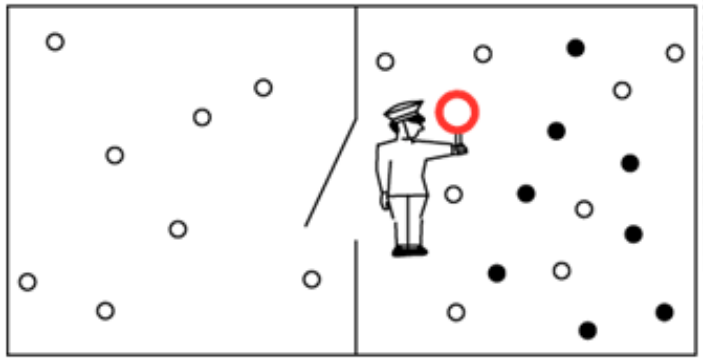
Формирование единой безопасной информационно-образовательной среды в школе. Защита знаний на основе контент фильтров и антивирусных решений.

Законодательство

- 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» (28.07.2012 N 139-ФЗ, 2013, 2014, 2015)
- Методические материалы для обеспечения информационной безопасности детей при использовании ресурсов сети Интернет (письмо Минобрнауки России № ДЛ-115/03 от 28.04.2014)

Методы контентной фильтрации



- «Белый» и «Черный» список

- Базы данных нежелательного и категоризированного контента
- Глубокий анализ получаемого контента (текст, изображение, видео и т.п.)

Реестры

- Федеральный список экстремистских материалов (http://minjust.ru/ru/extremist-materials)
- Единый реестр Роскомнадзора(http://eais.rkn.gov.ru/)
- Реестр не совместимых с образованием ресурсов (НСОР)

производство таких материалов, на основании представления прокурора или при производстве по соответствующему делу об административном правонарушении, гражданскому или уголовному делу.

Федеральный список экстремистских материалов формируется на основании поступающих в Минюст России копий вступивших в законную силу решений судов о признании информационных материалов экстремистскими.

При этом наименования и индивидуализирующие признаки информационных материалов включаются в федеральный список экстремистских материалов в строгом соответствии с резолютивной частью решения суда.

Обжалование решений судов о признании информационных материалов экстремистскими осуществляется в порядке, предусмотренном законодательством Российской Федерации.

Законодательством Российской Федерации установлена ответственность за массовое распространение экстремистских материалов, включенных в опубликованный федеральный список экстремистских материалов, а равно их производство либо хранение в целях массового распространения.

Скачать федеральный список экстремистских материалов

201.	Листовка «Хизб-ут-Тахрир аль-Ислам» под названием «Посредством установления Халифата спасем себя и мир» (решение Кузьминского районного суда г. Москвы от 26.10.2007 и определение Кузьминского районного суда г. Москвы от 21.03.2008).
202.	Листовка «Хизб-ут-Тахрир аль-Ислам» под названием «Делегация американского конгресса была почетно принята в Бейруте, несмотря на то, что ее глава унизил исламскую религию» (решение Кузьминского районного суда г. Москвы от 26.10.2007 и определение Кузьминского районного суда г. Москвы от 21.03.2008).
203.	Листовка-разъяснение от «Хизб-ут-Тахрир» в Индонезии по поводу взрыва возле Австралийского Посольства в Джакарте» (решение Кузьминского районного суда г. Москвы от 26.10.2007 и определение Кузьминского районного суда г. Москвы от 21.03.2008).
	Брошюра «Хизб-ут-Тахрир аль-Ислам» «Решение шариата относительно участия мусульман, живущих в западном мире в его политической жизни

Телефон: (495) 994-93-55
Адрес: 119991, ГСП-1, город Москва, улица Житная, дом 14

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО НАДЗОРУ В СФЕРЕ СВЯЗИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И МАССОВЫХ КОММУНИКАЦИЙ

Ru | En

РОСКОМНАДЗОР

ЕДИНЫЙ РЕЕСТР

доменных имен, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено

Просмотр реестра | Прием сообщений | Провайдерам хостинга | Операторам связи | FAQ

Федеральный закон от 27 июля 2006 года № 149-ФЗ
"Об информации, информационных технологиях и защите информации" (PDF)

Постановление Правительства Российской Федерации от 26 октября 2012 г. № 1101
"О единой автоматизированной информационной системе "Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено" (PDF)

Приказ от 11 сентября 2013 года №1022/368/666
"Об утверждении критериев оценки материалов и (или) информации, необходимых для принятия решений Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций, Федеральной службой российской федерации по контролю за оборотом наркотиков, Федеральной службой по надзору в сфере

Через форму, опубликованную ниже, вы можете получить данные о нахождении доменных имен, указателей страниц сайтов в сети "Интернет" и сетевых адресов, позволяющих идентифицировать сайты в сети "Интернет", содержащие информацию, распространение которой в Российской Федерации запрещено, в Едином реестре.

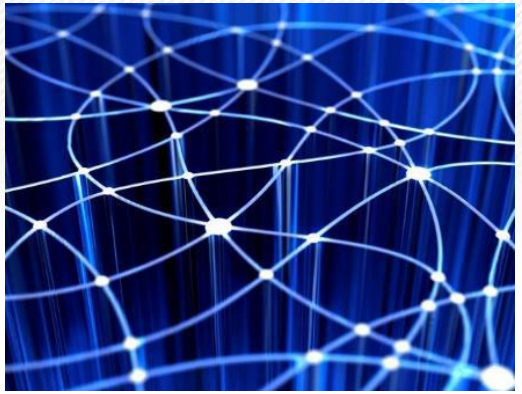
Для проверки ограничения доступа к сайтам и (или) страницам сайтов сети «Интернет» в рамках исполнения иных положений Федерального закона от 27.07.2006 года № 149-ФЗ «Об информации, информационных технологиях и защите информации», рекомендуем воспользоваться универсальным сервисом проверки ограничения доступа.

Искомый ресурс

Примеры: 1.2.3.4 (для ip адреса)
domain-xxx.ru (для доменного имени)
http://www.domain-xxx.ru/news/?id=2 (для URL адреса)

Защитный код:

Место контентной фильтрации



- Оператор связи

- Сервер, шлюз в школьной сети

- Рабочая станция

Где информация?

Информацию ребенок получает на рабочей станции !

Ответственный –тот, кто отвечает за рабочую станцию !

Школа или оператор связи?

Методические рекомендации Минобрнауки п. 3.2

«Техническое ограничение доступа пользователей к нежелательной информации (фильтрация) осуществляется непосредственно на клиентских рабочих местах, для чего используются специальные программные решения фильтрации, рекомендованные Минобрнауки России»

Пришла проверка

- Получить информацию:
  - Интернет-ресурс
  - Тип контента
  - Время (!)
- Зафиксировать результат проверки и сообщить в службу техподдержки

  support@.....ru
- После устранения неверной категоризации, подготовить ответ на предписание

НЕ ТЕРЯЕМ ВРЕМЯ!!!

Пришла проверка (часть 2)

- До проверки –тренировка
- Обращение в техподдержку:
  - Не зависит где и у кого куплен фильтр
  - Вопрос не только о работе фильтра, но и консультации по его настройке, подготовке ответа на предписание
- Не терять контакт с тем, кто устанавливал и настраивал фильтр; Или иметь все **данные по настройкам фильтра**

Антивирусные программы для образования

Задачи при организации комплексной защиты сети

- Комплексная защита от вирусов и спама
- Выполнение требований законодательства – построение системы защиты в соответствии с требованиями 152-ФЗ
- Централизованное управление всеми компонентами защиты
- Удобство и простота администрирования
- Богатый функционал
- Нетребовательность к ресурсам
- Совместимость приложений

№152-ФЗ «О персональных данных» Требования по антивирусной защите

Согласно закону требуется обеспечить:

- разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам
- предотвращение внедрения в информационные системы вредоносных программ
- использование средств антивирусной защиты при взаимодействии с сетью Интернет
- централизованное управление системой защиты персональных данных информационной системы


KASPERSKY
lab

Корпоративная линейка

Стандартный

- Защита компьютеров и ноутбуков
- Защита файловых серверов
- Защита мобильных устройств и планшетов

Расширенный

- Защита компьютеров и ноутбуков
- Защита файловых серверов
- Защита мобильных устройств и планшетов
- Шифрование данных

Dr.Web

Комплексная централизованная защита

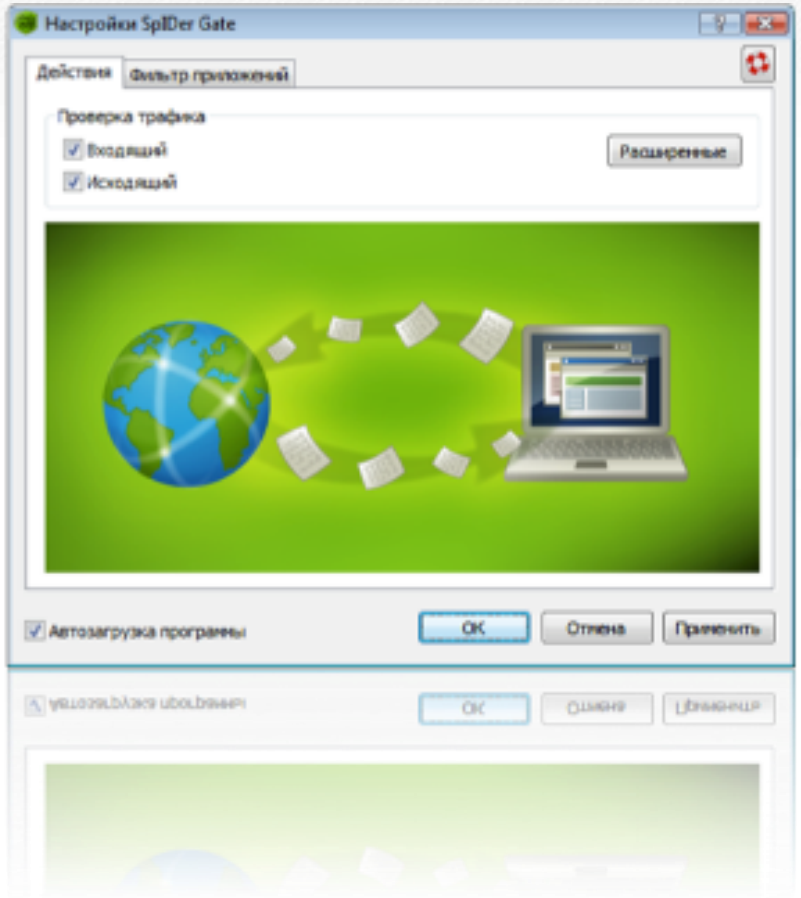
Решаемая задача:
полная защита от существующих угроз

- Установка на инфицированный ПК
- Запуск с внешнего носителя
- Повышенная вирусоустойчивость
- Лечение сложных вирусов (Shadow.based, Rustock, Sector, MaosBoot)
- Повышенный уровень самозащиты (Dr.Web SelfPROtect)
- Проверка архивов любого уровня вложенности
- Высочайшая точность выявления упакованных вредоносных объектов

Решаемая задача:
защита на опережение

- FLY-CODE – распаковка неизвестных упаковщиков
- Уникальная технология несигнатурного поиска Origins Tracing™
- Эвристический анализатор Dr.Web

Решаемая задача:
только чистый интернет-контент

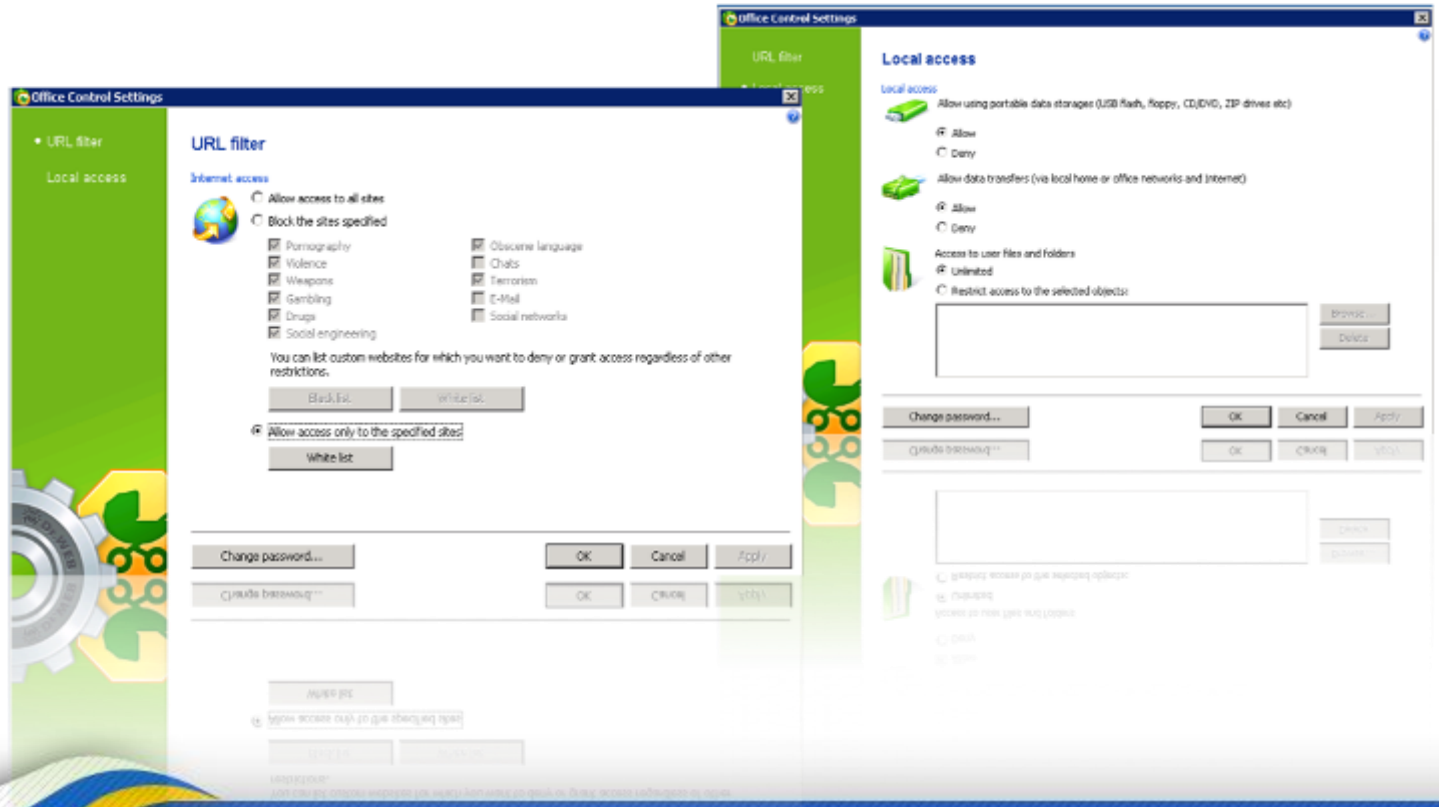


- Сканирует HTTP-трафик
- Фильтрация файлов, аплетов, скриптов
- Не зависит от используемого браузера
- Начинает сканирование сразу после установки в системе
- Блокировка фишинговых и других опасных сайтов по записям в соответствующих базах ссылок

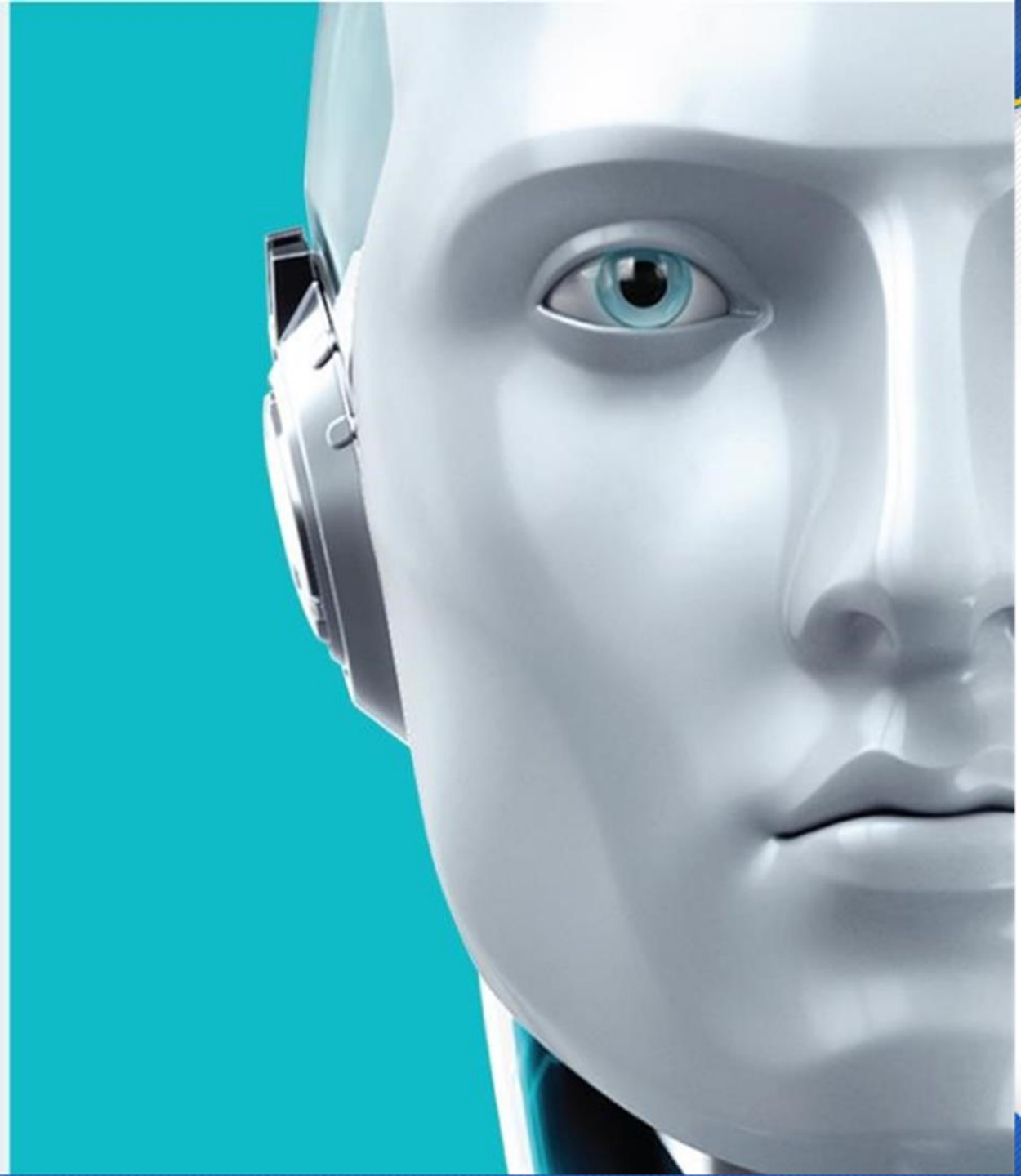
Решаемая задача:

защита конфиденциальной информации

Запрет доступа к файлам, папкам, съемным носителям



ESET: поддержка корпоративных клиентов.



БЕЗОПАСНОСТЬ. НИЧЕГО ЛИШНЕГО

ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ ESET NOD32

НАДЕЖНОСТЬ

Комплексная защита от всех видов угроз

- интеллектуальные технологии детектирования вредоносного ПО
- проактивные методы защиты корпоративной сети

Безопасность данных пользователя

- система предотвращения вторжений в сеть
- защита информации от хакерских атак
- аварийное восстановление системы

Защищенный Интернет и электронная почта

- двусторонняя проверка сетевого и почтового трафика
- безопасность сетевых соединений
- фильтрация нежелательной почты

ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ ESET NOD32

БЫСТРОДЕЙСТВИЕ

Минимальное влияние на производительность системы

- минимальные системные требования
- двусторонняя фильтрация трафика без нагрузки на канал
- компактные обновления вирусных баз
- идентификация типа компьютера для бережного использования ресурсов системы

Высокая скорость работы на любых компьютерах

- быстрая работа приложений при сканировании
- мониторинг угроз в режиме реального времени
- интеграция всех компонентов