REDCheck

Система анализа защищенности

общие технические сведения

RED Check

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.

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.

RedCheck разработан с учетом реальных потребностей отечественных компаний в области информационной безопасности и требований российских Регуляторов. Его применение 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

Обнаружение хостов

Поиск активных хостов и контроль целостности сети по заданному пулу сетевых адресов.

Аудит в режиме «Пентест»

Сетевое сканирование без привилегий в режиме «Черного ящика».

Аудит уязвимостей

Сетевое или локальное сканирование хостов на наличие уязвимостей ОС, общесистемного и прикладного ПО, сетевого оборудования.

Аудит обновлений

Поиск и обнаружение неустановленных обновлений безопасности на узлах сети.

Аудит конфигураций

Контроль параметров безопасности и оценка соответствия стандартам, политикам безопасности, рекомендациям вендоров.

Инвентаризация

Анализ и контроль изменений в составе программного и аппаратного обеспечения сети.

Фиксация (контроль целостности)

Сбор контрольных сумм конфигурационных файлов, папок, веток реестра и предупреждение об их изменении при сравнении с эталонными значениями.

Аудит СУБД

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

Аудит систем контейнеризации

Проверка безопасности для образов, реализованных на базе плафторм контейнеризации, а также систем оркестрации и масштабирования.

Аудит уязвимостей АСУ ТП

Сканирование на наличие уязвимостей протоколов АСУ ТП путем сопоставления сигнатур, хранящихся в БД RedCheck.

Проверка доступности

Анализ доступности добавленных хостов для любых системных режимов сканирования с привилегиями.

Документирование результатов аудита

Формирование отчетов в формате HTML, PDF, CSV или XML. Доставка отчетов по электронной почте или в сетевой каталог.

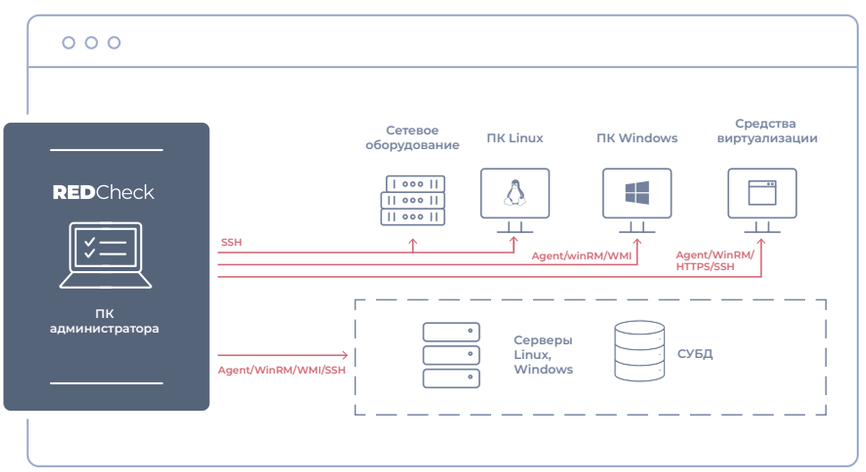
Архитектура

Гибкая архитектура и система лицензирования позволяют разворачивать RedCheck на отдельном узле, в локальной сети или в облаке, выстраивать распределенные структуры. RedCheck не имеет ограничений по масштабированию.

Сценарии применения

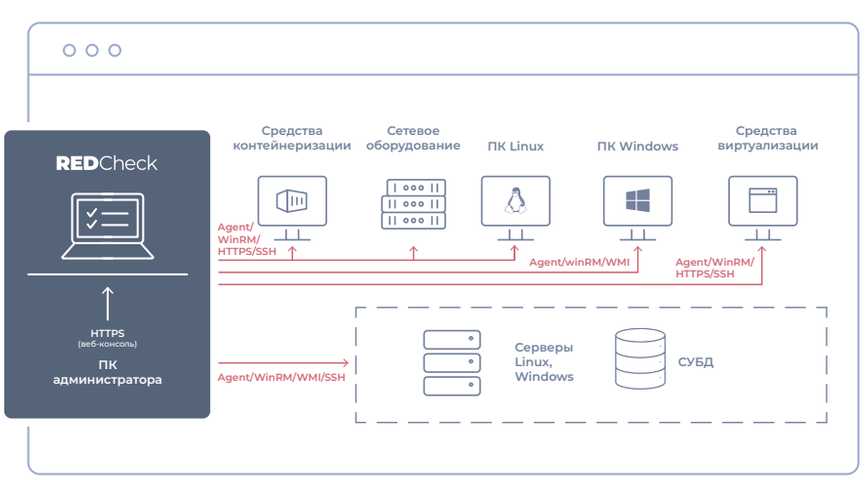
- Контроль защищенности малых и средних сетей

Для контроля малых и средних сетей RedCheck может быть развернут на АРМ администратора (ИБ) без существенной потери производительности компьютера. RedCheck может быть установлен на ноутбук для проведения выездных проверок.



- Контроль защищенности территориально удаленной сети

Наличие веб-консоли в RedCheck позволяет осуществлять удаленное управление и сканирование сети любого масштаба по всем типам аудитов без существенной нагрузки на каналы связи. Для повышения скорости сканирования Windows-систем и оптимизации сетевого трафика рекомендуется использование транспортов RedCheck Agent или WinRM.



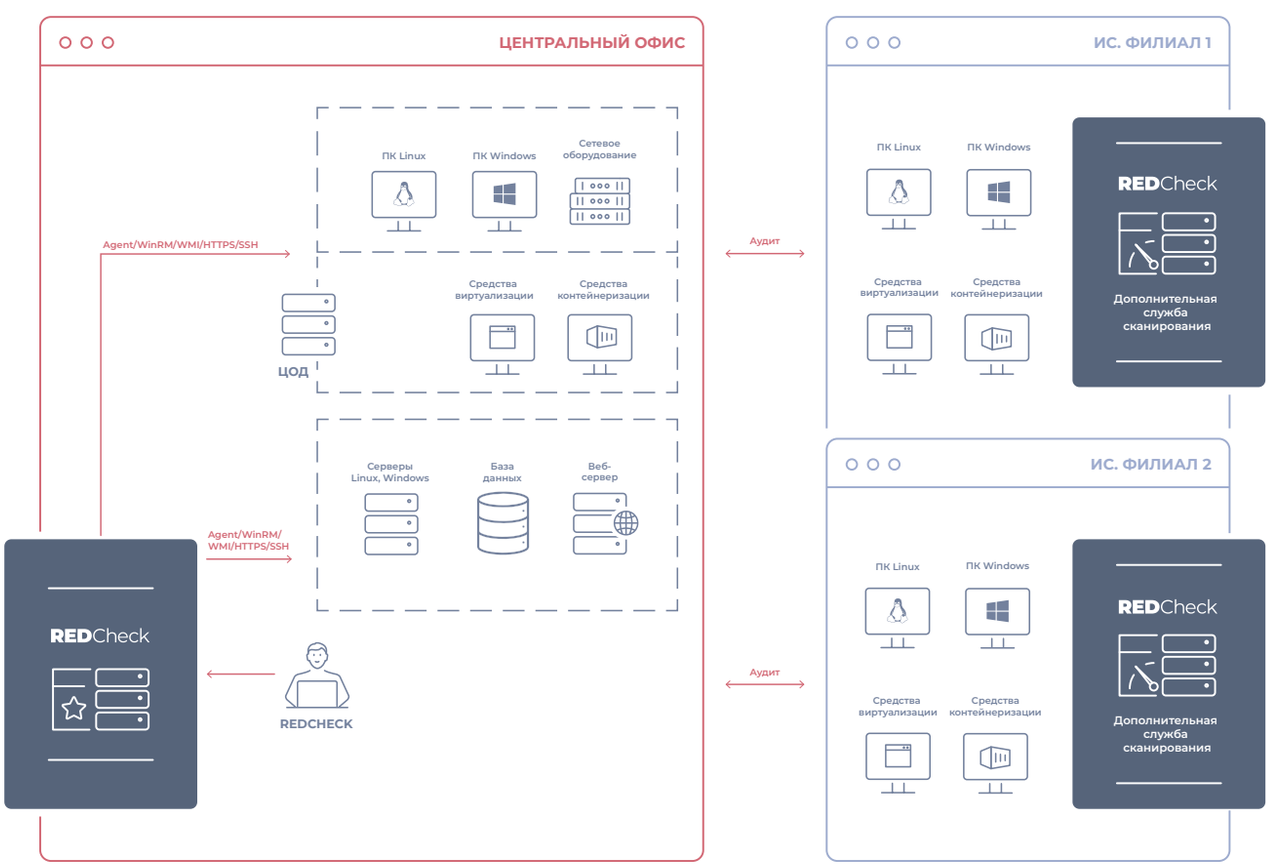
- Контроль (анализ) защищенности больших сетей с филиальной структурой

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

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

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

Для работы в изолированных сетях без доступа к Интернету используется специальный сервер обновлений, позволяющий работать со средствами однонаправленной передачи данных.



RedCheck Enterprise

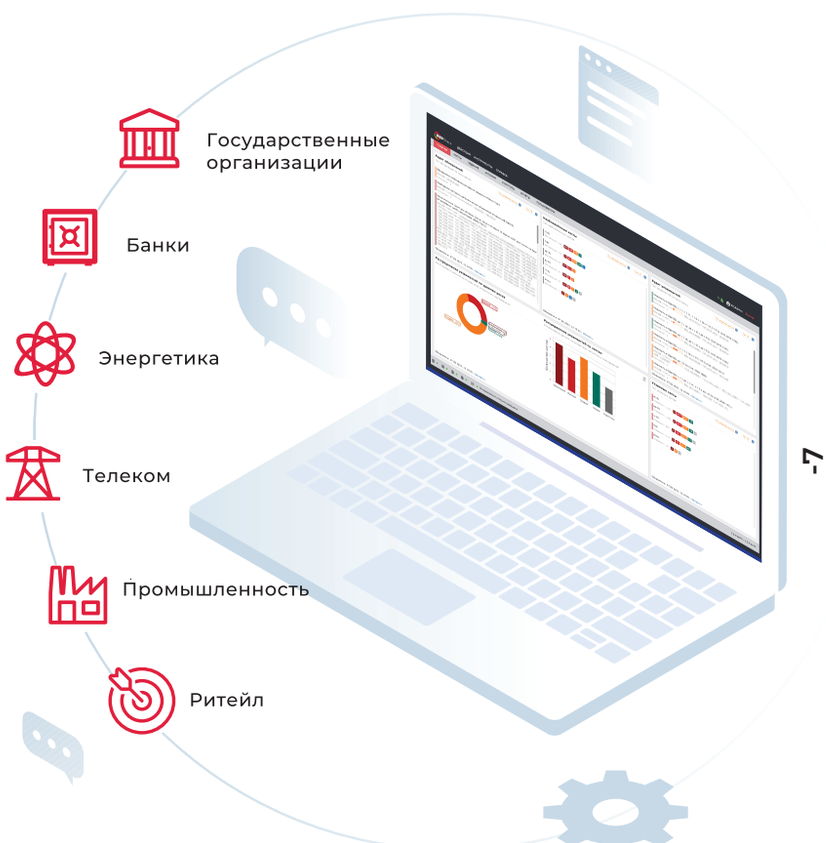
Для больших и распределенных информационных систем рекомендуется использование RedCheck в редакции Enterprise.

Данная редакция включает в себя все функциональные возможности, не имеет лицензионных ограничений по количеству сканируемых хостов.

Для масштабирования системы предусмотрено использование дополнительных модулей сканирования. Дополнительный модуль устанавливается на отдельный сервер.

Для работы на удаленных объектах могут использоваться один или несколько дополнительных модулей сканирования. Управление дополнительными модулями сканирования осуществляется с основного сервера RedCheck. Данные о результатах сканирований сохраняются в единой БД, не создавая нагрузки на каналы связи.

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



При сканировании Windows-систем для сокращения нагрузки на сеть и снижения требований к привилегиям доступа рекомендуется использование агента RedCheck. Использование агента не требует дополнительного лицензирования. RedCheck агент использует собственный транспорт для сканирования.

RedCheck содержит структурные компоненты:

- Сервер RedCheck Desktop
- Сервер управления RedCheck REST API
- Web-консоль управления
- Служба синхронизации
- Служба сканирования
- Дополнительные модули сканирования
- Сервер обновлений RedCheck
- Утилита синхронизации с AD
- Агенты сканирования Windows

Интеграция

С внешними аналитическими системами управления информационной безопасностью

RedCheck обладает универсальными инструментами интеграции и может быть источником информации для систем управления ИБ, например: Kaspersky, R-Vision, Security Vision. Использование типовых интерфейсов передачи данных для данного вида систем позволяет без особых проблем подключать и иные системы обработки и анализа машинно-генерируемых данных методом REST API.

Интеграция осуществляется через сервер управления REST API или путем машинного распознавания технических отчетов RedCheck в формате CSV или XML.

Сервер управления RedCheck REST API позволяет не только получать результаты сканирования, 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

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

- **Отечественные ОС:** ALT Linux, Astra Linux, RED OS, ROSA
- **Операционные системы Linux:** Amazon Linux, CentOS Linux, CentOS Stream, Debian, Fedora, FreeBSD, Linux Mint, Mageia, openSUSE, openSUSE Evergreen, openSUSE Leap, Oracle Solaris, Oracle Linux, Red Hat Enterprise Linux, Solaris, SUSE CaaS Platform, SUSE Linux Enterprise, Ubuntu
- **Операционные системы Microsoft Windows** XP, Vista, 7, 8, 8.1, 10, 11
- **Серверные операционные системы Microsoft Windows Server:** Server 2003 / 2008 / 2008 R2 / 2012 / 2012 R2 / 2016 / 2019 / 2022
- **Платформа** контейнеризации Docker **и система** оркестрации Kubernetes;
- **Сетевое оборудование:** Check Point GAiA, Cisco IOS, Cisco NX-OS, FortiGate, Huawei VRP, UserGate
- **Платформы виртуализации:** Брест, KVM, Microsoft, Hyper-V, VMware ESXi Server, VMware vCenter Server, VMware NSX, Xen
- **СУБД:** IBM Db2, Microsoft SQL Server, MySQL Server, Oracle Database Server, PostgreSQL, PostgreSQL Pro, SAP HANA
- **АСУ ТП:** Citect SCADA, Codesys V2, Codesys V3, Iconics GENESIS, IGSS, ISAGRAF, Siemens, VMware ESXi Server, Vmware NSX, VMware vCenter Server, Wonderware InTouch
- **ПЛК:** Advantech, Omron, Rockwell Automation, Siemens, Schneider Electric, Yokogawa FCN

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 позволяет 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 Linux или Windows.

Доступна интеграция с Active Directory, которая обеспечивает удобный и гибкий процесс импорта и актуализации сканируемых хостов в RedCheck.

Эффективная комбинация агентной и безагентной технологии сканирования, а также аудит в режиме «Пентест» позволяют 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 российский сканер безопасности, позволяющий осуществлять аудит платформ контейнеризации.

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

Собственная база уязвимостей OVALdb

Ключевой особенностью системы анализа защищенности RedCheck является его работа с унифицированным SCAP-контентом, получаемым из собственной базы уязвимостей OVALdb. Репозиторий OVALdb — крупнейший российский банк данных угроз в области ИБ, позволяющий формировать оценку защищенности информационных систем на основе открыто 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 экспертными ресурсами, такими как БДУ ФСТЭК России, НКЦКИ, бюллетени производителей и ряд других международных экспертных справочников. Публикации новых определений производятся на регулярной основе и проходят тщательную проверку.

Команды разработчиков СЗИ из России и других стран являются постоянными подписчиками OVALdb. Подписка на технические определения сигнатур OVALdb распространяется на индивидуальных условиях лицензионного договора.

OVALdb

На 1 сентября 2023 года репозиторий содержит **303 542 определения** в формате OVAL, из них:

69 709 **уникальных CVE** (Common Vulnerabilities and Exposures)

52 820 **уязвимостей** на семейство ОС Windows

136 671 **уязвимостей** для платформ Linux

114 244 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

- Контроль за установкой компонентов программного обеспечения ОПС.2
- Выявление, анализ уязвимостей информационной системы АН3.1
- Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации АН3.2
- Контроль работоспособности параметров настройки и правильности функционирования программного обеспечения и средств защиты информации АН3.3
- Контроль состава технических средств, программного обеспечения средств защиты информации АН3.4
- Контроль состава технических средств, программного обеспечения, включая программное обеспечение средств защиты информации ОЦЛ.1
- Контроль целостности виртуальной инфраструктуры и ее конфигураций ЗСВ.7

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

- 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

Base

Базовая редакция включает стандартный набор функций RedCheck, необходимых для проверки уязвимостей и обновлений на ОС Windows и Linux, а также «Аудит в режиме Пентест».

Professional

Профессиональная редакция, с полным набором аудитов всех поддерживаемых платформ. Доступны Аудит в режиме «Пентест», системный поиск уязвимостей ОС, проверка обновлений и соответствие конфигурациям безопасности.

Expert

Редакция содержит все функции и сканируемые платформы, а также позволяет проводить комплексный аудит безопасности образов на базе платформы контейнеризации Docker и системы оркестрации Kubernetes.

Enterprise

Корпоративная редакция для крупных или распределенных структур. Содержит все функции по сканированию и анализу, включая аудит образов систем контейнеризации. Не имеет ограничений по количеству сканируемых объектов.

Дополнительные лицензируемые модули

Сервер обновлений — выделенный промежуточный сервер загрузки обновлений контента безопасности для размещения в сетях DMZ. Может обслуживать несколько экземпляров RedCheck любых редакций.

Модуль АСУ ТП — дополнительный пакет, включающий возможность сканирования протоколов и контроллеров АСУ ТП, применяется к редакциям Professional, Expert, Enterprise.

Модуль сканирования — служба сканирования для установки на дополнительный сервер. Может использоваться к редакции Enterprise и решает задачи по распределению нагрузки сканирования между сегментами сети или платформами, увеличивает производительность.

Срок действия лицензии

Лицензия RedCheck является срочной и оформляется от 1 года. В период действия лицензии предоставляется техническая поддержка, доступ к актуальному контенту безопасности и обновлении версии.

Системные требования

• Типовые требования к аппаратному обеспечению

КОМПОНЕНТЫ	ПЛАТФОРМА	АППАРАТНЫЕ ТРЕБОВАНИЯ[1]
DESKTOP ВЕРСИЯ		
RedCheck	ПЭВМ	ПЭВМ ЦП не ниже Intel Core i5, частота не ниже 3,00 ГГц ОЗУ не менее 8 ГБ ПЗУ не менее 12 ГБ
WEB-ВЕРСИЯ (ОБЯЗАТЕЛЬНЫЕ К УСТАНОВКЕ КОМПОНЕНТЫ СИСТЕМЫ)		
Совместная установка		
Серверный компонент Консоль управления Служба сканирования Служба синхронизации	Серверная	ЦП Xeon, частота не ниже 1,86 ГГц, не менее 4 ядер ОЗУ не менее 12 ГБ ПЗУ не менее 2 ГБ
Раздельная установка		
Серверный компонент Консоль управления	Серверная	ЦП Xeon, частота не ниже 1,86 ГГц, не менее 2 ядер ОЗУ не менее 6 ГБ ПЗУ не менее 1 ГБ
Служба сканирования	Серверная	ЦП Xeon, частота не ниже 1,86 ГГц, не менее 2 ядер ОЗУ не менее 6 ГБ ПЗУ не менее 1 ГБ
Служба синхронизации	Серверная	ЦП Xeon, частота не ниже 1,86 ГГц, не менее 2 ядер ОЗУ не менее 4 ГБ ПЗУ не менее 1 ГБ
Сервер СУБД[2]	Серверная	ЦП Xeon, частота не ниже 1,86 ГГц, не менее 2 ядер ОЗУ не менее 6 ГБ ПЗУ не менее 100 ГБ
ДОПОЛНИТЕЛЬНЫЕ КОМПОНЕНТЫ		
Дополнительный модуль сканирования	Серверная	ЦП Xeon, частота не ниже 1,86 ГГц, не менее 2 ядер ОЗУ не менее 6 ГБ ПЗУ не менее 1 ГБ
RedCheck Agent	ПЭВМ, Серверная	ЦП не ниже Intel Pentium/ AMD Phenom, частота не ниже 2,00 ГГц ОЗУ не менее 2 ГБ ПЗУ не менее 500 МБ
RedCheck Update Agent	ПЭВМ, Серверная	ЦП не ниже Intel Pentium/ AMD Phenom, частота не ниже 2,00 ГГц ОЗУ не менее 2 ГБ ПЗУ не менее 500 МБ
RedCheck Update Server (офлайн-синхронизация)	Серверная	ЦП Xeon, частота не ниже 1,86 ГГц, не менее 2 ядер ОЗУ не менее 6 ГБ ПЗУ не менее 5 ГБ

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

• Средняя нагрузка на сеть при сканировании одного

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

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

• Требования к программному обеспечению

ОПЕРАЦИОННАЯ СИСТЕМА	Microsoft Windows 10 и выше, Microsoft Windows Server 2012R2 и выше. СУБД SQL Server 2014 (редакции Express, Standard, Enterprise) и выше, PostgreSQL 12.8 и выше. Jatoba 4.5.1. Браузеры Google Chrome или Edge, Web-сервер IIS, Microsoft .NET Framework 4.8 и выше, Microsoft Visual C++ 2013, 2015 Redistributable, Microsoft ASP.NET Core Runtime.

1 Расчет требуемого места на HDD приведен из условия хранения данных о результатах проверок — 1 год.

2 В случае размещения сервера СУБД совместно с компонентами RedCheck аппаратные требования складываются.

АО «АЛТЭКС-СОФТ»

141090, Московская область,
город Королев, микрорайон
Болшево, улица Маяковского,
дом 10А.

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

altx-soft.ru
redcheck.ru