Сетевой сканер безопасности XSpider 7.8.24

Инструкция по установке

2014

Порядковый № изменения	Подпись ответств. лица	Дата внесения изменения

Подп. и дата	
Инв. №	
Взам.	
Подп. и дата	
Инв. №	

ОГЛАВЛЕНИЕ

Порядковый № изменения	Подпись ответств. лица	Дата внесения изменения

Порядковый № изменения	Подпись ответств. лица	Дата внесения изменения

1. ТРЕБОВАНИЯ К СИСТЕМЕ

1.1. Требования к аппаратному и программному обеспечению

Данный раздел содержит информацию о том, какие требования к аппаратному и программному обеспечению предъявляются для развертывания сканера безопасности XSpider.

1.1.1 Требования к аппаратному обеспечению

Базовые требования к аппаратному обеспечению для XSpider определены в Табл. 1.

Табл. 1 Минимальные аппаратные требования к компонентам XSpider

Компонент	Процессор	Оперативная память	Жесткий диск
XSpider	PIV 1,6 ГГц	2 ГБ	5 ГБ

Разрешение монитора для установки и работы с системой должно составлять не менее 1280 x 1024 пикс.

Приведенные требования достаточны для установки системы, однако для работы в масштабных инсталляциях могут потребоваться дополнительные аппаратные ресурсы.

1.1.1.1. Процессор

При сканировании система не предъявляет дополнительных требований к центральному процессору.

Вычислительные процессы XSpider оптимизированы так, чтобы максимально использовать ресурсы сканирующего узла (т.е. узла, где расположен XSpider). В связи с этим существует прямая зависимость между увеличением тактовой частоты процессора и увеличением скорости сканирования. Однако наибольший прирост производительности дает использование нескольких процессоров или многоядерных решений. В Табл. 2 приведена зависимость скорости одновременного сканирования разного количества узлов от типа и количества процессоров компьютера, на котором установлен XSpider.

Табл. 2 Зависимость скорости сканирования (мин.) от количества процессоров

	Одноядерный	Двухъядерный	Два двухъядерных
1 узел	3-20	3-20	3-20
10 узлов	15-60	8-30	9-30
50 узлов	60-250	40-150	25-80
100 узлов	120-250	75-220	50-160

В таблице указан диапазон возможных значений, где границами является время сканирования стандартной рабочей станции Windows (Windows XP + Microsoft Office 2003) и сервера с большим количеством установленного программного обеспечения. При расчетах в зависимости от ситуации можно использовать среднее значение.

Таким образом, для увеличения скорости сканирования можно масштабировать процессорные мощности.

1.1.1.2. Оперативная память

Приведенные минимальные требования к ОЗУ (Табл. 1) достаточны для работы сканера XSpider в большинстве сетей. Однако в случае обработки результатов большого количества сканирований (например, при построении отчетов на основе данных из истории сканирования) может потребоваться дополнительный объем оперативной памяти. Пороговым значением является 300 узлов. В случае если сканер обслуживает более 300 узлов, рекомендуется устанавливать не менее 3 ГБ ОЗУ.

1.1.1.3. Жесткий диск

Требования к объему жесткого диска для сканера XSpider целиком зависят от количества сканируемых узлов и интенсивности сканирования. В Табл. 3 приведена информация о требуемом объеме дискового пространства сканера, обслуживающего различное количество узлов, при различной интенсивности сканирования.

Табл. 3 Требования к объему жесткого диска (МБ) из расчета на год в зависимости от частоты сканирования

	Ежедневно	Еженедельно	Ежемесячно
1 узел	360	55	12
10 узлов	3600	550	120
50 узлов	18000	2750	600
100 узлов	36000	5500	1200
1000 узлов	360000	55000	12000

Порядковый № изменения	Подпись ответств. лица	Дата внесения изменения

1.1.2 Программное обеспечение

Сканер XSpider разработан для функционирования на базе операционных систем линейки Windows. В настоящее время работоспособность системы была протестирована при использовании следующих ОС:

- Microsoft Windows XP SP 3 (x86) и старше;
- Microsoft Windows Server 2003 SP 2 (x86, x64) и старше;
- Microsoft Windows Vista SP 2 (x86,x64) и старше;
- Microsoft Windows Server 2008 SP2 (x86, x64) и старше;
- Microsoft Windows 7 (x86,x64) и старше;
- Microsoft Windows Server 2008 R2 (x64) и старше;
- Microsoft Windows 8 (x86,x64) и старше;
- Microsoft Windows Server 2012 (x64) и старше.

Внимание! Список совместимых систем постоянно расширяется. Для получения актуальной информации обратитесь в службу технической поддержки.

При выборе операционной системы следует учитывать, что при ряде проверок система XSpider интенсивно использует стек протоколов TCP/IP операционной системы. В связи с этим применение клиентских версий ОС (например, Windows XP) для проведения сканирования большого количества узлов неэффективно. В частности, уменьшается производительность сканера портов и ряда других механизмов.

Другим аспектом требующим внимания, является совместимость ОС с дополнительными программами, используемыми XSpider. Обязательными компонентами, без которых работа системы невозможна, являются:

- Microsoft Internet Explorer 7.0 и выше;
- Microsoft .NET Framework Version 3.5 SP1;
- Microsoft Runtime Libraries версии 9.0.30729.4148 для x86 систем (дистрибутив по ссылке:

http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=11895).

Требуется установка компонента Microsoft .NET Framework Version 3.5 SP1 в случае работы со следующими ОС:

- Microsoft Windows XP SP 3 (x86) и старше;
- Microsoft Windows Server 2003 SP 2 (x86, x64) и старше;
- Microsoft Windows Vista SP 2 (x86,x64) и старше;
- Microsoft Windows Server 2008 R2 (x64) и старше.

И требуется установить компонент Microsoft Internet Explorer 7.0 и выше при работе на следующих ОС:

- Microsoft Windows XP SP 3 (x86) и старше;
- Microsoft Windows Server 2003 SP 2 (x86, x64) и старше.

Загрузить дистрибутивы данных программ можно с сайта компании Microsoft (www.microsoft.com).

Порядковый № изменения	Подпись ответств. лица	Дата внесения изменения

1.2. Требования к сетевой инфраструктуре

В данном разделе изложена информация, которая поможет интегрировать сканер XSpider в существующую сетевую архитектуру.

2.2.1. Сетевые транспорты

Все параметры сетевой архитектуры тесно связаны с понятием транспорта. Система XSpider реализует концепцию сканирования узлов без применения заранее установленных агентов.

Транспорт – это набор сетевых протоколов, используемых сканером XSpider для проведения сканирования.

В системе XSpider используется транспорт RPC. Номера портов RPC присваиваются автоматически, в диапазоне 1024 – 65535 обычно используются для ОС Windows 2000\XP\2003, а для ОС Windows Vista\2008 используется диапазон 49152 – 65535.

2.2.2. Сетевое взаимодействие с объектом сканирования

Сканер XSpider использует сеть для связи с объектами сканирования. Так, расположение XSpider в непосредственной близости от объекта сканирования позволяет проводить оценку защищенности с минимальной нагрузкой на магистральные каналы связи.

2.2.3. Взаимодействие со средствами защиты

Средства обеспечения безопасности могут оказывать влияние на работу сканера XSpider. В связи с этим, на этапе планирования и развертывания рекомендуется провести тестовые сканирования и использовать методы снижения негативных последствий.

2.2.4. Межсетевые экраны

Межсетевые экраны (МЭ) осуществляют фильтрацию трафика и могут блокировать доступ к сетевым портам, на которых работают протоколы удаленного управления, используемые XSpider при проведении сканирования. Для решения этой проблемы можно использовать два подхода: открытие сетевых портов, используемых сканером на МЭ, или размещение сканера «за» межсетевым экраном в непосредственной близости от объекта сканирования.

Порядковый № изменения	Подпись ответств. лица	Дата внесения изменения

Оптимальным с точки зрения достоверности и скорости сканирования является отсутствие межсетевого экрана между объектом сканирования и сканером XSpider.

2.2.5. **Средства защиты прикладного уровня**

Большинство современных сетевых средств обеспечения безопасности содержат модули анализа прикладных протоколов (Stateful Inspection, Application Firewall). Данные механизмы могут вмешиваться в работу сканера, снижая достоверность полученных результатов. Так, например, сканирование веб-приложения через МЭ, поддерживающий функции защиты веб-приложений (Web Application Firewall), не будет достоверным, поскольку МЭ заблокирует ряд потенциально опасных запросов, используемых сканером.

Существуют и другие ситуации, когда фильтр прикладного уровня может оказывать негативное влияние на процесс сканирования. Так, фильтр протокола RPC в Microsoft Internet Security and Acceleration Server (ISA) 2004/2006 по умолчанию блокирует RPC-запросы. Из-за этого снижается производительность сканера, и некоторые проверки невозможно выполнить. Для того чтобы обеспечить полнофункциональное сканирование через ISA Server, необходимо выбрать соответствующее правило в окне Firewall Policy, вызвать контекстное меню и выбрать пункт «Configure RPC protocol». В появившемся окне необходимо отключить опцию «Enforce strict RPC compliance» (Рис. 1).

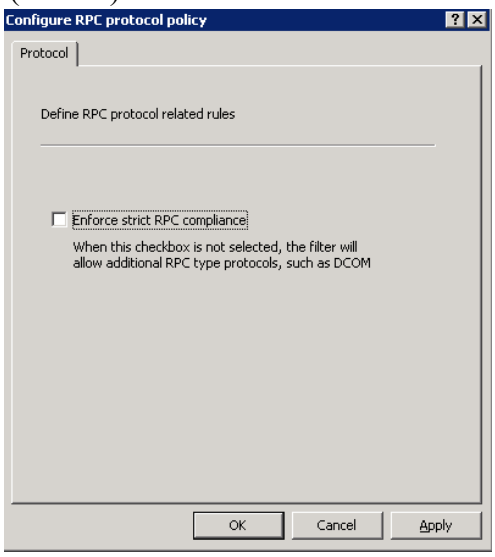

Рис. 1 Отключение проверки RPC в Microsoft ISA Server 2004/2006

В некоторых средствах защиты не существует возможности отключить фильтрацию прикладных протоколов только для отдельных узлов. При возникновении таких ситуаций рекомендуется выносить сканер за МЭ.

2.2.6. **Системы обнаружения и предотвращения атак**

Системы обнаружения/предотвращения атак в большинстве своем реагируют на процесс сканирования как на потенциальную атаку. Получение списка открытых портов, проверка стойкости паролей, доступ к протоколам удаленного управления – все это может привести к срабатыванию средств защиты. В случае если механизм

предотвращения атак не задействован, множественные срабатывания сигнатур приведут только к увеличению объема журналов системы обнаружения атак. Если механизм предотвращения атак включен, то система может вмешаться в процесс сканирования и исказить результаты работы сканера XSpider. В связи с этим, рекомендуется вносить узлы, на которых установлен XSpider, в список исключений системы обнаружения атак.

Порядковый № изменения	Подпись ответств. лица	Дата внесения изменения

2.2.7. **Средства защиты уровня узла**

В случае использования персональных межсетевых экранов и других средств защиты уровня узла (например, HIPS) на сканируемых объектах необходимо разрешить узлам, на которых установлен XSpider, доступ по используемым протоколам удаленного управления. Для входящего в поставку Microsoft Windows МЭ Windows Firewall это осуществляется путем добавления IP-адресов в параметр групповой политики Computer Configuration - Administrative Templates - Network - Network Connections - Windows Firewall - Domain Profile - Windows Firewall: Allow remote administration exception (Рис. 2). Дополнительно необходимо проверить, что параметр Computer Configuration - Administrative Templates - Network - Network Connections - Windows Firewall - Domain Profile - Windows Firewall: Do not allow exceptions отключен.

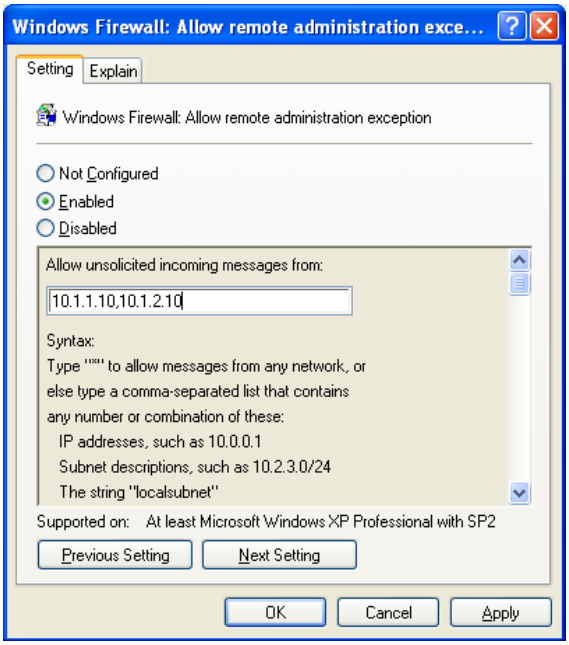

Рис. 2 Настройка исключений в Windows Firewall

Порядковый № изменения	Подпись ответств. лица	Дата внесения изменения

2. УСТАНОВКА СИСТЕМЫ

2.1. Подготовка к установке

Убедитесь, что технические характеристики системы соответствуют минимальным требованиям.

2.2. Установка сканера

После запуска мастера установки и начального приветствия предлагается выбрать каталог установки.

На следующем этапе необходимо задать пароль учетной записи, которая используется для входа в систему. Имя этой учетной записи (Administrator) фиксировано. Учетная запись Administrator имеет максимальные привилегии по отношению к данному сканеру XSpider.

Внимание! Используйте сложный пароль для учетной записи администратора.

На этом этапе установка сканера XSpider завершается.

Внимание! Правильная настройка даты и времени на сервере имеет большое значение для функционирования системы.

Порядковый № изменения	Подпись ответств. лица	Дата внесения изменения

2.3. Активация лицензии

Поставляемая в дистрибутиве лицензия является «свободной», т.е. не привязана к конкретному компьютеру. Свободная лицензия позволяет запускать и настраивать сканер. Для использования основных функций XSpider (сканирование, просмотр результатов, выпуск отчетов) необходимо активировать лицензию. При активации лицензия будет привязана к параметрам компьютера.

Внимание! После активации перенос лицензии на другой компьютер невозможен.

Если ключевые аппаратные характеристики компьютера изменятся, то лицензия может стать недействительной. В этом случае необходимо связаться со службой технической поддержки для получения дополнительной информации по обновлению лицензии.

Сканер XSpider автоматически пытается пройти активацию на глобальном сервере обновлений update.maxpatrol.com при первом подключении. При этом используются стандартные настройки (прямое подключение, порт 2002/TCP). В случае если подключение к сети Интернет ограничено (запрещено использование порта 2002/TCP или используется proxy-сервер), следует отказаться от автоматической активации и изменить настройки подключения к серверу обновлений на вкладке Настройки - Основные.

Успешность активации лицензии можно проверить на закладке Настройки – Основные, раздел Лицензия.

2.4. Активация лицензии в изолированной сети

Для активации лицензии XSpider на компьютере, который находится в изолированном от сети Интернет сегменте, необходимо сгенерировать запрос на активацию, разместить его на сервере https://service.maxpatrol.com и, получив ответ, активировать сканер.

Активация сканера XSpider в изолированной сети проводится через специальный веб-интерфейс на сайте https://service.maxpatrol.com (активируемая лицензия должна иметь возможность работать в режиме Offline).

Процедура активации сканера XSpider в изолированной сети через веб-интерфейс:

1 Запустите XSpider. В графическом интерфейсе убедитесь, что установлена опция «Обновление лицензий в Offline - режиме».

2 Нажмите кнопку «Активировать лицензию»  для активации лицензии. Если требуется обновление лицензии нажмите на кнопку «Сформировать запрос на обновление лицензии»  .

Порядковый № изменения	Подпись ответств. лица	Дата внесения изменения

3 Сохраните на съемный носитель файлы *.of r с запросом на активацию или обновление лицензии.

4 Загрузите файл запроса (*.ofr) через интерфейс offline-активации лицензий https://service.maxpatrol.com/ (необходимо наличие компьютера, подключенного к сети Интернет, и учетной записи для авторизации на данном ресурсе*).

5 После обработки появится соответствующее сообщение и ссылка для скачивания файла-ответа (*.ofl).

6 Скачайте файл *.ofl по указанной ссылке; имя ofl-файла соответствует имени ofr-файла.

7 Если возможность подключения к сети Интернет отсутствует, необходимо передать любым возможным способом файл запроса (*.ofr) разработчику. В ответ Вы получите файл *.ofl.

8 Чтобы загрузить *.ofl, нажмите кнопку  (импортировать лицензию в режиме offline) на вкладке « Сервер» панель «Лицензии» во вкладке « Настройки».

В случае возникновения вопросов Вы можете связаться со службой технической поддержки по тел. +7 (495) 744-01-44.

*Чтобы получить учетную запись для активации на странице https://service.maxpatrol.com, необходимо зарегистрироваться на сайте технической поддержки компании Positive Technologies (https://support.ptsecurity.ru) и отправить заявку с темой «Получение учетной записи для offline-активации лицензий XSpider». Вы получите учетную запись на указанный в заявке электронный адрес.

2.5. Обновление системы

Для корректной работы системы автоматического обновления необходимо наличие соединения с сервером обновлений (update.maxpatrol.com).

Для обновления переключитесь на закладку «Настройки – Основные» и нажмите кнопку «Обновить» в панели «Обновления».

Внимание! В ходе обновления консоль потеряет соединения с сервером и в течение некоторого времени (одной-двух минут) не сможет подключиться к системе.

2.6. Защита установки

Операционная система и дополнительные компоненты, используемые XSpider, могут содержать различные уязвимости и недочеты в стандартных настройках. Для устранения уязвимостей рекомендуется после установки провести сканирование компьютера, на котором установлен сканер XSpider, и устранить обнаруженные недочеты в соответствии с полученными рекомендациями.

Порядковый № изменения	Подпись ответств. лица	Дата внесения изменения

2.7. Использование XSpider в виртуальной среде с привязкой к электронным ключам eToken

Использование ключа eToken обеспечивает лицензионную защиту компонентов XSpider при работе в виртуальном окружении. На текущий момент такая возможность официально реализована только для виртуальных машин VMware ESXI 4.1 и Workstation 6.0 и выше.

При использовании других виртуальных машин данная функция реализуется с помощью программного или аппаратного обеспечения типа USB over IP Network.

Компания ЗАО «Позитив Текнолоджиз» обеспечивает техническую поддержку решений, которые базируются только на виртуальных машинах VMware ESXI 4.1 и Workstation 6.0 и выше. Если вы используете решения типа USB over IP Network, по всем вопросам, связанным с работой eToken, необходимо обращаться в службу технической поддержки компании-разработчика этого программного обеспечения.

Наличие постоянно подключенного ключа eToken является обязательным условием для работы XSpider на виртуальной машине.

3.8.1 Порядок использования XSpider с eToken

Для использования ПО XSpider в виртуальной среде необходимо запросить дистрибутив и соответствующую лицензию. Предоставление права использования ПО XSpider осуществляется по лицензионным договорам. Одновременно с передачей права использования ПО XSpider клиенту передается ключ eToken.

При отсутствии у клиента доступа к сети Интернет для инициализации и обновления ПО XSpider, необходимо уведомить об этом разработчика до момента оформления ключа eToken. Разработчик проведет его «привязку» к соответствующей лицензии на стадии формирования дистрибутива ПО XSpider.

Ключ eToken передается клиенту в безвозмездное пользование на весь срок действия лицензии.

В случае утраты ключа eToken по запросу клиента выпускается дополнительный ключ eToken на безвозмездной основе. В этом случае доставка ключа eToken клиенту осуществляется за его счет и с использованием его ресурсов.

В случае повторной и последующей утраты ключа eToken клиент приобретает дополнительный ключ eToken самостоятельно у компании Aladdin (http://www.aladdin-rd.ru/) и передает разработчику для его инициализации. Получение ключа eToken после инициализации осуществляется за счет клиента и с использованием его ресурсов.

Клиенты, которые ранее приобрели ПО XSpider и у которых есть необходимость перейти на использование ПО XSpider в виртуальной среде, обращаются в техническую

поддержку ЗАО «Позитив Текнолоджиз» с запросом на переоформление действующей лицензии. Одновременно с оформлением соответствующей лицензии формируется ключ eToken. Формирование ключа осуществляется бесплатно. Доставка ключа eToken клиенту осуществляется курьером компании ЗАО «Позитив Текнолоджиз» или по договоренности курьером компании клиента.

Для переноса рабочей инсталляции в виртуальное окружение необходимо дополнительно произвести конвертирование аппаратного сервера в виртуальный (см. раздел Перенос компонентов XSpider с аппаратного сервера в виртуальную среду).

3.8.2 Особенности установки компонентов XSpider с использованием eToken

После получения дистрибутива и ключа eToken можно приступить к развертыванию XSpider в виртуальном окружении. Алгоритм развертывания представлен ниже:

- Подготовьте виртуальную машину на базе VMware ESXI 4.1 или Workstation 6.0 и выше.
- При настройке аппаратных ресурсов VMware необходимо руководствоваться требованиями раздела 2.1 Требования к аппаратному и программному обеспечению.
- Установите XSpider из полученного дистрибутива. Процесс установки необходимо проводить при отключенном ключе eToken. Драйверы для ключа eToken интегрированы в дистрибутив и будут установлены автоматически, при этом события установщика драйверов записываются в конец Setup Log (журнал событий мастера установки системы XSpider). По умолчанию Setup Log расположен в каталоге C:\Program Files\Positive Technologies\ XSpider \server\Logs. Если ПО XSpider устанавливается в каталог, отличный от указанного, то журнал событий расположен в каталоге %путь к установке XSpider %\server\Logs.
- Подключите полученный ранее ключ eToken в USB-порт сервера VMware.
- В разделе “Settings” созданной виртуальной машины необходимо последовательно подключить USB controller и USB device. Если к VMware подключено несколько электронных ключей, необходимо выбрать ключ, полученный от ЗАО “Позитив Текнолоджиз”.

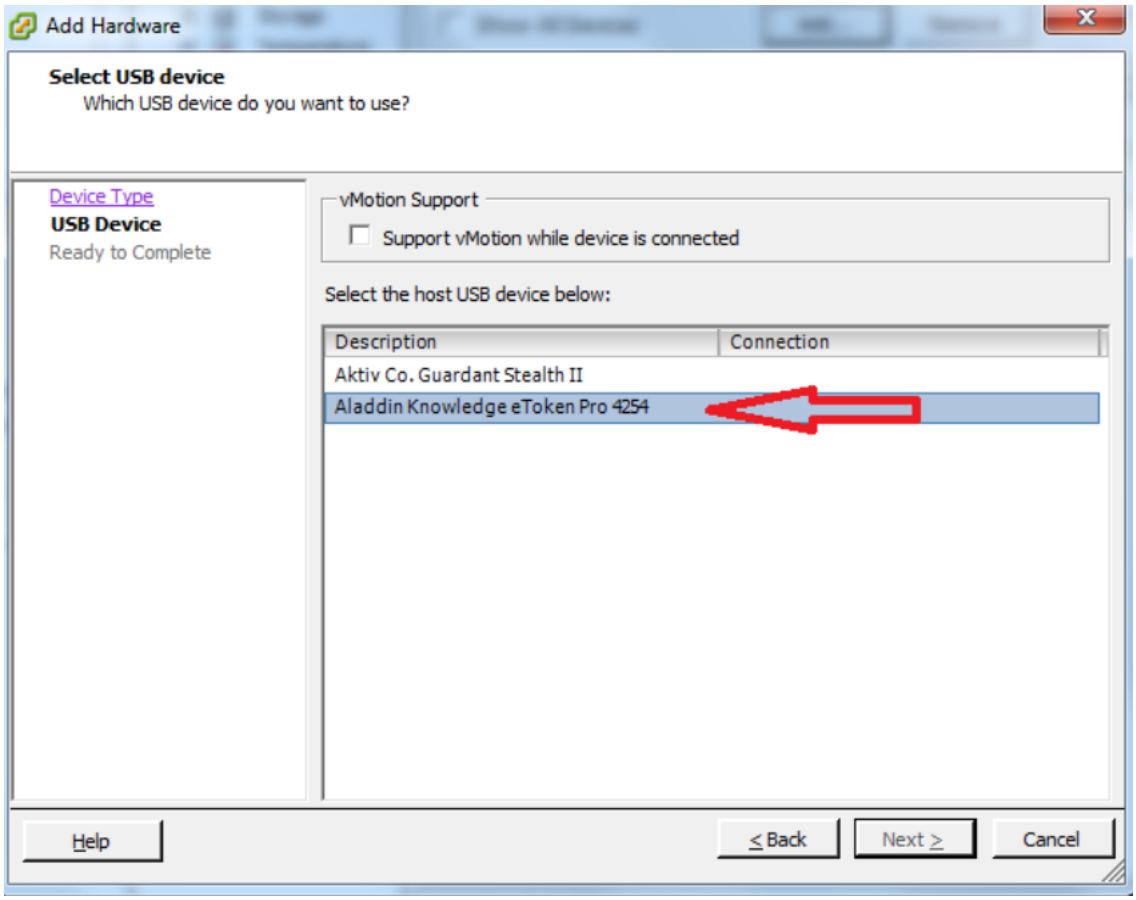

Рис. 3 Выбор электронного ключа

Порядковый № изменения	Подпись ответств. лица	Дата внесения изменения

- Запустите консоль XSpider. Перейдите на вкладку “Настройки” -> ”Сервер”. Активируйте лицензию XSpider согласно инструкции, приведенной в разделе 3.4 Активация лицензии Руководства администратора системы MaxPatrol. В процессе активации проверяется наличие подключенного ключа eToken и действительной лицензии. В дальнейшем для сохранения работоспособности XSpider требуется наличие постоянно подключенного ключа eToken. В случае отключения ключа eToken XSpider блокирует возможность работы с системой до подключения ключа eToken.

3.8.3 Перенос компонентов XSpider с аппаратного сервера в виртуальную среду

Для переноса компонентов XSpider с аппаратного сервера на виртуальную машину можно воспользоваться утилитой VMware Converter.

Скачать VMware vCenter Converter с официального сайта VMware
http://downloads.vmware.com/d/info/datacenter_downloads/vmware_vcenter_converter_standalone/4_0
Подробно процесс конвертирования описан в документе VMware vCenter Converter Documentation на сайте производителя VMware
http://www.VMware.com/support/pubs/vcc_pubs.html

По вопросам, связанным с конвертированием аппаратного сервера в виртуальный, следует обращаться в службу технической поддержки VMware. Компания ЗАО “Позитив Текнолоджиз” не несет ответственности за возможные проблемы, связанные с использованием утилиты VMware vCenter Convertor.

По окончании процесса конвертирования используйте полученный ранее дистрибутив XSpider с поддержкой eToken для повторной установки системы на виртуальной машине. Помните, что процесс установки должен происходить без подключенного ключа eToken.

В ходе установки используйте следующие параметры:
- режим установки “Переустановить XSpider ”;
- использовать данные предыдущей установки? Ответ – “Да”.

После завершения процесса установки подключите полученный ключ eToken в USB-порт сервера VMware.

В разделе “Settings” созданной виртуальной машины необходимо проверить доступность USB controller и подключить USB device (eToken).

В случае если к VMware подключено несколько электронных ключей, необходимо выбрать ключ, полученный от ЗАО “Позитив Текнолоджиз”.

Запустите консоль MaxPatrol. Перейдите на вкладку “Настройки” -> ”Сервер”. Активируйте лицензию MaxPatrol согласно инструкции, приведенной в разделе 3.4 Активация лицензии. В процессе активации проверяется наличие подключенного ключа

eToken и действительной лицензии. В дальнейшем для сохранения работоспособности XSpider требуется наличие постоянно подключенного ключа eToken. В случае отключения ключа eToken XSpider блокирует возможность работы с системой до подключения ключа eToken.

3.8.4 Диагностика и решение проблем

При проверке правильности установки драйверов eToken можно воспользоваться стандартными средствами диагностики Windows.

Если устройство не обнаружено, проверьте наличие неизвестных устройств в диспетчере устройств Windows. В случае успешной установки драйверов для eToken вы увидите устройство USB Token в разделе Universal Serial Bus Controllers.

Порядковый № изменения	Подпись ответств. лица	Дата внесения изменения

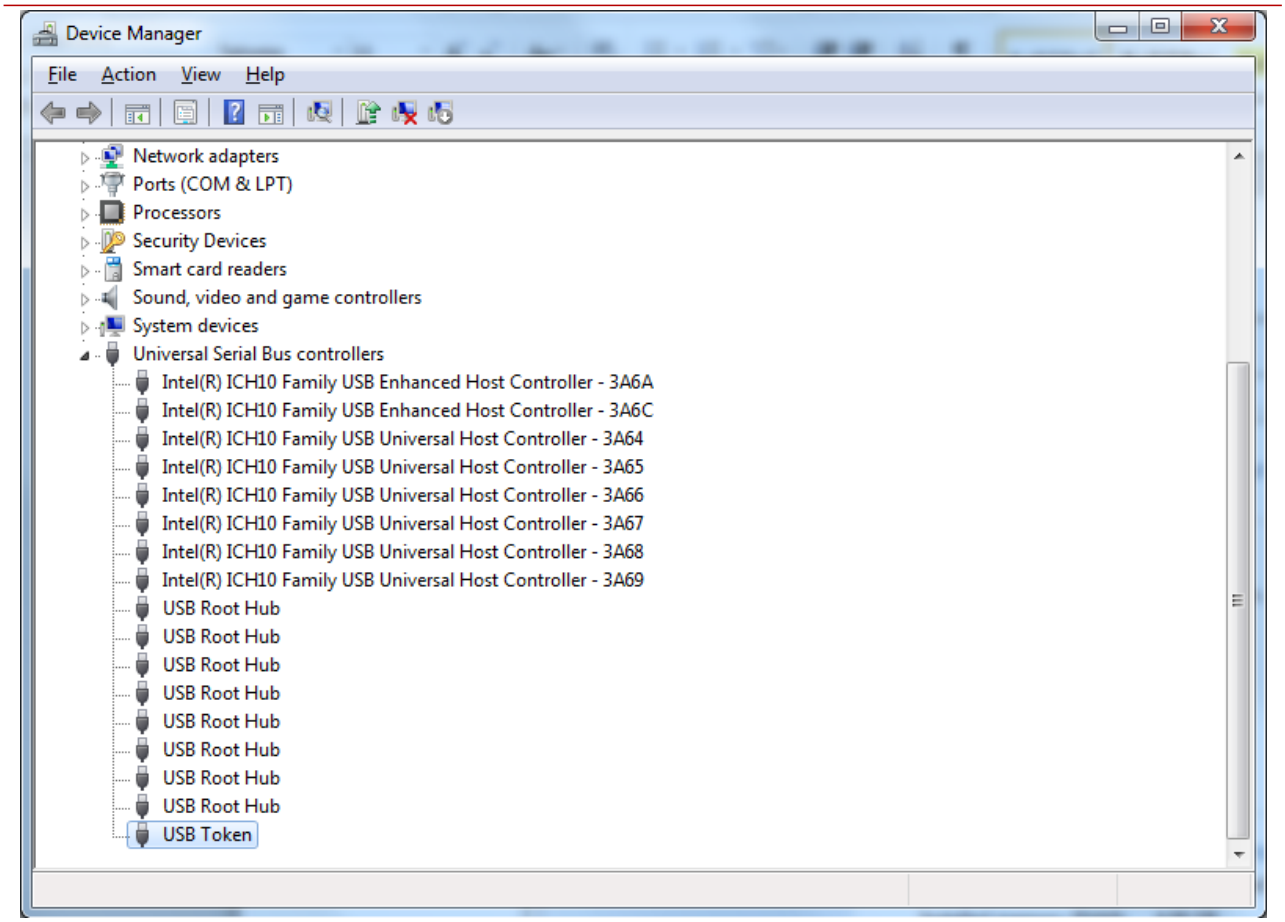

Рис. 4 Диспетчер устройств Windows

В случае отсутствия устройства USB Token, проверьте журнал Setup Log на наличие ошибок. Журнал Setup Log расположен в каталоге установки ПО XSpider. Стандартный каталог: C:\Program Files\Positive Technologies\ XSpider \server\Logs. Если ПО XSpider установлено в каталог, отличный от указанного, то журнал событий расположен в каталоге %путь к установке XSpider %\server\Logs. В случае успешной установки в разделе Driver install start не должно быть статусов Failure.

********** Driver install start ********** Check if the eToken libraries are already installed.
Success.
Creating current directory
Already exit
Current directory: C:\WINDOWS\system32\Setup\PT\eToken
Extracting driver files... Success.

Installing the USB drivers.
Read the .INF file: C:\WINDOWS\system32\Setup\PT\eToken\aksup.inf
Opening the .INF file...
Get the device class GUID and Name... Parsing the manufactures list...
Parsing the devices list: DeviceList...

Порядковый № изменения	Подпись ответств. лица	Дата внесения изменения

SetupCopyOEMInfA... Success.

Installing the scard drivers.
Read the .INF file: C:\WINDOWS\system32\Setup\PT\eToken\aksifdh.inf
Opening the .INF file...
Get the device class GUID and Name... Parsing the manufactures list...
Parsing the devices list: DeviceList... Creating device info set.
Registering devices.
Updating PnP Devices... Updated: *AKS0001
Updated: *AKS0009
Success.

********** End log **********

В случае возникновения ошибки “отказ в доступе” при работе с компонентами XSpider необходимо убедиться, что ключ eToken подключен и виден для системы.

При возникновении ошибок, связанных с подключением и настройкой eToken, необходимо обратиться в службу технической поддержки компании ЗАО “Позитив Текнолоджиз” (https://support.ptsecurity.ru). Для этого необходимо создать запрос, в котором подробно описать суть проблемы и приложить необходимые файлы журналов: Setup Log и PTkernel.log. По умолчанию эти файлы расположены в каталоге C:\Program Files\Positive Technologies\ XSpider \server\Logs.

Для более детального анализа проблем может также потребоваться файл DxDiag.log. В этом журнале содержится информация, которая позволяет определить присутствие USB-носителя в системе, а также определить версию драйвера, используемого при работе с устройством. Чтобы получить DxDiag.log, необходимо при помощи командной строки запустить утилиту dxdiag.exe и на вкладке System выбрать Save All Information. Полученный файл журнала следует отправить в службу технической поддержки компании ЗАО “Позитив Текнолоджиз”.

Компания ЗАО “Позитив Текнолоджиз” обеспечивает техническую поддержку решений, которые базируются только на виртуальных машинах VMware ESXI 4.1 и Workstation 6.0 и выше. Если вы используете решения типа USB over IP Network, то по всем вопросам, связанным с работой ключей eToken, необходимо обращаться в службу технической поддержки компании-разработчика этого программного обеспечени

Порядковый № изменения	Подпись ответств. лица	Дата внесения изменения

Порядковый № изменения	Подпись ответств. лица	Дата внесения изменения