АО «АЛТЭКС-СОФТ»

Программа контроля сертифицированной версии операционной системы Windows 7 («Seven_Check») в редакциях «Профессиональная», «Корпоративная» и «Максимальная»

РУКОВОДСТВО ПО ЭКСПЛУАТАЦИИ

Листов 43

2012

Содержание

Введение ... 3
1 Общие сведения ... 4
1.1 Архитектура приложения ... 4
1.2 Развитие функционала программ локальной настройки семейства «Check» ... 5
1.3 SCAP и репозитарий OVAL компании АЛТЭКС-СОФТ ... 6
1.4 Лицензирование программы ... 7
2 Установка программы. Общие функции программы ... 8
2.1 Установка и запуск на выполнение программы «Seven_Check» ... 8
2.2 Информационный контент программы. Организация online и offline режимов работы ... 10
2.3 Функции программы. Информационные статусы функций программы ... 12
2.4 Просмотр отчетов программы ... 16
2.5 Основные настройки программы ... 17
2.5.1 Установка параметров прокси-сервера ... 17
2.5.2 Поиск и диагностика неисправностей программы «Seven_Check» ... 17
2.5.3 Замена файла-конфигуратора параметров безопасности sceregvl.inf ... 18
2.5.4 Проверка сигнатур содержимого файлов контента ... 18
2.5.5 Личный кабинет пользователя ... 19
3 Автоматизированная настройка и контроль соответствия встроенных сертифицированных СЗИ Windows 7 ... 20
3.1 Просмотр информации о системе ... 20
3.2 Контроль сертифицированных обновлений безопасности ... 20
3.3 Фиксация и контроль встроенных СЗИ ... 24
3.4 Установка значений параметров безопасности на сертифицированные конфигурации ... 29
4 Функции дополнительного модуля аудита уязвимостей и конфигураций безопасности 33
4.1 Аудит обновлений ... 33
4.2 Аудит уязвимостей ... 34
4.3 Аудит конфигураций ... 36
4.4 Анализ сетевой активности ... 40
4.5 Проверка OVAL определений ... 42

Введение

Программа Seven_Check открывает новую линейку программ для настройки и контроля параметров безопасности сертифицированных продуктов Microsoft. Отличительной особенностью программ является поддержка международного протокола Security Content Automation Protocol (SCAP, протокол автоматизации управления контентом безопасности) и более расширенный (чем в предыдущих версиях) функционал.

Программа предназначена для реализации следующих функций программы:

- просмотр информации о системе;
- контроль сертифицированных обновлений безопасности;
- фиксация и контроль встроенных СЗИ;
- настройка и контроль сертифицированных конфигураций параметров.
- аудит обновлений;
- аудит уязвимостей;
- аудит конфигураций безопасности;
- анализ сетевой активности.

Обо всех вопросах и проблемах работоспособности программы сообщайте в службу технической поддержки АО «АЛТЭКС-СОФТ» по электронной почте support@altx-soft.ru.

1 Общие сведения

1.1 Архитектура приложения

Приложение представляет собой обновленную версию программы настройки и контроля сертифицированной версии Windows 7. Программа предназначена для реализации следующих функций программы:

1) Базовые функции программы
   - просмотр информации о системе;
   - контроль сертифицированных обновлений безопасности;
   - фиксация и контроль встроенных СЗИ;
   - настройка и контроль сертифицированных конфигураций параметров.

2) Дополнительные функции программы
   - аудит обновлений;
   - аудит уязвимостей;
   - аудит конфигураций безопасности;
   - анализ сетевой активности.

Базовые функции программы доступны в составе лицензии для пакета сертифицированной поддержки сертифицированной версии Windows 7. Они предназначены для настройки и проверки соответствия встроенных сертифицированных СЗИ (механизмов безопасности) Windows 7. Для реализации базовых функций программа использует актуальные сведения о сертифицированных обновлениях безопасности, получаемые из Центра сертифицированных обновлений организации-заявителя сертификации Windows 7 в Системе сертификации средств защиты информации по требованиям безопасности информации № РОСС RU.0001.01БИ00 компании ООО «Сертифицированные информационные системы» http://certsys.ru/updatecenter/.

Базовые функции программы доступны в локальном и сетевом режиме функционирования программы. В локальном режиме функционирования программы информационный контент программы обновляется непосредственно из Центра сертифицированных обновлений, управление базовыми функциями происходит непосредственно из окна программы. В сетевом режиме функционирования программы информационный контент программы обновляется с сервера программы Net_Check. Сетевой режим функционирования обеспечивается специальной службой (программой «Агент Net_Check»), предназначенной для функционирования в инфраструктуре программы Net_Check (http://www.altx-soft.ru/groups/page-268.htm). Для обеспечения локального режима работы установка Агента Net_Check не требуется.

Дополнительные функции – опциональный отдельно лицензируемый функционал, расширяющий базовые функции на всю вычислительную систему (операционную систему, а также общее и прикладное программное обеспечение). Дополнительные функции реализованы на основании обновляемого с централизованного Репозитория информационного контента безопасности, сформированного с использованием протокола SCAP (подробнее о SCAP и Репозитории в п.п. 1.3 настоящего Руководства).

Для доступа к «облачным» сервисам (Центру сертифицированных обновлений и Репозиторию SCAP контента) программы необходима установка сертификатов компании ООО «Сертифицированные информационные системы».

Подключение к «облачным» сервисам программы может осуществляться с использованием удаленной машины. В этом случае контент копируется на машину через личный кабинет Центра сертифицированных обновлений и сертификаты устанавливаются на данную удаленную машину.

Рисунок 1.1 Функциональная схема применения программы Seven_Check

1.2 Развитие функционала программ локальной настройки семейства «Check»

Программа Seven_Check открывает новую линейку программ для настройки и контроля параметров безопасности сертифицированных продуктов Microsoft. Отличительной особенностью программ является поддержка международного протокола Security Content Automation Protocol (SCAP, протокол автоматизации управления контентом безопасности) и более расширенный (чем в предыдущих версиях) функционал.

Унифицированные механизмы и функции **Seven_Check**, используют встроенные в программу OVAL и XCCDF интерпретаторы и предоставляют пользователям доступ к содержимому Репозитория контента безопасности http://ovaldbru.altx-soft.ru,, а также возможность использовать произвольный SCAP-контент, в том числе и всемирно известных компаний в области информационной безопасности, таких как: MITRE, NIST, DISA, SecPod, и др. Передовые технологии **Seven_Check** позволяют более оперативно реагировать на появляющиеся угрозы, значительно расширить область применения программ Check и повысить эффективность механизмов настройки и контроля параметров безопасности как сертифицированных продуктов Microsoft, так и другого программного обеспечения, включая наложенные СЗИ.

Seven_Check может использоваться **не только в составе сертифицированных продуктов**, но и как самостоятельное средство оценки уязвимости защищенных систем, построенных на платформе Microsoft.

Программа **Seven_Check** реализует **информационную панель**, позволяющую на основании проверок параметров программ мгновенно оценить степень соответствия системы безопасности принятому набору требований.

1.3 SCAP и репозитарий OVAL компании АЛТЭКС-СОФТ

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

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

  - Расширяемый формат описания контрольного списка конфигураций (XCCDF, 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).
- **Формат отчетов.** Форматы отчета SCAP представляют необходимые конструкции, для выражения собранной информации в стандартизированных форматах.
- **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).
- **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).
- **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 зашиты информации.

Статус SCAP как международного проекта обеспечивает участие в нем широкого круга специалистов в области ИБ. Протокол поддерживается ведущими мировыми вендорами, такими как Microsoft, Cisco, Symantec, Red Hat 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.

Встроенный в программы Check Интерпретатор языка OVAL, поддерживает последнюю на данный момент версию языка 5.10.1. Программы Check четвертого поколения со встроенными OVAL и XCCDF интерпретаторами дают возможность работы с произвольным SCAP-контентом для оценки состояния защищенности потенциально любых программных и аппаратно-программных продуктов.

Тематический 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 всего SCAP-сообщества.

1.4 Лицензирование программы

Лицензирование программы предполагает обязательное приобретение лицензии непосредственно на программу Seven_Check (что обеспечивает возможность использования базовых функций работы с сертифицированной версий Windows 7). Лицензия на программу бессрочная и действительна на всём периоде действия сертификата ФСТЭК на сертифицированную версию Windows 7.

Кроме того, возможно опциональное приобретение лицензии на дополнительные функции программы, реализованные в модуле анализа уязвимостей и конфигураций безопасности. Лицензия на модуль анализа уязвимостей и конфигураций безопасности действительна в течение года с момента установки программы. В течение указанного периода пользователь имеет возможность получать актуализированный и пополняемый контент безопасности из Репозитория SCAP-контента АЛТЭКС-СОФТ.

В случае приобретения лицензии на дополнительной модуль аудита уязвимостей и конфигураций безопасности срок лицензии отображается в окне "О программе", вызываемом из меню «Справка» программы (см. рисунок 1.2).

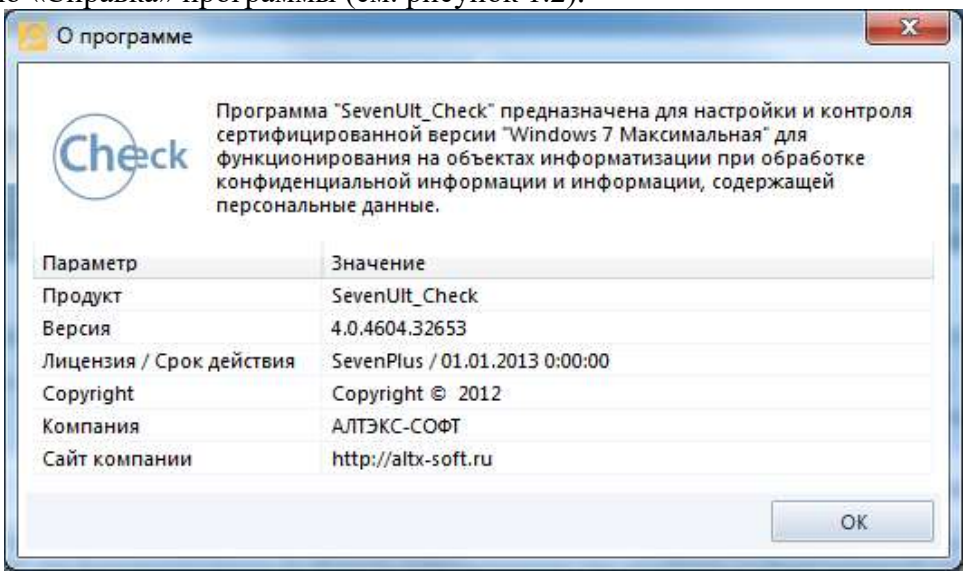


Рисунок 1.2. Окно «О программе».

2 Установка программы. Общие функции программы

2.1 Установка и запуск на выполнение программы «Seven_Check»

Для установки программы необходимо выполнить следующую последовательность действий:

1) Начать сеанс Microsoft Windows 7 с правами локального администратора.
2) Установить .NET Framework 4.0. Для этого запустить файл DotNetFX/ dotNetFx40_Full_x86_x64.exe с диска Media Kit и произвести процедуру инсталляции в директорию по умолчанию.
3) Произвести установку драйвера электронного ключа eToken с записанным цифровым сертификатом организации. Для этого выполнить файл etokenpkiclient51sp1/PKIClient-x32-5.1-SP1.msi с диска MediaKit.
4) Загрузить с Центра сертифицированных обновлений компании «Сертифицированные информационные системы» по адресу http://certsys.ru/updatecenter/ и произвести установку цифровых сертификатов удостоверяющих центров компании «СИС». Для этого произвести последовательную загрузку Сертификата № 1 и Сертификата №2 с сайта компании «СИС». Для этого необходимо щелкнуть мышью по соответствующей ссылке и появившемся окне нажать кнопку «Открыть» (см. рисунок 3.1). В появившемся окне нажать кнопку «Установить сертификат» (см. рисунок 3.2).
5) Примечание: а) Для обеспечения гарантированной корректной работы при наличии нескольких установленных браузеров обозревателем по умолчанию следует устанавливать Microsoft Explorer. В противном случае, для других обозревателей, установленных по умолчанию, может потребоваться ручная установка цифровых сертификатов (после их сохранения на локальный диск компьютера).
6) Выполнить файл setup.exe и произвести установку программы. В процессе установки программы будет предложено выбрать каталог программы и пользователей, для которых программа устанавливается.
7) Вставить электронный ключ eToken в USB-порт и произвести запуск программы «Seven_Check» выполнением исполняемого файла из каталога установки программы или меню «Пуск».

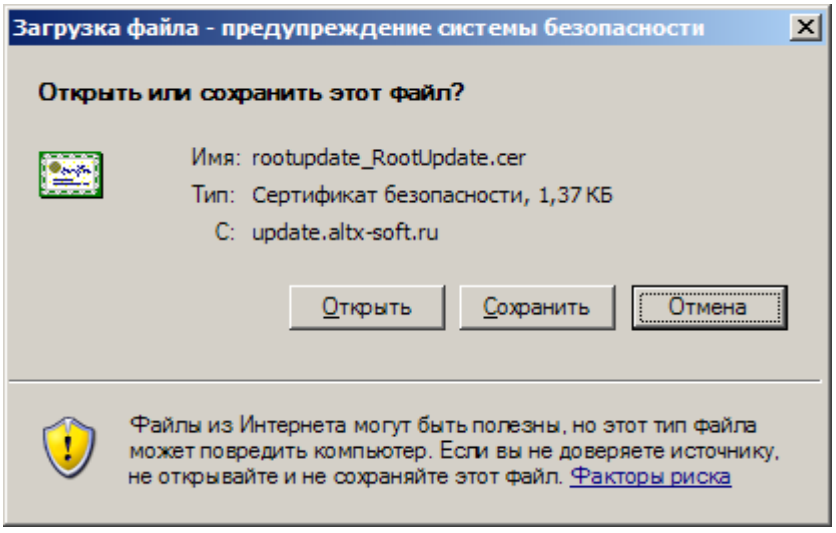


Рисунок 2.1- Открытие цифрового сертификатов удостоверяющего центра

Рисунок 2.2 - Установка цифрового сертификатов удостоверяющего центра

Рисунок 2.3 – Главное окно программы контроля сертифицированной версии Microsoft Windows 7

При каждом запуске программы на экран представляется окно на выбор пользовательского сертификата, записанного на электронный ключ eToken. При выборе

соответствующего сертификата необходимо ввести Pin-код для доступа к защищенной области памяти eToken.

При выборе корректного сертификата и вводе правильного Pin-кода программа получает доступ к «облачным» сервисам и на экран будет выведено главное окно программы, представленное на рисунке 2.3.

В случае некорректного ввода или нажатия кнопки программы «облачные» сервисы программы будут недоступны, но функционирование программы возможно на основании последнего обновленного с сервиса контента безопасности.

После первого запуска программы необходимо провести обновление контента (выбрать пункт главного меню «Обновить контент» или нажать ссылку «Обновить» в нижнем правом углу окна программы). В противном случае, выполнение базовых функций будет осуществляться на основании вложенного в дистрибутив программы (и актуального на момент его производства контента), а выполнение дополнительных функций будет невозможно.

2.2 Информационный контент программы. Организация online и offline режимов работы

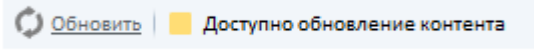
Информационный контент программы составляют следующие сведения:

- информация о лицензии на программу и дополнительный модуль аудита уязвимостей;
- сведения о сертифицированных обновлениях, применительно к версии ОС, на которой эксплуатируется экземпляр программы, контрольные суммы файлов обновлений;
- сведения об обновлениях ОС (актуальный список от вендора) и общего программного обеспечения – необходимы для функционирования дополнительного модуля аудита конфигураций и конфигураций безопасности;
- сведения об уязвимостях ОС и общего программного обеспечения, эксплуатирующего на локальном АРМ – необходимы для функционирования дополнительного модуля аудита конфигураций и конфигураций безопасности;
- сведения о конфигурациях параметров безопасности – необходимы для функционирования дополнительного модуля аудита конфигураций и конфигураций безопасности.

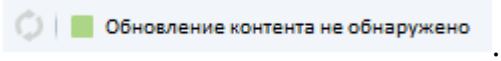
Online режим работы программы предполагает постоянное или периодическое (на время обновления информационного контента программы подключение к «облачным сервисам».

Для реализации online-режима работы программы необходим доступ к «облачным сервисам» с использованием сертификата на электронном ключе eToken. Если по какой либо причине доступ к сертификату (с вводом PIN кода) не произведен, необходимо перезапустить программу, при запуске программы выбрать сертификат пользователя, ввести PIN-код для доступа к защищенной части eToken.

В online режиме программа информирует пользователя о доступности на сервере программы в Интернете нового или обновленного контента. По этому факту пользователь информируется при появлении в левом нижнем углу программы надписи



. Обновление контента происходит при нажатии на ссылку «Обновить» либо при выборе пунтка меню «Обновить контент» главного меню программы. В случае успешно обновленного контента в левом нижнем углу появляется сообщение



.

Offline режим работы программы предполагает ручное копирование контента в рабочий каталог программы с закрытой части сайта компании «Сертифицированные информационные системы». Для этого необходимо:

1) В меню «Справка» выбрать пункт «Личный кабинет».
2) Перейти за https://update.certsys.ru/ . Выбрать сертификат пользователя. Ввести PIN-код.
3) В разделе «Обновление контента» скачать обновление контента для своей версии ОС.
4) Скопировать содержимое архива в папку Data рабочего каталога с программой.
5) Перезапустить программу.

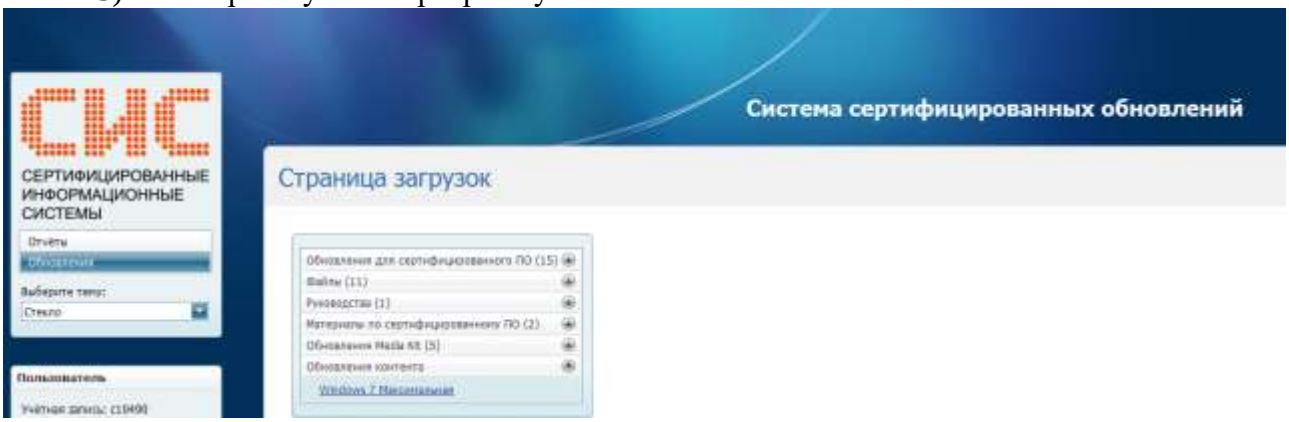


Рисунок 2.4 –Копирование информационного контента программы.

6) После копирования содержимого архива, становится доступным новые и обновленные «ленты» контроля в функциях «Аудит обновлений», «Аудит уязвимостей» и «Аудит конфигураций», становится доступным дополнительный функционал (доступный по лицензии на модуль аудита уязвимостей и конфигураций безопасности).

Ленты контроля доступны в модулях «Аудит обновлений», «Аудит уязвимостей» и «Аудит конфигураций» (см. рисунки 2.5, 2.6).

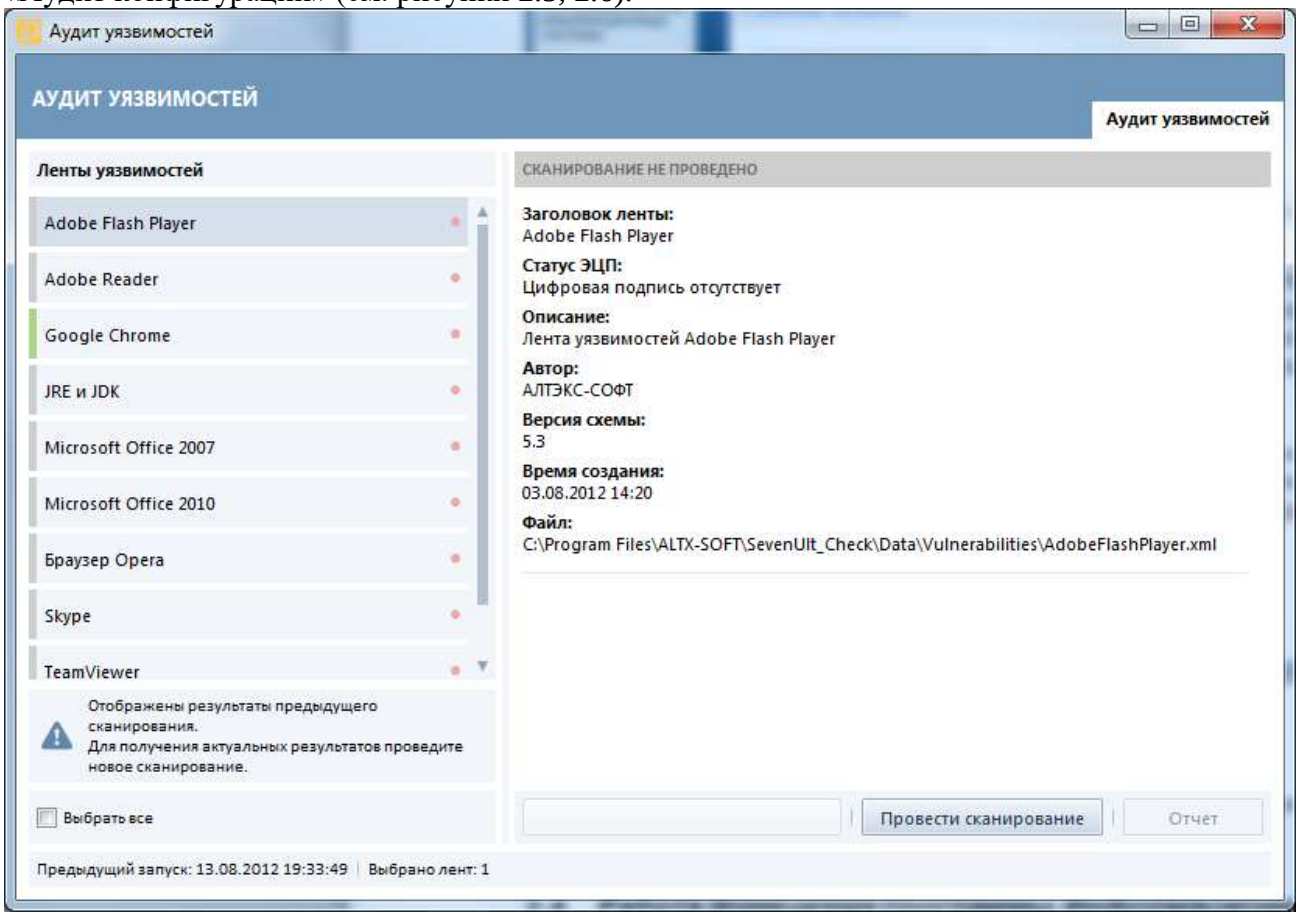


Рисунок 2.5 – Доступные ленты уязвимостей после проведения обновления контента

Наличие красной точки справа от наименования ленты говорит о том, что лента модифицирована, т.е возможно в неё были внесены несанкционированные изменения.

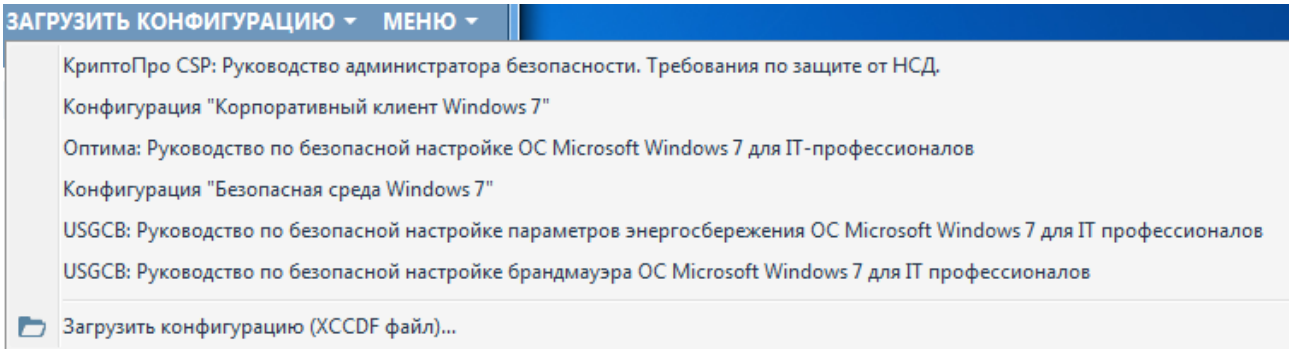
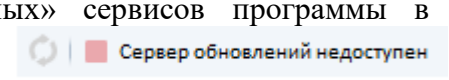


Рисунок 2.6. – Доступные конфигурации аудита в меню «Загрузить конфигурацию» модуля «Аудит конфигураций»

Примечание: При отсутствии доступа к «облачным сервисам» следует проверить настройки брэндмауэра и антивируса и при необходимости внести выполняемый файл программы «Seven_Check» для создания разрешающего правила брэндмауэра. В случае недоступности «облачных» сервисов программы в левом нижнем углу программы показывается сообщение 

.

2.3 Функции программы. Информационные статусы функций программы

Главное окно программы в центральной части содержит набор кнопок, доступ к которым производится с использованием горизонтальной области прокрутки. Описание функций приведено в таблице 2.1.

Таблица 2.1 Функции программы

Рисунок кнопки	Наименование кнопки	Реализуемые функции
	Информация о системе	Общие сведения о ОС Общие сетевые ресурсы и папки Переменные среды Информацию о локальных пользователях компьютера Информация о процессах Системные папки Информация о системных службах **Функция доступна по лицензии на программу**
	Аудит обновлений	Просмотр списков («лент») обновлений: контроль и ссылки на установку сертифицированных обновлений; контроль файла обновления по контрольной сумме **Функции доступны по лицензии на программу** аудит «лент» обновлений, доступных по лицензии на модуль аудита обновлений и конфигураций безопасности; **Ленты обновлений отличные от списка**

		сертифицированных обновлений доступны по лицензии на модуль аудита уязвимостей и конфигураций безопасности
	Аудит уязвимостей	Аудит уязвимостей ОС и другого программного обеспечения на основании данных информационного контента программы; - Microsoft Windows и Microsoft Office 2007, 2010; - продукты Adobe (Adobe Reader, Adobe Flash Player); - браузеры (Google Chrome, Opera); - другие продукты. **Функция доступна по лицензии на модуль аудита уязвимостей и конфигураций безопасности**
	Аудит конфигураций	Аудит рекомендованных расширенных конфигураций параметров безопасности. Аудит настройки наложенных СКЗИ и СЗИ. **Функция доступна по лицензии на модуль аудита уязвимостей и конфигураций безопасности**
	Фиксация и контроль	Фиксация и контроль по контрольным суммам целостности исполняемых файлов и библиотек Windows, других программных средств, с использованием встроенного сертифицированного программного средства «ФИКС-библиотека 1.0» **Функция доступна по лицензии на программу**
	Конфигурации безопасности	- контроль и настройка сертифицированных конфигураций безопасности в режиме «одной кнопки» и для каждого параметра в отдельности; - создание и применение произвольных пользовательских конфигураций параметров безопасности; **Функция доступна по лицензии на программу**
	Анализ сетевой активности	- мониторинг используемых TCP и UDP портов; - мониторинг приложений, ведущих сетевую активность; - создание разрешающих и запрещающих правил брэндмауэра Windows. **Функция доступна по лицензии на модуль аудита уязвимостей и конфигураций безопасности**

	Проверка OVAL определений	Проверка соответствия произвольному набору определений OVAL **Функция доступна по лицензии на модуль аудита уязвимостей и конфигураций безопасности**

Каждая функция, кроме «Информация о системе» и «Проверка OVAL определений», имеет набор цветовых статусов, определяемых на основании данных **предыдущего произведенного контроля**. Статусы сохраняются до проведения очередного контроля выбранной функции. Таким образом, можно получать информацию о состоянии контроля системы на основании данных предыдущего контроля, в т.ч. и при старте программы.

1. Нейтральный статус. Отображается в виде серо-синего цвета кнопки. Статус означает, что контроль функции не проводился.

   Пример отображения нейтрального статуса приведен на рисунке 2.7.

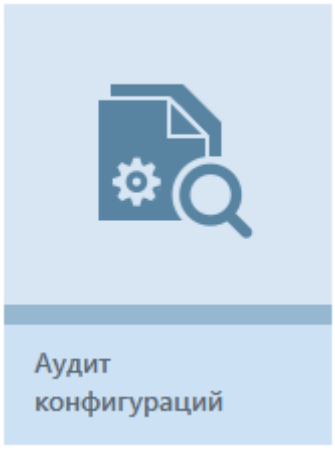


Рисунок 2.7. Пример нейтрального статуса

2. Статус «Несоответствие». Отображается в виде красного цвета кнопки. Означает, что на основании данных предыдущего контроля выявлено как минимум одно условие несоответствия. Детальная информация о статусе описана в таблице 2.2

   Таблица 2.2. Детальная информация о статусе «несоответствие»

Наименование функции	Описание
Аудит обновлений	Одна или несколько лент обновление при проведенном контроле обновлений имеет статус «требуется установка обновлений», что означает - в списке присутствует по крайней мере одно неустановленное обновление.
Аудит уязвимостей	Одна или несколько лент обновление при проведенном контроле обновлений имеет статус «требуется установка уязвимостей», что означает - в ленте зафиксирована по крайней мере одна уязвимость.
Аудит конфигураций	При последнем проведенном контроле при выборе определенной конфигурации параметров зафиксирован статус «требуется вмешательство», что означает, что по крайней мере один из контролируемых параметров не соответствует эталонному значению.
Фиксация и контроль	Имеется по крайней мере один факт нарушения целостности одного или нескольких заданий фиксации.
Конфигурации безопасности	При последнем проведенном контроле при выборе сертифицированной конфигурации параметров зафиксирован

	статус «требуется вмешательство», что означает, что по крайней мере один из контролируемых параметров не соответствует эталонному значению.
Анализ сетевой активности	В системе диагностированы «вирусные» порты или процессы

При наведении на кнопку со статусом «несоответствие» показывается сводная информация о проведенном контроле, аналогичная представленной на рисунке 2.8.

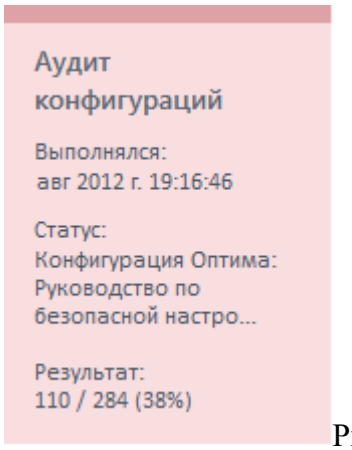


Рисунок 2.8. Пример статуса «несоответствие»

3. Статус «Ошибка». Отображается в виде оранжевого цвета кнопки. Означает, что на основании данных предыдущего контроля выявлено как минимум одно состояние ошибка, либо не произведен контроль для сформированного задания фиксации. Состояние ошибка применительно к состоянию аудита говорит об ошибочном файле информационного контента, в связи чем необходимо обратиться к разработчику программы.

При наведении на кнопку со статусом «несоответствие» показывается сводная информация о проведенном контроле, аналогичная представленной на рисунке 2.9.

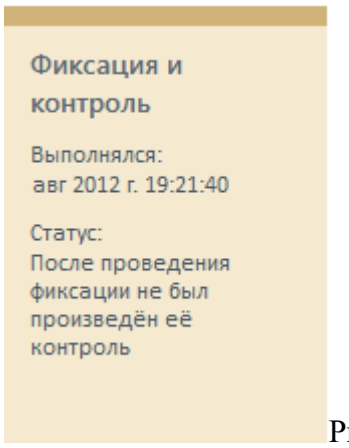


Рисунок 2.9. Пример статуса «ошибка»

4. Статус «Соответствие». Отображается в виде зеленого цвета кнопки. Означает, что на основании данных предыдущего контроля все данные соответствуют эталонным значениям. Детальная информация о статусе описана в таблице 2.3

Таблица 2.3. Детальная информация о статусе «соответствие»

Наименование функции	Описание
Аудит обновлений	При последнем проведенном контроле для всех выбранных лент обновлений все обновления в системе установлены
Аудит уязвимостей	При последнем проведенном контроле для всех выбранных лент уязвимостей в системе не

	обнаружено
Аудит конфигураций	В последней контролируемой конфигурации параметров все значения параметров соответствуют эталонным значениям
Фиксация и контроль	Все задания фиксации прошли успешный контроль (контрольные суммы контролируемых файлов соответствуют эталонным значениям)
Конфигурации безопасности	В последней контролируемой сертифицированной конфигурации параметров все значения параметров соответствуют эталонным значениям
Анализ сетевой активности	В системе не диагностированы «вирусные» порты или процессы

При наведении на кнопку со статусом «соответствие» показывается сводная информация о проведенном контроле, аналогичная представленной на рисунке 2.10.

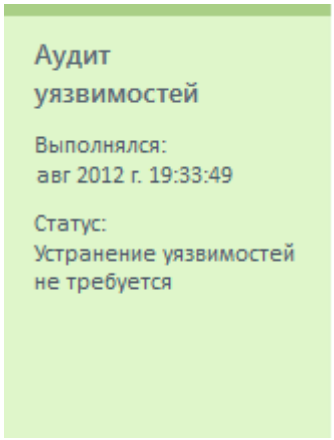


Рисунок 2.10. Пример статуса «соответствие»

2.4 Просмотр отчетов программы

Большинство функций (базовых и дополнительных) программы имеют возможность построения детальных отчетов. Отчеты программы отображаются в отдельном окне, пример которого показан на рисунке 3.4.

Верхняя панель кнопок окна отчета реализует функции работы с отчетом:

- поиск текстовой строки в отчете;
- печать отчета;
- просмотр с изменением масштаба отчета;
- экспорт документа во внешние форматы файлов;
- отправка документа, экспортированного во внешний формат;
- установка водяного знака.

Отдельно следует упомянуть о функции «экспорт во внешние форматы файлов». Список форматов файлов представлен на рисунке 2.11. С её помощью можно экспортировать отчет в файл для его последующего редактирования.

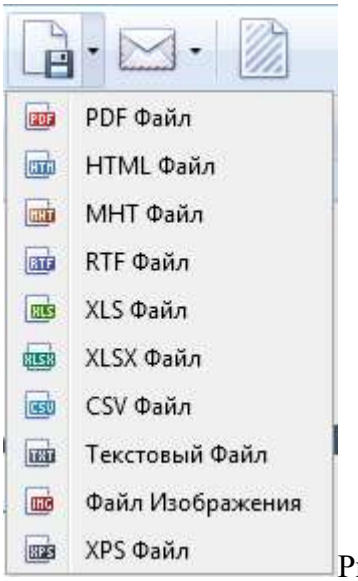


Рисунок 2.11. Экспорт отчетов во внешние форматы файлов.

2.5 Основные настройки программы

2.5.1 Установка параметров прокси-сервера

По умолчанию программа осуществляет работу с интернет с настройками подключения Internet Explorer. В случае, если необходимо установить специфичные настройки прокси-сервера следует нажать кнопку «Настройки» главного меню программы и в появившемся окне (см. рисунок 2.12) в ниспадающем списке «Прокси сервер» выбрать значение «HTTPS» и указать IP адрес и порт прокси, а в случае необходимости логин и пароль.

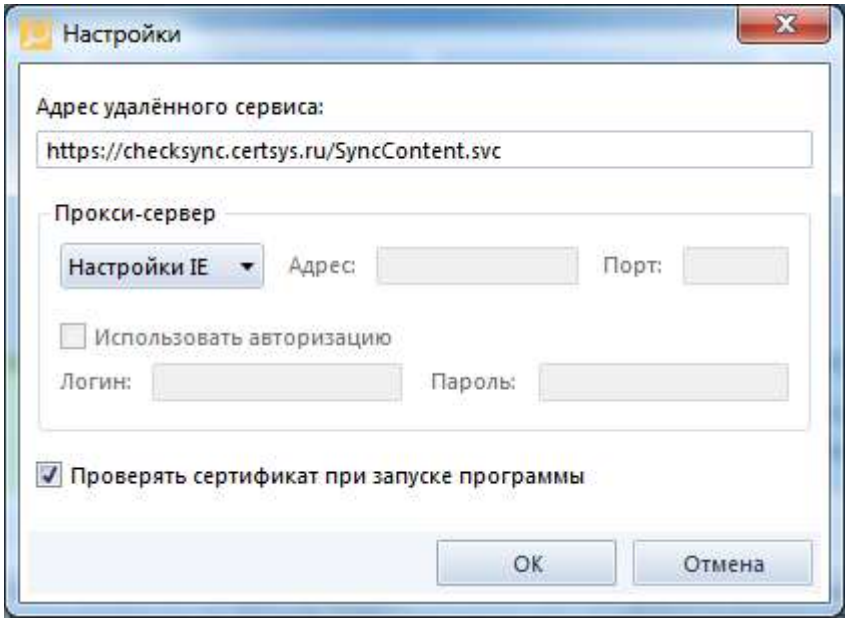


Рисунок 2.12 –Ввод параметров прокси-сервера

2.5.2 Поиск и диагностика неисправностей программы «Seven_Check»

Самой распространённой неисправностью является отсутствие доступа в интернет (т.е. с сервером «https://checks.certsys.ru/»). Проверьте Ваши настройки сетевого подключения, брандмауэр, антивирусное ПО. Возможно, указанные средства блокирует работу программы контроля, запрещая ей сетевую активность.

Все основные действия программы «Seven_Check» записываются в журнал (лог) работы программы (см. рисунок 2.13). При появлении ошибок следует вызвать журнал работы программы (нажать кнопку «Журнал событий» главного меню программы) и передать его содержание, а при необходимости и скриншоты экранов ошибок в службу технической поддержки АО «АЛТЭКС-СОФТ» support@altx-soft.ru для диагностики неисправности.

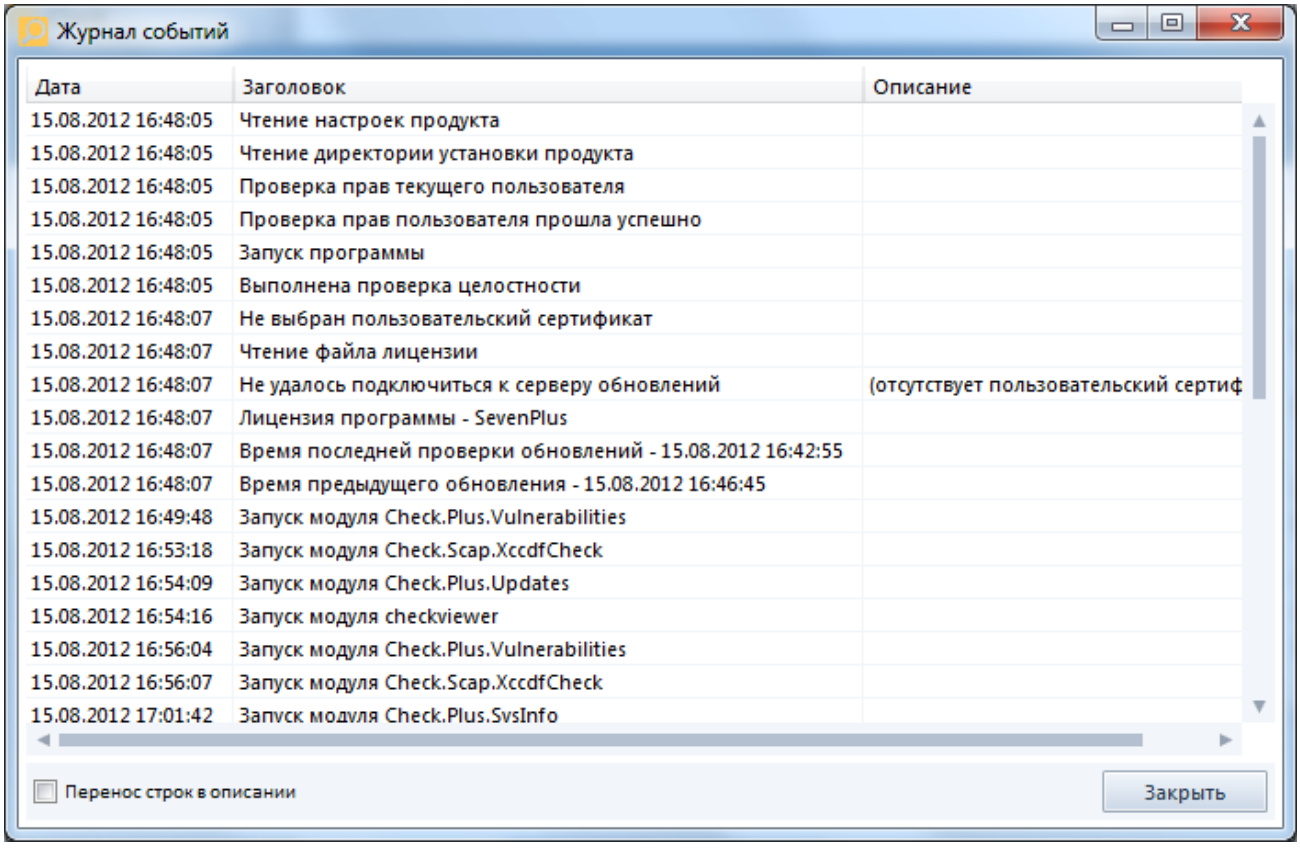


Рисунок 2.13 – Вид информационного окна программы, содержащей техническую информацию, при отсутствии доступа к серверу контроля.

2.5.3 Замена файла-конфигуратора параметров безопасности sceregvl.inf

Перед работой с сертифицированными конфигурациями параметров безопасности (базовая функция «Конфигурации безопасности») необходимо заменить файл настроек параметров безопасности, путем выбора пункта меню «Применить конфигуратор» главного меню программы программы. В результате данного действия будет замен файл <%System root%>\inf\sceregvl.inf.

После успешного выполнения функции будет представлено сообщение «Файл настроек параметров безопасности настроен».

2.5.4 Проверка сигнатур содержимого файлов контента

Проверка сигнатуры (хэш-значения) содержимого файлов контента программы производится для исключения возможности несанкционированной модификации файлов контента и получения неверных данных контроля и аудита.

Для проведения контроля необходимо выбрать пункт меню «Проверка сигнатур» основного меню программы. На экран будет представлено окно, в котором будет подсчитано количество файлов контента программы, сколько из них с верными и неверными сигнатурами.

Контент с неверной сигнатурой отображается в модулях аудита следующим образом:

(см. наличие красной точки справа от наименования ленты).

2.5.5 Личный кабинет пользователя

Для перехода в личный кабинет пользователя на закрытой части сайта ООО «Сертифицированные информационные системы» необходимо выбрать пункт меню «Личный кабинет» меню «Справка».

Для реализации online-режима работы программы необходимо использование сертификата на электронном ключе eToken. В личном кабинете пользователя (см. рисунок 2.14) в окне браузера доступны ряд функций, в частности скачивание:

- файлов сертифицированных обновлений;
- контента программы Seven_Check (см. п.п. 2.3 настоящего руководства);
- новые версии программы Seven_Check и Руководств;
- файлы шаблонов сертифицированных конфигураций параметров безопасности.

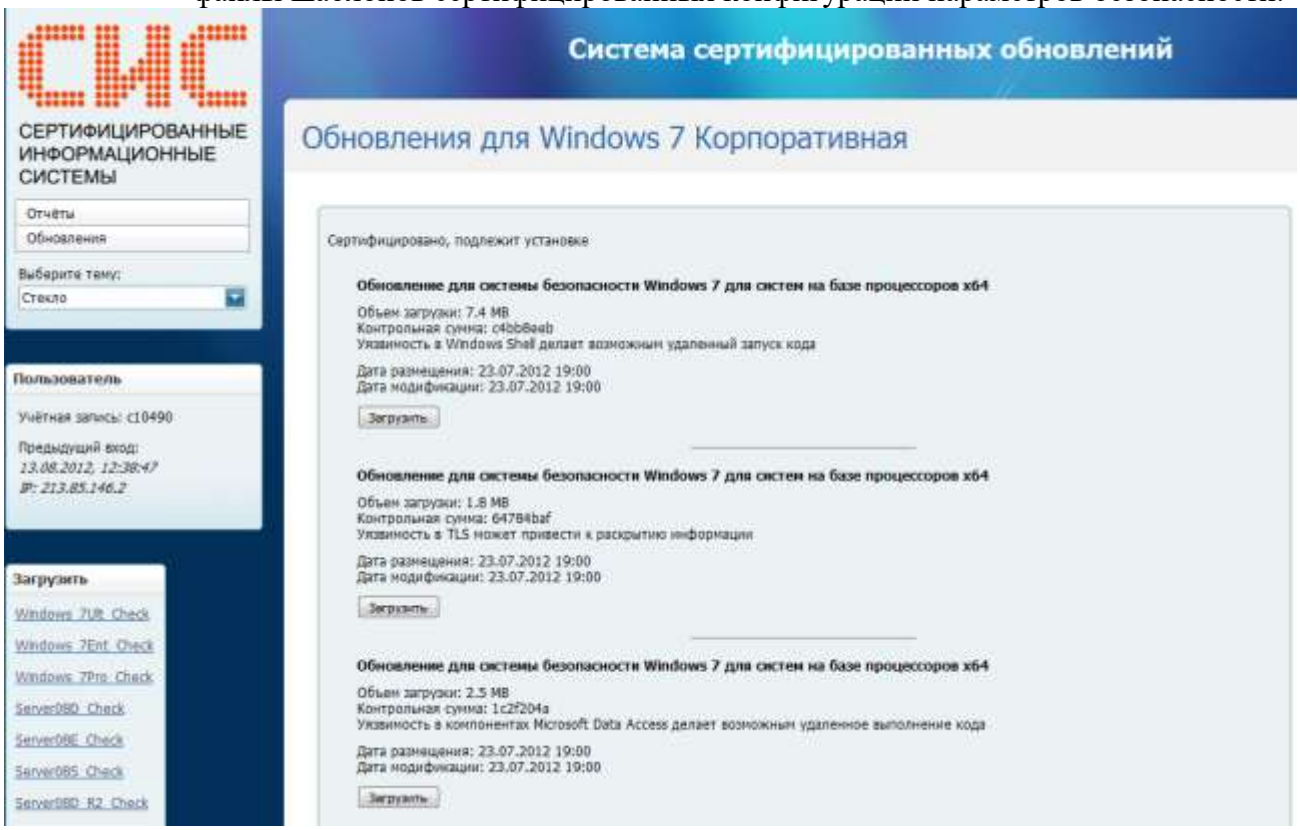


Рисунок 2.14 – Личный кабинет пользователя на сайте ООО «Сертифицированные информационные системы»

3 Автоматизированная настройка и контроль соответствия встроенных сертифицированных СЗИ Windows 7

3.1 Просмотр информации о системе

Для выполнения указанной функции необходимо нажать кнопку в центральной части окна программы.

Функция предоставляет справку о:

- общих сведениях о ОС;
- общих сетевых ресурсах и папках;
- переменных среды;
- информации о локальных пользователях компьютера;
- информации о процессах;
- системных папках;
- информации о системных службах.

При просмотре каждого подраздела функции в окне доступна ссылка на доступ к соответствующей системной информации Windows.

Функция доступна по лицензии на программу (базовой лицензии).

3.2 Контроль сертифицированных обновлений безопасности

Для выполнения указанной функции необходимо нажать кнопку в центральной части окна программы.

Целью контроля сертифицированных обновлений является регламентированное обновление встроенных СЗИ сертифицированной версии программы. Пользователи сертифицированной версии Windows 7 обязаны своевременно устанавливать сертифицированные обновления безопасности.

Список сертифицированных обновлений представлен в виде отдельной ленты в модуле «Аудит обновлений» (см. рисунок 3.1).

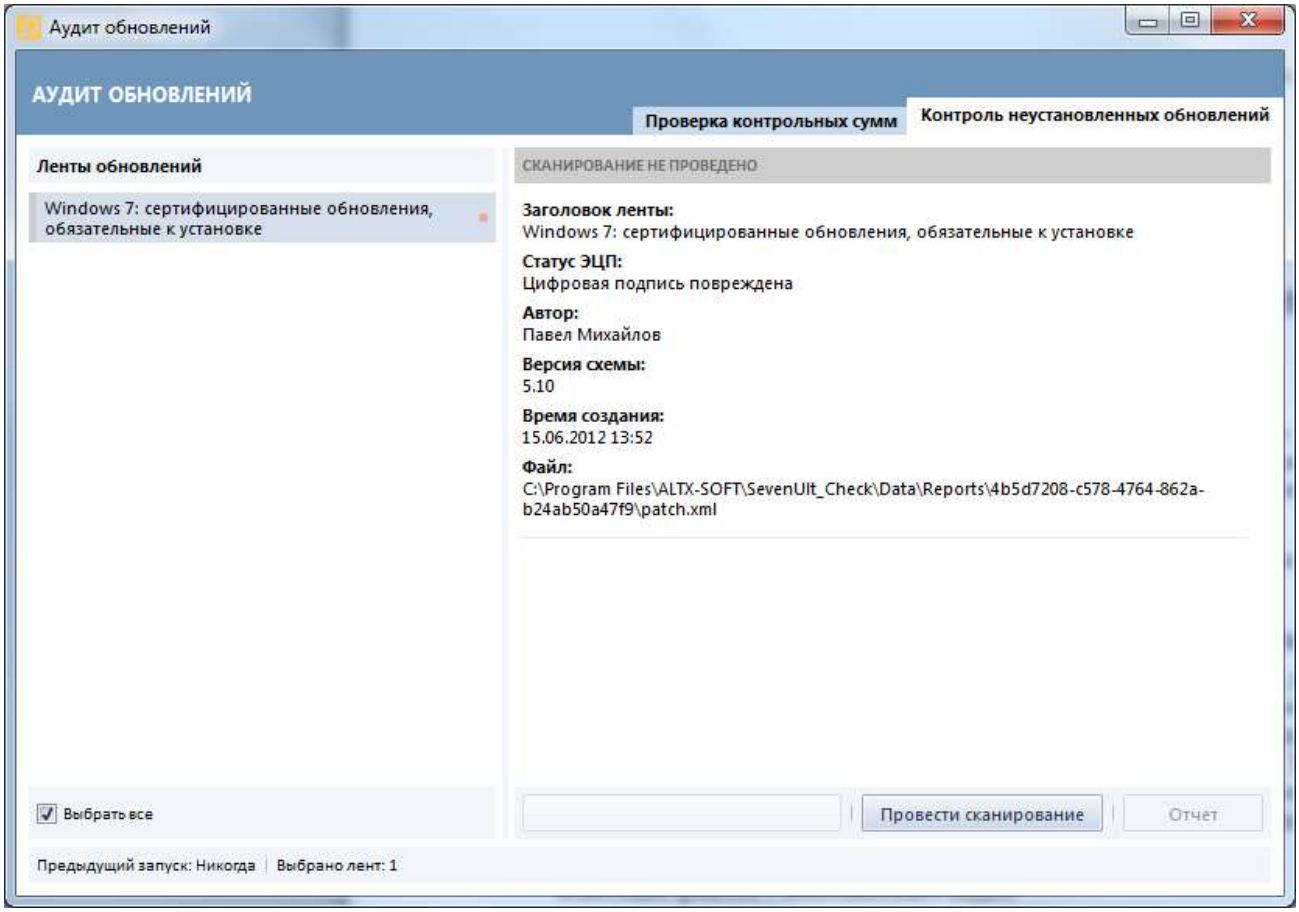


Рисунок 3.1 - Лента сертифицированных обнвлений.

Для проведения контроля необходимо нажать на кнопку «Провести сканирование». В результате проведенного сканирования возможны следующие статусы, показывающиеся в верхней части правой панели окна реализации функции:

- «требуется установка обновлений» (отображается красным цветом);
- «установка обновлений не требуется» (отображается зелёным цветом);
- «ошибка» (возникает, как правило, при повреждении контента программы, о чем необходимо сообщить в техническую поддержку программы), (отображается оранжевым цветом).

В случае необходимости установки сертифицированных обновлений безопасности можно просмотреть детальную информацию о каждом обновлении, нажав на красную кнопку «Не установлено». По ссылке на Microsoft KB необходимо перейти на страницу загрузки обновлений, скачать соотвествующее обновление (см. рисунок 3.2).

После закачки файла на локальную машину необходимо проверить его контрольную сумму. Для этого необходимо перейти на вкладку «Проверка контрольных суммы» и нажать в левой части окна кнопку «Выбрать файл» или «Выбрать каталог» (см. рисунок 3.3). В появившемся окне выбора файла отметить выбранный каталог/файл и нажать кнопку «Начать контроль». В случае успешного контроля в колонке «Эталон» таблицы показывается зеленая метка, в противном случае – красная (см. рисунок 3.3).

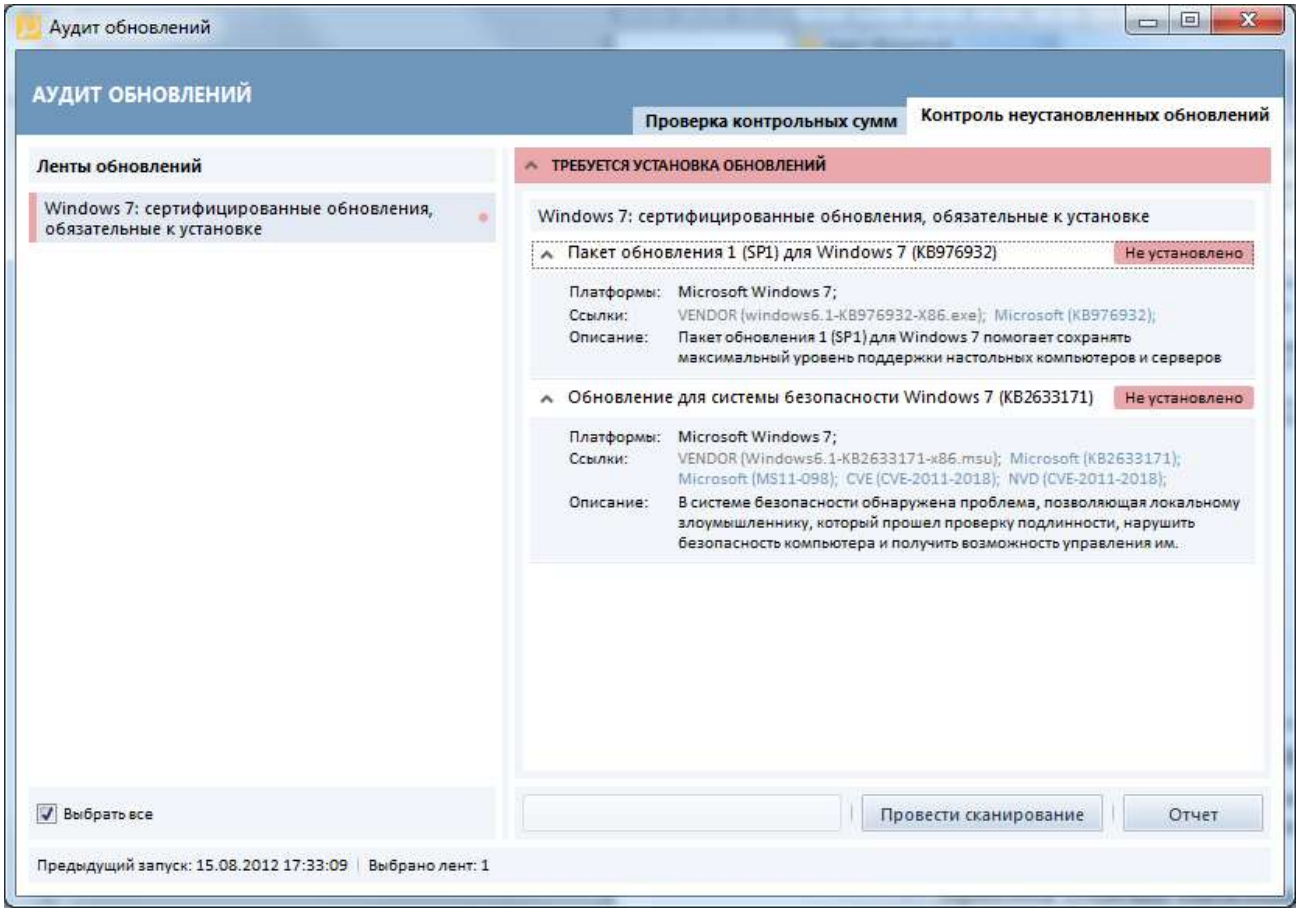


Рисунок 3.2 – Промотр сведений о неустановленных сертифицированных обновлениях

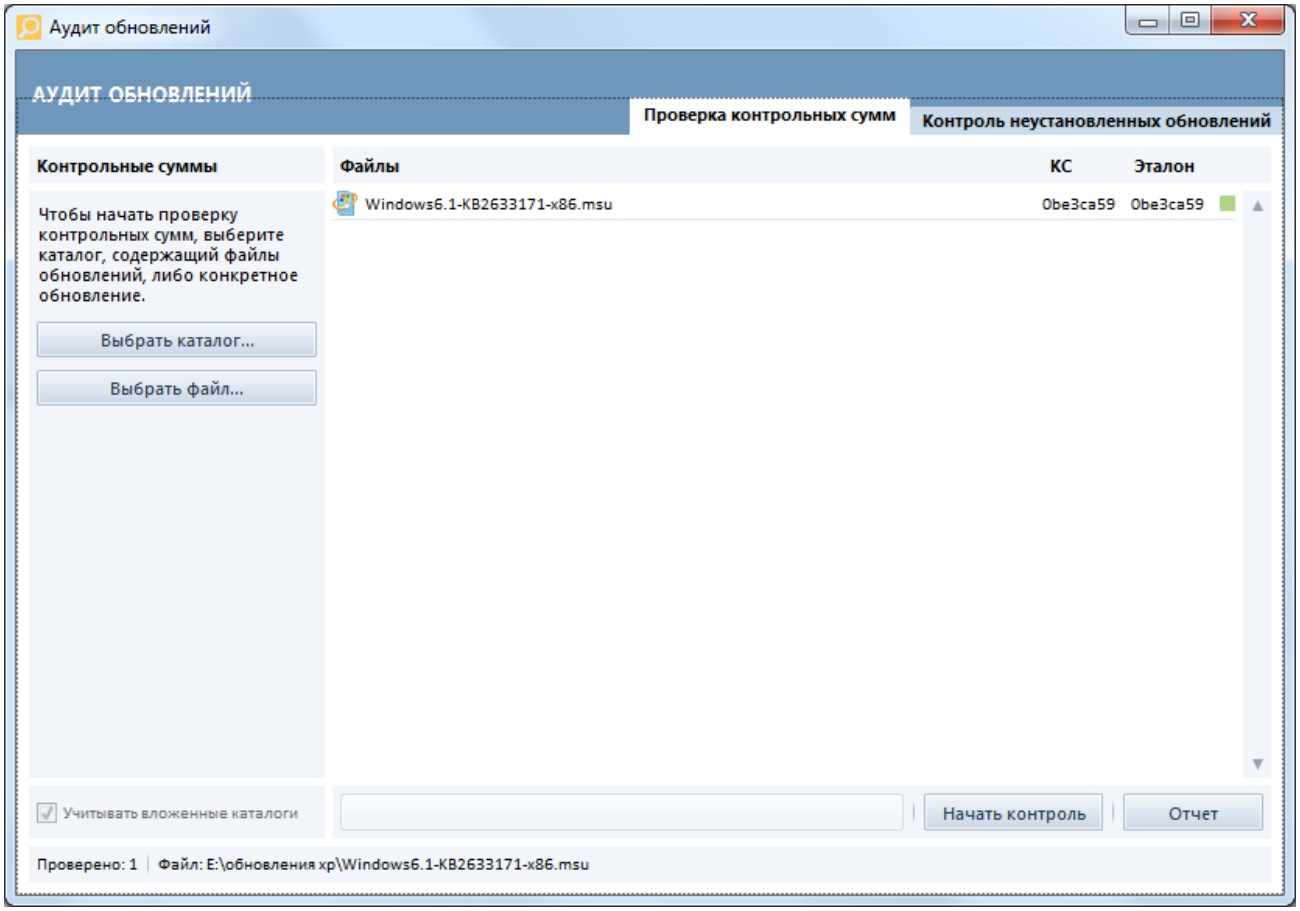


Рисунок 3.3 – Контроль сказанного файла сертифицированного обновления

В режимах «Контроль неустановленных обновлений» и «Проверка контрольных сумм» можно сформировать соответствующие отчеты путем нажатия на кнопку «Отчет» (см. рисунки 3.4 и 3.5).

АУДИТ ОБНОВЛЕНИЙ

ОТЧЕТ

15.08.2012 17:57	Windows 7 Максимальная ALTX-UZDEMIR\sau

Требуется установка обновлений

Windows 7: сертифицированные обновления, обязательные к установке

Требуется установка обновлений

Название	Имя файла	Описание	Продукты
Пакет обновления 1 (SP1) для Windows 7 (KB976932)	windows6.1-KB976932-X86.exe	Пакет обновления 1 (SP1) для Windows 7 помогает сохранять максимальный уровень поддержки настольных компьютеров и серверов	Microsoft Windows 7;
		Ссылки	
		windows6.1-KB976932-X86.exe	
		KB976932	
Обновление для системы безопасности Windows 7 (KB2633171)	Windows6.1-KB2633171-x86.msu	В системе безопасности обнаружена проблема, позволяющая локальному злоумышленнику, который прошел проверку подлинности, нарушить безопасность компьютера и получить возможность управления им.	Microsoft Windows 7;
		Ссылки	
		Windows6.1-KB2633171-x86.msu	
		KB2633171	
		MS11-098	
		CVE-2011-2018	
		CVE-2011-2018	

Рисунок 3.4 - Отчет о контроле сертифицированных обновлений

АУДИТ ОБНОВЛЕНИЙ / ПРОВЕРКА КС

ОТЧЕТ

15.08.2012 17:58	Windows 7 Максимальная ALTX-UZDEMIR\sau
Базовый каталог:	E:\обновления xp

Сертифицированные обновления

Файл	Контрольная сумма	Эталон
Windows6.1-KB2633171-x86.msu	0be3ca59	0be3ca59
		Всего файлов: 1

Рисунок 3.5- Отчет по проверке файлов обновлений

Функция доступна по лицензии на программу (базовой лицензии).

3.3 Фиксация и контроль встроенных СЗИ

Для выполнения указанной функции необходимо нажать кнопку в центральной части окна программы.

Программа «Seven_Check» позволяет производить фиксацию (и последующий контроль) исполняемых файлов или библиотек, отвечающих за реализацию механизмов СЗИ. Таким же образом могут быть проверены файлы системных каталогов Windows или установочных каталогов программ, работающих под управлением контролируемой операционной системы Microsoft Windows 7. Контроль зафиксированного состояния производится методом контрольного суммирования по уровню 3, согласно ГОСТ 28147-89 с контролем добавленных и удаленных файлов с использованием сертифицированной ФСТЭК «ФИКС-библиотеки» v. 1.0.

Фиксация файлов встроенных СЗИ

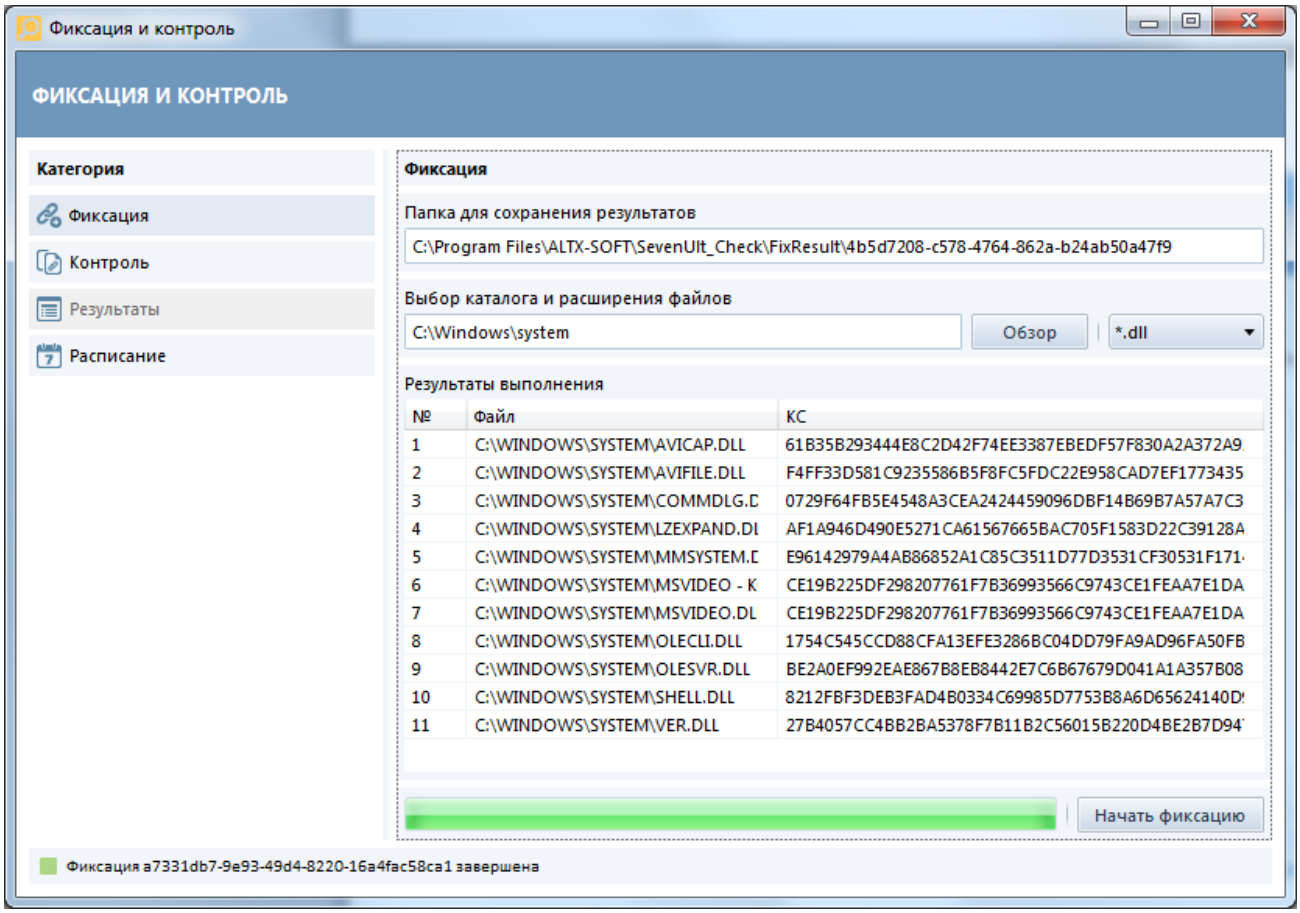


Рисунок 3.6 – Окно программы в режиме «Фиксация»

Для фиксации файлов с исполняемым кодом в левой части окне реализации функции нажать кнопку «Фиксация» и задать следующие данные (см. рисунок 3.6):

- папка, где будет формироваться файл отчета по контролю. По умолчанию – это папка «FixResults»;
- тип фиксируемых файлов (*.dll, *.exe, *.inf);
- папка расположения фиксируемых файлов.

После нажатия кнопки «Начать фиксацию» на экран будут представлены результаты проведенной фиксации – список зафиксированных файлов (см. рисунок 3.6).

Контроль файлов встроенных СЗИ

Контроль файлов может проводиться в ручном режиме или по заданию (в том числе и при загрузке ОС).

Важно: *Использование контроля файлов с исполняемым кодом при загрузке системы необходимо для обеспечения требований РД ФСТЭК «АС защита от НСД к информации. Классификация АС и требования к защите информации», приказа ФСТЭК № 58 «Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных», а именно обеспечение требования «…целостности программных средств при загрузке системы по наличию имен (идентификаторов) компонентов средств защиты информации» («…проверки по контрольным суммам компонентов средств защиты информации» в трактовке требования Приказа № 58 для многопользовательского режима работы).*

Для контроля зафиксированных файлов с исполняемым кодом **в ручном режиме** необходимо в левой части окна реализации функции нажать кнопку «Контроль». В представленном окне (см. рисунок 3.7) будут списком обозначены отчеты по фиксации, хранящиеся в папке FixResults рабочего каталога с программой. Предоставляется возможность выбрать один из отчетов по фиксации и нажать кнопку «Начать контроль». Будет проведен расчет текущих значений контрольных сумм файлов с исполняемым кодом в папке фиксации.

Для контроля зафиксированных файлов с исполняемым кодом **по заданию** необходимо в левой части окна реализации функции нажать кнопку «Расписание». На экран будет представлено окно, изображенное на рис. 3.8.

В данном окне пользователь может создать задачу планировщика Windows, состоящую в автоматизированном контроле выбранного результата фиксации файлов с исполняемым кодом. В данном окне пользователь может установить приоритет этого задания и выбрать необходимый результат фиксации. Программа Чек создает единственное задание планировщика задач, поэтому каждая последующая задача «затирает» предыдущую. При нажатии кнопки «Удалить задачу» - задача контроля файлов с исполняемым кодом удаляется из планировщика задач.

Пользователь имеет возможность просмотреть сформированное задание планировщика заданий при выборе ярлыка «Планировщик заданий» Панели управления Windows (задание Seven_Check Fix Control). В случае необходимости можно изменить параметры выполнения задания, например, поставить его на периодический контроль (см. рисунок 3.9). Результаты выполнения задания можно просмотреть в общем окне списка результатов (кнопка «Результаты», см. «Просмотр результатов» ниже в настоящем п.п.).

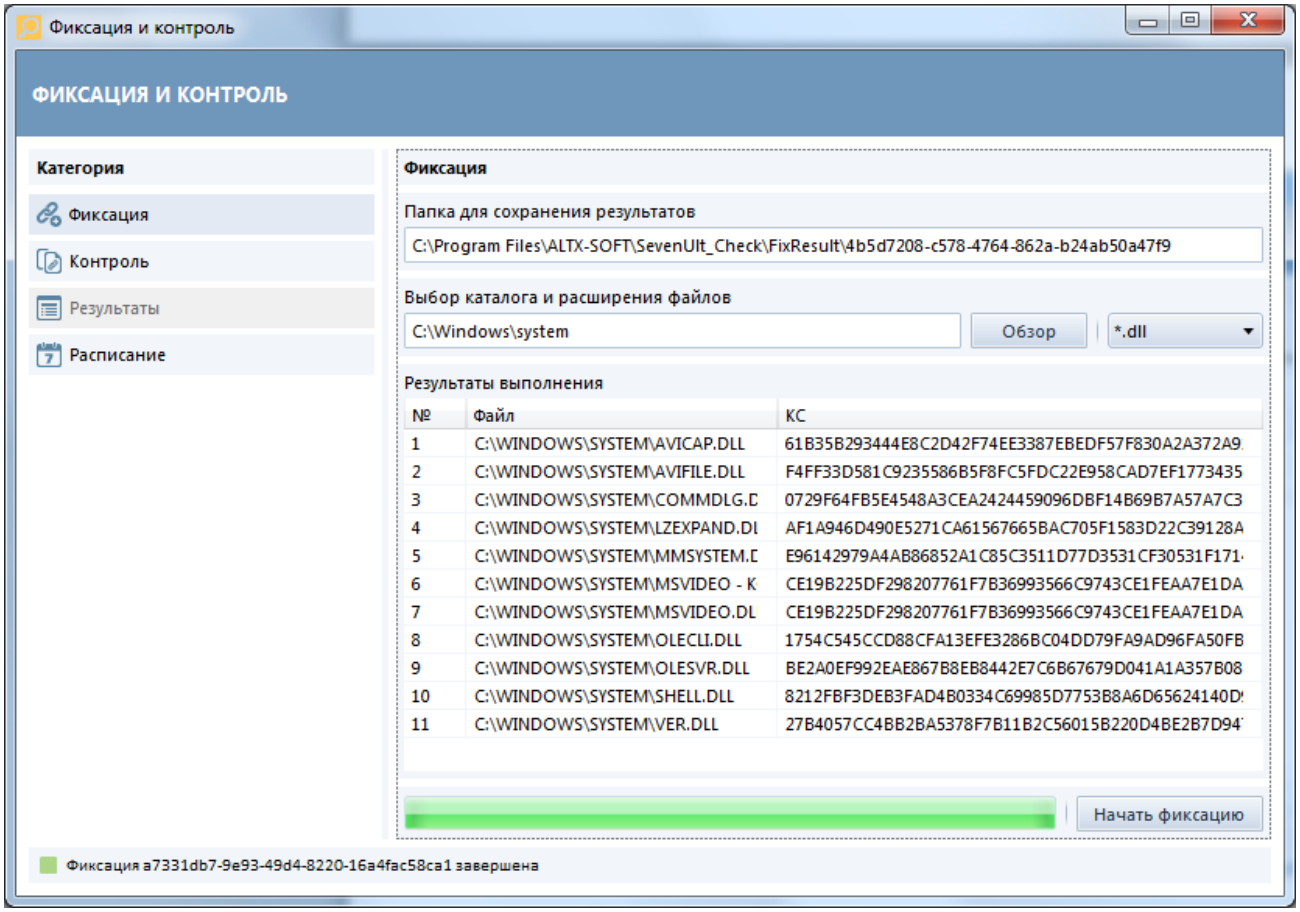


Рисунок 3.7 – Окно программы в режиме «Контроль»

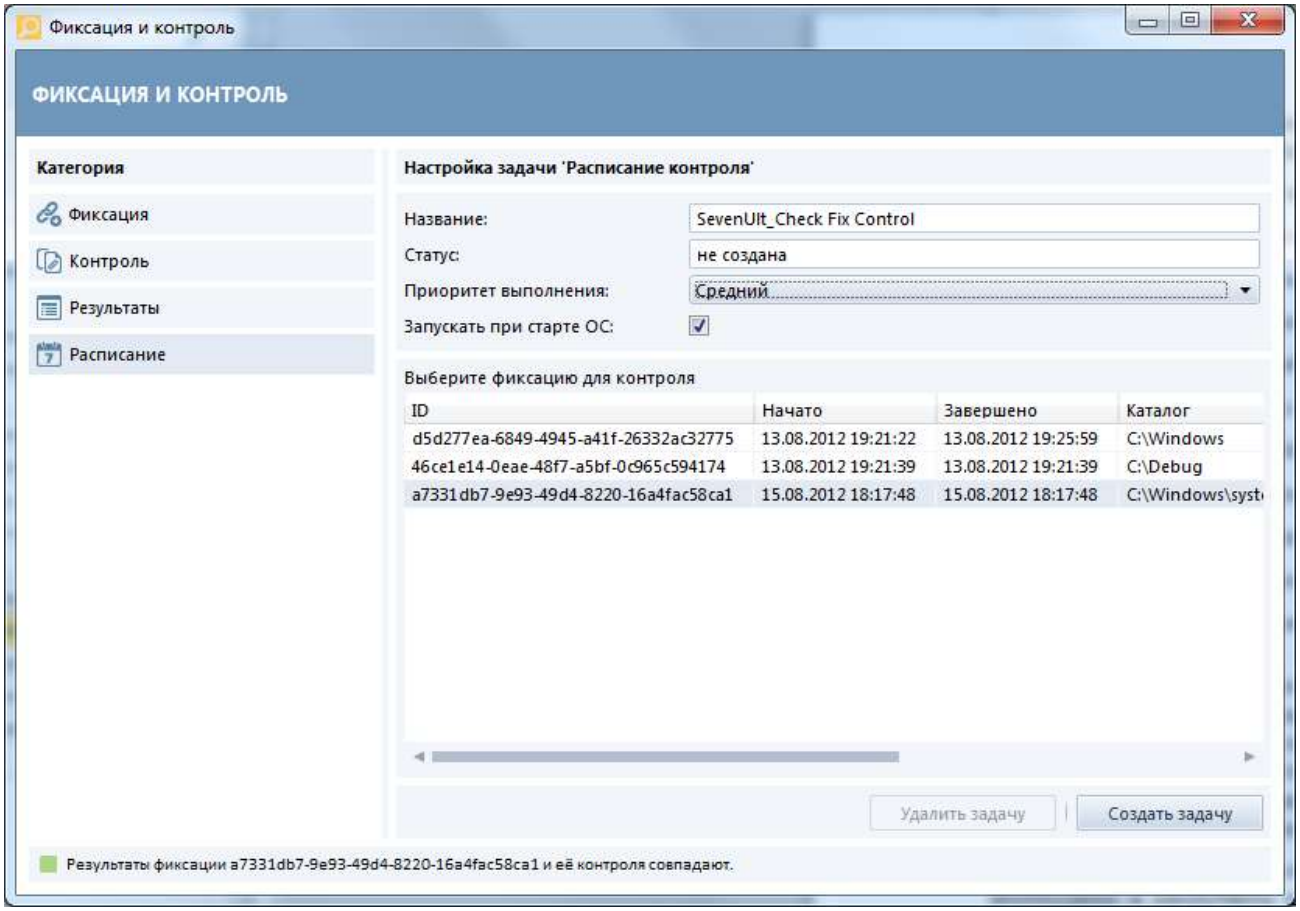


Рисунок 3.8 – Формирование задания на запуск контроля

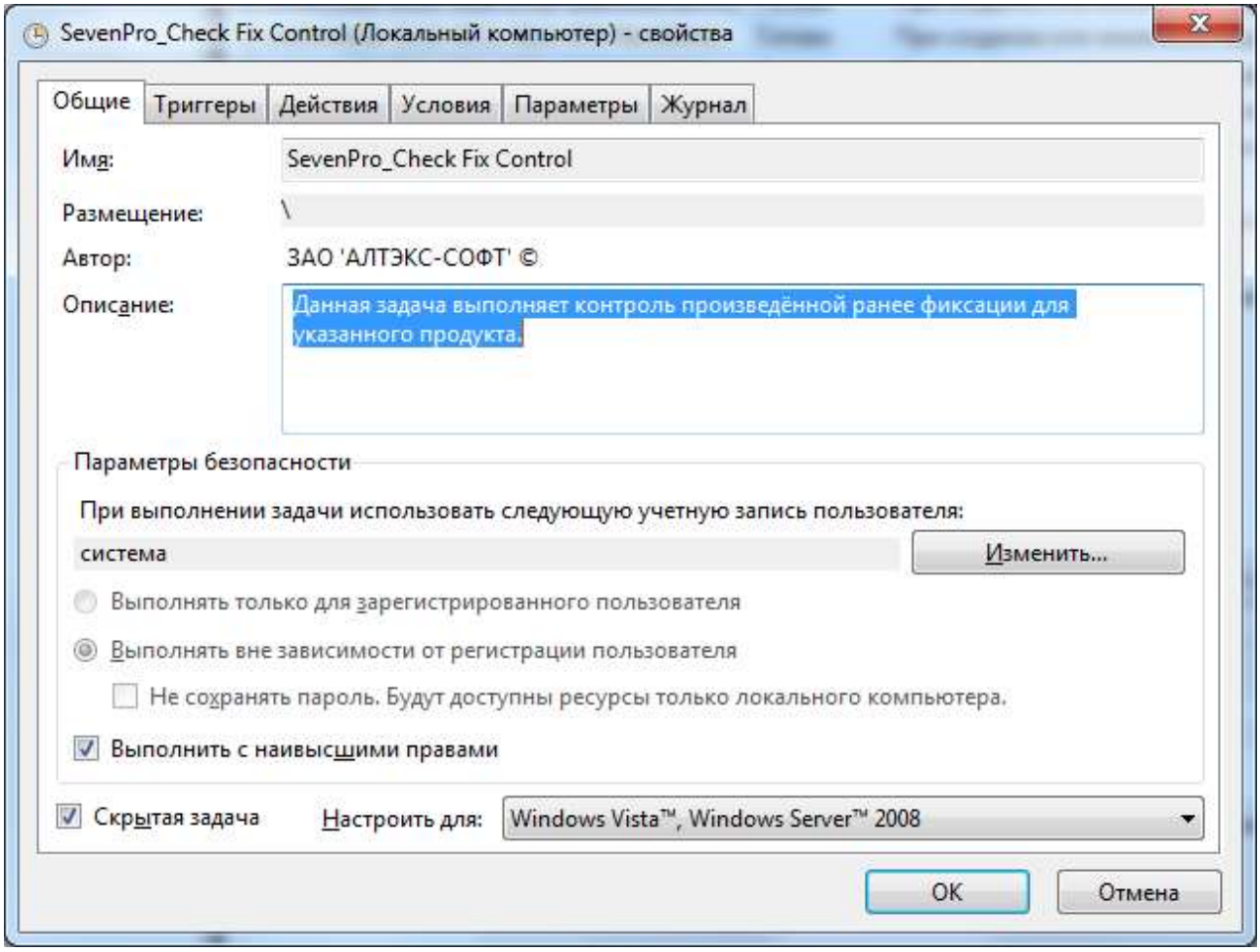


Рисунок 3.9 – Редактирование параметров задания планировщика задач для проведения контроля файлов при запуске системы

Просмотр результатов

Для просмотра результатов фиксации необходимо в левой части окна реализации функции нажать кнопку «Результаты». В окне, представленном на рисунке 3.10 необходимо выбрать результат фиксации и нажать кнопку «Далее». На следующем шаге контроля (см. рисунок 3.11) показываются все операции контроля, проведенные по выбранной фиксации с показом результата операции: контроль завершен **успешно** – означает, что в выбранных папках присутствуют все контролируемые файлы с исполняемым кодом, их контрольные суммы соответствуют эталонным, отсутствуют добавленные файлы с исполняемым кодом; **не успешно** – если обнаружены какие либо коллизии при контроле. В случае выбора неуспешной операции контроля и нажатия кнопки «Отчет» в представленном на рисунке 3.12 отчете можно просмотреть списки измененных, отсутствующих и добавленных файлов с исполняемым кодом.

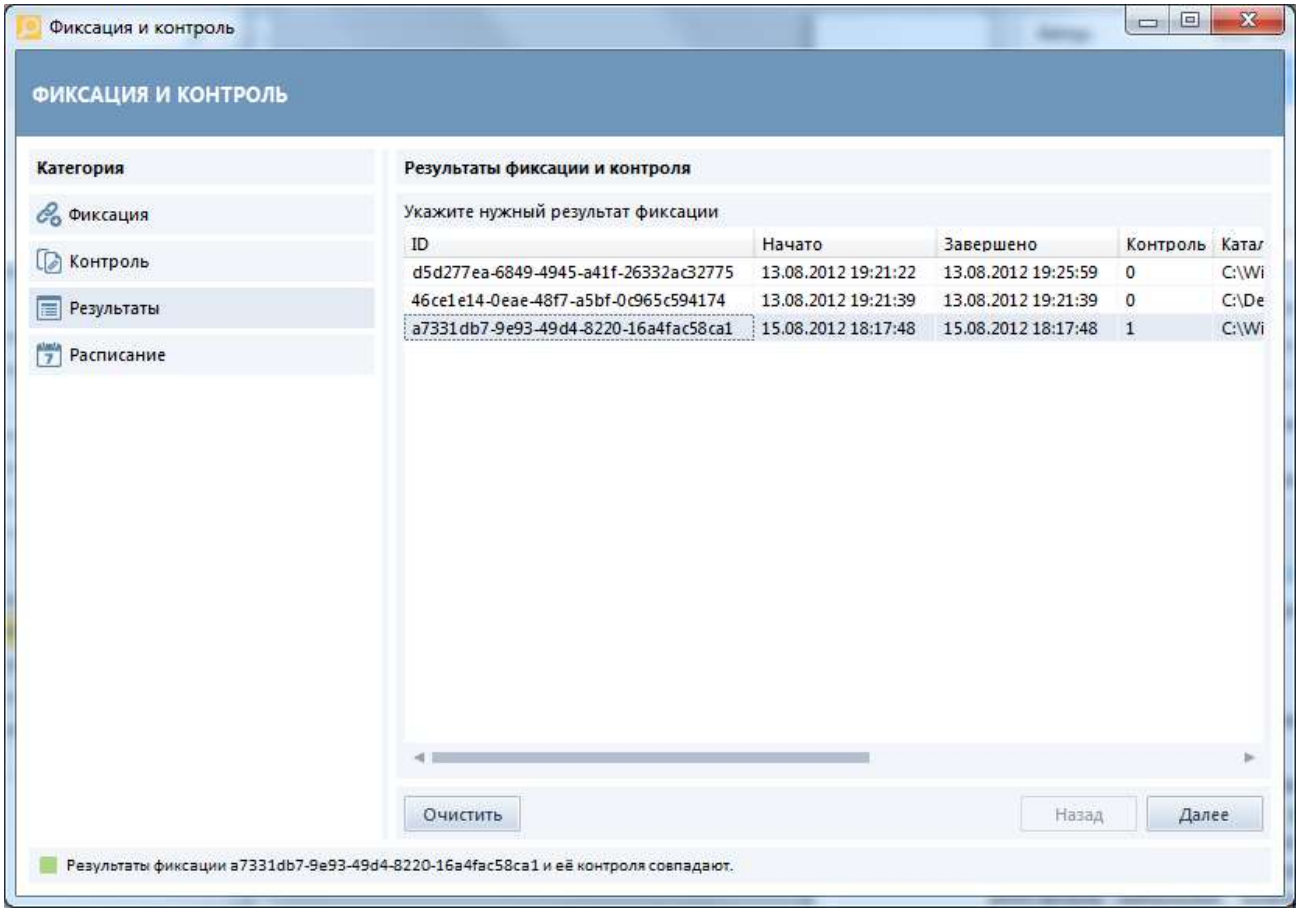


Рисунок 3.10 – Выбор результата фиксации

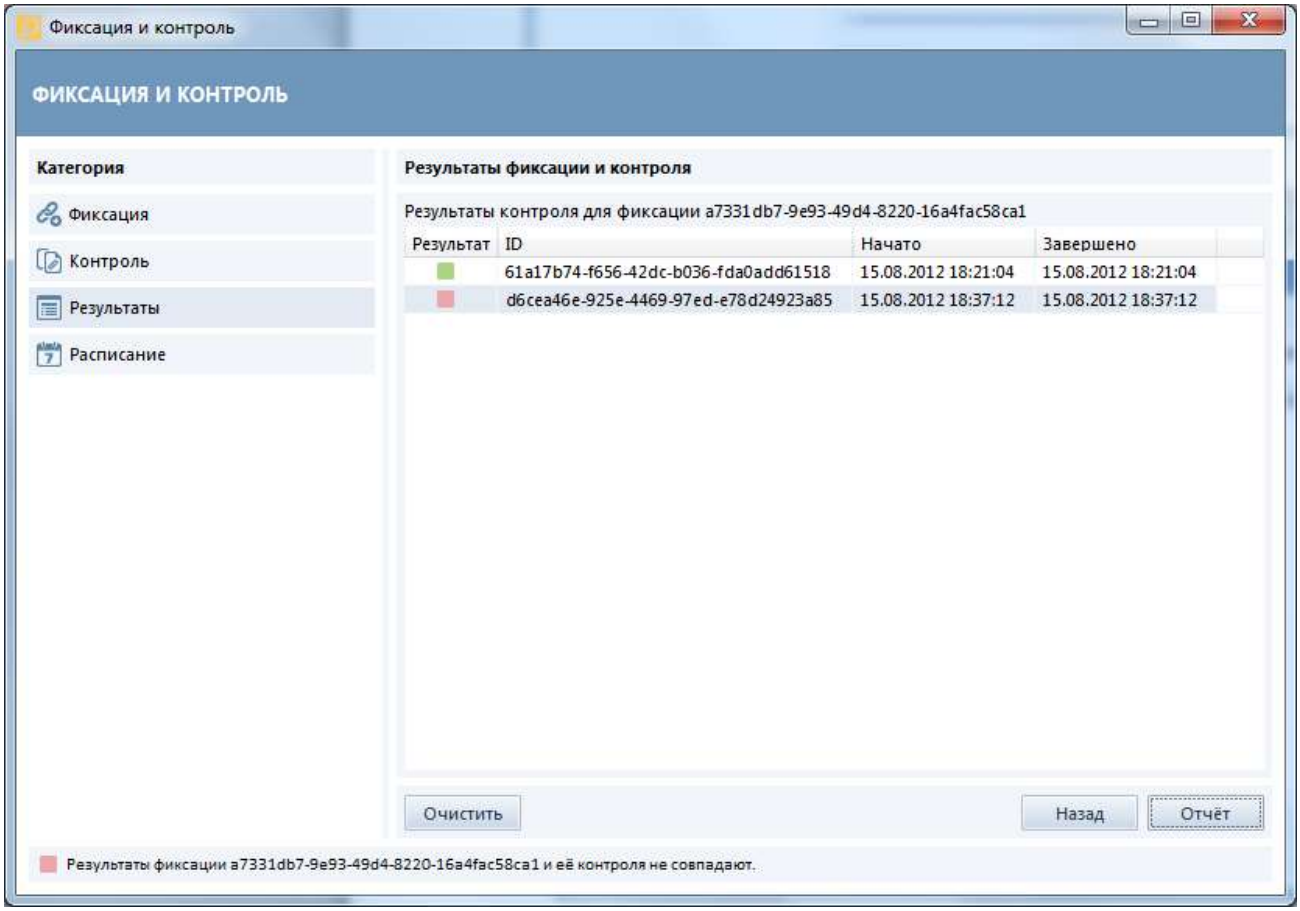
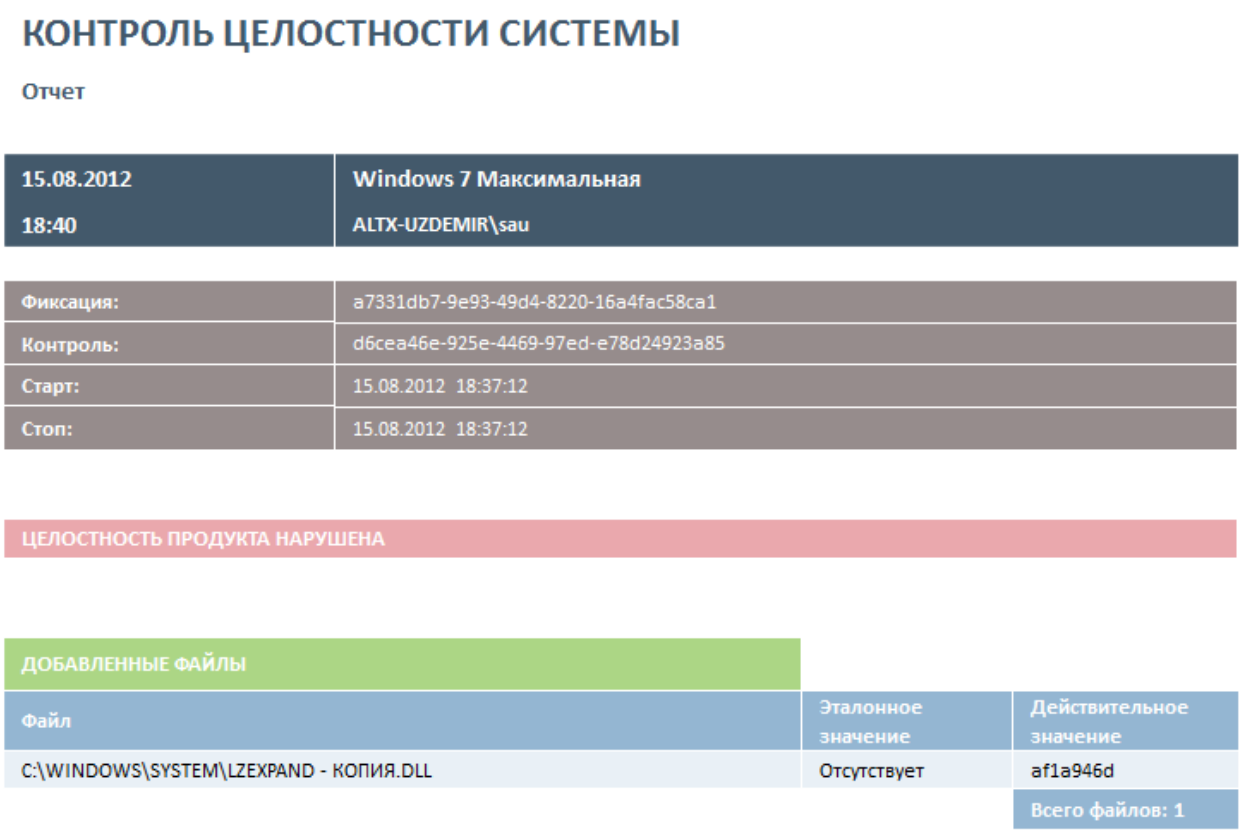


Рисунок 3.11 – Результаты контроля выбранной фиксации



КОНТРОЛЬ ЦЕЛОСТНОСТИ СИСТЕМЫ

Отчет

15.08.2012 18:40	Windows 7 Максимальная ALTX-UZDEMIR\sau

Фиксация:	a7331db7-9e93-49d4-8220-16a4fac58ca1
Контроль:	d6cea46e-925e-4469-97ed-e78d24923a85
Старт:	15.08.2012 18:37:12
Стоп:	15.08.2012 18:37:12

ЦЕЛОСТНОСТЬ ПРОДУКТА НАРУШЕНА

ДОБАВЛЕННЫЕ ФАЙЛЫ

Файл	Эталонное значение	Действительное значение
C:\WINDOWS\SYSTEM\LZEXPAND - КОПИЯ.DLL	Отсутствует	af1a946d
		Всего файлов: 1

Рисунок 3.12 – Отчет о контроле целостности СЗИ

Функция доступна по лицензии на программу (базовой лицензии).

3.4 Установка значений параметров безопасности на сертифицированные конфигурации

Для выполнения указанной функции необходимо нажать кнопку в центральной части окна программы.

Важно: Перед работой с параметрами безопасности необходимо заменить файл настроек параметров безопасности, путем выбора пункта меню «Меню\Применить конфигуратор». В результате данного действия будет замен файл <%System root%>\inf\sceregvl.inf.

С использованием программы «Seven_Check» можно произвести следующие операции по работе с сертифицированными конфигурациями безопасности и общим списком параметров безопасности:

- поиск параметра безопасности по названию;
- редактирование значений параметров безопасности;
- сохранение конфигурации параметров безопасности в файл настроек;
- загрузка и применение значений параметров безопасности из выбранного файла настроек;
- применение конфигурации параметров безопасности «Корпоративный клиент Windows 7»;

- применение конфигурации параметров безопасности «Безопасная среда Windows 7»;
- формирование и сохранение в формат html отчета о соответствии настроек безопасности конфигурациям «Корпоративный клиент Windows 7» или «Безопасная среда Windows 7».

Поиск параметра безопасности по названию

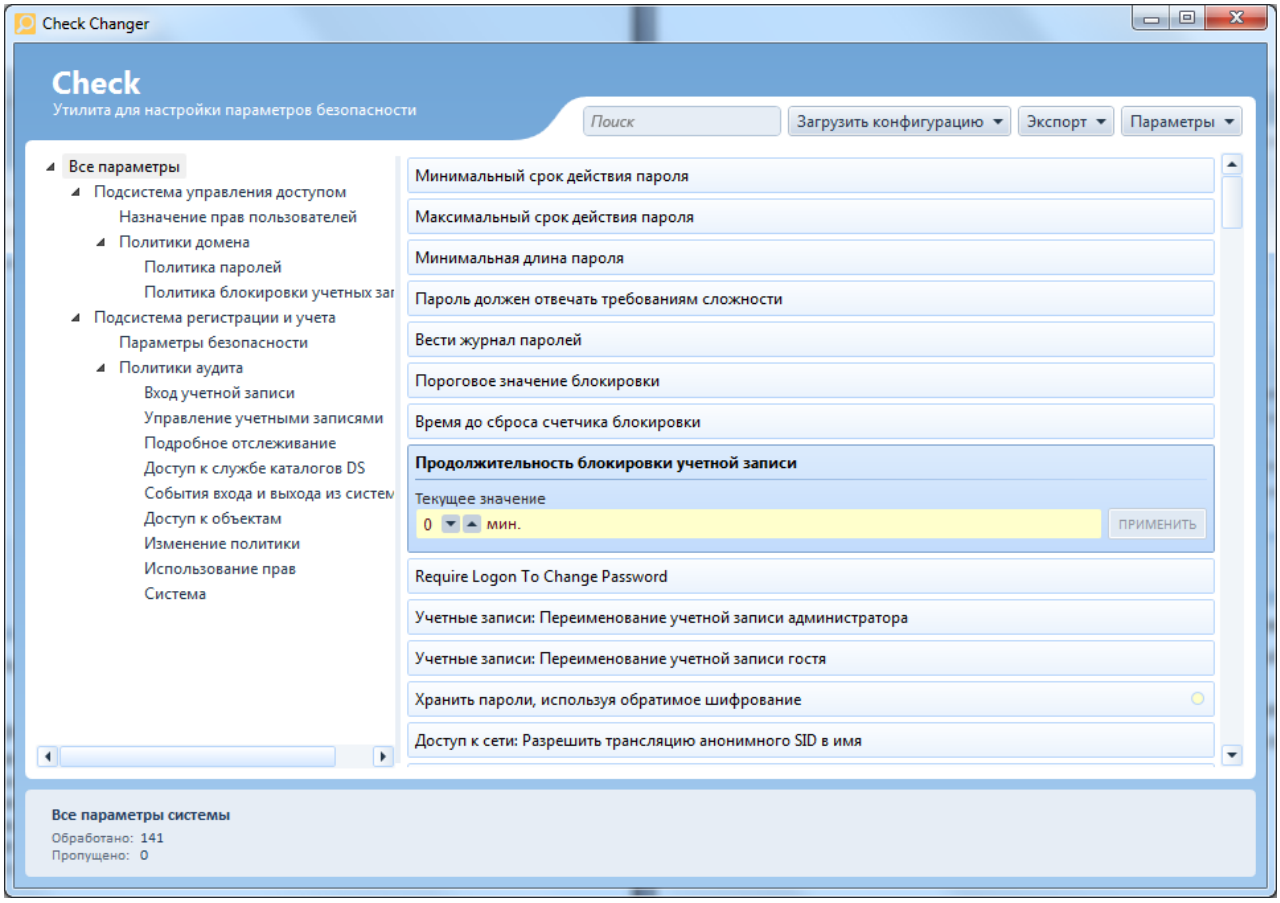


Рисунок 3.13 – Интерфейс программы по работе со значениями параметров безопасности

Поиск параметра по значению происходит при наборе соответствующей текстовой строки в поле «Поиск».

Примечание: 1) Несертифицированные (не заявленные в Задании по безопасности) параметры показаны в списке с желтой точкой (см. параметр «Хранить пароли, используя обратимое шифрование» на рисунке 3.14).

2) Описание отдельных параметров безопасности представлено в разделе 2 настоящего документа. Структур дерева параметров в программе «Seven_Check» соответствует структуре подпунктов раздела 2 настоящего документа.

3) Для загрузки текущих значений параметров безопасности из другого режима работы программы необходимо выбрать из ниспадающего меню «Загрузить конфигурацию» подпункт «Текущие значения параметров безопасности». В данном списке не отображаются параметры с неопределенными значениями.

4) Для отображения дерева всех доступных к редактированию параметров безопасности необходимо выбрать из ниспадающего меню «Загрузить конфигурацию» подпункт «Все доступные параметры системы».

Редактирование значений параметров безопасности

Для редактирования значения параметра безопасности необходимо его выбрать щелчком левой клавиши мыши, ввести необходимое значение и нажать кнопку «Применить».

Для редактирования числовых параметров доступно уменьшение и увеличение текущего значения на единицу и ручной ввод. Значения текстовых параметров вводятся в ручную. Для параметров, принимающих определенные значения – указанные значения оформляются в виде ниспадающего списка.

Сохранение конфигурации параметров безопасности в файл настроек

Для сохранения конфигурации параметров безопасности в файл настроек необходимо выбрать из ниспадающего меню «Экспорт» пункт «Сохранить текущую конфигурацию». Пользователю будет предоставлена возможность указания пути для сохранения *.inf файла с настройками значений параметров безопасности текущей конфигурации.

Данный файл в может быть использован для распространения сохраненных значений параметров безопасности на другие PC как с использованием программы Seven_Check так и с использованием стандартного инструментария Windows по работе с параметрами GPO (в том числе и применение их в домене)

Применение конфигурации параметров безопасности «Корпоративный клиент Windows 7»

ВАЖНО! Для успешного применения конфигурации «Корпоративный клиент Windows 7» при установках по умолчанию перед первым применением конфигурации необходимо: для параметра «Учетные записи: переименовании учетной записи «Администратор» и «Учетные записи: переименовании учетной записи «Гость» в поле «текущее значение» ввести значение, отличное от эталонного и нажать кнопку «Применить».

При этом указанные учетные записи на компьютере будут переименованы в значения, указанные в поле «текущее значение» и после применения конфигурации будут отключены.

Для реализации этой функции необходимо выбрать из ниспадающего меню «Загрузить конфигурацию» подпункт «Корпоративный клиент Windows 7». На экран будет представлено окно, показанное на рисунке 3.14.

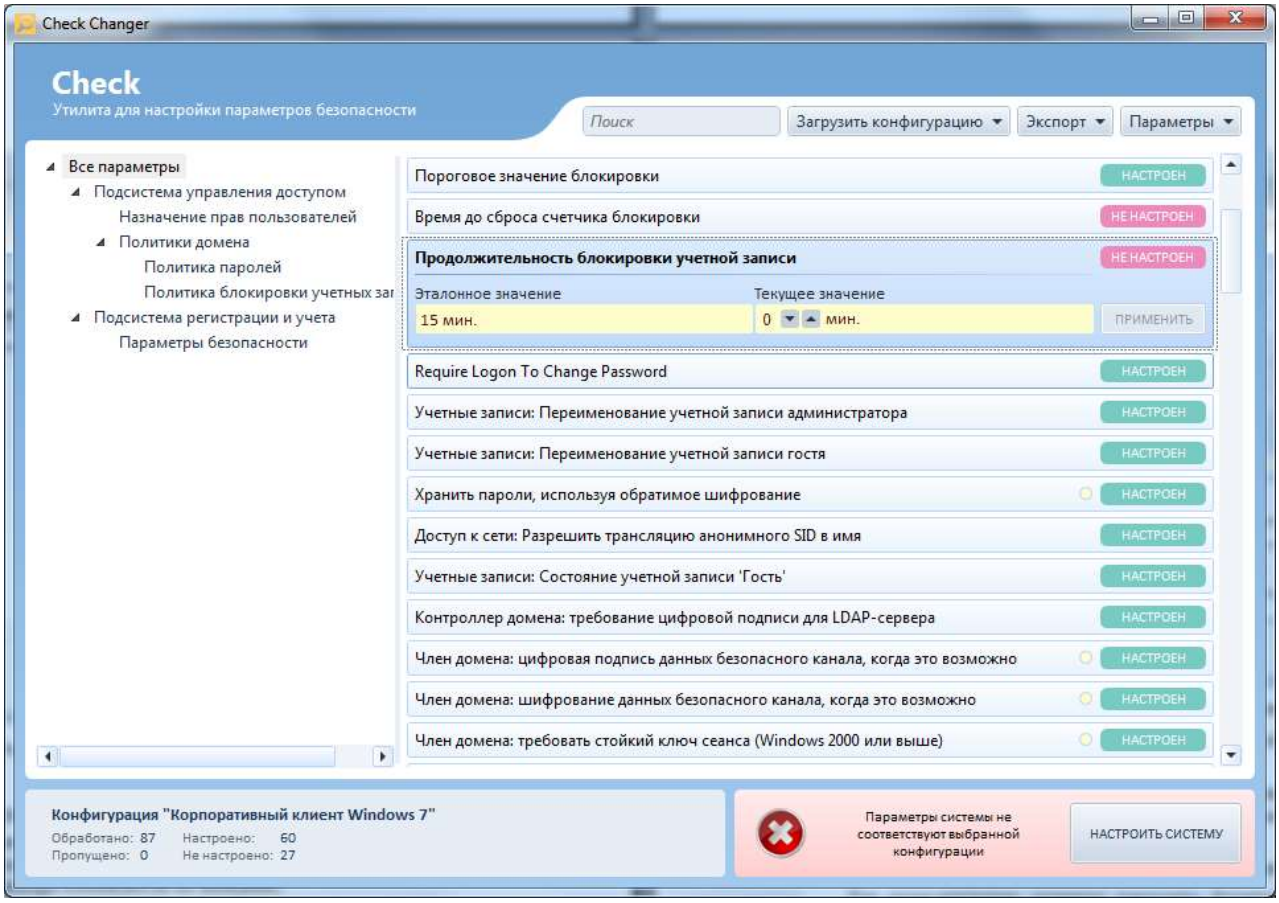


Рисунок 3.14– Окно программы «Seven_Check» при применении конфигурации «Корпоративный клиент Windows 7»

Каждый из параметров безопасности имеет эталонное значение согласно сертифицированной конфигурации и текущее значение конфигурации системы. В случае их равенства в правой части строки параметра располагается зеленая кнопка «Настроен» - параметр считается настроенным. В противном случае – параметр считается не настроенным и на этом месте располагается красная кнопка с надписью «Не настроен». В случает выбора из ниспадающего меню «Параметры» подпункта «Показывать только ненастроенные параметры» в списке параметров будут присутствовать только ненастроенные параметры безопасности.

В случае установки текущего значения равного эталонному вручную – кнопка «Не настроен» меняется на «Настроен».

Внизу в информационной панели присутствует следующая информация:

- общее количество параметров сертифицированной конфигурации;
- количество настроенных и ненастроенных параметров безопасности;
- информационное сообщение соответствуют ли настройки параметров безопасности системы в целом сертифицированной конфигурации.

При нажатии кнопки «Настроить систему» происходит установка эталонных значения для всех ненастроенных параметров безопасности.

Примечание: 1) Параметры аудита из подраздела 2.3 настоящего руководства в интерфейсе программы не присутствуют, однако при нажатии кнопки «Настроить систему» - происходит установка эталонных значения указанных параметров безопасности.

2) В дереве параметров программы сертифицированных конфигураций отсутствуют параметры со значением «не определено».

Применение конфигурации параметров безопасности «Безопасная среда Windows 7»

ВАЖНО! Для успешного применения конфигурации «Безопасная среда Windows 7» при установках по умолчанию перед первым применением конфигурации необходимо: для параметра «Учетные записи: переименовании учетной записи «Администратор» и «Учетные записи: переименовании учетной записи «Гость» в поле «текущее значение» ввести значение, отличное от эталонного и нажать кнопку «Применить».

При этом указанные учетные записи на компьютере будут переименованы в значения, указанные в поле «текущее значение» и после применения конфигурации будут отключены.

Выполнение этой функции аналогично выполнению функции Применение конфигурации параметров безопасности «Корпоративный клиент Windows 7».

Формирование и сохранение в формат html отчета о соответствии настроек безопасности конфигурациям «Корпоративный клиент Windows 7» или «Безопасная среда Windows 7»

Для выполнения данной функции необходимо из ниспадающего меню «Экспорт» выбрать подпункт «Создать протокол настроек». На экран будет предложена выбрать папку для сохранения файла отчета в формате html. Примерный вид этого отчета представлен на рисунке 3.15.

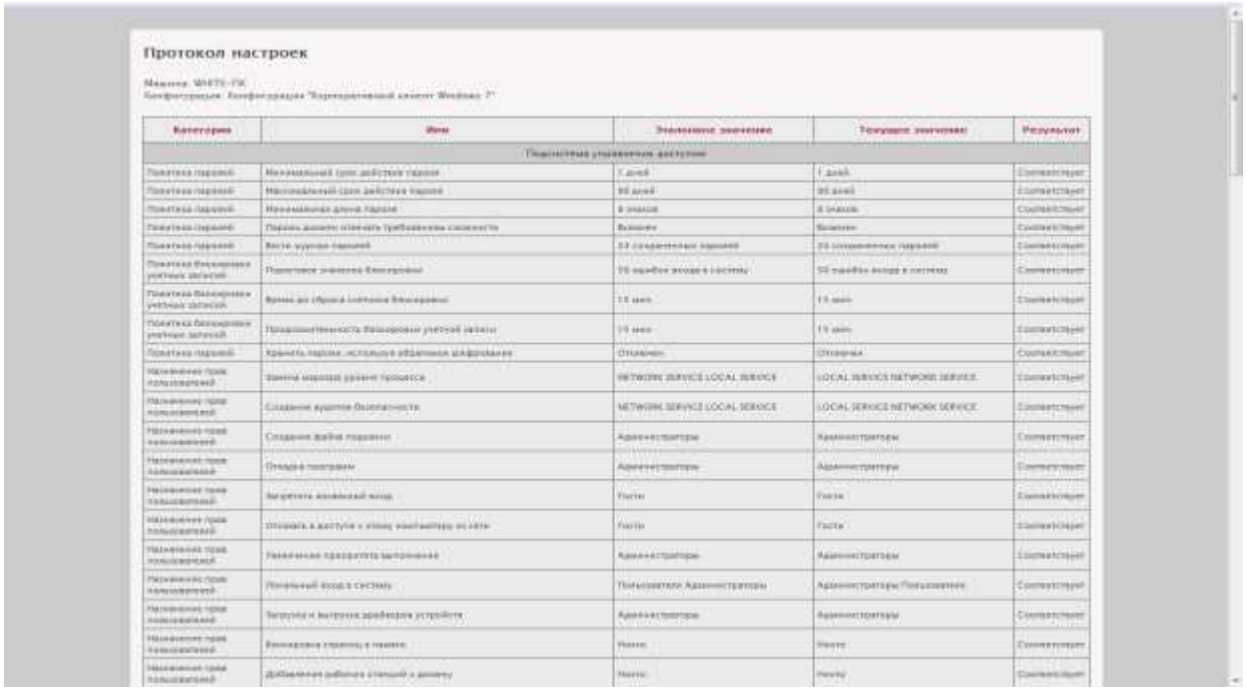


Рисунок 3.15 – Пример отчета о соответствии настроек безопасности конфигурациям «Корпоративный клиент Windows 7»/«Безопасная среда Windows 7»

Функция доступна по лицензии на программу (базовой лицензии).

4 Функции дополнительного модуля аудита уязвимостей и конфигураций безопасности

4.1 Аудит обновлений

Для выполнения указанной функции необходимо нажать кнопку в центральной части окна программы.

На экран будет показана окно, аналогичное представленному на рисунке 3.2. В нём, кроме ленты сертифицированных обновлений, будут показаны ленты обновлений,

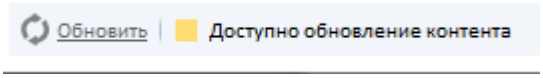
доступные по лицензии на дополнительный модуль аудита уязвимостей и конфигураций безопасности. Ленты привязаны к определенным программным продуктам.

Работа с лентами обновлений аналогична работе с лентой сертифицированных обновлений, описанной в п. 3.2 настоящего Руководства.

Для выбора всех лент обновлений для аудита следует выбрать флажок «Выбрать все» и нажать кнопку «Провести сканирование».

4.2 Аудит уязвимостей

Для выполнения указанной функции необходимо нажать кнопку в центральной части окна программы.

На экран будет представлено окно, аналогичное показанному на рисунке 4.1. В нём будут показаны ленты уязвимостей, доступные по лицензии на дополнительный модуль аудита уязвимостей и конфигураций безопасности. Ленты привязаны к определенным программным продуктам, т.е сканирование ленты уязвимостей означает проверку определенного программного продукта на наличие известных на данный момент уязвимостей. Контроль производится на основании регулярно обновляемого контента, получаемого с «облачного» сервиса (сервера) программы. Для получения актуальных данных следует обновлять контент при появлении надписи 

в левом нижнем углу программы в online режиме работы, и не реже одного раза в месяц при работе в offline режиме. Подробнее о режимах работы программы в п. 2.2 настоящего Руководства.

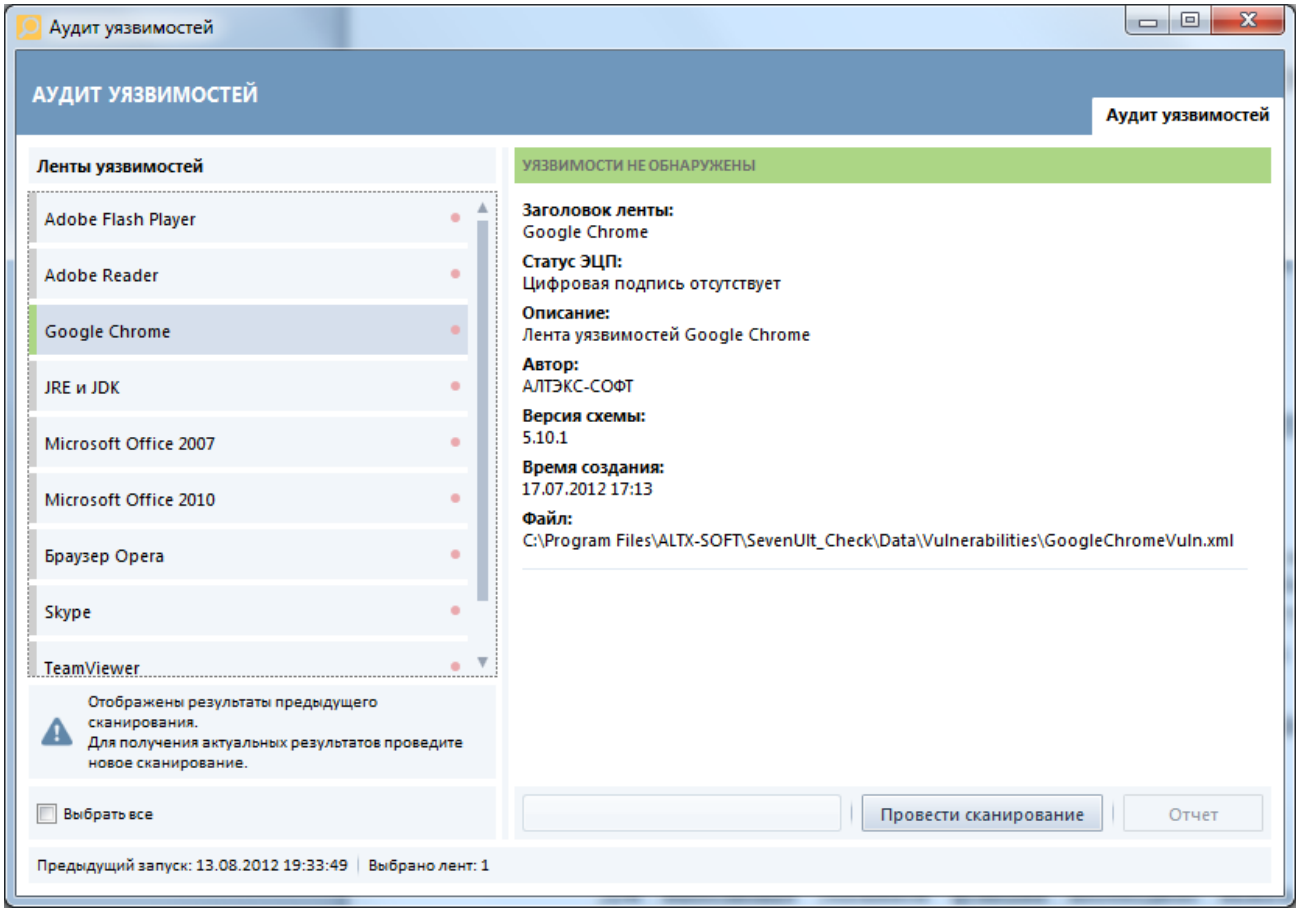


Рисунок 4.1 – Ленты уязвимостей функции «Аудит уязвимостей»

Для того чтобы проверить программный продукт (или несколько программных продуктов) из списка на наличие уязвимостей следует выбрать ленту уязвимостей с его наименованием в левой части окна реализации функции (используя в том числе множественное выделение клавишами Ctrl и Shift) или использовать флажок «Выбрать всё» и нажать кнопку «Провести сканирование».

В результате, для каждой из лент уязвимостей будет присвоен статус:

- «уязвимости не обнаружены» (отображается зелёным цветом). Показывается в том случае, если для продукта уязвимости не идентифицированы, или продукт на контролируемой ЭВМ не установлен вовсе;
- «требуется устранение уязвимости» (отображается красным цветом);
- «ошибка» (возникает, как правило, при повреждении контента программы, о чем необходимо сообщить в техническую поддержку программы), (отображается оранжевым цветом).

Устранение уязвимостей:

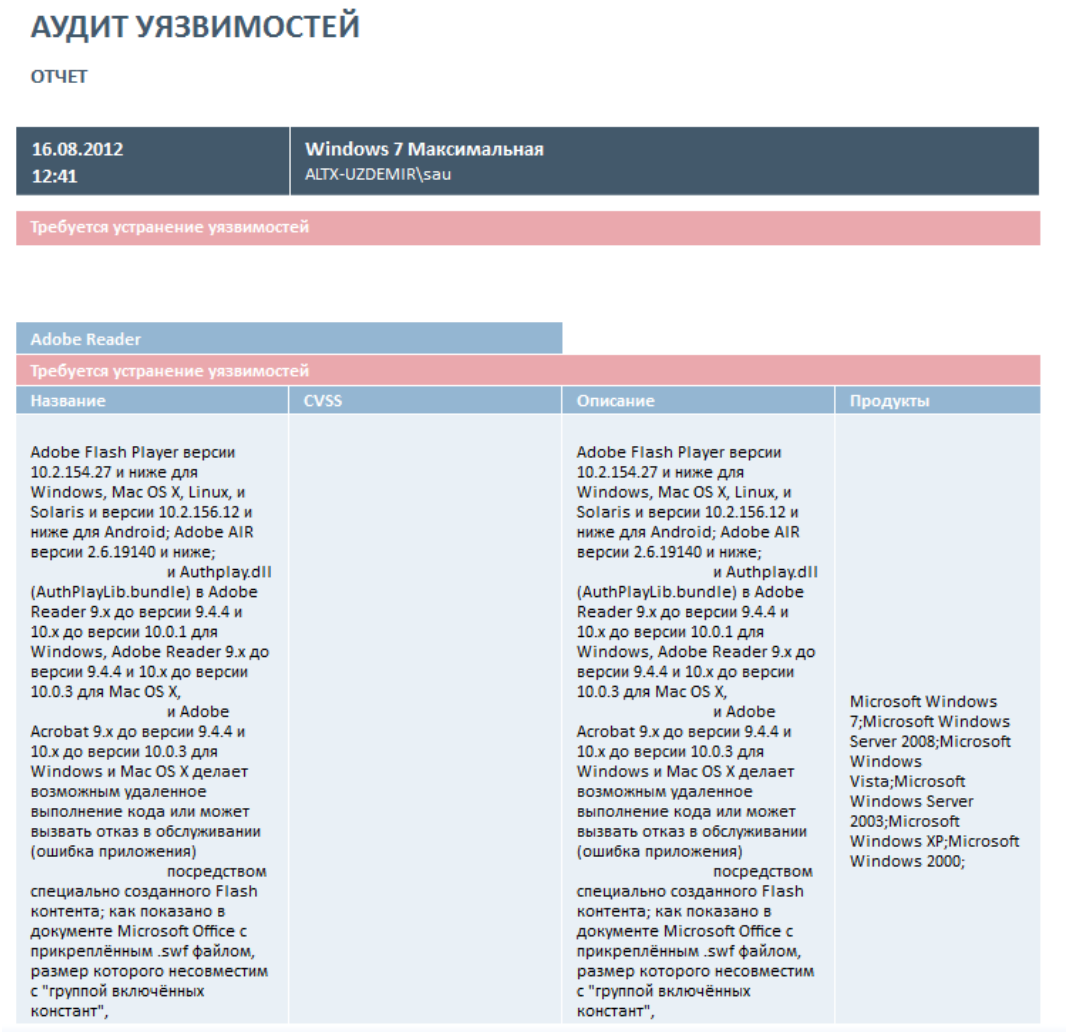
Для просмотра данных и устранения уязвимостей программа отображает описание уязвимостей со ссылкой на элемент Общий переченя уязвимостей и рисков (CVE®, Common vulnerabilities and exposures) в репозитории определений OVAL компании АЛТЭКС-СОФТ.

Устранение уязвимости, как правило, сводится к одному из следующих действий:

- установка новой версии контролируемой программы;
- установка обновления;
- установка валидного значения параметра безопасности.

Рисунок 4.2 – Описание уязвимости

Результаты проведенного контроля доступны в отчете (кнопка «Отчет»). Примерный вид отчета представлен на рисунке 4.3.



АУДИТ УЯЗВИМОСТЕЙ

ОТЧЕТ

16.08.2012 12:41	Windows 7 Максимальная ALTX-UZDEMIR\sau

Требуется устранение уязвимостей

Adobe Reader

Требуется устранение уязвимостей

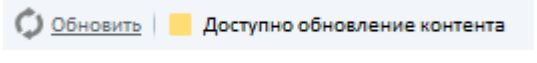
Название	CVSS	Описание	Продукты
Adobe Flash Player версии 10.2.154.27 и ниже для Windows, Mac OS X, Linux, и Solaris и версии 10.2.156.12 и ниже для Android; Adobe AIR версии 2.6.19140 и ниже; и Authplay.dll (AuthPlayLib.bundle) в Adobe Reader 9.x до версии 9.4.4 и 10.x до версии 10.0.1 для Windows, Adobe Reader 9.x до версии 9.4.4 и 10.x до версии 10.0.3 для Mac OS X, и Adobe Acrobat 9.x до версии 9.4.4 и 10.x до версии 10.0.3 для Windows и Mac OS X делает возможным удаленное выполнение кода или может вызвать отказ в обслуживании (ошибка приложения) посредством специально созданного Flash контента; как показано в документе Microsoft Office с прикреплённым .swf файлом, размер которого несовместим с "группой включённых констант",		Adobe Flash Player версии 10.2.154.27 и ниже для Windows, Mac OS X, Linux, и Solaris и версии 10.2.156.12 и ниже для Android; Adobe AIR версии 2.6.19140 и ниже; и Authplay.dll (AuthPlayLib.bundle) в Adobe Reader 9.x до версии 9.4.4 и 10.x до версии 10.0.1 для Windows, Adobe Reader 9.x до версии 9.4.4 и 10.x до версии 10.0.3 для Mac OS X, и Adobe Acrobat 9.x до версии 9.4.4 и 10.x до версии 10.0.3 для Windows и Mac OS X делает возможным удаленное выполнение кода или может вызвать отказ в обслуживании (ошибка приложения) посредством специально созданного Flash контента; как показано в документе Microsoft Office с прикреплённым .swf файлом, размер которого несовместим с "группой включённых констант",	Microsoft Windows 7;Microsoft Windows Server 2008;Microsoft Windows Vista;Microsoft Windows Server 2003;Microsoft Windows XP;Microsoft Windows 2000;

Рисунок 4.3 – Отчёт об уязвимостях

4.3 Аудит конфигураций

Для выполнения указанной функции необходимо нажать кнопку в центральной части окна программы.

На экран будет представлено окно, аналогичное показанному на рисунке 4.4. В нём при нажатии на кнопку «Загрузить конфигурацию» показаны доступные для контроля конфигурации. Конфигурации привязаны к определенным программным продуктам, т.е аудит конфигурации означает проверку параметров безопасности ОС, как среды выполнения указанного продукта, на соответствие эталонным значениям (диапазонам значений, указанных в конфигурации). Аудит производится на основании регулярно обновляемого контента, получаемого с «облачного» сервиса (сервера) программы. Для получения актуальных данных следует обновлять контент при появлении надписи



в левом нижнем углу программы в online режиме работы, и не реже одного раза в месяц при работе в offline режиме. Подробнее о режимах работы программы в п. 2.2 настоящего Руководства.

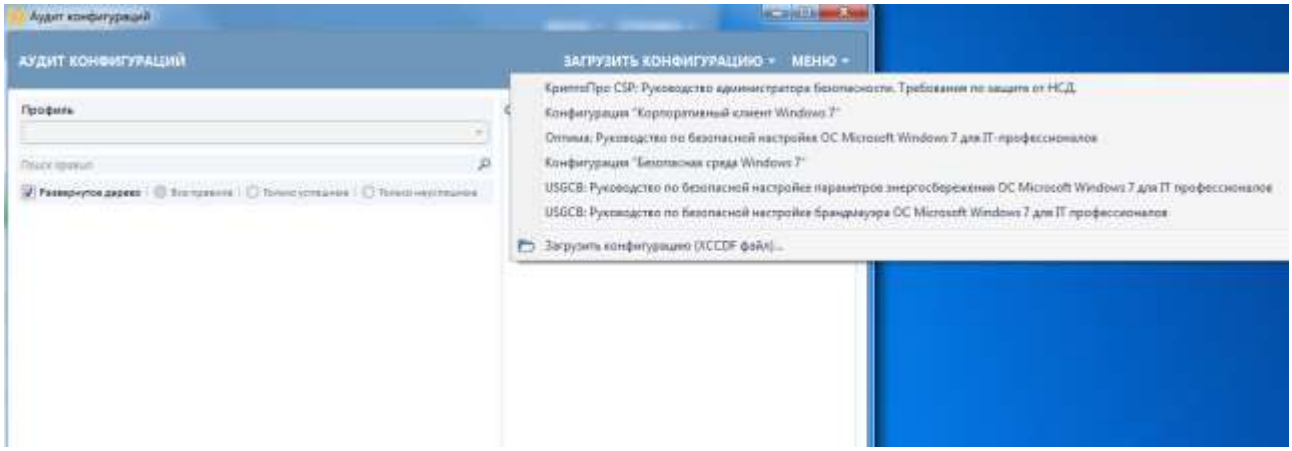


Рисунок 4.4 – Контролируемые конфигурации функции «Аудит конфигураций»

Для того, чтобы провести контроль необходимо выбрать одну из конфигураций. При этом в левой части окна будет показано «дерево» параметров (см. рисунок 4.5).

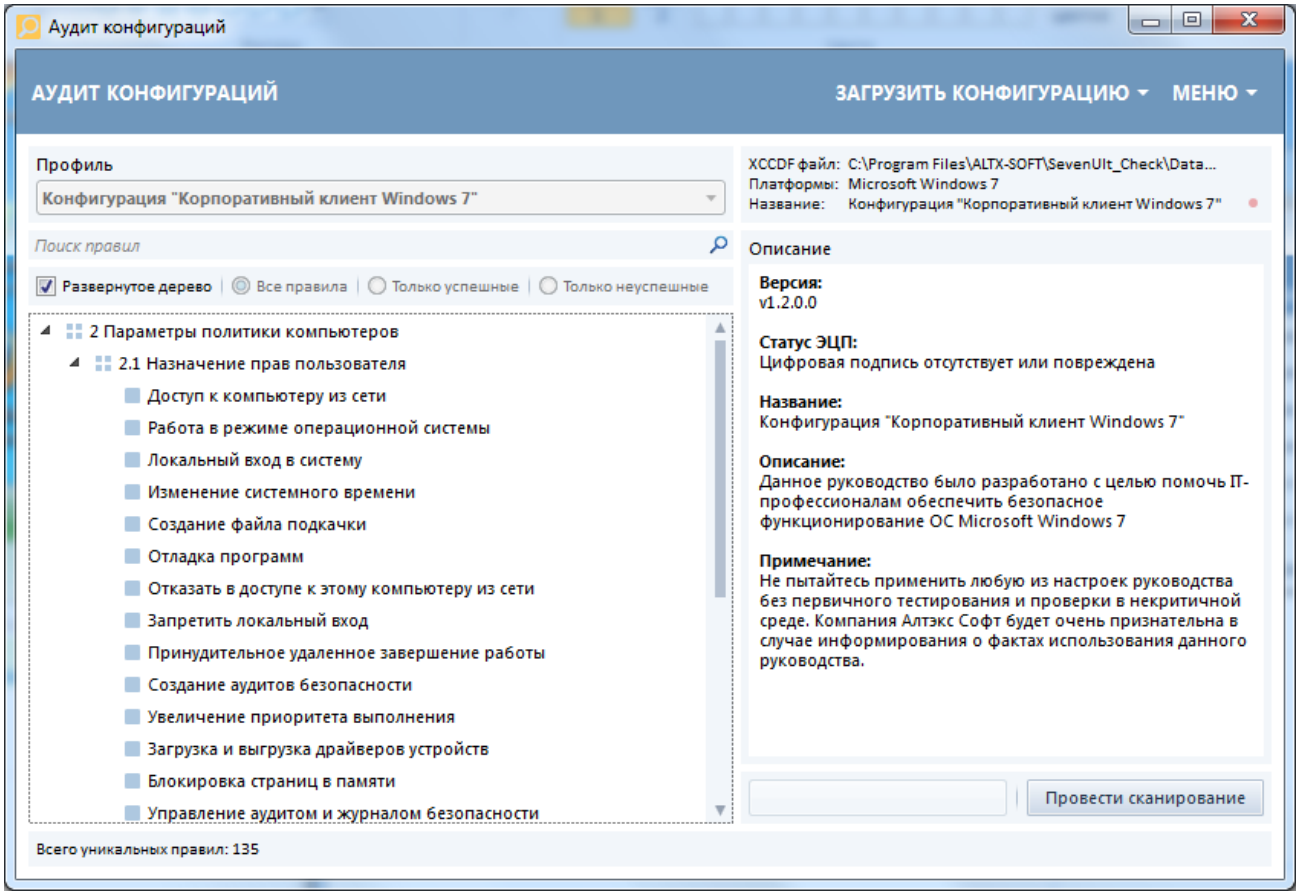
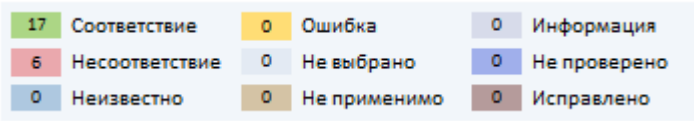


Рисунок 4.5 – Выбор конфигурации для аудита

Для проведения аудита соотвествия параметров безопасности требованиям конфигурации (значениям или диапазону значений параметров безопасности) необходимо нажать кнопку «Провести сканирование». Примерный вид результатов аудита представлен на рисунке 4.6.

Каждый из параметров конфигурации может иметь следующие статусы аудита:



Практическую значимость имеют следующие статусы:

1) Соответсвие. Значения параметра безопасности соответствует эталонному значению для конфигурации. Эталонное значение для ряда конфигураций приведено в правой части окна в текстовой области «Описание».

2) Несоответсвие. Значения параметра безопасности несоответствует эталонному значению для конфигурации.

3) Неизвестно или не проверено. Элемент конфигурации не имеет условий проверки, как правило это означает, что элемент конфигурации описывает организационную процедуру или носит справочный характер.

При «отщелкивании» флажка меню «Меню\Параметры\Отображать пункты не содержащие правил» из дерева меню будут убраны элементы конфигурации, не содержашие правил проверки.

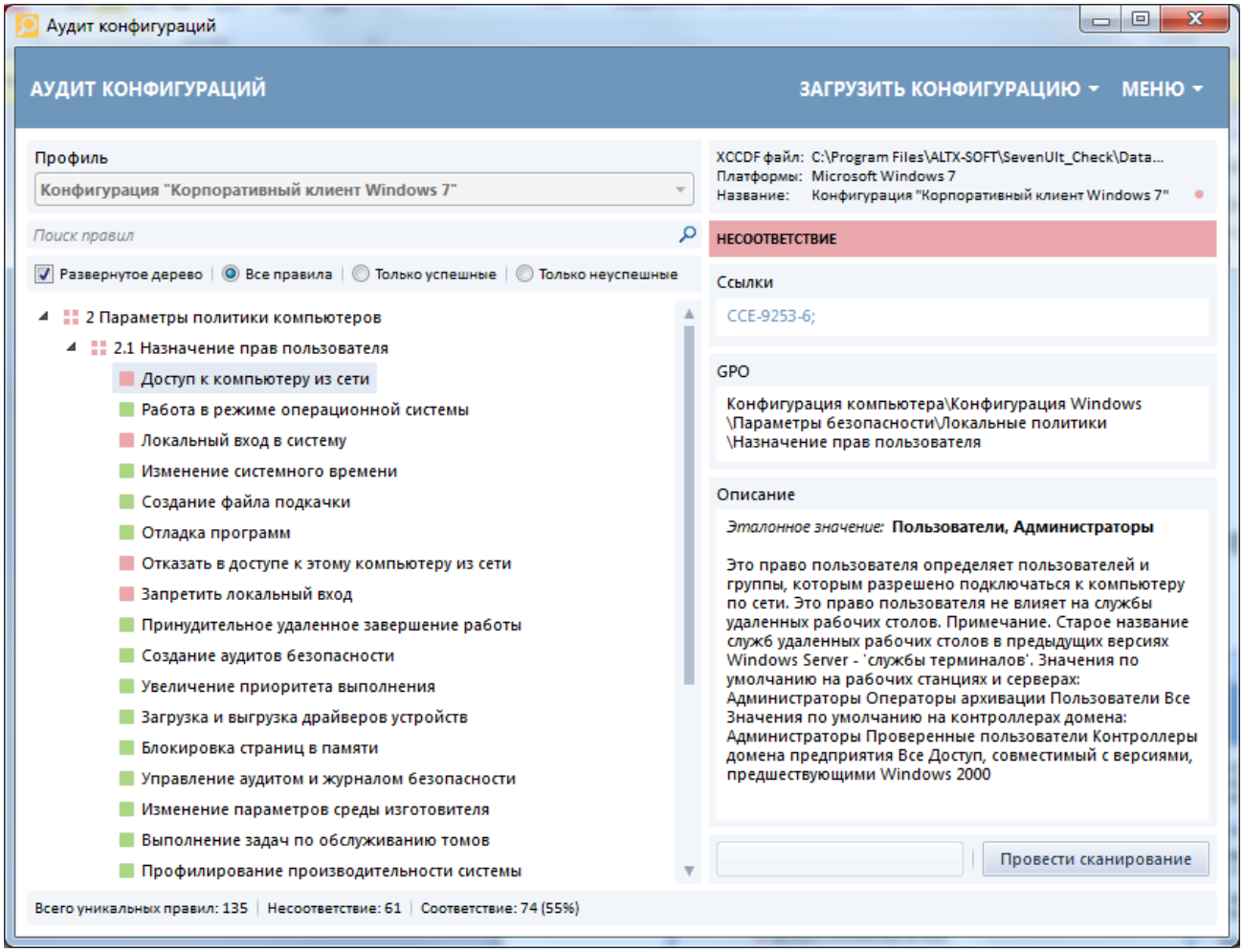


Рисунок 4.6 – Вид окна после проведения аудита конфигурации

Для каждого параметра конфигурации при выделении его мышью показывается следующая информация:

- ссылка на элемент Общего перечня конфигураций (CCE ™, Common configuration enumeration) в репозитории определений OVAL компании АЛТЭКС-СОФТ;
- путь к параметру в консоли GPO:
- описания параметра с эталонным значением параметра.

Результаты проведенного контроля доступны в отчете (меню «Отчет»). Примерный вид отчета представлен на рисунке 4.7.

Рисунок 4.7 – Отчёт об аудите конфигурации

Программа имеет возможность загружать произвольный SCAP контент, например сформированный с использованием Microsoft Security Compliance Manager, контент конфигураций безопасности USGCB (United States Government Configuration Baseline, http://usgcb.nist.gov/usgcb/microsoft/download_win7.html). Для этого необходимо в меню «Загрузить конфигурацию» выбрать «Загрузить конфигурацию (XCCDF) файл». Далее в окне выбора файла необходимо выбрать XCCDF файл, имеющий расширение .xml (см. рисунок 4.8). Остальной SCAP контент, должен присутствовать в этой же папке. Работа с произвольной конфигурацией ничем не отличается от работы с встроенной конфигурацией (см. рисунок 4.9).

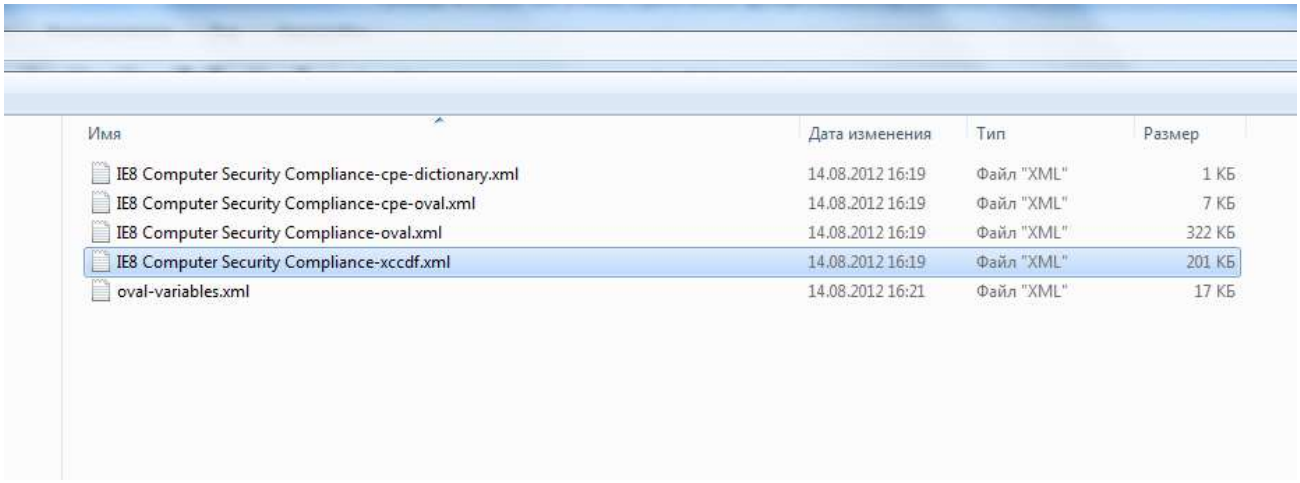


Рисунок 4.8 – Выбор произвольной конфигурации для аудита

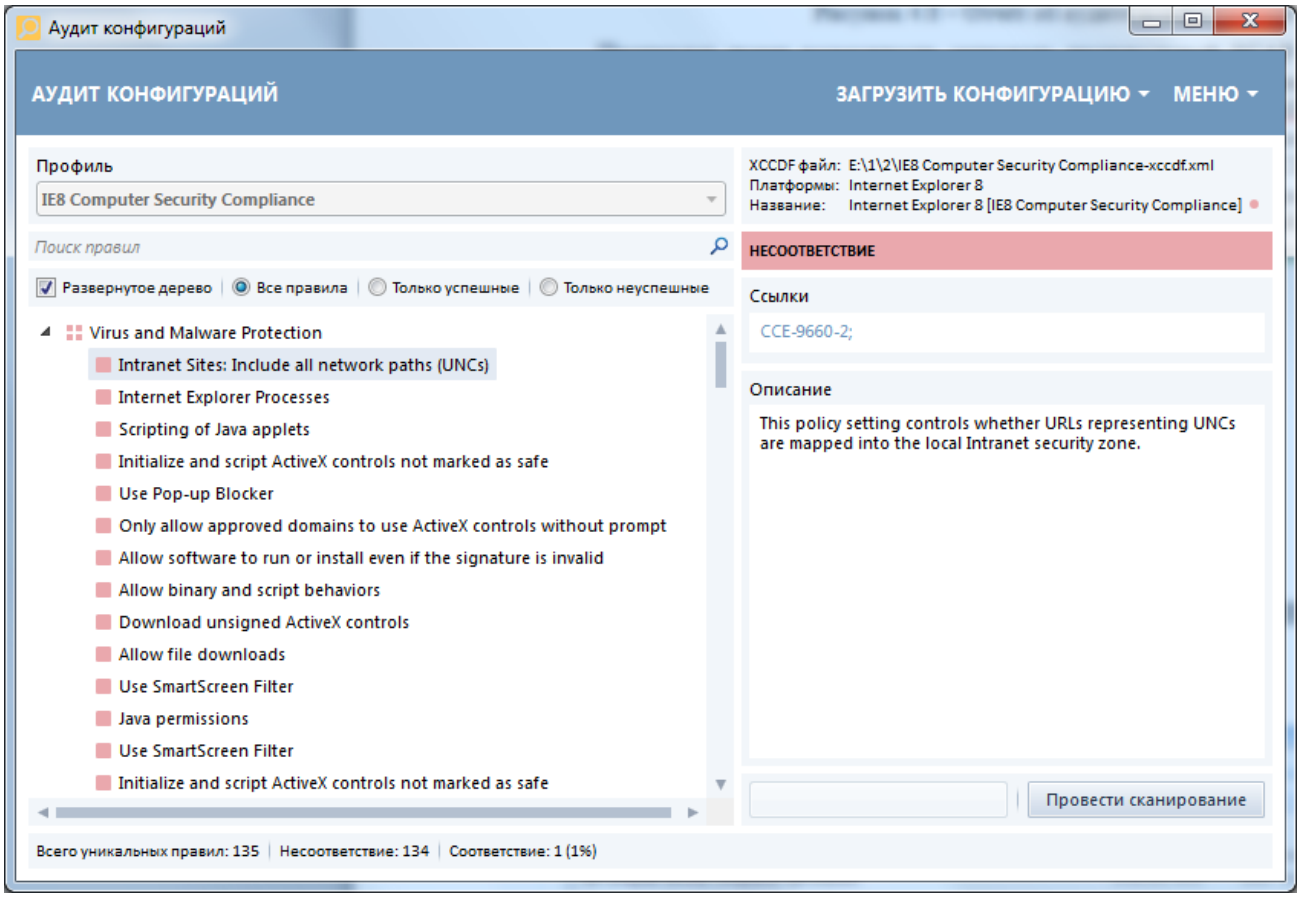


Рисунок 4.9 – Аудит произвольной конфигурации

4.4 Анализ сетевой активности

Для выполнения указанной функции необходимо нажать кнопку в центральной части окна программы.

На экран в отдельном окне будет выведен список процессов, ведущих сетевую активность (см. рисунок 4.10). При выборе мышью в правой части окна отображается детальная информация о нём.

Каждый из процессов или портов имеет 3 возможных статуса:

- «неизвестный» (отображается оранжевым цветом);
- «безопасный» (отображается зелёным цветом);

- «вирусный» (отображается красным цветом).

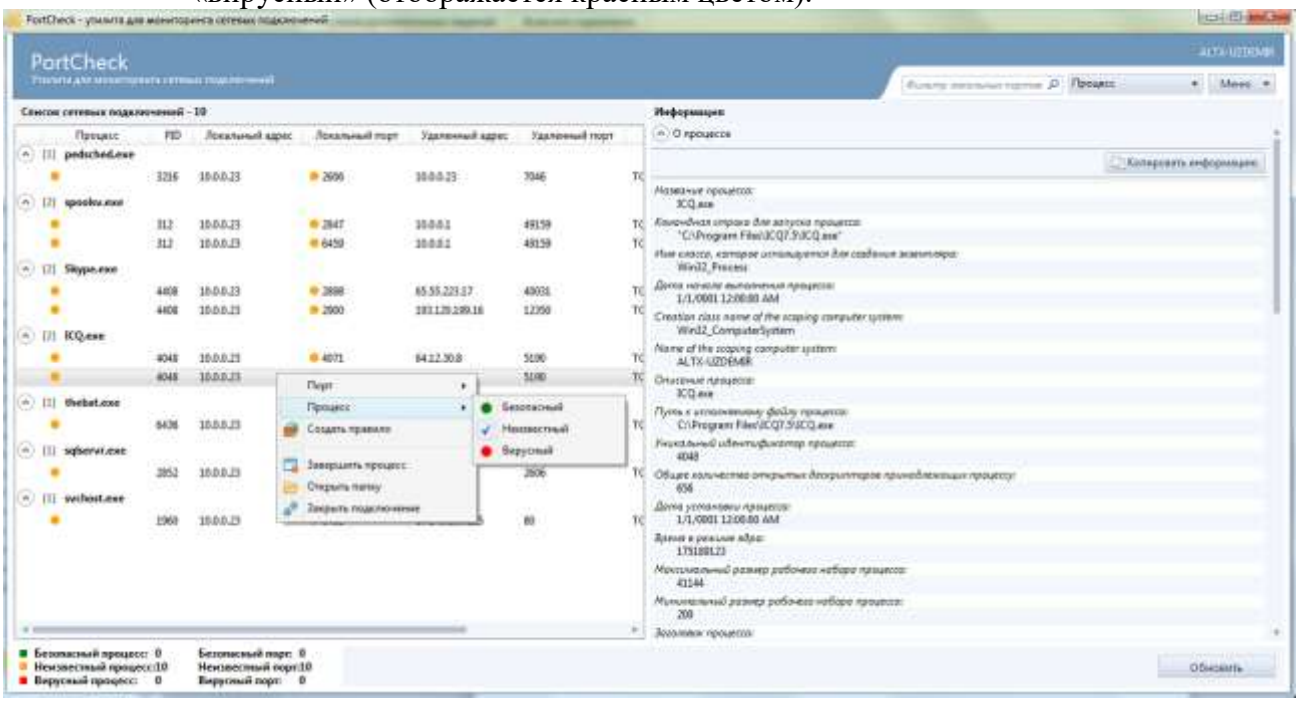


Рисунок 4.10 – Окно функции «Анализ сетевой активности»

При нажатии правой кнопки мыши на выделенном процессе доступно контекстное меню, которое обеспечивает выполнение следующих операций:

- изменение статуса порта/процесса;
- создать правило брандмауэра для процесса;
- завершить процесс
- открыть папку, содержащую файл, ассоциированный с процессом;
- закрыть сетевое подключение процесса.

При выборе пункта контекстного меню «Создать правило» пользователю будет предоставлен «мастер» создания правила для брандмауэра для выбранного процесса, где он последовательно вводит следующую информацию (см. рисунок 4.11):

- направление (для входящих или исходящих подключений);
- путь к исполняемому файлу
- тип протокола (TCP/UDP) и локальный и удаленные порты;
- локальный и удаленный IP-адреса;
- типы интерфейсов (локальный доступ, беспроводная сеть, удалённый доступ);
- разрешающее/запрещающее правило;
- профиль (доменный, частный, публичный);
- имя правила.

Список текущих портов и процессов, отмеченных как вирусные доступен в меню модуля «Меню\Список вирусных портов» или «Меню\Список вирусных процессов».

Программа реализует функцию сравнения сетевой активности по временным срезам. Для этого необходимо:

1) Сохранить первоначальное состояние путем выбора пункта меню «Меню\Сохранить отчёт». Пользователю будет предложено в окне сохранения файла выбрать место сохранения файла первоначального состояния.
2) Выбрать пункт меню «Меню\Сравнить отчёт». На экран будет представлено пустое окно отчета.
3) В окне отчета в меню «Отчет» выбрать «Открыть базовый отчёт» или «Открыть расширенный отчёт». В окне выбора файла указать файл, сохраненный в п.1
   В базовом сравнительном отчете будут для каждого из процессов будет выведена только основная информация (PID, тип протокола, локальные и удаленные адреса и порты). Расширенный отчет для каждого из процессов выводит детальную

информацию (изображаемую в правой части окна при выделении процесса), поэтому может использоваться как детальный отчет состоянии сетевой активности локального PC.

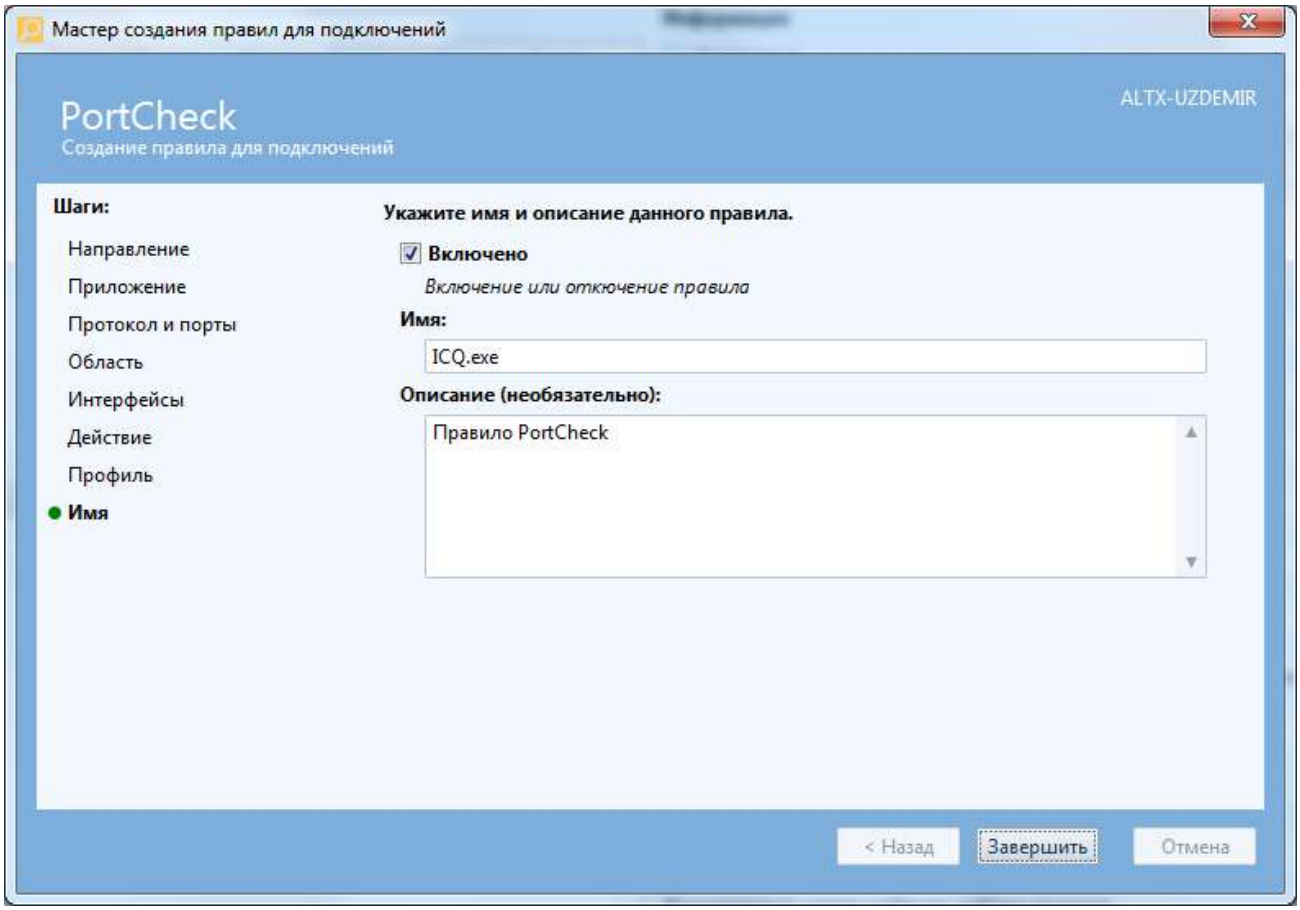


Рисунок 4.11 – Создание правила для брэндмауэра

Список сетевой активности обновляется с периодом времени, настраивом в меню «Меню\Обновить». Период обновления может состовлять 5, 10 или 15 секунд.

4.5 Проверка OVAL определений

Для выполнения указанной функции необходимо нажать кнопку в центральной части окна программы.

Функция позволяет загружать произвольный набор определений OVAL, полученный от сторонних источников. Это могут быть списки обновлений, уязвимостей и другой SCAP контент.

Для реализации проверки нужно в меню окна реализации функции выбрать пункт «Загрузить файл определений…». Далее в окне выбора файла необходимо выбрать файл определений OVAL, имеющий расширение .xml (см. рисунок 4.12). Остальной SCAP контент, должен присутствовать в этой же папке. Работа с произвольным набором OVAL определений аналогична реализации функции «Аудит уязвимостей» или «Аудит обновлений» (см. рисунок 4.13).

Функция может работать с набором OVAL определений, сформированным с использованием Microsoft Security Compliance Manager, определениями в составе конфигураций безопасности USGCB (United States Government Configuration Baseline, http://usgcb.nist.gov/usgcb/microsoft/download_win7.html). В этом случае для выполнения функции после выбора OVAL файла необходимо загрузить файл внешних переменных oval-

variables.xml с использованием пункта меню «Меню\Загрузить файл внешних переменных…».

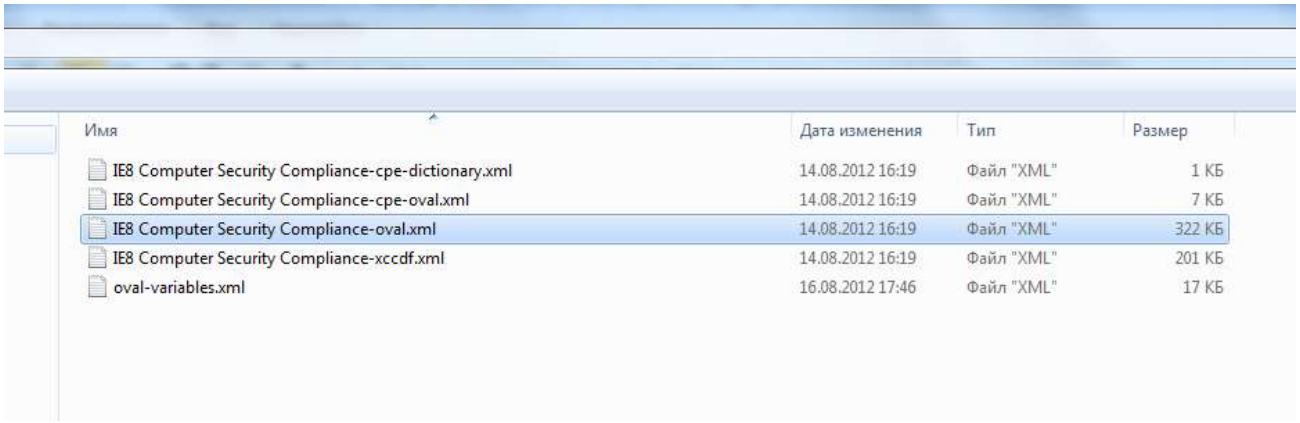


Рисунок 4.12 – Загрузка файла с определениями OVAL

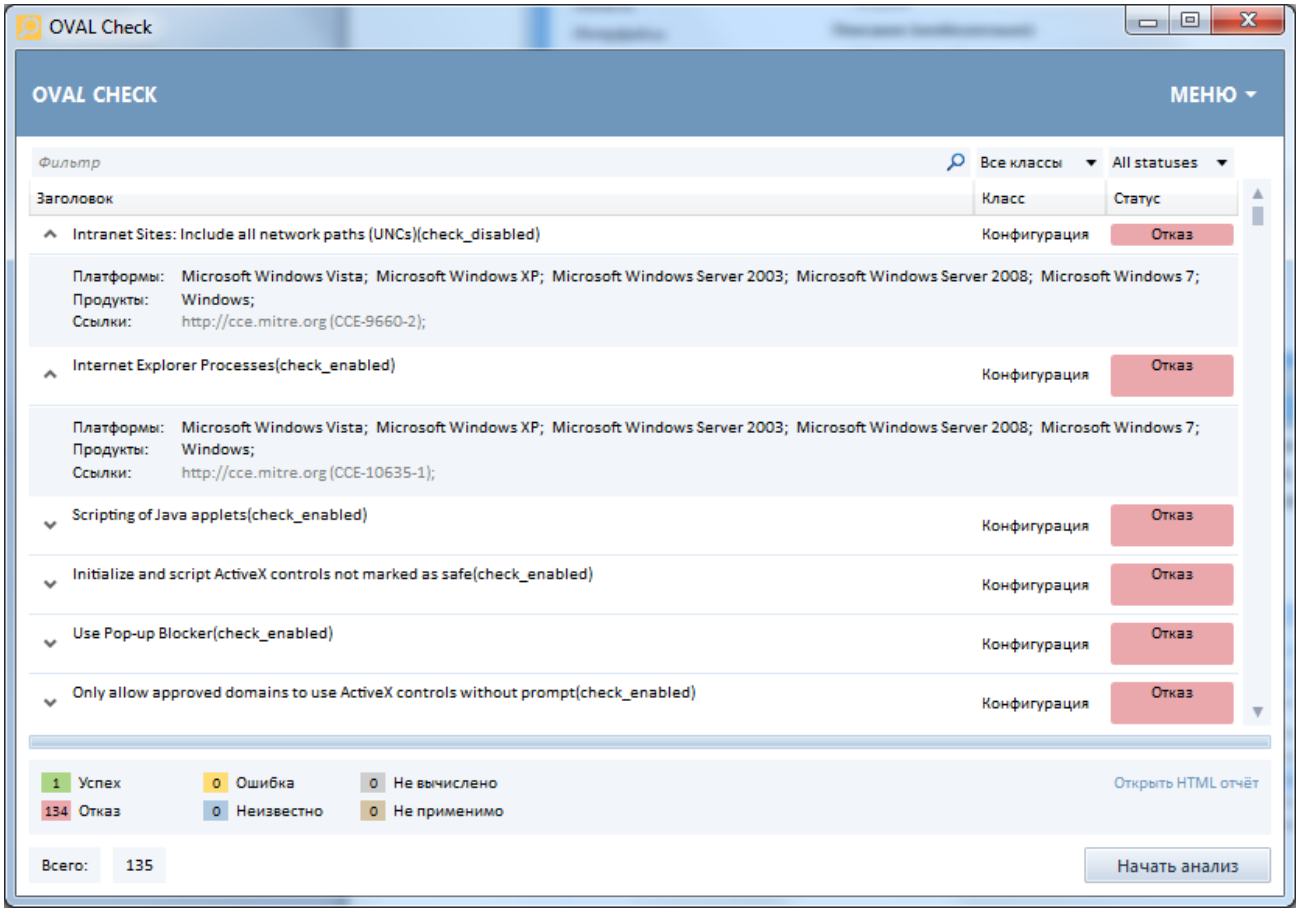


Рисунок 4.13 – Проверка OVAL определений