**

Имя	ИД п...	Описание	Состояние	Группа
Power	764	Питание	Выполняется	DcomLaunch
PrintNotify		Расширения и уведомления для п...	Остановлено	print
PrintWorkflowUserSvc		PrintWorkflow	Остановлено	PrintWorkflow
PrintWorkflowUserSvc_61166		PrintWorkflow_61166	Остановлено	PrintWorkflow
ProfSvc	3736	Служба профилей пользователей	Выполняется	netsvcs
PushToInstall		Служба PushToInstall Windows	Остановлено	netsvcs
QWAVE		Quality Windows Audio Video Experi...	Остановлено	LocalServiceA...
RasAuto		Диспетчер автоматических подкл...	Остановлено	netsvcs
RasMan	2012	Диспетчер подключений удаленн...	Выполняется	netsvcs
RedCheckReportsSvr		RedCheckWeb Reports Service	Остановлено	
<b>RedCheckAgent</b>	<b>578</b>	<b>RedCheck Update Agent</b>	<b>Выполняется</b>	
RemoteAccess		Маршрутизация и удаленный дост	Запустить	
RemoteRegistry		Удаленный реестр	Остановить	
RmSvc		Служба управления радио	<b>Перезапустить</b>	N...
RpcEptMapper	864	Сопоставитель конечных точек RP		
RpcLocator		Локатор удаленного вызова проце	Открыть службы	
RpcSs	864	Удаленный вызов процедур (RPC)	Поиск в Интернете	
RSoPProv		Поставщик результирующей поли	Подробнее	
sacsvr		Модуль поддержки специальной к...	Остановлено	netsvcs
SamSs	660	Диспетчер учетных записей безоп...	Выполняется	
SCardSvr		Смарт-карта	Остановлено	LocalServiceA...
ScDeviceEnum		Служба перечисления устройств ч...	Остановлено	LocalSystemN...
Schedule	1520	Планировщик заданий	Выполняется	netsvcs

Меньше [Открыть службы](#)



## 4.12 Журнал событий (логи)

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 каталогах `/var/opt`

- `/redcheck-api/log` – серверный компонент;
- `/redcheck-scan-service/log` – служба сканирования;
- `/redcheck-sync-service/log` – служба синхронизации;
- `/redcheck-client/log` – консоль управления;
- `C:\ProgramData\ALTEX-SOFT\RedCheck\Logs\Agent` – агент сканирования;

## Расширенные логи

Расширенные логи находятся в каталоге `/var/opt/redcheck-scan-service/jobs/uuid_job/*.xml`

- UID\_Задания: **История** →  → **Свойства** → поле **UID**;
- `uniqueid`: UUID хоста;

## 4.13 Настройка сервиса доставки отчетов

**Шаг 1.** Раскройте **Инструменты** → **Настройки** → перейдите в **Доставка** → в разделе **Настройка сервиса доставки на электронную почту** отметьте **Включить сервис доставки**;

Настройка сервиса доставки на электронную почту

Включить сервис доставки

mail.test-domain.com

8888

SSL/TLS

Check certificate revocation

Использовать аутентификацию

Логин

Пароль

tets@test-domain.ru

UTF8

Задание {JobScanType} ({JobId}) завершено.

Название: {JobName}

Описание: {JobDescription}

Начало сканирования: {JobStartTime}

Хостов в задании: {JobTargetsCount}

Успешно просканированных: {JobSuccessfullyScannedTargetsCount}

#TARGET#

Хост: {TargetName} | Статус: {TargetScanResult}

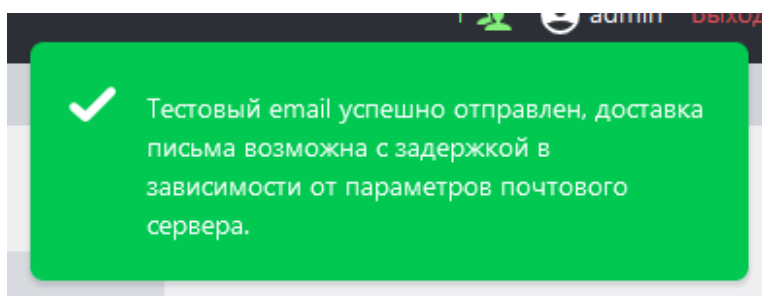
Установить шаблон по умолчанию

some\_email@mail.ru

Отправить тестовое письмо

Сохранить Отмена

**Шаг 2.** Укажите необходимые данные для отправки писем → нажмите **Отправить тестовое письмо** для проверки;



**Шаг 3.** Чтобы добавить email, нажмите **Добавить адрес доставки**;

ALTXMAP

RedCheck может доставлять на сетевые ресурсы или на электронную почту данные о сканирова

**ДОСТАВКА**

Адреса доставки отчетов (сетевые ресурсы и адреса электронной почты)

ID	Тип	Путь/Адрес	Учётная запись
Нет данных д			

20

Добавить адрес доставки ...

**Шаг 4.** Укажите **Тип** адреса доставки **Email** и адрес почты в поле **Путь/Адрес** → **Сохранить**;

**Новый адрес доставки (сетевой каталог или электронная почта)**

Укажите требуемые параметры для нового или редактируемого адреса доставки.

Тип: Email

Путь/Адрес: some\_address@mail.ru

Учётная запись:

Сохранить Отмена

Для отправки отчетов на почту после завершения задания необходимо создать [шаблон отчетов](#).

## 4.14 Исключения для средств защиты (САЗ, СЗИ)

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 директорий и исполняемых файлов, подлежащих добавлению в списки исключений средств защиты, используемых в сети предприятия:

Список директорий установки	Исполняемый файл
<b>Основные компоненты RedCheck</b>	
<b>Серверный компонент (RestAPI):</b> /opt/redcheck-api	/redcheck-api /reports-export/redcheck-reports-export-service
<b>Консоль управления:</b> /opt/redcheck-client	/redcheck-web
<b>Служба сканирования:</b> /opt/redcheck-scan-service /opt/altxmap	/redcheck-scan-service  /nmap /nping
<b>Служба синхронизации:</b> /opt/redcheck-sync-service	/redcheck-sync-service
<b>Дополнительные компоненты (Windows-компоненты)</b>	

<p><b>Сервер обновлений:</b></p> <p>C:\Program Files (x86)\ALTEX-SOFT\RedCheckUpdateServer</p>	<p>\RcUpdSrv.exe</p>
<p><b>Агент сканирования:</b></p> <p>C:\Program Files\ALTEX-SOFT\RedCheckAgent</p> <p>C:\Program Files (x86)\ALTEX-SOFT\RedCheckAgent</p>	<p>\RedCheckAgent.exe</p>

## 5 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 «АЛТЭК-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	<a href="#">Импорт хостов из CSV-файла</a>
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
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
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
PDF	Portable Document Format – межплатформенный открытый формат электронных документов
SCAP	Security Content Automation Protocol – протокол автоматизации управления данными безопасности. Набор открытых стандартов, определяющих технические спецификации для представления и обмена данными безопасности
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
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



XML	eXtensible Markup Language – расширяемый язык разметки
-----	--