RedCheck

СРЕДСТВО АНАЛИЗА ЗАЩИЩЕННОСТИ

Руководство администратора

АЛМЮ.501410.RC02-01.РА

Часть 1. Руководство по основным компонентам программы

Версия документа 2.6.5.ru

Содержание

Аннотация

Настоящий документ является Руководство администратора Программного средства анализа защищенности - **RedCheck** (далее - Программа). Документ содержит рекомендации по установке и первичным настройкам программы, а также о возможностях и функциях программы, условиях и порядке применения.

Условные обозначения

Важная и дополнительная информация оформлена в виде примечаний. Степень важности обнаруживает пиктограммы на полях.

 ***- важная информация, которую необходимо принять во внимание!***

Введение

Глобальное проникновение информационных технологий во все сферы жизни сделало наш мир хрупким и уязвимым. Тысячи километров, отделяющие нас от международных террористов, спецслужб недружественных государств или криминальных группировок, не могут гарантировать нам безопасность. Сегодня как никогда важно сохранять бдительность, иметь возможность управлять рисками, уязвимостями и ресурсами информационных систем. Какова бы ни была квалификация сотрудников безопасности, они уже не способны самостоятельно противостоять многообразию современных информационных угроз. Средства анализа защищенности стали основным инструментом диагностики и мониторинга информационных систем обнаружения возможных проблем безопасности, кроме того, они позволяют оперативно оценивать и устранять уязвимости.

RedCheck - профессиональное средство анализа защищенности (сканер безопасности), предназначенное для использования IT-специалистами, службами информационной безопасности, а также органами по аттестации объектов информатизации. Сканер применяется для централизованного и/или локального определения уязвимостей системного и прикладного программного обеспечения, потенциально опасных настроек и параметров, контроля соответствия требованиям политик и стандартов, контроля целостности, инвентаризации оборудования и программ, документирования результатов аудита.

1. Общие сведения

1.1 Функциональные возможности

RedCheck является программным средством анализа защищенности от несанкционированного доступа, реализующим функции автоматизированного обнаружения уязвимостей в информационных системах с целью оценки возможности преодоления нарушителем системы защиты информационной системы и предотвращения реализации угроз безопасности информации.

Областью применения программы являются ведомственные и корпоративные вычислительные сети, и системы, обрабатывающие как открытую, так и информацию ограниченного доступа, не содержащую государственную тайну.

Программа предназначена для использования администраторами вычислительных сетей и специалистами служб информационной безопасности на этапах внедрения и эксплуатации информационных систем, при проведении работ по аудиту информационной безопасности, а также при проведении аттестации объектов информатизации по требованиям безопасности.

Основные функциональные возможности Программы:

- аудит обновлений системного и прикладного ПО,
- аудит уязвимостей системного и прикладного ПО,
- аудит уязвимотей в режиме "Пентест",
- аудит конфигураций безопасности,
- аудит безопасности АСУ ТП,
- аудит конфигураций безопасности СУБД*,
- аудит защищенности сетевого оборудования (Cisco IOS, Huawei, Булат, S-Terra, CheckPoint),
- аудит защищенности платформ виртуализации (VMware ESXi Server и VMware vCenter Server, Hyper-V),
- инвентаризация программного и аппаратного обеспечения,

- установка недостающих обновлений безопасности, в том числе сертифицированных,
- фиксация и контроль целостности заданных файлов и каталогов,
- идентификация открытых портов, сервисов и поиск уязвимостей,
- подбор паролей методом перебора,
- документирование результатов проверок.

Сертифицированная на соответствие требованиям безопасности (ФСТЭК России) версия RedCheck может использоваться в составе АС до класса защищенности 1Г и информационных системах персональных данных (ИСПДн) и государственных информационных системах (ГИС) до 1 класса (уровня) защищенности включительно.

С помощью RedCheck могут быть реализованы меры защиты согласно «Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (утверждённым приказом ФСТЭК России № 17 от 11.02.2013) и «Составу и содержанию организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (утверждённым приказом ФСТЭК России № 21 от 18.02.2013), «Требованиям к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» (утверждённых приказом ФСТЭК России от №31 от 14.03.2014):

- Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежа-щих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения (ОПС.2).
- Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных (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 и средств защиты информации (АНЗ.4).
- Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации (ОЦЛ.1).
- Контроль целостности виртуальной инфраструктуры и ее конфигураций (ЗСВ.7).

Также RedCheck может применяться при реализации мер по обеспечению безопасности согласно документу «Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» (утверждённым приказом ФСТЭК России № 239 от 25.12.2017):

- Инвентаризация информационных ресурсов (АУД.1).
- Анализ уязвимостей и их устранение (АУД.2).
- Мониторинг безопасности (АУД.7).
- Проведение внутренних аудитов (АУД.10).
- Проведение внешних аудитов (АУД.11).
- Контроль целостности программного обеспечения (ОЦЛ.1).
- 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).

** - полный перечень поддерживаемых СУБД указан в списке поддерживаемых платформ*

Содержание главы...

1.2 Архитектура сканера

Программа условно может быть представлена как 3-х уровневое приложение.

1-й уровень - развернут на доверенной части интернет-сайта компании АЛТЭКС-СОФТ и представляет собой репозиторий OVALdb, содержащий информационный контент безопасности и Web-службы, позволяющие синхронизировать необходимую информацию локальной БД RedCheck с OVALdb. Здесь же расположены средства активации и учета действующих лицензий.

2-й уровень - основной исполнительный компонент, включающий: консоль управления, службу сканирования RedCheckSVR и службу синхронизации RedCheckSyncSvr. Разворачивается на сервере компании или ПЭВМ администратора безопасности. Данный компонент выполняет основные функции RedCheck: сканирование, сбор и обработку данных, синхронизацию (обновление) контента, генерацию отчетов.

К **3-му уровню** относится агент программы RedCheck (далее - агент RedCheck). Агент RedCheck устанавливается на сканируемом хосте и реализует функции службы сканирования RedCheckSVR. Использование агента RedCheck позволяет повысить скорость сканирования, снизить нагрузку на сеть, а также использовать минимальные полномочия, необходимые при авторизации на сканируемом хосте.

Схемы развертывания и применения RedCheck

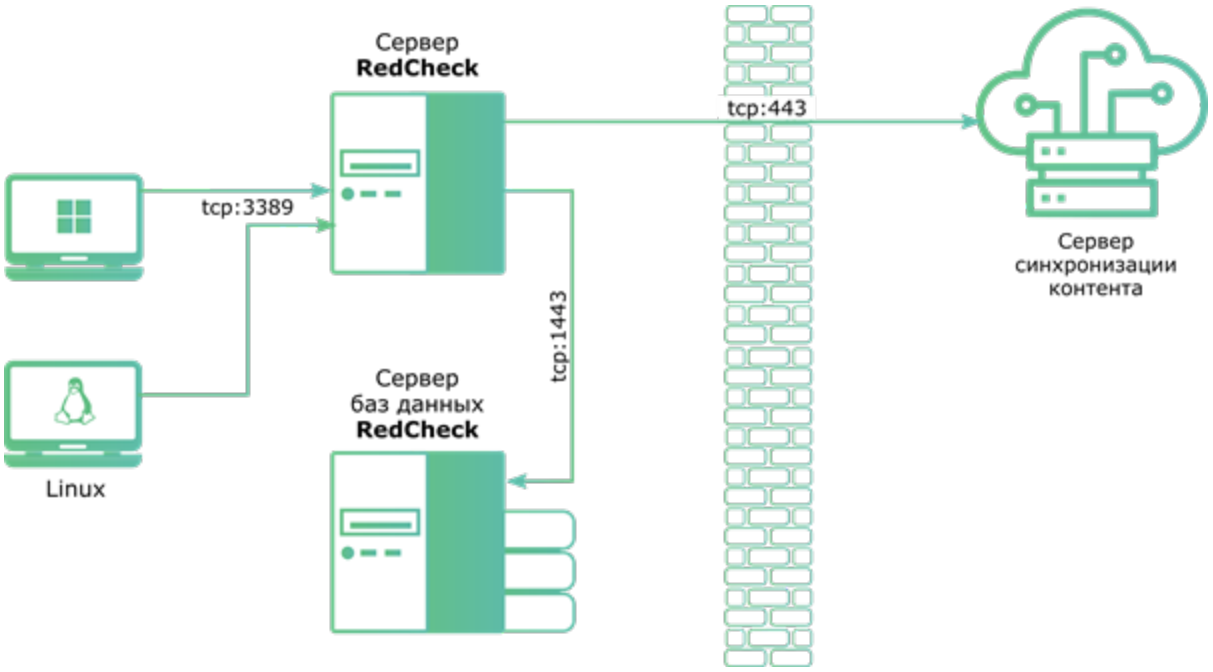
САЗ RedCheck поставляется в редакциях: Base, Professional, Enterprise. Редакция Enterprise не имеет ограничений по масштабированию.

Редакции Base и Professional позволяют установить сканер на единый сервер, совмещенный с СУБД, или с отдельным подключением к серверу СУБД. Подходит для малых и средних организаций, не требует дополнительных серверов.

Используемые дистрибутивы (https://portal.altx-soft.ru/downloads/):

1. RedCheck.msi - Сервер RedCheck;

2. RedCheckAgent.msi - Агент RedCheck;



В редакции Enterprise возможно распределение модулей сканирования по различным площадкам (филиалам) или размещение в едином ЦОД. Это позволяет оптимизировать передачу сетевого трафика во время сканирования, разделить сканирование различных платформ с особыми привилегиями между сканерами, увеличить скорость сканирования за счет параллельной работы сканеров и оперативно получить результаты. Можно использовать промежуточный сервер обновлений RedCheck в DMZ. Данное решение рекомендуется для средних и больших организаций.

Используемые дистрибутивы (https://portal.altx-soft.ru/downloads/):

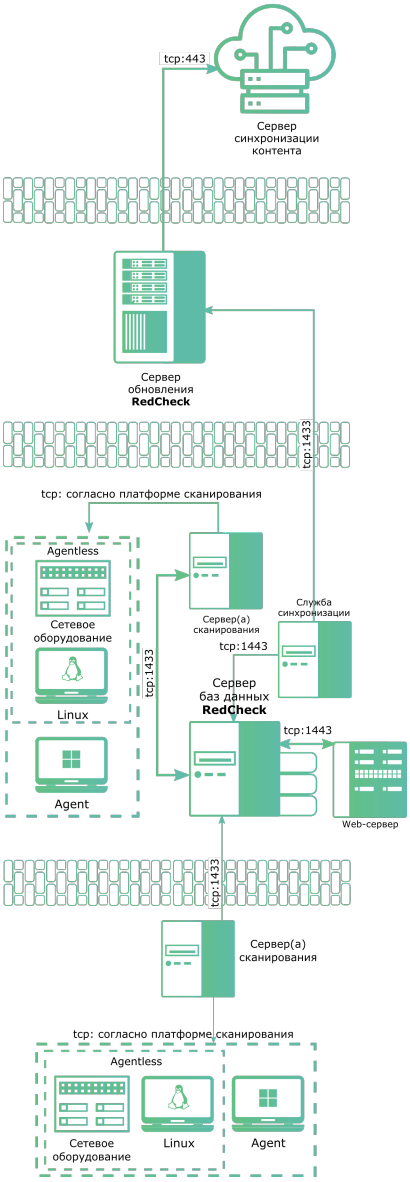
1. RedCheck.msi - Сервер RedCheck;

2. RedCheckAgent.msi - Агент RedCheck;

3. RedCheckScanService.msi - Сервер сканирования RedCheck;

4. RedCheckSyncService.msi - Служба синхронизации RedCheck;

5. RedCheckSyncServer.msi - Сервер обновлений RedCheck.



Для редакций Professional и Enterprise можно установить Web-консоль и получить одновременный доступ к САЗ RedCheck нескольким администраторам безопасности с помощью web-обозревателя с любого устройства.

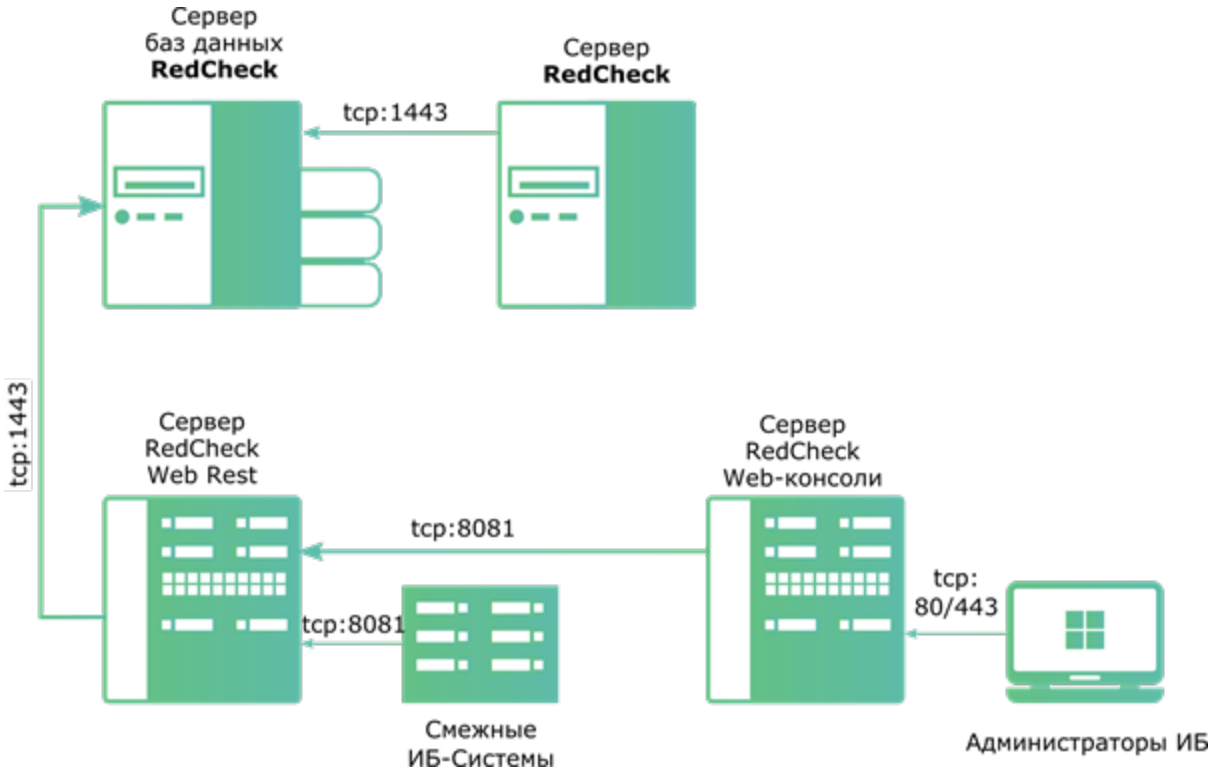
Web-консоль использует вспомогательный компонент Rest-сервиса RedCheck, который обеспечивает интеграцию с SIEM или другими ИБ-системами. Требования для работы Web-консоли доступны по ссылке.

Используемые дистрибутивы (https://portal.altx-soft.ru/downloads/):

1. RedCheck.msi – Сервер RedCheck

2. RedCheckWebRestSetup.msi – Сервер Rest RedCheck

3. RedCheckWebClientSetup.msi - Сервер Web-консоли RedCheck



Начиная с RedCheck версии 1.4, агент требуется только для проверок Windows систем, СУБД и наложенных средств защиты. Для сканирования Linux/Solaris/Unix систем используется безагентское сканирование (agentless). Аудит обновлений, аудит уязвимостей и инвентаризация ОС семейства Microsoft Windows могут быть реализованы и без установки агента RedCheck на сканируемый хост.

Начиная с RedCheck версии 1.6.2 появилась поддержка нового способа получения данных для Windows - Remote Engine. На текущий момент воспользоваться им можно для следующих типов заданий - Аудит уязвимостей, Аудит обновлений, Аудит конфигураций.

В случае сканирования без агента требуется настроить соответствующий доступ к целевому хосту.

[Содержание главы...]

1.3 SCAP и репозиторий OVALdb компании АЛТЭКС-СОФТ

RedCheck работает с унифицированным SCAP-контентом безопасности (обновления, уязвимости, конфигурации, политики безопасности), получаемым из открытого репозитория OVALdb компании АЛТЭКС-СОФТ. На сегодняшний день репозиторий содержит более 100 000 проверок безопасности, верифицированных компанией АЛТЭКС-СОФТ для различных программных и аппаратно-программных платформ, полученных из авторитетных экспертных российских и зарубежных источников.

Security Content Automation Protocol (SCAP, протокол автоматизации управления контентом безопасности) включает в себя ряд открытых стандартов, поддерживаемых международным сообществом профессионалов в области информационной безопасности. Актуальная версия (версия 1.2) SCAP состоит из одиннадцати компонентов протокола в 5 категориях:

1. **Языки**

Языки SCAP стандартизуют словари и выражения, описывающие политику безопасности, механизмы контроля и результаты оценки. SCAP включает в себя, в том числе, следующие компоненты:

- Расширяемый формат описания контрольного списка конфигураций (XCCDF, The Extensible Configuration Checklist Description Format);
- Открытый язык описания уязвимостей и проведения оценок (OVAL®, Open vulnerability and assessment language);
- Открытый интерактивный язык описания контрольного списка (OCIL™, Open checklist interactive language).

2. **Формат отчетов.**

Форматы отчета SCAP представляют необходимые конструкции для выражения собранной информации в стандартизированных форматах.

3. **Перечни.**

Перечни SCAP определяют стандартизованные спецификации, официальные перечни (словари), выраженные с использованием этих спецификаций. SCAP включает в себя следующие перечни:

- Общий перечень платформ (CPE, Common platform enumeration);
- Общий перечень конфигураций (CCE, Common configuration enumeration);
- Общий перечень уязвимостей и рисков (CVE, Common vulnerabilities and exposures);
- Общий перечень слабостей (CWE, Common Weakness Enumeration).

4. **Измерение и оценка систем.**

В SCAP это выражается в оценке определенных особенностей уязвимости (например, слабых мест программного обеспечения и проблем конфигурации безопасности) и определении количественного значения влияния уязвимости (метрики). Метрики SCAP в терминах системных технических требований описываются Общей системой оценки уязвимости (CVSS, Common vulnerability scoring system) и Общей системой оценки конфигурации (CCSS, Common configuration scoring system).

5. **Целостность.**

Спецификация целостности SCAP предназначена для обеспечения целостности информационного SCAP-контента и полученных с помощью него результатов. Модель доверия для данных об автоматизации безопасности (TMSAD, Trust Model for Security Automation Data) является спецификацией целостности SCAP.

SCAP призван автоматизировать процесс управления конфигурациями безопасности, унифицировать форматы представления и спецификации уязвимостей, стандартизовать способы их выявления, а также обеспечить информационный обмен между производителями и пользователями средств защиты информации.

Статус SCAP как международного проекта обеспечивает участие в нем широкого круга специалистов в области ИБ. Протокол поддерживается ведущими мировыми вендорами и регуляторами, такими как ***Microsoft***, ***Cisco***, ***Symantec***, ***Red Hat***, ***Debian***, ***HP***, ***SUSE***, ***NIST*** и др.

Компания АЛТЭКС-СОФТ также присоединилась к сообществу и получила официальный статус OVAL Adopter. АЛТЭКС-СОФТ первой в России создала и поддерживает репозиторий определений на языке OVAL, в котором систематизирован информационный контент безопасности (SCAP-контент) для наиболее распространенных в России программных и аппаратно-программных средств. Компания активно работает над созданием и публикацией информационного SCAP-контента не только для известных продуктов иностранного производства, но и для отечественных средств защиты. Ресурс имеет статус Definition Repository в программе *OVAL Adoption*. Также, продукт RedCheck компании АЛТЭКС-СОФТ имеет статус CVE compatible.

АЛТЭКС-СОФТ имеет статус Top Contributor и входит в тройку лидирующих организаций, сделавших наибольший вклад в развитие протокола SCAP и, в частности, OVAL.

Используемый в сканере RedCheck интерпретатор поддерживает последнюю на данный момент версию языка 5.11.1. RedCheck с реализованными OVAL и XCCDF интерпретаторами дает возможность работы с произвольным SCAP-контентом для оценки состояния защищенности потенциально любых программных и аппаратно-программных продуктов.

Web-ресурс АЛТЭКС-СОФТ, посвященный OVAL, и решения, построенные с использованием протокола SCAP, позволяют широкому кругу специалистов по информационной безопасности воспользоваться опытом и знаниями не только нашей компании, но и всего SCAP-сообщества.

Содержание главы...

1.4 Лицензирование программы

Программа лицензируется по количеству сканируемых хостов или по количеству инсталляций, в зависимости от редакции программы (подробная информация о каждой редакции приведена в *Таблице 2*).

Лицензия на программу срочная, по умолчанию срок лицензии составляет - **1 год**. В последующем, по запросу лицензия может быть продлена. В течение действия лицензии, пользователю предоставляется техническая поддержка, обновление контента безопасности и программы данной версии.

При инсталляции программы необходимо ввести 32-разрядный лицензионный ключ для активации, указанный на фирменном бланке лицензии RedCheck. После активации лицензии, будет доступен функционал программы согласно выбранной редакции.

Если по каким-либо причинам необходимо перенести консоль управления на другой компьютер, ключ активации может оказаться недействительным. В этом случае, необходимо связаться со службой технической поддержки для получения информации по повторной активации лицензии.

При приобретении лицензии на дополнительное количество сканируемых хостов после очередной синхронизации контента произойдет автоматическое добавление доступных для сканирования хостов.

Таблица 2. Лицензирование программы

Технические возможности	RedCheck Base	RedCheck Professional, RedCheck Professional для сертифицированных версий Microsoft	RedCheck Enterprise

Лицензирование	по IP	по IP	по инсталляциям
Архитектура и масштабирование			
Возможность подключения дополнительных модулей (служб) сканирования	–	–	+
Многопоточное сканирование Windows-систем	–	+	+
Роли пользователей	+	+	+
Коннекторы для внешних систем (SIEM, BI, СУИБ и т.п.)	–	+	+
Дополнительная Web-консоль	–	+	+
Оценка защищенности			
Аудит уязвимостей	+	+	+
Аудит конфигураций (compliance)	–	+	+
Аудит обновлений	+	+	+
Аудит СУБД	–	+	+
Инвентаризация	+	+	+
Контроль целостности	+	+	+
Установка обновлений	–	+	+
Управление сертифицированными обновлениями Microsoft (в случае использования	–	Только для RedCheck Professional для сертифицированных версий Microsoft	Опционально

сертифицированных продуктов Microsoft)[2]			
Сетевые проверки, брутфорс	+	+	+
Сканируемые платформы			
Windows	+	+	+
Linux	+	+	+
Solaris	+	+	+
Сетевое оборудование (Cisco, Huawei, Булат и пр.)	_	+	+
СУБД (MS SQL, Oracle, MySQL, PostgreSQL, IBM Db2)	_	+	+
Сервера приложений (web-сервера)	_	+	+
VMware	_	+	+
Сервисы и удобства			
Расширенная поддержка	за доп. плату	за доп. плату	+
Расширенный доступ к OVALdb	за доп. плату	за доп. плату	+
Адаптация compliance	_	за доп. плату	+

Дополнительный модуль (служба) сканирования RedCheck предназначен для масштабирования сканера. Модуль по своим функциональным возможностям аналогичен основной службе сканирования RedCheck и работает под ее управлением. Лицензируется отдельно, количество подключаемых дополнительных модулей сканирования не ограничено.

Содержание главы...

1.5 Требования к аппаратному обеспечению

Раздел содержит информацию о требованиях к аппаратному и программному обеспечению, предъявляемых к системе для развертывания RedCheck.

Требования к аппаратному обеспечению необходимые для корректной работы RedCheck приведены в Таблице 3.

Таблица 3. Требования к аппаратному обеспечению.

Редакция/Компонента	СУБД	Узлов не более	Аппаратные компоненты	Частота сканирования		
				1 раз в неделю	1 раз в месяц	1 раз в квартал
RedCheck Base/Pro	MS SQL Express установлена 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 E5 (не менее 2 физических ядер)		
			RAM	6 ГБ		
			HDD	2 ГБ		
RedCheck Base/Pro	MS SQL Server (отдельный сервер)	200	HDD[2]	21,8 ГБ	5,8 ГБ	2,6 ГБ
		500	HDD[2]	53 ГБ	13	5 ГБ

					ГБ	
		2 000				
RedCheck Enterprise			CPU	Intel Xeon E5 (не менее 4 физических ядер)		
			RAM	6 ГБ		
			HDD[1]	2 ГБ		
	MS SQL Server (отдельный сервер)		SSD[3]	400 ГБ	100 ГБ	35 ГБ
Дополнительный модуль сканирования (ScanModul RedCheck)			CPU	Intel Xeon E5 (не менее 2 физических ядер)		
			RAM	6 ГБ		
			HDD[1]	1 ГБ		
	MS SQL Server (отдельный сервер)		HDD[2]	209 ГБ	49 ГБ	17 ГБ
Локальный сервер обновлений (Update Server RedCheck)	MS SQL Server (отдельный или совмещенный сервер)		CPU	Intel Xeon E5 (не менее 2 физических ядер)		
			RAM	6 ГБ		
			HDD[1]	2 ГБ		
Агенты сканирования Windows-систем (Agent RedCheck) и установки обновлений (Agent Update RedCheck)			CPU	Intel Pentium/ AMD Phenom и выше		
			RAM	2 ГБ		
			HDD[1]	5 ГБ		

В таблице указаны требования к размеру свободного места жестких дисках (HDD) без учета размещения на них операционных систем, СУБД и пр. системного и прикладного ПО.

[1]Параметры аппаратной платформы для операционной системы и MS SQL соответствует 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 настройки работы СУБД.

Рекомендации приведены со следующими допущениями:

- указаны торговые марки CPU Intel, допускается использование аналогичных по характеристикам CPU AMD;
- станция, на которой установлен RedCheck не используется в рабочих процессах предприятия;
- параметры аппаратной платформы для операционной системы, на которой разворачивается RedCheck и MS SQL соответствует требованиям Microsoft;
- SQL server может быть развернут как локально, так и на удалённой машине, относительно сканера RedCheck. При локальном расположении необходимо учитывать дополнительные системные требования для СУБД.

Выделяемый объем HDD, предназначен для хранения контента безопасности и результатов сканирования RedCheck.

На объем требуемого пространства влияют такие факторы как:

- частота проводимых сканирований;
- количество сканируемых узлов;
- период хранения результатов сканирования в БД.

В среднем, результаты сканирования одного хоста вместе со сформированным отчетом (PDF) занимают 2 МБ.

Для определения приблизительно объема требуемого пространства, нужно среднее значение одного результата сканирования (2 Мб) умножить на количество сканируемых хостов, а полученный результат умножить на количество сканирований в заданный период.

Например, для еженедельного сканирования 100 хостов, с последующим хранением полученных данных в течение полугода (26 недель) необходимо:

2 МБ (средний объем данных одного сканирования) *100 ед. (кол-во хостов) *26 недель (период хранения) = 5,2 ГБ.

 *При использовании СУБД Microsoft SQL Server 2012 Express Edition существует ограничение на объем хранимых результатов сканирования, связанное с максимальным размером базы данных - 10 ГБ.*

Содержание главы...

1.6 Состав дистрибутива RedCheck

- RedCheck - консоль управления RedCheck (графический интерфейс);
- RedCheckAgent (x86) - агент обновления RedCheck (для 86-х ОС);
- RedCheckAgent (x64) - агент обновления RedCheck (для 64-х ОС);
- RedCheckUpdateAgent (x86) - агент обновления RedCheck (для 86-х ОС);
- RedCheckUpdateAgent (x64) - агент обновления RedCheck (для 64-х ОС);
- Wsus Kit - надстройка RedCheck, для взаимодействия консоли RedCheck и WSUS сервера;
- RedCheckWeb Client Setup - графический интерфейс Web-консоли RedCheck;
- RedCheckWeb Rest Setup - сервер управления Web-консоли RedCheck.

Содержание главы...

1.7 Требования к программному обеспечению

Консоль администратора RedCheck

Сканер безопасности RedCheck предназначен для функционирования под управлением ОС Windows, исключая домашние редакции, начиная с версии Windows 7 (редакции Professional и выше) и Windows Server 2008 SP2 (редакции Standard и выше).

На рабочей машине должен быть установлен Windows Installer, начиная с версии 2.0.

Список поддерживаемых ОС постоянно расширяется. Актуальный перечень поддерживаемых платформ, указан в пп. 1.10, настоящего Руководства Администратора.

Для обеспечения работы консоли администратора RedCheck требуется наличие следующего ПО:

- Microsoft .NET Framework full 4.6.1 или выше (для версий консоли 2.6.5...);
- СУБД SQL Server 2012 и выше (все редакции, включая Express);
- Microsoft Visual C++ 2013 Redistributable (актуальную версию пакета можно скачать с официального сайта - https://www.microsoft.com/ru-RU/download/details.aspx?id=40784, выбрать файл для 32-битной версии: vcredist_x86.exe);
- Microsoft Visual C++ 2015 Redistributable (актуальную версию пакета можно скачать с официального сайта - https://www.microsoft.com/en-US/download/details.aspx?id=48145, выбрать файл для 32-битной версии: vc_redist.x86.exe);
- Npcap (актуальную версию компонента можно скачать с официального сайта - https://nmap.org/, либо установить его из дистрибутива RedCheck).

 *В программе RedCheck версии 2.1 и выше, поддержка СУБД версии 2008 - отсутствует.*

 *RedCheck 2.6.6 и выше работает только под управлением 64-х разрядных ОС.*

RedCheck агенты

RedCheck, RedCheck Update агенты функционирует под управлением ОС Windows, начиная с версии Windows Vista SP2 и Windows Server 2008 SP2.

На рабочей машине должен быть установлен Windows Installer, начиная с версии 2.0, Microsoft .NET Framework full версии 4.6.1 или выше.

Содержание главы...

1.8 Требования к сетевой инфраструктуре

RedCheck предназначен для использования в сетях на основе протокола TCP/IP. На компьютере должны быть установлены компоненты операционной системы, обеспечивающие работу со стеком сетевых протоколов TCP/IP.

Взаимодействие между RedCheck и агентом RedCheck для Windows-систем осуществляется на основе протокола TCP.

Взаимодействие между RedCheck и Linux/Solaris-систем происходит с помощью протокола TCP на транспортном, и SSH на прикладном уровне.

Таблица 1.8. 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	32 000	16 800	434 000	5 000
Среднее время сканирования*, мин	00:02:40	00:02:20	00:15:00	00:02:20

** - Показатели приведены для режима «Аудит уязвимости, полное сканирование», данный режим является наиболее ресурсоемким.*

Для синхронизации контента безопасности RedCheck с репозиторием OVALdb используется протокол HTTPS.

Содержание главы...

1.9 Взаимодействие с СЗИ от НСД

 *Не рекомендуется устанавливать RedCheck на один сервер с другими СА3, в противном случае могут быть внесены изменения в библиотеки среды функционирования, что нарушит работу RedCheck.*

Общий перечень папок и исполняемых файлов, подлежащих добавлению в списки исключений СЗИ от НСД, используемых в сети предприятия:

Список директорий установки	Исполняемый файл
Агента сканирования: C:\Program Files\ALTEX-SOFT\RedCheckAgent; C:\Program Files (x86)\ALTEX-SOFT\RedCheckAgent	\RedCheckAgent.exe
Агента обновлений: C:\Program Files\ALTEX-SOFT\RedCheckUpdateAgent; C:\Program Files (x86)\ALTEX-SOFT\RedCheckUpdateAgent	\RedCheckUpdateAgent.exe
Сканера RedCheck: C:\Program Files\ALTEX-SOFT\RedCheck; C:\Program Files (x86)\ALTEX-SOFT\RedCheck	\RedCheck.exe; \RedCheckSnc.exe; \RedCheckSvc.exe
Дополнительной службы сканирования: C:\Program Files\ALTEX-SOFT\RedCheckScanService; C:\Program Files (x86)\ALTEX-SOFT\RedCheckScanService	\RedCheckSvc.exe

Дополнительной службы синхронизации: C:\Program Files\ALTEX-SOFT\RedCheckSyncService; C:\Program Files (x86)\ALTEX-SOFT\RedCheckSyncService	\RedCheckSnc.exe

Инсталляционный пакет
RedCheck-....msi
RedCheckAgent-...-x64.msi
RedCheckAgent-...-x86.msi
RedCheckUpdateAgent-...-x64.msi
RedCheckUpdateAgent-...-x86.msi
RedCheckApiServer-....msi
RedCheckScanService-....msi
RedCheckSyncService-....msi
RedCheckWeb.Client.Setup-x64-....msi
RedCheckWeb.Rest.Setup-x64-....msi

1.10 Перечень поддерживаемых платформ

Таблица 4

Платформы
Microsoft Windows
• XP/XP Embedded[1]/Vista/7/8/8.1/10 • Server 2003/2008/2008R2/2012/2012R2/2016/2019[2]
Linux
• Amazon Linux AMI • CentOS Linux 5/6/7 • Debian 8/9 • Debian GNU/FreeBSD 6/7 • Debian GNU/Linux 2.2/3.0/3.1/4/5/6/7 • FreeBSD 6/7/10/11/12 • Mageia 4/5/6/7 • openSUSE 11.4/12.1/12.2/12.3/13.1/13.2 • openSUSE Evergreen 11.4 • openSUSE Leap 42.1/42.2/42.3 • Oracle Linux 5/6/7 • Photon 1/2 • Red Hat Enterprise Linux 5/6/7/8 • Solaris 10/11 • SUSE Linux Enterprise Desktop 10/10 SP4/11/11 SP1/11 SP2/11 SP3/11 SP4/12/15 SP2 • SUSE Linux Enterprise Server 10/10 SP2/10 SP3/10 SP4/11/11 SP1/11 SP2/ 11 SP3/11 SP4/12/15 SP2 • 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/ 11.04/11.10/12.04/12.10/13.04/13.1014.04/14.10/15.04/15.10/16.04/16.10/ 17.04/17.10/18.04 **Отечественные ОС** • ALT Linux 6/7 • ALT Linux SPT 6/7

- ALT 8 SP
- ALT 8/9
- Astra Linux Смоленск 1.5/1.6
- Astra Linux Орёл 2.12
- РЕД ОС 7.2/7.2c
- ROSA DX COBALT 1.0
- ROSA SX COBALT 1.0

Сетевое оборудование

- Check Point GAiA
- Cisco IOS
- Huawei VRP
- S-Terra IOS[3]

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.
- VMware ESXi Server 5.1/5.5/6.0/6.5/6.7
- VMware vCenter Server 5.1/5.5/6.0

СУБД

- Microsoft SQL Server 2005/2008/2008 R2/2012/2014/2016/2017
- MySQL Server 5.5/5.6/5.7
- Oracle Database Server 11/12
- PostgreSQL 8/9/10/11
- IBM Db2
- SAP HANA

Scada

- ArchestrA 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

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

[2]Для Windows Server 2019 не применим функционал PatchManagment.

[3]Сканирование оборудования S-Terra возможно с учетной записью пользователя, имеющего возможность подключения к удаленной системе по протоколу SSH.

*В **Таблице 5** представлены возможные режимы сканирования для соответствующих типов заданий.*

Таблица 5

Цели сканирований/Типы заданий		Windows	Linux	Cisco	Huawei	VMWare	Solaris	FreeBSD	Check Point
Аудит уязвимостей		A/AL/RE	AL	AL	AL	AL	AL	AL	AL
Аудит обновлений		A/AL/RE	AL	-	AL	AL	-	NA	-
Аудит конфигураций		A/RE	AL*	AL	AL	AL	AL	NA	AL
Аудит СУБД	MS SQL	A/RE	AL	NA	NA	NA	NA	NA	NA
	MySQL	A/RE	AL	NA	NA	NA	NA	NA	NA
	БД Oracle	A/RE	AL	NA	NA	NA	NA	NA	NA
	PostgreSQL	A/RE	AL	NA	NA	NA	NA	NA	NA
	IBM Db2	A/RE	AL	NA	NA	NA	NA	NA	NA
	SAP HANA	A/RE	AL	NA	NA	NA	NA	NA	NA
Сканирование портов		AL+ Pentest	AL+ Pentest	AL+ Pentest	AL+ Pentest	AL+ Pentest	AL+ Pentest	AL+ Pentest	AL+ Pentest
Подбор паролей		AL+ NMAP	AL+ NMAP	NA	NA	NA	AL+ NMAP	AL+ NMAP	NA

Инвентаризация	A/AL/RE	AL	AL	-	AL	-	-	AL
Фиксация	A	AL	AL	-	AL	-	-	AL

** - Кроме РЕД ОС.*

Условные обозначения:

«A» -агент;

«AL» - безагент (WMI, SSH);

«RE» - WinRM;

NMAP - с использованием NMAP-ALTX (входит в состав Изделия);

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

« - » - указанный режим сканирования для данного типа задания не поддерживается.

Содержание главы...

1.11 Установка .Net Framework

На хостах, предназначенных для развертывания RedCheck и агентов RedCheck должен быть установлен компонент *.Net Framework 4.6.1 или выше.* Дистрибутив данного компонента доступен на странице Центра загрузок корпорации Microsoft.

Содержание главы...

1.12 Подготовка СУБД

Для работы RedCheck необходимо наличие СУБД Microsoft SQL Server 2012 и выше.

Взаимодействие с СУБД возможно в двух режимах:

- Используя локальные УЗ в СУБД
- Используя Доменные УЗ в СУБД

Режим авторизации в СУБД можно изменить в любое время, как при инсталляции, в мастере установки, так и после установки используя Management Studio.

Установка внешней SQL Server может быть произведена на любой, доступной по сети рабочей станции или сервере сети

 *Подключение СУБД после инсталляции RedCheck не предусмотрено.*

Содержание главы...

1.13 Настройка СУБД в режиме смешанной авторизации

Для корректного взаимодействия RedCheck и СУБД Microsoft SQL Server, в экземпляре СУБД должен использоваться смешанный тип аутентификации.

При использовании смешанной авторизации, необходимо:

- В пользователи СУБД добавить локального пользователя, от имени которого будет происходить обращение к БД.
- Добавить членство локального пользователя в ролях базы данных *db_ddladmin, db_datareader, db_datawriter* или в роли *db_owner, db_creator*

В случае использования СУБД только для ПО RedCheck, допускается добавление членства пользователя в роли *db_owner.*

Содержание главы...

1.14 Настройка СУБД в режиме Доменной авторизации

Для корректного взаимодействия RedCheck и СУБД Microsoft SQL Server, в экземпляре СУБД должен использоваться смешанный тип аутентификации.

При использовании доменной авторизации, необходимо:

- В пользователи СУБД добавить доменного пользователя, от имени которого будет происходить обращение к БД.
- Добавить членство доменного пользователя в ролях базы данных *db_ddladmin, db_datareader, db_datawriter* или в роли *db_owner, db_creator*.

В случае использования СУБД только для ПО RedCheck, допускается добавление членства пользователя в роли db_owner.

Для обеспечения отказоустойчивости работы компонентов RedCheck с БД, необходимо убедиться, что глобальная доменная политика не блокирует запуск служб от имени доменного пользователя.

Либо добавить разрешение в глобальной политике разрешающее запуск службы от имени доменного пользователя. Для этого необходимо:

Создать/редактировать GPO назначенную для серверов с компонентами RedCheck.

Отредактировать GPO: *Computer Configuration > Windows Settings > Security Settings > Local policies > User Rights Assignment*.

В параметрах:

- Log on as a batch job
- Log on as a service

добавить имя учетной записи, выбранной для работы с БД RedCheck.

Содержание главы...

1.15 Подключение внешней СУБД

Для корректного подключения к БД необходимо произвести настройку подключения:

- Запустить Диспетчер конфигурации SQL Server. Диспетчер запускается через меню ***Пуск-Программы-Microsoft SQL Server 2012 -Configuration tools*** (Средства настройки)-***SQL Server Configuration Manager*** (Диспетчер конфигурации SQL Server)
- В левой части окна программы настройки выделить необходимый экземпляр ***«SQL Server Network Configuration» -«Protocols for REDCHECKINSTANCE»***(«Протоколы для SQLEXPRESS» в случае использования редакции Express)
- В правой части окна программы настройки для протокола TCP/IP с помощью контекстного меню выберать команду ***«Enable»*** (Включить).
- В окне предупреждения нажать кнопку ***«OK»***
- В левой части окна программы настройки выделить ***«SQL Native Client 11.0 Configuration» - «Client protocols»***
- В правой части окна в настройках для протокола TCP/IP с помощью контекстного меню выберать команду ***«Enable»*** (Включить)
- В появившемся окне предупреждения нажмать кнопку ***«OK»***
- Для того что бы изменения вступили в силу необходимо перезапустить ***SQL Server***
- Для этого в левой части окна программы выделить ***«SQL ServerServices»***. В правой части окна выбрать ***SQL Server (REDCHECKINSTANCE)***, вызвать контекстное меню и нажать кнопку ***«Restart»*** (Перезапустить)

Процесс настройки завершен.

Содержание главы...

1.16 Получение дистрибутива RedCheck

Сертифицированная версия RedCheck может быть получена только в виде верифицированного дистрибутива на CD-диске в рамках поставки.

Несертифицированная версия RedCheck может быть получена как на CD-диске, так и загружена по ссылке, указанной производителем. Для получения демоверсии необходимо заполнить форму на сайте http://www.redcheck.ru.

Содержание главы...

2. Установка программы

2.1 Установка сканера RedCheck

 *Установка консоли управления RedCheck должна проводиться на сервер не являющийся Контроллером доменов!*

Для работы программы RedCheck необходимо наличие следующего дополнительного программного обеспечения:

- Microsoft .NET Framework full 4.6.1 или выше (для версий консоли 2.6.5...);
- ***СУБД SQL Server 2012*** и выше (все редакции, включая Express).

Если на компьютере предустановлено выше указанное программное обеспечение, то можно воспользоваться дистрибутивом ***RedCheck.msi***.

 *Установка пакета должна проводиться от имени учетной записи, имеющей административные привилегии на АРМ.*

В мастере задания необходимо пошагово принять лицензионное соглашение, указать номер лицензии, которая планируется использоваться, выбрать путь для установки.

По умолчанию, используются следующие каталоги:

- Для 32-х битных систем: ***«C:\Program Files\ALTEX-SOFT\RedCheck\»***
- Для 64-х битных систем: ***«C:\Program Files (x86)\ALTEX-SOFT\RedCheck\»***

Указать данные для подключения к СУБД:

- В текстовом поле ***«Сервер базы данных»*** введите IP-адрес или полное доменное имя (FQDN) сервера SQL и экземпляра SQL;
- Если необходимо использовать нестандартный порт для доступа к SQL серверу, укажите номер требуемого порта, отделенный запятой.

Указать имя сервера и экземпляра SQL (в качестве имени сервера может быть использован IP-адрес или доменное имя).

Взаимодействие с СУБД возможно в двух режимах:

- Используя локальные УЗ в СУБД;

  Если используется локальная УЗ в СУБД, необходимо указать имя пользователя и пароль учетной записи SQL Server.

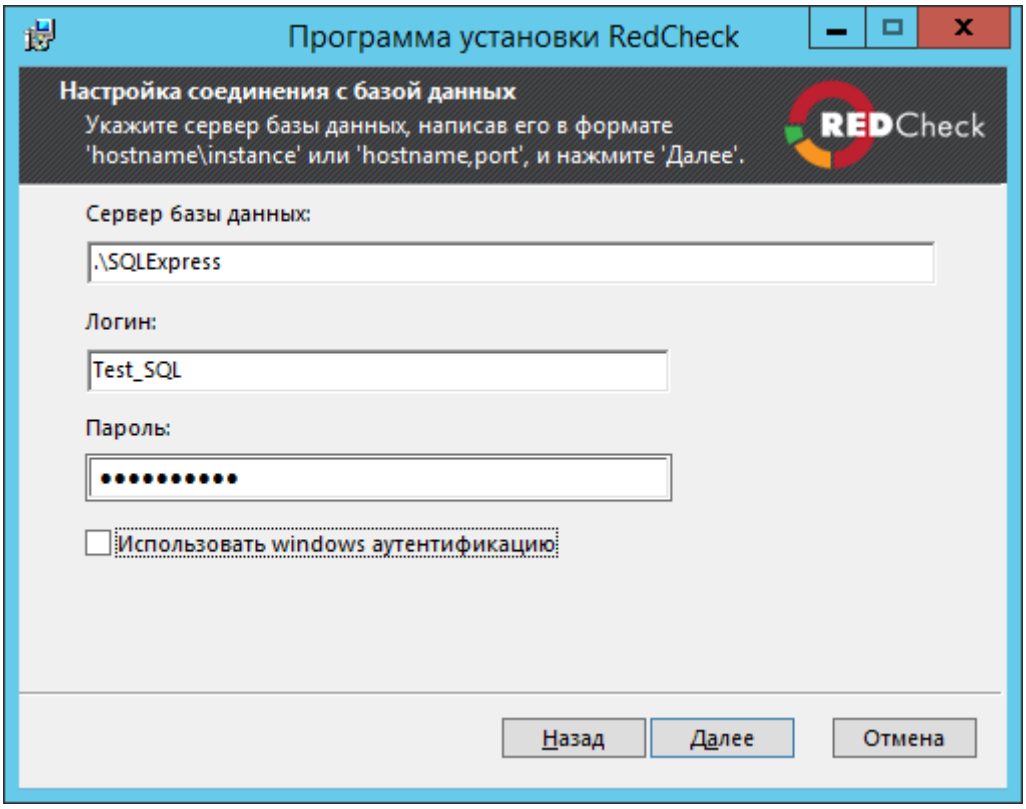


Рисунок 2.1.1

- Используя Доменные УЗ в СУБД:

Если используется УЗ windows для подключения к СУБД, то необходимо поставить галочку ***«Использовать windows аутентификацию»*** и ***«Использовать учётные данные другого пользователя для доступа к БД через аутентификацию Windows»***.

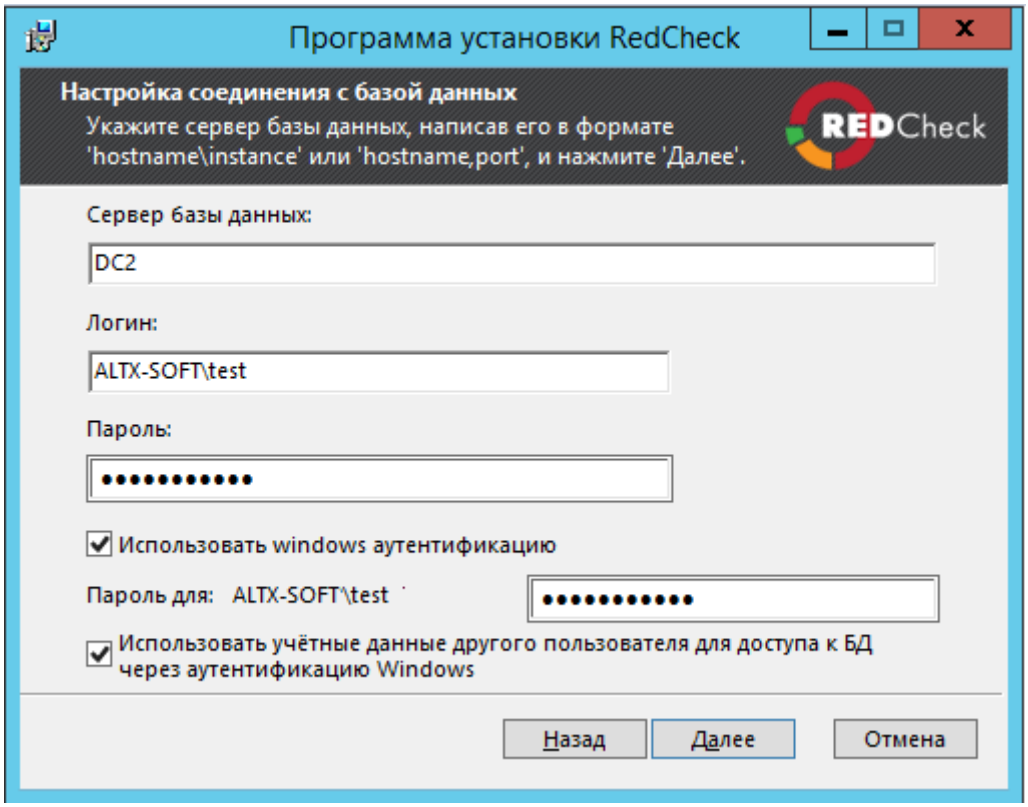


Рисунок 2.1.2

В случае использования авторизации windows, мастер установки RedCheck необходимо запускать от имени той УЗ, от имени которой будет осуществляться подключение к СУБД.

В случае использования авторизации windows, службы RedCheck, в диспетчере служб (services.msc), должны быть запущены от имени той УЗ, от имени которой осуществляется подключение к СУБД.

Ввести имя базы данных для RedCheck. Если у Вас уже есть ранее созданная БД, то выбрать пункт ***«Подключиться к существующей»***, в противном случае выбрать пункт ***«Создать БД»***.

Для правильной работы программы необходимо, чтобы пользователь входил в группу ***«REDCHECK_ADMINS»***, в противном случае, если группа не создана или пользователь в ней отсутствует, будет предложено диалоговое окно с выбором пунктов ***«Создать группу …»*** и ***«Добавить текущего пользователя в группу …»***, если данные опции выбраны, инсталлятор создаст соответствующую группу и добавит в нее текущего пользователя автоматически, для применения этих настроек

необходимо выйти из системы и войти в нее заново либо перезагрузить систему после окончания процесса установки.

В случае если консоль управления RedCheck установлена на компьютере, находящемся в доменной сети предприятия, необходимо, чтобы пользователь (который запускает консоль RedCheck) входил в доменную группу *«REDCHECK_ADMINS»* либо в любую другую согласно ролевой модели.

Далее программа предложит Вам выбрать Тип синхронизируемого контента. На данном шаге инсталлятора необходимо выбрать тип контента, который будет загружаться в БД, для последующего выполнения на клиентских АРМ в процессе сканирования.

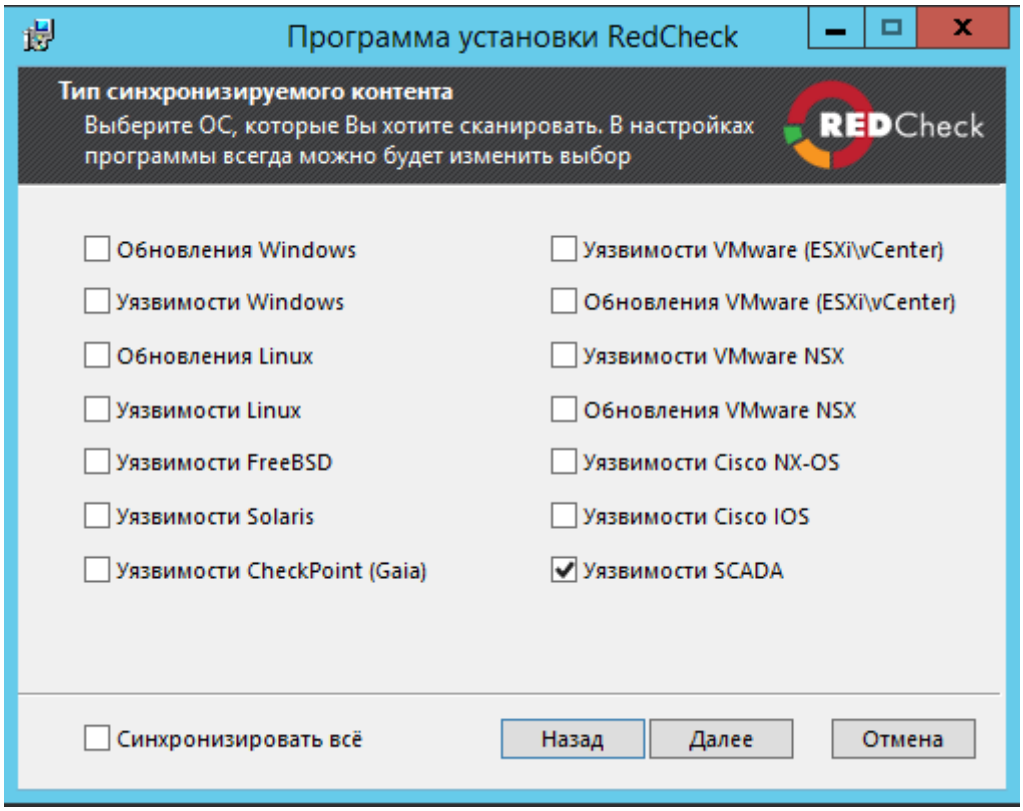


Рисунок 2.1.3

Если возникнет необходимость изменить выбор типа загружаемого контента, это можно сделать в любой момент времени в настройках программы, на вкладке *«Синхронизация»*.

Далее необходимо выбрать тип синхронизации контента:

- Синхронизация вручную;
- Автоматически ежедневно по расписанию (Необходимо указать удобное время синхронизации).

Предварительная настройка завершена и после нажатия кнопки ***«Далее»***, появится статусная строка установочного процесса.

По окончании процесса установки появится соответствующее окно. Установка RedCheck завершена.

 *В случае необходимости установки программы через командную строку Windows, необходимо выполнить следующие команды:*

- ***msiexec /i "D:\Desktop\RedCheck.msi" DATABASE_SERVER= DATABASE_USERNAME= DATABASE_PASSWORD=* LICENSE="*" NEED_CREATE_DATABASE=0 DATABASE_NAME=RedCheck /qb CREATEGROUP=1 ADDUSERTOGROUP=1*** - установка консоли управления RedCheck,
- ***msiexec /x "D:\Desktop\RedCheck.msi" /qn NEED_REMOVE_DATABASE=0 SILENT_MODE=1*** - удаление консоли управления RedCheck

 *В случае возникновения ошибок во время установки, обратитесь к файлу, журналу установки, расположенному по следующему пути: %temp%/ALTEX-SOFT/RedCheckSetup.txt. Для разрешения нештатной ситуации рекомендуется обратиться в службу поддержки support@altx-soft.ru. При обращении необходимо описать проблему и приложить файл RedCheckSetup.txt.*

 *После установки программы и перед началом работы с ней необходимо убедиться в том, что все службы RedCheck запущены, об этом свидетельствуют зеленые индикаторы соответствующих служб, в нижней части окна консоли управления RedCheck. После запуска служб необходимо выполнить синхронизацию контента безопасности.*

Содержание главы...

2.2 Установка и настройка дополнительных службы сканирования и синхронизации RedCheck

На крупных предприятиях с территориально-распределенной филиальной структурой могут возникать затруднения с организацией систем информационной безопасности.
ИТ-инфраструктура должна удовлетворять потребностям развития предприятия, должна быть гибкой. Необходимо спланировать адекватное управление всеми системами компании, обеспечить бесперебойность и безопасность работы.
Благодаря функции масштабирования, программа RedCheck поможет решить вышеперечисленные вопросы, организовать единую систему мониторинга на больших и с филиальной структурой предприятиях.
Адаптация к сложной инфраструктуре обеспечивается с помощью использования дополнительной службы сканирования. Такой метод позволяет сканировать удаленные ЛВС и получать информацию о результатах проверок в филиалах организации.


Использование дополнительного модуля сканирования доступно только для лицензий редакции Enterprise.

Запустить дистрибутив ***RedCheckScanService.msi.*** Дождаться появления окна приветствия. Следовать инструкциям мастера установки.

На одном из этапов ввести настройки соединения с БД программы RedCheck, совместно с которой будет использоваться данный модуль.

После завершения процесса установки дополнительно службы сканирования, необходимо перезапустить консоль RedCheck, перейти: ***Инструменты → Настройки → Дополнительно → Автопроверка новых задач***, установить флаг ***«Включить автопроверку сервисом новых задач»***.

*Учётная запись, которая используется для сканирования через дополнительную службу сканирования, не должна быть сохранена с использованием шифрования. Данная опция настраивается в **Инструменты → Менеджер учётных записей**, выбираем необходимую учетную запись, правой кнопкой мыши - редактирование, далее внизу открывшегося окна **Шифрование**. В том случае, если учетная запись была создана ранее с использованием шифрования, необходимо либо удалить и создать заново, без использованием шифрования текущую учетную запись, либо создать новую без использованием шифрования.*

Содержание главы...

Установка дополнительной службы синхронизации необходима в случае сканирования закрытого сегмента сети (ДМЗ), при условии, что использование оффлайн режима не приемлемо, либо не удобно.

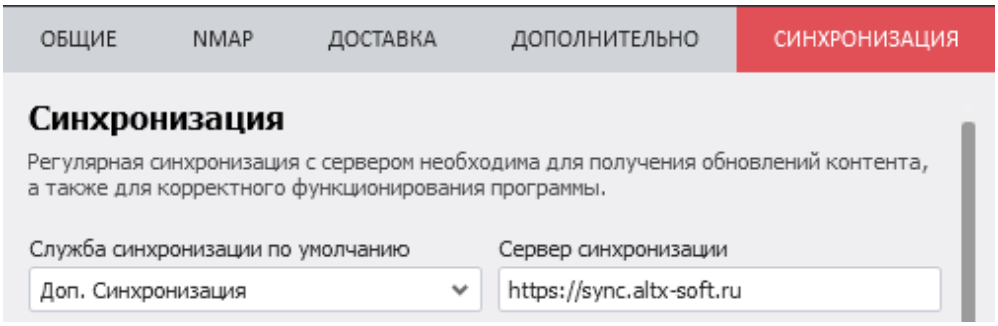
В указанной ситуации дополнительная служба синхронизации разворачивается за периметром ДМЗ и выполняет безопасное обновление базы разрешающих правил сканера RedCheck.

Запустить дистрибутив ***RedCheckSyncService.msi.***

Дождаться появления окна приветствия.

Следуйте инструкциям мастера установки.

После завершения процесса установки дополнительноq службы синхронизации, необходимо перезапустить консоль RedCheck, перейти: ***Инструменты - Настройки - Синхронизация - Служба синхронизации по умолчанию***, выбрать нужную службу и ниже установить флаг напротив ***«Включить проверку триггера обновления»*** .



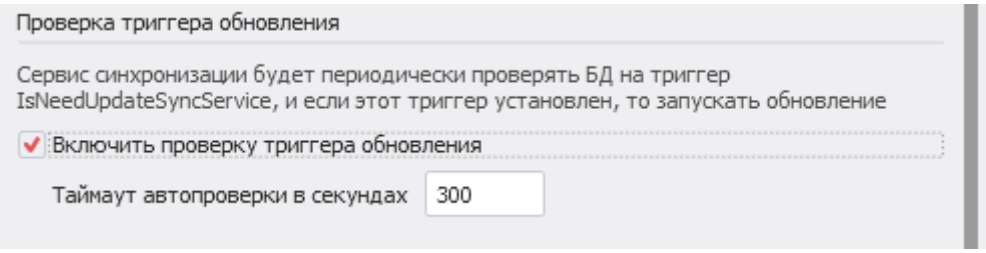


Рисунок 2.2.2

Режим упрощенной синхронизации позволяет уменьшить объем передаваемых данных, между базой данных и компонентами RC, тем самым ускоряя процесс синхронизации контента.

Содержание главы...

2.3 Установка агента

Установка агента и настройка параметров сетевого взаимодействия может быть произведена локально непосредственно на сканируемом хосте либо при помощи средств централизованного управления **Microsoft Active Directory** или другими инструментами администрирования сетей.


*Дистрибутив агента имеет возможность принимать параметр запуска службы: **DELAYED_AUTO_START.***

Возможные значения: 0 - автоматический запуск; 1 - отложенный запуск.

Пример выполнения команды на установку агента:


В случае необходимости установки программы через командную строку Windows, необходимо выполнить следующую команду:

msiexec /i "C:\Distr\RedCheckAgent.msi" DELAYED_AUTO_START=0 /qb

*Дистрибутив агента имеет возможность принимать параметр запуска службы: **DELAYED_AUTO_START.** Возможные значения: 0 - автоматический запуск; 1 - отложенный запуск.*

Опция отложенного запуска позволяет оптимизировать процесс загрузки системы и облегчает настройку приложений для последовательной автозагрузки.


В целях повышения быстродействия сканирования ОС Windows рекомендуется использование следующих транспортов (в порядке приоритетности): Агентский способ, сканирование при помощи временного агента (WinRM), безагентский способ (WMI). Сканирование с использованием WMI рекомендуется проводить для заданий сканирования либо с быстрым профилем, либо с ограниченным количеством проверок. Данная особенность связана с очень большим количеством сигнатур, которые рекурсивно сканируют файловую

систему ОС в поиске уязвимых компонентов, что приводит к постоянной загрузке машины, канала и увеличению времени сканирования.

Содержание главы...

Для повышения производительности сканирования, а также в случае необходимости проведения контроля целостности Windows-систем на удаленных контролируемых хостах, а также СЗИ от НСД Secret Net и Dallas Lock на удаленных и локальных хостах, требуется установка агента RedCheck.

Установка агента должна выполняться от имени учетной записи, имеющей административные привилегии.

Запустить пакет ***RedCheckAgent.msi***, из дистрибутива RedCheck. Дождаться появления окна приветствия и следовать инструкциям от мастера установки.

Рекомендуется выполнять установку в каталог по умолчанию.

Для автоматического разрертывания агента RedCheck можно воспользоваться скриптом.

Примеры выполнения команд на установку агента:

msiexec /i "C:\Distr\RedCheckAgent.msi" DELAYED_AUTO_START=0 /qb

Возможные значения: 0 - автоматический запуск; 1 - отложенный запуск;

CREATEGROUP="1" - создание группы REDCHECK_ADMINS;

SILENT_MODE="1" - блокировка всех сообщений

Содержание главы...

В сетях с доменной структурой, доступна возможность централизованной установки агента RedCheck на целевые хосты.

- Открыть консоль управления групповыми политиками. Нажать ***«Пуск»> «Панель управления»> «Администрирование»> «Управление групповой политикой».***
- В дереве консоли последовательно развернуть дерево, интересующего леса и домена и указать расположение объектов групповой политики.
- Воспользовавшись правой кнопкой мыши создать новый либо изменить существующий объект GPO.

С помощью редактора объектов групповой политики:

- В разделе «Конфигурация компьютера» развернуть раздел ***«Конфигурация программ»*** и выбрать пункт ***«Установка программ»***.
- При помощи контекстного меню вызываемого правой кнопкой мыши создать новый ***«Пакет»***. В появившимся окне выбрать сетевое расположение инсталляционного файла. В параметрах установки указать тип установки ***«Назначенный»***. Сетевое расположение инсталляционного файла должно быть доступно для «чтения» компьютеров, на которых будет произведено развертывание.

Содержание главы...

2.4 Установка компонента Nmap

RedCheck поддерживает возможность интеграции с утилитой сканирования IP-сетей **Nmap**.

Активация утилиты **Nmap** позволяет использовать в RedCheck функции ***«Сканирование портов»***, ***«Подбор паролей» и «Поиск уязвимостей» (Пентест)***.

Утилита Nmap включена в установочный дистрибутив RedCheck. Для её активации, на этапе установки консоли управления RedCheck, необходимо выбрать один из двух вариантов:

- Установить сертифицированную версию Namp;
- Указать путь к установленному Nmap (в случае, если ПО уже установлено в данной OS).

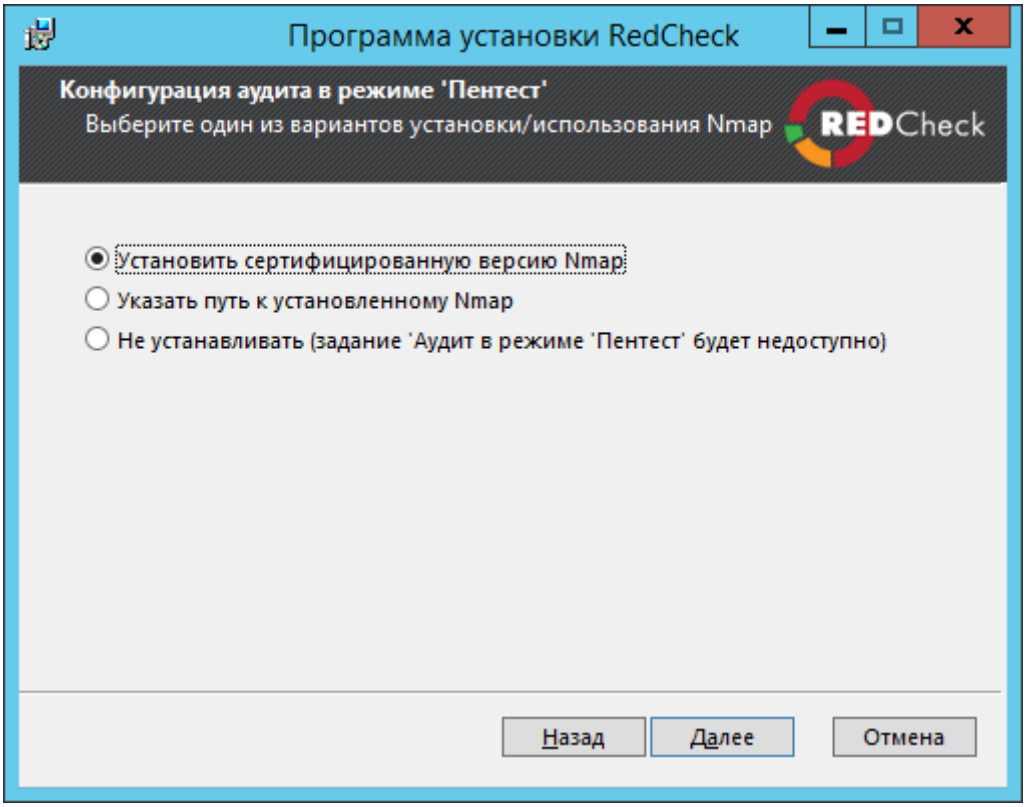


Рисунок 2.4.1

*Для корректной работы **Nmap** в консоли управления RedCheck, необходимыми условиями являются установка следующих пакетов и компонент:*

- *Microsoft Visual C++ 2013 Redistributable (актуальную версию пакета можно скачать с официального сайта - https://www.microsoft.com/ru-RU/download/details.aspx?id=40784, выбрать файл для 32-битной версии: **vcredist_x86.exe;***
- *Microsoft Visual C++ 2015 Redistributable (актуальную версию пакета можно скачать с официального сайта - https://www.microsoft.com/en-US/download/details.aspx?id=48145, выбрать файл для 32-битной версии: **vc_redist.x86.exe**);*
- *Npcap (актуальную версию компонента можно скачать с официального сайта - http://nmap.org, либо установить его из дистрибутива RedCheck).*

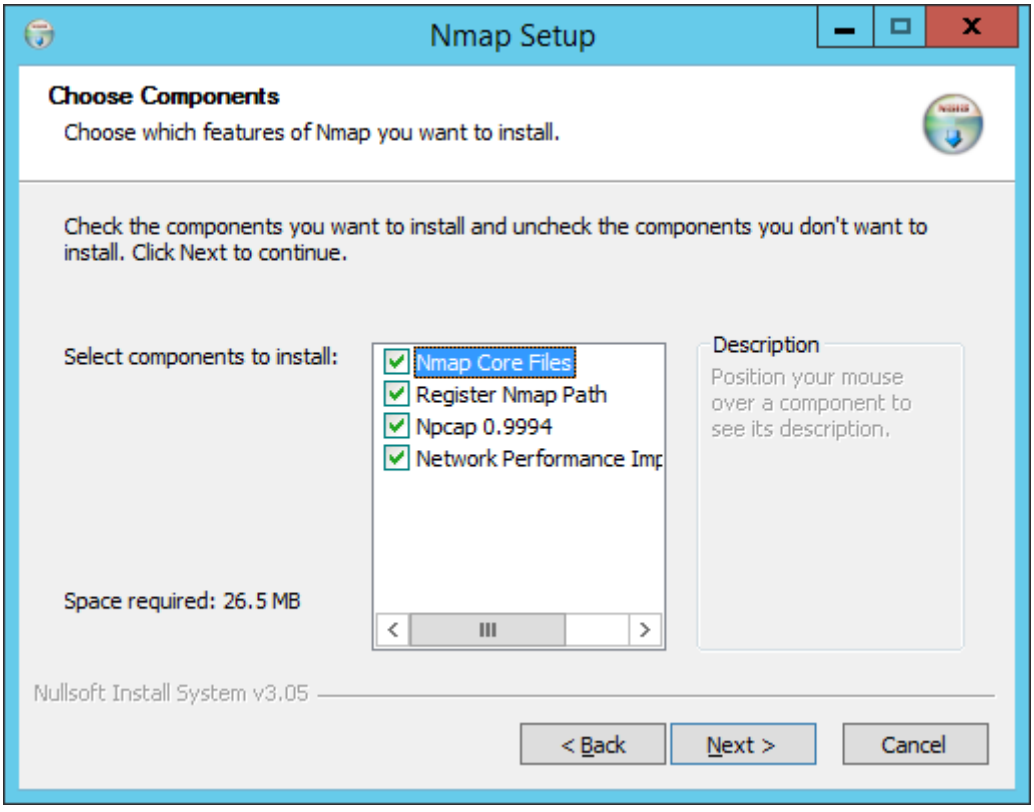


Рисунок 2.4.2

В случае использования Nmap версии отличной от поставляемой в комплекте дистрибутива, некоторые функции могут отсутствовать либо работать не стабильно.

*Все установленные компоненты **Nmap** необходимо добавить в исключения СЗИ от НСД.*

Содержание главы...

2.5 Типы учетных записей для работы с консолью RedCheck

Для работы консоли RedCheck рекомендуется использовать следующие типы учетных записей:

- Учетные записи, запускающие консоль управления RedCheck в сеансе Windows
- Учетные записи для проведения сканирования удаленных хостов (учетные записи сканирования). Они задаются в ***«Менеджере учетных записей»*** и имеют несколько типов - **Windows, Linux, Solaris, Cisco, Huawei, SQL, VMware**, которые используются для различных объектов сканирования и создаются заранее с использованием средств ОС (СУБД SQL Server, Oracle Database, MySQL, PostgreSQL, IBM Db2)
- Учетные записи для установки обновлений. С помощью данного типа УЗ можно производить установку обновлений, на основе проведенного аудита

Содержание главы...

В программе RedCheck присутствует механизм управления доступом пользователей через роли. Где роль - представляет собой набор прав. Для этого в системе создаются дополнительные группы, участникам которых присваиваются определённые права.

Главная идея, данной модели контроля доступа, основана на максимальном приближении логики работы системы к реальному разделению функций персонала в организации.

Понятие роль можно определить, как совокупность действий и обязанностей, связанных с определенным видом активности сотрудников. В данной модели одна и та же роль может использоваться несколькими различными пользователями. Таким образом, модель управления доступом обеспечивает простоту управления и позволяет разделить обязанности.

Основные задачи ролей в программе RedCheck (**Таблица 6**).

Таблица 6

Роль	Задачи
Admins	Участники данной группы обладают неограниченными правами в программе. Им доступен весь перечень операций. Данная группа подойдёт для малых предприятий, где обслуживанием компьютерной сети занимается малый штат сотрудников.
AdminIS	Данная группа предназначена для работы администраторов по информационной безопасности. Её участник может выполнять следующие функции: • Поддерживать систему в рамках выбранной политики

	безопасности • Проверять и обеспечивать целостность данных. • Отслеживать информацию об уязвимостях, обновлениях системы и своевременно принимать меры • Документирование результатов проверок, своей работы
Systems	Учётным записям, входящим в данную группу, будут предоставлены следующие возможности: • Настройка и обновление программы • Инструменты по добавлению хостов и настройке учетных записей • Инструменты по анализу и устранению возможных проблем при работе с программой Можно сделать вывод, что данная роль в первую очередь предназначена для системных администраторов.
Users	Учётным записям, входящим в данную группу, будут предоставлены следую-щие возможности: • Запуск заданий • Просмотр результатов сканирований • Создание отчётов. Данная роль подойдёт для рядового пользователя ИБ, который может прове-рить степень уязвимости машины.

Для организаций, где требуется четкая централизованная система управления доступа, при которой каждый пользователь имеет ровно столько информации сколько ему положено, безопасность и надежность данных является основным приоритетом, необходимо использовать данный метод доступа с иерархией. Обычно - это большие организации, где функции всех ее членов строго регламентированы. Как правило, для данной схемы используются следующие роли: **Systems, AdminIS, Users.**

Systems – это системный администратор, который настраивает программу, а также имеет доступ к учётным данных машин.

AdminIS – это администратор ИБ, который следит за надёжностью сети, машин предприятия, решает какими способами достичь этого.

Users – это пользователь ИБ, который может запустить сканирования, либо посмотреть их результаты, на основе работы проделанной администратором ИБ.

Таблица 7

Роли		Роль - RedCheck*			
		Admins	AdminIS	Systems	Users
Тип операций		Супер пользователь	Админ ИБ	Системный Админ	Пользователь ИБ
Работа с лицензиями		+		+	
Настройки программы		+		+	
Определение учетных данных для сканирования		+		+	
Работа с хостами	Автоматизированный импорт из AD/Nmap/Файлов	+	+	+	
	Ручное создание/удаление хостов	+	+	+	
	Создание/удаление групп/Группировка хостов	+	+	+	
Создание/редактирование/удаление заданий		+	+		
Создание/удаление контроля		+	+		+
Запуск заданий		+	+		+
Построение отчётов		+	+		+

Просмотр аудитов/конфигураций	+	+		+
Синхронизация	+	+	+	+
Импорт OVAL-сигнатур	+	+		
Проверка целостности программы и контента	+	+	+	+
Журнал событий	+	+	+	
Переподключение к службам	+	+	+	+
Перезапуск служб	+	+	+	
Диагностика проблем	+	+	+	+
Справочные элементы, руководство	+	+	+	+

В доменной сети предприятия для реализации ролевой модели необходимо создать глобальные группы безопасности согласно именованию указанной в **Таблице 6**.

С последующим добавлением пользовательских УЗ в группы, согласно их правам доступа в программе.

В случае работы сканера безопасности RedCheck в одноранговой сети, группы безопасности необходимо создавать на локальном хосте где установлен сканер.

Для работы и взаимодействия с агентом сканирования, необходимо создать группу **RedCheck_Admins** на сканируемом хосте и добавить в группу УЗ от имени которой будет происходить сканирование.

 *В том случае, если УЗ пользователя находиться одновременно в нескольких группах, то пользователь будет обладать сумарными, максимальными правами тех групп, в которых состоит его УЗ.*

Содержание главы...

Для работы с консолью администратора программы RedCheck - необходимо настроить рабочую машину. Настройки будут разными, в зависимости от: используется доменная или одноранговая сеть, на предприятии предусмотрено использование иерархического метода доступа пользователей, либо без. Соответствующие настройки приведены в **Таблице 8**.

Таблица 8

Тип сети	Доменная	Одноранговая
1	Учетная запись должна состоять в **глобальной** группе REDCHECK_*, где * - роль RedCheck	Учетная запись должна состоять в **локальной** группе REDCHECK_*, где * - роль RedCheck
2	Учетная запись должна иметь привилегии, равные привилегиям учетной записи локального администратора	

Консоль управления RedCheck может работать, если учетная запись, из-под которой она запущена, не имеет привилегии локального администратора. В таком случае будет ограничен функционал программы: манипуляции со службами, смена лицензии программы.

*Если создать новую группу **REDCHECK_*** и добавить туда пользователя, то после этого необходимо применить изменения на машине: выполнить выход из системы, либо перезагрузку компьютера.*

При планировании работы с программой RedCheck, следует разделять УЗ под которыми осуществляется вход на консоль администратора и для сканирования удаленных хостов.

Содержание главы...

Для работы консоли RedCheck рекомендуется использовать следующие типы учетных записей:

- Учетные записи, запускающие консоль управления RedCheck в сеансе Windows
- Учетные записи для проведения сканирования удаленных хостов (учетные записи сканирования). Они задаются в ***«Менеджере учетных записей»*** и имеют несколько типов - **Windows, Linux, Solaris, Cisco, Huawei, SQL, VMware**, которые используются для различных объектов сканирования и создаются заранее с использованием средств ОС **(СУБД SQL Server, Oracle Database, MySQL, PostgreSQL, IBM Db2)**
- Учетные записи для установки обновлений. С помощью данного типа УЗ можно производить установку обновлений, на основе проведенного аудита

Содержание главы...

С целью удовлетворения требований по стойкости рекомендуются следующие настройки для учетных записей:

- Длина и сложность пароля учетной записи должны удовлетворять требованиям существующей в организации политике безопасности паролей администраторов;
- Срок действия пароля не должен быть ограничен;
- Учетной записи должно быть запрещено изменять свой пароль;

Если политика организации не допускает неограниченных по времени сроков действия пароля - администратор должен действовать по своему усмотрению. Ограничение срока действия пароля приведет к необходимости периодически изменять учетные данные в Консоли управления RedCheck, что делает процедуру работы со сканером менее удобной, хотя и повышает безопасность системы в целом.

Содержание главы...

Настройка сетевого взаимодействия для сканирования Windows-систем с применением агента

1. Если используется доменная ЛВС, то должны быть созданы доменные глобальные группы REDCHECK_ADMINS и Ваша УЗ в ней.

Если сеть одноранговая, то группа (локальная) должна присутствовать на всех хостах ЛВС и сервере с консолью управления RedCheck.

2. Для корректного взаимодействия между консолью управления и агентом RedCheck на хостах необходимо открыть **TCP-порт 8732**. Чтобы открыть порт в стандартном брандмауэре ОС Microsoft Windows (на примере ОС Microsoft Windows 7) следуйте инструкциям ниже:

- Открыть компонент ***«Брандмауэр Windows»***. Нажать кнопку ***«Пуск»*** и выберать пункт ***«Панель управления»***.
- В поле поиска ввести запрос ***«брандмауэр»*** и затем, в списке результатов выберать пункт ***«Брандмауэр Windows»***.
- В области слева выбрать пункт ***«Дополнительные параметры»***. В открывшемся окне кликнуть по пункту ***«Правила для входящих подключений»*** и в области справа нажать на кнопку ***«Создать правило»***.
- Выбрать тип правила ***«Для порта»***.
- Указать тип протокола ***TCP*** и локальный порт ***8732***. В зависимости от метода организации сети указать необходимый профиль.

3. Если в вашей ЛВС установлены сторонние СЗИ от НСД, то необходимо внести RC в исключения.

После изменения настроек необходимо перезагрузить контроллер доменов, хосты и сервер с консолью управления RedCheck.

Настройка сетевого взаимодействия для безагентского сканирования с использованием службы WMI

Для сканирования с использованием службы WMI (без использования агента) требуется обеспечить подключение сканера к службе Windows Management Instrumentation (WMI) сканируемого узла, произвести настройки удаленного доступа, и при необходимости службы DCOM. Настройки могут быть произведены локально на узле или централизованно с помощью групповых политик Windows, а также другими средствами администрирования сети. Ниже приведены локальные настройки сканируемого узла.

Разрешение WMI (локальная настройка)

Открыть компонент *«Брандмауэр Windows»*. Нажать кнопку *Пуск* и выбрать пункт *Панель управления*. В поле поиска ввести брандмауэр и затем выбрать пункт *Брандмауэр Windows*.

В области слева выбрать пункт *«Разрешить запуск программы или компонента через брандмауэр Windows»*.

В поле *«Разрешенные программы и компоненты»* найти строку *«Инструментарий управления Windows (WMI)»*, и поставить флаг в зависимости от метода организации сети: *домен* или *рабочая группа*. Нажать *«ОК»*.

Настройка службы DCOM (при необходимости, по умолчанию в ОС служба DCOM включена)

Для включения и настройки службы DCOM выполнить следующие действия:

- Открыть каталог *C:\Windows\System32*, запустить утилиту *dcomcnfg*. В результате, появится окно *«Службы компонентов»*
- Последовательно открыть закладки: *«Службы компонентов» → «Компьютеры» → «Мой компьютер» → «Свойства»*

- В окне *«Свойства: Мой компьютер»*перейти на вкладку *«Свойства по умолчанию»* и убедиться, что опция *«Разрешить использование DCOM на этом компьютере»* включена
- Перейти на вкладку *«Набор протоколов»* и указать в области *«Протоколы DCOM»* протокол *«TCP/IP с ориентацией на подключения»*
- Если протокол *«TCP/IP с ориентацией на подключения»* не добавлен, нажать *«Добавить»*
- На экране появится окно *«Выбор протокола DCOM»*
- В окне *«Выбор протокола DCOM»* из списка *«Последовательность протоколов»* выбрать протокол *«TCP/IP с ориентацией на подключения»* и нажать *«OK»*

Чтобы настроить удаленный доступ для учетной записи, от имени которой производится сканирование, выполнить следующие действия:

- Перейти на вкладку *«Безопасность COM»*
- В области *«Права доступа»* нажать кнопку *«Изменить ограничения»* и проверить, что выбрана опция *«удаленный доступ»*
- После изменения настроек перезагрузить узел

После изменения настроек перезагрузить хост.

Настройка сетевого доступа

Для проверки и настройки сетевого доступа выполнить следующие действия:

- Запустить оснастку *«Редактор локальной групповой политики»*. Для этого выполнить *(«Пуск» - «Выполнить»)* команду *gpedit.msc.* На экране появится окно оснастки *«Редактор локальной групповой политики»*
- Перейти в каталог: *«Конфигурация компьютера»→ «Конфигурация Windows»→ «Параметры безопасности» → «Локальные политики» → «Параметры безопасности»*
- Выбрать политику *«Сетевой доступ: модель совместного доступа и безопасности для локальных сетевых записей»*

- Через контекстное меню перейти в свойства политики и проверить, что выбрано значение *«Обычная: локальные пользователи удостоверяются как они сами»*

Настройка контроля учетных записей пользователей

Убедиться, что функция контроля учетных записей пользователей (UAC) настроена верно. Можно использовать один из описанных ниже способов:

- Полностью отключить функцию UAC для учетной записи, которая используется для сканирования (не рекомендуется)
- Отключить функцию UAC для всех учетных записей сканируемого узла, но только для удаленных подключений
- Использовать доменную учётную запись (рекомендуется)

Полное отключение UAC

- В командной строке *(«Пуск» - «Выполнить»)* выполнить *msconfig*. На экране появится окно *«Конфигурация системы»*
- В окне *«Конфигурация системы»* перейдити на вкладку *«Сервис»*
- В колонке *«Название средства»* выбрать *«Настройка контроля учетных записей»* и нажать *«Запуск»*
- В открывшемся окне установить положение *«Никогда не уведомлять»* и нажать *«OK»*
- После изменения настроек перезагрузить узел

 *Отключить UAC также возможно без использования GUI, при помощи корректировки определённого ключа реестра.*

Отключение UAC для всех учетных записей сканируемого узла при удаленных подключениях

Выполнить следующие действия:

- В командной строке *(«Пуск» - «Выполнить»)* выполнить *regedit.* На экране появится окно *«Редактор реестра»*

- Перейти в каталог *«Компьютер» - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System»*
- В списке параметров найти **LocalAccountTokenFilterPolicy**. Если параметр отсутствует, щелкнуть правой кнопкой мыши на каталоге *«System»* и выбрать опцию *«Создать»→«Параметр DWORD (32 бита)»*
- Отредактировать параметр *LocalAccountTokenFilterPolicy*, задав значение ключа *«1»* (опция «Изменить в контекстном меню»)
- После изменения настроек перезагрузить узел

Использование доменной учётной записи

Необходимо создать доменную учётную запись (без административных полномочий) и добавить её в группу локальных администраторов сканируемой системы. При использовании такой учётной записи настройки UAC не будут влиять на сканирование. Данный вариант настройки UAC является предпочтительным

Настройка сетевого взаимодействия для сканирования с использованием службы Remote Engine (WinRM)

Windows Remote Management **(WinRM)** - реализация компанией Microsoft протокола WS-Management для удаленного управления узлами сети. Отличительным преимуществом реализации для систем на платформе Windows является возможность создания Shell сессии на удаленном узле и выполнение команд и скриптов на языке сценариев PowerShell.

Для сканирования методом **WinRM** требуется настройка как сервера RedCheck, так и сканируемого узла.

- *Windows PowerShell присутствует в составе Windows 7\Windows Server 2008 R2 и более поздних версий Windows. Для более ранних версий Windows необходимо отдельно скачать и установить Windows PowerShell на все сканируемые узлы.*

- *Windows Remote Management присутствует в составе Windows VistaIWindows Server 2008 и более поздних версий Windows. Для более ранних версий Windows необходимо отдельно скачать и установить пакет Windows Management Framework.*
- *Дальнейшие настройки необходимо производить из консоли PowerShell, запущенной от имени Администратора.*

Настройка сервера управления RedCheck

Следующие команды позволяют выполнить подключение к серверу по протоколу **HTTP** или **HTTPS**.

Для HTTP:

Enter-PSSession -ComputerName Host -Port 5985 -Credential User

Enter-PSSession -ComputerName Host -Credential User

Для HTTPS:

Enter-PSSession -ComputerName Host -Port 5986 -Credential User -UseSSL

Enter-PSSession -ComputerName Host -Credential User -UseSSL

На сервере управления RedCheck требуется определить доверенные сканируемые хосты, выполнив в командной строке следующую строку:

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

предварительно можно проверить настройки клиента WinRM с помощью:

winrm get winrm/config/client

В случае возникновения проблем с подключением рекомендуется следовать руководству, расположенному по адресу https://technet.microsoft.com/ru-ru/library/hh847850.aspx.

Настройка сканируемого узла

1. Необходимо включить службу ***Windows Remote Management (WS-managment) / Служба удаленного управления Windows*** и открыть порты для работы WinRM-туннеля.

WinRM-туннель по умолчанию использует порт 5985 для HTTP-соединения и 5986 для HTTPS-соединения. В RedCheck присутствует возможность задать произвольный порт для WinRM от 1 до 65535.

Для установки настроек по умолчанию можно вызвать специальную утилиту для автоматического конфигурирования, выполнив в командной строке: ***winrm qc***

Для этого при создании учетной записи Windows необходимо включить параметр ***«Указать WinRM порт»*** и задать номер порта.

Для изменения номера порта существующей учетной записи в консоли RedCheck необходимо открыть ***«Инструменты» - «Менеджер учетных записей»***, нажатием правой кнопкой мыши на необходимую учетную запись Windows вызвать контекстное меню и выбрать пункт ***«Редактировать»***, после чего включить параметр ***«Указать WinRM порт»*** и задать номер порта.

2. Расширить квоту по использованию памяти с 150 Мб (по умолчанию) до рекомендованных 2 Гб, для стабильной работы «Remote Engine». Для этого нужно в оболочке PowerShell выполнить следующую команду: ***Set-Item wsman:localhost\Shell\MaxMemoryPerShellMB 2048***

Для корректного взаимодействия между консолью управления и агентом RedCheck на хостах необходимо открыть используемый WinRM порт на входящие подключения (по умолчанию - **порт 5985** для HTTP, **порт 5986** для HTTPS).

Таблица 9

	Тип сети	
Тип	Одноранговая	Доменная

сканирования		
Безагентский метод сканирования	Учетная запись должна состоять в локальной группе «Администраторы» или группе, предоставляющей аналогичные привилегии доступа к файловой системе, реестру Windows и WMI	Учетная запись должна состоять в группе «Администраторы домена» или группе, предоставляющей аналогичные привилегии доступа к файловой системе, реестру Windows и WMI
Сканирование с помощью агента RedCheck	Учетная запись должна состоять в локальной группе безопасности REDCHECK_ADMINS.	Учетная запись должна состоять в глобальной группе безопасности REDCHECK_ADMINS.
Сканирование с помощью Агента WinRM	Учетная запись должна состоять в локальной группе Администраторы» или группе, предоставляющей аналогичные привилегии доступа к файловой системе, реестру Windows и WinRM. Необходимо настроить Windows Remote Management. В свойствах учетной записи должен быть задан порт.	Учетная запись должна состоять в локальной группе Администраторы» или группе, предоставляющей аналогичные привилегии доступа к файловой системе, реестру Windows и WinRM. Необходимо настроить Windows Remote Management. В свойствах учетной записи должен быть задан порт.

Содержание главы...

В организациях с большим количеством машин в сети - увеличивается число уникальных учетных записей. Как следствие, чтобы провести сканирование определённой группы хостов приходится создавать несколько заданий.

Если на компьютере была изменена УЗ, то задание не может выполниться из-за проблемы с аутентификацией.

RedCheck позволяет избежать этих ситуаций, благодаря режиму **«Использовать сохраненные учетные данные при наличии»**.

Данная опция выбирается на этапе **«Учетные данные задания»**, во время создания новой задачи. Она позволяет использовать сведения **«по умолчанию»**, и заранее указанные учетные записи для каждого из хостов. Также будут учитываться ранее успешно выполненные сканирования.

Задать привязку УЗ к машине можно через меню Редактирование: ***«Вкладка Хосты»*** - вызвать контекстное меню на интересующей машине - ***Редактировать*** - вкладка ***«Учетные данные».***

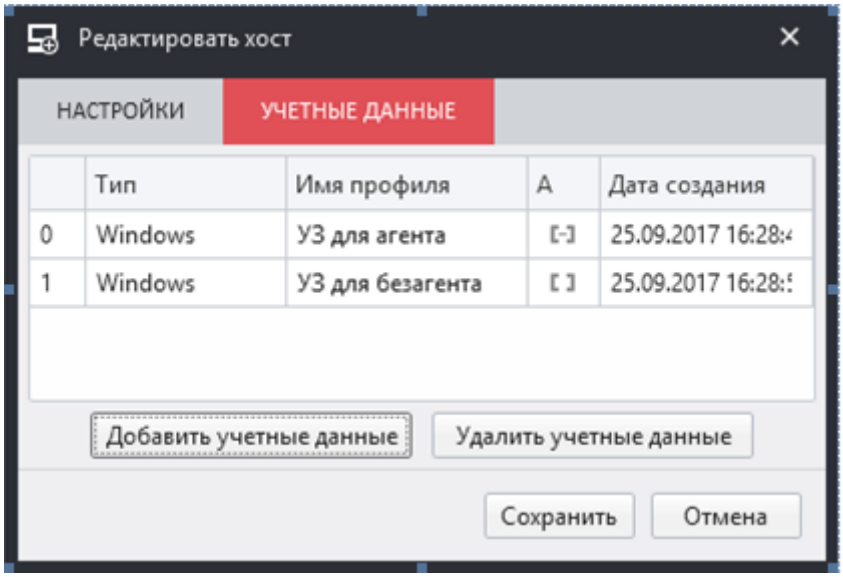


Рисунок 2.5.2.3.1

УЗ может быть использована только для того типа сканирования, для которого была добавлена. Если УЗ позволяет выполнять несколько режимов - нужно добавить для каждого из них.

Содержание главы..

При сканировании Linux-систем (сканирование осуществляется по безагентской технологии) в качестве транспорта используется **SSH-протокол** не ниже версии 2 с включенным модулем поддержки протокола **SFTP**.

Для проведения сканирования RedCheck требуется, чтобы пользователь, от имени которого выполняется сканирование, имел права ***root*** или возможность использовать ***Sudo***, для повышения привилегий.

Для сканирования удаленной системы могут использоваться следующие типы учетных записей:

- учетная запись суперпользователя
- учетная запись привилегированного пользователя
- учетная запись непривилегированного пользователя

 *Использование учетной записи привилегированного пользователя является рекомендуемым типом учетной записи для сканирования удаленной системы.*

 *Для сканирования удаленной системы в качестве основного транспорта используется протокол SSH. Убедитесь, что SSH-сервер установлен и настроен, а выбранная учетная запись пользователя имеет возможность подключения к удаленной системе по протоколу SSH. Осуществить проверку подключения можно с помощью любого удобного SSH-клиента.*

 *Если на целевом хосте включен режим "bracketed paste mode", то необходимо его принудительно выключить, для УЗ с правами которой выполняется сканирование удаленного хоста, для этого:*

1. *Войти под этой УЗ на хост;*

2. *Выполнить команду echo "set enable-bracketed-paste off" >> ~/.inputrc;*
3. *Перезайти на хост с правами этой УЗ;*
4. *Проверить, что изменения вступили в силу bind -v | grep bracketed.*

Для сканирования удаленной системы, допускается использовать существующую учетную запись пользователя **Linux**, либо необходимо создать отдельную учетную запись.

В общем случае, для создания отдельной учетной записи пользователя с именем *redcheck* (как пример, наименование учетной записи может быть произвольное) на удаленной системе необходимо выполнить следующую команду: **adduser redcheck**

Задайте пароль для вновь созданной учетной записи пользователя с помощью команды: ***passwd redcheck***

Криптография

- 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 узла:

- RSA
- DSS
- ED25519
- ECDsaNistP256
- ECDsaNistP384
- ECDsaNistP521

Поддерживаемые алгоритмы имитовставки:

- MD5
- SHA1
- SHA256
- SHA512

Аутентификация

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

Перечень выполняемых команд, в момент сканирования:

- printf
- dirname
- basename
- bash
- find
- grep
- sudo
- ls
- env
- echo
- sort
- rpm
- dpkg
- dpkg-query
- ps
- uniq
- nginx
- apachectl
- php
- cat
- stat
- systemctl
- uname
- sysctl
- getent
- last
- date
- getfacl

- lsb_release
- dmidecode
- ip
- mktemp
- chmod
- rm
- md5sum
- sha1sum
- sha512sum
- ufix

Настройка учетной записи суперпользователя

Данный тип учетной записи пользователя предназначается для использования при необходимости получения всех данных и полной оценке защищенности удаленной системы и/или в случаях, когда невозможно использовать другие типы учетных записей.

По умолчанию в Linux-системах учетная запись суперпользователя имеет имя ***root***.

 *Программа не накладывает ограничений на использование **root** в качестве учетной записи суперпользователя. Допустимо использовать любую другую учетную запись суперпользователя с отличным от root именем, если таковые существуют на удаленной системе.*

По умолчанию на некоторых Linux-системах учетная запись суперпользователя ***root*** может быть неактивна. Чтобы активировать учетную запись суперпользователя ***root***, выполните команду смены пароля: ***passwd root***

По умолчанию 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.

Для настройки SSH-сервера отредактируйте конфигурационный файл, добавив в него следующую директиву со значением: ***PermitRootLogin yes***

 *По умолчанию конфигурационный файл SSH-сервера имеет имя/etc/ssh/sshd_config.*

Конфигурационный файл SSH-сервера уже может содержать директиву*PermitRootLogin*. В таком случае просто измените значение директивы на *yes*.

Если политика безопасности в отношении данной системы не позволяет использование учетной записи суперпользователя, необходимой для осуществления сканирования, воспользуйтесь другими типами учетных записей пользователя.

Настройка учетной записи привилегированного пользователя

Данный тип учетной записи пользователя является рекомендуемым для всех случаев сканирования удаленных систем.

Здесь и далее подразумевается, что настраиваемая учетная запись пользователя уже существует на удаленной системе.

Для сканирования удаленной системы с помощью данного типа учетной записи, у пользователя требуется наличие прав на выполнение ***sudo,*** на удаленной системе. Если программа ***sudo*** отсутствует на удаленной машине, необходимо выполнить ее установку или воспользоваться другими типами учетных записей.

 *По умолчанию на большинстве Linux-систем уже установлена программа sudo. Для проверки наличия программы sudo на удаленной системе выполните команду: sudo -V.*

Настройка учетной записи непривилегированного пользователя

Данный тип учетной записи предназначается для использования только при необходимости получения данных, не требующих для своего доступа отдельных прав, и не может применяться для полной оценки защищенности удаленной системы.

Здесь и далее подразумевается, что настраиваемая учетная запись пользователя уже существует на удаленной системе.

Для сканирования удаленной системы с помощью данного типа учетной записи пользователя дополнительных настроек не требуется.

Содержание главы..

Для сканирования удаленной системы в качестве основного транспорта используется протокол **SSH**. Убедитесь, что **SSH-сервер** установлен и настроен, а выбранная учетная запись пользователя имеет возможность подключения к удаленной системе по протоколу SSH. Осуществить проверку подключения можно с помощью любого удобного **SSH-клиента.**

Для сканирования удаленной системы, допускается использовать существующую учетную запись пользователя Solaris, либо необходимо создать отдельную учетную запись.

Содержание главы...

Для сканирования **Cisco IOS** (сканирование осуществляется по безагентской технологии) в качестве транспорта для сканирования используется **SSH- протокол** (по умолчанию 22 порт).

Для проведения сканирования RedCheck требуется, чтобы пользователь, от имени которого выполняется сканирование, имел возможность перехода в привилегированный режим.

Для сканирования должна использоваться учетная запись пользователя с возможностью перехода в привилегированный режим с вводом пароля **«Enable»**.

Использование учетной записи с возможностью перехода в привилегированный режим является рекомендуемым типом учетной записи при любом типе сканирования удаленной системы.

Для сканирования оборудования Cisco существует возможность использовать учетную запись без возможности перехода в привелигированный режим и ввода пароля ***«Enable».***

Для реализации такого типа сканирования, необходимо дополнительно настраивать разрешающие правила для учетной записи.

Для сканирования удаленной системы в качестве транспорта используется протокол SSH. Перед проведением сканирования, убедиться, что служба **SSH** включена и настроена, а выбранная учетная запись пользователя имеет возможность подключения к удаленной системе по протоколу SSH. Осуществить проверку подключения можно с помощью любого удобного SSH-клиента.

Криптография

- 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 узла:

- RSA
- DSS
- ED25519
- ECDsaNistP256
- ECDsaNistP384
- ECDsaNistP521

Поддерживаемые алгоритмы имитовставки:

- MD5
- SHA1
- SHA256

- SHA512

Аутентификация

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 удаленной системы допускается использование непривелигированной учетной записи, созданной на оборудовании Cisco IOS. Для такой учетной 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 *(enable)* режиме:

- show file information
- show running-config all
- show logging
- show snmp group
- show startup-config

Содержание главы...

Сканирование **Huawei VRP** осуществляется по безагентской технологии. Для сканирования должна использоваться учетная запись пользователя с возможностью перехода в привилегированный режим с вводом пароля ***«super»*** и указанием уровня доступа данного пользователя используемого для конкретного типа оборудования, но не ниже 3-го.

Для сканирования удаленной системы в качестве транспорта используется протокол **SSH**, порт по умолчанию **TCP:22**. Перед проведением сканирования, убедиться, что служба **SSH** включена и настроена, а выбранная учетная запись пользователя имеет возможность подключения к удаленной системе по протоколу **SSH**. Осуществить проверку подключения можно с помощью любого удобного **SSH-клиента**.

Для сканирования удаленной системы допускается использование либо существующей учетной записи пользователя **Huawei**, либо создание отдельной учетной записи.

Аналогичные настройки учетных 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

Содержание главы...

Для возможности сканирования **СУБД Microsoft SQL Server**, в экземпляре СУБД может использовать режим проверки подлинности Windows или режим проверки подлинности SQL Server и Windows. Созданная для сканирования учетная запись должна быть добавлена в консоль управления RedCheck.

*Минимальные требования для учетной записи: роль сервера - «**public**» учётная запись должна быть включена для базы данных «**master**»*

*Учетная запись **sa** часто становится мишенью злоумышленников. Не включайте её, если это не требуется для работы приложения. Помните, что для имени входа **sa** очень важно использовать надежный пароль.*

Содержание главы..

Для возможности сканирования **СУБД Oracle**, в экземпляре СУБД должен использоваться смешанный тип аутентификации (проверка подлинности Oracle).

По умолчанию, для сканирования **СУБД Oracle** используется порт **1521**.

В случае использования альтернативного порта, в инфраструктуре сети, необходимо указать соответствующий.

Созданная для сканирования учетная запись должна быть добавлена в консоль управления RedCheck.

Для сканирования СУБД допускается использование непривилегированной учетной записи. Такой учетной записи потребуется предоставить необходимые разрешения, выполнив указанные ниже команды, от имени привилегированного пользователя:

```
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>,

где <USER NAME> - имя непривилегированной учетной записи.

Содержание главы...

Для возможности сканирования **СУБД MySQL**, в экземпляре СУБД должен использоваться смешанный тип аутентификации (проверка подлинности MySQL).

Созданная для сканирования учетная запись должна быть добавлена в консоль управления RedCheck.

Содержание главы...

Общая информация

Поддерживаются все редакции указанных, в п. 1.8 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**.

Общий перечень команд выполняемых при сканировании **VMware ESXi Server и vCenter Server**:

- Login
- Logout
- RetrieveServiceContent
- ContinueRetrievePropertiesEx
- RetrievePropertiesEx
- CreateContainerView
- DestroyView
- HostImageConfigGetAcceptance
- HostImageConfigGetProfile
- QueryLockdownExceptions
- RetrieveHostAccessControlEntries
- Команда выполняемая при сканировании VMware ESXi Server:
- VimEsxCLIsoftwareviblist

При сканировании **VMware ESXi Server и VMware vCenter Server** заданием типа ***«Фиксация»*** в качестве транспорта используется **SSH**-протокол не ниже версии 2 с включенным модулем поддержки протокола **SFTP**.

Используемая технология доступа к данным - **VMware Infrastructure Management (VIM)**.

Настройка сетевого взаимодействия сканирования VMware ESXi Server

Для проведения сканирования **VMware ESXi Server** посредством RedCheck требуются:

- Активированная лицензия на продукт с включенной в нее ***feature vSphere API***
- Наличие учетной записи ***root***
- Присутствие учетной записи пользователя состоящей в группе Администраторы, а так же добавленный в список исключений ***Lockdown Mode***
- Редакция RedCheck не ниже Professional

Для проведения сканирования **VMware ESXi Server** посредством RedCheck заданием типа ***«Фиксация»***, помимо обозначенных выше, требуются:

- 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
- Редакция RedCheck не ниже Professional

 *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***

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

Рисунок 2.5.2.11.1

На сервере **ESXi**, нажать клавишу *F2* и авторизуйтесь при помощи учетной записи *root*.

Рисунок 2.5.2.11.2

В меню *System Customization* выбрать *Troubleshooting Options*.

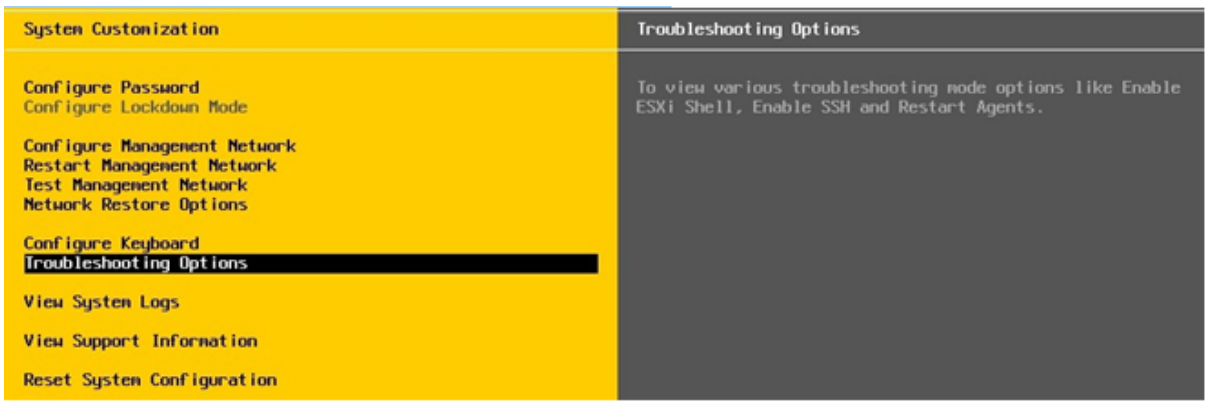


Рисунок 2.5.2.11.3

В разделе *Troubleshooting Mode Options* выбрать пункт *Enable SSH*, включить.

Рисунок 2.5.2.11.4

Для возврата в основное меню, нажать *ESC*.

Включение SSH при помощи веб-клиента vSphere

Запустите браузер, ввести в адресной строке адрес *VMware* сервера, перейти и авторизоваться на сервере *ESXi* через интерфейс **vSphere Web Client.**

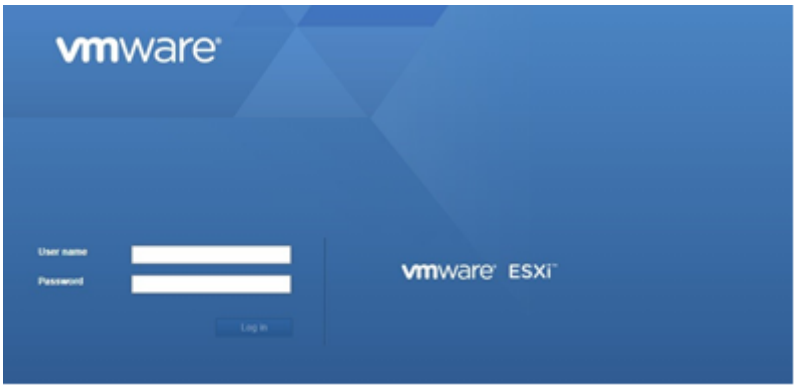


Рисунок 2.5.2.11.5

В открывшемся окне выбрать *Host - Actions*.

В выпадающем меню выбрать *Services - Enable Secure Shel (SSH)*.

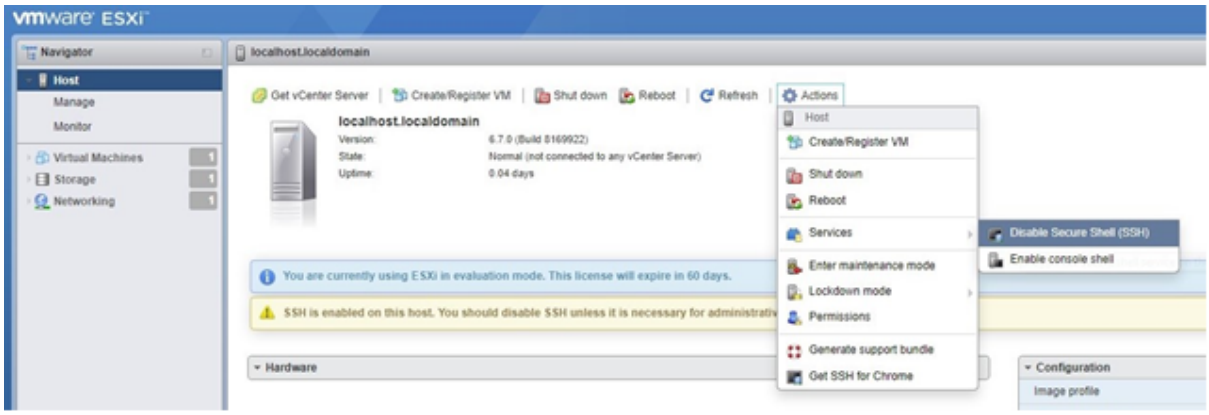


Рисунок 2.5.2.11.6

Так же, активировать SSH можно через вкладку меню **Manage - Services**.

Найдите в списке служб **TSM-SSH**, **ПКМ вызвать контекстное меню - Start.**

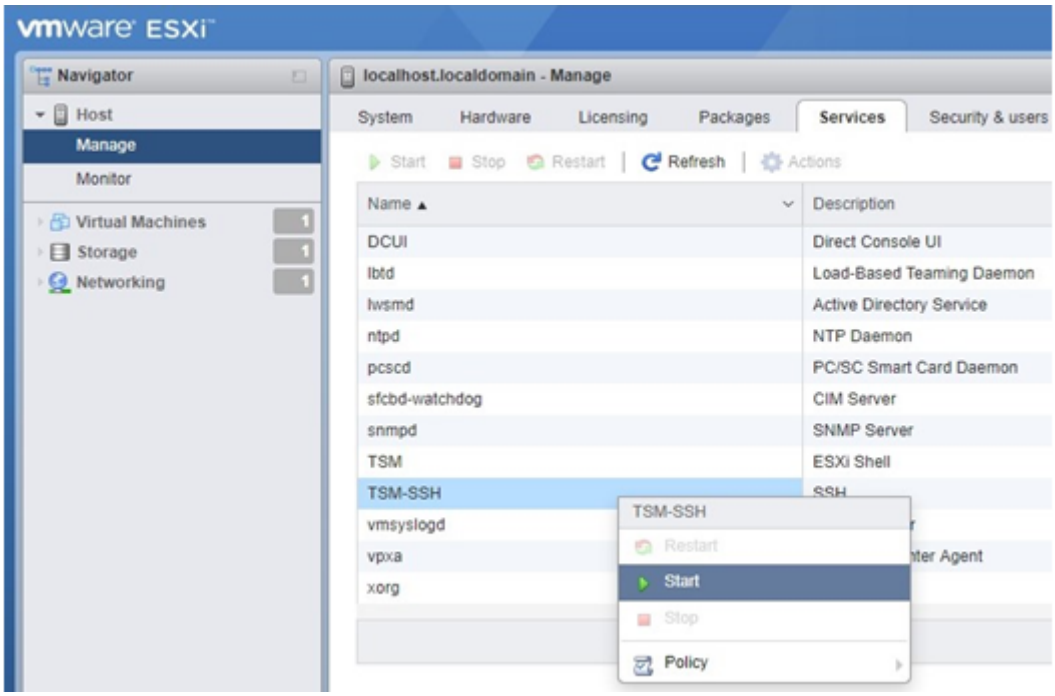


Рисунок 2.5.2.11.7

Настройка SSH-туннеля завершена.

Настройка сетевого взаимодействия для сканирования VMware vCenter Server

Для проведения сканирования **VMware vCenter Server** посредством RedCheck требуются:

- Активированная лицензия на продукт с включенной в нее feature vSphere API
- Наличие учетной записи администратора (администратора или **root** для задания типа ***«Фиксация»***)
- Редакция RedCheck не ниже Professional

Для проведения сканирования **VMware vCenter Server** посредством RedCheck заданием типа ***«Фиксация»***, помимо обозначенных выше, требуются*:*

- 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;
- Редакция RedCheck не ниже Professional.

 *Перед началом сканирований, рекомендуется проверить доступность соответвущего туннеля для каждого из хостов, участвующих в проверке, посредством функции **«Пинг»**, для заданной учетной записи.*

Сканирование удаленной **VMware**-системы осуществляется по безагентской технологии.

Для сканирования **VMware ESXi Server** заданиями типа *«Аудит обновлений»*, *«Аудит уязвимостей»*, *«Аудит конфигураций»* и *«Инвентаризация»* необходимо использовать учетную запись пользователя **VMware ESXi Server**. Для сканирования **VMware vCenter Server** в режимах *«Аудит обновлений»*, *«Аудит уязвимостей»*, *«Аудит конфигураций»* и *«Инвентаризация»* необходимо использовать учетную запись пользователя **VMware vCenter Server**.

Для сканирования **VMware vCenter Server и VMware ESXi Server** заданием типа ***«Фиксация»*** необходимо использовать учетную запись пользователя Linux.

Созданная для сканирования учетная запись должна быть добавлена в консоль управления RedCheck.

Настройка сетевого взаимодействия сканирования VMware NSX Data Center for vSphere

При сканировании **VMware NSX Data Center for vSphere** в качестве транспорта используется протокол **HTTPS**.

Для проведения сканирования **VMware NSX Data Center for vSphere** посредством RedCheck требуются:

- Наличие включенной учетной записи ***Auditor***
- Проверка доступности транспорта внешними средствами (пример: ***Postman***)

- Редакция RedCheck не ниже Professional

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

Содержание главы...

Сканирование СУБД **Postgre SQL** осуществляется по технологии агента и **WinRM** для Windows и по безагентской технологии для Linux-систем.

Для сканирования сервера **PostgreSQL** необходимо создать учетную запись (создадим ***«RedCheckPG»***), с правами достаточными для выполнения запросов. Минимальная настройка прав представлена в **Таблице 10**:

Таблица 10

API	Объект
SELECT	pg_settings
	pg_roles
	pg_database
	pg_user
	pg_class
	pg_authid
	pg_shadow
EXECUTE	has_schema_privilege('public','public','create')

Созданная для сканирования учетная запись должна быть добавлена в консоль управления RedCheck. Алгоритм работы с учетными записями в RedCheck описан в разделе **Добавление учетных записей**.

В файл *«pg_hba.conf»*, который находится по следующему пути:

- для Windows-систем *C:\Program Files\PostgreSQL\9.6\data*
- для Linux-систем: */var/lib/pgsql/data/*

необходимо добавить строку:

host all RedCheckPG 192.168.10.1/32 md5

 *Это минимальная рекомендация по настройке аутентификации. Данное значение рекомендуется настраивать согласно политике безопасности, используемой на предприятии.*

Содержание главы...

Сканирование СУБД **IBM Db2** осуществляется по технологии агента и **WinRM** для Windows и по безагентской технологии для Linux-систем.

 *Для сканирования СУБД на сервер с консолью управления RedCheck необходимо установить IBM Data Server Client!*

Созданная для сканирования учетная запись должна быть добавлена в консоль управления RedCheck. Алгоритм работы с учетными записями в RedCheck описан в разделе 5.1.2.

Содержание главы...

Сканирование СУБД **SAP HANA** осуществляется по по безагентской технологии для Linux-систем.

 *Для сканирования СУБД на сервер с консолью управления RedCheck необходимо установить SAP HANA Database Client!*

Созданная для сканирования учетная запись должна быть добавлена в консоль управления RedCheck. Алгоритм работы с учетными записями в RedCheck описан в разделе 5.1.2.

Содержание главы...

Для сканирования **Check Point** (сканирование осуществляется по безагентской технологии) в качестве транспорта для сканирования используется **SSH**- протокол (по умолчанию **22 порт**).

Перечень команд выполняемых при сканировании **Check Point** :

- show version all
- show software-version
- show interfaces
- show asset all
- cpinfo -y all
- cpstat os

Содержание главы...

3. Обновление консоли управления RedCheck

Алгоритм обновления консоли:

1. Любым доступным ПО, сделать **backup** Вашей базы данных RedCheck.
2. Скачать необходимый дистрибутив ***RedCheck.msi***: https://portal.altx-soft.ru/downloads/.
3. Запустить установку дистрибутива ***RedCheck.msi*** и следовать инструкциям мастера установки (в случае обновления программы, вводить номер лицензии, имя сервера и учетные данные экземпляра уже не требуется, программа самостоятельно их проставит).
4. После установки необходимо перезапустить сервер с установленной программой.

 *В случае обновления RedCheck 2.1.1 до текущей версии, необходимо удалить текущий экземпляр RedCheck с сохранением БД и данных приложения!*

При обновлении консоли управления RedCheck, рекомендуется обновить **RedCheckAgent** на целевых хостах. Обратная совместимость с агентами более старых версий поддерживается, но в случае возникновения проблем, они могут быть устранены в агенте с версией, аналогичной версии сканера RedCheck. Удаление «старого» **RedCheckAgent**, при обновлении, не требуется!

4. Интерфейс программы

4.1.1 Графический интерфейс

Графический интерфейс консоли управления RedCheck (Рисунок 4.1.1.1) состоит из следующих элементов:

- **Вкладки** *(Главная, Хосты, Задания, История, Контроль, Отчеты)*
- **Пункты меню** (*Действия, Инструменты, Справка*)
- **Статусная панель**

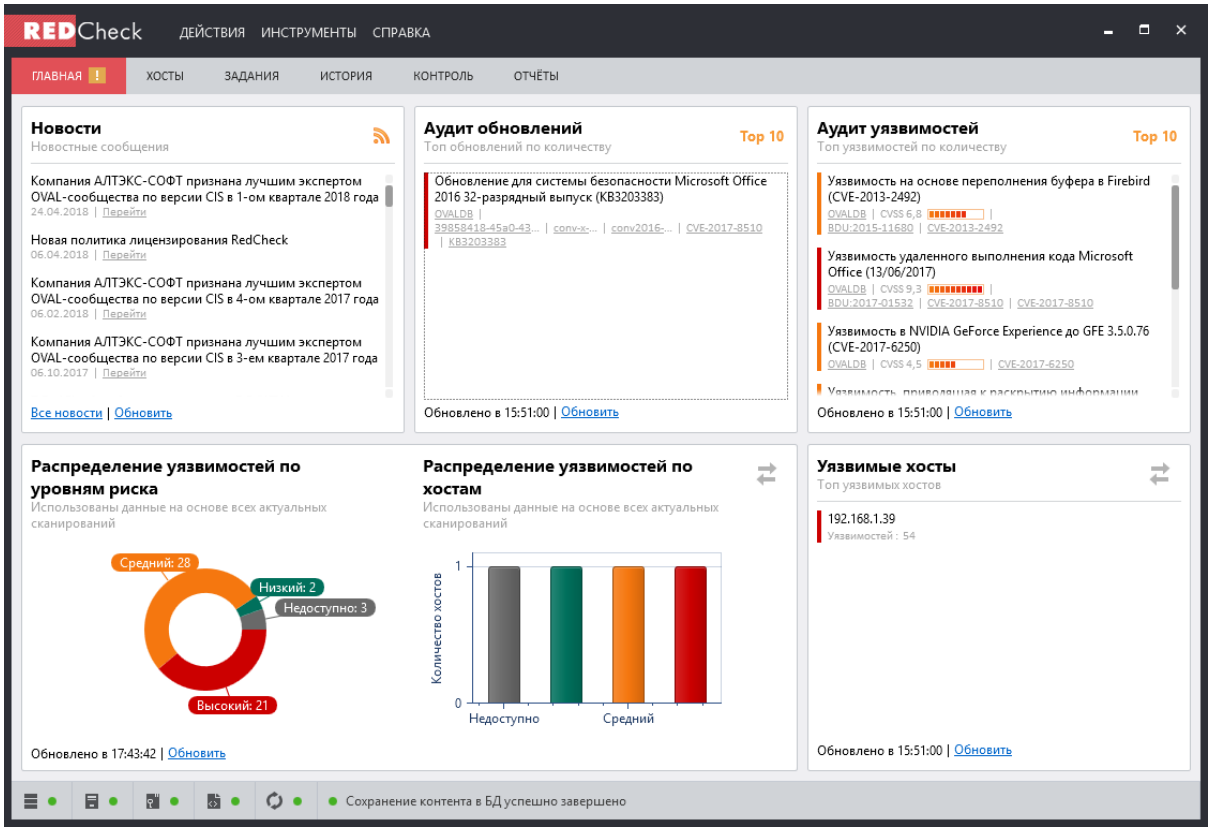


Рисунок 4.1.1.1

Содержание главы...

4.1.2 Статусная панель

В нижней части рабочего окна консоли управления находится специальная панель (Рисунок 4.1.2.1), на которой отображаются статусы основных компонентов RedCheck.

Рисунок 4.1.2.1

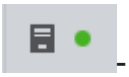
Статус подключения к БД

 - данный статус показывает результат проверки соединения консоли RedCheck с базой данных.

Зеленый маркер означает, что проверка соединения с БД прошла успешно.

Красный маркер означает, что соединиться с БД не удалось.

Статус подключения к службе сканирования

 - данный статус показывает результат проверки подключения к службе сканирования.

Зеленый маркер означает, что проверка подключения к службе сканирования прошла успешно.

Красный маркер означает, что подключение к службе сканирования не удалось.

*Красный маркер подключения к службе сканирования может проявляться, если с момента установки сканера RedCheck до первого запуска консоли не были произведены **«Выход из системы»** либо перезагрузка компьютера.*

Статус лицензии

 - данный статус показывает результат проверки лицензии. Проверка лицензии выполняется на уровне сервера лицензирования.

Зеленый маркер означает, что лицензия прошла проверку и является валидной.

Красный маркер означает, что лицензия была введена неверно, либо закончился срок ее действия.

Подробное описание лицензирования программы в **разделе 1.3.** настоящего Руководства.

Статус контента

 - данный статус показывает актуальность контента.

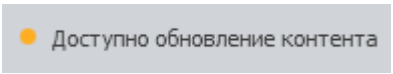
Зеленый маркер означает, что контент содержит последние обновления.

Оранжевый маркер означает, что контент на рабочей машине должен обновиться до более свежих баз, расположенных на сервере. Также, данный статус может говорить о том, что базы не обновлялись более 2х недель.

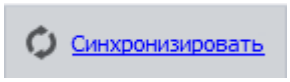
Красный маркер означает, что контент недоступен или отсутствует.

Статус проверки обновления контента

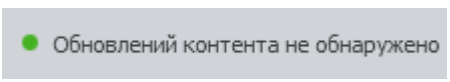
В зависимости от результатов проверки статус может принимать несколько значений:



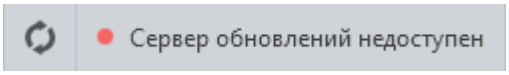
- контент на сервере обновлений отличается от контента, присутствующего в БД RedCheck.



- необходимо нажать для обновления контента.

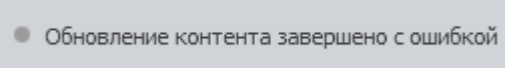


- В БД находится актуальный контент. Никаких дополнительных действий выполнять не нужно.



- возникла ошибка соединения с сервером обновлений. Необходимо проверить корректность настройки сетевого подключения, прокси-сервера.

- запись о времени последней синхронизации отсутствует. Такой статус возможен при первичной установке программы, либо после переустановки. Необходимо произвести синхронизацию.



- данный статус отображается, если при синхронизации с сервером обновлений возникла ошибка. Как правило, данная проблема возникает, если отсутствует доступ к серверу обновлений, поэтому необходимо проверить сетевое подключение.

Содержание главы...

4.2 Вкладки программы

Вкладка **«Главная»** (стартовая вкладка) содержит 5 информативных окон (фреймов):

- ***«Новости»***

В данном фрейме публикуются новости о RedCheck, репозитории OVALdb и деятельности компании АЛТЭКС-СОФТ, связанной с деятельностью в области разработки и применения средств анализа защищенности. Содержимое ленты загружается (в формате RSS) с новостного раздела сайта altx-soft.ru (Рисунок 4.2.1.1).

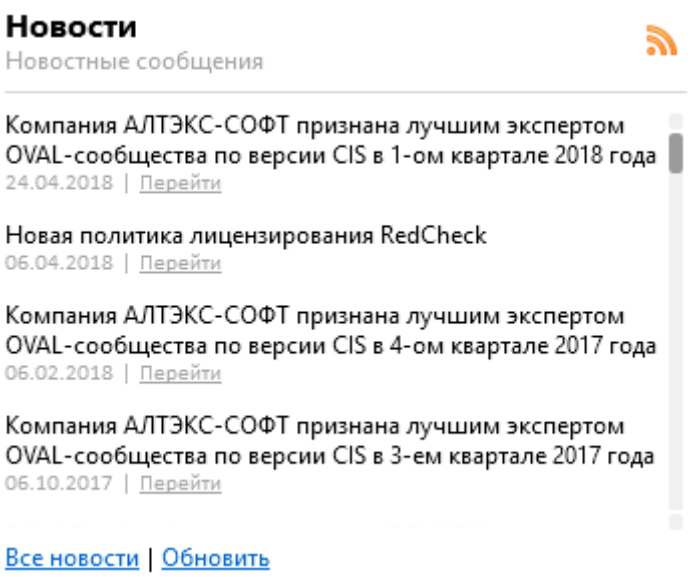


Рисунок 4.2.1.1

- ***«Аудит обновлений»***

Отображает десять наиболее критичных обновлений безопасности, выявленных при сканировании компьютеров за последнее время (Рисунок 4.2.1.2).

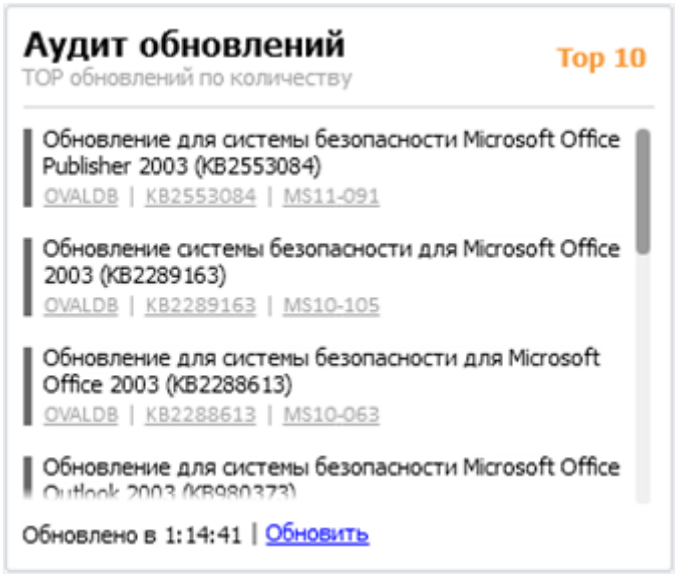


Рисунок 4.2.1.2

- *«Аудит уязвимостей»*

Отображает десять наиболее критичных уязвимостей, найденных на компьютерах пользователей за последнее время (Рисунок 4.2.1.3).

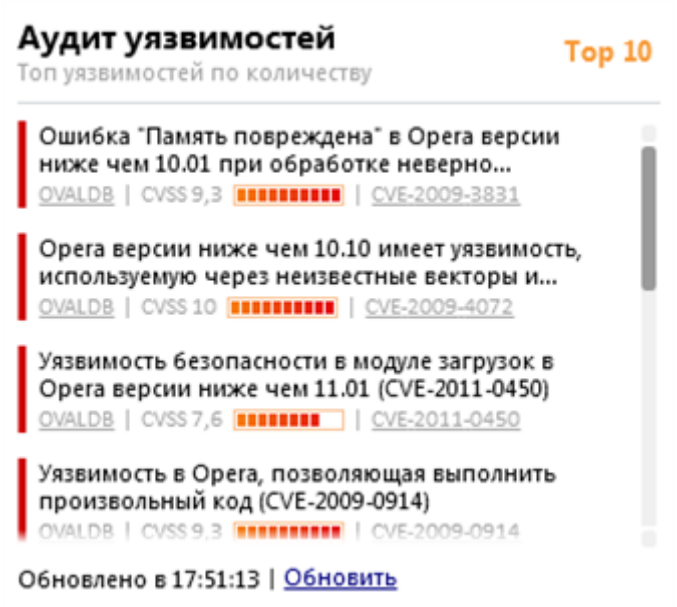


Рисунок 4.2.1.3

- *«Распределение уязвимостей по уровням»*

Отображает диаграмму, наглядно демонстрирующую процентное соотношение уязвимостей в зависимости от их вектора атаки в градации CVSS (Рисунок 4.2.1.4).

Рисунок 4.2.1.4

- *«Распределение уязвимостей по хостам»*

Отображает соответствие количества сканируемых хостов уязвимостям разных уровней риска (Рисунок 4.2.1.5).

Рисунок 4.2.1.5

- *«Распределение обновлений по уровням»*

Отображает диаграмму, наглядно демонстрирующую процентное соотношение уязвимостей в зависимости от их вектора атаки в градации CVSS (Рисунок 4.2.1.6).

Рисунок 4.2.1.6

- **«Распределение обновлений по хостам»**

Отображает соответствие количества сканируемых хостов неустановленным обновлениям разных уровней риска (Рисунок 4.2.1.7).

Рисунок 4.2.1.7

*Переключить режим отображения **«Распределение уязвимостей по уровням»**, **«Распределение уязвимостей по хостам»** и **«Распределение обновлений по уровням», «Распределение обновлений по хостам»** можно с помощью кнопки , расположенной в правом верхнем углу информативного окна (Рисунок 4.2.1.5 , Рисунок 4.2.1.7).*

«Необновленные/Уязвимые хосты». Отображает топ необновленных и уязвимых хостов.

Переключить режим отображения можно с помощью кнопки , расположенной в правом верхнем углу информативного окна (Рисунок 4.2.1.8).

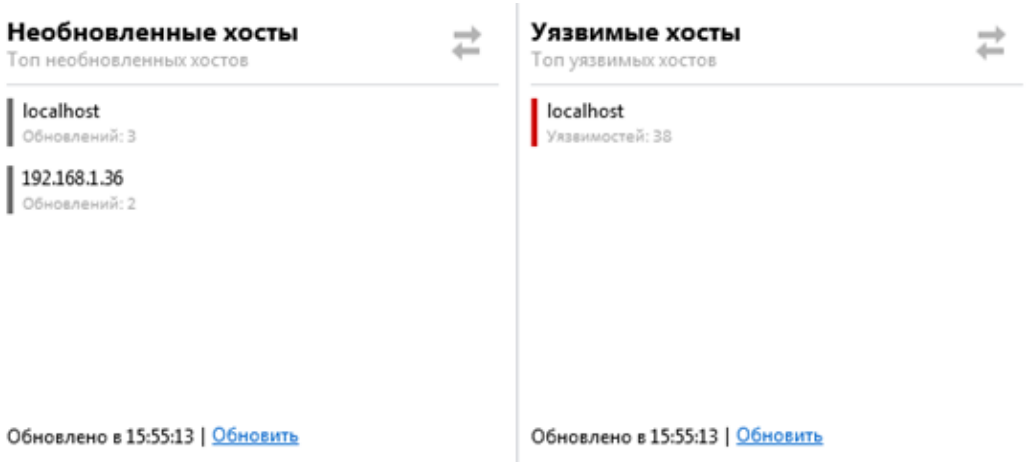


Рисунок 4.2.1.8

Содержание главы...

Вкладка ***«Хосты»*** включает в себя таблицы ***«Группы»***, ***«Группа: по умолчанию»*** и боковую панель, содержащую фильтры для управления хостами. Таблица ***«Группы»*** содержит группу ***«По умолчанию»***, в которую помещаются все добавленные хосты, а также созданные группы хостов. Критерий создания групп определяется администратором самостоятельно. Например, это может быть разделение всех хостов по подразделениям организации, к которым они относятся (Рисунок 4.2.2.1).

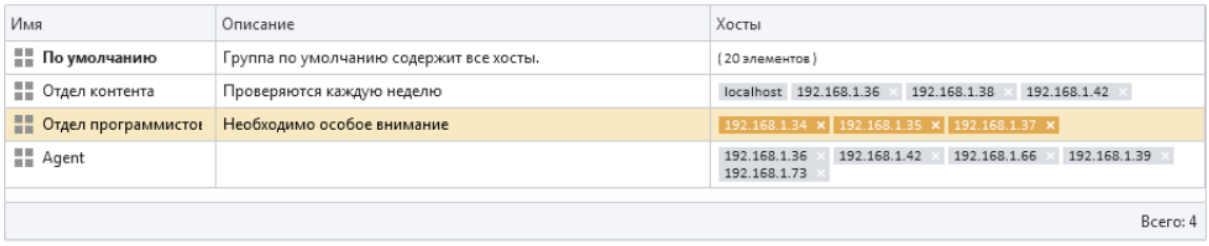


Рисунок 4.2.2.1

Таблица ***«Группы»*** содержит следующие атрибуты (**Таблица 11**):

Таблица 11

Атрибут	Описание
Имя	Название группы хостов
Описание	Описание группы хостов
Хосты	Список или количество хостов, состоящих в данной группе

Вызов контекстного меню правой кнопкой мыши по группе из этого списка позволит (**Таблица 12**):

Таблица 12

Действие	Описание
Создать задание для выбранной группы	Для выбранных хостов создать задание
Создать группу	Объединить группу хостов
Редактировать	Изменить название или состав группы
Удалить	Удалить группу
История	Посмотреть историю операций для данных хостов
Обновить	Обновление данных
Экспорт в CSV	Экспорт в файл

Вызов контекстного меню правой кнопкой мыши по группе из этого списка позволит (**Таблица 13**):

 *Для WEB-версии, вызов контекстного меню осуществляется путем щелчка левой кнопкой мыши по иконке*  *, справа от выбранной группы (**Таблица 13**).*

Таблица 13

Действие	Описание
Редактировать	Изменить название или состав группы
История	Просмотреть историю операция для данных хостов
Пинг	Открыть окно для пинга хостов

Удалить	Удалить группу

Рисунок 4.2.2.2 , содержит список хостов, состоящих в выбранной группе.

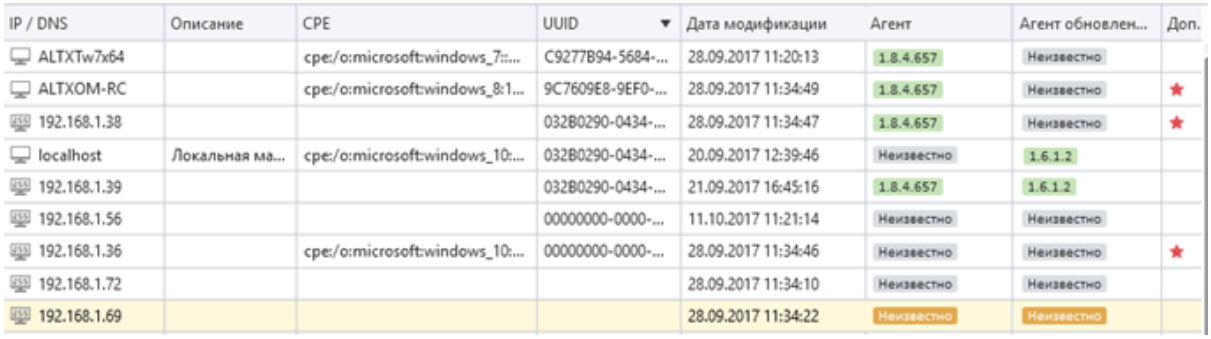


Рисунок 4.2.2.2

Вызов контекстного меню правой кнопкой мыши по хосту из этого списка позволит (**Таблица 14**):

Таблица 14

Действие	Описание
Создать хост	Добавление нового хоста
Пинг	Проверка соединения с хостом
Редактировать	Изменение описания хоста, и привязанных УЗ
Создать задание для выбранных хостов	Вызвать мастер создания заданий для хостов
Удалить	Удалить хост
История	Посмотреть историю для выбранных хостов
Менеджер лицензий хостов	Переход в модуль "Менеджера лицензий хостов"
Обновить	Обновить данные программы

Импорт	Импорт данных из файла CSV
Экспорт CSV	Экспорт данных в файл CSV

*Для WEB-версии, вызов контекстного меню позволит (**Таблица 15**).*

Таблица 15

Действие	Описание
Свойства	Просмотр параметров хоста
Редактировать	Изменение описания хоста, и привязанных УЗ
История	Посмотреть историю для выбранных хостов
Пинг	Проверка соединения с хостом
Удалить	Удалить хост

Таблица ***«Группа: по умолчанию»*** содержит следующие атрибуты (**Таблица 16**):

Таблица 16

Атрибут	Описание
IP / DNS	Отображает IP-адрес либо DNS-имя хоста
Описание	Содержит описание хоста
CPE	Common Platform Enumeration (идентифицирует установленную ОС на хосте)
UUID (в WEB версии отсутствует)	Уникальный идентификатор ПО

Дата модификации	Отображает дату последнего изменения информации о хосте, либо дата его добавления в список
Агент	Отображает информацию о наличии установленного на данный хост агента
Агент обновлений	Отображает информацию о наличии установленного на данный хост агента обновлений
Дополнительные модули	Отображает наличие дополнительных лицензий на хосте, например, «Модуля аудита безопасности серверов и приложений»
Учетные данные	Учетные данные, которые привязываются к хосту

*Для определения статусов хоста необходимо запустить команду **Пинг,** предусмотренную в консоли RedCheck. Подробнее о запуске команды Пинг можно прочитать в разделе 5.2.3.*

«Статус агента» (для WEB-версии, столбик отсутствует). Отображает информацию о наличии и возможности подключения к данному агенту.

Боковая панель ***«Управление хостами и группами хостов»*** предоставляет возможность фильтрации хостов по таким параметрам как:

- ***Интервал*** - задает промежуток времени, когда хост был создан или модифицирован. Например, сегодня, вчера, на этой неделе, в этом месяце, году, на всём промежутке времени, или позволяет задать другое значение (при выборе варианта «Другой», становятся доступны следующие элементы фильтра: «Хост создан с» и «По»);
- ***Хост создан с*** - начальная дата создания или модификации хоста. Опция фильтра доступна, если в пункте «Интервал», установлено значение «Другой»;
- ***По*** - конечная дата создания или модификации хоста. Опция фильтра доступна, если в пункте «Интервал», установлено значение «Другой»;
- ***Хост*** - полное или частичное название искомого хоста (можно указать IP-адрес или DNS-имя хоста);
- ***CPE*** - поиск по CPE машины.

Для фильтрации хостов выбранной группы необходимо задать искомые параметры и нажать кнопку ***«Применить фильтр»***. Таблица с хостами будет отфильтрована в соответствии с заданными параметрами фильтра.

Содержание главы...

Вкладка ***«Задания»*** содержит таблицу, в которой перечислены все сформированные задания: ***«Активные задания»*** и ***«Завершенные задания»***.

Вызов контекстного меню правой кнопкой мыши по заданию из этого списка позволит (**Таблица 17**):

Таблица 17

Действие	Описание
Перезапустить	Запустить повторное выполнение задания
Приостановить	Выполнить временную остановку задания, паузу (доступно не для всех типов заданий)
Остановить	Произвести полную остановку выполнения задания
Удалить	Выполнить безвозвратное удаление задания
Создать расписание	Позволяет создать время выполнения задания
Свойства	Открывает сведения задания
История	Посмотреть историю выполнения задания
Создать задание	Создать новое задание
Обновить	Обновить данные
Экспорт CSV	Экспорт данных в CSV-файл

Таблица заданий имеет следующие атрибуты (**Таблица 18**):

Таблица 18

Атрибут	Описание
Id	Уникальный идентификатор задания
Имя	Название задания
Агент	Тип сканирования: с использованием задания или без
Статус	Статус выполнения задания
Тип сканирования	Тип задания
Тип запуска	Запуск задания по расписанию или по требованию
Дата создания	Дата создания задания
Время запуска	Время запуска задания
Время завершения	Время завершения выполнения задания
Длительность	Общее время выполнения задания
Время следующего запуска	Запланированное время запуска
Хосты/группы	Сканируемые хосты в задании
Служба сканирования	Отображение службы сканирования для которой назначено задание
Текущий хост	Текущий сканируемый хост
Процент	% выполнения (обобщенный или детальный, в зависимости от типа задания)
Сообщения	Сообщения программы о выполнении

	задания

Кликнув правой кнопкой мыши по атрибутам таблицы - можно выбрать необходимые пользователю для удобной работы.

В заголовке вкладки имеется счётчик активных заданий. Активными считаются выполняющиеся задания и задания в очереди (Рисунок 4.2.3.1).

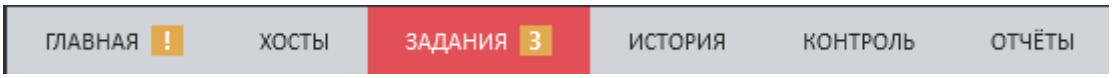


Рисунок 4.2.3.1

Для удобства работы, задания можно группировать по типу сканирования и по типу запуска. Также доступен режим отображения ***«Диспетчер»***, отображает задания, которые выполняются в данный момент, либо находятся в очереди на выполнение, отображает прогресс выполнения заданий, вплоть до сбора конкретного OVAL объекта.

Боковая панель ***«Создание заданий сканирования и управления ими»*** предоставляет возможность фильтрации заданий по таким параметрам как:

- ***Период создания*** - промежуток времени, когда было создано задание. Например, сегодня, вчера, на этой неделе, в этом месяце, году, на всём промежутке времени, или другое значение (при выборе варианта ***«Другой»***, становятся доступны элементы фильтра: задание ***«Создано с»*** и ***«Создано по»***)
- ***Создано с*** - начальная дата создания завершенного задания. Опция фильтра доступна, если в пункте ***«Период создания»***, установлено значение ***«Другой»***
- ***Создано по*** - конечная дата создания завершенного задания. Опция фильтра доступна, если в пункте ***«Период создания»***, установлено значение ***«Другой»***
- Задание - название искомого задания (можно указать целое или частичное название задания вручную, или открыть диалоговое окно, нажав на кнопку «...», и выбрать задание из списка)

- *Хост* - хост, который был просканирован (можно указать целый или частичный IP-адрес, DNS-имя хоста вручную, или открыть диалоговое окно, нажав на кнопку «...», и выбрать хост из списка)
- *Тип сканирования* - тип задания (в выпадающем списке перечислены все типы заданий, например, аудит конфигураций, инвентаризация, ...)
- *Служба сканирования* - выбор службы, с помощью которой выполняется сканирование машины
- *Тип запуска* - отбор заданий по типу запуска по требованию, по расписанию)
- *Статус* - выбор заданий по типу статуса (в выпадающем списке перечислены все типы заданий, например, аудит конфигураций, инвентаризация, ...)

Для фильтрации завершенных заданий необходимо задать искомые параметры и нажать кнопку *«Применить фильтр»*.

Содержание главы...

На вкладке ***«История»*** находится таблица с историей выполнения всех заданий и фильтр для поиска интересующих Вас заданий.

На рисунке ***«История сканирований»*** (Рисунок 4.2.4.1) содержится информация о выполненных ранее заданиях, *непросмотренные записи помечаются строками серого цвета.*

Таблица содержит такие атрибуты как (**Таблица 19**):

Таблица 19

Атрибут	Описание
Номер (№)	Уникальный идентификатор записи в истории
Хост	IP-адрес либо DNS-имя хоста
Статус	Статус выполнения
Риск	Графически отображает результаты сканирования (цветом)
Контроль	Результат контроля задания (пройден или нет)
Задание	Название задания
Агент	Сканирование по агенту или без
Тип задания	Тип сканирования
E	Идентификатор выполнения задания
Начало	Дата и время начала выполнения задания
Завершение	Дата и время завершения выполнения задания
Время	Общее время выполнения

Примечание	Дополнительные сведения

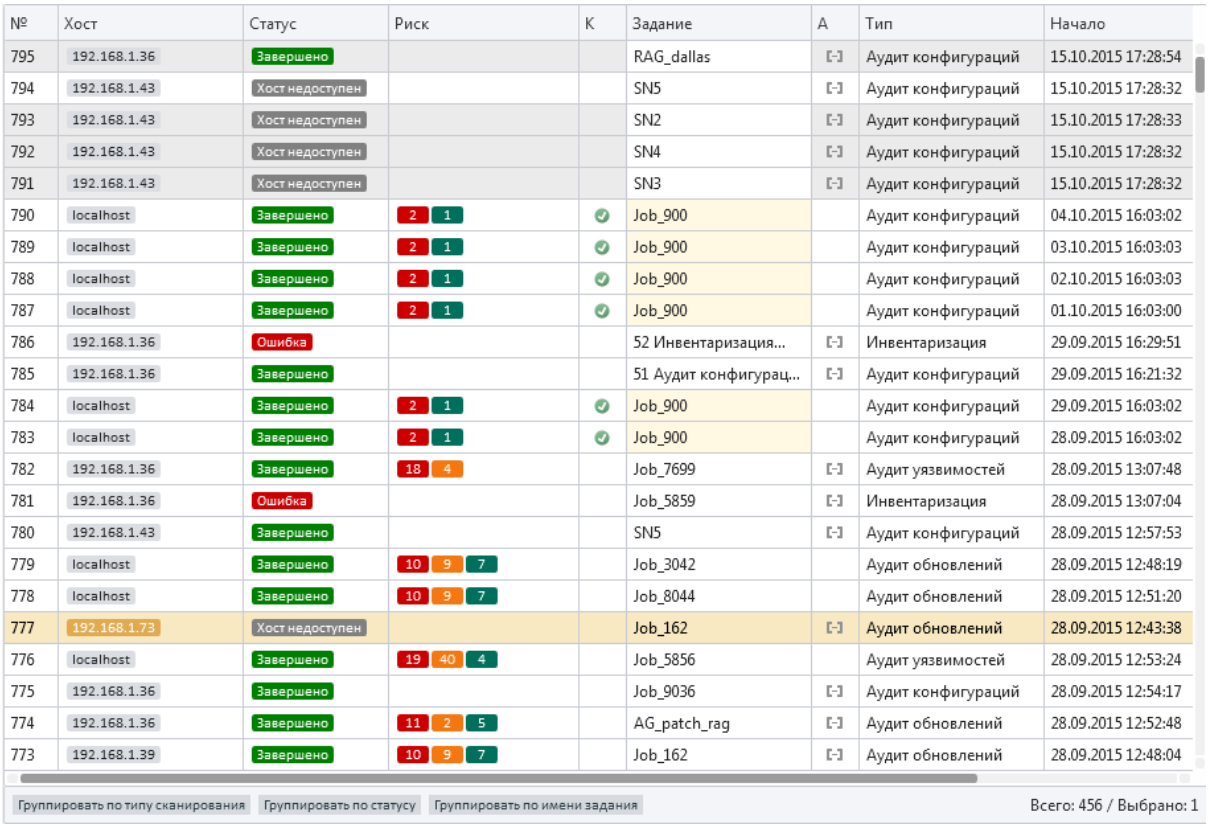
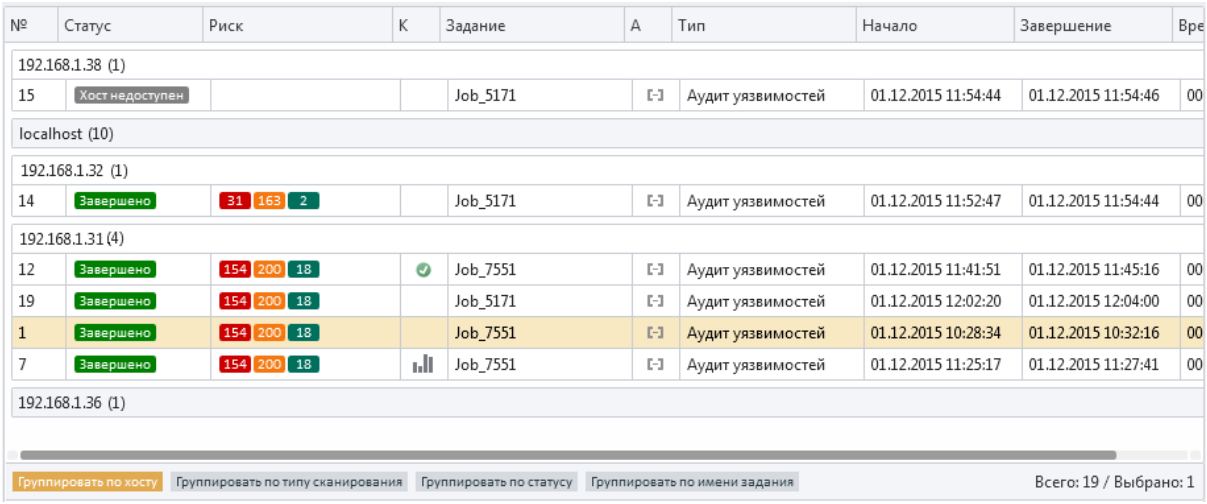


Рисунок 4.2.4.1

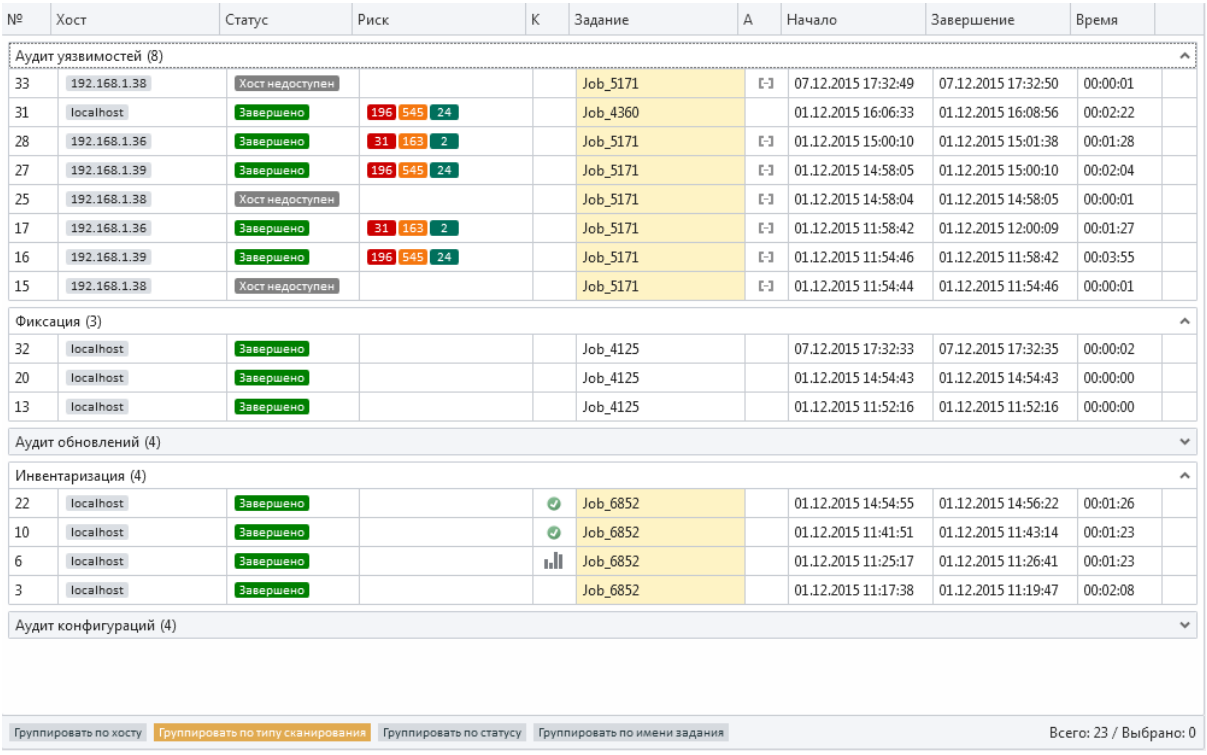
Для удобства работы, историю можно группировать по хосту (Рисунок 4.2.4.2), по типу сканирования (Рисунок 4.2.4.3), по статусу (Рисунок 4.2.4.4), по имени задания (Рисунок 4.2.4.5) или использовать сразу несколько типов группировки.



№	Статус	Риск	К	Задание	А	Тип	Начало	Завершение	Вре
192.168.1.38 (1)									
15	Хост недоступен			Job_5171	[-]	Аудит уязвимостей	01.12.2015 11:54:44	01.12.2015 11:54:46	00
localhost (10)									
192.168.1.32 (1)									
14	Завершено	31 163 2		Job_5171	[-]	Аудит уязвимостей	01.12.2015 11:52:47	01.12.2015 11:54:44	00
192.168.1.31 (4)									
12	Завершено	154 200 18		Job_7551	[-]	Аудит уязвимостей	01.12.2015 11:41:51	01.12.2015 11:45:16	00
19	Завершено	154 200 18		Job_5171	[-]	Аудит уязвимостей	01.12.2015 12:02:20	01.12.2015 12:04:00	00
1	Завершено	154 200 18		Job_7551	[-]	Аудит уязвимостей	01.12.2015 10:28:34	01.12.2015 10:32:16	00
7	Завершено	154 200 18		Job_7551	[-]	Аудит уязвимостей	01.12.2015 11:25:17	01.12.2015 11:27:41	00
192.168.1.36 (1)									

Группировать по хосту | Группировать по типу сканирования | Группировать по статусу | Группировать по имени задания | Всего: 19 / Выбрано: 1

Рисунок 4.2.4.2



№	Хост	Статус	Риск	К	Задание	А	Начало	Завершение	Время
Аудит уязвимостей (8)									
33	192.168.1.38	Хост недоступен			Job_5171	[-]	07.12.2015 17:32:49	07.12.2015 17:32:50	00:00:01
31	localhost	Завершено	196 545 24		Job_4360		01.12.2015 16:06:33	01.12.2015 16:08:56	00:02:22
28	192.168.1.36	Завершено	31 163 2		Job_5171	[-]	01.12.2015 15:00:10	01.12.2015 15:01:38	00:01:28
27	192.168.1.39	Завершено	196 545 24		Job_5171	[-]	01.12.2015 14:58:05	01.12.2015 15:00:10	00:02:04
25	192.168.1.38	Хост недоступен			Job_5171	[-]	01.12.2015 14:58:04	01.12.2015 14:58:05	00:00:01
17	192.168.1.36	Завершено	31 163 2		Job_5171	[-]	01.12.2015 11:58:42	01.12.2015 12:00:09	00:01:27
16	192.168.1.39	Завершено	196 545 24		Job_5171	[-]	01.12.2015 11:54:46	01.12.2015 11:58:42	00:03:55
15	192.168.1.38	Хост недоступен			Job_5171	[-]	01.12.2015 11:54:44	01.12.2015 11:54:46	00:00:01
Фиксация (3)									
32	localhost	Завершено			Job_4125		07.12.2015 17:32:33	07.12.2015 17:32:35	00:00:02
20	localhost	Завершено			Job_4125		01.12.2015 14:54:43	01.12.2015 14:54:43	00:00:00
13	localhost	Завершено			Job_4125		01.12.2015 11:52:16	01.12.2015 11:52:16	00:00:00
Аудит обновлений (4)									
Инвентаризация (4)									
22	localhost	Завершено			Job_6852		01.12.2015 14:54:55	01.12.2015 14:56:22	00:01:26
10	localhost	Завершено			Job_6852		01.12.2015 11:41:51	01.12.2015 11:43:14	00:01:23
6	localhost	Завершено			Job_6852		01.12.2015 11:25:17	01.12.2015 11:26:41	00:01:23
3	localhost	Завершено			Job_6852		01.12.2015 11:17:38	01.12.2015 11:19:47	00:02:08
Аудит конфигураций (4)									

Группировать по хосту | Группировать по типу сканирования | Группировать по статусу | Группировать по имени задания | Всего: 23 / Выбрано: 0

Рисунок 4.2.4.3

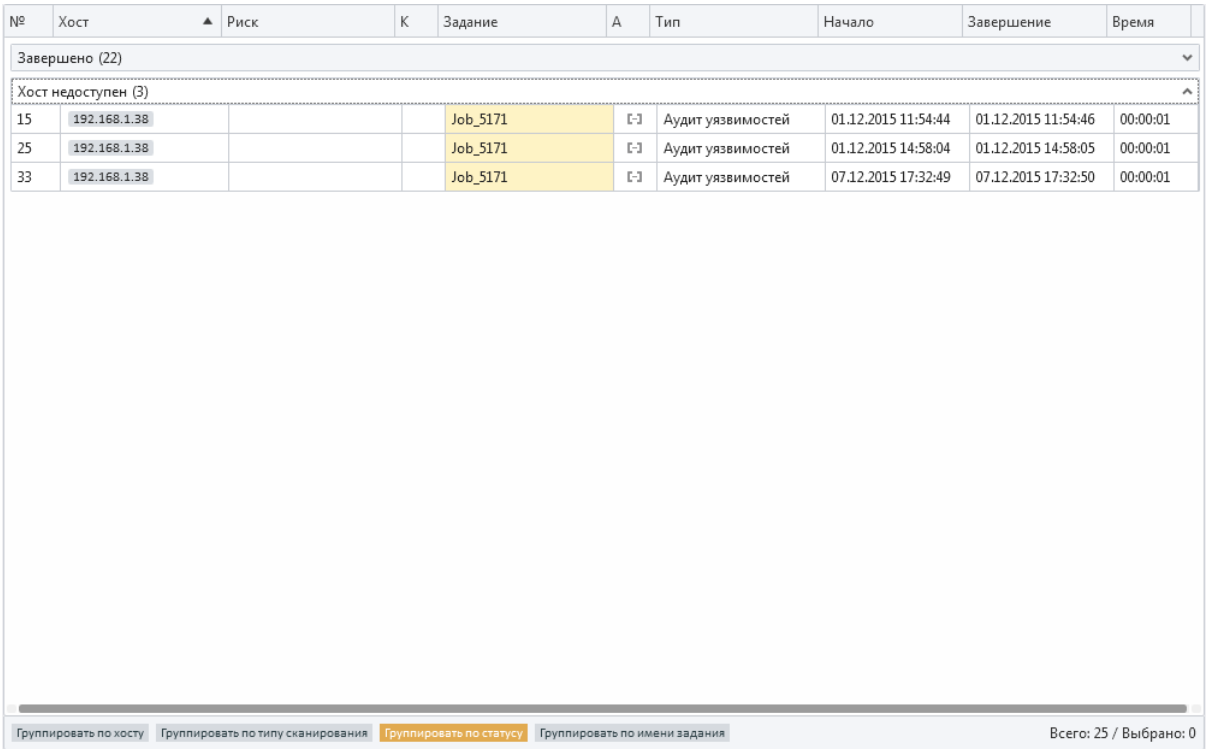


Рисунок 4.2.4.4

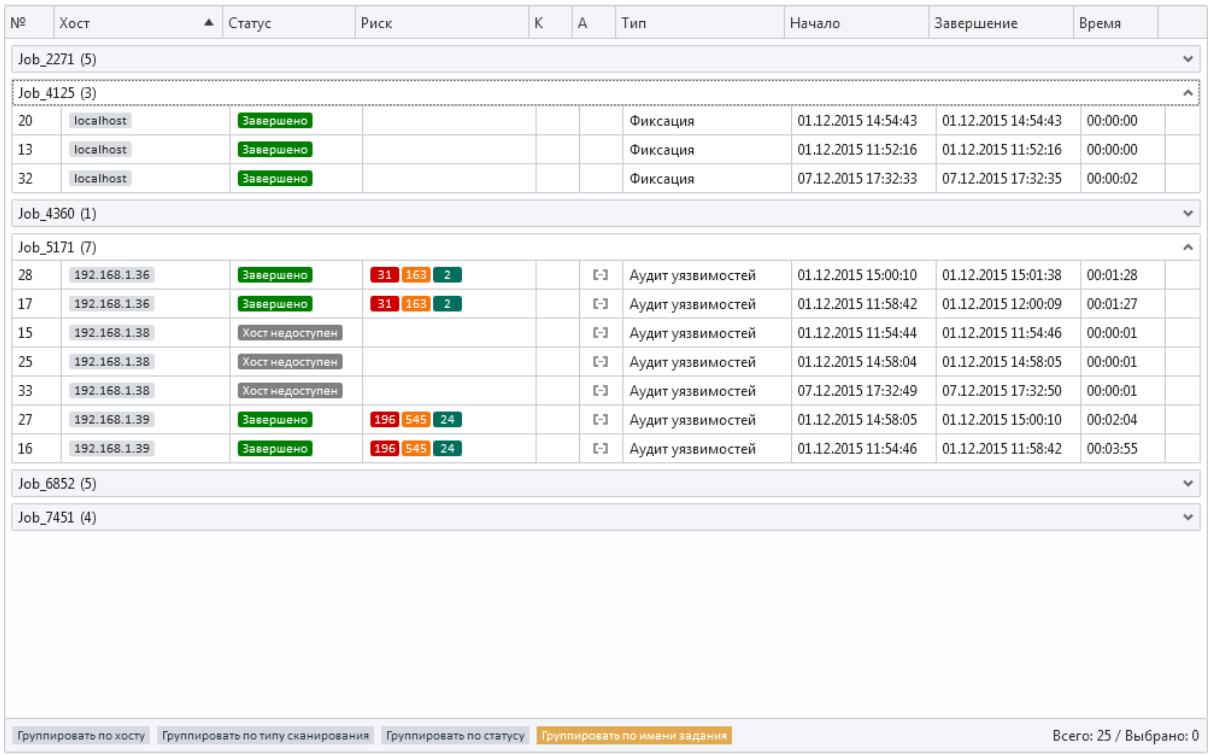


Рисунок 4.2.4.5

Риск может отображать следующие значения (Рисунок 4.2.4.5):

96 - индикатор отображает число найденных элементов с высоким риском;

48 - индикатор отображает число найденных элементов со средним риском;

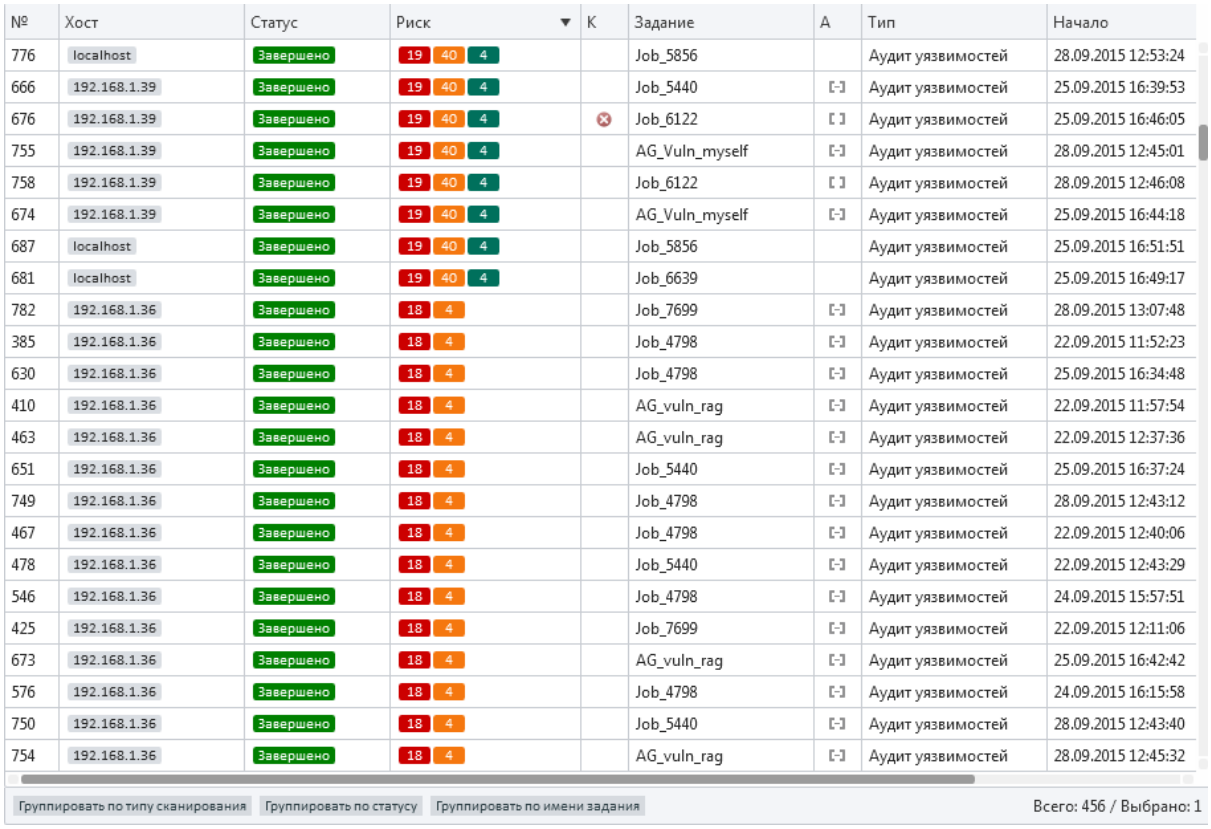
2 - индикатор отображает число найденных элементов с низким риском.

Задание может иметь следующие статусы (Рисунок 4.2.4.1):

Завершено - статус означает, что задание было успешно выполнено;

Хост недоступен - статус означает, что хост по каким-либо причинам недоступен для сканирования;

Ошибка - статус означает, что задание было выполнено с ошибкой. Открытие свойств задания, выполненного с ошибкой, укажет, что именно произошло, если RedCheck смог самостоятельно ее диагностировать.



№	Хост	Статус	Риск	К	Задание	А	Тип	Начало
776	localhost	Завершено	19 40 4		Job_5856		Аудит уязвимостей	28.09.2015 12:53:24
666	192.168.1.39	Завершено	19 40 4		Job_5440		Аудит уязвимостей	25.09.2015 16:39:53
676	192.168.1.39	Завершено	19 40 4		Job_6122		Аудит уязвимостей	25.09.2015 16:46:05
755	192.168.1.39	Завершено	19 40 4		AG_Vuln_myself		Аудит уязвимостей	28.09.2015 12:45:01
758	192.168.1.39	Завершено	19 40 4		Job_6122		Аудит уязвимостей	28.09.2015 12:46:08
674	192.168.1.39	Завершено	19 40 4		AG_Vuln_myself		Аудит уязвимостей	25.09.2015 16:44:18
687	localhost	Завершено	19 40 4		Job_5856		Аудит уязвимостей	25.09.2015 16:51:51
681	localhost	Завершено	19 40 4		Job_6639		Аудит уязвимостей	25.09.2015 16:49:17
782	192.168.1.36	Завершено	18 4		Job_7699		Аудит уязвимостей	28.09.2015 13:07:48
385	192.168.1.36	Завершено	18 4		Job_4798		Аудит уязвимостей	22.09.2015 11:52:23
630	192.168.1.36	Завершено	18 4		Job_4798		Аудит уязвимостей	25.09.2015 16:34:48
410	192.168.1.36	Завершено	18 4		AG_vuln_rag		Аудит уязвимостей	22.09.2015 11:57:54
463	192.168.1.36	Завершено	18 4		AG_vuln_rag		Аудит уязвимостей	22.09.2015 12:37:36
651	192.168.1.36	Завершено	18 4		Job_5440		Аудит уязвимостей	25.09.2015 16:37:24
749	192.168.1.36	Завершено	18 4		Job_4798		Аудит уязвимостей	28.09.2015 12:43:12
467	192.168.1.36	Завершено	18 4		Job_4798		Аудит уязвимостей	22.09.2015 12:40:06
478	192.168.1.36	Завершено	18 4		Job_5440		Аудит уязвимостей	22.09.2015 12:43:29
546	192.168.1.36	Завершено	18 4		Job_4798		Аудит уязвимостей	24.09.2015 15:57:51
425	192.168.1.36	Завершено	18 4		Job_7699		Аудит уязвимостей	22.09.2015 12:11:06
673	192.168.1.36	Завершено	18 4		AG_vuln_rag		Аудит уязвимостей	25.09.2015 16:42:42
576	192.168.1.36	Завершено	18 4		Job_4798		Аудит уязвимостей	24.09.2015 16:15:58
750	192.168.1.36	Завершено	18 4		Job_5440		Аудит уязвимостей	28.09.2015 12:43:40
754	192.168.1.36	Завершено	18 4		AG_vuln_rag		Аудит уязвимостей	28.09.2015 12:45:32

Группировать по типу сканирования | Группировать по статусу | Группировать по имени задания | Всего: 456 / Выбрано: 1

Рисунок 4.2.4.6

Вызов контекстного меню правой кнопкой мыши по заданию из этого списка позволит выбрать один из пунктов (**Таблица 20**):

Таблица 20

Действие	Описание
Результаты сканирования	Отображение полученных результатов выполненного задания. Представлены результаты сканирования и oval-инвентари
Свойства задания	Сведения о выполненном задании: тип, дата создания, время запуска, имя, учетные данные, метод сканирования, контент, список сканируемых хостов, время запуска и завершения выполнения задания
Создать контроль	Позволяет выбрать результаты сканирования в качестве «эталона» для постановки на «контроль»
Удалить контроль	Удаляет из результатов сканирования статус «эталона»
Перезапустить	Повторное выполнение выбранного задания
Удалить	Удаление записи из истории сканирований
Обновить	Обновление данных
Экспорт CSV	Экспорт результатов выполненного задания в файл в формате CSV

Результаты сканирования для задания ***«Аудит уязвимостей»*** выглядят, как показано на рисунках Рисунок 4.2.4.7 и Рисунок 4.2.4.8. Для удобства работы результаты можно группировать по риску и по продуктам.

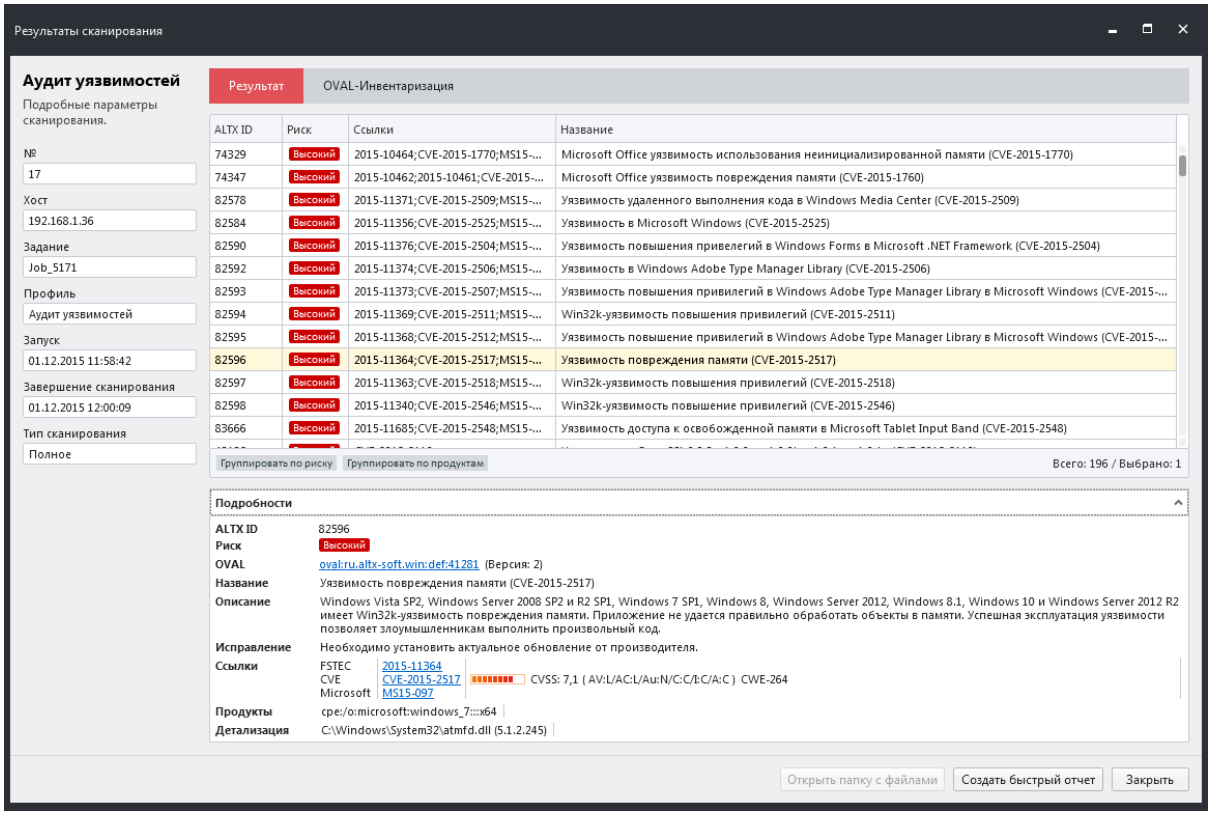


Рисунок 4.2.4.7

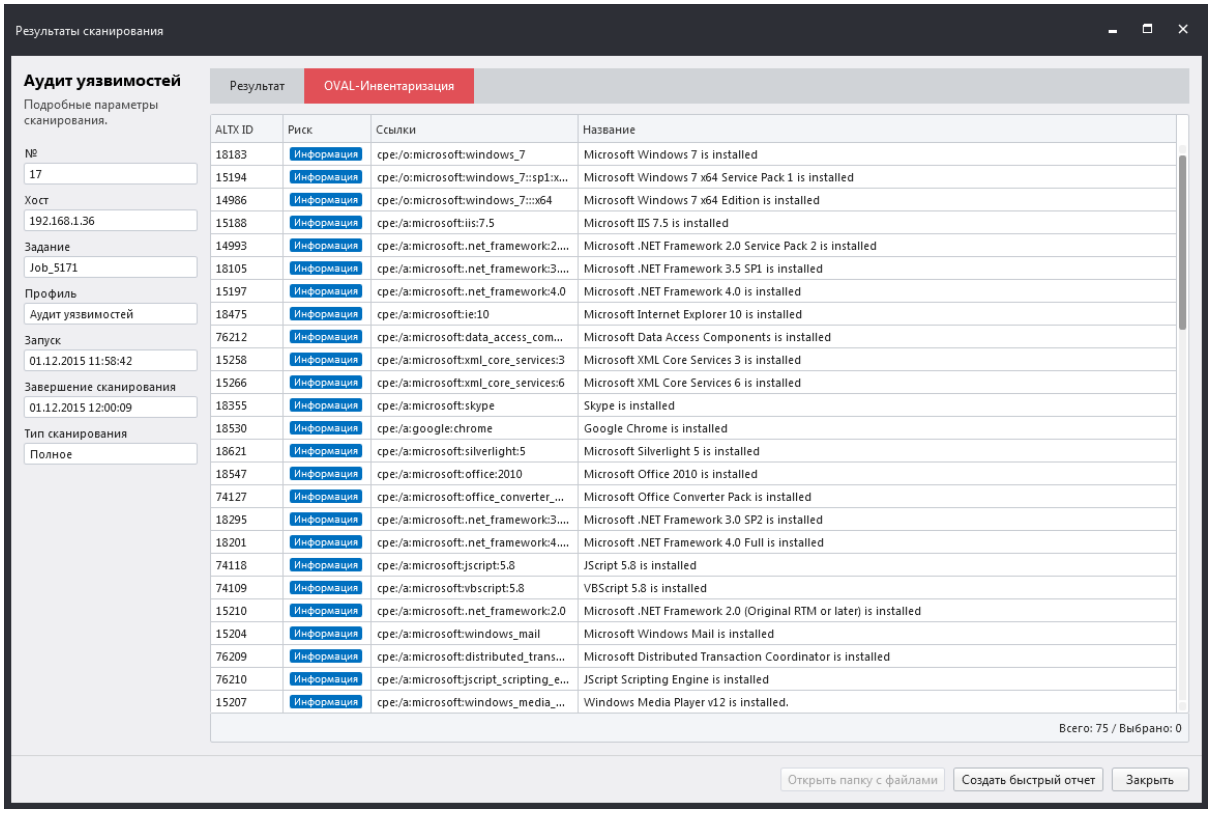


Рисунок 4.2.4.8.

На боковой панели вкладки расположен ***«Фильтр сканирований заданий»***, выполняющий фильтрацию истории выполнения заданий по таким параметрам как:

- ***Интервал*** - промежуток времени, когда проводилось сканирование. Например: сегодня, вчера, на этой неделе, в этом месяце, году, на всём промежутке времени, или другое значение (при выборе варианта ***«Другой»***, становятся доступны следующие элементы фильтра: ***«Дата начала» и «Дата завершения»*** сканирования)
- **Дата начала** - дата начала сканирования. Опция фильтра доступна, если в пункте ***«Интервал»***, установлено значение ***«Другой»***
- ***Дата завершения*** - дата завершения сканирования. Опция фильтра доступна, если в пункте ***«Интервал»***, установлено значение ***«Другой»***
- ***Быстрый фильтр*** - доступные значения: ***«Сеть - Обновления»***, ***«Сеть - Уязвимости»***. Позволяет отфильтровать историю результатов сканирований по следующим критериям: актуальность заданий (все сканирования должны быть актуальны), по типу задания (обновления или уязвимости)
- **Хост** - имя хоста, на котором проводилось сканирование (можно указать полный или частичный IP-адрес, или DNS-имя хоста вручную, либо открыть диалоговое окно, нажав на кнопку «...», и выбрать доступный хост из списка)
- **Группа** - группа, в которую входит искомый хост (можно указать полное или частичное название группы вручную, либо открыть диалоговое окно, нажав на кнопку «...», и выбрать из списка уже имеющихся групп)
- ***Задание*** - название искомого задания (можно указать полное или частичное название задания вручную, либо открыть диалоговое окно, нажав на кнопку «...», и выбрать из списка уже имеющихся заданий)
- ***ID выполнения задания*** - поиск задания, по уникальному идентификатору выполнения задания
- ***Тип*** - тип задания (в выпадающем списке перечислены все типы заданий, например, аудит конфигураций, инвентаризация, ...)
- ***Ссылки*** - ссылки (**CVE, CPE**, ...). Например, если вы хотите найти в истории сканирования с уязвимостью **POODLE**, укажите ссылку ***CVE-2014-3566***
- ***Статус*** - фильтрация заданий на основе статуса их выполнения: ***«Завершено»*** либо ***«Ошибка»***

- ***Сканирования*** - отображаются ***«Все»*** сканирования, или только ***«Актуальные»***, то есть последнее успешное сканирование, по каждому из заданий

Для фильтрации истории сканирований необходимо задать искомые параметры фильтрации и нажать кнопку ***«Применить фильтр»***. Таблица с результатами сканирований будет отфильтрована в соответствии с заданными параметрами фильтра.

Содержание главы...

Вкладка ***«Контроль»*** содержит таблицу со сведениями о результатах сравнения выполненных заданий с эталонными показателями.

Контроль можно выполнять только для заданий: ***фиксация, инвентаризация, аудит конфигураций, аудит уязвимостей.***

На рисунке 4.2.5.1, находятся результаты сравнения 2-х сканирований, одно из которых является «эталоном». Таблица содержит такие атрибуты как (**Таблица 21**):

Таблица 21

Действие	Описание
Номер (№)	Уникальный идентификатор записи контроля
Хост	DNS/IP хоста
Статус	Отображает статус контроля (соответствие/несоответствие)
Задание	Имя задания
№ сканирования	Номер сканирования
Тип	Тип сканирования
Дата создания	Дата начала проведения контроля
Дата завершения	Дата завершения контроля

№	Хост	Задание	№ сканирования	Тип	Дата создания	Дата завершен...	Статус
1	localhost	Job_1611	16	Аудит конфигураций	31.07.2015 16:45:32	22.09.2015 12:31:58	Несоответствие
3	localhost	Job_5856	26	Аудит уязвимостей	31.07.2015 17:48:29	22.09.2015 12:44:52	Несоответствие
7	192.168.1.39	Job_6122	36	Аудит уязвимостей	18.08.2015 15:39:10	22.09.2015 12:48:23	Несоответствие
18	localhost	Job_900	547	Аудит конфигураций	24.09.2015 17:34:00	24.09.2015 17:34:44	Соответствие

Рисунок 4.2.5.1

В нижней части таблицы, результаты можно группировать по типу сканирования, статусу и по имени задания. (Рисунок 4.2.5.2)

Рисунок 4.2.5.2

Для того, чтобы установить эталонное значение, пользователю необходимо перейти на вкладку ***«История»***. В списке истории выбрать задание (фиксация, инвентаризация, аудит конфигураций или аудит уязвимостей), результаты которого будут «эталоном». Далее, правой кнопкой мыши, вызвать контекстное меню и выбрать опцию ***«Создать контроль»*** (на вкладке ***«История»***, в столбце «К» эталон помечается символом). (Рисунок 4.2.5.3)

После перезапуска эталонного задания, будут зафиксированы все изменения, произведенные на сканируемом хосте (на вкладке ***«История»***, указывается в столбце «К») - несоответствие эталону ( ), либо их отсутствие- соответствие эталону ( ).

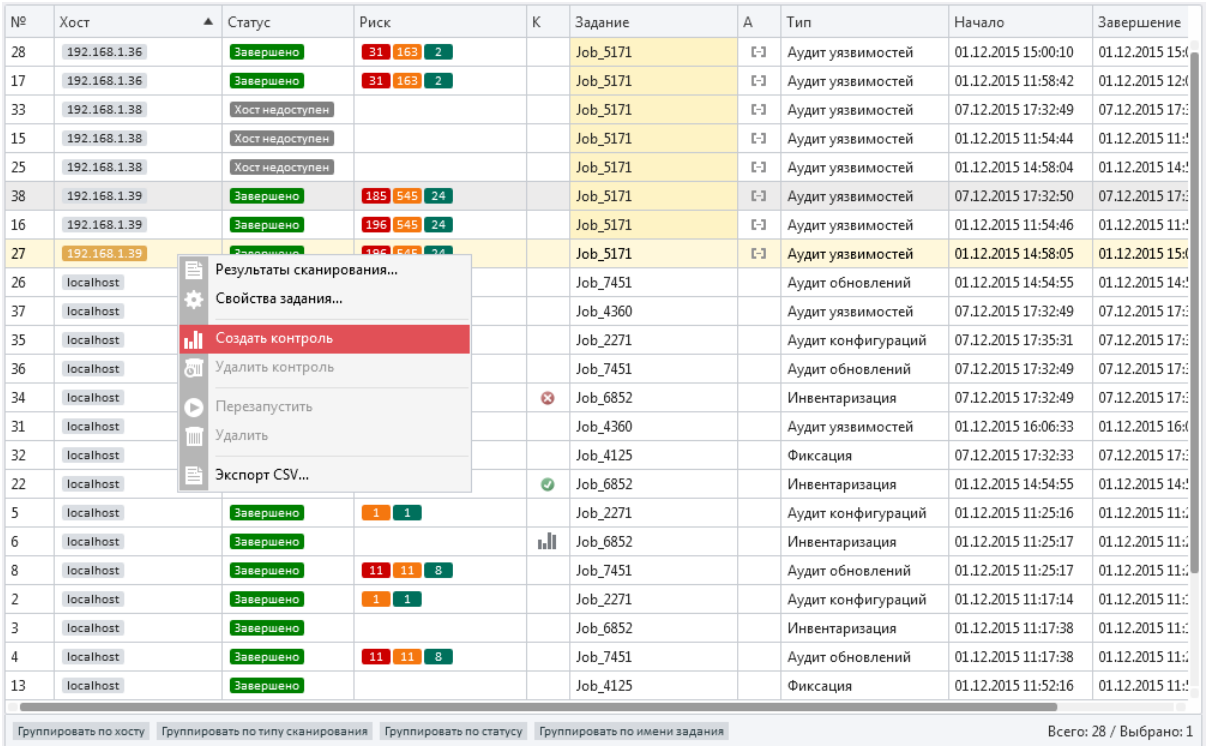


Рисунок 4.2.5.3

На боковой панели вкладки ***«Контроль»*** расположен ***«Фильтр средств сравнения с эталонными показателями»***, осуществляющий фильтрацию истории выполненных заданий по таким параметрам как:

- **Интервал** - промежуток времени между контролями. Например, сегодня, вчера, на этой неделе, в этом месяце, году, на всём промежутке времени, или другое значение (при выборе варианта ***«Другой»***, становятся доступны следующие элементы фильтра: ***«Дата начала» и «Дата завершения»*** контроля).
- ***Дата начала*** - начальная дата контроля. Опция фильтра доступна, если в пункте «Интервал», установлено значение «Другой».
- **Дата завершения** - дата завершения контроля. Опция фильтра доступна, если в пункте ***«Интервал»***, установлено значение ***«Другой»***.
- ***Контроль/История*** - переключение между сущностями ***«Контроль»*** и ***«История»*** выполнений контроля.
- ***Хост*** - хост, на котором проводился контроль (можно указать полный или частичный IP-адрес, или DNS-имя хоста вручную, либо открыть диалоговое окно, нажав на кнопку «...», и выбрать из списка уже имеющихся хостов).

- *Группа* - группа, в которую входит контролируемый хост (можно указать полное или частичное название группы вручную, либо открыть диалоговое окно, нажав на кнопку «...», и выбрать из списка уже имеющихся групп).
- **Задание** - название искомого задания (можно указать полное или частичное название задания вручную, либо открыть диалоговое окно, нажав на кнопку «...», и выбрать из списка уже имеющихся заданий).
- **Тип** - тип задания (в выпадающем списке перечислены все типы заданий, например: фиксация, инвентаризация, ...).
- *Статус* - фильтрация заданий контроля на основе статуса их выполнения: *«Не проведен»*, *«Несоответствие»*, *«Соответствие»* или *«Ошибка»*.

Для фильтрации заданий «контроль», необходимо задать искомые параметры и нажать кнопку *«Применить фильтр»*.

Для просмотра результатов контроля необходимо совершить двойной клик левой кнопкой мыши по строке с нужным заданием, или кликом правой кнопки мыши по строке вызвать контекстное меню и выбрать пункт *«Результаты контроля»* (Рисунок 4.2.5.4).

В левой части открывшегося окна *«Результаты контроля»* находится краткая информация о задании, такая как: наименование сканируемого хоста, ID задания, профиль сканирования, а также дата и время начала и завершения сканирования.

- кнопки навигации, позволяют просматривать результаты контроля других заданий в текущем окне.

В центральной части окна представлен список изменений, результаты сравнения сканирования с эталонным заданием.

В правом нижнем углу находятся кнопки (**Таблица 22**):

Таблица 22

Кнопка	Описание
Эталон	Открывает окно с результатами сканирования эталонного задания

Результат	Открывает окно с результатами последнего сканирования данного задания
Создать быстрый отчет	Создает отчет по данному заданию. Получившийся отчет можно просмотреть на вкладке ***«Отчеты»***. Его имя начинается с префикса «Quick_», а описание содержит строку «Автогенерируемый отчет вкладки «Контроль».
Закрыть	Закрывает окно «Результаты сканирования»

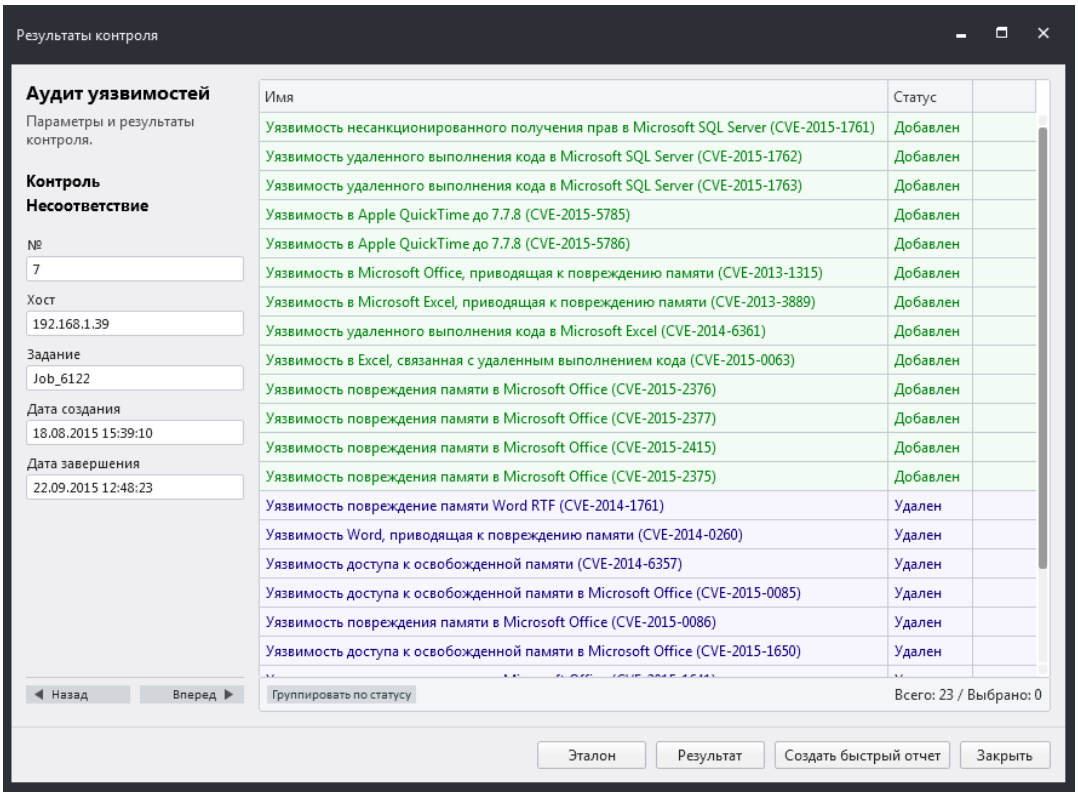


Рисунок 4.2.5.4

Содержание главы...

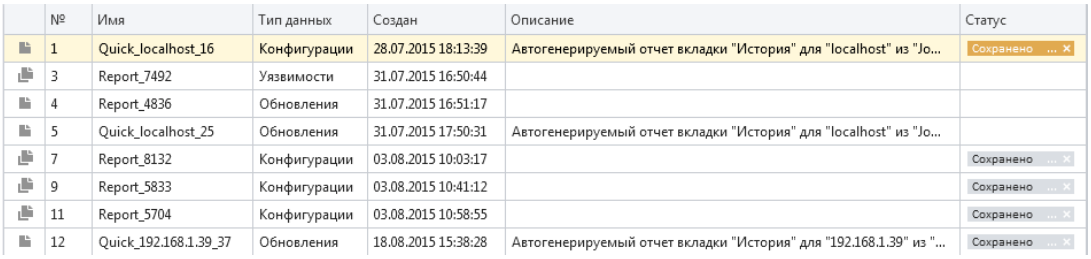
На вкладке ***«Отчеты»*** расположена таблица со сформированными отчетами и фильтр отчетов.

Сформированные отчеты можно сохранить как PDF, HTML, XML документы или как Web-архив.

Таблица ***«Список отчетов»*** (Рисунок 4.2.6.1) содержит такие атрибуты как (**Таблица 23**):

Таблица 23

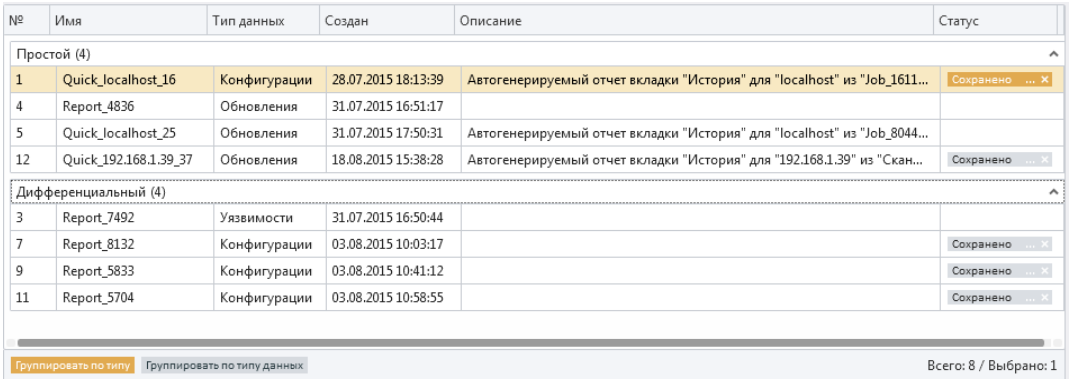
Атрибут	Описание
Номер (№)	Порядковый номер отчета
Тип отчета	Простой, дифференциальный
Имя	Имя файла отчета
Тип данных	Тип данных содержащихся в отчете (обновления, уязвимости, инвентаризация и т.д.)
Создан	Дата и время создания
Статус	Статус сохранения отчета. В иконке встроены кнопки: «Показать в папке», либо «Удалить файл»
Описание	Описание отчета



	№	Имя	Тип данных	Создан	Описание	Статус
	1	Quick_localhost_16	Конфигурации	28.07.2015 18:13:39	Автогенерируемый отчет вкладки "История" для "localhost" из "Jo...	Сохранено
	3	Report_7492	Уязвимости	31.07.2015 16:50:44		
	4	Report_4836	Обновления	31.07.2015 16:51:17		
	5	Quick_localhost_25	Обновления	31.07.2015 17:50:31	Автогенерируемый отчет вкладки "История" для "localhost" из "Jo...	
	7	Report_8132	Конфигурации	03.08.2015 10:03:17		Сохранено
	9	Report_5833	Конфигурации	03.08.2015 10:41:12		Сохранено
	11	Report_5704	Конфигурации	03.08.2015 10:58:55		Сохранено
	12	Quick_192.168.1.39_37	Обновления	18.08.2015 15:38:28	Автогенерируемый отчет вкладки "История" для "192.168.1.39" из "...	Сохранено

Рисунок 4.2.6.1

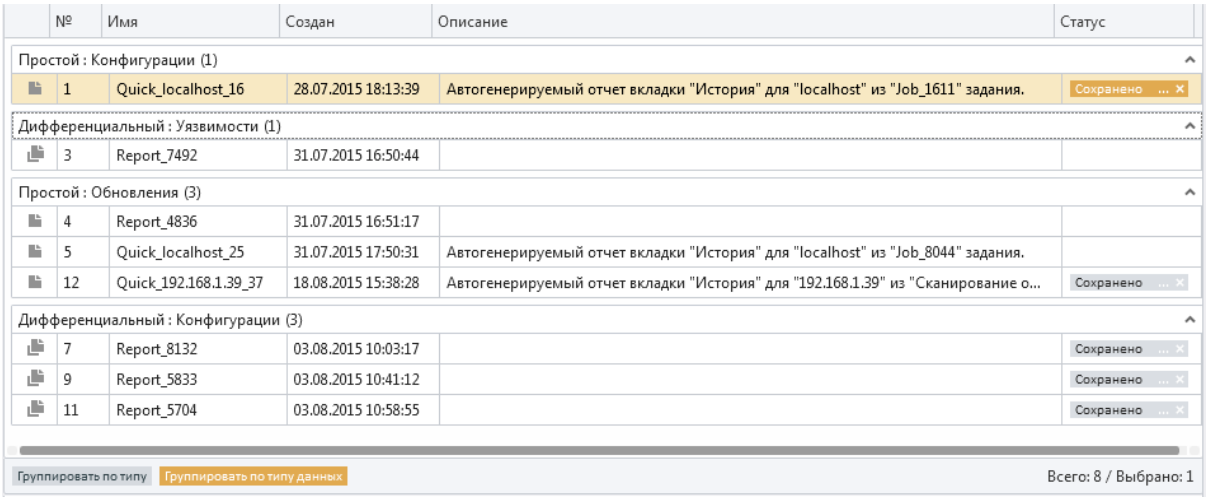
Отчеты можно группировать по типу сканирования (Рисунок 4.2.6.2) и по типу данных (Рисунок 4.2.6.3).



№	Имя	Тип данных	Создан	Описание	Статус
Простой (4)					
1	Quick_localhost_16	Конфигурации	28.07.2015 18:13:39	Автогенерируемый отчет вкладки "История" для "localhost" из "Job_1611...	Сохранено
4	Report_4836	Обновления	31.07.2015 16:51:17		
5	Quick_localhost_25	Обновления	31.07.2015 17:50:31	Автогенерируемый отчет вкладки "История" для "localhost" из "Job_8044...	
12	Quick_192.168.1.39_37	Обновления	18.08.2015 15:38:28	Автогенерируемый отчет вкладки "История" для "192.168.1.39" из "Скан...	Сохранено
Дифференциальный (4)					
3	Report_7492	Уязвимости	31.07.2015 16:50:44		
7	Report_8132	Конфигурации	03.08.2015 10:03:17		Сохранено
9	Report_5833	Конфигурации	03.08.2015 10:41:12		Сохранено
11	Report_5704	Конфигурации	03.08.2015 10:58:55		Сохранено

Группировать по типу | Группировать по типу данных | Всего: 8 / Выбрано: 1

Рисунок 4.2.6.2



	№	Имя	Создан	Описание	Статус
Простой : Конфигурации (1)					
	1	Quick_localhost_16	28.07.2015 18:13:39	Автогенерируемый отчет вкладки "История" для "localhost" из "Job_1611" задания.	Сохранено
Дифференциальный : Уязвимости (1)					
	3	Report_7492	31.07.2015 16:50:44		
Простой : Обновления (3)					
	4	Report_4836	31.07.2015 16:51:17		
	5	Quick_localhost_25	31.07.2015 17:50:31	Автогенерируемый отчет вкладки "История" для "localhost" из "Job_8044" задания.	
	12	Quick_192.168.1.39_37	18.08.2015 15:38:28	Автогенерируемый отчет вкладки "История" для "192.168.1.39" из "Сканирование о...	Сохранено
Дифференциальный : Конфигурации (3)					
	7	Report_8132	03.08.2015 10:03:17		Сохранено
	9	Report_5833	03.08.2015 10:41:12		Сохранено
	11	Report_5704	03.08.2015 10:58:55		Сохранено

Группировать по типу | Группировать по типу данных | Всего: 8 / Выбрано: 1

Рисунок 4.2.6.3

На боковой панели вкладки расположен ***«Фильтр отчетов»***, позволяющий выполнять фильтрацию по таким параметрам как:

- ***Интервал*** - промежуток времени, когда был создан отчет. Например, сегодня, вчера, на этой неделе, в этом месяце, году, на всём промежутке времени, или другое значение (при выборе варианта ***«Другой»***, становятся доступны следующие элементы фильтра: ***«Начиная с» и «Заканчивая»***).
- ***Начиная с*** - начальная дата создания отчета. Опция фильтра доступна, если в пункте ***«Интервал»***, установлено значение ***«Другой»***.
- ***Заканчивая*** - конечная дата создания отчета. Опция фильтра доступна, если в пункте ***«Интервал»***, установлено значение ***«Другой»***.
- ***Имя и описание*** - полное или частичное имя, или описание отчета.
- ***Тип отчета*** - простой или дифференциальный.
- ***Имя и описание*** - название искомого задания (можно указать полное или частичное название задания вручную, либо открыть диалоговое окно, нажав на кнопку «...», и выбрать из списка уже имеющихся заданий).
- ***Тип отчёта*** - тип отчёта (в выпадающем списке перечислены все типы заданий, например, аудит конфигураций, инвентаризация, ...).
- ***Тип данных*** - данное поле доступно, если указан ***«Тип отчета»***. Определяет тип задания (в выпадающем списке перечислены все типы заданий, например, аудит конфигураций, инвентаризация, ...).

Для фильтрации отчетов, необходимо задать искомые параметры и нажать кнопку ***«Применить фильтр».***

Содержание главы...

4.3 Меню программы

Меню RedCheck позволяет создавать задания и отчеты, предоставляет доступ к сервисным функциям и настройкам, содержит сведения о программе.

Меню ***«Действия»*** включает в себя такие команды как ***«Создать задание»***, ***«Создать отчет» и «Выйти из программы»***, а также команды, позволяющие переключиться на конкретный тип задания.

Команда ***«Создать задание»***

Нажатие этой кнопки запускает мастер создания задания (Рисунок 4.3.1.1).

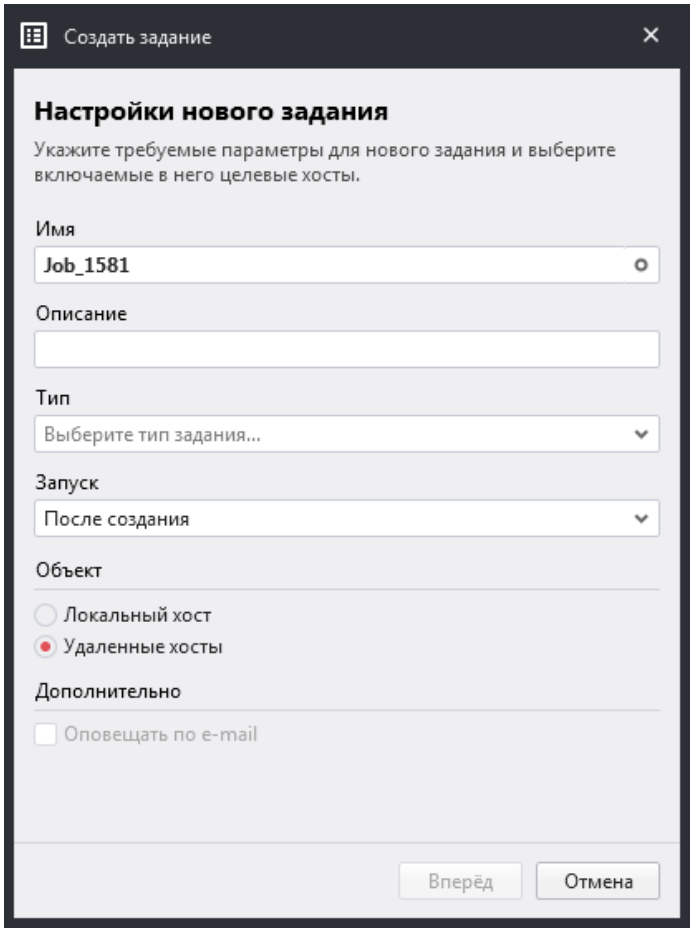


Рисунок 4.3.1.1

В окне ***«Настройки нового задания»*** можно задать следующие атрибуты:

- ***Имя*** - имя задания
- ***Описание*** - описание задания

- *Тип* - тип сканирования компьютера
- *Запуск* - определить момент запуска задания
- Запустить сразу после закрытия мастера
- *Объект* - задание объекта сканирования (локальный или удаленный)
- Оповещение о результатах сканирования по e-mail

В данном меню пользователь может сразу выбрать необходимое ему задание, поле «тип» будет автоматически заполнено в мастере создания задания (Рисунок 4.3.1.2).

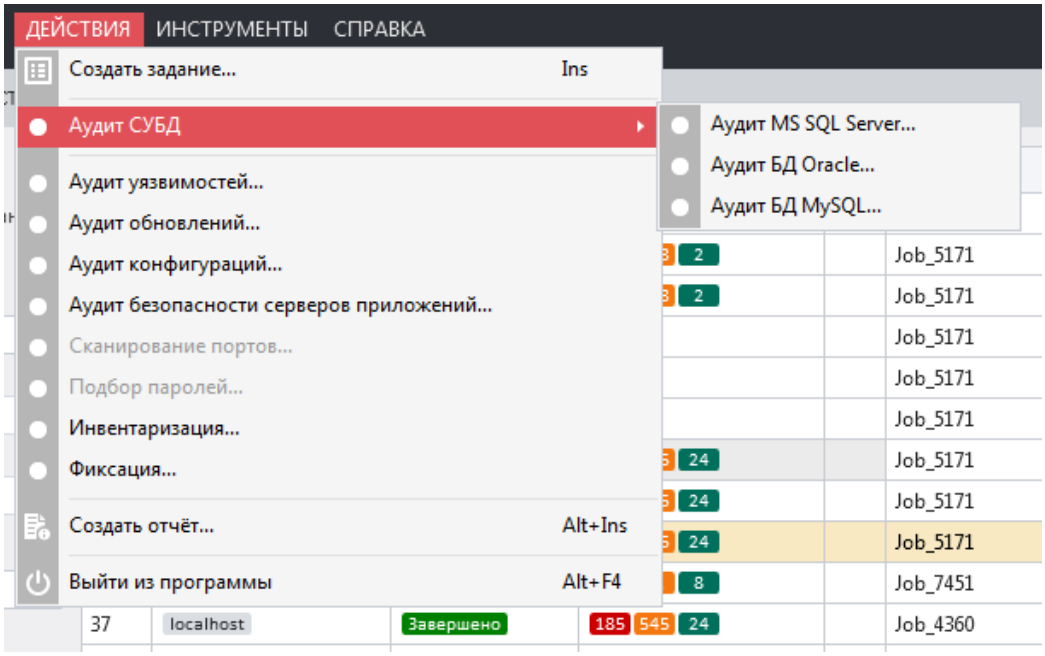


Рисунок 4.3.1.2

Команда *«Создать отчет»*.

Нажатие этой кнопки запускает мастер создания отчета (Рисунок 4.3.1.3).

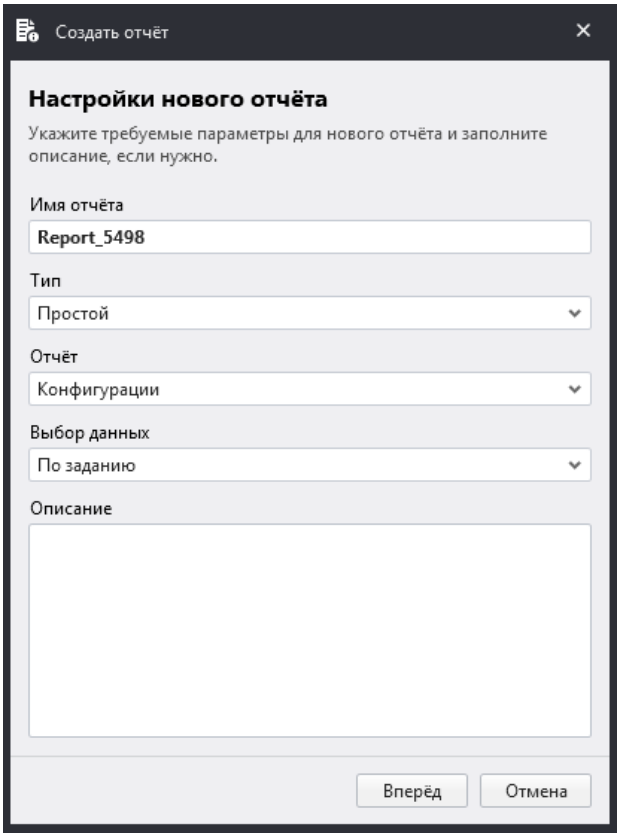


Рисунок 4.3.1.3

Окно создания нового отчета содержит следующие атрибуты:

- ***Имя отчета***
- ***Тип*** - выбор типа отчета (простой или дифференциальный)
- ***Отчет*** - выбор типа сканирования, по которому строится отчет
- ***Выбор данных*** - тип выборки (по заданию, по хостам, по единичному хосту)
- ***Описание*** - комментарии к отчету
- Команда ***«Выйти из программы»***

Содержание главы...

4. Интерфейс программы » 4.3 Меню программы » 4.3.2 Меню «Инструменты»

При выборе пункта меню «***Менеджер учетных записей***» (Рисунок 4.3.2.1) появляется возможность создавать, редактировать и назначать учетные данные пользователя, от имени которого будет проводиться сканирование.

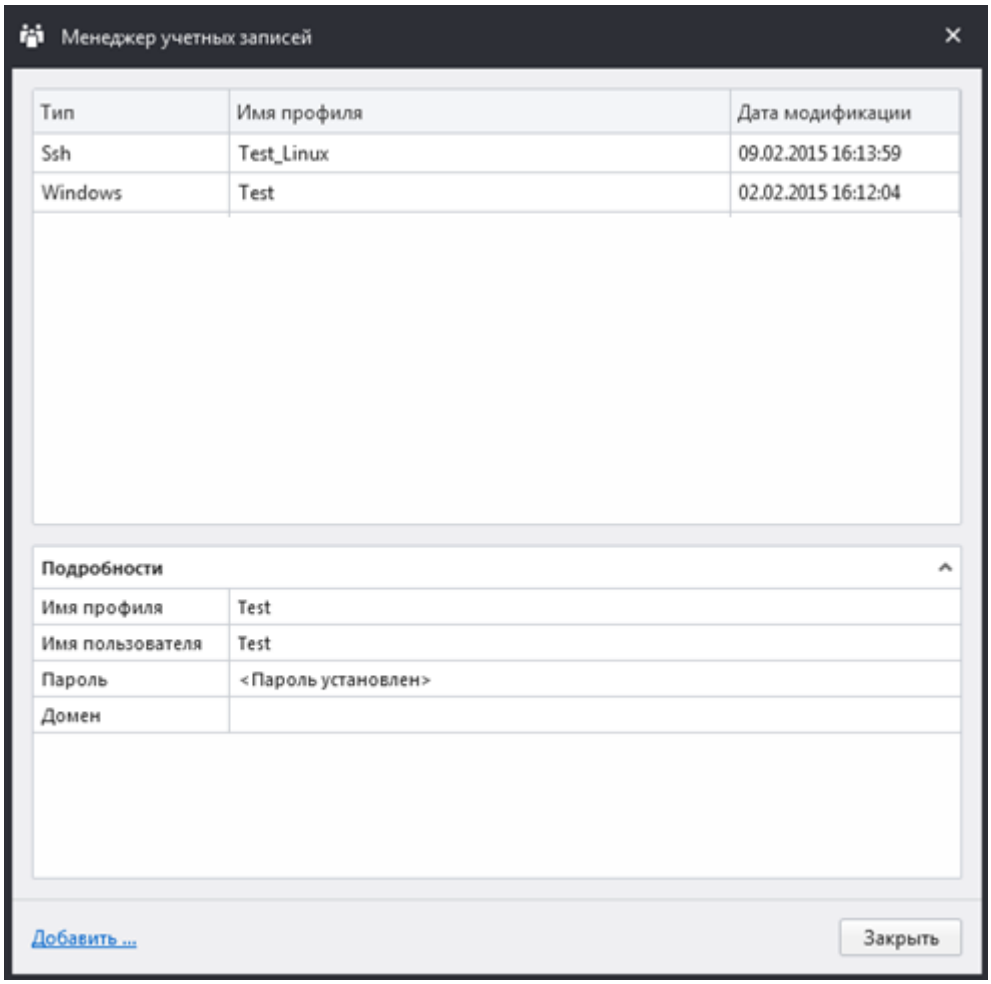


Рисунок 4.3.2.1

При выборе пункта меню «***Менеджер сетевых каталогов***» (Рисунок 4.3.2.2) можно назначать сетевые каталоги, в которые будут сохраняться отчеты с результатами выполнения заданий (**Функционал доступен только в WEB-версии продукта**).

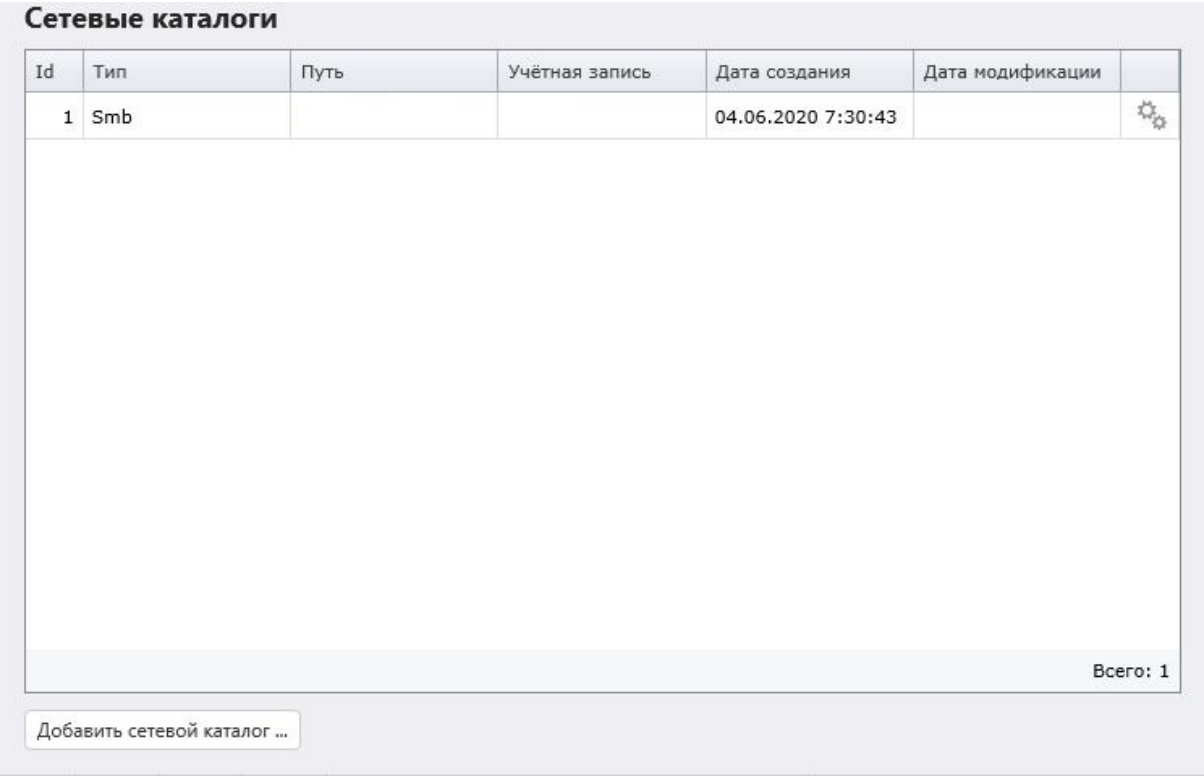


Рисунок 4.3.2.2

При выборе пункта меню «***Менеджер аудитов***» в режиме **«аудиты»** демонстрируются все доступные проверки уязвимостей, каждой из которых дано подробное описание в стандартизированном формате CVE (Рисунок 4.3.2.3). В режиме ***«Профили»*** пользователю предоставляется возможность самостоятельно создавать/редактировать ленты обновлений или уязвимостей, на основе уже имеющихся в базе (Рисунок 4.3.2.3).

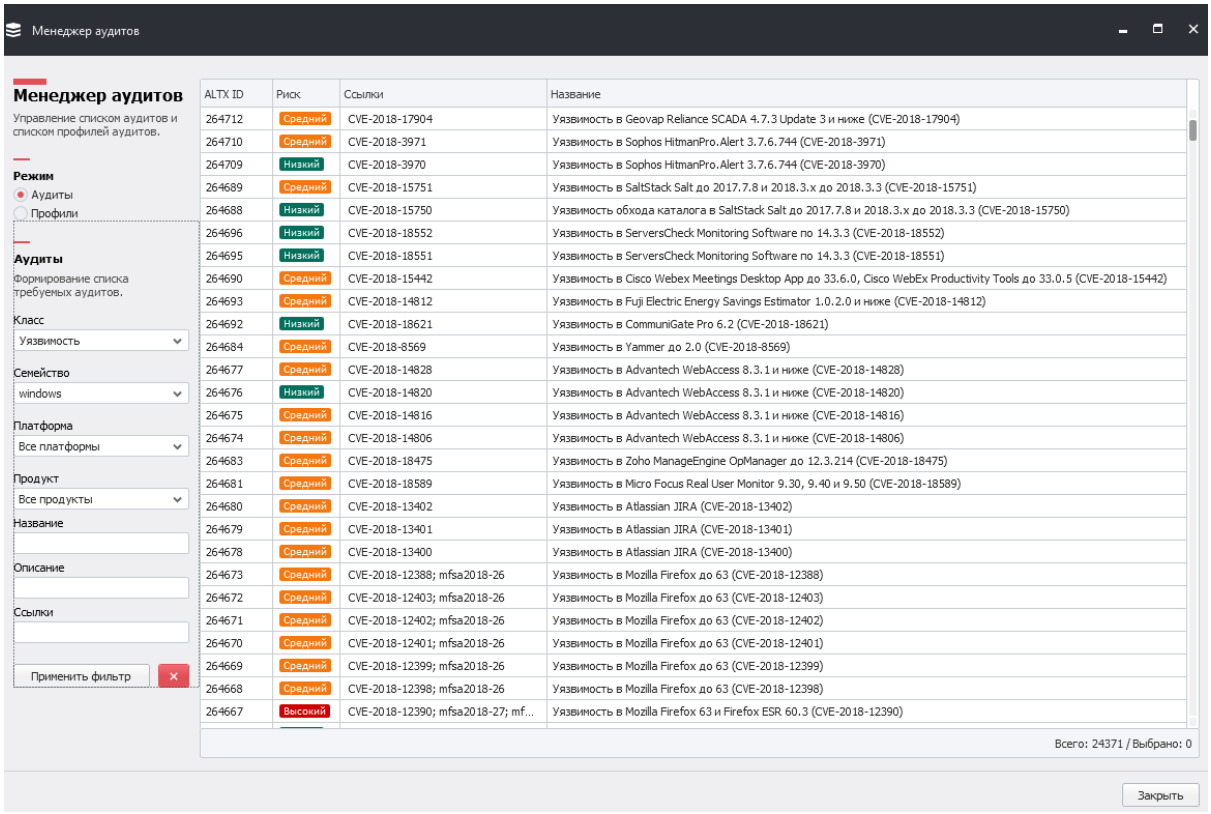


Рисунок 4.3.2.3

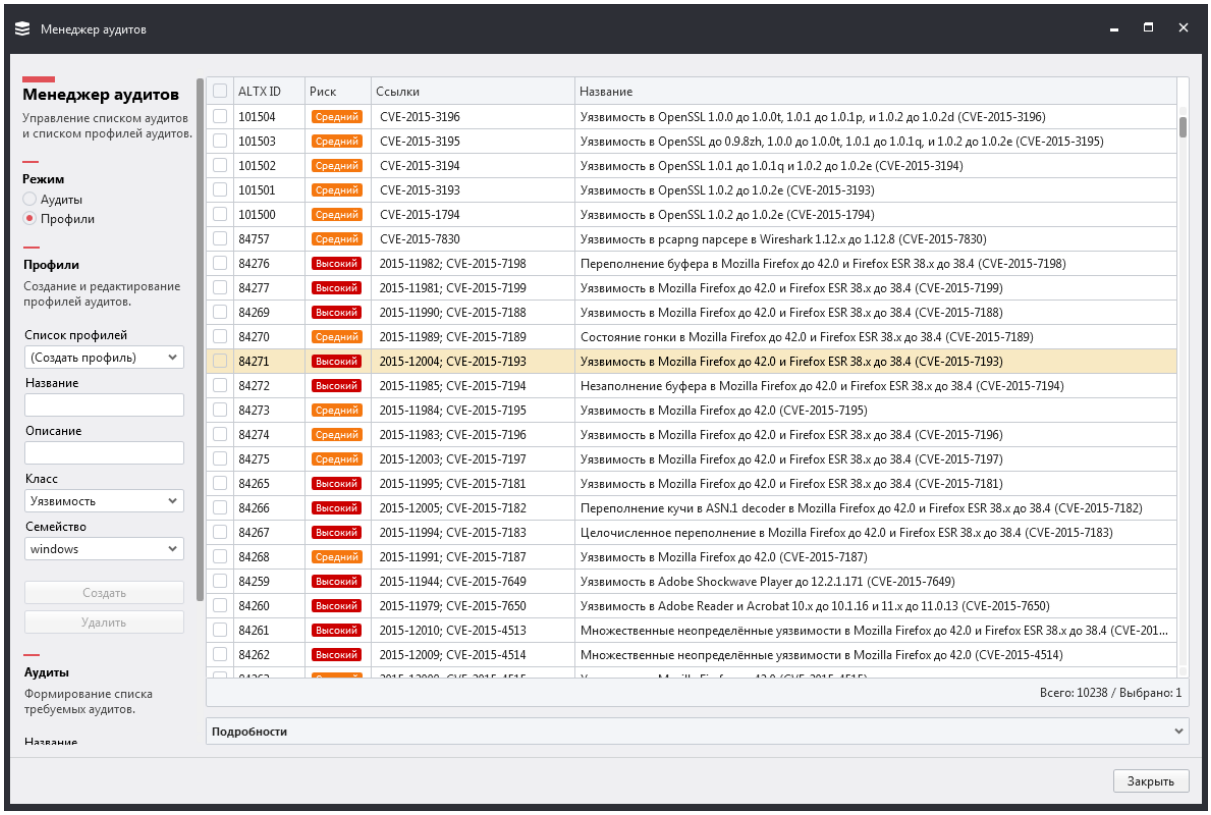


Рисунок 4.3.2.4

При выборе пункта меню «*Менеджер конфигураций*» отображаются все доступные конфигурации безопасности (Рисунок 4.3.2.5). Для удобства выбора можно использовать ниспадающее меню *«Фильтр по платформам», «Фильтр по продуктам»*, а также поиск по конфигурациям, расположенные в верхней части окна. В правой части окна находится поле с подробным описанием конфигураций:

Название (конфигурации);

- *Версия*
- *Файл* - имя файла конфигурации
- *Платформа* - список платформ, с которыми совместима выбранная конфигурация
- *Описание* - описание выбранной конфигурации
- *Примечание* - дополнительные комментарии

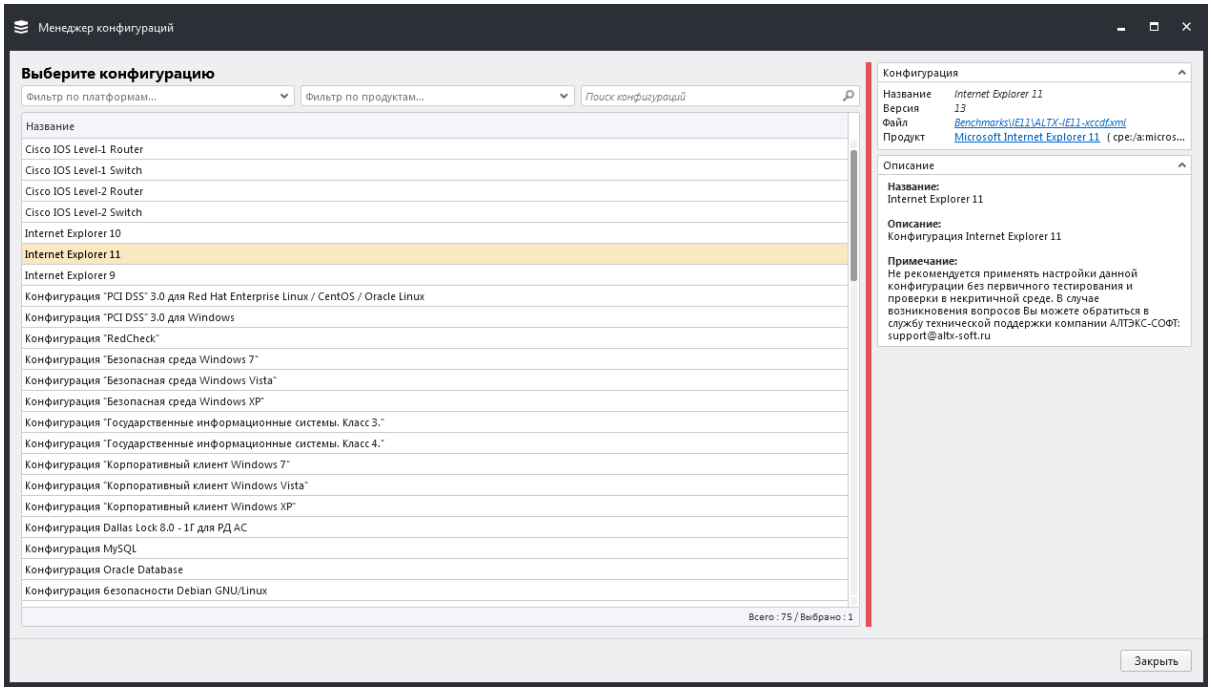


Рисунок 4.3.2.5

Пункт меню *«Консоль WSUS»* (Рисунок 4.3.2.6) позволяет открыть модуль для работы со WSUS'ом, где можно настроить загрузку файлов обновлений.

Описание данной функции в составе модуля *«Патч Менеджмент»* представлено в документе PatchManagement.pdf. Доступ из программы: *Справка - Руководство*.

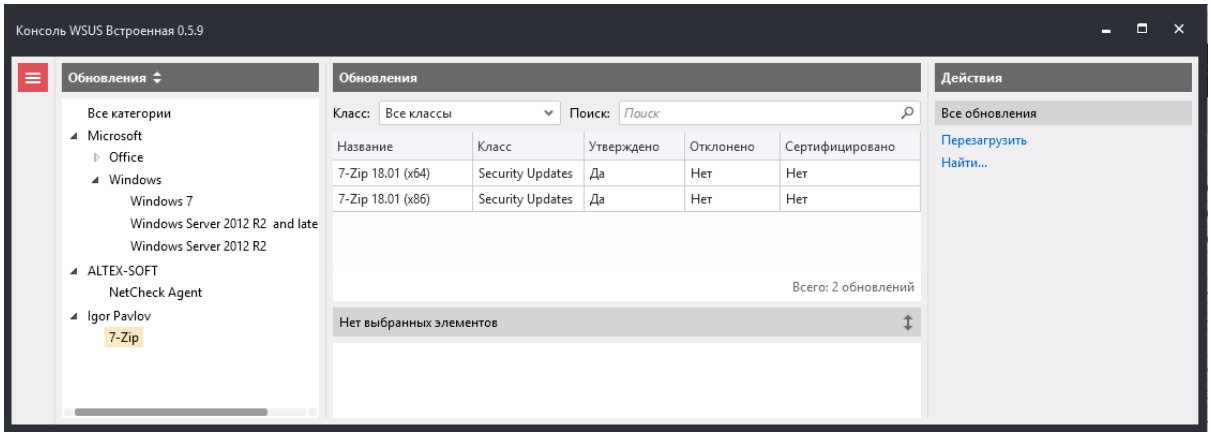


Рисунок 4.3.2.6

Пункт меню «***Создать группу***» (Рисунок 4.3.2.7) позволяет группировать хосты. После группировки, созданная группа появится на вкладке ***«Хосты»*** в таблице ***«Группы хостов»***.

В окне создания новой группы хостов можно определить следующие параметры:

- ***Имя*** - имя создаваемой (редактируемой) группы
- ***Описание*** - комментарии о создаваемой (редактируемой) группе
- ***Хосты*** - список хостов, которые входят в создаваемую (редактируемую) группу

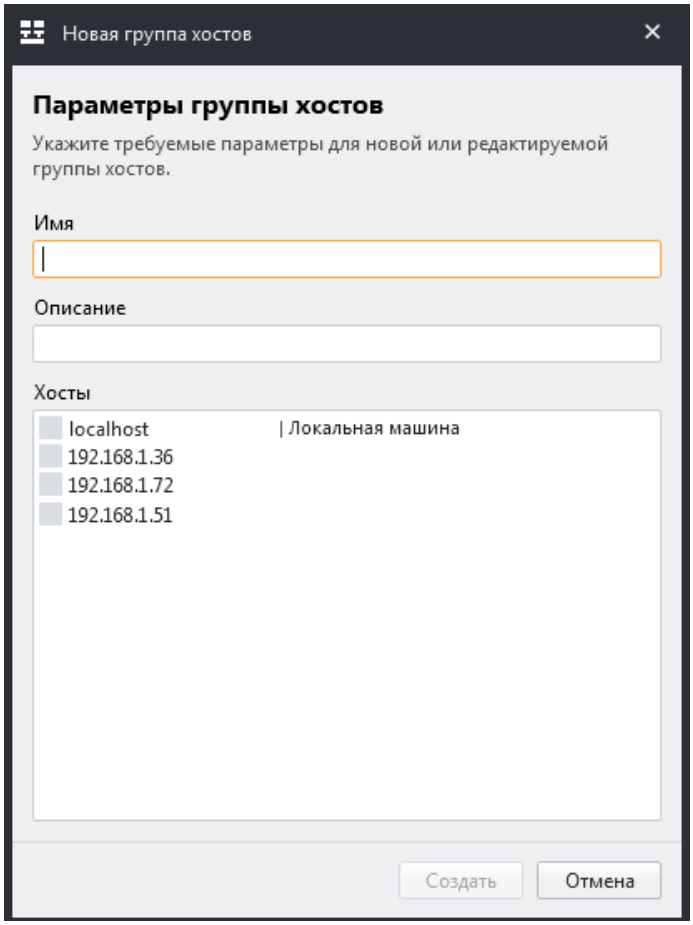


Рисунок 4.3.2.7

В пункте меню ***«Создать хост»*** можно добавить новый хост (Рисунок 4.3.2.8).

В окне создания можно определить следующие параметры:

- ***Хосты*** - задать хост;
- ***Описание*** - внести комментарии о создаваемом хосте;
- ***Группы*** - указать группы, в которые будет входить хост.

После создания хост появится на вкладке ***«Хосты»*** в таблице ***«Хосты»***, в ***«Группе: по умолчанию»*** и в ранее заданной группе.

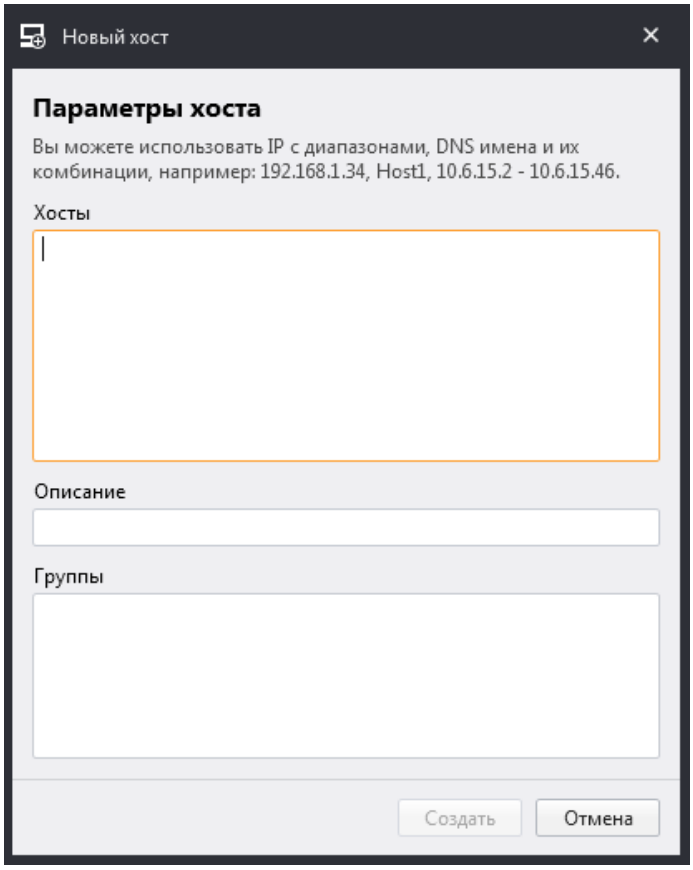


Рисунок 4.3.2.8

Пункт меню ***«Импорт хостов»*** позволяет импортировать хосты используя:

- ***Active Directory*** (Рисунок 4.3.2.9);
- Утилиту сканирования IP-сетей Nmap (Рисунок 4.3.2.10).
- Csv-file (данный метод описан в ПРИЛОЖЕНИЕ Б).

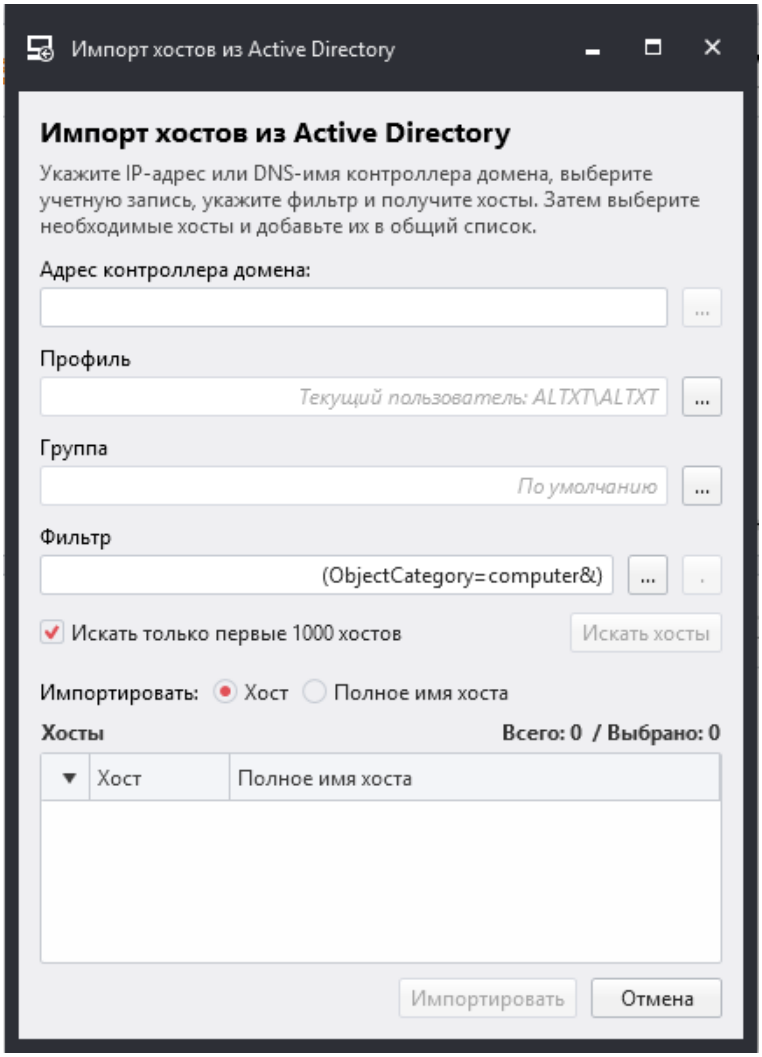


Рисунок 4.3.2.9

Поле ***«Адрес контроллера домена»*** может быть заполнено как автоматически (если выбрана состоящая в домене учетная запись), так и вручную. Данное поле дает возможность задать не только имя домена, но и, например, имя организационной единицы в формате ***«ou=Seven,dc=altx-soft,dc=ru»***.

Поле ***«Профиль»*** позволяет задать учетные данные для поиска элементов Active Directory.

Поле ***«Группа»*** позволяет выбрать группу, в которую будут импортированы Active Directory.

Поле ***«Фильтр»*** позволяет отфильтровать результаты поиска в AD. По умолчанию поле ***«Фильтр»*** имеет значение ***«(&ObjectCategory=computer)»***, что позволяет произвести выборку объектов типа ***«Компьютер»***.

Если нажать на кнопку « . » - откроется список хостов в виде дерева, из которого можно будет выбрать только интересующие машины.

Доступен выбор: импортировать хост или полное имя хоста.

 *Значение фильтра не может быть пустым. При попытке выполнить поиск хостов с пустым значением фильтра будет выполнен поиск со значением фильтра «(&ObjectCategory=computer)».*

Примеры и возможные значения фильтра приведены в ПРИЛОЖЕНИЕ А.

Поле ***«Хосты»*** содержит выборку, возвращенную в результате поиска.

Сетевой сканер Nmap (Рисунок 4.3.2.10).

Данный пункт меню доступен, если на компьютере установлен компонент NMAP, его можно настроить ***«Инструменты» - «Настройки» - «Компонент Nmap»***.

В форме задаётся IP-адрес сети в CIDR-формате. Например, 192.168.1.0/24 означает, что будут сканироваться хосты от 192.168.1.1 до 192.168.1.254. После задания маски необходимо нажать на кнопку ***«Искать хосты»***.

По завершению сканирования, результаты будут представлены в таблице ***«Хосты»***. Искомые ip-адреса надо выделить и нажать кнопку ***«Импортировать»***.

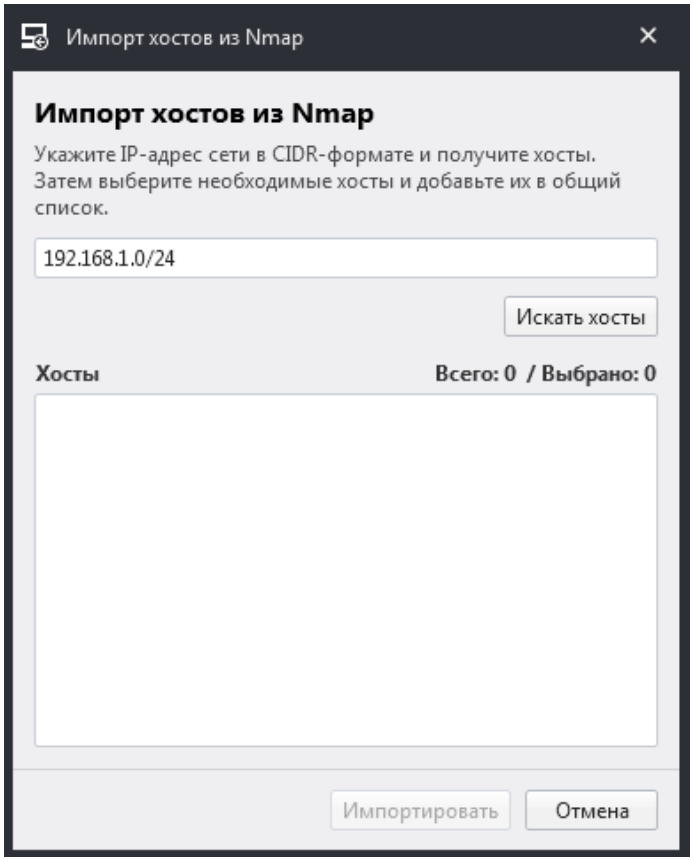


Рисунок 4.3.2.10

Пункт меню ***«Синхронизация»*** позволяет выполнять обновление информационного контента безопасности.

Для выполнения офлайн синхронизации необходимо указать локальную или сетевую папку, в которую был предварительно помещен информационный контент безопасности.

Пункт меню ***«Импорт OVAL определений»*** позволяет расширить функционал программы в части аудита обновлений и аудита уязвимостей системного и прикладного ПО, с помощью импорта произвольных сигнатур, описанных в виде OVAL определения. Функция позволяет добавлять описания уязвимостей и обновлений, еще отсутствующме в репозиторий OVALdb. Подробнее об OVAL можно узнать по ссылке: https://oval.mitre.org.

Раздел «*Настройки*» включает в себя следующие подразделы:

- *Общие*
- *Компонент Nmap*

- *Доставка*
- *Дополнительно*
- *Синхронизация*

Вкладка *«Общие»* содержит следующие настройки (Рисунок 4.3.2.11):

- *Число параллельных заданий* (одновременно запущенных)
- *Использовать кэш инвентарей для ускорения сканирования*
- *Отображать статистику на главной вкладке*
- *Таймаут операций с агентом*
- *Сервер БД* - строка подключения к базе данных RedCheck
- *Имя БД* - имя базы данных RedCheck
- *Имя пользователя* - имя пользователя(login) базы данных RedCheck
- *Пароль* - пароль пользователя (password) базы данных RedCheck
- *Таймаут операций с БД* - диапазон допустимых значений от 60 и до 600 секунд. Позволяет пользователю вручную увеличивать тайминг, если возникают какие-либо задержки при соединении с БД
- *Проверить соединение с БД* - проверка соединения с консоли управления с базой данных. Если индикатор имеет зеленый цвет - соединение установлено, при красном цвете индикатора - соединение отсутствует
- *Путь к папке* (по умолчанию RedCheck\Data), содержащей контент безопасности и другие данные
- *Путь к папке* с временными файлами (по умолчанию: RedCheck\Reports)
- *Путь к папке* с отчетами (по умолчанию: RedCheck\Reports)
- *Формат отчёта по умолчанию* - можно по умолчанию установить формат отчёта pfd или html
- *Язык* - доступны английский и русский языки интерфейса.

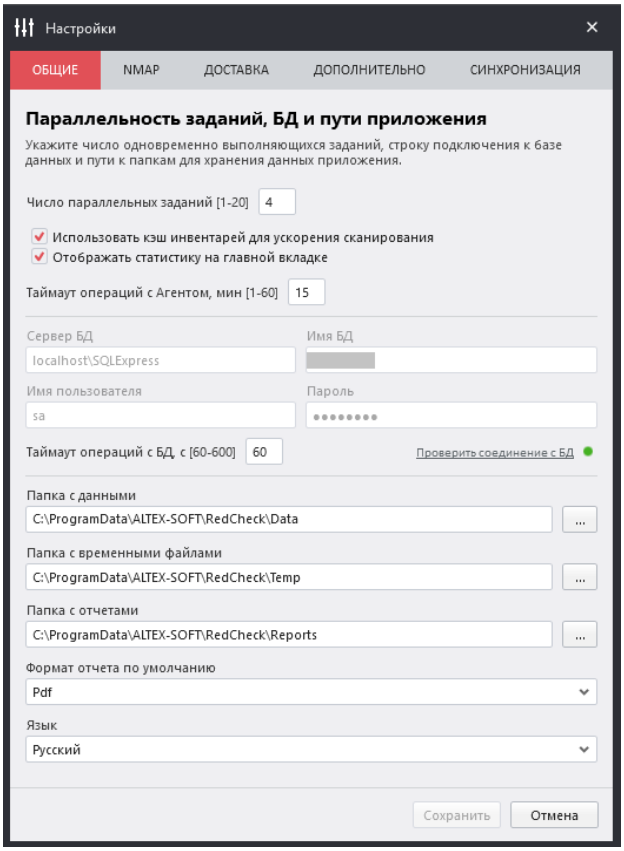


Рисунок 4.3.2.11

Вкладка ***«Компонент Nmap»*** содержит следующие настройки:

- ***Использовать Nmap*** - включение/выключение интеграции с Nmap;
- ***Путь к Nmap*** - путь к утилите Nmap;
- ***Путь к словарю логинов/паролей*** - источник словарей логинов/паролей компоненты. (Рисунок 4.3.2.12).

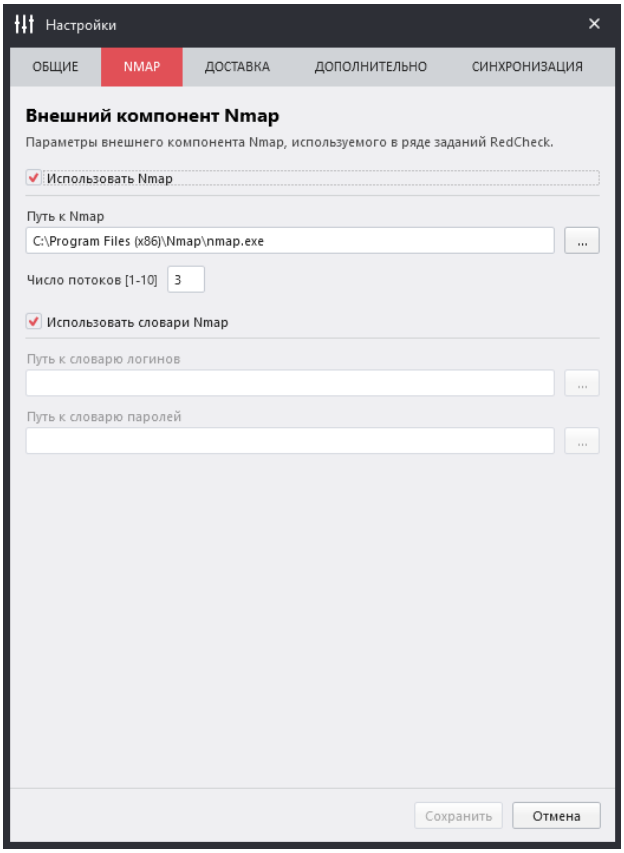


Рисунок 4.3.2.12

Во вкладке ***«Доставка»***, можно настроить отправку электронных писем с результатами сканирований, отчётов и другой важной информации (Рисунок 4.3.2.13).

Вкладка ***«Доставка»*** содержит следующие настройки:

- **Включить сервис доставки** - активация функции отправки электронных писем с результатами сканирований
- **Адрес сервера исходящих сообщений**
- **Порт**
- **Включение SSL**
- **Логин**
- **Пароль**
- **E-mail отправителя**
- **E-mail получателя**
- **Кодировка писем**

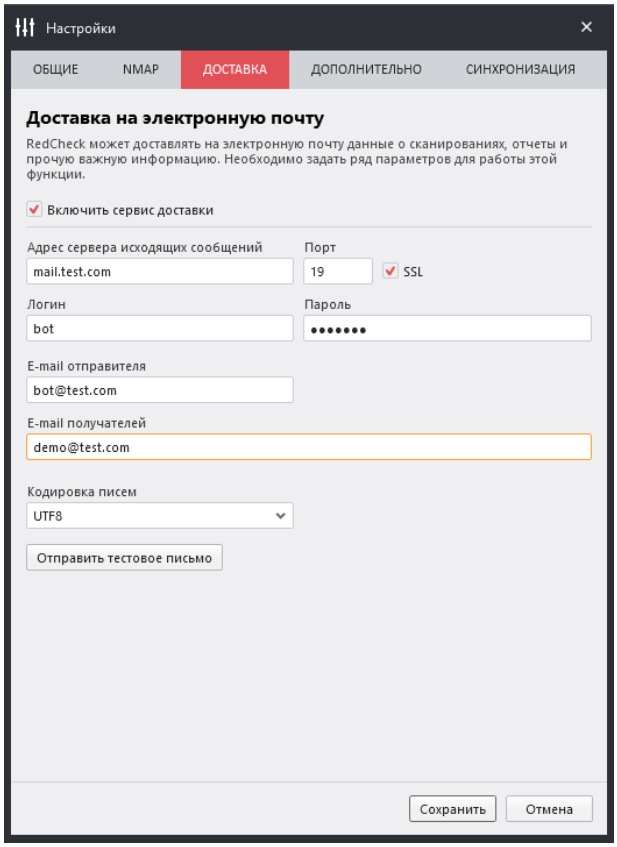


Рисунок 4.3.2.13

Вкладка ***«Дополнительно»*** содержит следующие настройки (Рисунок 4.3.2.14):

- ***Вход*** - по умолчанию вход в приложение доступен для всех пользователей, но можно ограничить доступ, задав имя пользователя и пароль
- ***Группы Безопасности пользователя*** - приложение может проверять доменные и локальные группы. Выбирается в соответствии с типом сети в которой работает RedCheck

Генератор имен:

- Позволяет задавать шаблоны для формирования имён заданий, по которым осуществляются подстановки
- ***«Использовать генератор имен по умолчанию»*** - заданный паттерн будет применяться для всех имен новых заданий
- Автопроверка новых задач - служба сканирования будет периодически проверять БД на наличие новых задач. Данная опция позволяет удаленным службам сканирования с заданной периодичностью опрашивать базу

данных на предмет существования заданий, требуемых к выполнению данной службой.

- Проверка триггера обновлений - служба будет периодически проверять БД на необходимость запуска обновления. Данная функция предназначена для работы с удалённым подключением RedCheck.

Логирование:

- Сохранение промежуточных результатов сканирований в файл, генерация html-файла, сохранение системных характеристик для OVAL-сканирований;
- Сохранение файлов-результатов для инвентаризации;
- Сохранение файлов-результатов для компонента NMAP;
- Сохранение подробного лога работы RedCheck.

Служба RC WSUS Service:

- Настройка адреса, порта, а также логина и пароля при использовании авторизации.
- Прокси-сервер:
- Настройка адреса, порта, а также логина и пароля при использовании авторизации, а также использовать аутентификацию Windows.

- *Параметр: «Не использовать прокси службой сканирования» означает, что заданные настройки не будут применяться для службы сканирования, а только для консоли управления и службы синхронизации.*
- *Для работы аутентификации Kerberos, необходимо использовать DNS-имя прокси сервера, а не его IP-адрес.*

Для того, чтобы задать имя пользователя и пароль для входа в RedCheck, необходимо установить флаг ***«Включить вход по паролю»***. При последующих входах в программу, необходимо будет указать заполненные учётные данные.

Для того, чтобы войти в мастер «Генератора имён», необходимо установить флаг в ***«Использовать генератор имен по умолчанию»***, а также нажать на кнопку «...» справа от поля ***«Паттерн по умолчанию»***.

В открывшемся ***«Генераторе имён»*** содержится 4 таблицы (Рисунок 4.3.2.15):

- ***Переменные*** – список доступных к использованию переменных с примерами значений. Для автоматического добавления переменной в шаблон, необходимо совершить двойной клик мышью по нужному параметру
- ***Справочные данные*** – содержится информация, описывающая особенности каждой из переменных, для использования её в шаблоне
- ***Входная строка*** – здесь задаётся шаблон названия, используя переменные
- ***Выходная строка*** – отображение примера названия, полученного на основе шаблона (входной строки)

Для того, чтобы выполнить офлайн синхронизацию, необходимо:

- В разделе ***«Синхронизация по расписанию»*** поставить галочку в пункте ***«Автоматически офлайн (ежедневно)»***
- Выбрать директорию, откуда будет выполняться синхронизация контента, можно нажав многоточие
- Далее необходимо указать время ежедневной синхронизации
- По желанию пользователя, можно активировать функцию оповещения о завершении синхронизации, выбрав пункт ***«По завершении синхронизации отправлять e-mail»***
- Настройка отправки электронных писем выполняется на вкладке ***«Доставка»: «Инструменты» →«Настройки» → «Доставка»***

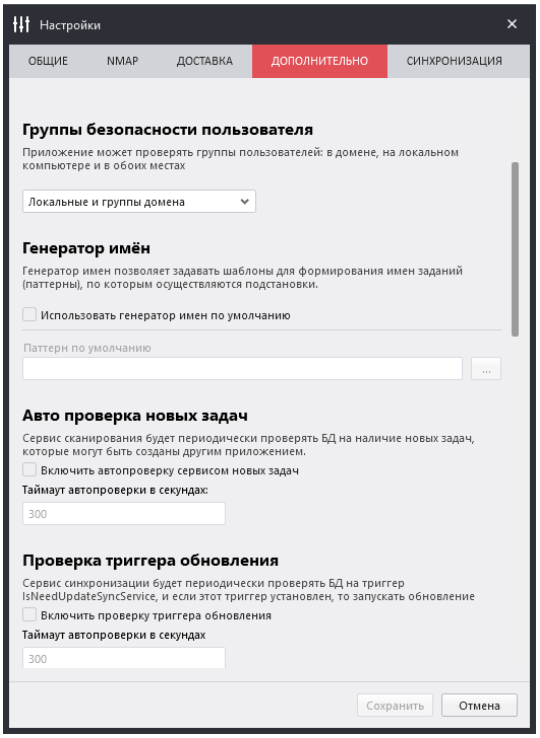


Рисунок 4.3.2.14

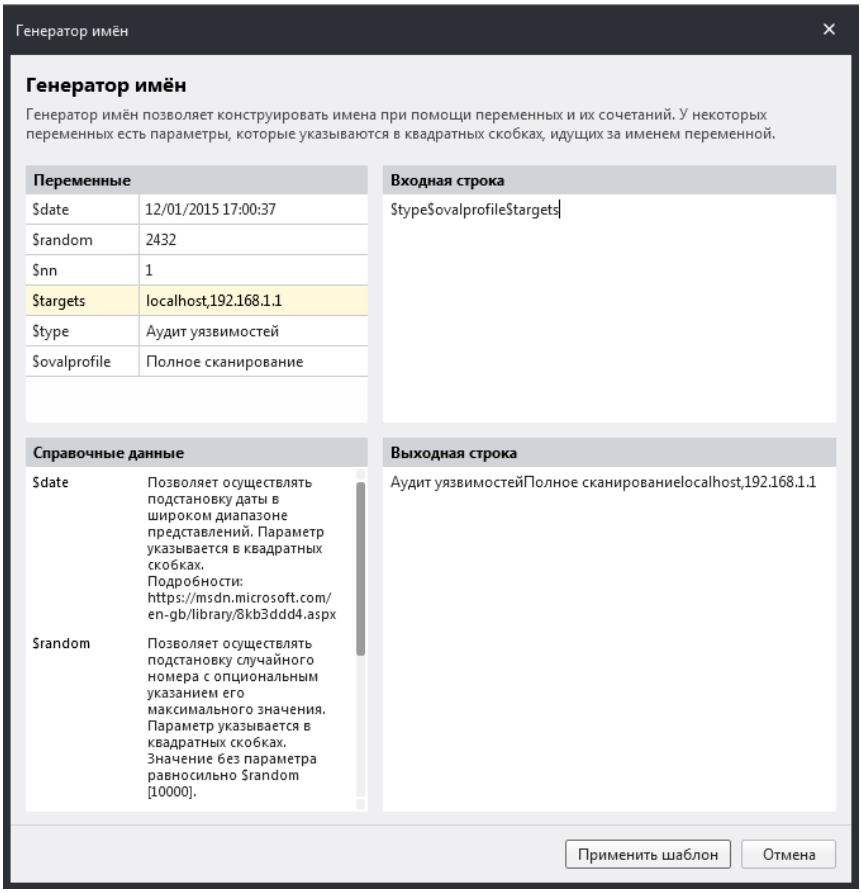


Рисунок 4.3.2.15

Вкладка ***«Синхронизация»*** содержит следующие настройки:

- ***Служба синхронизации по умолчанию***. ***«Локально»***, если на АРМе с установленной консолью RedCheck есть свободный доступ в Интернет, это позволяет производить синхронизацию контента безопасности в Вашу БД через прямой доступ к сети интернет, либо, если на сервере с консолью RedCheck нет свободного доступа в Интернет, устанавливаем автономную службу синхронизации на удаленном сервере с доступом к сети интернет, присваивая ей имя в мастере установки и выбираем ее в выпадающем списке как службу через которую RedCheck будет производить обновления контента безопасности
- ***Сервер синхронизации***. В случае необходимости изменения адреса синхронизации, в поле «Сервер синхронизации» можно будет указать новый адрес сервера
- ***Синхронизация вручную, автоматическая или автоматическая офлайн синхронизация по расписанию***
- ***Доставка.*** По завершении синхронизации отправлять e-mail - при включении этой функции, на указанный e-mail будет отправляться информирующее письмо после каждой синхронизации контента безопасности RedCheck (настройки почты проводятся на вкладке «Доставка»)
- ***Токен доступа для файлов ПМ -*** токен для авторизации со службой синхронизии, используется для работы ПМ

Выбор пункта меню ***«Журнал событий»*** (Рисунок 4.3.2.16) открывает лог, содержащий сведения о произошедших событиях, связанных с работой консоли управления, службой сканирования, сервера синхронизации и базой данных.

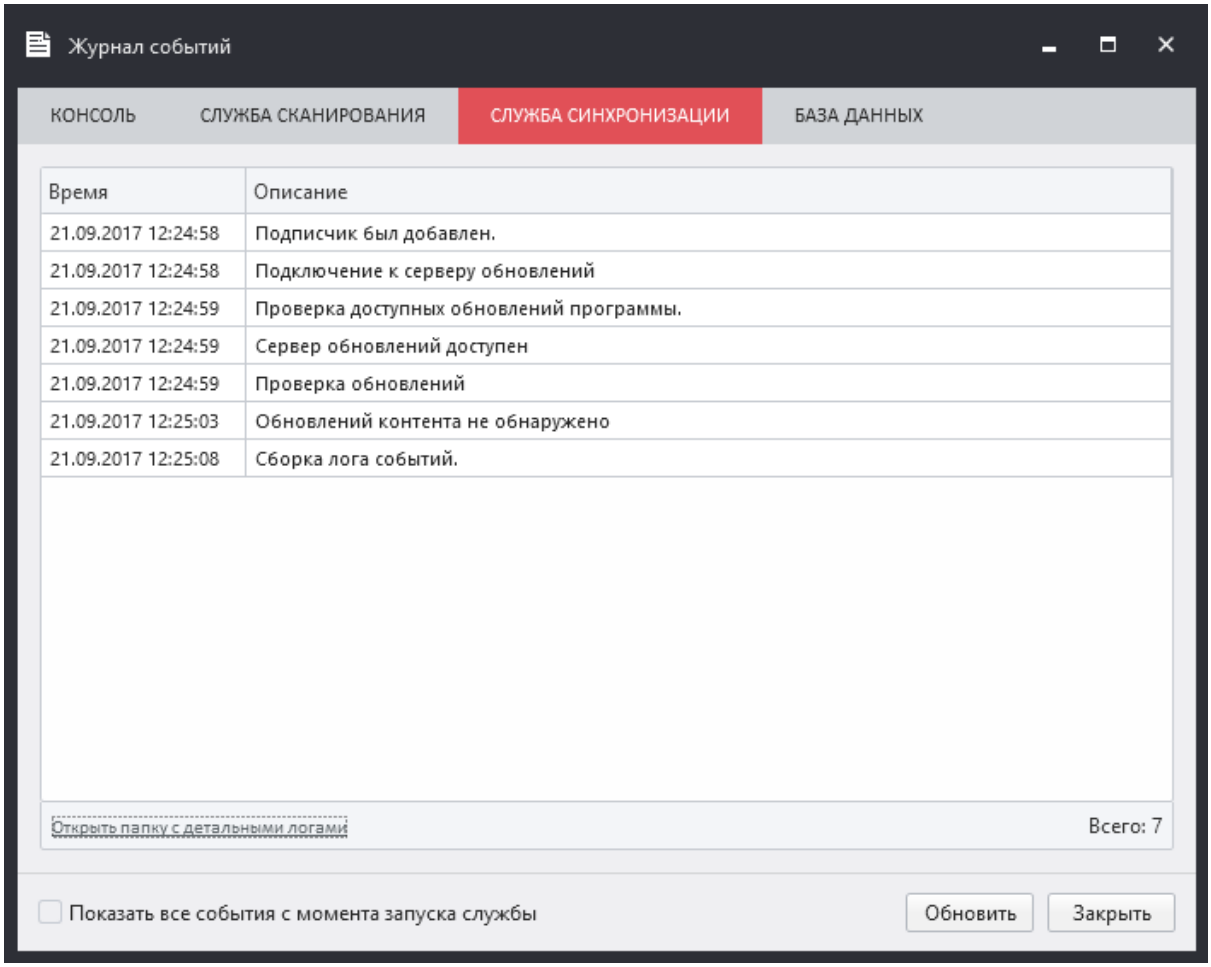


Рисунок 4.3.2.16

Пункт меню ***«Подключения»***, позволяет:

- переподключиться к службе сканирования;
- перезапустить службу сканирования / синхронизации.

Пункт меню ***«Диагностика»***, включает в себя ***«Мастер диагностики проблем» и «Проверку целостности контента»***.

Пункт меню ***«Мастер диагностики проблем»***.

Данное меню позволяет провести анализ состояния отдельных компонентов RedCheck, таких как: база данных, служба сканирования и синхронизации, система лицензий, а также решить возможные проблемы или получить подробную информацию о том, что делать, если проблему решить не удается (Рисунок 4.3.2.17).

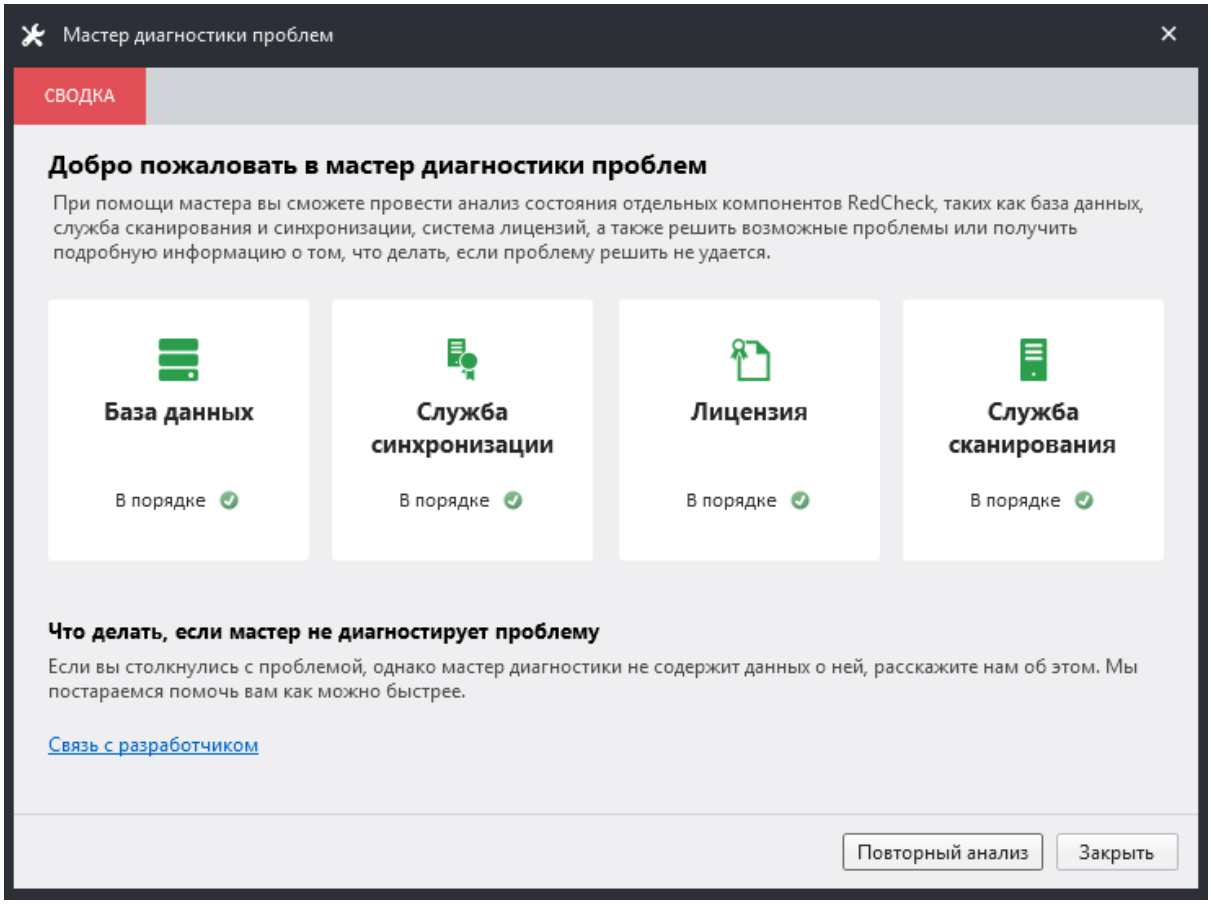


Рисунок 4.3.2.17

Пункт меню ***«Проверка целостности контента»***.

Данное меню позволяет, проверить наличие избыточных или осиротевших элементов контента в базе RedCheck.

Содержание главы...

Меню ***«Справка»*** включает в себя следующие подразделы:

«*Руководство*» - открывает файл с руководством администратора.

«*Разработчик*» - быстрый переход на сайт разработчика RedCheck - http://altx-soft.ru/.

«*Сменить лицензионный ключ*» - позволяет указать другой лицензионный ключ программы.

«*Проверить целостность*» - сравнение контрольных сумм исполняемых файлов и библиотек с эталонными значениями.

«*О программе*» - отображает информацию о программе, в частности (Рисунок 4.3.3.1) сведения о программе:

- Версия программы
- Версия Scap-процессора
- Версия контента
- Время последней синхронизации
- Версию БД
- Уникальный ID программы
- Лицензионный ключ
- Тип лицензии
- Статус лицензии
- Аудит VmWare
- Патч Менеджмент
- Аудит уязвимостей
- Количество хостов в лицензии
- Количество используемых хостов
- Дата активации

- Дата окончания срока действия
- Общая длительность срока действия лицензии
- Оставшееся время
- Владелец лицензии
- Код активации
- Сайт разработчика
- Сайт продукта
- Группы безопасности пользователя

Информация о модуле аудита безопасности серверов приложений:

- Активность модуля
- Количество хостов лицензии
- Дата окончания срока действия

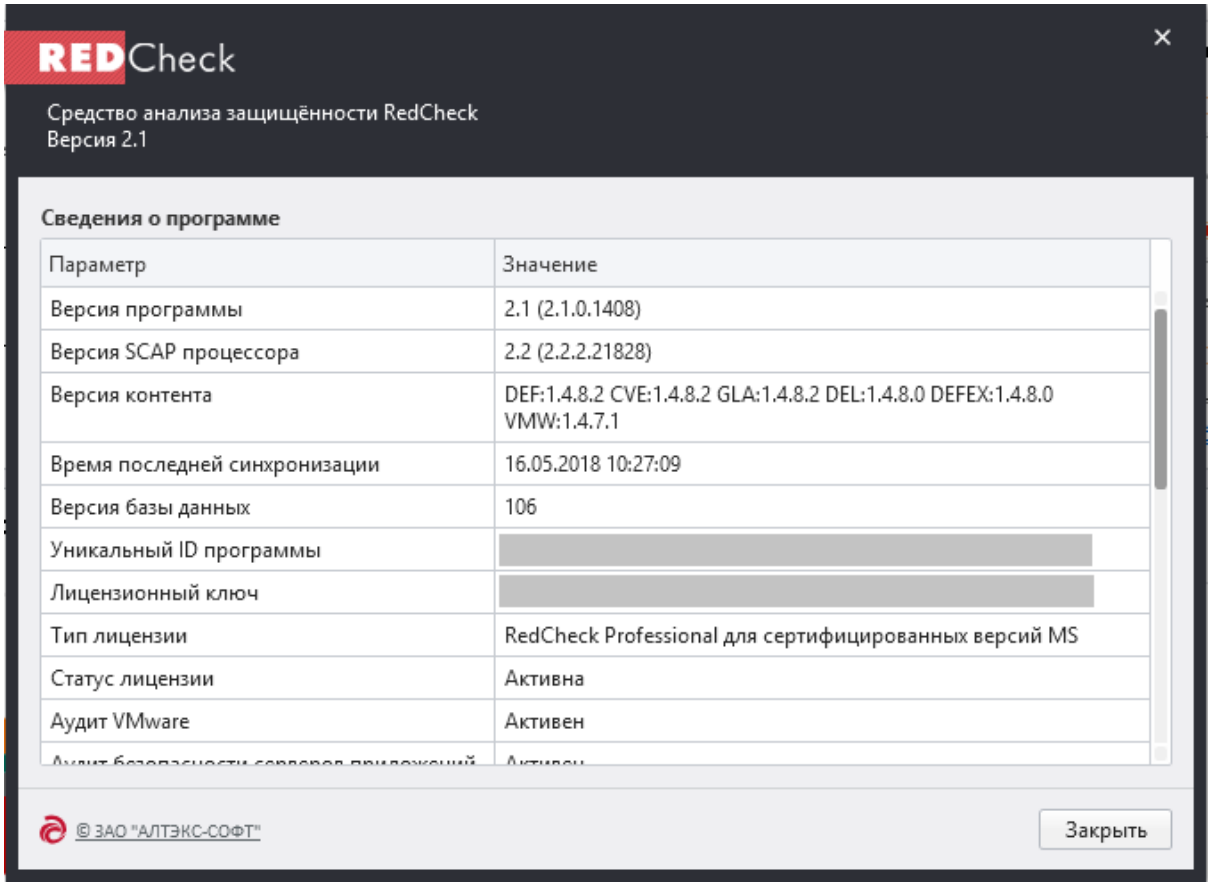


Рисунок 4.3.3.1

Содержание главы...

5. Работа с программой

5.1 Предварительная настройка

 *Синхронизация контента в RedCheck работает посредством протокола защиты не ниже TLS 1.2!*

Загрузка обновлений контента безопасности может быть выполнена двумя способами:

- Синхронизация через интернет (по умолчанию)
- Синхронизация без доступа в интернет

Синхронизация через интернет является предпочтительным методом загрузки обновлений контента безопасности.

Синхронизация через интернет

Данный способ используется, если система имеет подключение к сети Интернет, и получение траффика из узла обновлений https://sync.altx-soft.ru по протоколу ***HTTPS*** не противоречит политике безопасности.

1. Для выполнения обновления запустить RedCheck любым удобным способом. Например, в меню пуск ввести имя RedCheck и запустить приложение.

 *Для применения изменений, связанными с учётными записями и группами, потребуется выполнить **log out - log in** (в доменной сети потребуется **log out - log in** контроллера домена и клиентской машины).*

2. Если в нижней части окна отобразится сообщение ***«Доступно обновление контента»***, а индикатор красного цвета, то контент отсутствует полностью, если желтого цвета, это означает, что контент утратил актуальность и необходимо выполнить обновление. Активируйте функцию

«Синхронизировать» и дождитесь окончания обновления. В случае успешной синхронизации обновления - на статусной панели появится сообщение «Сохранение контента в БД успешно завершено», а индикатор состояния контента изменит цвет на зеленый.

Синхронизация без доступа в интернет

Если компьютер, на котором установлен RedCheck, невозможно подключить к Интернету, то обновление контента выполняется через синхронизацию без доступа в Интернет. Для выполнения данного типа синхронизации необходимо следующее:

Активация лицензии:

1. Если лицензия не была активирована, для активации открыть выпадающее меню *«Справка»* и выбрать пункт *«О программе»*. Скопировать строку *«Код активации»* и *«Лицензионный ключ»*: для этого левой кнопкой мыши выделить строку и нажать комбинацию клавиши *Ctrl + C*.

2. Далее обратиться в компанию АЛТЭКС-СОФТ, написав запрос на электронную почту support@altx-soft.ru с просьбой сформировать файл лицензии. Указать в письме лицензионный ключ и код активации программы.

3. Если лицензия ранее была активирована, но необходимо получить файл лицензии, то:

- Войдите на закрытую часть https://update.altx-soft.ru (рекомендуется использовать браузер **Internet Explorer**), авторизуйтесь при помощи ключа *e-token*.
- Перейдите в раздел *«RedCheck»* и выбрать пункт *«RedCheck лицензии»*. Выбрать нужную лицензию кликом левой кнопки мыши.
- Далее, в открывшемся окне будет отображена информация о лицензии. Для того, чтобы загрузить лицензию, нажать на кнопку *«Скачать»*.
- Сохранить файл лицензии **license.xml** в директорию по умолчанию: *C:\ProgramData\ALTEX-SOFT\RedCheck\Data*. Если в указанной директории нет каталога *\ALTEX-SOFT\RedCheck\Data*, проверить его наличие в директории *C:\Users\All Users*.

*По умолчанию, каталог **«ProgramData»**- скрытый. Настроить отображение скрытых файлов можно в: **Панель управления→Все элементы панели управления→Параметры папок→Вид***

- Перезапустить консоль RedCheck.

Обновление контента безопасности:

1. Получить контент безопасности в центре сертифицированных обновлений АЛТЭКС-СОФТ: https://update.altx-soft.ru (рекомендуется использовать браузер **Internet Explorer**). Это можно сделать с любой системы, имеющей выход в сеть интернет.
2. Авторизоваться на сайте https://update.altx-soft.ru при помощи ключа ***e-token***.
3. Перейти в раздел ***«Файлы»***.
4. Выбрать и скачать ***RedCheck_OfflineData***.
5. Загруженный контент представляет собой архив в формате **zip**.
6. Если по каким-либо обстоятельствам невозможно совершить данную процедуру - обратитесь в службу поддержки support@altx-soft.ru.
7. Любым удобным способом перенести контент на систему с установленным RedCheck. Распаковать **zip** архив в папку, из которой будет выполняться обновление.
8. Запустить RedCheck, открыть выпадающее меню ***«Инструменты» - «Синхронизация»*** и выбрать ***«Офлайн-синхронизация»***. В открывшемся окне указать папку, в которую ранее был распакован контент. Нажать ***«ОК»*** и дождаться окончания синхронизации. В случае успешного выполнения синхронизации на нижней статусной панели консоли RedCheck появится сообщение ***«Сохранение контента в БД успешно завершено»***.

Содержание главы...

В менеджере учетных записей создаются учетные записи, от имени которых будет осуществляться реализация основного функционала RedCheck на клиентских компьютерах.

Для добавления новой учетной записи необходимо перейти в ***«Инструменты» →«Менеджер учетных записей»***.

*По умолчанию, учётная запись хранится в БД в зашифрованном виде: установлен флаг на пункте **«Сохранять, используя шифрование»**. Рекомендуется хранить УЗ в незашифрованном виде в случае использования технологии удаленного управления.*

Для создания новой учетной записи RedCheck необходимо:

- В нижнем левом углу формы ***«Менеджер учетных записей»***, нажать на кнопку ***«Добавить»***, либо в таблице «учетных записей» вызвать контекстное меню, правой кнопкой мыши и выбрать пункт ***«Добавить»***.
- В появившемся ***«Редакторе учетных записей»*** задать имя профиля, на усмотрение администратора.
- Указать тип учетной записи. В зависимости от типа рабочих станций, на которых требуется провести сканирование, выберите платформу для учетной записи **(MS Windows, MS SQL, MySQL, IBM Db2, Oracle Database, Cisco, Huawei, Linux, Solaris, или VMware)**.

Задать учетные данные пользователя:

- *Учетные данные для **Windows*** включают: *имя пользователя*, *пароль, подтверждение пароля, домен* (если необходимо) и *WinRM порт* (если необходимо);

- *Учетные данные для* **Linux-систем** включают: *имя пользователя, пароль, ключ, проверочную фразу* и *ключ, отпечаток ключа сервера* (SSH порт, если необходимо), *настройку привилегий* (нет, не превышать или sudo);
- *Учетные данные для* **CiscoIOS** включают: *имя пользователя, пароль* или *ключ, проверочную фразу* и *ключ, отпечаток ключа сервера* (если необходимо), *SSH порт* (если необходимо), *настройку привилегий* (пароль для Enable), разделитель терминального пейджера.
- *Учетные данные для* **Huawei** включают: *имя пользователя, пароль, ключ, проверочную фразу* и *ключ, отпечаток ключа сервера* (если необходимо), *SSH порт* (если необходимо), *настройку привилегий* (пароль для Enable), *разделитель терминального пейджера*;
- *Учетные данные для* **MSSQL** включают в себя: *хост, экземпляр, порт, логин, пароль*, а также *кнопка* ***«Проверки соединения с БД»***. Доступна возможность Windows-аутентификации;

В случае необходимости сканирования MS SQL с помощью доменной учетной записи Windows, в учетных данных, Логин, необходимо указывать в следующем виде: ***"Имя пользователя@домен"*** *(Рисунок 5.1.2.1):*

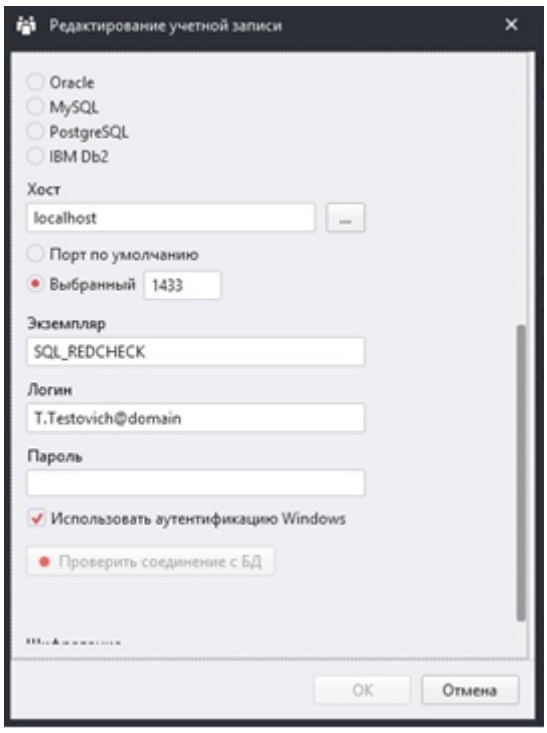


Рисунок 5.1.2.1

- *Учетные данные для* **Oracle Database**, включают в себя: *хост, экземпляр, порт, логин, пароль, привилегии DBA*, а также *кнопка* ***«Проверки соединения с БД»***;
- *Учетные данные для* **MySQL**, включают в себя: *хост, экземпляр, порт, логин, пароль,* а также кнопка ***«Проверки соединения с БД»***;
- *Учетные данные для* **Postgre SQL**, включают в себя: *хост, порт, база данных, логин, пароль, Timeout, Comand Timeout, Protocol (2,3), SslMode,* кнопка ***«Проверки соединения с БД»***;
- *Учетные данные для* **IBM Db2**, включают в себя: *хост, порт, база данных, логин, пароль, кнопка* ***«Проверки соединения с БД»***;
- *Учетные данные для* **SAP HANA**, включают в себя: *хост, порт, база данных, логин, пароль, кнопка* ***«Проверки соединения с БД»***;
- *Учетные данные для* **VMware**, существуют 3-х типов ***ESXi, vCenter, NSX*** и включают в себя: *имя пользователя, пароль, VIM-порт (по умолчанию 443), возможность проверки сертификата* (если необходимо);
- *Учетные данные для* **Solaris** включают: *имя пользователя, пароль, ключ, SSH порт* (если необходимо), *настройку привилегий* (нет, не превышать или sudo, pfexec), *шифрование*;
- Учетные данные для **Check Point**, включают: *имя пользователя, пароль, SSH порт* (если необходимо), *Разделитель терминального пейджера* (разделяет всю полученную информацию на информационные блоки), *шифрование*;
- Учетные данные для **FreeBSD**, включают: *имя пользователя, пароль или ключ, или проверочную фразу и ключ, отпечаток ключа сервера* (если необходимо, SSH порт (если необходимо), *настройку привилегий* (нет, не превышать или sudo), *шифрование*.

После заполнения учётных данных, необходимо нажать кнопку ***«OK»***. Учетная запись будет добавлена в список.

Содержание главы...

Добавление, редактирование или удаление учетных записей выполняется через пункт меню ***Инструменты*** в **Менеджере учетных записей**. Работа с УЗ осуществляется через контекстное меню, вызываемое правой кнопкой мыши.

При выборе пункта «***Добавить***» программа предложит добавить новую учётную запись.

При выборе пункта «***Переименовать***» программа предложит ввести новое имя профиля.

При выборе в контекстном меню пункта «***Редактировать***» откроется окно ***«Редактирование учетной записи»***, в котором изменению могут быть подвергнуты все атрибуты кроме типа учетной записи.

При выборе пункта **«*Удалить*»** информация об учетной записи будет удалена из БД RedCheck и из интерфейса **«Менеджер учетных записей»**.

Содержание главы...

В организациях с большим количеством машин в сети - увеличивается число уникальных учетных записей. Как следствие, чтобы провести сканирование определённой группы хостов - приходится создавать несколько заданий.

Если на компьютере были проведены изменения с УЗ, то задание не может выполниться из-за проблемы с аутентификацией.

RedCheck позволяет избежать подобных ситуаций, благодаря режиму ***«Использовать сохраненные учетные данные при наличии»***.

Данная опция выбирается на этапе ***«Учетные данные задания»***, во время создания новой задачи. Она позволяет использовать вместо сведений ***«по умолчанию»*** заранее указанные учетные записи для каждого из хостов, либо ранее успешно использованные для сканирования данные.

При первом положительном выполнении сканирования, УЗ, которая была указана для авторизации, будет автоматически привязана к хосту. В дальнейшем, при создании задания, можно выбрать опцию ***«Использовать сохраненные учетные данные при наличии»****.*

Задать привязку УЗ к машине можно через меню **Редактирование**: вкладка **Хосты** - вызвать контекстное меню на интересующей машине - **Редактировать** - вкладка **Учетные данные**.

При указании УЗ только на сканирование по безагентскому режиму, программа не сможет использовать данные для агентского режима (и наоборот).

При планировании работы с программой RedCheck, следует разделять УЗ под которыми осуществляется вход на консоль администратора и для сканирования удаленных хост.

Содержание главы...

Для проведения заданий ***«Аудит обновлений»*** и ***«Аудит уязвимостей»***, по конкретному списку обновлений/уязвимостей, необходимо создать ***«Профиль»*** аудитов:

- Пункт меню **Инструменты** - **Менеджер аудитов**.
- Режим - **Профили**.
- В левом блоке указать атрибуты создаваемого профиля, а в правом блоке выбрать проверки, которые необходимо включить в создаваемый профиль и которые будут применены для АРМ в процессе сканирования данным профилем.
- Нажать на кнопку ***«Создать»***.

Содержание главы...

5.2 Хосты

Изначально, в RedCheck присутствует одна группа - ***«По умолчанию»***, в которую автоматически добавляются все новые хосты, добавленные администратором консоли управления.

Создать новую группу хостов можно несколькими способами:

- Пункт меню **Инструменты** - ***Создать группу***....
- Вкладка **Хосты**, в таблице **Группы** вызвать контекстное меню и выбрать пункт ***Создать группу***....
- Используя импорт из CSV-файла.

В появившемся окне необходимо задать имя группы. При необходимости можно сделать описание группы и выбрать хосты для включения в группу. Указание хостов на данном этапе не является обязательным, их можно будет добавить позже. По завершению ввода данных следует нажать кнопку «Создать».

Содержание главы...

В консоли управления RedCheck реализовано несколько способов добавления новых хостов:

- Через пункт меню **Инструменты** → ***Создать хост***... (Или “Alt+T”).
- Вкладка **Хосты**, в таблице **Хосты** вызвать контекстное меню и выбрать пункт ***Создать хост***....
- Добавление хостов из **AD**.
- Добавление хостов из CSV-файла.
- Добавление хостов с помощью **NMap**.

В появившемся окне необходимо задать **IP-адреса** и\или **DNS** имена хостов и, при необходимости, добавить их описание. Примеры задания диапазона хостов можно увидеть в этом же окне.

Информация о добавленных хостах вносится в БД RedCheck. Для просмотра и редактирования хосты доступны из группы, в которую они были добавлены, либо из группы ***«По умолчанию»***.

Содержание главы...

Для проверки работоспособности туннелей RedCheck, а также агента, необходимо перейти на вкладку **«Хосты»**, выделить выбранный хост (для выбора группы хостов можно использовать сочетание ***Ctrl*** и ***Shift***), вызвать контекстное меню нажатием правой кнопкой мыши и выбрать ***«Пинг»***. В открывшемся окне необходимо выбрать соответствующую учетную запись от которой будет осуществляться проверка. После выбора учетной записи, указываются туннели, которые необходимо протестировать **(Agent, Update Agent, WMI, WinRM, Share, Thief, SSH, HTTP)**. Далее необходимо нажать кнопку ***«Пинг»***, после чего закрыть окно.

Процесс проверки работоспособности туннелей можно прервать в любой момент, нажав на кнопку ***«Отмена»***.

Если хост доступен, то в соответствующей ячейке появится красный индикатор. Если в ячейка пустая, то хост недоступен, сканирование не проводилось или завершилось ошибкой.

*Более подробные результаты проверки доступности хоста, используя функцию **Пинг**, находятся в логах программы. В данном журнале событий указана причина недоступности или ошибки, по которой проверка хоста не была осуществлена успешно.*

Содержание главы...

5.3 Задания

Задание на выполнение сканирования (проверок) определяется параметрами:

Имя. Название однозначно идентифицирует задания. По умолчанию состоит из 2 частей – постоянной части **«Job»** и уникального номера.

Пользователь может изменить шаблон для текущего названия задания. Для входа в ***«Генератор имён»*** необходимо в поле ***«Имя»*** нажать на кружок, расположенный справой стороны. Более подробная информация о ***«Генераторе имён»*** находится в описании меню ***«Инструменты»***.

Описание. Вносятся комментарии к заданию.

Тип. Существует **9 типов** заданий: **аудит уязвимостей, аудит обновлений, аудит конфигураций, аудит СУБД, инвентаризация, фиксация, установка обновлений, аудит уязвимостей SCADA-систем и аудит в режиме «Пентест»**. Каждое задание реализует соответствующие проверки RedCheck.

Служба сканирования. Позволяет выбрать службу, с помощью которой будет выполняться сканирование хоста. Данная опция позволяет осуществлять сканирование узлов параллельно. Службы могут быть установлены на разных машинах, что представляет собой вариант горизонтального масштабирования. Данный пункт доступен для настройки сканирований только удалённых хостов.

 *Удаленная служба сканирования доступна не для всех типов лицензии программы RedCheck.*

Запуск. В RedCheck реализовано два сценария запуска заданий.

1. После создания. При выборе запуска «После создания» задание начнет выполняться сразу по завершению создания.
2. По расписанию. При выборе запуска «По расписанию» администратор сможет указать дату, время и периодичность запуска задания.

 *Задание, запуск которого выполняется по расписанию, можно преобразовать в **«мгновенное задание»**. В этом случае, задание единовременно выполнится и в дальнейшем запускаться по расписанию не будет. Для этого необходимо кликом правой кнопки мыши вызвать контекстное меню и выбрать **«Преобразовать в задание без расписания»**.*

Объект. Сканирование (проверка) может осуществляться на локальном и на удаленных компьютерах.

- При выборе режима ***«Локальный»*** задание будет отработано на рабочей станции, с которой в данный момент запущена консоль RedCheck.
- При выборе режима ***«Удаленный»*** администратору будет дана возможность выбора хостов, на которых требуется провести сканирование.

Дополнительно.

- ***«Оповещать по e-mail»*** - при включении этой функции, на указанный e-mail будет отправляться информирующее письмо о завершения задания сканирования (настройки почты проводятся на вкладке «Доставка»);
- ***«Расширенная идентификация хоста»*** - при включении этой функции, в результатах сканирования добавятся такие параметра сканируемого хоста как DNS-имя, FQDN, NetBIOS-имя, IPv4, MAC;

Группы & Хосты. При выборе удаленного режима сканирования после нажатия кнопки ***«Вперед»*** открывается окно **«Группы & Хосты»**, в котором необходимо выбрать Группы хостов и/или отдельные хосты, на которых следует выполнить создаваемое задание. Также имеется возможность повторно запустить сканирование, в случае прерывания. Данное правило распространяется на сканирование двух или более хостов. Чтобы активировать данный пункт, необходимо поставить флаг в поле ***«В случае прерывания запускать сканирование сначала»***.

 *При создании заданий нельзя использовать добавленный по IP локальный хост.*

Учетные данные задания. На следующем шаге на вкладке «Учетные данные задания» необходимо указать учетные данные, от имени которых будет

проводиться сканирование, а также выбрать метод получения данных («безагентский механизм» / «С использованием агента»).

Учетные данные выбираются на основании таблицы, представленной в **Менеджере учетных записей**. Для выбора необходимых учетных данных - необходимо нажать на кнопку ..., после чего произойдет переход в ***«Менеджер учетных записей»***, где возможно добавить учетные данные.

 *На этапе **«Учетные данные задания»** можно использовать функцию **«Использовать сохраненные учетные данные при наличии»**. Это позволит программе использовать УЗ после ранее успешно проведенного сканирования, вместо учетных данных по умолчанию.*

Содержание главы...

Создать новое задание в программе RedCheck можно одним из следующих способов:

1. В меню ***«Действия»*** выбрать необходимый тип задания.
2. Вызов мастера создания задания горячей клавишей: ***«Insert»***.
3. Открыть вкладку ***«Задания»***. Нажать правой кнопкой мыши в пустом месте поля таблицы. В контекстном меню выбрать ***«Создать задание»***.

Далее следуйте инструкциям в мастере создания заданий.

*Для **WEB-консоли** возможен только вариант **№1**.*

*Для контроля **Linux-систем**: (например, SELinux), необходимо обеспечить доступ на чтение и запись в каталог временных файлов для пользователей, от имени которых должно производится сканирование.*

Содержание главы...

Сканер безопасности выполняет централизованное и локальное сканирование хостов в сети на наличие уязвимостей операционных систем, специального и прикладного ПО. Проверки построены на сопоставлении состояния параметров системы - сигнатурам уязвимостей, содержащихся в открытом репозитории OVALdb и описанных в формате SCAP. Сегодня в базе данных RedCheck имеются описания уязвимостей для многих современных платформ и популярных прикладных программ.

Контент уязвимостей ежедневно актуализируется и пополняется новыми продуктами.

На этапе **«профили сканирования»** необходимо выбрать профиль: **«без профиля»** (идёт сканирование по всему диапазону проверок безопасности) или **«выбранные вручную»** (использовать ранее созданные профили в ***«Инструменты» - «Менеджер аудитов»***).

Также необходимо выбрать ***«Тип сканирования»***: **«полное»** (сканирование проходит по всему диапазону проверок безопасности) или **«быстрое»** (сканируются только проверки безопасности, не помеченные флагом «долгие»).

Содержание главы...

*Выполняя задание **Аудит обновлений** с целью дальнейшего использования его в задании **Установка обновлений**, выполняйте задание с помощью УЗ состоящей как в группе **REDCHECK_ADMINS** так и в группе **REDCHECK_Update**. Т.к. задание **Установка** обновлений использует УЗ из выбранного аудита обновлений на основании которого будет проводиться их установка.*

Задачей любого администратора является своевременная установка вышедших обновлений для ликвидации потенциальных угроз.

RedCheck быстро и точно указывает на недостающие в системе обновления, устаревшие версии программ и программы снятые с поддержки разработчиком (**End-Of-Life**). В базе сканера содержатся сведения об обновлениях серверных и клиентских операционных систем **Microsoft**, популярных **Linux** платформ, а также большого количества прикладных программ.

Специально для пользователей, сертифицированных по требованиям безопасности продуктов **Microsoft**, разработан и постоянно обновляется профиль для сканирования сертифицированных обновлений безопасности (для контроля ограничений, накладываемых сертификатом ФСТЭК).

*В связи с особенностями системы обновлений, задание **«Аудит обновлений»** для **Cisco IOS** не используется. Для **Cisco IOS** достаточным является задание **«Аудит уязвимостей»**, позволяющий выявить необходимые для установки обновления.*

На этапе ***«профили сканирования»*** необходимо выбрать: ***«без профиля»*** (сканирование по всему диапазону проверок безопасности), ***«сертифицированные обновления»*** (профиль для сканирования сертифицированных обновлений безопасности продуктов **Microsoft**) или ***«выбранные вручную»*** (использовать ранее созданные профили в ***«Инструменты»*** - ***«Менеджер аудитов»***).

Также необходимо выбрать ***«Тип сканирования»***: ***«полное»*** (сканирование проходит по всему диапазону проверок безопасности) или ***«быстрое»*** (сканируются только проверки безопасности, не помеченные флагом **«долгие»**).

Все результаты сканирования, можно посмотреть в вкладке ***«История»***.

В связи с тем, что многие последущие обновления содержут в себе предыдущие обновления, в RedCheck реализована возможность скрыть замененные обновления (нажать кнопку ***Скрыть заменённые***) в **Результатах сканирования**. Тем самым пользователь видит эффективный список, необходимых для установки обновлений, что в свою очередь позволяет сократить время затраченное на установку.

Содержание главы...

RedCheck позволяет автоматизировать процесс контроля за параметрами безопасности и осуществлять оценку соответствия информационных систем, ее отдельных компонентов или узлов стандартам, политикам безопасности, рекомендациям вендоров и другим "Best Practices". Пользователь может создавать собственные конфигурации и закладывать их в планы проверок.

В программу включен ряд готовых конфигураций (политик), разработанных на основе требований международных стандартов и рекомендаций, в частности: **CIS, MSCM, SCW, PCI DSS, FDCC, USGCB** и др.

По мере развития предприятия, увеличивается и количество машин, обслуживающихся на нем. Внутри одной организации могут использоваться компьютеры для разных целей, с разным ПО (сервер, для рядового сотрудника, и т.п.), с разными УЗ. В связи с этим увеличивается нагрузка на администратора ИБ по количеству создаваемых заданий, для обеспечения должного уровня проверки.

Программа RedCheck упростила данный момент: внутри одного задания аудит конфигураций можно проводить сканирование хостов с разным ПО, с разными УЗ. Также, возможна корректировка задания уже после его создания, запуска.

 *Невозможно выполнить задание **«Аудит конфигураций»** без установки агента RedCheck на удаленных и локальных хостах для **СЗИ НСД Dallas Lock**. Выполнение задания **«Аудит конфигураций»** в режиме метода получения данных **WinRM** возможно для всех конфигураций, кроме конфигураций для **СЗИ НСД Dallas Lock**.*

Для того, чтобы провести ***Аудит конфигурации*** **Secret Net и Dallas Lock** на локальной машине потребуются следующие действия:

- Установите агент RedCheck на локальную машину.
- Добавьте DNS локального компьютера в хосты.

- Сканируйте локальный хост, как удалённый. Для этого на этапе создания задания, в поле ***«Объект»*** необходимо присвоить значение ***«Удаленные хосты»*** - и далее выбрать DNS локального компьютера.

 *Начиная с версии 1.6, RedCheck поддерживает выполнение правил XCCDF-конфигураций, анализирующих значения пользовательских настроек сканируемой системы. RedCheck предоставляет ряд готовых конфигураций, в которых все или некоторые правила анализируют пользовательские настройки. Как правило, такие конфигурации имеют в заголовке слово **"Пользователь" ("User")**.*

В уже созданном задании можно изменить список сканируемых конфигураций. Для этого необходимо, на выбранном задании, вызвать контекстное меню - ***«Свойства»*** - ***Конфигурации***.

Содержание главы...

Сканер безопасности RedCheck позволяет проводить аудит таких систем управления базами данных как: **MS SQL Serevr**; **Oracle; MySQL**; **PostgreSQL; IBM Db2; SAP HANA**.

Для проведения задания **Аудит СУБД**, необходимо выбрать учетные данные для сканировани интересующей СУБД и указать дополнительные учетные данные для операционной системы, на которой установлена СУБД.

Все результаты сканирования, можно посмотреть в вкладке ***«История»***.

Содержание главы...

Сканер RedCheck позволяет получить информацию об операционных системах, пакетах обновлений и исправлениях, установленном ПО, запущенных процессах, общих папках, аппаратном обеспечении и многом другом. Глубокая детализация позволяет отслеживать даже самые незначительные изменения в составе программного и аппаратного обеспечения.

Содержание главы...

RedCheck помогает реализовать меры по контролю целостности программного обеспечения, включая средства защиты информационных систем. Фиксация и контроль целостности исполняемых файлов, библиотек, а также произвольных файлов осуществляется методом контрольного суммирования ГОСТ 2012-256 с использованием сертифицированной библиотеки ***«КриптоПро»***. Кроме того, для фиксации могут быть использованы методы контрольного суммирования MD5, SHA1, SHA256, SHA512, Уровню 3 (ГОСТ 28147-89).

*Метод контрольного суммирования **«Уровень 3»** считается устаревшим, оставлен для совместимости со старыми агентами и в будущих версиях RedCheck будет убран.*

*Для задания **«Фиксация»** на хостах под управлением **ОС Microsoft Windows** доступен только агентский режим работы.*

На вкладке ***«Фиксация файловой системы»*** необходимо указать следующую информацию:

- В списке ***«Каталоги»*** указать каталоги файловой системы, которые должны быть зафиксированы;
- В списке ***«Исключаемые каталоги»*** при необходимости указать каталоги файловой системы, которые должны быть исключены из области фиксации;
- В строке ***«Шаблоны поиска»*** можно указать расширение файлов, подлежащих фиксации;
- Переключатель ***«Включить подкаталоги»*** включает\выключает фиксацию подкаталогов выбранного каталога.

Для добавления контролируемого каталога в список: необходимо ввести путь к этому каталогу и нажать кнопку с изображением ***«+»***. По нажатию кнопки ***«+»*** каталог добавится в список.

На вкладке ***«Фиксация реестра»*** (доступна только для среды **Windows**) необходимо указать следующую информацию:

- В списке ***«Ключи реестра»*** выбрать из раскрывающегося списка ключи реестра, которые должны быть зафиксированы;
- В списке ***«Исключаемые ключи реестра»*** можно указать ключи реестра, которые должны быть исключены из области фиксации;
- Переключатель ***«Включить подключи»*** включает/выключает фиксацию подключений, выбранных ключей реестра.

Для добавления ключа в список необходимо ввести путь к этому ключу и нажать кнопку с изображением **«+»**. По нажатию кнопки **«+»** ключ реестра добавится в список.

 *При формировании путей фиксации не допускается использование специальных символов и регулярных выражений. Имена файлов не могут содержать символы: \/:*?"<>|.*

Не рекомендуется выполнять фиксацию файлов размером более 500Мб, т.к. это влечет за собой максимальную нагрузку (на длительное время) на ЦП, что может привести к сбоям в работе, либо повлечь за собой отказ сканируемого оборудования.

Для проведения успешной фиксации на linux-платформах рекомендуется, чтобы имена сканируемых файлов/каталогов, не содержали пробелов и русских букв, только цифры и латинские символы.

Содержание главы...

Описание данной функции в составе модуля ***«Патч Менеджмент»*** представлено в отдельном документе **PatchManagement.pdf**. Доступ из программы: **Справка - Руководство**.

Задание «Установка обновлений» недоступно для web-консоли.

Содержание главы...

Данный функционал доступен при включенном модуле ***SCADA**, в лицензии RedCheck.*

На этапе ***«Модули сканирования»*** необходимо выбрать один или несколько модулей из следующих:

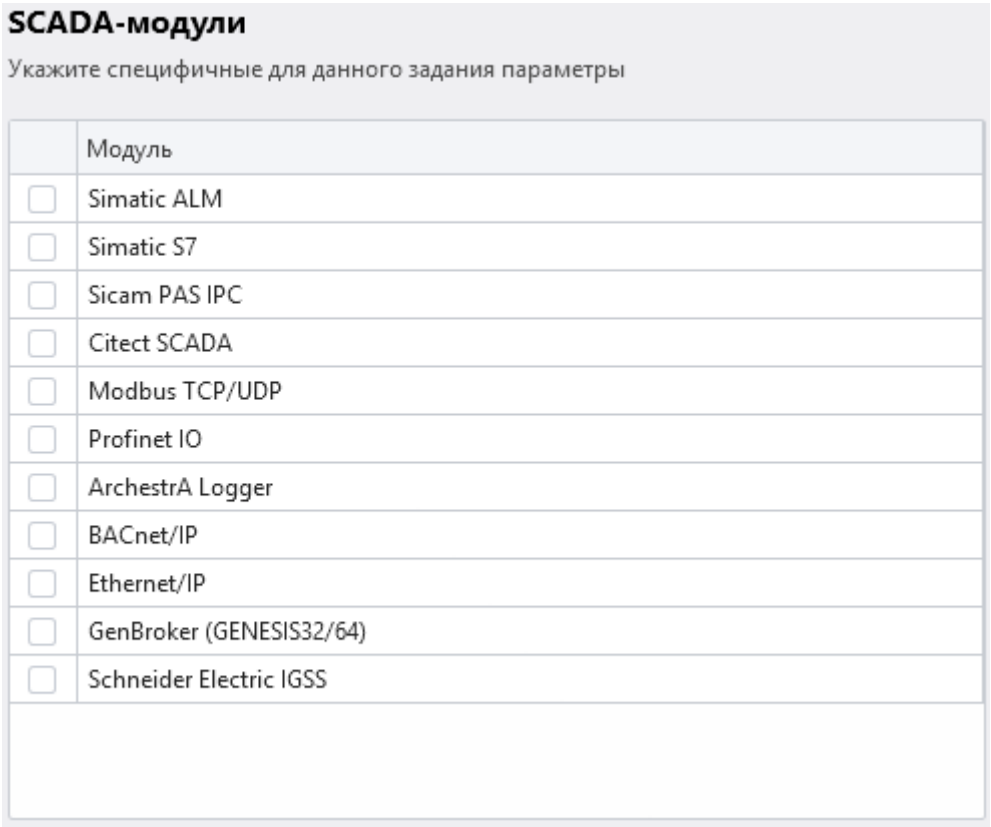


Рисунок 5.3.2.8.1

Все результаты сканирования, можно посмотреть в вкладке ***«История»***.

*В случае работы с **BacNET**, устройство отвечает броадкастом (пакеты отправляются ко всем хостам сети), поэтому необходимо что-бы модуль смог получить данный ответ. По умолчанию фаервол Windows блокирует получение*

ответа, поэтому модуль или программу нужно добавлять в исключения для получения UDP-траффика.

Содержание главы...

 Функция доступна при установленной на компьютере и настроенной для работы утилите **Nmap**.

На первом этапе создания задания, необходимо выбрать один из 3-х типов сканирования (Рисунок 5.3.2.9.1):

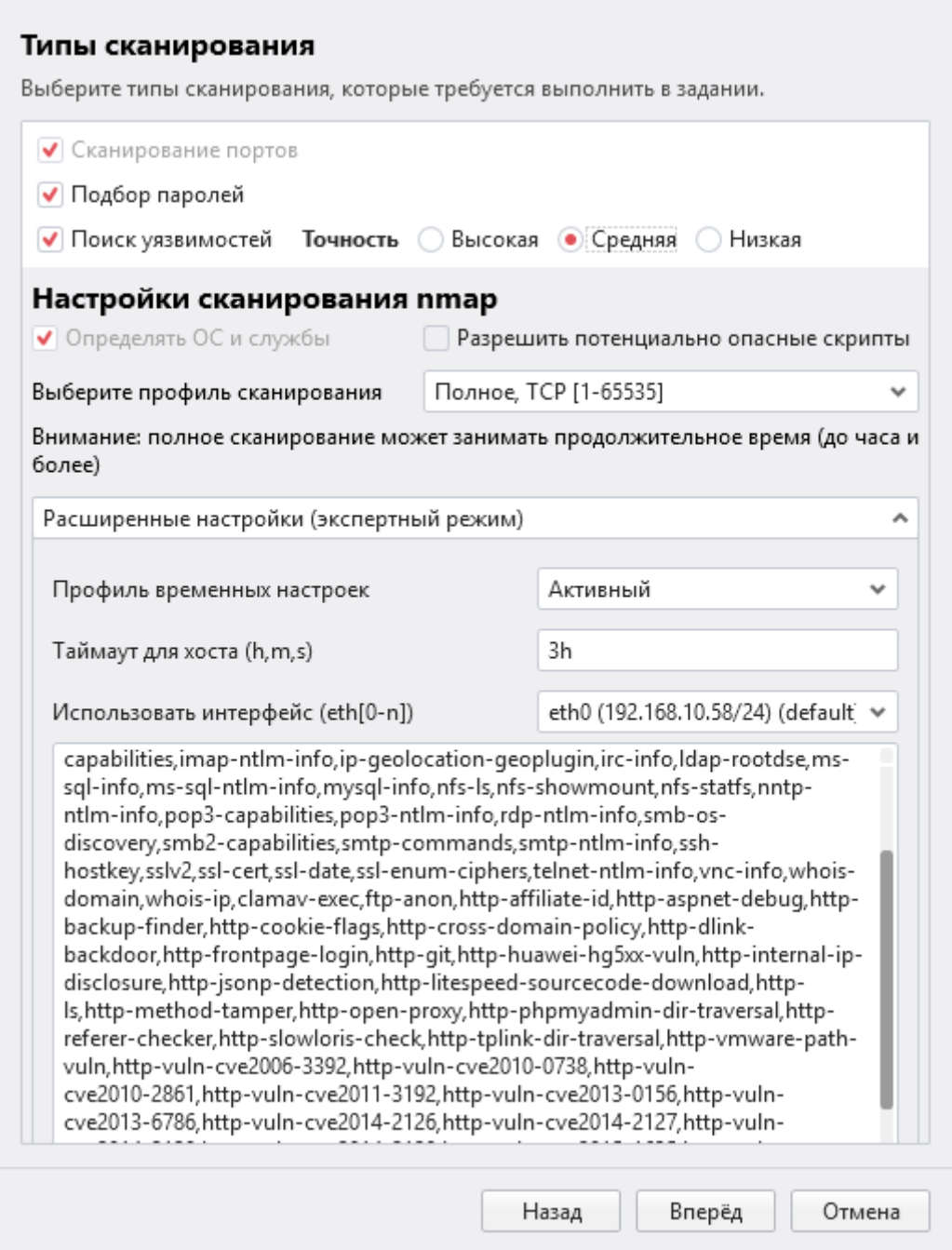


Рисунок 5.3.2.9.1

*Для задания **Аудит** в режиме **«Пентест»**, доступен только безагентский режим работы.*

*Тип сканирования **«Поиск уязвимостей»**, позволяет выбрать точность совпадения номера версии уязвимости (совпадение номера версии найденной уязвимости, с номером версии в базе данных RedCheck).*

Далее необходимо выбрать ***«Профиль временных настроек»*** (Рисунок 5.3.2.9.2):

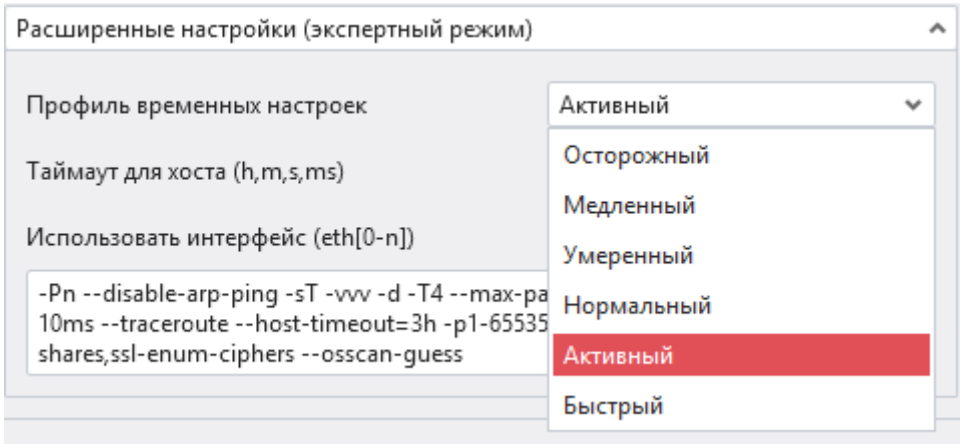


Рисунок 5.3.2.9.2

Отличия между профилями временных настроек: https://nmap.org/book/performance-timing-templates.html

*В мастере создания задания **«Аудит в режиме «Пентест»,** присутствует возможность «ручного» ввода необходимых пользователю параметров.*

В полях ***«Имя экземпляра»*** и ***«Порт»*** необходимо задать имя экземпляра и порт, по которому он доступен. Так же можно установить переключатель ***«Сканировать все экземпляры»*** - RedCheck произведет поиск экземпляров БД и, в случае успеха поиска, просканирует их согласно выбранным параметрам.

Подбор пары логин-пароль осуществляется на основании данных содержащихся в соответствующих словарях.

Содержание главы...

5.4 История

Для просмотра результата сканирования необходимо открыть вкладку ***«История»***. Можно воспользоваться фильтром, расположенном на левой панели, и нажать ***«Применить фильтр»***.

Если сканирование хоть раз выполнялось консолью RedCheck и его результаты не были удалены администратором, то они будут отображены в таблице.

Для просмотра результата сканирования совершите двойной клик левой кнопкой мыши по строке с найденным заданием, или кликом правой кнопки мыши по строке вызвите контекстное меню и выберите пункт ***«Результаты сканирования»***.

В левой части открывшегося окна ***«Результаты сканирования»*** находится краткая информация о задании включающая в себя: наименование сканируемого хоста, ID задания, профиль сканирования, дату и время начала и завершения сканирования.

В правом нижнем углу находятся кнопки:

- ***«Открыть папку с файлами»*** - открывает папку, в которую сохраняются: файл результатов, HTML-файл, файл системных характеристик, файл результатов (инвентаризации).
- ***«Создать быстрый отчет»*** - создает отчет по заданию. Получившийся отчет можно просмотреть на вкладке ***«Отчеты»***. Его имя начинается с префикса «***Quick***», а описание содержит строку «Автогенерируемый отчет вкладки «История».
- Кнопка ***«Закрыть»***, которая закрывает окно ***«Результаты сканирования»***.

Быстрый отчёт создаётся в соответствии с применёнными фильтрами в результатах сканирования.

Содержание главы...

В центральной части окна вкладки ***«Результат»*** представлены параметры и группы параметров, прошедшие контроль на соответствия эталонной конфигурации, выбранной пользователем RedCheck.

Для удобства просмотра результатов сканирования, можно в один клик свернуть и развернуть дерево правил (кнопка ***«Развернуть»***), посмотреть результаты для разных профилей, найти интересующий элемент с помощью поля «поиск правил», воспользоваться фильтром: вывести правила отфильтровав по ***«Результатам»***, либо по ***«Критичности»***.

Кликом правой клавиши мыши по конкретному параметру конфигурации можно вызвать контекстное меню, в котором будет доступно: ***«Детализация», «Показать собранные элементы» или «Копировать»***.

Функция ***«Детализация»*** показывает место обнаружения проблемы в системе.

Функция ***«Показать собранные элементы»*** позволяет по конкретному параметру из результата аудита определить ветку реестра, где расположены сведения о проблемных местах, путь к папке и другую информацию.

При аудите пользовательских настроек, правила, которые анализируют настройки пользователей системы, помимо общего результата выполнения имеют отдельный результат для каждого пользователя. Результаты для пользователей отображаются в виде дополнительного уровня вложенности под общим результатом.

Общий результат выполнения правила учитывает состояние той или иной настройки у всех пользователей системы, а каждый из вложенных результатов - состояние настройки только того пользователя, чье имя указано напротив данного результата. При этом, если правило анализирует и пользовательские, и системные настройки, то каждый из пользовательских результатов данного правила учитывает эти же самые системные настройки.

В правой части окна ***«Результаты сканирования»*** находится краткая информация об эталонной конфигурации, сравнение с которой проводилось в рамках выполнения данного задания, либо о параметре безопасности, прошедшем проверку на соответствие. Здесь же указаны результат сравнения (***«Легенда»***), уровень опасности (***«Критичность»***), ссылки на описание данного параметра (элемент ***«Ссылки»***), путь для настройки данного параметра из интерфейса **ОС Windows** (элемент ***«GPO»***), фактическое значение параметра (***«Фактическое значение»***), описание данного параметра (***«Описание»***) и другая информация (***«Дополнительно»***).

Во вкладке ***«OVAL-Конфигурация»*** содержится список выполнившихся определений, а также следующая информация: **ALTX ID, риск, результат, ссылки, название.**

Во вкладке ***«OVAL-Инвентаризация»***, пользователь может увидеть список инвентарей, сработавших на этом компьютере, а также следующую информацию: **ALTX ID, риск, ссылки, название.**

Содержание главы...

Во вкладке ***«Инвентаризация»*** представлен список программных и аппаратных средств, данные о которых были получены в результате проведения сканирования. Нажатие символа «▷», перед названием группы компонентов системы, позволит «развернуть» эту группу для получения более детальной информации.

Во вкладке ***«OVAL-Инвентаризация»*** представлен список инвентарей, сработавших на сканируемом компьютере, а также следующая информация: **ALTX ID, риск, ссылку, название, описание, версия.**

Представленные инвентари идентифицируют программное обеспечение, которое установлено на сканируемой машине.

Содержание главы...

В центральной части окна во вкладке ***«Результаты»*** представлен список обновлений безопасности, которые не установлены на проверяемой системе. Список содержит уникальный идентификационный номер обновления, риск, ссылку и краткое описание обновления.

Если выбрать строку с неустановленным обновлением, а в нижней части экрана нажать кнопку ***«Подробности»***, появится дополнительная панель с подробной информацией:

- Идентификатор обновления;
- Риск - степень ее опасности;
- Ссылка на базу данных в ovaldbru.altx-soft.ru;
- Название обновления;
- Описание обновления;
- Детализация - показывает место обнаружения продукта в системе;
- Ссылка на описание данного обновления, где можно получить дополнительную информацию, в том числе, и описание методов по ее устранению, ссылка на производителя;
- Продукты, требующие обновления.

Кликом правой клавиши мыши по конкретному обновлению можно вызвать контекстное меню, в котором будет доступно: ***«Показать собранные элементы» и «Экспорт CSV»***.

Функция ***«Показать собранные элементы»*** позволяет по конкретному обновлению из результата аудита определить расположение продуктов, требующих обновления, а также ветку реестра, где расположены сведения о программе, ее версию и другие сведения.

Во вкладке ***«OVAL-Инвентаризация»***, показан список инвентарей, сработавших на сканируемом компьютере, а также следующая информация: **ALTX ID, риск, ссылку, название, описание, версию.**

Содержание главы...

В центральной части окна во вкладке ***«Результаты»*** представлены найденные уязвимости. Список содержит уникальный идентификационный номер уязвимости (***ALTX ID*** **репозитория уязвимостей** OVALdb), риск, ссылку и краткое описание уязвимости.

Если выбрать строку с интересующей уязвимостью и в нижней части экрана нажать кнопку ***«Подробности»***, «развернется» дополнительная панель с подробной информацией:

- Идентификатор уязвимости;
- Риск - степень ее опасности;
- Ссылка на базу данных в ovaldbru.altx-soft.ru;
- Название уязвимости;
- Описание уязвимости;
- Исправление - указаны необходимые шаги действий по устранению возможных угроз;
- Детализация - показывает место обнаружения уязвимого продукта в системе;
- Ссылка на описание данной уязвимости по классификации организации MITRE, где можно получить дополнительную информацию об уязвимости в том числе и описание методов по ее устранению;
- Продукты, которые подвержены уязвимости.

Кликом правой клавиши мыши по конкретной уязвимости можно вызвать контекстное меню, в котором будет доступно: ***«Показать собранные элементы»*** и ***«Экспорт CSV»***.

Функция ***«Показать собранные элементы»*** позволяет по конкретной уязвимости из результата аудита определить расположение продуктов имеющих данную уязвимость, а также ветку реестра, где расположены сведения о программе, ее версию и другие сведения.

Во вкладке ***«OVAL-Инвентаризация»***, находится список инвентарей, сработавших на сканируемом компьютере, а также следующая информация: **ALTX ID, риск, ссылку, название, описание, версия.**

Содержание главы...

В центральной части окна представлены разделы ***«Файловая система» и «Реестр»***, однако отображаются лишь те, которые были указаны пользователем RedCheck при создании задания ***«Фиксация»***.

В разделе ***«Файловая система»*** представлены файлы, отсканированные в задании, а также их контрольная сумма.

В разделе ***«Реестр»*** указаны ветки и ключи реестра, а также их текущие значения.

Содержание главы...

В центральной части окна представлены параметры и группы параметров, прошедшие процедуру оценки соответствия эталонной конфигурации, выбранной пользователем RedCheck.

Переключатель ***«Развернутое дерево»*** позволяет **«свернуть»** представление параметров до отображения только групп параметров, либо **«развернуть»** группы параметров до представления всех параметров конфигурации. Найти интересующий элемент можно с помощью поля «поиск правил» (кнопка ***«Развернуть»***), воспользоваться фильтром: вывести правила отфильтровав по «***Результатам»***, либо по ***«Критичности»***.

Кликом правой клавиши мыши по конкретному параметру конфигурации можно вызвать контекстное меню, в котором будет доступно: ***«Детализация», «Показать собранные элементы» или «Копировать»***.

Функция ***«Детализация»*** показывает место обнаружения продукта в системе.

Функция ***«Показать собранные элементы»*** позволяет определить ветку реестра, где расположены сведения о проблемных местах, путь к папке и другие сведения.

В правой части окна ***«Результаты сканирования»*** находится краткая информация об эталонной конфигурации, сравнение с которой проводилось в рамках выполнения данного задания, либо о параметре безопасности, прошедшем проверку на соответствие. Здесь же указаны ссылки на описание данного параметра (элемент ***«Ссылки»***), путь для настройки данного параметра из интерфейса **ОС Windows** (элемент **«GPO»**) и описание данного параметра.

Во вкладке ***«OVAL-Конфигурация»*** содержится список выполнившихся определений.

Во вкладке ***«OVAL-Инвентаризация»***, содержится список инвентарей, сработавших на сканируемом компьютере, а также следующая информация: **ALTX ID, риск, ссылка, название, описание, версия.**

Содержание главы...

В центральной части окна представлена таблица с указанием найденных уязвимостей СУБД, результатом инвентаризации портов, подобранных программой пар логин/пароль и информацией о сканируемом хосте (Рисунок 5.4.7.1):

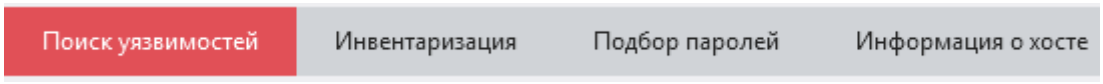


Рисунок 5.4.7.1

Содержание главы...

5.5 Отчеты

На вкладке ***«Отчеты»*** можно создавать отчеты по всем проведенным заданиям сканирования.

В RedCheck предусмотрено 2 типа отчетов:

- **Простой** отчет содержит информацию о результатах сканирования (контроля) выбранного задания.
- **Дифференциальный** отчет показывает **«логическую разницу»** между двумя результатами выполнения одного и того же задания в различные моменты времени.

Также в нижней части вкладки ***Отчеты*** доступна группировка по типу построения отчета (простой и дифференциальный) и по типу данных (типу задания).

Содержание главы...

Для создания отчета необходимо перейти на вкладку ***«Отчеты»***, открыть контекстное меню и выбрать пункт ***«Создать отчет»***.

В Web-версии RC, для создания отчета необходимо вызвать пункт меню: **«Действия» - «Создать отчет»**.

Выберите необходимый тип отчета в поле ***«Тип»***.

В выпадающем списке ***«Отчет»*** выберите тип задания.

В поле ***«Выбор данных»*** пользователь может определить тип выбора данных: по заданию, по хостам или по единичному хосту.

Если установить переключатель ***«По заданию»***, мастер создания отчета предложит выбрать задание, результаты которого будут использованы при формировании отчета, а потом уже - один из результатов выполнения этого задания. Данная опция может быть необходима при большом количестве заданий и результатов сканирований.

Если установить переключатель ***«По хостам (актуальные сканирования)»***, на последующих страницах мастера создания отчета пользователю RedCheck будет предложено выбрать хосты, актуальные результаты сканирования (последнее успешное) которых следует учитывать при формировании отчета.

Если выбрать ***«По единичному хосту (с выбором сканирования)»***, мастер создания отчета автоматически предложит выбрать хост, и выбрать необходимое сканирование.

Дополнительно, можно настроить получение копии отчёта по почте, предварительно поставив флаг в поле: ***«После создания отправить PDF-отчёт по email»***, или отправить отчет в указанный сетевой каталог (доступно только для WEB-версии программы), предварительно выбрав значение: ***«После создания отправить отчёт в сетевой каталог».***

После создания отправить PDF-отчёт по email»

 *Настройка уведомнений по почте производится в:*
***Инструменты→ Настройка→ Доставка**.*

В зависимости от выбранного типа отчета и включенных опций, мастер создания отчета может предложить пользователю указать некоторые дополнительные данные.

Содержание главы...

Указанный функционал доступен для RedCheck версии 2.6.6 и выше.

На данном этапе необходимо выбрать результаты, которые будут включены в отчёт (Рисунок 5.5.2):

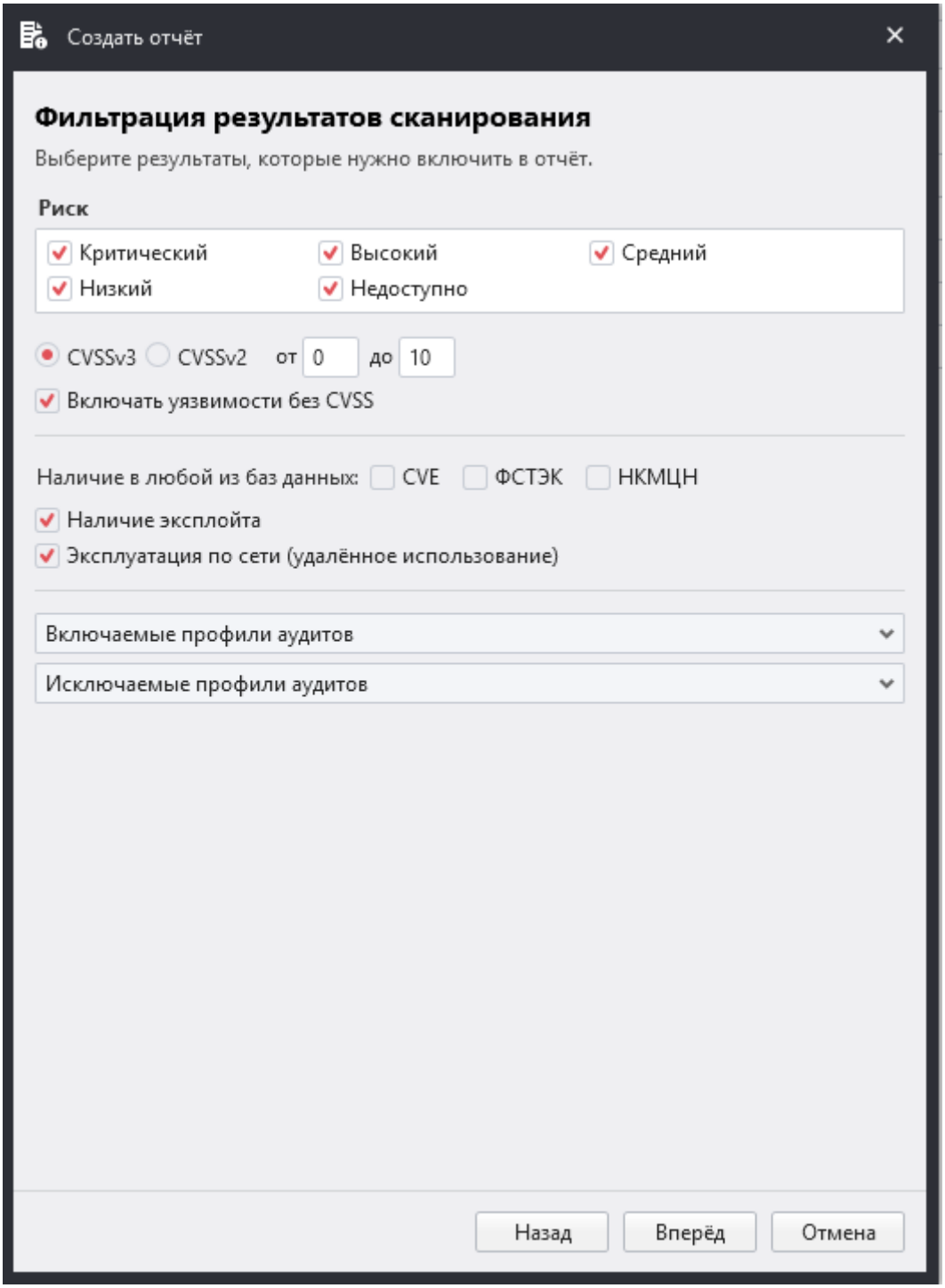


Рисунок 5.5.2

- Степень риска по CVSS;
- Версию CVSS (при выборе параметра, в отчет выводится уязвимости с CVSSv3 и CVSSv2);
- Включать или нет в отчет уязвимости без CVSS;
- База данных уязвимостей;

- Наличие эксплойта (***при выборе параметра, в отчет не попадут уязвимости без описанного эксплойта***);
- Эксплуатация уязвимости по сети (удаленное использование) (***при выборе параметра, в отчет не попадут уязвимости без CVSS***);
- Включить или исключить профили аудитов, по которым было проведено задание.

На данном этапе необходимо выбрать компоненты для построения отчёта.

Доступен выбор содержимого компонентов отчёта, можно применить фильтр по результатам и критичности сканирования правил.

Содержание главы...

5.7 Работа с web-сервисом OVALdb

Для получения расширенной информации о найденных с помощью RedCheck проблемах безопасности необходимо выполнить следующие действия:

1. Перейти на вкладку ***«История»*** в консоли RedCheck
2. Открыть свойства необходимого сканирования, например, **«Аудит уязвимостей»**
3. Найти в открывшемся списке интересующую уязвимость (обновление) и нажать на иконку ***«Подробности»*** в нижней части окна
4. В строке под названием OVAL нажать левой кнопкой мыши на представленной гиперссылке

Откроется окно браузера, используемого по умолчанию в системе, и произойдет переход на страницу сайта https://ovaldb.altx-soft.ru/ содержащую сведения о выбранной уязвимости.

В верхней части странице находится справочная инфформация **«описания»** (Рисунок 5.7.1.1), содержащая спрвочные сведения об уязвимости: описание, семейство ОС и платформа, к которым применима уязвимость, продукт, ссылки на зарегистрированный идентификатор (информация с сайта mitre.org, а так же другая информация от вендора.

Рисунок 5.7.1.1

В нижней части страницы находится **«функциональная»** часть - раздел ***Критерии*** (Рисунок 5.7.1.2), содержащая сведения о логике и критериях обнаружения уязвимости.

Рисунок 5.7.1.2

Наличие в открытом виде определений, хранящихся в **OVALdb** позволяет, пользователям самостоятельно проверять корректность полученных с помощью RedCheck заключений о выявленных проблемах безопасности.

Содержание главы...

В RedCheeck используется собственный контент безопасности, хранящийся в репозитории компании **АЛТЭКС-СОФТ - OVALdb**. Помимо определений, используемых сканером, ресурс содержит и другуую информацию, которя может использоваться как дополнительный источник знаний при оценке защищенности информационных систем.

Что бы попасть на web-страницу **OVALdb** необходимо перейти по ссылке https://ovaldb.altx-soft.ru/ .

Поиск доступен по таким классам проверок (Рисунок 5.7.2.1) как:

- ***«конфигурация» (Compliance)*** - проверки на соответствие параметров безопасности системы определенным эталонным значениям;
- ***«инвентарь» (Inventory)*** - проверки установленного ПО, в том числе операционных систем и их компонентов;
- ***«обновления» (Patch)*** - проверки установленных в системе обновлений для операционных систем, ее компонентов, а также для наиболее распространенного ПО (Java, Google Chrome, Flash Player и многого другого);
- ***«уязвимости» (Vulnerability)*** - проверки на присутствие в системе разнообразных уязвимостей;
- ***«разное» (Miscellaneous)*** - сюда входят проверки, которые не относятся к остальным классам.

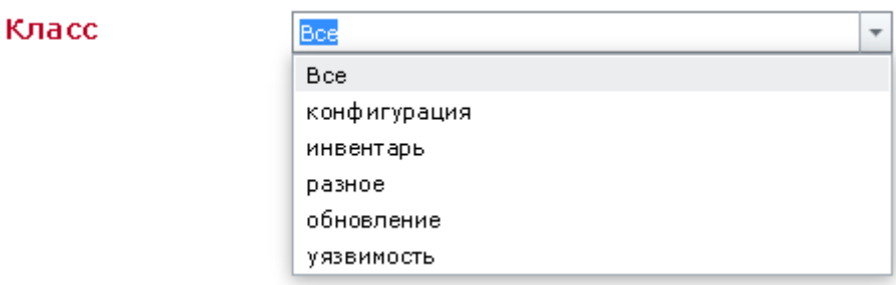


Рисунок 5.7.2.1

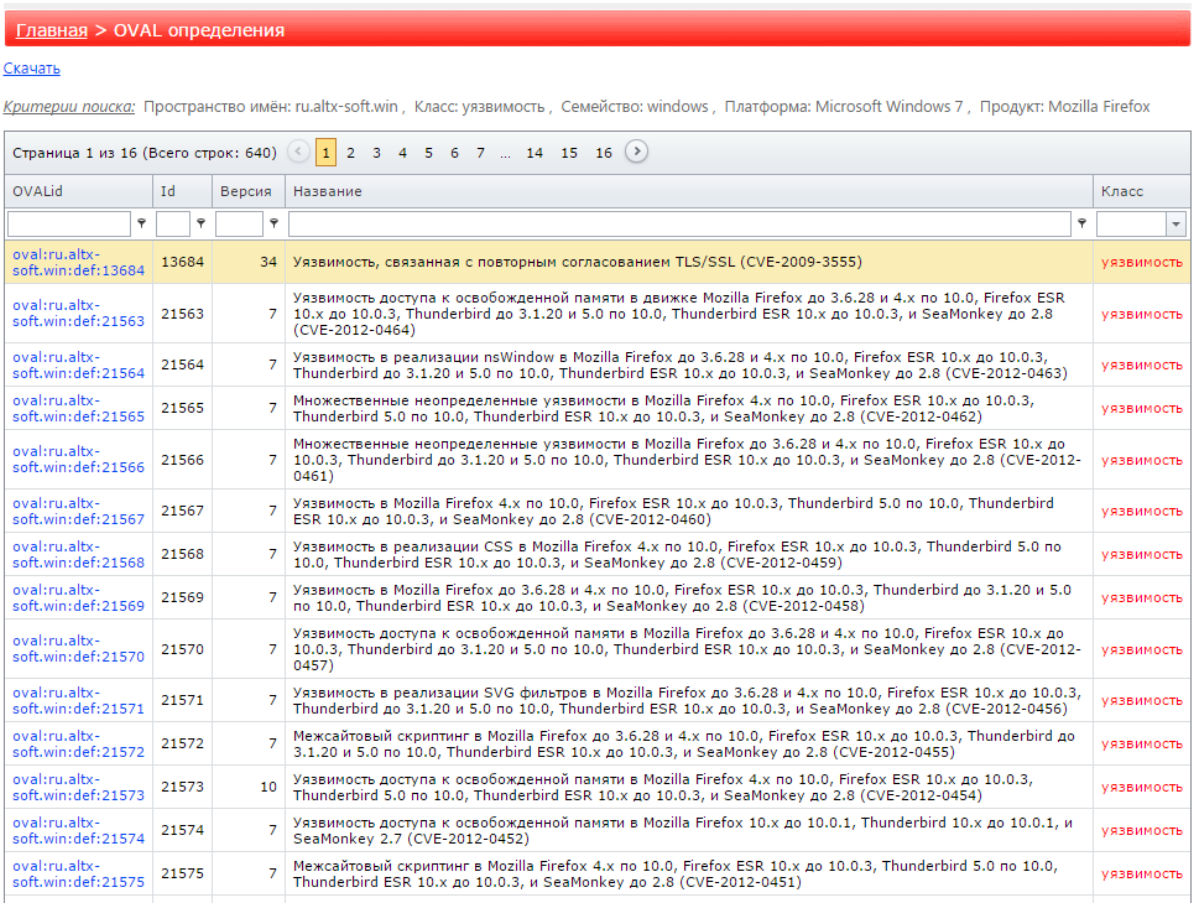
Помимо этого, страница поиска содержит следующие поля:

- **Поле** ***«ALTXid»*** - здесь вводится уникальный идентификатор, под которым определение хранится в базе;
- **Поле** ***«Язык»*** - предоставляется выбор языка, на котором написаны описания и названия определений;
- **Поле** ***«Важность»*** - показывает степень угрозы данного определения на основе метрики **CVSS** (высокая, средняя, низкая, информация, нет доступа);
- ***«Id»*** - данное поле позволяет выполнять поиск по заранее известному **ID OVAL-определения**. **OVAL**-определение (*от англ. «definition» - «описание, определение», далее «определение»*) - это основная структурная единица **OVALdb**, включающая в себя, как правило, набор критериев для проверки одной сущности - будь то уязвимость, обновление или параметр конфигурации (***Compliance***). Определение представляет собой XML-документ, в котором на языке **OVAL** описаны методы проверки элемента выбранного класса, а также указана определенная метаинформация. Например, в качестве метаинформации может выступать ссылка на CVE-идентификатор уязвимости, ссылка на скачивание требуемого к установке обновления. Зачастую это облегчает процесс обнаружения и устранения проблемы безопасности;
- Непосредственно ID имеет вид ***oval:ru.altx-soft.win:def:3803***, где ***oval:ru.altx-soft.win*** - пространство имен (*«namespace»)*, указывающее на происхождение определения, ***def*** указывает на тип объекта (в данном случае - определение *(«definition»)*, а *3803* - порядковый номер записи в базе. OVALdb включает определения, принадлежащие репозиториям Center for Internet Security *(org.cisecurity)*, Mitre (**org.mitre.oval** и **ALTEX-SOFT)**. Первые два репозитории являются открытыми, **OVALdb** является коммерческим ресурсом, часть информации скрыта и доступная только авторизованным пользователям;
- **Поле** ***«Версия»*** - указывает сколько раз определение было модифицировано. После создания определения, оно может корректироваться - совершенствоваться проверки, уточняться описание и другое;

- **Поле** ***«Название»*** определяет заголовок определения. Например, можно указать название какого-либо распространенного продукта, например, набрав **Chrome или FireFox** поиск **OVALdb** вернет список определений, относящихся к этим продуктам. Возможен поиск определений, например, описывающих обновления Microsoft; для этого в поле «Название» необходимо указать номер статьи базы знаний – например, *«KB2753842»* - в результатах поиска отобразится список обновлений, применимых к различным операционным системам;
- ***«Описание»*** - поле содержит подробную информацию об определении;
- ***«Ссылка»*** - метаданные, относящиеся к определению. Здесь можно указать идентификатор уязвимости (например, *«CVE-2013-5045»*), или имя файла обновления, или номер бюллетеня безопасности вендора;
- ***«Ссылка URL»*** - содержит ссылку типа URL, например, на идентификатор уязвимости, где можно ознакомиться с более подробной информацией, или ссылка на скачивание обновления, и другое;
- ***«Ссылка Источник»*** - содержит сведения о типе источника, например, *CVE, CCE*;
- ***«Пространство имен»*** - это пространство имен, к которому относится определение. Можно выбрать сразу интересующее вас пространство имен и поиск будет проводиться только по нему, либо оставить ***«Все»*** и искать во всех пространствах имен. Более подробно рассмотрено выше;
- ***«Класс»*** - здесь указывается класс необходимых проверок;
- ***«Семейство»*** - «семейство» операционных систем, для которых предназначена проверка. На данный момент поддерживаются **iOS, Mac OS, PixOS, VRP, Unix и Windows**;
- **«Платформа»** - необходимая платформа. Под платформой подразумевается операционная система;
- ***«Продукт»*** - поле содержит полный перечень продуктов, для которых имеются определения в базе OVALdb;
- ***«Устаревший»*** - выводит либо устаревшие, либо актуальные проверки безопасности;
- Ниже расположены **5 полей** для поиска тестов, объектов, значений и переменных – с возможностью поиска по ID, комментарию, типу, значению и по критерию устаревания. Данный поля предназначены для специалистов, непосредственно работающих с контентом;

Пример: Необходимо найти все определения, содержащие проверки на уязвимости браузера **Mozilla Firefox**. Для этого нужно:

- Выбрать ***Класс*** - уязвимости, ***Продукт*** - Mozilla FireFox.
- Нажать кнопку ***«Искать»***. Отобразится список всех имеющихся в **OVALdb** проверок для **Mozilla Firefox** с заданными критериями (Рисунок 5.7.2.2)



Главная > OVAL определения

Скачать

Критерии поиска: Пространство имён: ru.altx-soft.win , Класс: уязвимость , Семейство: windows , Платформа: Microsoft Windows 7 , Продукт: Mozilla Firefox

Страница 1 из 16 (Всего строк: 640) 1 2 3 4 5 6 7 ... 14 15 16

OVALid	Id	Версия	Название	Класс
oval:ru.altx-soft.win:def:13684	13684	34	Уязвимость, связанная с повторным согласованием TLS/SSL (CVE-2009-3555)	уязвимость
oval:ru.altx-soft.win:def:21563	21563	7	Уязвимость доступа к освобожденной памяти в движке Mozilla Firefox до 3.6.28 и 4.x по 10.0, Firefox ESR 10.x до 10.0.3, Thunderbird до 3.1.20 и 5.0 по 10.0, Thunderbird ESR 10.x до 10.0.3, и SeaMonkey до 2.8 (CVE-2012-0464)	уязвимость
oval:ru.altx-soft.win:def:21564	21564	7	Уязвимость в реализации nsWindow в Mozilla Firefox до 3.6.28 и 4.x по 10.0, Firefox ESR 10.x до 10.0.3, Thunderbird до 3.1.20 и 5.0 по 10.0, Thunderbird ESR 10.x до 10.0.3, и SeaMonkey до 2.8 (CVE-2012-0463)	уязвимость
oval:ru.altx-soft.win:def:21565	21565	7	Множественные неопределенные уязвимости в Mozilla Firefox 4.x по 10.0, Firefox ESR 10.x до 10.0.3, Thunderbird 5.0 по 10.0, Thunderbird ESR 10.x до 10.0.3, и SeaMonkey до 2.8 (CVE-2012-0462)	уязвимость
oval:ru.altx-soft.win:def:21566	21566	7	Множественные неопределенные уязвимости в Mozilla Firefox до 3.6.28 и 4.x по 10.0, Firefox ESR 10.x до 10.0.3, Thunderbird до 3.1.20 и 5.0 по 10.0, Thunderbird ESR 10.x до 10.0.3, и SeaMonkey до 2.8 (CVE-2012-0461)	уязвимость
oval:ru.altx-soft.win:def:21567	21567	7	Уязвимость в Mozilla Firefox 4.x по 10.0, Firefox ESR 10.x до 10.0.3, Thunderbird 5.0 по 10.0, Thunderbird ESR 10.x до 10.0.3, и SeaMonkey до 2.8 (CVE-2012-0460)	уязвимость
oval:ru.altx-soft.win:def:21568	21568	7	Уязвимость в реализации CSS в Mozilla Firefox 4.x по 10.0, Firefox ESR 10.x до 10.0.3, Thunderbird 5.0 по 10.0, Thunderbird ESR 10.x до 10.0.3, и SeaMonkey до 2.8 (CVE-2012-0459)	уязвимость
oval:ru.altx-soft.win:def:21569	21569	7	Уязвимость в Mozilla Firefox до 3.6.28 и 4.x по 10.0, Firefox ESR 10.x до 10.0.3, Thunderbird до 3.1.20 и 5.0 по 10.0, Thunderbird ESR 10.x до 10.0.3, и SeaMonkey до 2.8 (CVE-2012-0458)	уязвимость
oval:ru.altx-soft.win:def:21570	21570	7	Уязвимость доступа к освобожденной памяти в Mozilla Firefox до 3.6.28 и 4.x по 10.0, Firefox ESR 10.x до 10.0.3, Thunderbird до 3.1.20 и 5.0 по 10.0, Thunderbird ESR 10.x до 10.0.3, и SeaMonkey до 2.8 (CVE-2012-0457)	уязвимость
oval:ru.altx-soft.win:def:21571	21571	7	Уязвимость в реализации SVG фильтров в Mozilla Firefox до 3.6.28 и 4.x по 10.0, Firefox ESR 10.x до 10.0.3, Thunderbird до 3.1.20 и 5.0 по 10.0, Thunderbird ESR 10.x до 10.0.3, и SeaMonkey до 2.8 (CVE-2012-0456)	уязвимость
oval:ru.altx-soft.win:def:21572	21572	7	Межсайтовый скриптинг в Mozilla Firefox до 3.6.28 и 4.x по 10.0, Firefox ESR 10.x до 10.0.3, Thunderbird до 3.1.20 и 5.0 по 10.0, Thunderbird ESR 10.x до 10.0.3, и SeaMonkey до 2.8 (CVE-2012-0455)	уязвимость
oval:ru.altx-soft.win:def:21573	21573	10	Уязвимость доступа к освобожденной памяти в Mozilla Firefox 4.x по 10.0, Firefox ESR 10.x до 10.0.3, Thunderbird 5.0 по 10.0, Thunderbird ESR 10.x до 10.0.3, и SeaMonkey до 2.8 (CVE-2012-0454)	уязвимость
oval:ru.altx-soft.win:def:21574	21574	7	Уязвимость доступа к освобожденной памяти в Mozilla Firefox 10.x до 10.0.1, Thunderbird 10.x до 10.0.1, и SeaMonkey 2.7 (CVE-2012-0452)	уязвимость
oval:ru.altx-soft.win:def:21575	21575	7	Межсайтовый скриптинг в Mozilla Firefox 4.x по 10.0, Firefox ESR 10.x до 10.0.3, Thunderbird 5.0 по 10.0, Thunderbird ESR 10.x до 10.0.3, и SeaMonkey до 2.8 (CVE-2012-0451)	уязвимость

Рисунок 5.7.2.2

В левом верхнем углу находится кнопка ***«Скачать»***, которая позволяет загрузить весь найденный контент. Перейдя по одной из ссылок открывается карточка, содержащая детальную информация об уязвимости. Например, http://ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:21569 (Рисунок 5.7.2.3).

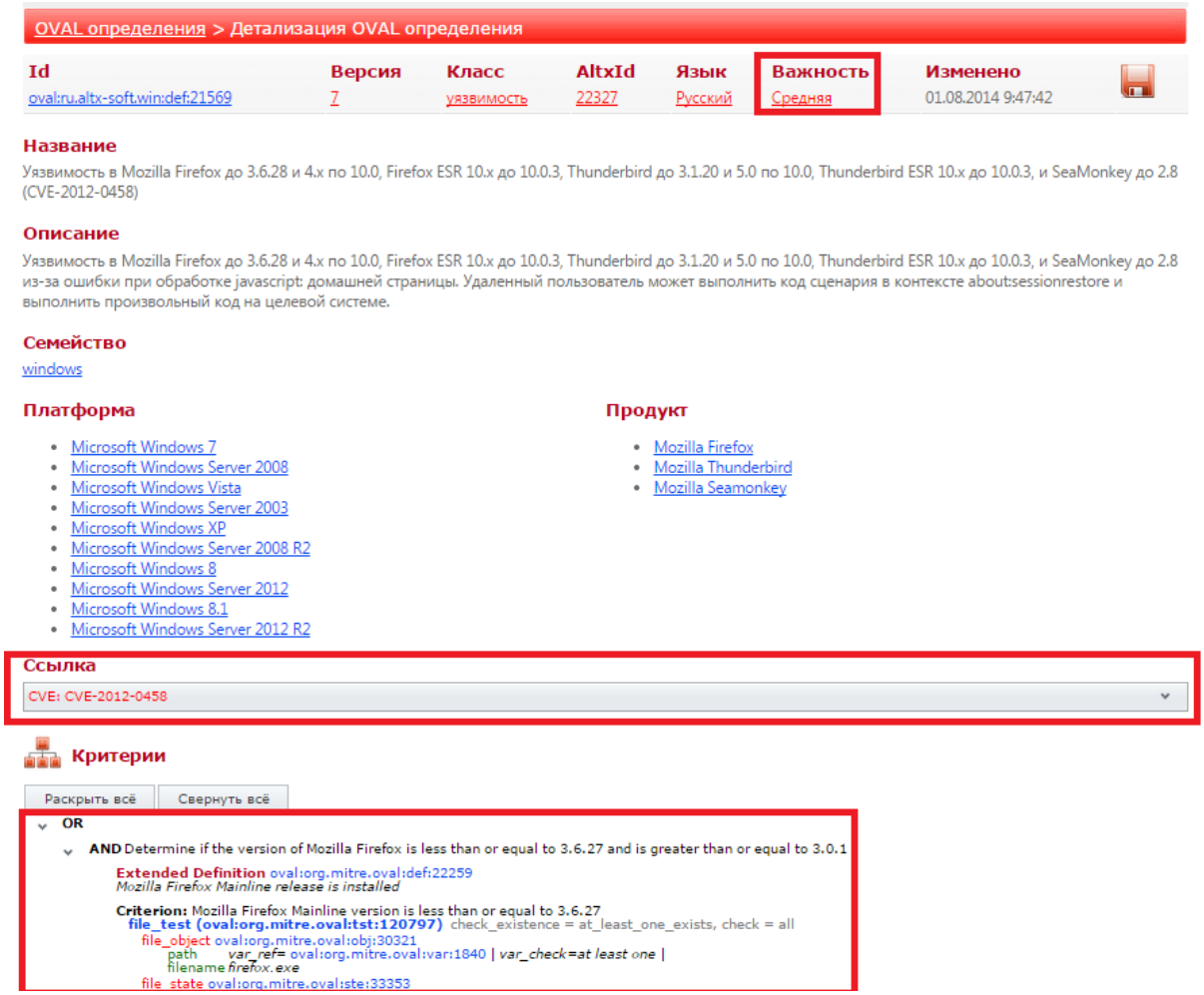


Рисунок 5.7.2.3

Карточка определения содержит исчерпывающую информацию, включающую: заголовок, метаданные , описание, применимые семейства\платформы\продукты, а также критерии определения проблем безопасности. Критерии определения описаны на языке **OVAL**, и могут скачаны в виде XML-файл для применения в составе сторонних стандартизованных OVAL-интерпретаторов.

Содержание главы...

На (Рисунок 5.7.3.1) изображена информационная панель, содержащая ссылки на другие возможности ресурсса **OVALdb**.

Рисунок 5.7.3.1

OVAL определения - полный перечень имеющихся в базе OVALdb определений в табличном виде с возможностью поиска по части строки (для этого нужно нажать на значок справа от поля фильтра и выбрать «Contains»).

OVAL объекты - определения для тестов, объектов, эталонных значений и переменных.

Облако тегов - наиболее часто употребляемые в OVALdb слова («ключевые слова») ресурса.

Категории -полный список определений какой-либо категории, например, содержащих ссылку на идентификатор CVE, или же относящихся к Microsoft Security Bulletin (бюллетени безопасности Microsoft).

RedCheck -инициирует переход на сайт redcheck.ru, посвященный САЗ RedCheck.

О проекте -краткая информация об **OVALdb, SCAP и OVAL**, международные статусы репозитория, условия доступа.

Содержание главы...

6. Разрешение проблем

6.1 Мастер диагностики проблем

Мастер диагностики проблем предназначен для анализа работоспособности основных компонентов программы:

- Базы данных;
- Службы синхронизации;
- Лицензия;
- Службы сканирования.

Мастер так же позволяет решать некоторые другие проблемы, либо получить подробную информацию о том, что делать, если решение проблемы невозможно средствами RedCheck.

Для определения состояния каждого из компонентов используется цветовая индикация:

- Зеленый - компонент работает корректно;
- Оранжевый - возникла проблема с работой компонента, которую программа устранит самостоятельно (с разрешения пользователя), либо предложит инструкцию для ее решения. Для разрешения проблемы необходимо левой кнопкой мыши нажать на компонент, в работе которого произошел сбой, после чего произойдет переход в меню с соответствующими инструкциями.
- Красный - обнаружена неопределенная ошибка, для устранения которой у программы отсутствует сценарий. При этом необходимо обратиться в службу поддержки. Для более подробной информации о возникшей ошибке необходимо левой кнопкой мыши нажать на компонент, в работе которого произошел сбой, после чего произойдет переход в меню с соответствующими инструкциями.

Запуск **Мастера диагностики** проблем происходит автоматически при каждом старте консоли управления RedCheck. Самостоятельно запустить **Мастер** можно в меню *«Инструменты»→ «Диагностика» → «Мастер диагностики проблем»*.

Содержание главы...

6.2 Проверка целостности контента

Модуль проверки целостности контента позволяет определить наличие отсутствующих, либо избыточных элементов контента безопасности.

Избыточный контент не влияет на работоспособность программы, таким образом, присутствие записей в поле ***«Лишние элементы»*** допустимо. В случае обнаружения недостающих элементов рекомендуется выполнить синхронизацию контента или дождаться, когда синхронизация выполнится автоматически по заданному расписанию.

Чтобы произвести проверку целостности контента, загруженного в программу RedCheck, необходимо перейти в меню ***«Инструменты»*** → ***«Диагностика»*** → ***«Проверка целостности контента».***

Если в результате обновления контента, поле отсутствующих элементов содержит какие-либо записи, рекомендуется обратиться в службу технической поддержки компании АЛТЭКС-СОФТ: support@altx-soft.ru.

Содержание главы...

6.3 Службы сканирования и синхронизации недоступны

Возможных причин может быть несколько. Последовательно выполните проверку согласно инструкциям ниже.

- В окне консоли управления RedCheck откройте выпадающее меню ***«Инструменты»*** и выберите опцию ***«Переподключиться к службе сканирования и серверу синхронизации»***.
- Если переподключение не дало результатов, возможно, остановлена сама служба. В окне консоли управления RedCheck откройте выпадающее меню ***«Инструменты»*** и выберите опцию ***«Перезапустить службу сканирования и сервер синхронизации»***.
- Возможна ситуация, когда служба сканирования не запускается даже в результате принудительного перезапуска. Это связано с тем, что служба **RedCheck Communication Server** не может получить доступ к базе данных.
- Проверьте корректность подключения к базе данных.

В случае если описанные выше рекомендации не помогли, убедитесь, что пользователь, от имени которого выполняется запуск программы, состоит в группе *REDCHECK_ADMINS*.

Содержание главы...

6.4 Сканирование в агентском режиме завершается с ошибкой

- Убедитесь, что хост доступен по сети.
- Убедитесь, что на сканируемом хосте, агент RedCheck установлен корректно.
- Если агент RedCheck установлен, но не отвечает, убедитесь, что служба *RedCheckAgent* запущена.
- В случае, когда агент RedCheck установлен, а служба RedCheck запущена, удостоверьтесь, что выполнены все требования по настройке.
- Убедитесь, что используется корректная учетная запись, от имени которой выполняется сканирование.

Содержание главы...

6.5 Сканирование в безагентском режиме завершается с ошибкой

- Убедитесь, что хост доступен по сети.
- Удостоверьтесь, что выполнены все требования, указанные в п.п. 2.3.4
- Убедитесь, что используется корректная учетная запись, от имени которой выполняется сканирование.

Содержание главы...

6.6 Сканирование в режиме Remote Engine (WinRM) завершается с ошибкой

- Убедитесь, что хост доступен по сети.
- Удостоверьтесь, что выполнены все требования, указанные в п.п. 2.5.2.2.
- Убедитесь, что используется корректная учетная запись, от имени которой выполняется сканирование.

Содержание главы...

6.7 Заблокирована возможность создания заданий "Аудит в режиме "Пентест"

- Проверьте, установлен ли компонент **Nmap**. В случае отсутствия, компонент можно скачать на официальной странице: www.Nmap.org
- Если компонент **Nmap** установлен, проверьте подключение **Nmap** к RedCheck.

Для этого в выпадающем меню ***«Инструменты»***, выберать пункт ***«Настройки»***, и перейти на вкладку ***«Сканирование»***. Активировать опцию ***«Использовать Nmap»***, после чего укажите путь к файлу *Nmap.exe*, нажмите «Сохранить».

Стандартный путь установки сканера **Nmap**:

- для 64-разрядных систем - ***«C:\Program Files (x86)\Nmap\Nmap.exe»***
- для 32-разрядных систем - ***«C:\Program Files\Nmap\Nmap.exe»***

Содержание главы...

6.8 Заблокирована возможность создания заданий аудита

- Убедитесь, что служба сканирования доступна. Причины недоступности указаны в п. 6.3.
- Выполните обновление контента. В случае если контент не был загружен, возможность созданий заданий блокируется во время синхронизации.

Содержание главы...

7. Обслуживание СУБД

В процессе эксплуатации RedCheck происходит естественное увеличение данных хранимых в базе данных, объем которых может быть критически увеличен для используемой системы.

В целях обеспечения стабильности и бесперебойности в работе СУБД рекомендуется, согласно внутреннего регламента, выполнять обслуживание СУБД для поддержания ее в актуальном состоянии.

Под обслуживанием подразумевается **четыре основных действия**:

1. Систематическое **бекапирование БД RedCheck**, для исключения потери данных в случае проблем в работе ПО или его окружения;

2. Очистка лога транзакций СУБД, которые чаще всего составляют большую долю информации хранящейся в СУБД;

3. Очистка неактуальных данных результатов сканирования по сроку давности.

4. Сжатие объема используемого СУБД на диске, **«Shrink»**.

Для очистки лога транзакций необходимо использовать **MSSQL Management Studio** и выполнить ряд действий:

- Подключиться к используемому экземпляру СУБД и выбрать БД RedCheck;
- В свойствах БД на вкладке параметры установить **Модель восстановления**: **Простая;**
- ПКМ на БД выбрать пункт ***Задачи→ Сжать→ Файлы***, в окне выбрать **Тип Файла**: **Журнал;**
- Выбрать операцию сжатия ***Сжать файлы*** до: **"установить желаемый размер, либо указать 0Мб";**
- Выполнить оптимизацию **«OK».**

Для удаления неактуальных данных хранящихся в БД, используя **MSSQL Management Studio**, необходимо выполнить следующие скрипты:

- Подключиться к используемому экземпляру СУБД и выбрать БД RedCheck;
- На панели инструментов выбрать пункт *«Создать запрос»* либо в пункте меню *Файл → Создать → Запрос в текущем соединении;*
- В открывшемся окне ввести команду без двойных кавычек *«DELETE FROM [dbo].[Scan] where [start] < cast('2019-11-21' as date)».*

Дата указана для примера, при выполнении данного пункта необходимо указывать правильную дату. Данный запрос удалит все результаты сканирования которые были получены до указанной даты.

- В открывшемся окне ввести команду без двойных ковычек *«DELETE FROM [dbo].[Report] WHERE createDate < cast('2019-11-21' as date)»*

Дата указана для примера, при выполнении данного пункта необходимо указывать правильную дату. Данный запрос удалит все сформированные отчеты которые были получены до указанной даты.

Для оптимизации объема занимаемого места БД на файловой системе необходимо выполнить ряд действий:

- Подключиться к используемому экземпляру СУБД и выбрать **БД RedCheck**
- ПКМ на БД выбрать пункт *Задачи → Сжать→ Файлы*, в окне выбрать *Тип Файла*: **Данные**
- Выбрать операцию сжатия **Сжать файлы** до: *«установить минимальное значение»*
- Выполнить оптимизацию *«ОК»*
- ПКМ на БД выбрать пункт *Задачи → Сжать → Данные*
- Выполнить оптимизацию *«ОК»*

ПРИЛОЖЕНИЕ А

Пример использования LDAP-фильтра

LDAP-фильтры используются для получения данных из Active Directory.

Фильтр определяет необходимые условия для включения объекта в результат запроса. **LDAP-фильтр** может содержать одно или более условий.

Примеры использования фильтра:

- Фильтр всех компьютеров:

(objectCategory=computer)

- Поиск всех доменов:

(objectCategory=domain)

- Выбор компьютеров без описания:

(&(objectCategory=computer)(!description=))*

- Поиск всех пользователей с общем именем начинающимся на ***«Bac»***:

(&(objectCategory=person)(objectClass=user)(cn=Bac))*

- Фильтр всех машин с Windows 10/ Windows Server 2016

(&(objectCategory=computer)(operatingSystem=Windows 10))*

(&(objectCategory=computer)(operatingSystem=Windows Server 2016))*

- Поиск всех Exchange-серверов

(&(objectCategory=computer)(servicePrincipalName=exchangeMDB)(operatingSystem=Windows Server*))*

- Выбор всех SQL-серверов, с любой серверной ОС, у которых зарегистрирован servicePrincipalName:

(&(objectCategory=computer)(servicePrincipalName=MSSQLSvc)(operatingSystem=Windows Server*))*

ПРИЛОЖЕНИЕ Б

Импорт/экспорт хостов через csv-файл

В программе RedCheck присутствует экспорта/импорта хостов через csv-файл.

Данный формат достаточно популярен. Позволяет представить информацию в виде списка, который, в дальнейшем, можно импортировать.

 *Содержимое файла должно быть написано в кодировке **UTF-8**, чтобы избежать проблем с импортом русскоязычных символов.*

Для выполнения данной процедуры необходимо перейти: ***Инструменты → Импорт хостов → Csv-file***, либо воспользоваться комбинацией клавишь **«Alt» + «F»**.

В (**Таблица 28**) представлено описание атрибутов csv-файла.

Таблица 28

Название параметра	Описание
GROUP	Имя группы
GroupDesc	Описание группы
Host	Имя хоста
HostDesc	Описание хоста
CPE	CPE хоста

Чтобы загрузить сразу всю информацию по хостам, группам и членством в группах, необходимо представить данные в следующем виде, как показано в (**Таблица 29**).

Таблица 29

Group	GroupDesc	Host	HostDesc	CPE
G1	GD1	H1	HD1	cpe:/o:microsoft:windows_7::sp1:x64
G1	GD1	H2	HD2	cpe:/o:microsoft:windows_7::sp1:x64
G1	GD1	H3	HD3	cpe:/o:microsoft:windows_7::sp1:x64
G2	GD2	H4	HD4	cpe:/o:microsoft:windows_7::sp1:x64
G2	GD2	H5	HD5	cpe:/o:microsoft:windows_7::sp1:x64
G2	GD2	H6	HD6	cpe:/o:microsoft:windows_7::sp1:x64

По скольку, заполнение всех колонок является необязательными, то с помощью этого формата можно загрузить только часть информации, например группы, как показано в (**Таблица 30**).

Таблица 30

Group	GroupDesc
G1	GD1
G2	GD2

Или только хосты, как показано в (**Таблица 31**).

Таблица 31

Host	HostDesc

H1	HD1
H2	HD2
H3	HD3
H4	HD4
H5	HD5
H6	HD6

- *Столбец, данные которого не планируется загружать (например, данные по группам) должен присутствовать, но быть пустым.*
- *Разделитель по умолчанию - точка с запятой. В окне импорта присутствует возможность его переопределения.*