Обзор CoSoSys Endpoint Protector 4

Иван Бойцов

Обозреватель Anti-Malware.ru

Endpoint Protector 4 — новое DLP-решение на российском рынке, разработанное немецкой компанией CoSoSys. В данном обзоре мы рассмотрим функциональность Endpoint Protector и попробуем оценить, сможет ли данное средство составить конкуренцию именитым игрокам рынка DLP-решений в России.

Сертификат AM Test Lab

Номер сертификата: 160

Дата выдачи: 22.03.2016

Срок действия: 22.03.2021

Реестр сертифицированных продуктов »

Введение

Рынок DLP-решений в России сформировался давно, и вендорам не приходится разъяснять, что это за продукты и зачем они нужны заказчикам. Все понимают, что утечки конфиденциальной информации чаще всего производятся руками инсайдеров — сотрудников компаний. На нашем сайте неоднократно публиковались обзоры и сравнения игроков рынка DLP-решений. Защита от утечек — активно развивающаяся сфера, где закрепились десяток крупных отечественных вендоров, конкуренцию которым составляют именитые международные игроки рынка ИБ. Но потенциал рынка нельзя считать полностью раскрытым. С каждым годом увеличивается число внедрений DLP-систем, но множество крупных компаний, государственных информационных систем, а также малых и средних предприятий все еще не защищены от утечек информации. Все это дает возможность выхода на рынок новых игроков, и сегодня мы оцениваем один из таких продуктов — CoSoSys Endpoint Protector 4.

Компания CoSoSys основана в 2004 году и с момента возникновения занимается разработкой средств защиты информации с акцентом на защите от утечек. В портфель компании, кроме флагманского продукта Endpoint Protector, входят средство криптографической защиты EasyLock и облачная версия продукта в SaaS-решении My Endpoint Protector. Решения поддерживают операционные системы Windows, Linux и MAC OSX и предназначены как для малого и среднего бизнеса, так и для больших предприятий.

Endpoint Protector разрабатывается давно и имеет множество успешных внедрений в крупных международных компаниях — Philips, Sony, LG, Suzuki, Verbatim, Toyota, Центральный банк Швейцарии и многих других. Также Endpoint Protector активно используется государственными заказчиками в странах Евросоюза, Азии и США.

Функциональные возможности

Основные функциональные возможности CoSoSys Endpoint Protector условно делятся на шесть больших групп:

- **Контроль устройств** — позволяет контролировать подключение любых устройств к защищаемому компьютеру. Определяются отдельные правила для подключаемых мобильных телефонов, цифровых камер, медиаустройств, биометрических считывателей, сетевых карт, включая беспроводные, 3G/4G-модемов, принтеров, систем хранения, FireWire-устройств и множества других типов аппаратного обеспечения.

Поддерживается настройка политик на уровне отдельных пользователей и групп пользователей, компьютеров и всей защищаемой сети. Доступ настраивается гранулярно — можно не только полностью запретить или разрешить подключение устройств, но и настроить доступ только для чтения.

Контролируются все факты переноса информации на внешние устройства, создаются теневые копии отчуждаемых файлов и ведутся подробные журналы аудита для расследования возможных инцидентов. Дополнительно поддерживается интеграция с системой шифрования — возможно настроить разрешение на запись во внешние устройства только для зашифрованных файлов.

Разработчики предусмотрели сценарий удаленной работы, когда защищаемый компьютер выносится за

пределы сети и не подключен к управляющему серверу. Для этого CoSoSys Endpoint Protector поддерживает временные пароли, которые могут быть введены в клиентской части Endpoint Protector для получения доступа к подключаемым устройствам. В случае необходимости администратор может удаленно санкционировать подключение устройства, передав пароль пользователю по любому каналу связи.

- **Контентный анализ** — сигнатурный и лингвистический контроль содержимого файлов, передаваемых по каналам связи, позволяет обнаружить локальные и сетевые утечки информации, даже в случае частичной передачи содержимого конфиденциальных данных и их маскировки.

Контентный анализ производится на основании предустановленных фильтров, настроенных на обнаружение персональной идентификационной информации (SSN, e-mail-адреса и другие типы данных), и на основании настраиваемых администратором словарей, ключевых слов и регулярных выражений. Поддерживается настройка фильтров для обнаружения утечек по разрешениям файлов без разбора контента.

Так же, как и с контролем устройств, политики могут настраиваться для конкретного пользователя, групп пользователей, компьютеров или глобально для всей сети. Поддерживается два режима работы — блокировка передачи или разрешение передачи с подробным журналированием инцидентов. Все передаваемые данные сохраняются в теневых копиях для последующего анализа. Журналы могут быть отправлены в SIEM-систему.

CoSoSys Endpoint Protector способен анализировать множество видов интернет-трафика — протоколы электронной почты, веб-трафик (включая HTTPS), системы обмена сообщениями (Skype, ICQ, AIM, MSN, Yahoo Messenger и т. д.), облачные системы хранения (Dropbox, iCloud, SkyDrive, Yandex Disk и другие), P2P-протоколы (BitTorrent, Kazaa и другие), FTP-протокол и множество других, включая TeamViewer, iTunes и Samsung Kies. Чтобы исключить влияние на бизнес-приложения и избежать нагрузки в системе, поддерживается белый список веб-сайтов, доменов, конкретных файлов и видов файлов, сканирование которых не проводится, и, соответственно, блокировка при срабатывании контентного анализа не осуществляется.

В продукте реализован контентный анализ данных, выводимых на печать, и контроль размещения конфиденциальных данных в буфере обмена. Дополнительно могут блокироваться функции создания снимков экрана для предотвращения утечки информации через изображения.

- **Контроль мобильных устройств (MDM)** — в продукте встроены функции по контролю мобильных устройств, обеспечивающие единую инфраструктуру для защиты от утечек в организации.

Endpoint Protector позволяет управлять политиками безопасности мобильных устройств —парольная защита, шифрование данных, разрешение и запрет использования Wi-Fi-сетей и VPN-соединений и т. д. В случае когда устройство утрачено, доступны функции по его поиску, удаленной блокировке и полному удалению всей конфиденциальной информации.

Дополнительно Endpoint Protector позволяет управлять мобильными приложениями — производить удаленную установку программ, определять разрешенные к запуску приложения и удалять запрещенное ПО.

В продукте присутствует также ряд дополнительных функций: возможность запрета доступа к камере, отключение функций по синхронизации с облачными сервисами, блокировка подключения мобильного устройства к компьютеру, запрет сопряжения с Bluetooth-устройствами и многие другие.

Политики безопасности могут быть привязаны к местоположению устройства. Например, доступ к камере устройства можно заблокировать только для контролируемой территории.

- **Шифрование данных** — обеспечивает защиту информации на съемных носителях путем интеграции с продуктом CoSoSys EasyLock. При совместной работе Endpoint Protector позволяет применять политики шифрования EasyLock на защищаемые компьютеры. EasyLock шифрует файлы на внешних носителях, на локальных дисках, папках и при передаче в облачные хранилища по криптостойкому алгоритму AES с ключом в 256 бит.

CoSoSys Endpoint Protector поддерживает интеграцию с Active Directory путем импорта пользователей и групп при первоначальной установке и дальнейшей синхронизации базы пользователей с контроллером домена. Кроме того, в продукте поддерживается интеграция с SIEM-системами, что позволяет встроить продукт в общую инфраструктуру информационной безопасности организации.

Защитный клиент CoSoSys Endpoint Protector может работать в явном режиме с иконкой в панели задач и выдачей уведомлений, либо в скрытом режиме, не афишируя свое присутствие в системе. В CoSoSys Endpoint Protector встроены функции самозащиты, что позволяет обеспечивать защиту для пользователей, обладающих правами локального администратора.

Системные требования и архитектура

CoSoSys Endpoint Protector является клиент-серверным приложением. Серверная часть выполнена в виде виртуальной машины, работающей под управлением ОС GNU/Linux. Поддерживается работа в следующих системах виртуализации:

- VMware Workstation 7.1.4 и 9.0.2;
- VMware Player 6.0.0;
- VMware Fusion 5.0.0;
- VMware vSphere (ESXi) 5.1.0;
- Oracle VirtualBox 4.2.18;
- Parallels Desktop for Mac 9.0.2;
- Microsoft Hyper-V Server 2008 и 2012;
- Citrix XenServer 64bit 6.2.0.

Другие среды виртуализации не тестировались производителем, но могут также поддерживаться. Возможен вариант установки сервера управления в облаке CoSoSys или в Amazon Web Services.

Дополнительно производитель поставляет аппаратные решения с установленным сервером CoSoSys Endpoint Protector. Устройств несколько, они отличаются мощностью, форм-фактором и максимальным количеством защищаемых компьютеров. Полный перечень устройств перечислен в таблице 1.

Таблица 1. Перечень моделей аппаратного решения CoSoSys Endpoint Protector

Модель	Количество защищаемых компьютеров	Дополнительное добавочное число защищаемых компьютеров	Форм-фактор	Процессор	Жесткий диск
A20	20	4	Отдельный	ULV Single Core	320GB

A50	50	10	1U	ULV Dual Core	320GB
A100	100	20	1U	ULV Dual Core	320GB
A250	250	50	1U	Pentium 2 Core	500GB
A500	500	100	1U	Pentium 2 Core	1TB
A1000	1000	200	1U	Intel Xenon 4 Core	2x1TB (Raid 1)
A2000	2000	400	2U	2x Intel Xenon 4 Core	4x1TB (Raid 5)
A4000	4000	800	3U	2x Quad Core	6x1TB (Raid 5)

Клиентская часть CoSoSys Endpoint Protector поддерживает следующие операционные системы:

- Windows XP/ Vista/7/8/10 (32 bit/64 bit);
- Windows Server 2003/2008/2012 (32 bit/64 bit);
- Mac OS X 10.4-10.11;
- Linux (Ubuntu/openSUSE, CentOS, RedHat).

Мобильный клиент защиты функционирует в следующих операционных системах:

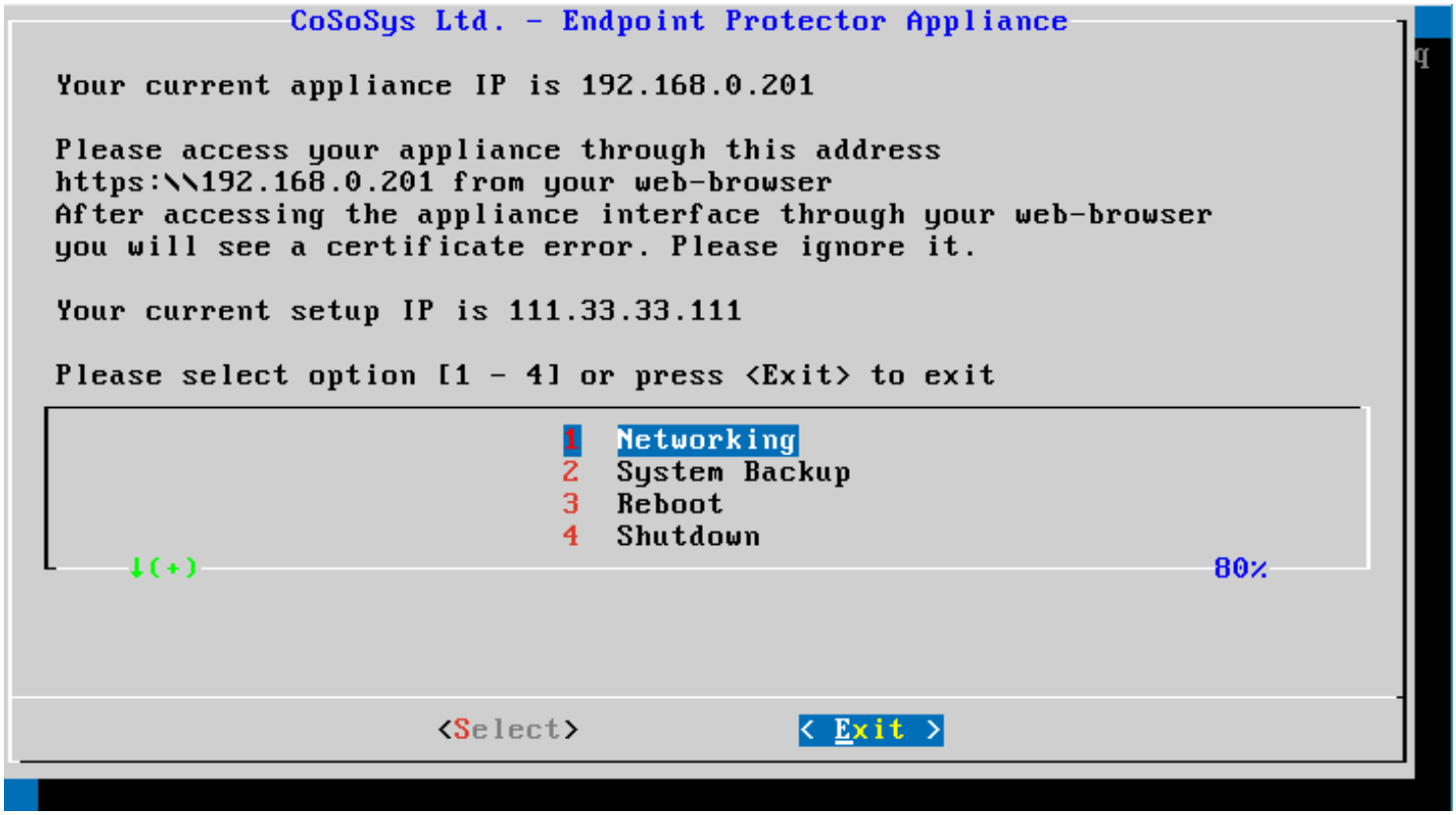
- Apple iOS 4, 5, 6, 7, 8, 9;
- Android 2.2 и старше.

Установка и развертывание

Установка виртуального сервера CoSoSys Endpoint Protector не требует специальных навыков. С помощью встроенных средств системы виртуализации производится импорт образа виртуальной машины, загруженного с сайта производителя, и настраиваются сетевые интерфейсы для работы в локальной сети организации.

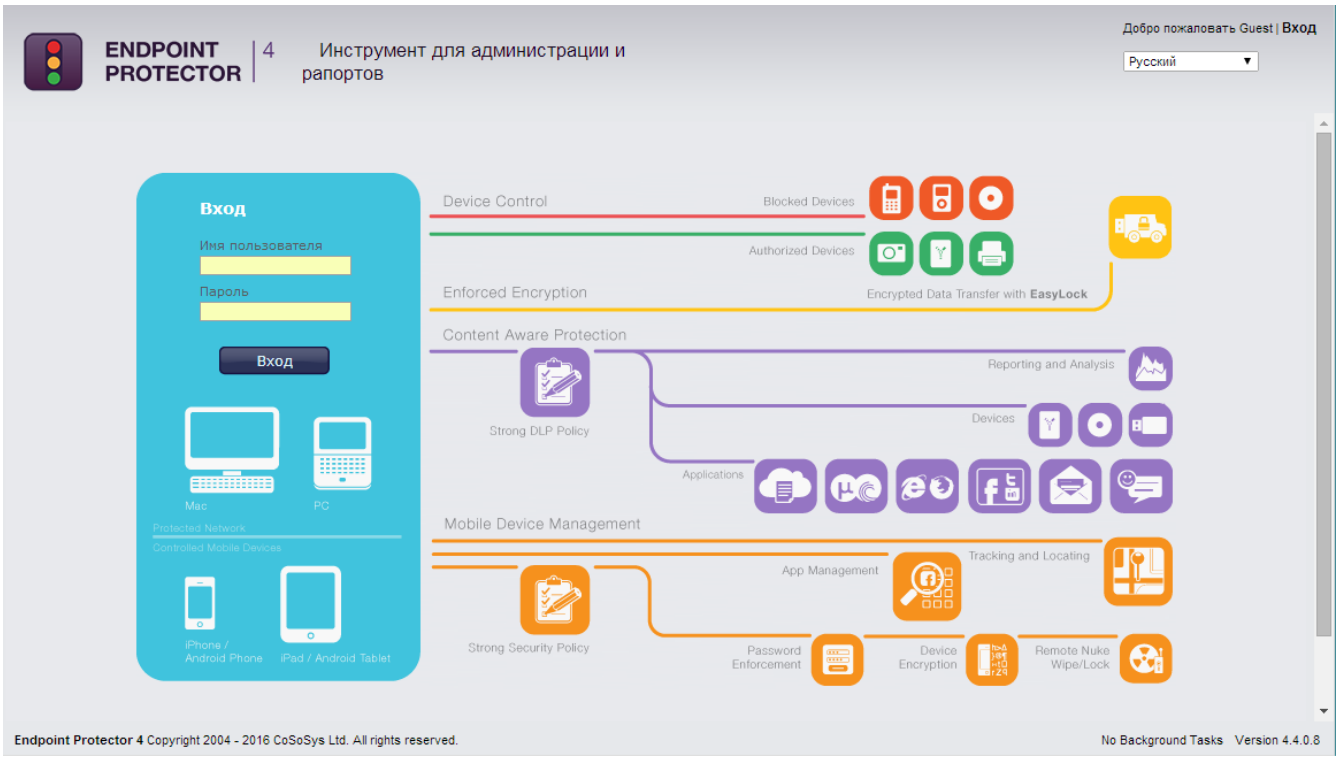
После включения и загрузки виртуальной машины отображается системный интерфейс CoSoSys Endpoint Protector, не требующий авторизации. В данном интерфейсе присутствует четыре пункта — настройка сетевых интерфейсов, работа с резервным копированием и восстановлением настроек, а также перезагрузка и выключение сервера.

Рисунок 1. Интерфейс работы с сервером CoSoSys Endpoint Protector



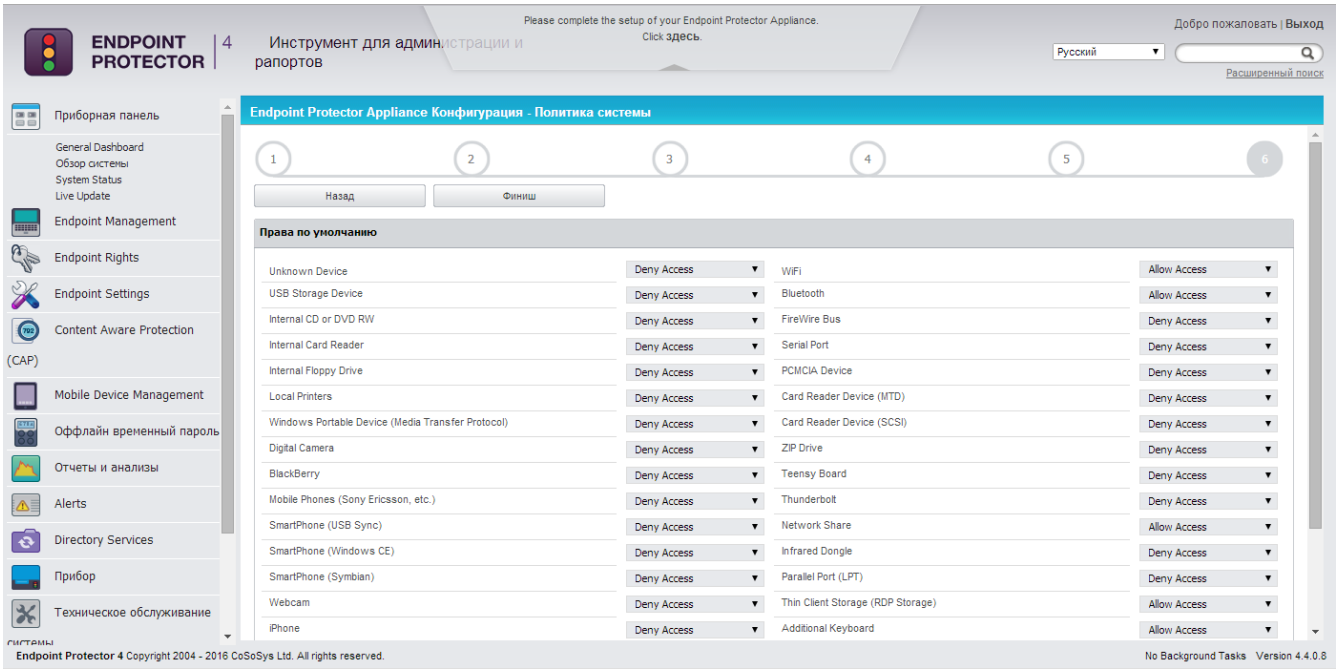
Все остальное взаимодействие с продуктом осуществляется через веб-интерфейс по защищенному протоколу HTTPS. При первом входе используется предустановленное имя пользователя и пароль, которые в дальнейшем необходимо изменить. Интерфейс продукта по умолчанию отображается на английском языке, но можно выбрать русский с помощью выпадающего меню в правом верхнем углу экрана.

Рисунок 2. Окно авторизации в веб-интерфейсе CoSoSys Endpoint Protector



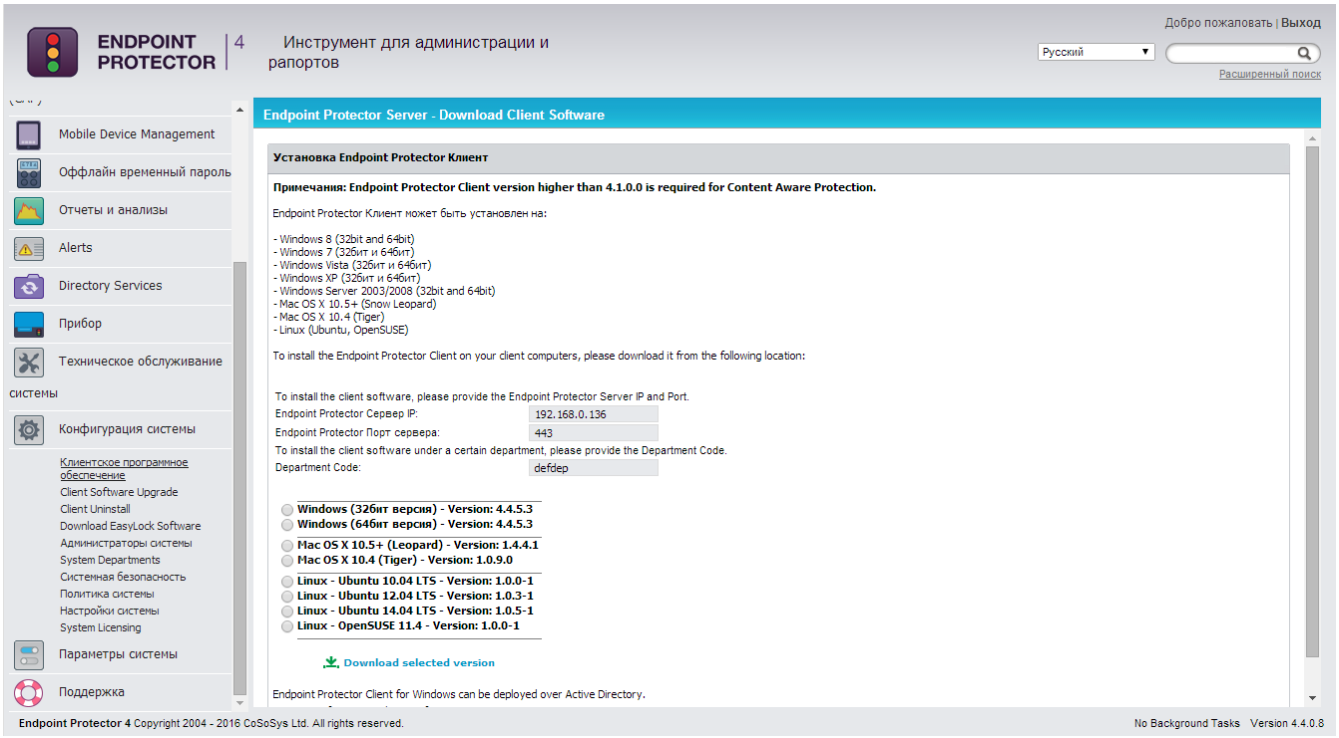
После первой авторизации открывается интерактивный мастер первой настройки продукта. За шесть шагов задаются общие параметры инфраструктуры — часовой пояс, название организации, учетные данные администратора, настройки сервера электронной почты и глобальные настройки контроля устройств.

Рисунок 3. Один из этапов мастера первой настройки CoSoSys Endpoint Protector



После первоначальной настройки необходимо развернуть клиентскую часть продукта на защищаемых компьютерах. Инсталлятор агента защиты загружается из раздела «Клиентское программное обеспечение» в меню «Конфигурация системы». Из списка выбирается тип загружаемого пакета — версия и разрядность операционной системы. После выбора браузер администратора предлагает сохранить сгенерированный пакет. В дальнейшем необходимо перенести пакет на клиентский компьютер и выполнить установку. Настройки подключения к серверу закладываются в инсталляционный пакет, поэтому при установке не требуется указание каких-либо параметров. Поддерживается развертывание пакета установки через групповые политики Active Directory, подробная инструкция открывается по ссылке из окна загрузки пакетов.

Рисунок 4. Окно загрузки пакета установки клиентской части CoSoSys Endpoint Protector

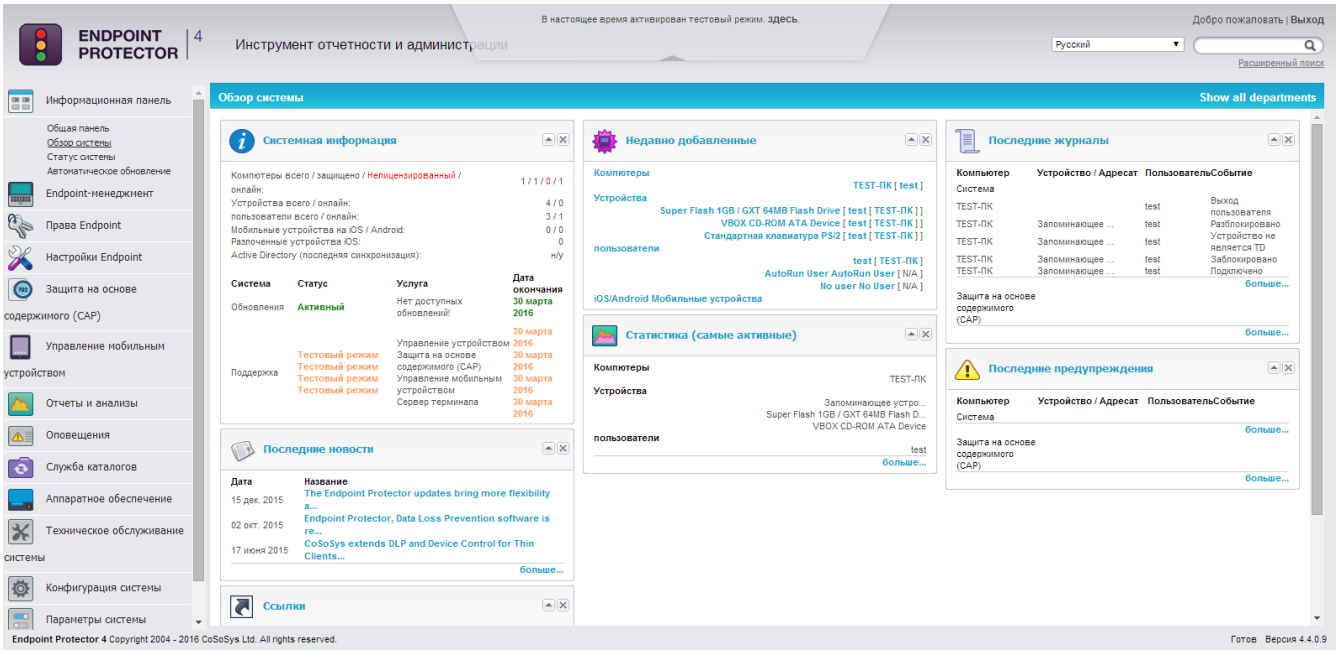


Процесс развертывания можно контролировать по появлению компьютеров в разделе «Компьютеры» меню Endpoint Management. После установки защищаемый компьютер нужно перезагрузить, агент защиты начинает функционировать сразу после установки, но не обновляет политики и не передает журналы аудита до перезагрузки.

Работа с продуктом

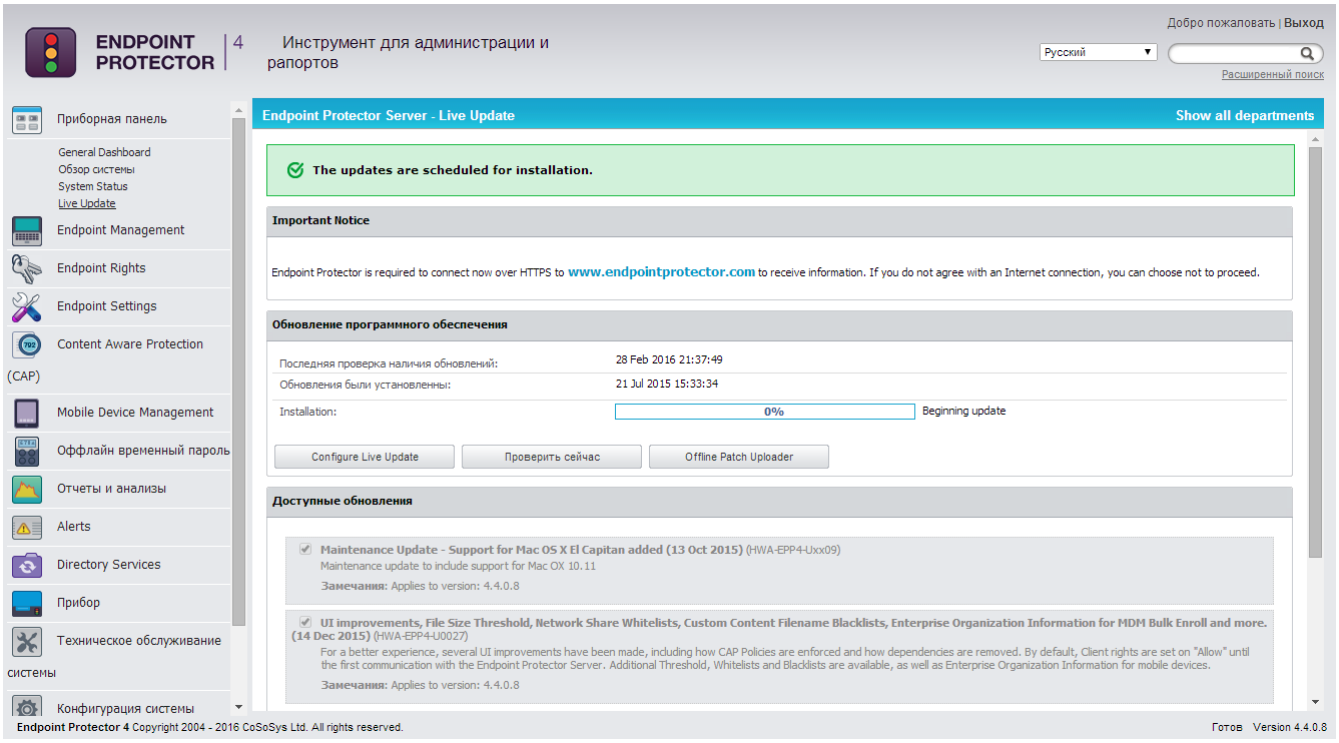
Основная навигация по функциям продукта осуществляется из иерархического меню в левой части экрана. В раздел «Приборная панель» вынесены различные экраны основного состояния системы защиты. «Общая панель» — основные графики по системе, количество защищаемых устройств, график наиболее активных пользователей, список защищенных мобильных устройств и так далее. На экране «Обзор системы» отображается информация о последних событиях — данные о лицензиях, последние добавленные устройства и компьютеры, список последних событий и другая информация.

Рисунок 5. Обзор системы в CoSoSys Endpoint Protector



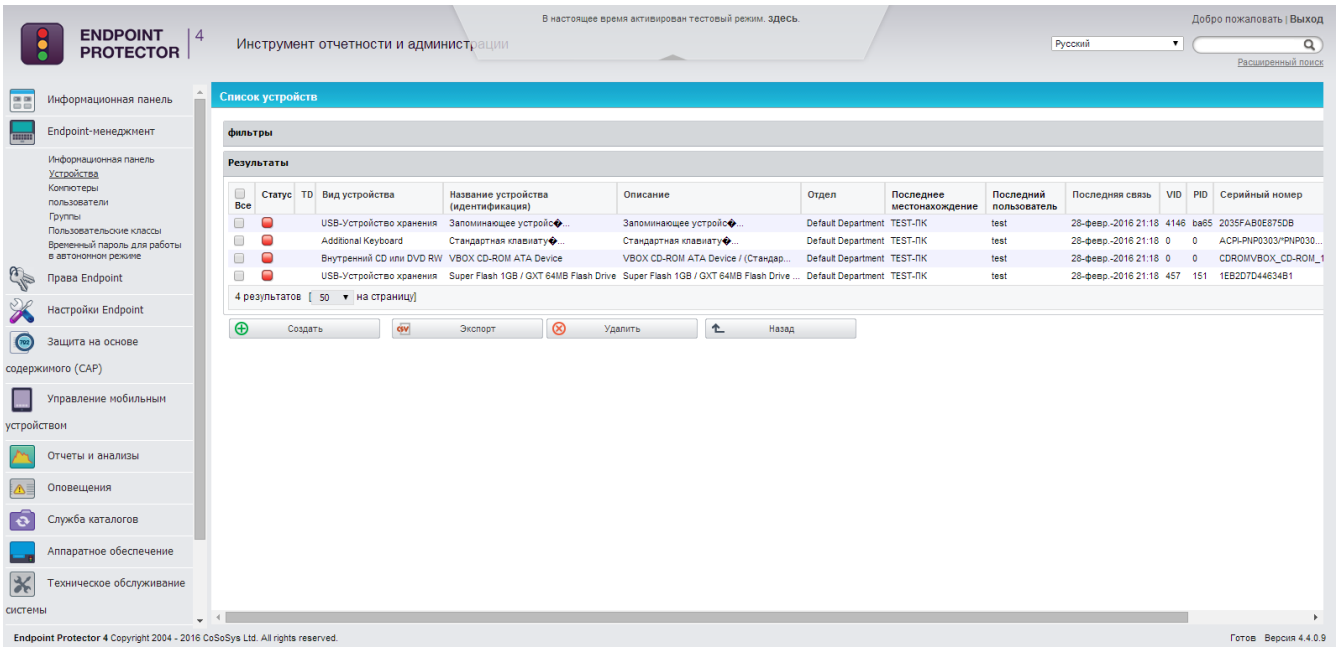
В разделе «Статус системы» размещена информация о функционировании системы защиты, а с помощью раздела «Автоматическое обновление» можно получить и установить последнюю версию продукта. В тестовой среде демоверсия продукта, загруженная с сайта производителя, предложила установить обновления, и после установки произошли значительные изменения — поменялась группировка интерфейса, значительно улучшилось качество локализации и добавились новые поддерживаемые версии операционных систем. По каждому из обновлений представлена подробная информация о нововведениях и изменениях в Endpoint Protector. Установка обновлений занимает непродолжительное время, при этом система работает в штатном режиме. После завершения обновлений потребовалось обновить страницу в браузере, при этом никаких неудобств или перерывов в доступе не возникло.

Рисунок 6. Автоматическое обновление CoSoSys Endpoint Protector



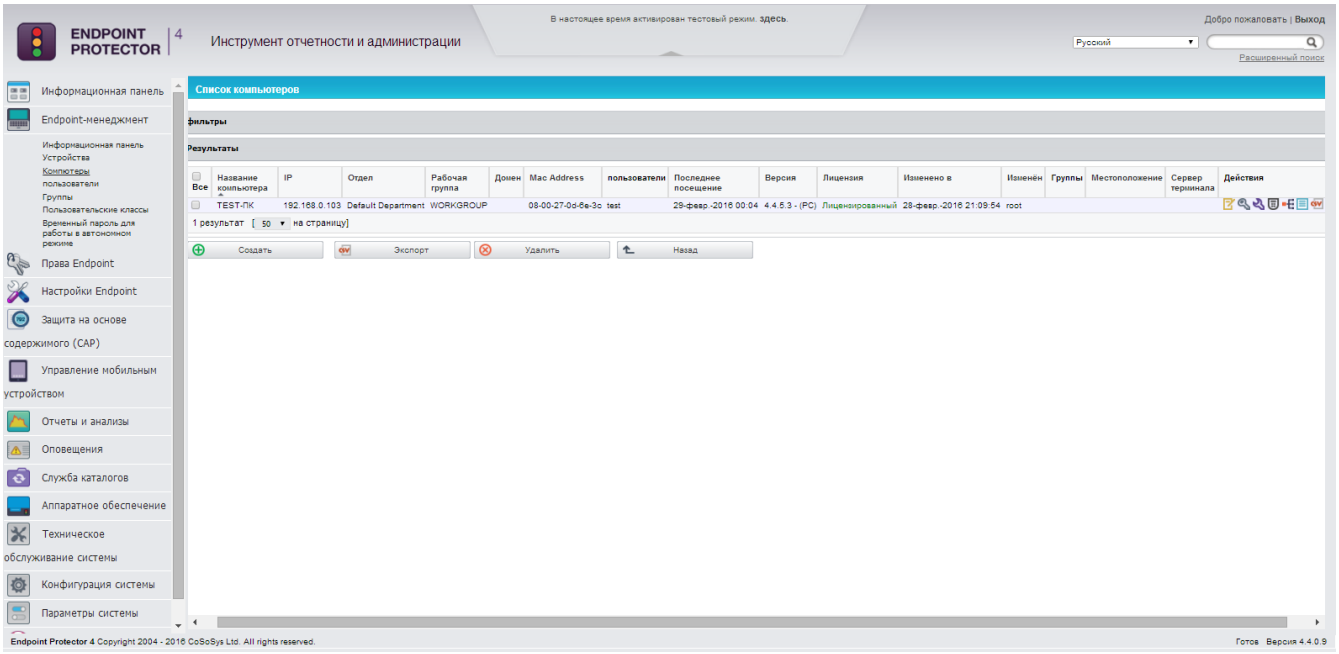
Раздел Endpoint Management предоставляет функции по управлению контролем устройств. В данном разделе осуществляется управление правами доступа к устройствам на уровне компьютеров, пользователей и групп пользователей, отдельных устройств или глобальных настроек. При переходе к управлению устройствами в интерфейсе отображается всё известное аппаратное обеспечение, когда-либо подключавшееся к защищаемым компьютерам. По каждому устройству показана подробная информация о дате, времени и месте подключения, а также данные о марке, модели и типе устройства.

Рисунок 7. Перечень известных устройств в CoSoSys Endpoint Protector



При переходе в раздел управления компьютерами открывается интерфейс со списком защищаемых рабочих станций и серверов. Из данного окна можно осуществить переход к управлению правами доступа контроля устройств, настройкам работы агента, а также в другие разделы панели управления.

Рисунок 8. Список компьютеров в CoSoSys Endpoint Protector

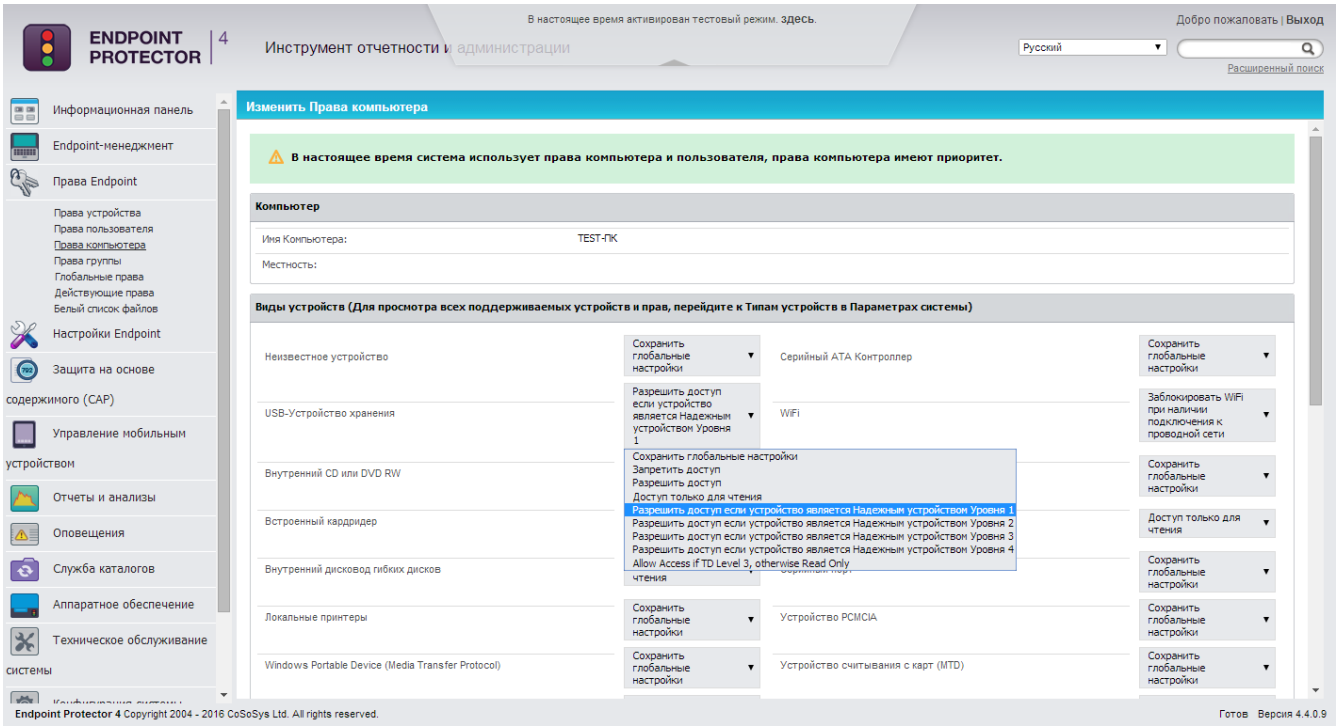


Политики контроля устройств настраиваются на уровне классов устройств, моделей или отдельно взятого устройства. Для каждого из классов аппаратного обеспечения можно разрешить или запретить подключение, и дополнительно для отдельных видов устройств существуют специальные настройки. Для устройств ввода-вывода можно указать режим «только чтение» и разрешить подключение без возможности произвести запись. Для беспроводных соединений можно включить режим работы только при условии отсутствия проводного подключения. Для съемных накопителей можно ограничить доступ в зависимости от надежности устройства (Trusted Device Level). Уровни надежности предустановлены в продукте по маркам и моделям устройств и считаются следующим образом:

- 1 уровень — любой flash-накопитель, зашифрованный с помощью EasyLock;
- 2 уровень — устройства, защищенные с помощью встроенного программного шифрования или с биометрической аутентификацией (устройства UT169, UT176, AT1177 и Trek ThumbDrive);
- 3 уровень — устройства, защищенные с помощью аппаратного шифрования (модели Verbatim: V-Secure, Secure Data USB Drive, модели Kanguru: Defender Elite, Elite 30, Elite 200, Defender Elite 2000, Flashtrust, устройства IronKey Secure Drive и Buffalo Secure Lock, а также устройства, защифрованные при помощи Bitlocker или FileVault 2);
- 4 уровень — устройства, защищенные с помощью аппаратного шифрования и прошедшие процедуру сертификации (устройства Stealth MXP Bio и SafeStick BE).

Перечень моделей и устройств, подпадающих под определенные уровни доверия, устанавливается CoSoSys и может пополняться при общем обновлении системы.

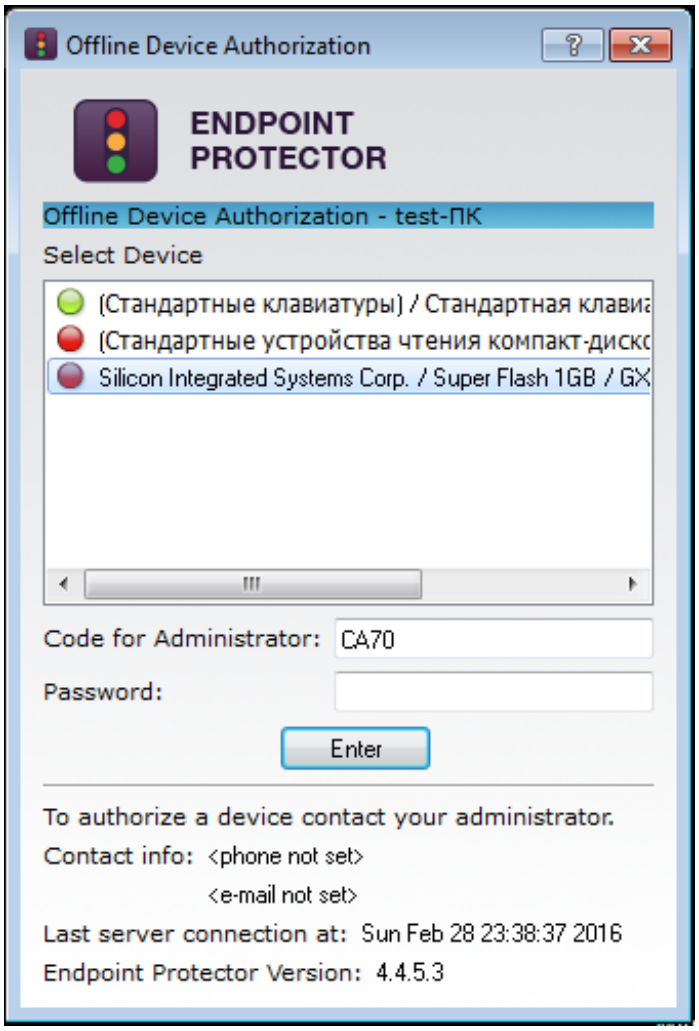
Рисунок 9. Управление политикой контроля устройств для компьютера в CoSoSys Endpoint Protector

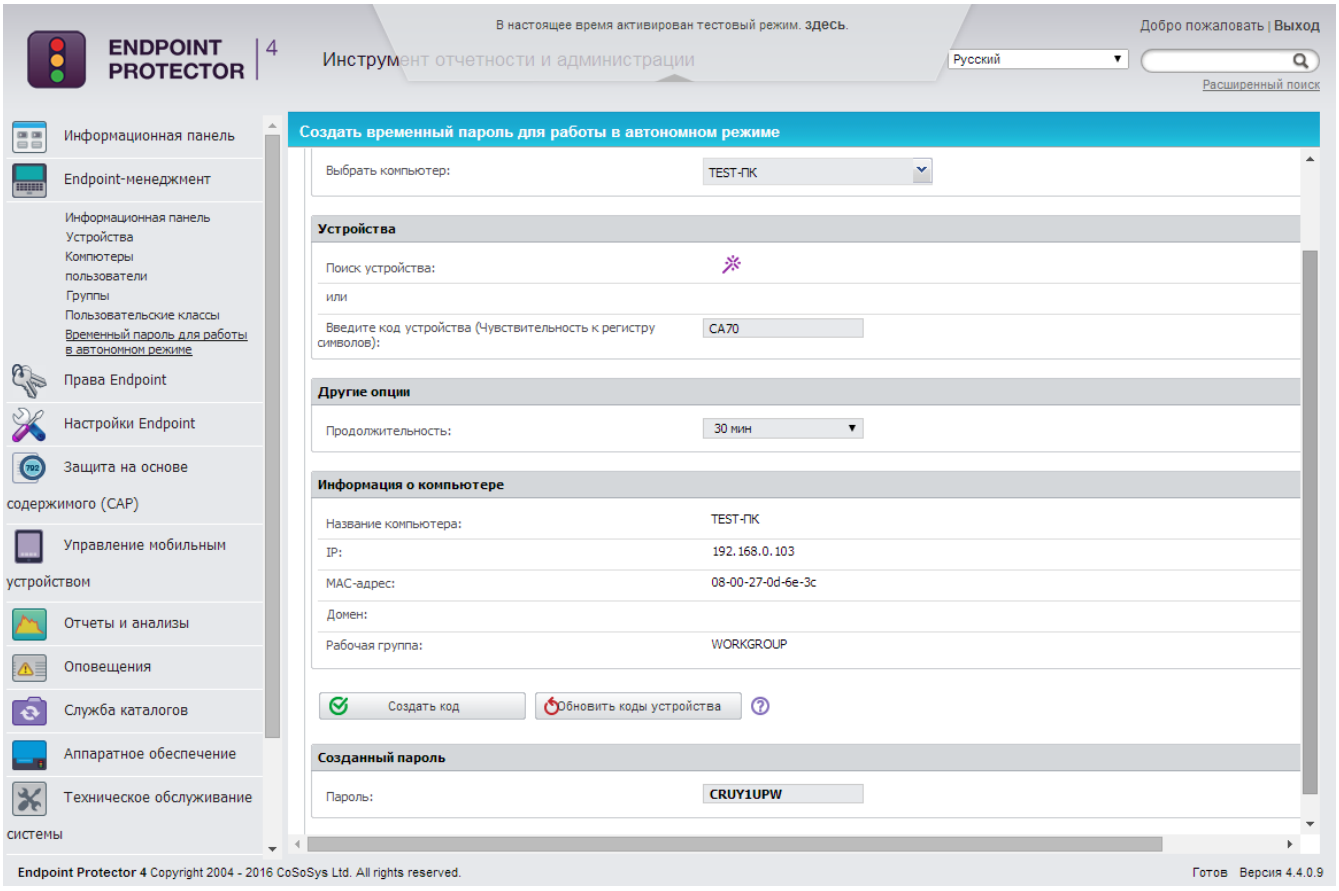


Раздел «Временный пароль для работы в автономном режиме» позволяет разрешить работу с устройством для компьютера, который не подключен к сети. Для получения доступа пользователь на защищаемом компьютере открывает интерфейс CoSoSys Endpoint Protector из панели задач, находит в списке нужное устройство и передает его код администратору системы. Администратор системы выбирает из списка компьютер, задает код устройства, указывает максимальное время работы, после которого доступ снова будет закрыт, и получает временный пароль. Когда пользователь укажет пароль на своем компьютере, устройство сразу же будет подключено.

Рисунок 10. Интерфейс пользователя CoSoSys Endpoint Protector для запроса доступа к устройству

Рисунок 11. Генерация временного пароля для доступа к устройству в CoSoSys Endpoint Protector

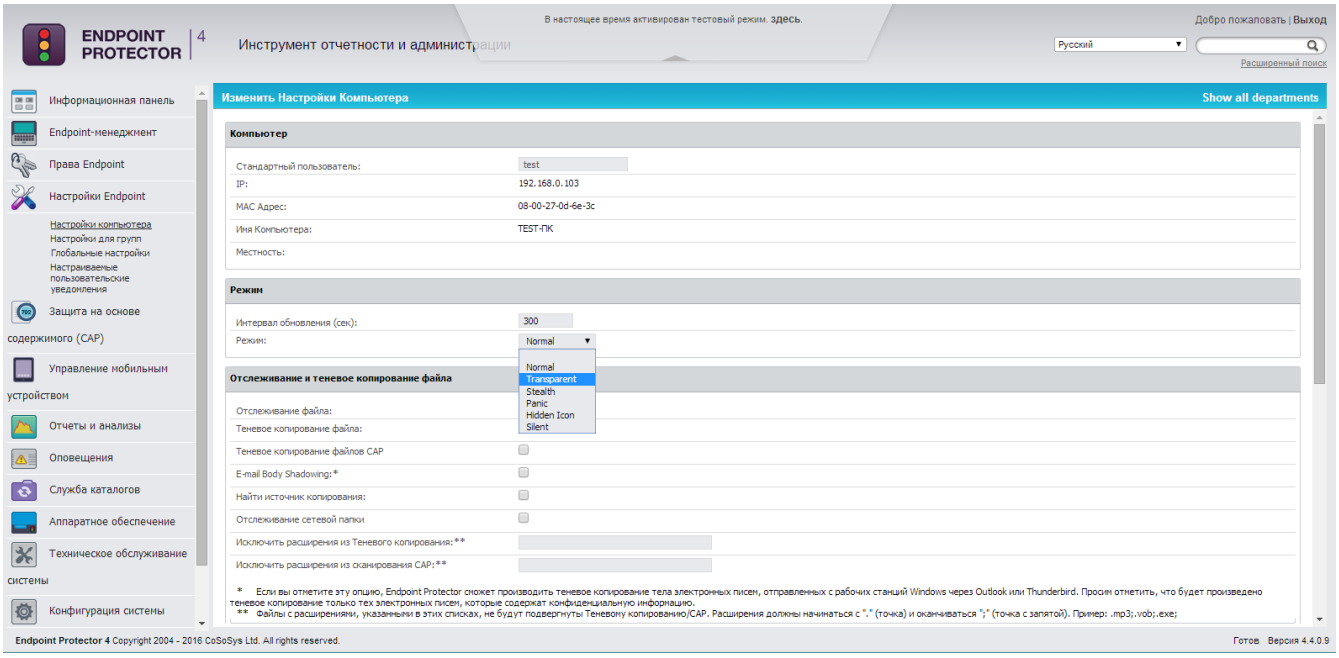




Раздел «Права Endpoint» в основном дублирует раздел «Endpoint-менеджмент» и предназначен также для конфигурирования политик контроля устройств. Из недоступного в предыдущем разделе тут присутствует ссылка для управления глобальными правами доступа, интерфейс управления белым списком файлов, а также раздел «Действующие права», в котором можно определить, какие права доступа применяются для конкретной связки пользователь-компьютер-устройства, и, таким образом, разобраться в наложении прав доступа для разных классов субъектов и объектов.

В разделе «Настройки Endpoint» осуществляется конфигурирование общего поведения системы и параметры работы отдельных агентов. К таким параметрам относится режим работы агента, опции теневого копирования, параметры подключения к серверу и другие настройки.

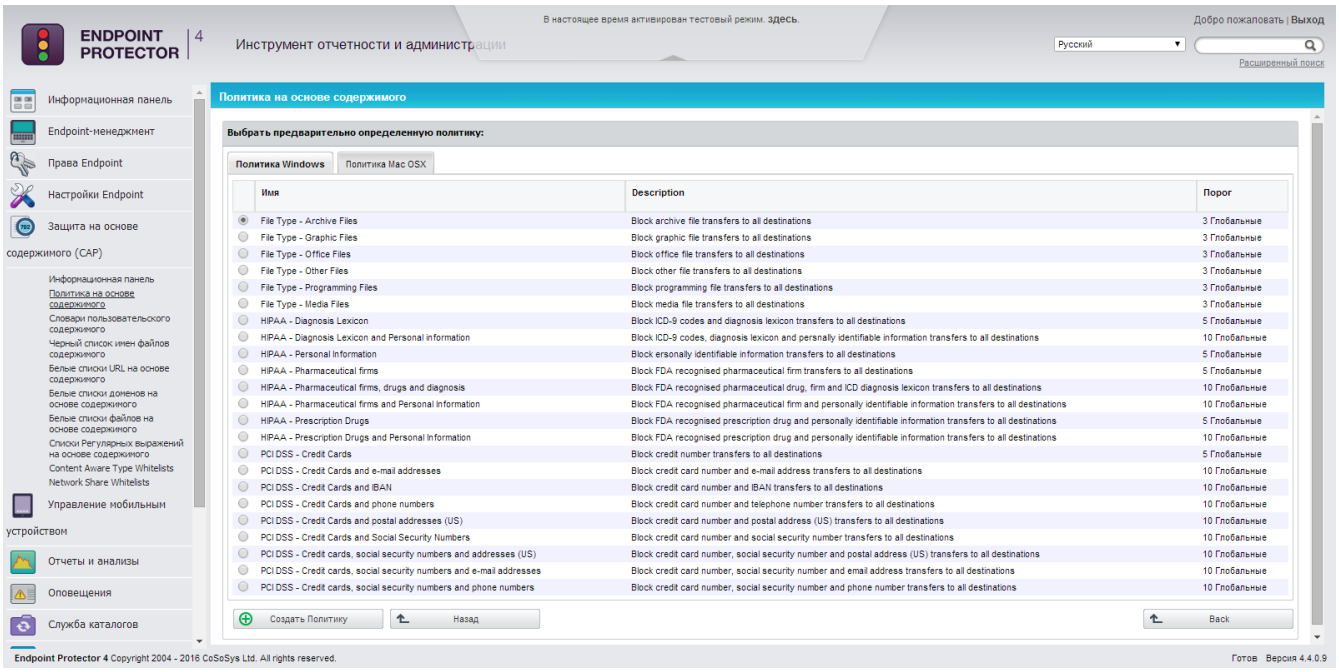
Рисунок 12. Настройки агента в CoSoSys Endpoint Protector



Все настройки контентного анализа собраны в разделе «Защита на основе содержимого». В отдельном разделе открывается информационная панель, похожая на интерфейс обзора системы, но отражающая события и состояние только контекстных детекторов.

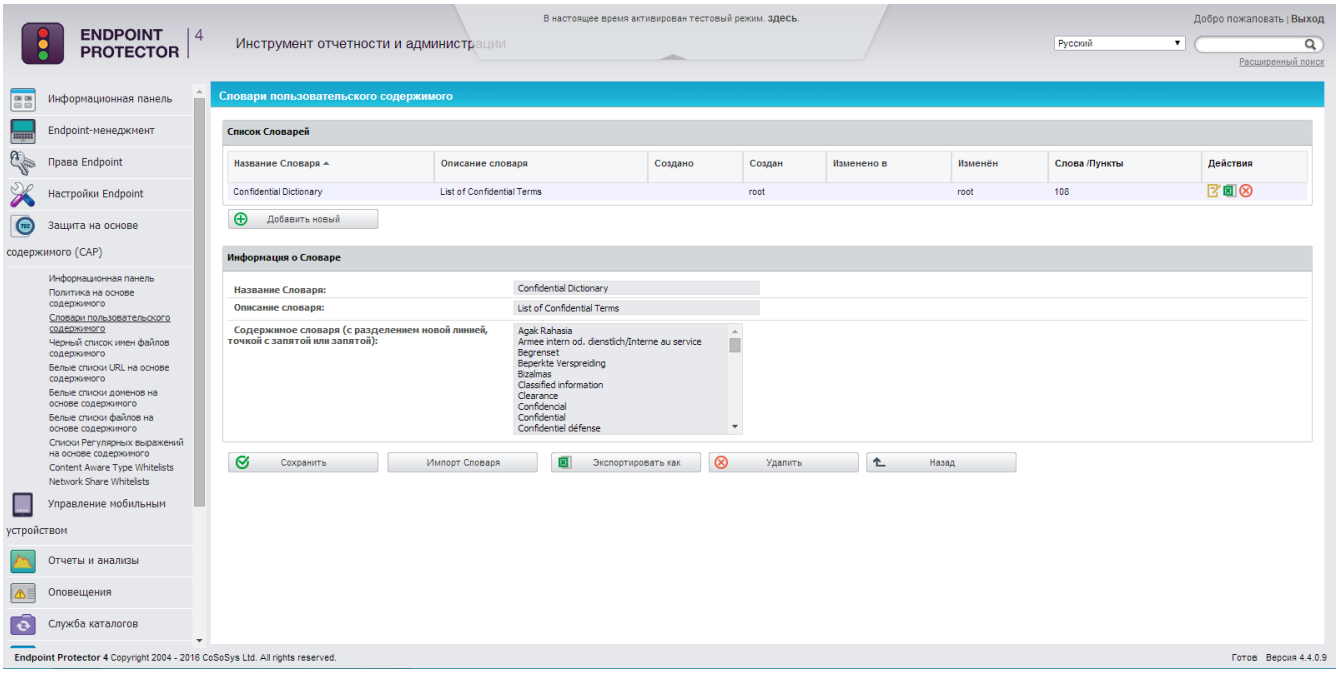
Настройка политик защиты на основе содержимого выполняется из нескольких разделов, пункт меню «Политика на основе содержимого» содержит возможность выбора различных предустановленных типов информации — на основе расширений файлов и шаблоны по стандартам HIPAA и PCI DSS.

Рисунок 13. Выбор шаблонов политик на основе содержимого в CoSoSys Endpoint Protector



Пользовательские ключевые слова и фразы, которые будут детектироваться в сетевом трафике и отчуждаемых файлах, задаются в разделе словарей. Каждый словарь представляет собой отдельный элемент, содержащий название, описание и перечень ключевых фраз.

Рисунок 14. Настройка словарей контентного анализа в CoSoSys Endpoint Protector



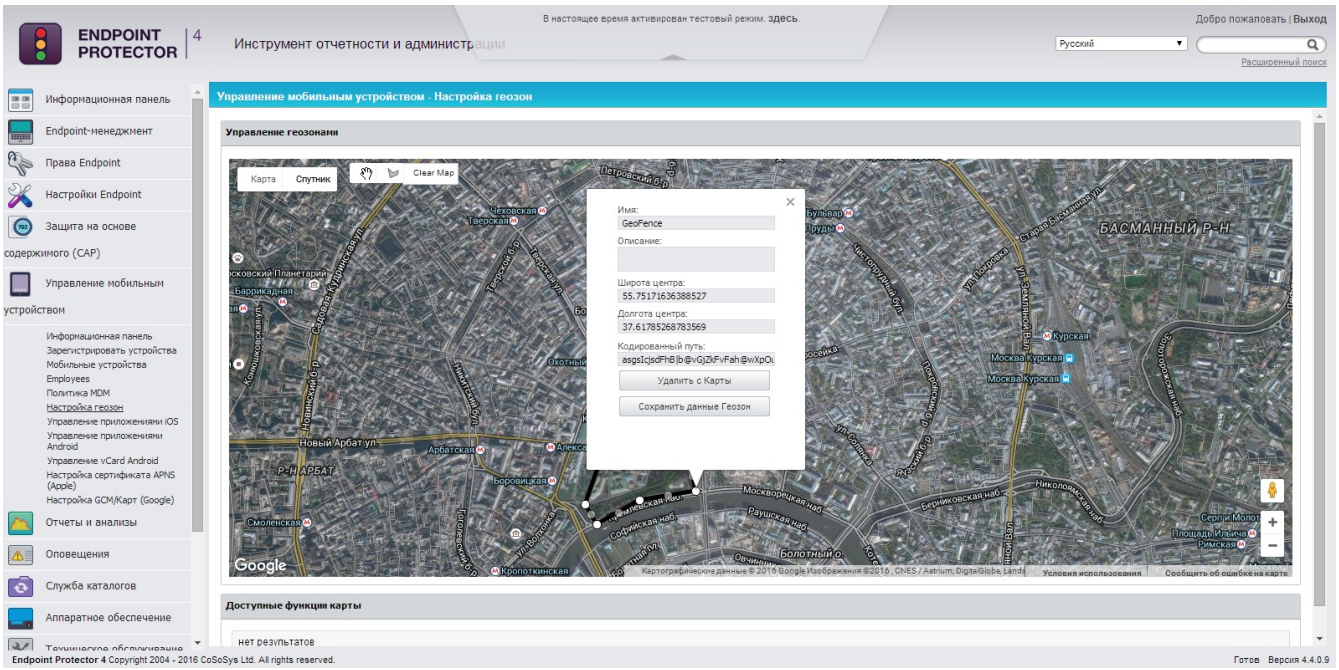
Отдельно настраиваются черные списки имен файлов, которые будут блокироваться всегда, белые списки файлов и веб-сайтов, для которых не применяется запрет, и дополнительные конфигурации политик. Из

дополнительных функций стоит отметить возможность задания регулярных выражений, которые могут дополнять пользовательские словари, однако разобраться с механизмом задания регулярных выражений для неподготовленного администратора будет сложно.

Управление защитой мобильных устройств (MDM) также вынесено в отдельный раздел со своей информационной панелью и набором политик безопасности. С помощью интерфейса CoSoSys Endpoint Protector можно осуществить регистрацию и контроль защищаемых устройств, определить их местоположение и активировать удаленные команды, такие как блокировка и очистка данных.

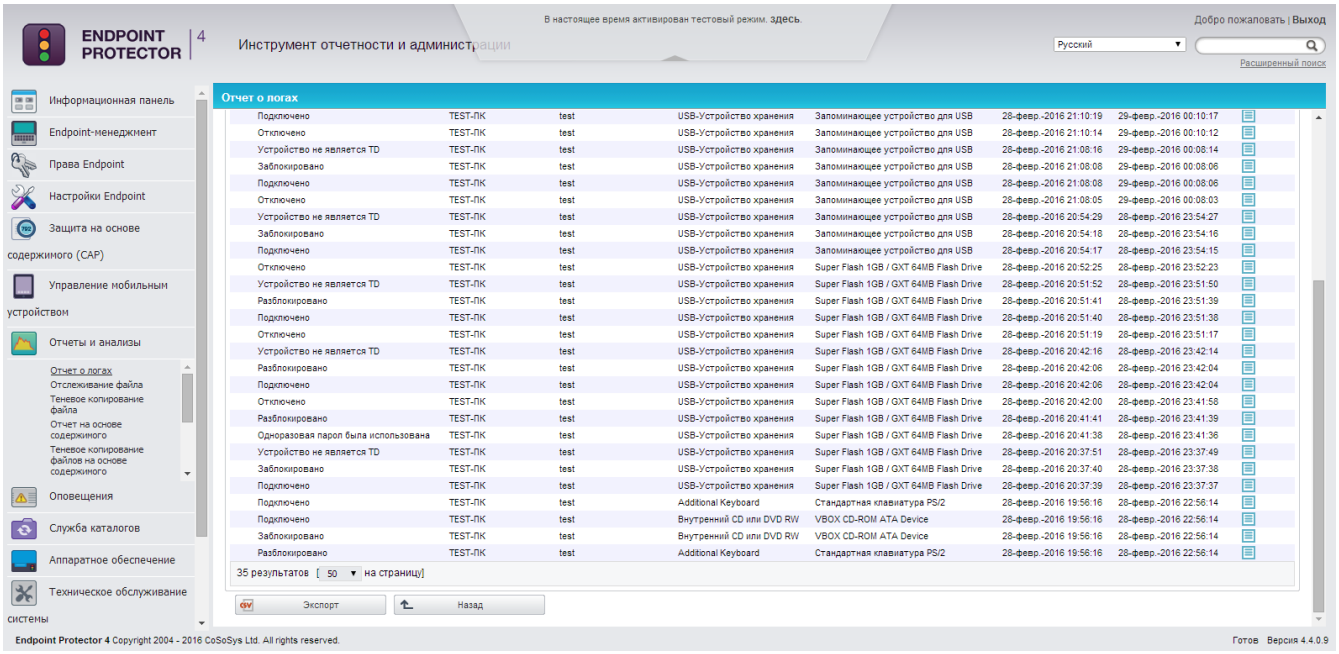
Политики защиты мобильных устройств могут привязываться к географическим зонам, которые задаются в удобном интерфейсе, использующем карты Google. Привязка политик к геозонам позволяет обеспечить разные настройки блокировок для мобильных устройств при их нахождении на определенной территории.

Рисунок 15. Управление геопривязкой политик контроля мобильных устройств в CoSoSys Endpoint Protector



Работа с аудитом и событиями производится в разделе «Отчеты и анализ». Возможно просматривать все события системы, в том числе доступен аудит в разрезе компьютеров, пользователей, устройств и отдельных файлов. Дополнительные отчеты содержат информацию о теневых копиях, действиях администраторов в системе и онлайн-активности в защищаемой сети. Кроме того, в интерфейсах «Активные компьютеры» и «Активные пользователи» можно в режиме реального времени увидеть список включенных компьютеров и авторизованных пользователей.

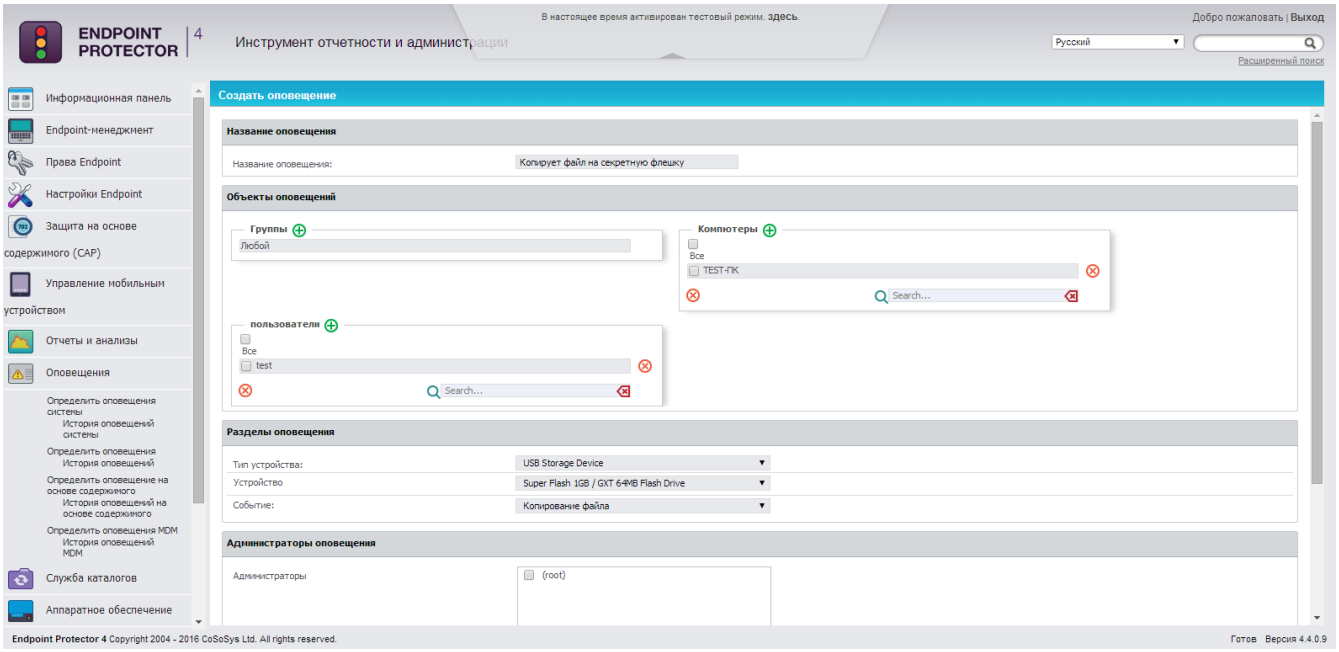
Рисунок 16. События журнала аудита CoSoSys Endpoint Protector



К подборкам событий можно применить различные правила фильтрации и сортировки. В продукте нет готовых отчетов и общей аналитики, поэтому обработка результатов выполняется только во внешних программах. Для этого выбранные события экспортируются в виде CSV-файла, с которым можно работать как с электронными таблицами.

В продукте CoSoSys Endpoint Protector реализована система оперативных уведомлений. Любые события, происходящие в системе, можно поставить на оперативный контроль. В разделе «Оповещения» находится четыре группы тревог — системные, контроля устройств, защиты на основе содержимого и защиты мобильных устройств. Интерфейс всех разделов унифицирован — в каждом из них может создаваться произвольное число условий для генерации оповещений. Указывается источник события, его тип, привязывается пользователь, компьютер или устройство, и при дальнейшем появлении в системе событий, подпадающих под фильтр, выбранные администраторы получают оповещение.

Рисунок 17. Создание фильтра для оповещения в CoSoSys Endpoint Protector



Остальные разделы предназначены для выполнения разовых служебных задач:

- «Служба каталогов» — управление импортом и синхронизацией учетных записей с Active Directory;
- «Аппаратное обеспечение» — информация о сервере CoSoSys Endpoint Protector, управление сетевыми настройками сервера и конфигурирование интеграции с SIEM-системами;
- «Техническое обслуживание системы» — служебные задачи по созданию резервных копий настроек и журналов, а также по их восстановлению;
- «Конфигурация системы» — управление программным обеспечением, загрузка дистрибутива агента, удаленное обновление и удаление клиентского ПО, работа с EasyLock, управление административными учетными записями, настройки системы и лицензирование;
- «Параметры системы» — управление типами устройств, возможными правами доступа и регистрацией событий;
- «Поддержка» — ссылки на документацию и онлайн-форма отправки запроса в техническую поддержку CoSoSys.

Выводы

Продукт CoSoSys Endpoint Protector является многофункциональной хостовой DLP-системой, которая пользуется спросом на международном рынке. Появление нового игрока на российском рынке всегда идет на пользу отрасли, конкуренция подталкивает производителей к усилению собственной разработки и поиску новых уникальных идей. Особенно когда появляется сильный международный игрок, решение которого не уступает мировым и российским конкурентам.

К сильным сторонам продукта можно отнести многоплатформенность (агент работает не только на Windows, но и на Mac OS и Linux), легкость установки и настройки, гибкость в управлении политиками на уровне устройства, пользователя, компьютера и сети, подробное протоколирование всех действий и большой набор дополнительных функциональных возможностей.

CoSoSys Endpoint Protector ориентирован не только на крупный, но и средний и малый бизнес и идеологически развивается как максимально простой в настройке и использовании. Поэтому некоторых функций, привычных для «тяжелых» корпоративных DLP-систем, в нем нет. В частности, несмотря на наличие ряда функций по анализу передаваемого трафика и отчуждаемой информации, в продукте не реализована технология цифровых отпечатков, он не умеет определять лексические и технические модификации конфиденциальных данных и не поддерживает функции распознавания текста на изображениях и определения запароленных архивов. Однако в большинстве небольших компаний эти функции едва ли будут востребованы.

При изучении продукта CoSoSys Endpoint Protector заметно сильное влияние различных международных и национальных стандартов по защите информации: есть разделение внешних накопителей по уровням надежности, продукт обладает сертификатом соответствия по «Общим критериям», в маркетинговых материалах делается особый упор на соответствие требованиям. Но при выходе на российский рынок хочется видеть в продукте адаптацию под выполнение российских нормативных требований в сфере ИБ, которые во многом отличаются от международных (разработчики планируют добавить готовые шаблоны для российских типов персональных данных в 2016 году). Также продукту явно не хватает сертификации на соответствие требованиям отечественных регуляторов.

Несмотря на выявленные недостатки, можно ожидать, что в будущем разработчики будут активно трудиться над решением. Продукт развивается, регулярно выходят новые версии, которые привносят множество улучшений. Кроме того, CoSoSys Endpoint Protector обладает функциями автоматического применения обновлений — оно незаметно для пользователей и администраторов, что является дополнительным аргументом в пользу этого решения для внедрения.

Достоинства:

- Поддержка интеграции с Active Directory, SIEM-системами и средством шифрования EasyLock.
- Полная локализация продукта на русский язык.
- Большой набор поддерживаемых агентом операционных систем (включая Mac OS и Linux).
- Наличие встроенных функций по контролю мобильных устройств.
- Гибкие настройки оповещения администраторов.
- Встроенное шифрование.
- Частые обновления продукта и прозрачные механизмы применения новых версий.

Недостатки:

- Отсутствие сертификатов соответствия, выданных отечественными регуляторами.
- Слабые возможности контентного анализа.
- Отсутствие полноценных отчетов с графиками, статистикой и корреляцией между событиями аудита.

Реестр сертифицированных продуктов »

Присоединяйтесь к нам!