Эшелон
комплексная безопасность

Сканер-ВС

швейцарский нож администратора безопасности

Митков Максим,

заместитель директора департамента программных разработок

ЗАО «НПО «Эшелон»

Назначение

- Оперативный контроль (сканирование)
- Мониторинг и анализ защищенности системы от атак (программно-аппаратных воздействий)
- Контроль соблюдения требований защищенности, а также инвентаризации сети.

Эшелон
комплексная безопасность

Возможности

- Загрузка доверенной среды с любого компьютера (по технологии Live-CD/Live-flash) с автоматическим определением сетевого оборудования, подключенного к вычислительной сети
- Поиск остаточной информации на накопителях (поддерживаются различные кодировки, словари паттернов)
- Локальный (на любом ПК) и сетевой аудит парольной защиты
- инвентаризация (фиксация) ресурсов компьютерной сети (узлов, портов, сервисов)
- Выявление (сканирование) уязвимостей сетевых сервисов
- Проверка возможности осуществления атак на отказ в обслуживании и подмены адреса
- Анализ сетевого трафика (в т.ч. в коммутируемых сетях, физически разделенных)
- Аудит парольной информации для множества протоколов
- Аудит общесистемной информации и истории подключений USB-устройств.

Эшелон
комплексная безопасность

Состав комплекса

Сканер сети предназначен для проверки безопасности сети посредством поиска хостов, в которых открыты определенные порты.

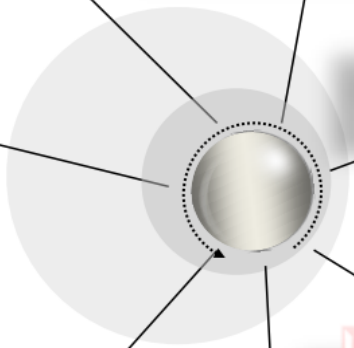
сканер сети

сканер безопасности

Средство локального аудита паролей предназначено для поиска и выявления паролей, содержащих легко подбираемые символьные комбинации, непосредственно на рабочей станции.

средство локального аудита паролей

средство поиска остаточной информации



Средство сетевого аудита паролей предназначено для удаленного поиска и выявления паролей, содержащих легко подбираемые символьные комбинации.

средство сетевого аудита паролей

Сетевой анализатор предназначен для использования администратором сети при проверке и детальном анализе правильности конфигурации сетевого программного обеспечения.

сетевой анализатор

средство обнаружения USB-подключений

Эшелон
комплексная безопасность

Преимущества

- Организация выделенного или виртуального рабочего места администратора безопасности
- Возможность применения при проведении сертификационных и аттестационных испытаний
- Активное выявление уязвимостей сетевых сервисов
- Аудит парольной информации для множества протоколов
- Контроль памяти и трафика
- В комплект поставки входит бесплатный курс обучения администратора «Сканер-ВС»

Эшелон
комплексная безопасность

Варианты поставки

1. CD-ROM
2. Flash-носитель
3. Ноутбук с уже предустановленным средством

Эшелон
комплексная безопасность

Нормативные основания применения

1) Приказ ФСТЭК России от 5 февраля 2010 г. N 58 г. Москва "**Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных**". Регистрационный №16456.

- **Пункты Положения:** 2.4, 2.6.

2) Постановление Правительства РФ от 17 ноября 2007 г. N 781 "Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных".Пункты Положения: 11. д)

Эшелон
комплексная безопасность

Нормативные основания применения

3) **Руководящий документ.** Автоматизированные системы. Защита от несанкционированного доступа к информации Классификация автоматизированных систем и требования по защите информации.

- **Требование руководящего документа к классам защищенности:** 3Б, 3А, 2Б, 2А, 1Д, 1Г, 1В, 1Б, 1А о периодическом тестирование функций СЗИ НСД при изменении программной среды и персонала АС с помощью тест-программ, имитирующих попытки НСД.

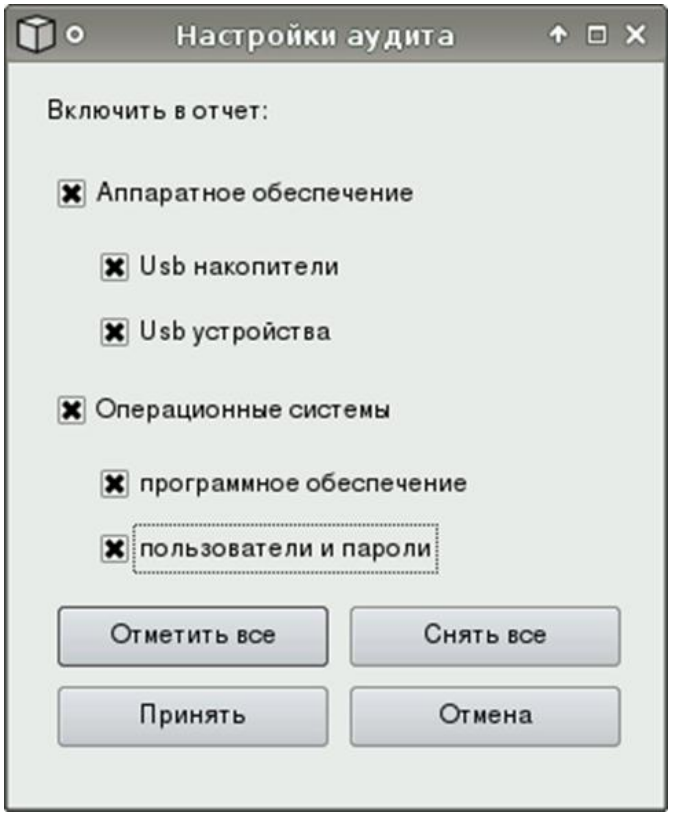
5) **Доктрина информационной безопасности Российской Федерации**, утвержденная Президентом Российской Федерации 9 сентября 2000 г. № Пр-1895.

6) **«Общие требования по обеспечению безопасности информации в ключевых системах информационной инфраструктуры»** утверждены Заместителем директора ФСТЭК России 18 мая 2007 г.

Системный локальный аудит

Системный аудитор предназначен для сканирования рабочей станции на предмет определения параметров:

- установленных операционных систем;
- системных, коммуникационных и периферийных устройств, в том числе USB-устройств;
- перечень использованных на компьютере USB-носителей;
- снимок программно-аппаратной конфигурации.



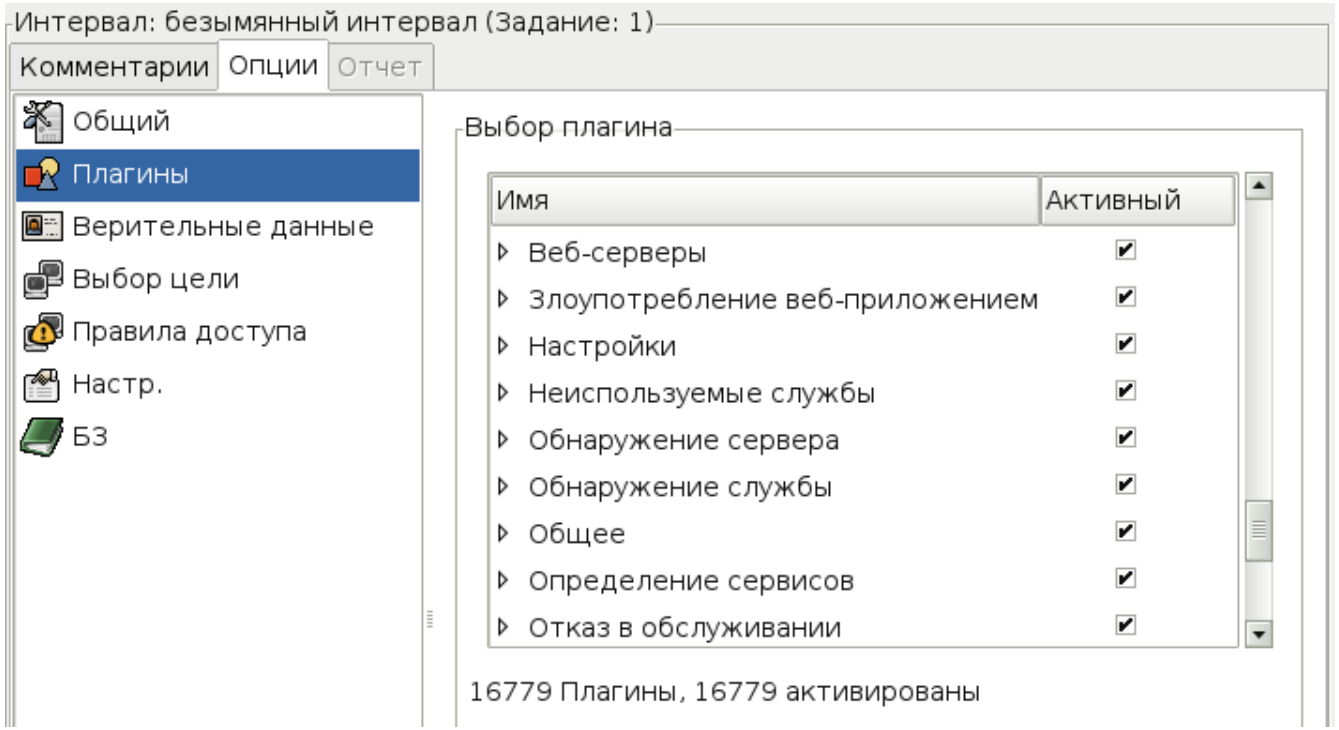
Эшелон
комплексная безопасность

Сканер безопасности

- Сканер безопасности позволяет осуществлять поиск уязвимостей в сетевых сервисах, предлагаемых операционными системами, межсетевыми экранами, маршрутизаторами и другими сетевыми компонентами.
- Для поиска уязвимостей используются как стандартные средства тестирования и сбора информации о конфигурации и функционировании сети, так и специальные средства, эмулирующие действия злоумышленника по проникновению в системы, подключенные к сети.

Сканер безопасности

Выбор плагинов:

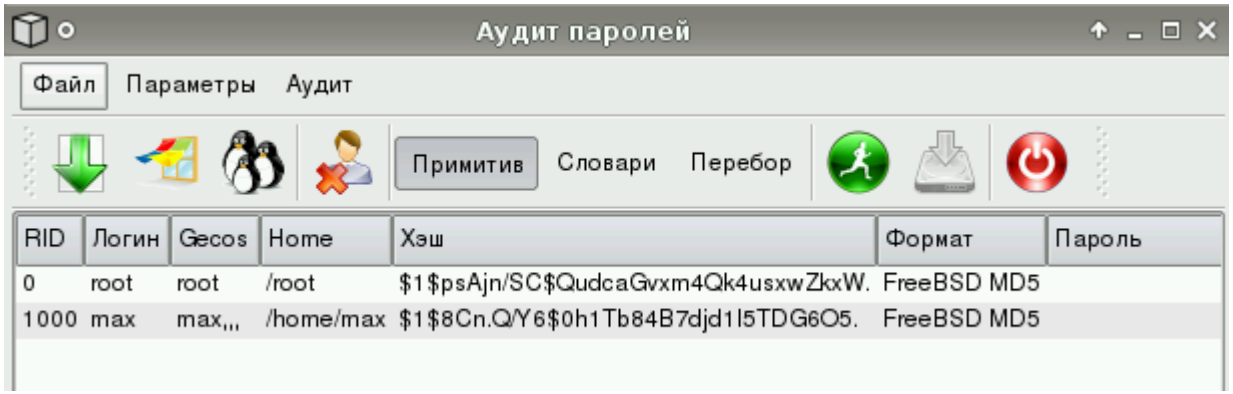


Эшелон
комплексная безопасность

Аудит паролей локальный

Средство предназначено для поиска и выявления паролей, содержащих легко подбираемые символьные комбинации, непосредственно на рабочей станции.

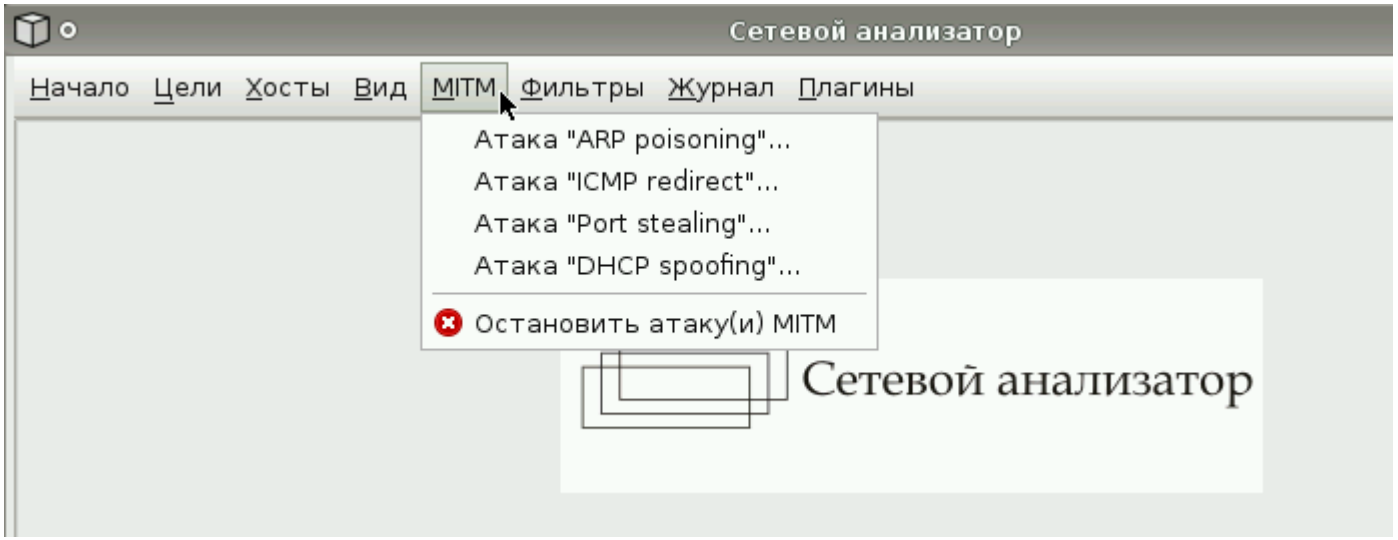
- Широкий перечень поддерживаемых ОС: Windows (2000, XP, Vista, 7), Linux (ОС МСВС, Linux XP, Astra Linux).



Эшелон
комплексная безопасность

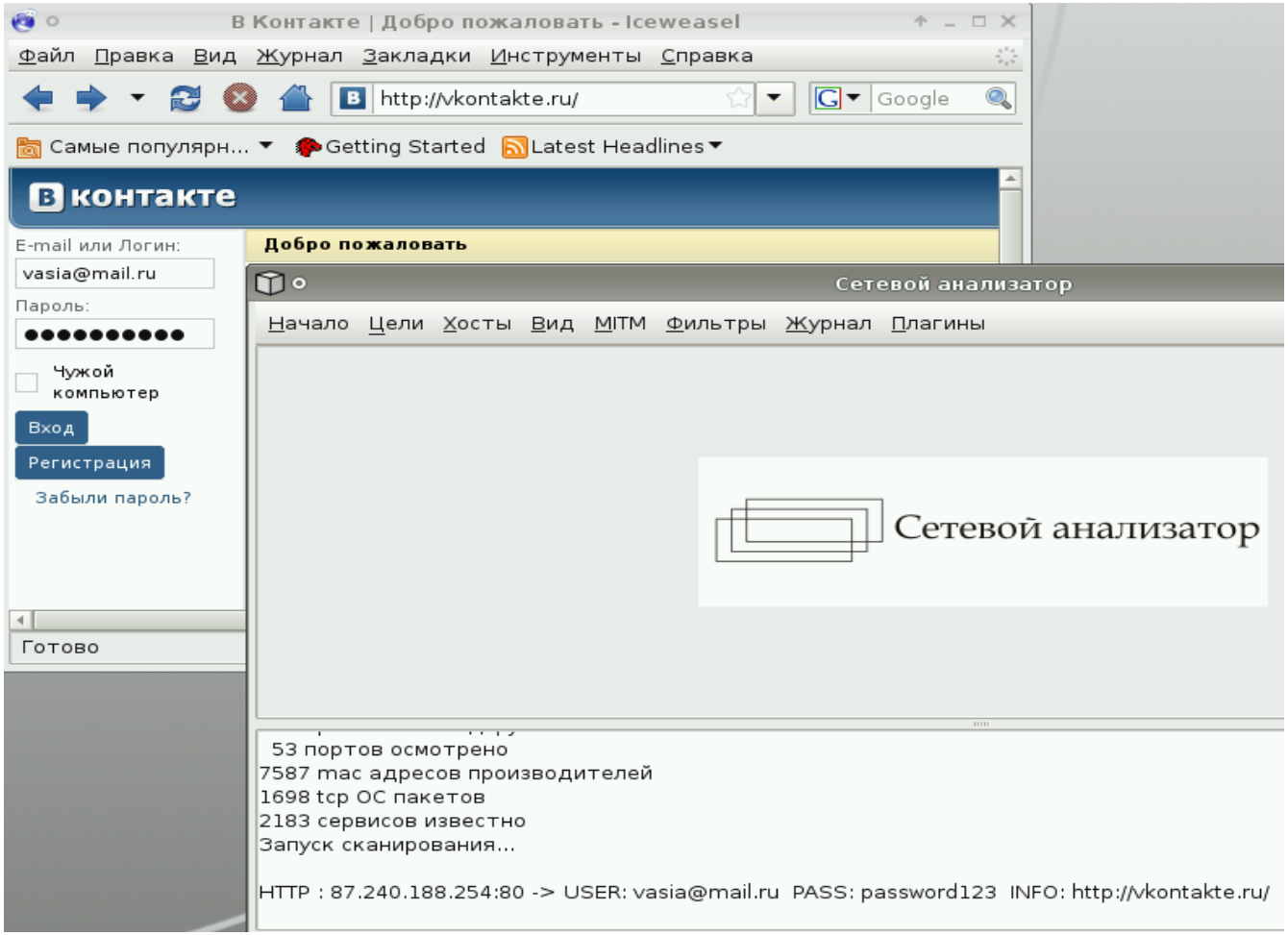
Перехват трафика

Сетевой анализатор предназначен для использования администратором сети при проверке и детальном анализе правильности конфигурации сетевого программного обеспечения.



Эшелон
комплексная безопасность

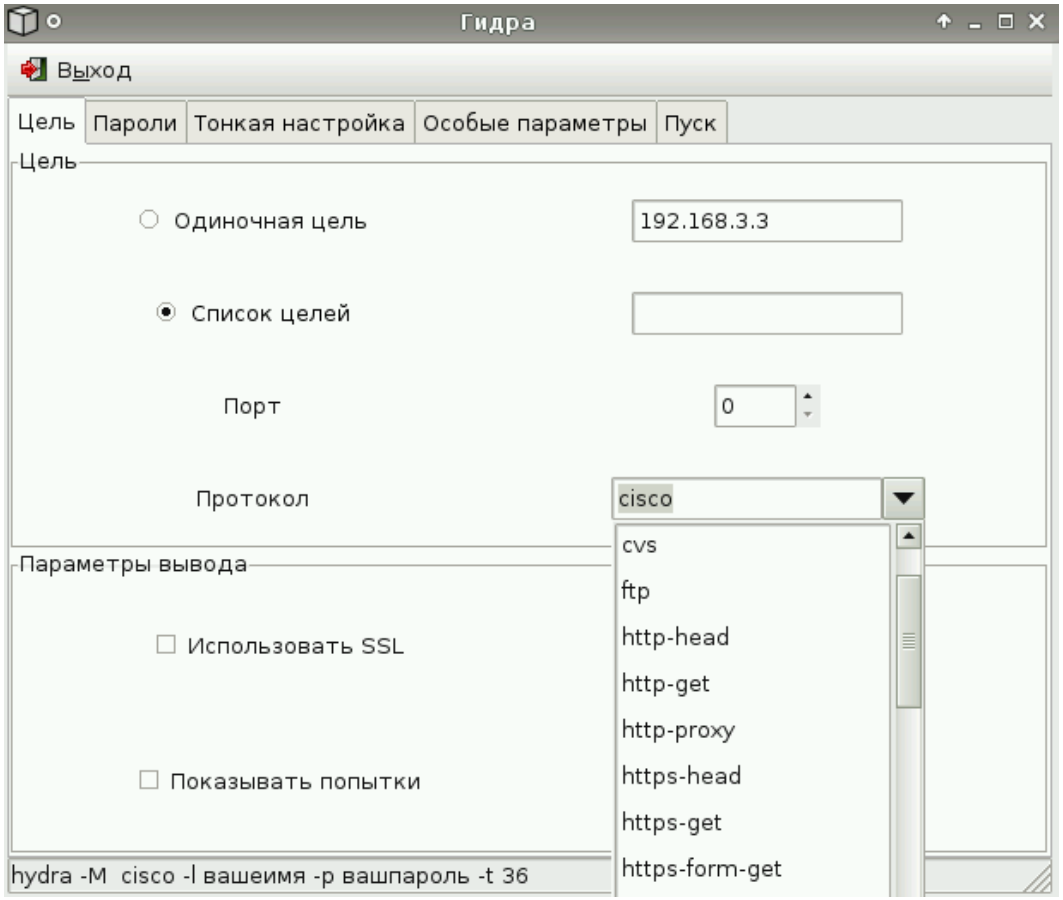
Перехват трафика



Эшелон
комплексная безопасность

Подбор сетевых паролей

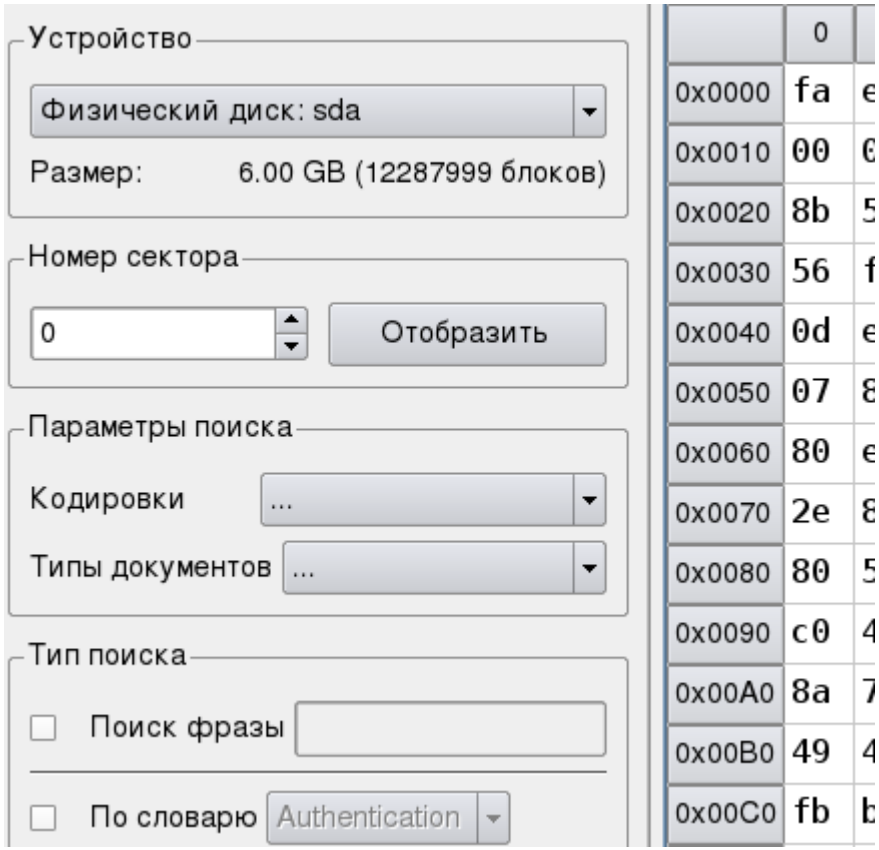
- Поддержка множества сетевых протоколов
- Перебор по словарю
- Многопоточный перебор



Эшелон
комплексная безопасность

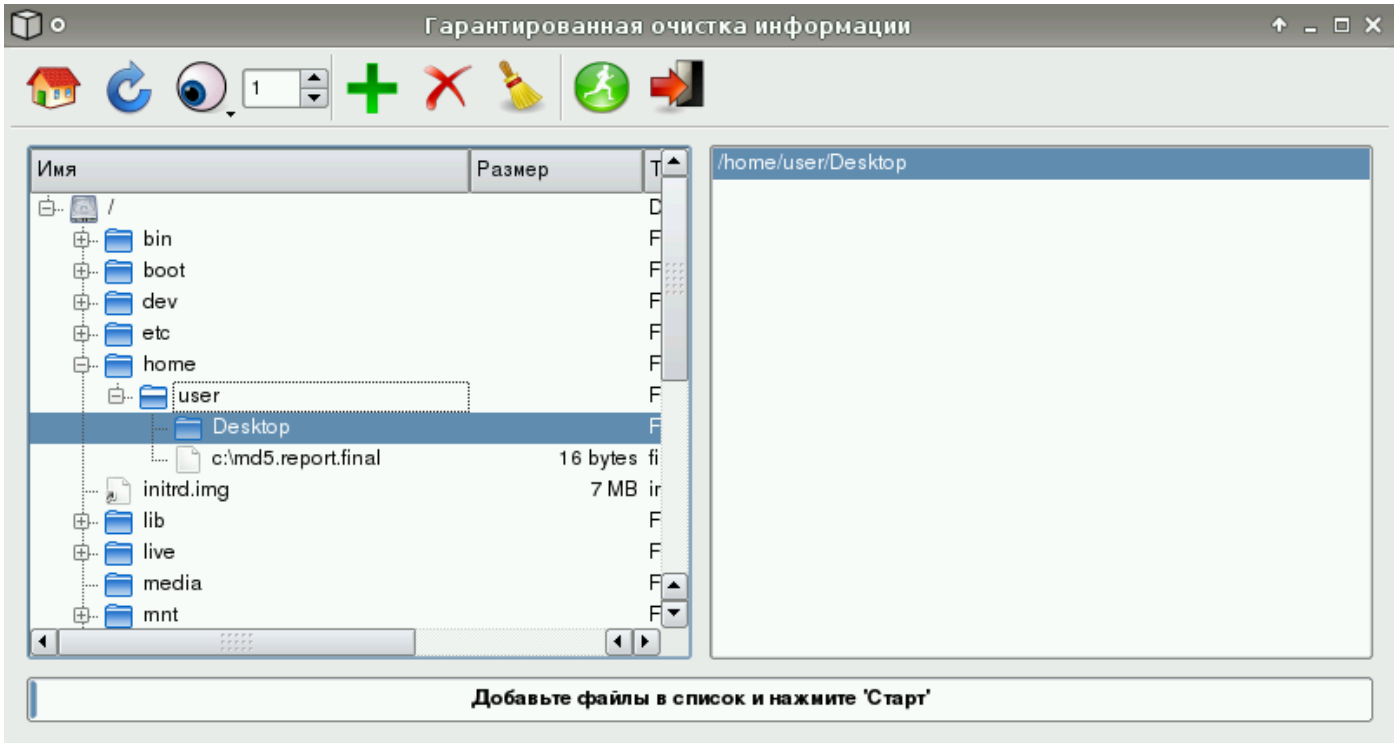
Поиск информации

Средство поиска по диску предназначено для поиска информации по ключевым словам на носителях данных (жестких дисках, дискетах, оптических дисках).



Эшелон
комплексная безопасность

Гарантированное уничтожение информации



- ✓ Реализует алгоритм Питера Гутмана
- ✓ Вплоть до 32 итераций стирания

Эшелон
комплексная безопасность

Сравнение продуктов

Сканер-ВС	Аналогичный сертифицированный продукт
Локальный аудит паролей	-
Сетевой аудит паролей	-
Сканер безопасности	Обычный сканер безопасности
Системный аудитор	-
Сканер сети	-
Поиск остаточной информации	Обычное средство поиска остаточной информации
Гарантированная очистка информации	Обычное средство гарантированной очистки информации
Программа инспекционного контроля — снятие контрольных сумм	Обычное средство контроля целостности
Анализатор протоколов	-

- Наличие операционной системы не требуется
- Требуется наличие сертифицированной версии операционной системы

Эшелон
комплексная безопасность

Сертификаты

Сертификат Минобороны России

Сертификат ФСТЭК России

Эшелон
комплексная безопасность

Контакты для приобретения

ЗАО "НПО "Эшелон"

107023, ул. Электрозаводская, д. 24

Телефоны и факсы: +7(495) 645-38-09, 645-38-10, 645-38-11

E-mail: mail@npo-echelon.ru

www.npo-echelon.ru

Эшелон
комплексная безопасность