

RedCheck

Система анализа
защищенности

общие
технические
сведения

Комплексное решение
для мониторинга защищенности
IT-инфраструктуры предприятия

RedCheck — система анализа защищенности и соответствия стандартам, предоставляющая широкий круг возможностей по управлению информационной безопасностью для предприятий любого масштаба.

3

Система предназначена для получения данных о параметрах ИТ-инфраструктуры, влияющих на защищенность объектов информатизации, а также для поддержки принятия решений по устранению выявленных уязвимостей и созданию эффективных конфигураций безопасности контролируемых систем.

Сканер разработан с учетом реальных потребностей отечественных компаний в области информационной безопасности и требований российских Регуляторов. Применение RedCheck позволяет решать широкий спектр задач: от поиска уязвимостей до оценки соответствия отечественным и международным стандартам безопасности, а также реализовывать ряд мер защиты, обязательных для информационных систем персональных данных (ИСПДн), государственных информационных систем (ГИС), автоматизированных систем управления производственными и технологическими процессами (АСУ ТП), значимых объектов критической информационной инфраструктуры (ЗО КИИ) и автоматизированных систем, обрабатывающих конфиденциальную информацию.

Функциональные возможности



Аудит уязвимостей

Централизованное и локальное сканирование узлов сети на наличие уязвимостей операционных систем, общесистемного и прикладного ПО.



Аудит конфигураций

Контроль конфигураций и оценка соответствия стандартам и политикам безопасности.



Аудит СУБД

Расширенные аудиты СУБД и ее среды функционирования на предмет конфигураций безопасности, уязвимостей, неустановленных обновлений.



Инвентаризация сети

Сбор сведений о составе технических средств и ПО на узлах сети, контроль изменения конфигурации сети.



Аудит безопасности АСУ ТП

Быстрый и достоверный аудит уязвимостей промышленных систем. Поддержка распространённых SCADA-протоколов и специального ПО.



Аудит контейнеров Docker

Полноценный аудит уязвимостей контейнеров и платформы Docker, системы управления контейнерами Kubernetes.



Аудит в режиме «Пентест»

Оценка уровня защищенности информационных систем без привилегий и знаний о сканируемом хосте (метод «Черного ящика»).



Фиксация и контроль целостности

Контроль целостности папок, файлов и веток реестра (для Windows) узлов сети. Различные алгоритмы хэширования, включая ГОСТ.



Аудит платформ виртуализации

Детальный аудит безопасности платформ виртуализации Hyper-V и VMware.



Аудит и установка обновлений

Поиск и установка недостающих обновлений безопасности, сканер интегрирован с Microsoft WSUS.



Аудит серверов приложений

Отдельное направление аудита серверов приложений, web-серверов и их компонентов.



Документирование результатов аудита

Детализированные и интегральные отчеты по каждому направлению аудита.

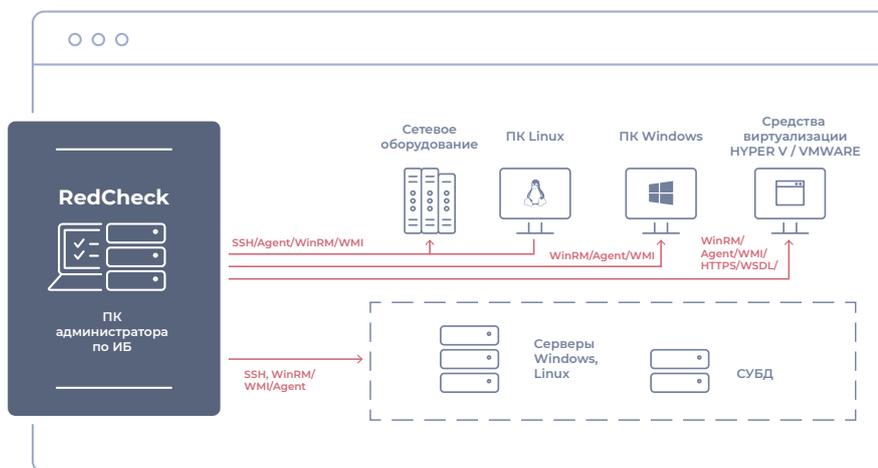
Архитектура

Гибкая архитектура и система лицензирования позволяют разворачивать RedCheck как на отдельном узле, так и в локальной сети, выстраивать распределенные структуры и получать полную картину состояния защищенности всей системы или отдельных ее сегментов. RedCheck не имеет ограничений по масштабированию.

Возможные сценарии применения

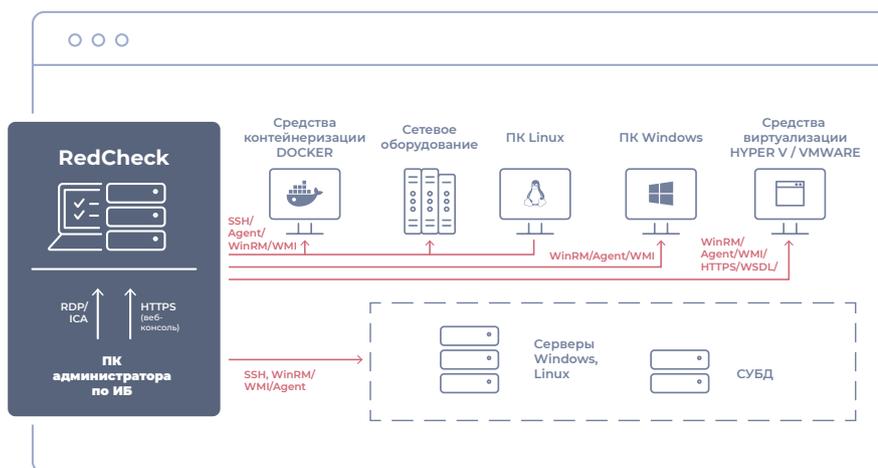
- Контроль защищенности малых и средних сетей (АРМ администратора безопасности)

Для контроля малых и средних сетей (до 200 узлов) RedCheck может быть непосредственно развернут на АРМ администратора (администратора безопасности) без существенной потери производительности компьютера. RedCheck может быть установлен на ноутбук для проведения выездных проверок (аудита).



- Контроль защищенности территориально удаленной сети (установка на выделенный сервер)

Наличие в RedCheck разнообразных транспортов и протоколов управления позволяет осуществлять удаленное сканирование сети любого масштаба по всем направлениям аудита без существенной нагрузки на каналы связи. Для повышения скорости сканирования Windows-систем и оптимизации сетевого трафика рекомендуется использование агента программы RedCheck Agent или Remote Engine (WinRM).



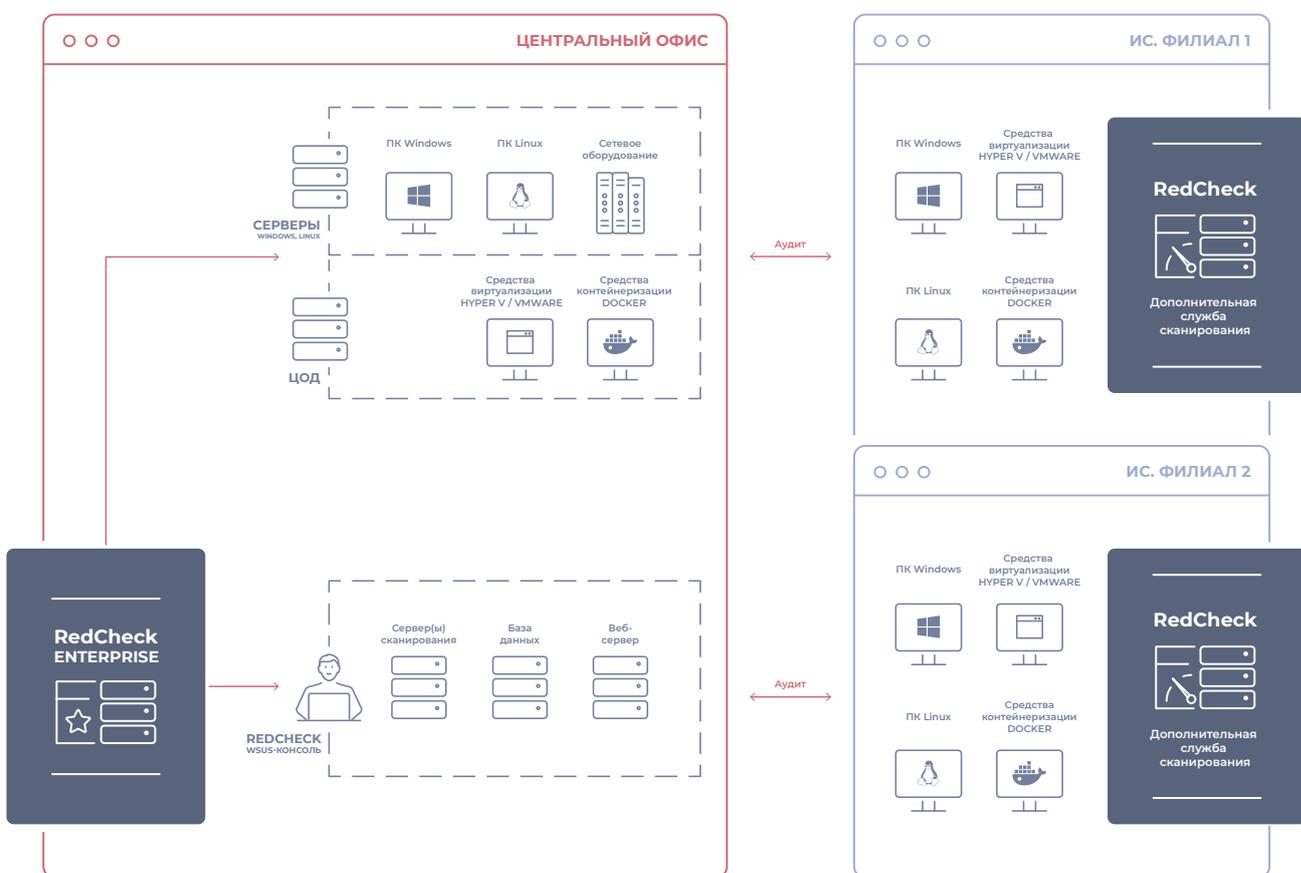
- **Контроль (анализ) защищенности крупных сетей и сетей с филиальной структурой**

Для работы в крупных и распределенных корпоративных структурах оптимальным решением является использование веб-версии RedCheck включающей сервер управления REST, веб-консоль и серверы сканирования, развернутые в головном офисе или ЦОД компании.

Для пользователей системы реализована ролевая модель доступа, со сканером одновременно может работать несколько специалистов в соответствии с их сферой ответственности.

В целях масштабирования могут устанавливаться дополнительные модули (серверы), поддерживающие многопоточное сканирование.

Для установки недостающих обновлений, выявленных в процессе аудитов, может применяться интегрированная со сканером надстройка на сервер обновлений Microsoft WSUS. Для работы в изолированных сетях без доступа к Интернету используется специальный сервер обновлений, позволяющий работать со средствами одноплатной передачи данных.



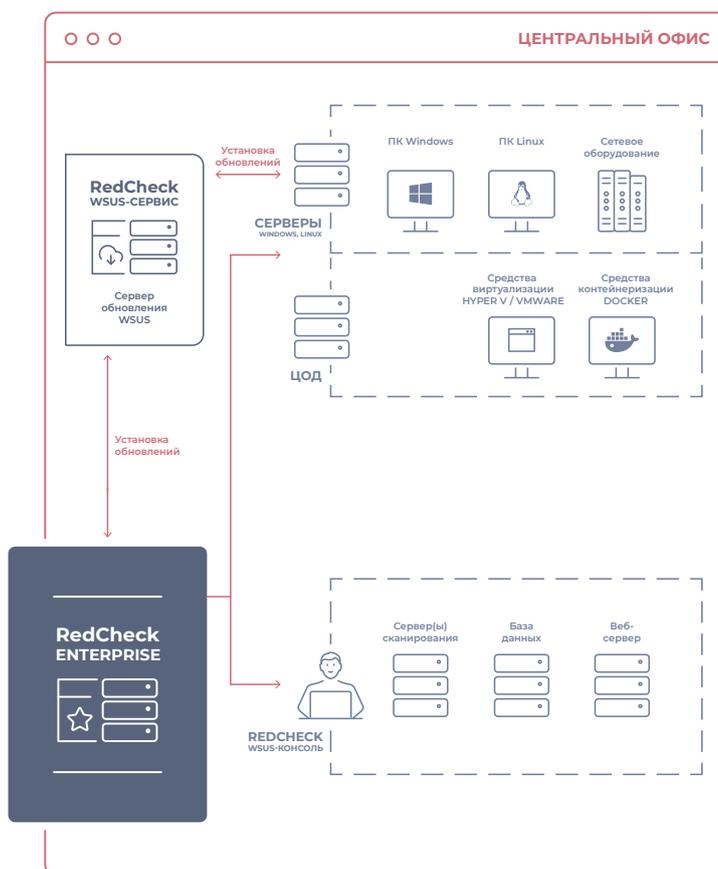
RedCheck Enterprise

Для больших информационных систем (более 2500 узлов) рекомендуется использование RedCheck в редакции Enterprise. Enterprise включает в себя все функциональные возможности программы, не имеет лицензионных ограничений по количеству сканируемых узлов и ориентирована на крупные и распределенные информационные системы с возможностью неограниченного масштабирования.

Для масштабирования системы предусмотрено использование дополнительных модулей (серверов) сканирования. Для повышения производительности дополнительный модуль может устанавливаться на отдельный сервер или на тот же, где развернут RedCheck.

Для работы на небольших территориально удаленных объектах достаточно установки одного дополнительного модуля, подключенного к основному экземпляру RedCheck Enterprise, развернутому в центральном офисе или в одном из филиалов. Данные о результатах проверки сохраняются в единой БД, не создавая ощутимой нагрузки на каналы связи.

Enterprise включает в себя максимум функциональных возможностей программы, не имеет лицензионных ограничений по количеству сканируемых узлов



При сканировании Windows-систем для сокращения нагрузки на сеть и снижения требований к привилегиям доступа рекомендуется использование агента RedCheck. Использование агента не требует отдельного лицензирования, агенты могут использоваться совместно с транспортом WMI, WinRM, SSH.

В общем случае максимальный состав системы RedCheck Enterprise может включать следующие структурные **компоненты:**

- Сервер RedCheck Enterprise
- Сервер управления RedCheck REST
- Консоль управления (Web-консоль)
- Дополнительные модули сканирования
- Сервер обновлений Update Server RedCheck
- Модуль синхронизации с AD
- Консоль управления MS WSUS
- Агенты установки обновлений
- Агенты сканирования Windows

Интеграция

С системами управления событиями информационной безопасности (SIEM)

RedCheck обладает универсальными инструментами интеграции и может быть источником информации для SIEM и IRP, в частности HP ArcSight, Splunk, R-Vision, NEURODAT, eplat4m Security GRC. Использование типовых интерфейсов передачи данных для данного вида систем, позволяет без особых проблем подключать и иные системы обработки и анализа машинно-генерируемых данных.

Интеграция осуществляется через модуль API (REST-HTTP) или путем получения данных напрямую из базы данных RedCheck. Все данные структурированы, хранятся и передаются в формате XML.

Заложенные технические возможности позволяют не только передавать во внешние системы полученные результаты проверок (типовая возможность большинства конкурентных продуктов), но и осуществлять управление RedCheck из внешних систем, в том числе создавать и запускать задания, формировать отчеты, дополнять базу сигнатур собственными определениями, представленными в стандартизованном формате OVAL/XCCDF.

Поддержка платформ

Система обеспечивает анализ защищенности следующих программных и программно-аппаратных средств:

- **клиентские операционные системы:**
Microsoft Windows XP/Vista/7/8/8.1/11;
- **серверные операционные системы Microsoft Windows Server:**
2008/2008R2/2012/2012R2/2016/2019/2022;
- **операционные системы Linux:**
CentOS, Debian, Oracle Linux, openSUSE, Red Hat, SUSE, Ubuntu, Astra Linux, ALT Linux, POCA и др.;
- **платформа** контейнеризации Docker **и система** оркестрации Kubernetes;
- **СУБД:** Microsoft SQL Server 2005-2019, Oracle Database Server 11/12, PostgreSQL, IBM DB2, MySQL;
- **платформы виртуализации:**
VMware, Microsoft Hyper-V;
- **сетевое оборудование** Cisco, Huawei, Fortinet, Check Point и др.;
- **офисные пакеты** Microsoft Office 2003-2019, LibreOffice, Adobe;
- **веб-серверы и приложения:**
Apache, nginx, IIS, Apache Tomcat, .NET Framework;
- **SCADA:** ArcestrA Logger, BACnet/IP, Citect SCADA, Ethernet/IP, GenBroker (GENESIS32/64), Modbus TCP/UDP, Profinet IO, Schneider Electric IGSS, Sicam PAS IPC, Simatic ALM, Simatic S7 и др.

А также более **700**
различный **приложений**

Основные преимущества



Встроенные полнофункциональные интерпретаторы OVAL и XCCDF позволяют осуществлять полный спектр проверок на базе собственного репозитория OVALdb, а также использовать унифицированный SCAP-контент других вендоров.



Программа имеет понятный графический интерфейс, не предъявляет высоких требований к подготовке пользователя при установке и использовании.



Реализация планировщика заданий и гибкая система профилей делает удобным применение программы при повседневном контроле за безопасностью корпоративной сети.



Неограниченная масштабируемость, развернутая ролевая модель и многопользовательский режим позволяют использовать RedCheck в SOC и других центрах кибербезопасности.



Для работы не требуется больших аппаратных мощностей, RedCheck может быть установлен на любой клиентской или серверной операционной системе Microsoft.



Доступна интеграция с Active Directory, что обеспечивает удобный и гибкий процесс разворачивания и поддержания в актуальном состоянии базы идентификационных данных сканируемых хостов.



Эффективная комбинация агентной и безагентной технологии сканирования, позволяет существенно сократить время проверок и обеспечить требуемый уровень безопасности.



Открытое описание определений безопасности (уязвимостей, обновлений, конфигураций) позволяет глубоко анализировать результаты контроля, определять причины и способы выявления уязвимостей.



RedCheck — первый отечественный сканер, позволяющий осуществлять широкий спектр аудитов платформы контейнеризации Docker.

Ключевой особенностью сканера RedCheck является его работа с унифицированным SCAP-контентом, получаемым из собственной базы уязвимостей OVALdb.

Собственная база уязвимостей

Ключевой особенностью сканера RedCheck является его работа с унифицированным SCAP-контентом, получаемым из собственной базы уязвимостей OVALdb. Репозиторий OVALdb — один из крупнейших международных банков данных в области ИБ, позволяющий формировать оценку защищенности информационных систем на основе публикуемых в нем определений уязвимостей, параметров конфигураций, инвентаризационных данных и другого смежного контента.

Информация в репозитории OVALdb представлена на основе языков и классификаторов, входящих в набор открытых стандартов SCAP (Security Content Automation Protocol). Определения уязвимостей разработаны на языке OVAL (Open Vulnerability and Assessment Language). Содержание OVALdb синхронизировано с репозиториями международных экспертных организаций, таких как CIS, MITRE, NIST и другими источниками, включая БДУ ФСТЭК России и НКЦКИ. Публикации новых определений производятся на регулярной основе и проходят тщательную проверку.

Постоянными подписчиками OVALdb являются также команды разработчиков СЗИ из России, Индии, Израиля и Евросоюза.



На 1 октября 2021 года репозиторий содержит **225 000 определений** в формате OVAL, из них:

53 000	уникальных CVE (Common Vulnerabilities and Exposures)	90 000	уязвимостей для платформ Linux
38 000	уязвимостей на семейство ОС Windows	65 000	определений, коррелированных с БДУ БИ ФСТЭК России и НКЦКИ.

Сертифицированная версия

RedCheck внесен в Единый реестр российских программ для электронных вычислительных машин и баз данных.

Сканер безопасности RedCheck имеет действующий сертификат ФСТЭК России, который подтверждает соответствие РД «Требования доверия» по 4 Уровню доверия. RedCheck может использоваться в составе АС до класса защищенности 1Г, а также ИСПДн, ГИС и АСУ ТП КВО до 1 класса (уровня) защищенности включительно.

RedCheck может использоваться:

для реализации мер защиты согласно приказам ФСТЭК России № 17, 21, 31

для реализации мер по обеспечению безопасности КИИ согласно приказу ФСТЭК России №239

- | | |
|--|---|
| <ul style="list-style-type: none"> • Контроль за установкой компонентов программного обеспечения ОПС.2 • Выявление, анализ уязвимостей информационной системы АНЗ.1 • Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации АНЗ.2 • Контроль работоспособности параметров настройки и правильности функционирования программного обеспечения и средств защиты информации АНЗ.3 • Контроль состава технических средств, программного обеспечения средств защиты информации АНЗ.4 • Контроль состава технических средств, программного обеспечения, включая программное обеспечение средств защиты информации ОЦЛ.1 • Контроль целостности виртуальной инфраструктуры и ее конфигураций ЗСВ.7 | <ul style="list-style-type: none"> • Инвентаризация информационных ресурсов (АУД.1). • Анализ уязвимостей и их устранение (АУД.2). • Регистрация событий безопасности (АУД.4). • Мониторинг безопасности (АУД.7). • Проведение внутренних аудитов (АУД.10). • Проведение внешних аудитов (АУД.11). • Контроль целостности программного обеспечения (ОЦЛ.1) • Контроль целостности информации (ОЦЛ.2) • Идентификация объектов управления конфигурацией (УКФ.1). • Поиск, получение обновлений программного обеспечения от доверенного источника (ОПО.1). • Контроль целостности обновлений программного обеспечения (ОПО.2). • Установка обновлений программного обеспечения (ОПО.4). |
|--|---|

Лицензирование

RedCheck лицензируется по количеству сканируемых (проверяемых) IP-адресов одной программой или по количеству инсталляций экземпляров программ. Для корпоративного использования предусмотрено четыре редакции RedCheck, отличающиеся следующими функциональными возможностями:

-
- **RedCheck Base**

Младшая редакция продукта, включающая необходимые инструменты для полноценного аудита уязвимостей и обновлений Windows и Linux систем. Позволяет осуществлять контроль целостности, инвентаризацию, сетевые проверки и другие процедуры, необходимые при повседневном контроле защищенности информационных систем.

 - **RedCheck Professional**

Полнофункциональная редакция, включающая широкий арсенал инструментов для мониторинга и управления защищенностью сетей корпоративного уровня. Лицензируется по количеству сканируемых IP-адресов (DNS-имен).

 - **RedCheck Professional**

Для сертифицированных версий Microsoft

По своим возможностям программа аналогична редакции RedCheck Professional при этом дополнена возможностью управлять конфигурациями и установкой обновлений для сертифицированных по требованиям безопасности версий Microsoft. Редакция поставляется пользователям сертифицированного программного обеспечения Microsoft.

 - **RedCheck Enterprise**

Редакция включает все имеющиеся функциональные возможности программы и ориентирована на крупные и распределенные информационные системы с возможностью неограниченного масштабирования. Лицензируется по количеству инсталляций, не имеет ограничений на количество сканируемых IP-адресов. Для масштабирования возможно подключение дополнительных модулей сканирования (ScanModul RedCheck). В состав лицензии включена расширенная техническая поддержка.

 - **RedCheck SCADA**

Отдельно лицензируемый SCADA-модуль для сканирования уязвимостей элементов АСУ ТП (Iconics, Rockwell Automation, Schneider Electric, Siemens, Simatic и др.).
-

Срок действия продуктовой лицензии

По умолчанию срок действия продуктовой лицензии составляет 1 год, возможно приобретение ПО RedCheck сразу на 2 или 3 года. В период действия лицензии пользователю RedCheck предоставляется техническая поддержка, доступ к актуальному контенту безопасности и обновлениям программ для данной версии.

Системные требования

- Типовые требования к аппаратному обеспечению

РЕДАКЦИЯ / КОМПОНЕНТА	СУБД	УЗЛОВ НЕ БОЛЕЕ	АППАРАТНЫЕ КОМПОНЕНТЫ ¹	ЧАСТОТА СКАНИРОВАНИЯ		
				1 раз в неделю	1 раз в месяц	1 раз в квартал
RedCheck Base/Pro/PostgreSQL	MS SQL Express установлен на одном ПК с RedCheck	200	CPU	Intel Core i5-7400 (4 ядра) и выше		
			RAM	8 ГБ		
			HDD ²	12 ГБ (10ГБ ограничение MS SQL Express)		
RedCheck Base/Pro	—	200 и более	CPU	Intel Xeon (не менее 2 физических ядер)		
			RAM	6ГБ		
			HDD	2 ГБ		
	PostgreSQL/MS SQL Server (для выделенного сервера)	200	HDD ²	21,8 Г Б	5,8 Г Б	2,6 Г Б
		500	HDD ²	53 Г Б	13 Г Б	5 Г Б
		2000				
RedCheck Enterprise	—	—	CPU	Intel Xeon (не менее 4 физических ядер)		
			RAM	6ГБ		
			HDD ¹	2 ГБ		
	PostgreSQL/MS SQL Server (для выделенного сервера)	—	SSD ³	400 Г Б	100 Г Б	35 Г Б
Дополнительный модуль сканирования (ScanModul RedCheck)	—	—	CPU	Intel Xeon (не менее 2 физических ядер)		
			RAM	6 ГБ		
			HDD ¹	1 ГБ		
Локальный сервер обновлений (Update Server RedCheck)	—	—	CPU	Intel Xeon (не менее 2 физических ядер)		
			RAM	6ГБ		
			HDD ¹	2 ГБ		
Агенты сканирования Windows-систем (Agent RedCheck) и установки обновлений (Agent Update RedCheck)	—	—	CPU	Intel Pentium/AMD Phenom и выше		
			RAM	2ГБ		
			HDD ¹	10 МБ		

- Средняя нагрузка на сеть при сканировании одного узла

	СПОСОБЫ / ТРАНСПОРТЫ СКАНИРОВАНИЯ			
	Агент	Remote Engine (WinRM)	WMI	SSH
Скорость передачи данных, Кбит/с	121	637	10 200	160
Суммарный объем трафика на узел, КБ	8 000	16 800	434 000	5 000
Среднее время сканирования ¹ , мин	2,40	2,20	15,00	2,20

- Требования к программному обеспечению

ОПЕРАЦИОННАЯ СИСТЕМА	Microsoft Windows 7-10, Microsoft Windows Server 2008-2019. СУБД SQL Server 2012 (редакции Express, Standard, Enterprise) и выше, PostgreSQL 11 и выше.
ДОПОЛНИТЕЛЬНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ	Microsoft .NET Framework full версии 4.7 или выше.

- 1 В таблице не указаны требования к аппаратной части операционной системы, на которой развернут RedCheck и СУБД. Параметры аппаратной платформы для операционной системы и MS SQL должны соответствовать требованиям Microsoft.
- 2 Расчет требуемого места на HDD приведен из условия хранения данных о результатах проверок — 1 год.
- 3 Для редакций Enterprise рекомендуется СУБД располагать на SSD диске для обеспечения быстродействия и уменьшения временных интервалов выполняемых операций с базой данных. Использование SSD диска должно применяться совместно с выполнением работ по оптимизации и тонкой настройке работы СУБД.
- 4 Показатели приведены для режима «Аудит уязвимости, полное сканирование», данный режим является наиболее ресурсоемким.



АО «АЛТЭКС-СОФТ»

141067, Московская область,
город Королев, микрорайон
Болшево, улица Маяковского,
дом 10А.

+7 (495) 543 31 01
info@altx-soft.ru

altx-soft.ru
redcheck.ru