Визитка

ВЛАДИМИР БЕЗМАЛЫЙ
Kaspersky Certified Trainer Microsoft Security Trusted Advisor cybercop@outlook.com

Ревизия аппаратного
и программного обеспечения корпоративной сети

Казалось бы, бессмертному произведению Гоголя уж скоро 200 лет, а фраза «К вам едет ревизор!» до сих пор вгоняет в ступор многих руководителей ИТ. Причина проста: в бесконечной круговерти дел они зачастую утрачивают контроль над элементарными вещами. То же относится и к департаменту информационных технологий. В этой статье мы рассмотрим элементы проведения ревизии с помощью продукта Kaspersky Endpoint Security 11.

Уже давно стоит принимать во внимание, что KESB 11 – инструмент для работы не только администратора безопасности, но и ИТ-аналитика, впрочем как и аналитика ИБ.

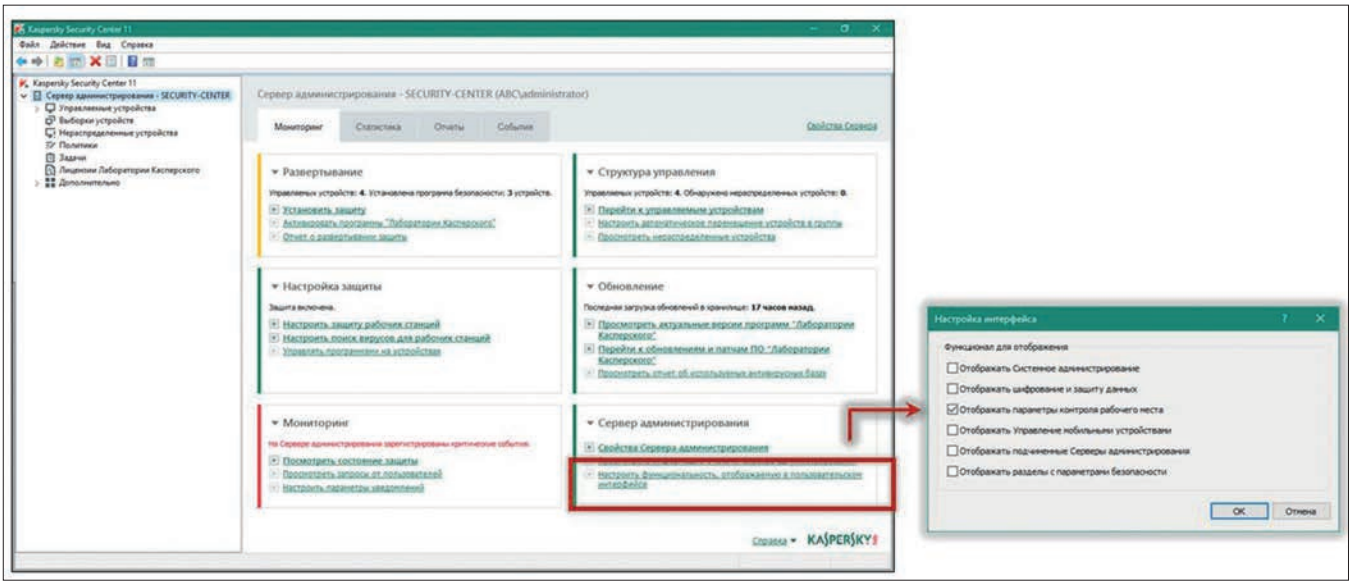
Не знаю как у вас обстоят дела с инвентаризацией установленного на рабочих станциях ПО, но на моей памяти вопрос об этом обычно вгоняет руководителя ИТ, я уже не говорю о руководителе службы технической поддержки, просто в ступор. Как правило, в ответ вы услышите либо нечто невнятное, либо вообще ничего. Чаще всего вас просто пошлют в бухгалтерию за результатами инвентаризации.

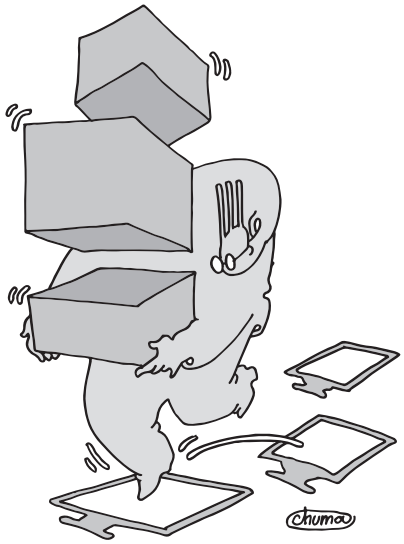
Причина тоже понятна. Программное обеспечение часто устанавливается службой технической поддержки, администраторами, а в случае, если пользователь имеет права локального администратора, то и самим пользователем. Естественно, порядка при таком раскладе просто не может быть. Так как же правильно ответить на вопрос об имеющемся в наличии программном обеспечении?

Методы инвентаризации аппаратного, а зачастую и программного обеспечения чаще всего сводятся к элементарному, но ужасно неудобному и затратному «встали и побежали». Именно так рекомендуют проводить инвентаризацию в статье «Идентификаторы для инвентаризации ИТ оборудования это легко и просто» [1]. Или в статье того же автора «Простой и правильный учёт оборудования» [2]. На мой взгляд, такой подход, безусловно, может существовать. Но давайте все же задумаемся. Мы ведь с вами инженеры, не так ли?

Для точного ответа на предприятии необходимо проводить инвентаризацию установленного программного обеспечения. Увы, это совсем не быстрый процесс, даже если вы сумеете его правильно автоматизировать. Кроме того, нужно учесть,

Рис. 1. Отображение Контролей в MMC-консоли





Методы инвентаризации аппаратного, а зачастую и программного обеспечения чаще всего сводятся к элементарному, но ужасно неудобному и затратному «встали и побежали»

что этот процесс требует значительных ресурсов и довольно сильно загружает вашу корпоративную сеть, а значит, вам придется проводить его по отдельным участкам.

Компоненты контроля требуют лицензию уровня KESB Стандартный и устанавливаются по умолчанию.

В MMC-консоли в политике Kaspersky Endpoint Security 11.1 по умолчанию не отображаются настройки *Шифрования и компонентов Контроля*. Включить отображение этих настроек можно в главном окне Консоли по ссылке: *Настроить функциональность, отображаемую в пользовательском интерфейсе*:

Учтите, что при использовании Web Console никаких дополнительных настроек интерфейса не требуется. Весь необходимый функционал доступен сразу.

Стоит отметить, что компоненты контроля по умолчанию включены в свойствах пакета Kaspersky Endpoint Security 11.1, который создается автоматически при установке Сервера администрирования.

Единственный нюанс – при установке на серверную операционную систему не все компоненты будут там установлены.

Задача инвентаризации

По умолчанию данная задача не создается. То есть в список исполняемых файлов попадают только те, которые запускались на компьютерах с работающим компонентом Контроль программ. Может пройти немало времени, пока та или иная программа станет доступной через список на Сервере администрирования. Чтобы не ждать, нужно создать и запустить задачу инвентаризации.

В результате выполнения данной задачи будут найдены файлы, запускаемые редко или нерегулярно.

Крайне важно выполнять регулярно задачу инвентаризации эталонных компьютеров.

Данная задача может быть групповой или для набора компьютеров. При стандартных настройках поиск файлов выполняется в каталогах:

- *%SystemRoot%*
- *%ProgramFiles%*
- *%ProgramFiles(x86)%*

Список проверяемых папок можно изменить или дополнить. Информация о найденных файлах поступает на Сервер администрирования и доступна через Web Console во вкладке Операции – Программы сторонних производителей – Исполняемые файлы, либо в контейнере «*Исполняемые файлы сервера администрирования*». С помощью данной задачи вы можете обнаружить исполняемые файлы внутри архивов и установочных пакетов.

Следует учесть, что поиск исполняемых файлов сопровождается вычислением их контрольных сумм, что, естественно, снижает быстродействие компьютеров.

Для экономии ресурсов можно отключить проверку файлов, которые не изменялись (*Проверять только новые и измененные файлы*). Информация об изменениях поступает в рамках технологии iSwift и не требует почти никаких вычислений.

В результате продолжительной работы вы получите полный список установленного в вашей компании программного обеспечения, причем не только по названию и производителю, но и с учетом используемых версий. Я не удивлюсь, если этот список вас немало озадачит, и более того, скорее всего, выяснится, что далеко не все установленное у вас программное обеспечение вам действительно необходимо.

Рекомендуется выполнять задачу в нерабочее время.

Реестр программ

Основная цель Реестра программ – предоставить администратору информацию об установленных в сети приложениях. Используя эту информацию, администратор видит, на каких компьютерах установлено то или иное приложение. Например, если в сети обнаружился интернет-браузер старой версии, администратор может принудительно обновить версию браузера на всех компьютерах. Также Реестр

Реальная картина состояния аппаратного обеспечения чаще всего отсутствует, так как для ее формирования нужно приложить немало усилий

программ может использоваться для отслеживания появления на компьютерах пользователей запрещенного в компании программного обеспечения. Например, в компании может быть запрещено использование IM-мессенджеров.

Обнаружив в списке запрещенную программу, администратор может принять меры по ее удалению.

Список приложений

Список установленных приложений отображается в контейнере ***Реестр программ*** узла ***Управление программами.*** Сбор данных осуществляется ***Агентом администрирования***. При этом информация берется из веток реестра, формирующих в операционных системах список Программы и компоненты (в старых версиях операционных систем – ***Установка и удаление программ***). В зависимости от разрядности отслеживаются ветки реестра:

> *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall*

> *HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall*

Сканирование веток реестра происходит при старте Агента администрирования или при изменениях в ветке реестра.

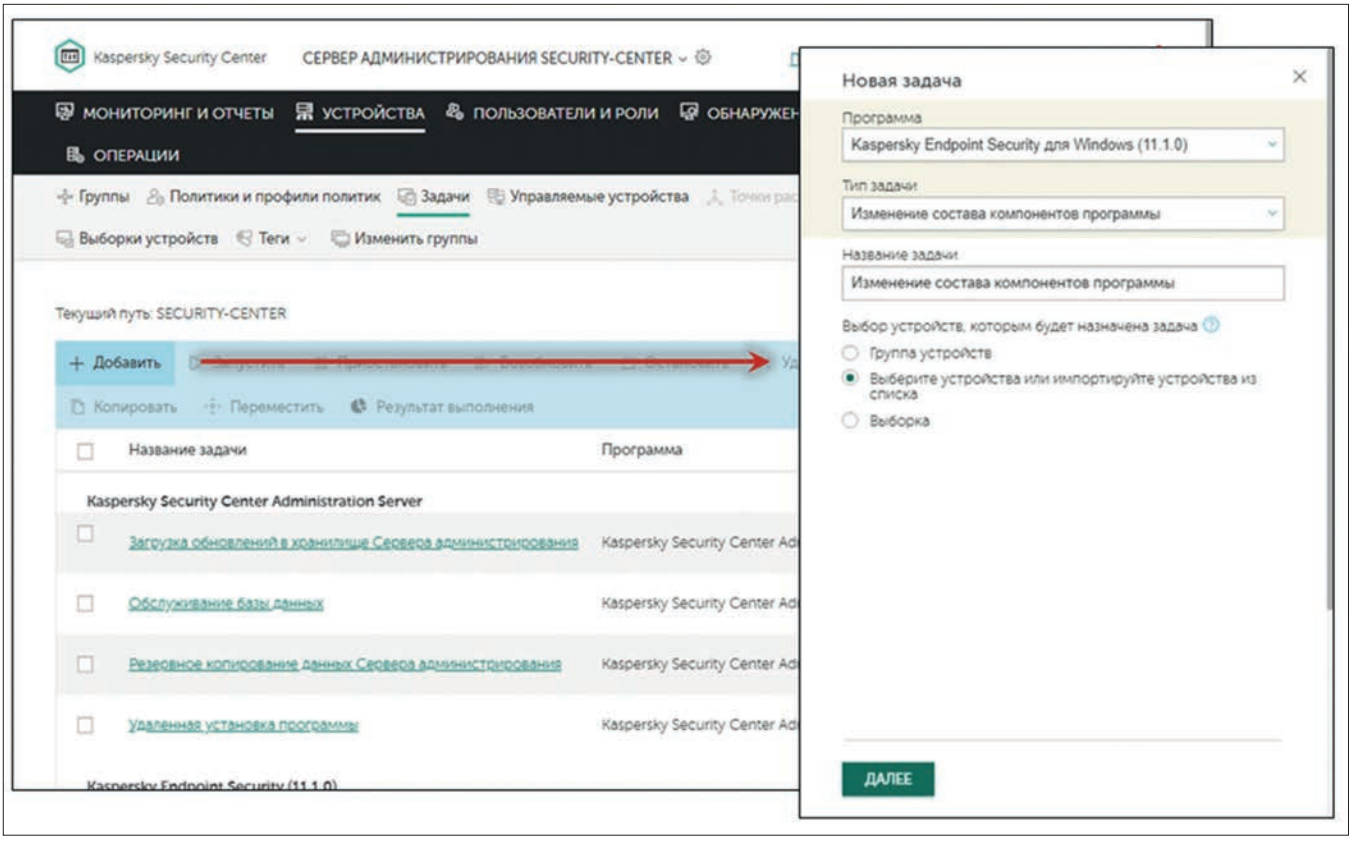
За передачу информации на Сервер администрирования отвечает опция ***Информация об установленных программах*** в свойствах политики Агента администрирования. По умолчанию опция включена, т.е. Сервер получает информацию об установленных приложениях, при желании ее можно отключить.

В контейнере ***Реестр программ*** есть возможность задать конкретные приложения, для которых будут публиковаться события об установке программы на клиентском компьютере. Список наблюдаемых приложений задается в свойствах контейнера Реестр программ в секции ***Наблюдаемые программы***. Чтобы получать уведомления об установке/удалении наблюдаемых программ, нужно указать тип уведомления (по почте, по SNMP и т.д.) для события ***Установлена наблюдаемая программа / Удалена наблюдаемая программа*** в политике Агента администрирования.

Ревизия аппаратного обеспечения

На самом деле ревизия аппаратного обеспечения в департаменте ИТ, как правило, если и проводится, то достаточно формально. В лучшем случае учитывается объем оперативной памяти и свободное место на жестком диске. Реальная же картина состояния аппаратного обеспечения чаще всего отсутствует, так как для ее формирования нужно приложить немало усилий.

Рис. 2. Создание задачи инвентаризации



От редакции

Kaspersky Endpoint Security – очень неплохой, но не единственный инструмент, при помощи которого можно провести инвентаризацию ПО, в том числе и на предмет поиска уязвимостей.

Например, существуют облачные решения, например, Complaud, разрабатываемый в России, который позволяет выполнить поиск уязвимостей, проверку на соответствие требованиям безопасной конфигурации (Compliance) устройств (Linux, MS Windows) и выполнить инвентаризацию ПО (страничка продукта: https://complaud.com/)

Однако мир ИТ-безопасности в целом очень многогранен. Поэтому выбор инструментов в конечном итоге зависит от специфики бизнеса и ИТ-инфраструктуры. И чем с большим числом продуктов мы познакомимся, чем больше интересных материалов прочитаем, тем эффективней могут быть наши решения

В любом случае решающую роль играют опыт и практика, а также эрудиция и уровень подготовки специалиста по безопасности..

В действительности эта задача довольно просто решается с помощью Kaspersky Endpoint Security для бизнеса. Единственное, что вам потребуется, – это лицензия на использование компонента System Management, которая входит в состав Kaspersky Endpoint Security для бизнеса уровня Расширенный.

Основная задача реестра аппаратного обеспечения – предоставить администратору информацию об аппаратном обеспечении компьютера. Используя эту информацию, администратор может находить компьютеры, на которых мало оперативной памяти или недостаточный объем жесткого диска. Также администратору будет полезна информация, например, о компьютерах со старой версией операционной системы.

Сведения об аппаратном обеспечении на клиентских компьютерах собирает агент администрирования; он передает ее серверу. Просмотреть информацию об аппаратном обеспечении можно в свойствах каждого компьютера в разделе «Информация о системе, Реестр оборудования».

Для получения сводной информации об аппаратном обеспечении на всех клиентских компьютерах необходимо воспользоваться шаблоном отчета – отчетом о реестре оборудования. По каждому компьютеру в таблице отображается детальная информация, а также есть сводка по всем устройствам. В отчете, как и в свойствах компьютера, отображается такой немаловажный параметр, как свободное место на диске.

Утилита глобального поиска компьютеров на сервере администрирования позволяет искать компьютеры по наличию устройств определенного типа, производителя, по объему оперативной памяти или размеру диска, а также по версиям драйверов устройств и еще ряду параметров; также можно искать по версии операционной системы. Это делается на закладках «Оборудование» и «Операционная система». Для этих же целей можно использовать окно «Выборки компьютеров».

Для получения сводной информации об аппаратном обеспечении на всех клиентских компьютерах необходимо воспользоваться шаблоном отчета – Отчет о реестре оборудования. По каждому компьютеру в таблице отображается детальная информация, а также есть сводка по всем устройствам с указанием количества каждого. В отчете, как и в свойствах компьютера, отображается немаловажный параметр – свободное место на диске.

Утилита глобального поиска компьютеров на Сервере администрирования – Поиск, позволяет искать компьютеры по наличию устройств определенного типа, производителя, по объему оперативной памяти или размеру диска, а также по версиям драйверов устройств и еще ряду параметров, также можно искать по версии операционной системы. Это делается на закладках Оборудование и Операционная система.

Таким образом вы сможете вовремя понять, на каких компьютерах нужно обновить драйверы или заменить определенные компоненты. А, возможно, и заменить компьютер целиком. Главное, что у вас будет постоянно обновляемый реестр аппаратного обеспечения.

Реестр оборудования

Однако помимо компьютеров в сети существует масса иного оборудования. Можно ли осуществить и его ревизию? Оказывается – да. Для этого служит составление реестра оборудования.

Реестр оборудования – это централизованный реестр всех корпоративных устройств, который может использоваться для проведения инвентаризации и предоставления отчетности. Также на основании информации из реестра, администратор может делать выборки и накладывать NAC-политики.

Информация об обнаруженных устройствах отображается в контейнере ***Оборудование*** узла ***Хранилища***. Стоит учесть, что по умолчанию, узел не отображается в интерфейсе, поэтому настройки интерфейса нужно предварительно изменить.

При этом данные об устройствах в сети поступают из различных источников:

- *Подсистема обнаружения компьютеров* – все те же методы, которые используются для обнаружения компьютеров в Kaspersky Security Center: сканирование сети Microsoft, сканирование Active Directory, сканирование IP-подсетей. Кроме компьютеров, таким образом, могут быть обнаружены сетевые принтеры и другие сетевые устройства. Фактически, устройства, обнаруженные при сканировании сети и отображаемые в узле ***Нераспределенные устройства***, дополнительно передаются в реестр оборудования и отображаются в узле ***Хранилища – Оборудование***
- *Подсистема NAC* – при помощи прослушивания широковещательных ARP и DHCP-запросов определяет список имеющихся в корпоративной сети устройств. Более детальная информация об обнаруженном устройстве определяется при помощи утилиты Nmap.
- *Агент администрирования* – дополняет информацию о найденных компьютерах данными из ***Реестра аппаратного обеспечения компьютера***, на котором он установлен
- *Управление мобильными устройствами* – передает информацию о мобильных устройствах, подключенных к Серверам мобильных устройств
- *Контроль устройств в составе Kaspersky Endpoint Security* – предоставляет информацию об устройствах, подключенных к клиентским компьютерам

В контейнере Оборудование могут отображаться устройства следующих типов:

- Компьютеры
- Мобильные устройства
- Сетевые устройства
- Периферийные устройства
- Сменные носители
- IP-телефоны
- Сетевые хранилища

Основным идентификатором для устройств, подключенных к сети, считается ***MAC-адрес***. Для мобильных устройств – идентификатор, переданный ***Сервером мобильных устройств***, для устройств, подключаемых к компьютеру – ***идентификатор устройства, переданный компонентом Контроль устройств***. Информация о новом устройстве отображается автоматически, после появления в корпоративной сети.

Обновление информации в контейнере ***Оборудование*** происходит раз в час. Если устройство не отображается автоматически, можно добавить его вручную. Делается это из контекстного меню контейнера Оборудование командой ***Новый – Устройство***.

Каждое устройство имеет огромное количество атрибутов, некоторые могут определяться автоматически, такие как MAC-адрес, версия операционной системы, аппаратные характеристики. Вместе с тем вручную вы можете добавить такие характеристики как инвентарный и серийный номера, владелец, местоположение и т.д. Для упрощения процедуры редактирования свойств весь список устройств с атрибутами можно экспортировать в Excel-файл, отредактировать его и импортировать обратно в ***Консоль администрирования***.

Помимо предустановленных атрибутов, администратор может создавать собственные, исходя из своих нужд. Делается это в свойствах контейнера ***Оборудование*** в разделе ***Пользовательские поля.***

Информация об устройствах в контейнере Оборудование может использоваться в условиях поиска при создании выборок компьютеров. В частности можно создавать выборки для поиска компьютеров по версии операционной системы, размеру оперативной памяти, размеру жесткого диска и т.д. Кроме того, администратор имеет возможность отслеживать историю изменений атрибутов устройства.

Каждое изменение сопровождается записью в журнал предыдущего состояния. Например, администратор изменил владельца и местоположение устройства, после сохранения изменений в журнале будет создана запись об изменениях. При автоматическом изменении атрибутов, например, поменялась версия операционной системы или изменились аппаратные характеристики устройства, также будет создана запись в журнале.

Журнал изменений атрибутов можно посмотреть из контекстного меню конкретного устройства по команде ***История изменения атрибутов***.

Таким образом, фактически вы сможете вести не только журнал текущего оборудования, а и журнал изменений вашего оборудования.

Но как быть, если со временем оборудование выходит из строя и просто списывается?

Для решения этой проблемы помимо атрибутов, каждому из устройств можно присвоить два статуса:

- *Корпоративное устройство* – используется как один из критериев для задания NAC-политики, т.е. устройства, имеющие статус ***Корпоративное устройство*** могут автоматически получать доступ в корпоративную сеть. По умолчанию статус присваивается вручную, но можно настроить автоматическое присвоение статуса для различных типов устройств. Настраивается это в свойствах контейнера ***Оборудование*** узла Хранилища. Устройства, добавленные вручную, получают статус Корпоративное устройство автоматически.
- *Устройство списано* – списанное устройство, удаленное из списка вручную может быть найдено повторно, чтобы избежать этого, необходимо присвоить устройству статус Устройство списано.

Для получения сводной информации обо всех устройствах сети необходимо воспользоваться новым шаблоном отчета – Отчет об оборудовании. По каждому устройству в таблице отображается детальная информация со всеми атрибутами. В отчете также можно использовать фильтр по атрибутам.

> Работа по инвентаризации аппаратного и программного обеспечения, с одной стороны, кажется довольно сложной и уж очень «нудной». Но с другой, хотелось бы напомнить, что построение безопасности всегда должно начинаться с аудита

Заключение

Работа по инвентаризации аппаратного и программного обеспечения, с одной стороны, кажется довольно сложной и уж очень «нудной». Но с другой, хотелось бы напомнить, что построение безопасности всегда должно начинаться с аудита. А разве может быть аудит ИТ и ИБ без осознания того, какими активами вы владеете? Безусловно, нет. Но кроме того, вам необходимо понимать что без проведения подобной инвентаризации вы никогда не сможете грамотно проводить обновление аппаратной составляющей и тем более обновлять программные средства третьих производителей. Впрочем, об обновлении программных средств мы поговорим в следующей статье. EOF

[1] Идентификаторы для инвентаризации ИТ оборудования это легко и просто https://habr.com/ru/post/205802/
[2] Простой и правильный учёт оборудования https://habr.com/ru/post/205862/
[3] В. Безмалый Ревизия программных средств https://www.osp.ru/winitpro/2016/04/13048959/
[4] Учебный курс KL 002.11 «Kaspersky Endpoint Security and Management»
[5] Учебный курс KL 302.10 «Kaspersky Endpoint Security and Management Масштабирование»

Ключевые слова: Kaspersky Endpoint Security, контроль программ, инвентаризация, инвентаризация программного обеспечения, инвентаризация аппаратного обеспечения, реестр оборудования.