POSITIVE TECHNOLOGIES

ЗАО «ПОЗИТИВ ТЕКНОЛОДЖИЗ»
107061, МОСКВА, ПРЕОБРАЖЕНСКАЯ ПЛ., Д. 8
ТЕЛ. +7 495 744-01-44, ФАКС. +7 495 744-01-87, PT@PTSECURITY.COM
PTSECURITY.RU, MAXPATROL.RU, SECURITYLAB.RU

СИСТЕМА MAXPATROL

РУКОВОДСТВО ПО УСТАНОВКЕ

ОГЛАВЛЕНИЕ

1. Архитектура и состав системы

Система контроля защищенности и соответствия стандартам MaxPatrol построена на основе трехуровневой архитектуры, что обеспечивает высокое масштабирование и позволяет внедрять систему в компаниях любого размера.

Основным компонентом системы является *MaxPatrol Server* (MP Server) — серверный компонент, выполняющий все основные функции распределенного сканера безопасности: сканирование, сбор данных, их обработку, сохранение в базу данных и выпуск отчетов.

В состав MP Server входит:

- модуль управления;
- база знаний, содержащая информацию о проверках, уязвимостях и стандартах;
- база данных, содержащая историю сканирования;
- сканирующее ядро.

Минимальное развертывание системы MaxPatrol состоит из одного сервера.

Сканирующее ядро, входящее в состав MP Server, называется *MaxPatrol Scanner* и выполняет сканирование: собирает и обрабатывает информацию о сканируемых узлах и передает ее в базу данных. При необходимости к MP Server могут быть добавлены дополнительные сканеры, что позволяет увеличить производительность и учитывать топологию сети при сканировании (например, наличие межсетевых экранов и средств защиты). Кроме того, дополнительный MP Scanner можно вынести за пределы исследуемого сегмента сети и одновременно выполнять сканирование как внутри сети, так и снаружи.

Сервер консолидации — *MaxPatrol Consolidation Server* — аккумулирует информацию различных серверов MP Server и позволяет выстроить целостную картину защищенности крупной распределенной информационной системы. Для сохранения информации может использоваться встроенная база данных (MP Mobile Server и MP Server) или корпоративная СУБД (MP Server). В качестве встроенной БД используется Microsoft SQL Server 2008 R2 SP1 редакции Express Edition. А Microsoft SQL Express, Standard или Enterprise можно использовать как внешнюю базу данных.

Локальный сервер обновлений — *MaxPatrol Local Update Server (LUS)* — используется как единая точка поддержки базы знаний и исполняемых модулей компонентов в актуальном состоянии.

Также существует специализированная версия MP Server для работы на мобильных компьютерах — *MaxPatrol Mobile Server*. Компонент представляет собой полнофункциональный модуль сканирования, однако не поддерживает функцию подключения дополнительных сканеров. Наличие встроенного модуля консолидации позволяет после проверки территориально удаленных сетей и подразделений или физически изолированных сегментов использовать результаты в общей отчетности системы на базе *MP Consolidation Server.*

Управление системой *MaxPatrol* осуществляется с помощью консоли управления *MaxPatrol Console* — графического интерфейса администраторов, операторов и пользователей системы.

Основные компоненты системы MaxPatrol, их условные обозначения и особенности приведены в Табл. 1.

Таблица 1. Основные компоненты MaxPatrol

Название и код	Описание	Особенности
MP Server (MP-SRV)	Система управления MaxPatrol и одно сканирующее ядро. Является необходимым и достаточным компонентом для сканирования, построения отчетов и управления системой	Является единицей масштабирования системы и единицей разграничения доступа. Содержит независимую базу данных учетных записей и групп, которые могут использоваться для разграничения доступа к элементам системы (задачам, отчетам и т. п.). Для хранения большого объема данных использует внешнюю СУБД. Для хранения тестовых данных может использоваться встроенная БД
MP Mobile Server (MP-M)	Мобильный комплекс на базе MP Server со сканирующим ядром и встроенным модулем консолидации	Лицензируется для использования только на мобильных компьютерах. Не поддерживает функцию подключения внешних сканеров
MP Scanner (MP-SCN)	Дополнительное сканирующее ядро (сканер), подключаемое к MP Server	Реализует механизмы PenTest, Audit, Compliance и Forensic. Не может использоваться самостоятельно, всегда находится под контролем MP Server. Управление осуществляется через MP Console
MP Consolidation Server (MP-CS)	Сервер консолидации собирает результаты сканирования территориально распределенных серверов (включая MP Mobile Server) и сканеров и сохраняет их для дальнейшего анализа	Поддерживает генерацию отчетов по данным сканирования различных серверов и сканеров. Требуется для формирования единой отчетности в случае использования двух и более MP Server. Связь между MP Server и MP Consolidation Server достаточно устанавливать периодически. Результаты сканирования также можно передавать на съемных носителях
MP Local Update Server (MP-LUS)	Локальный сервер обновлений системы MaxPatrol	Позволяет загружать обновления для компонентов MaxPatrol из сети Интернет только на данный сервер. Остальные компоненты получают данные с этого локального сервера обновлений. Позволяет обновлять компоненты в изолированных сегментах сети, получая информацию с другого локального сервера обновлений без помощи сети (например, через съемный носитель информации)
MP Console (MP-CON)	Консоль управления системой MaxPatrol	Пользовательский интерфейс системы

В зависимости от функциональных возможностей каждый компонент может иметь дополнительные суффиксы в коде (см. Табл. 2).

Таблица 2. Дополнительные возможности компонентов MaxPatrol

Название	Код	Описание
Remote Database	-RD	Возможность хранения данных в удаленной СУБД
Remote Scanner	-RS	Возможность подключения внешнего сканера
Consolidation Client	-CL	Возможность работы с Consolidation Server
PenTest	-P	Поддержка тестирования на проникновение (PenTest) — для сервера и сканера
PenTest & Audit	-PA	Поддержка тестирования на проникновение (PenTest) и системных проверок (Audit) — для сервера и сканера
PenTest & Audit & Compliance	-PAC	Поддержка тестирования на проникновение (PenTest), системных проверок (Audit) и контроля соответствия стандартам (Compliance) — для сервера и сканера
PenTest & Audit & Compliance & Forensic	-PACF	Поддержка тестирования на проникновение (PenTest), системных проверок (Audit), контроля соответствия стандартам (Compliance) и поиска противоправных действий (Forensic) — для сервера и сканера

Указанные в таблице модификаторы могут комбинироваться; например, MP-SRV-PAC-RD-CL — это компонент MP Server, поддерживающий работу с удаленной СУБД и консолидацию данных.

Исключением являются механизмы мониторинга, для которых существует только три сочетания: -P, -PA и -PAC. Это означает, что нельзя приобрести, например, систему MaxPatrol с поддержкой системных проверок и без поддержки тестирования на проникновение.

2. Требования к системе

Данный раздел содержит информацию о том, какие требования к аппаратному и программному обеспечению, а также сетевой и системной инфраструктуре предъявляются для развертывания системы контроля защищенности и соответствия стандартам MaxPatrol.

2.1. Требования к аппаратному обеспечению

Для установки компонентов MaxPatrol можно использовать как физическое, так и виртуальное оборудование. В Табл. 3 приведены аппаратные требования для физического или виртуального оборудования, на которое планируется установить системные приложения и серверные компоненты MaxPatrol.

Если планируется установка на виртуальное оборудование, то необходимо учитывать требование по использованию USB eToken для защиты лицензии. Необходимо, чтобы физическое оборудование гипервизора имело достаточное количество USB-портов, а функциональность гипервизора обеспечивала подключение USB-устройств к гостевой операционной системе. Если эти условия не выполняются, то необходимо использовать решения класса USB-over-Network, например Digi AnywhereUSB.

2.1.1. Типовые требования к аппаратному обеспечению

Данные Табл. 3 можно использовать с учетом следующих условий.

- Для процессора требования указывают количество ядер, которые доступны операционной системе, а частота указана как для физического, так и для виртуального процессора.
- Требования указаны для оборудования, которое будет использоваться только для MaxPatrol.
- Требования к оборудованию указаны для типовых случаев. Во всех остальных случаях требования к аппаратному обеспечению нужно уточнять в службе технической поддержки.
- Под параметром HDD в таблице понимается свободное дисковое пространство.
- Параметр «Узлов не более» означает хранение информации о сканировании совокупного количества узлов, сканируемого как самим компонентом, так всеми подключенными компонентами.
- Максимальное значение параметра «Узлов не более» — 5000. Если планируется хранение информации о большем количестве узлов, то требуемое свободное дисковое пространство увеличивается линейно.

Таблица 3. Типовые аппаратные требования к серверным компонентам

Компонент	СУБД	Узлов не более	Параметр	Частота сканирования		
				1 раз в неделю	1 раз в месяц	1 раз в квартал
MaxPatrol Server MaxPatrol Mobile Server	Встроенная	500	CPU	2x2,4 ГГц		
			RAM	8 ГБ		
			HDD	50 ГБ		
MaxPatrol Server	MS SQL Server		CPU	2x2,4 ГГц		
			RAM	16 ГБ		
		1000	HDD	650 ГБ	180 ГБ	90 ГБ
		3000		1870 ГБ	460 ГБ	180 ГБ
		5000		3090 ГБ	750 ГБ	280 ГБ
MaxPatrol Consolidator	MS SQL Server		CPU	4x2,8 ГГц		
			RAM	16 ГБ		
		1000	HDD	845 ГБ	230 ГБ	120 ГБ
		3000		2430 ГБ	600 ГБ	230 ГБ
		5000		4020 ГБ	970 ГБ	360 ГБ
MaxPatrol Consolidator	СУБД установлена на отдельном оборудовании		CPU	2x2,4 ГГц		
			RAM	8 ГБ		
			HDD	50 ГБ		
Отдельный сервер СУБД MS SQL Server для MaxPatrol Server			CPU	2x2,4 ГГц		
			RAM	12 ГБ		
		1000	HDD	650 ГБ	180 ГБ	90 ГБ
		3000		1870 ГБ	460 ГБ	180 ГБ
		5000		4020 ГБ	970 ГБ	360 ГБ
Отдельный сервер СУБД MS SQL Server для MaxPatrol Consolidator			CPU	2x2,4 ГГц		
			RAM	12 ГБ		
		1000	HDD	845 ГБ	230 ГБ	120 ГБ
		3000		2430 ГБ	600 ГБ	230 ГБ
		5000		4020 ГБ	970 ГБ	360 ГБ
MaxPatrol Scanner			CPU	2x2,4 ГГц		
			RAM	4 ГБ		
			HDD	50 ГБ		

Таблица 3. Типовые аппаратные требования к серверным компонентам

Компонент	СУБД	Узлов не более	Параметр	Частота сканирования		
				1 раз в неделю	1 раз в месяц	1 раз в квартал
MaxPatrol LUS			CPU	2x2,4 ГГц		
			RAM	4 ГБ		
			HDD	50 ГБ		

Кроме серверых компонентов MaxPatrol существуют два дополнительных компонента: MaxPatrol Console и MaxPatrol Offline Scanner, которые не требуется устанавливать на отдельное оборудование. MaxPatrol Console устанавливается на рабочую станцию, которая используется для управления серверными компонентами MaxPatrol. MaxPatrol Offline Scanner запускается с внешнего USB-носителя, подключенного к сканируемому компьютеру, и не требует установки.

В Табл. 4 указаны требования к компьютерам, на которых планируется использовать дополнительные компоненты, и к внешнему носителю для MaxPatrol Offline Scanner.

Таблица 4. Аппаратные требования к дополнительным компонентам MaxPatrol

Компонент	Требования	Примечание
MaxPatrol Console	CPU: 1 ГГц или выше RAM: свободной памяти не менее 512 МБ HDD: свободного места не менее 150 МБ Разрешение экрана: 1280x1024	Устанавливается на любую рабочую станцию под управлением Microsoft Windows XP SP 3, Microsoft Windows Server 2003 SP 2 и выше
Компьютер, сканируемый MaxPatrol Offline Scanner	CPU: 1 ГГц или выше RAM: свободной памяти не менее 512 МБ HDD: свободного места не менее 50 МБ	Можно сканировать любой компьютер под управлением Microsoft Windows XP SP 3, Microsoft Windows Server 2003 SP 2 и выше
USB-носитель для MaxPatrol Offline Scanner	Свободного места не менее 1 ГБ	MaxPatrol Offline Scanner копируется на любой дисковый накопитель с интерфейсом USB

2.1.2. Примеры конфигурации оборудования для серверных компонентов MaxPatrol

- При использовании физического оборудования (см. пример в Табл. 5)

Таблица 5. Оборудование для серверных компонентов MaxPatrol

Компонент	Пример оборудования	Конфигурация
MaxPatrol Server MaxPatrol Consolidator MS SQL Server для MaxPatrol MaxPatrol Scanner MaxPatrol LUS	Dell PowerEdge R210 II Fujitsu PRIMERGY RX100 S7 HP ProLiant DL160 G6 IBM x3530 M4 или аналоги	CPU: 1 x Intel Xeon E3 Family или аналог RAM: от 8 ГБ (4 ГБ для MaxPatrol Scanner и LUS) HDD: от 250 ГБ (SATA или SAS) Для хранения данных о большом количестве узлов может потребоваться полка для дисков, например, HP D2600, HP D2700, IBM System Storage DS3500, Dell PowerVault MD1200 или аналоги
MaxPatrol Mobile Server (устанавливается на ноутбук)	Acer Travelmate B113 ASUS U24E Dell Latitude E6330 HP EliteBook 2170p Lenovo x230 или аналоги	CPU: Intel Core i5 или аналог RAM: от 8 ГБ HDD: от 50 ГБ

- При использовании виртуального оборудования (см. пример параметров виртуальной машины для MaxPatrol Server со встроенной базой на рис. 1, 2, 3).

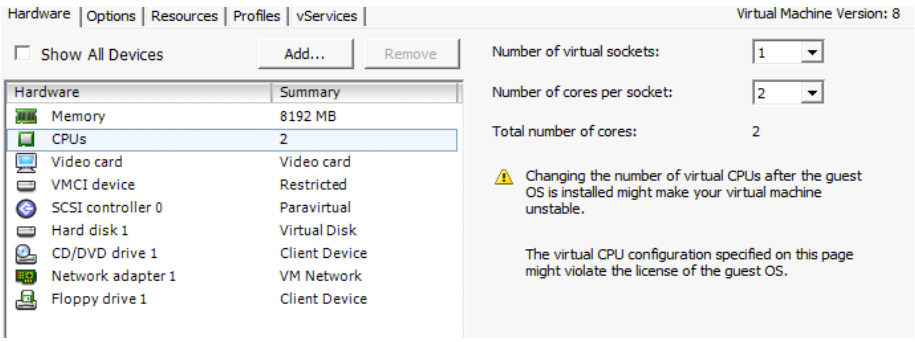

Рис. 1 – Параметры настройки CPU

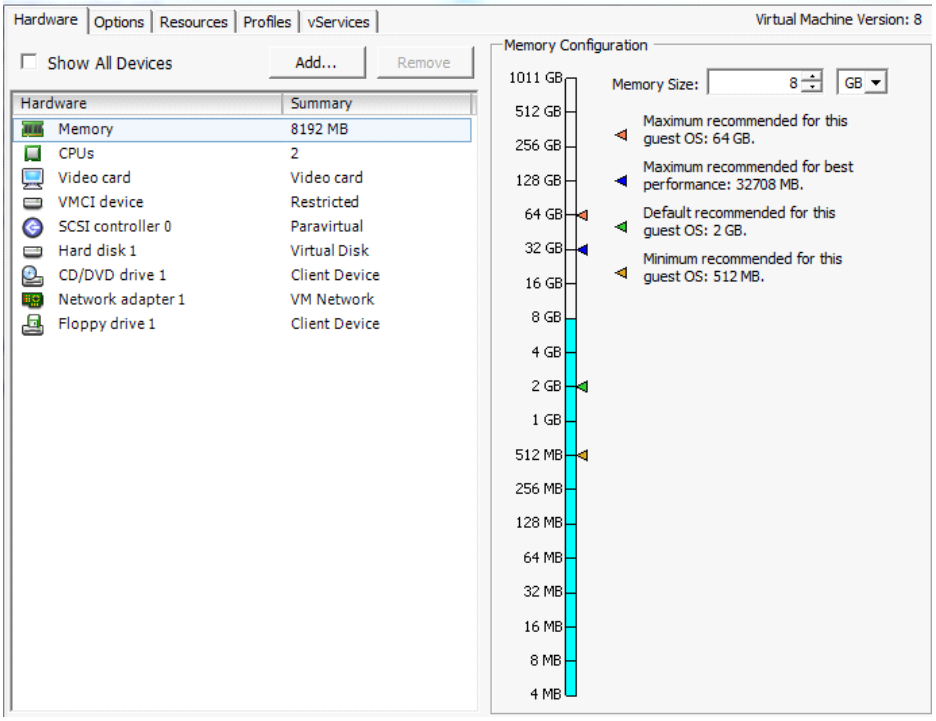

Рис. 2 – Параметры настройки RAM

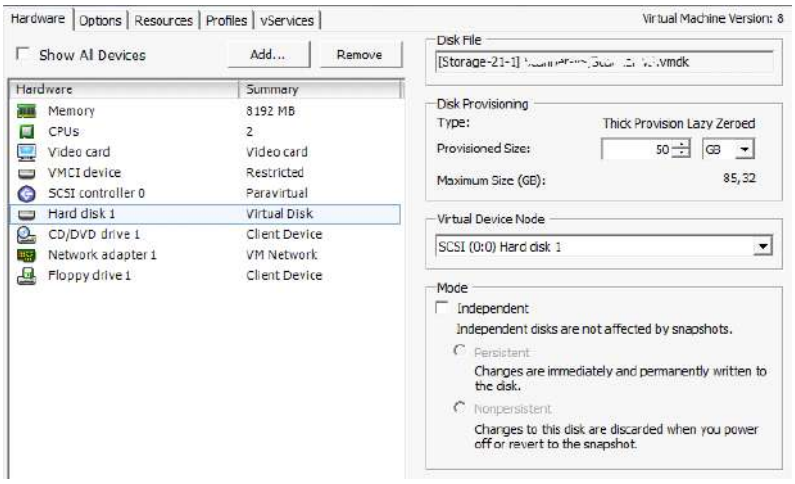

Рис. 3 – Параметры настройки HDD

Если гипервизор позволяет зарезервировать ресурсы, выделяемые виртуальной машине, то рекомендуется установить резерв ресурсов со значениями не меньше указанных в Табл. 3.

2.1.3. Требования к аппаратному обеспечению сканируемых узлов

Нагрузка на узел при сканировании зависит от типа узла и способа сбора информации, но так или иначе значительной нагрузки не создается. Не рекомендуется сканировать узлы, находящиеся на грани предельной загрузки,

т.е. когда процессор загружен более чем на 70%, свободной оперативной памяти менее 256 МБ, свободного места на системном диске менее 50 МБ.

2.1.4. Возможные проблемы с производительностью

В Табл. 6 представлены типовые проблемы производительности аппаратного обеспечения и способы их диагностики и исправления.

Таблица 6. Типовые проблемы производительности MaxPatrol

Тип проблем	Как диагностировать	Как исправить
Проблемы, связанные с недостатками аппаратного обеспечения	Замедленная работа MaxPatrol проявляется постоянно во всех режимах работы. Для точной диагностики необходимо провести замеры с помощью счетчиков производительности Microsoft для ОС Windows и СУБД SQL Server по инструкции службы технической поддержки	После диагностики и выявления проблемного компонента аппаратного обеспечения заменить физическое или изменить параметры виртуального оборудования
Проблемы, связанные с избыточной нагрузкой на СУБД	Замедленная работа MaxPatrol проявляется при генерации отчетов. Сканирование работает нормально, если в это же время не производится генерация отчетов	Соблюдать условия эксплуатации: разделять во времени процессы сканирования и генерации отчетов, избегать генерации одного отчета по большому количеству узлов с выводом детальной информации (рекомендуется не включать в отчет более 100 узлов с подробной информацией)
Проблемы, не связанные с аппаратным обеспечением	Медленное сканирование узлов, доступ к которым осуществляется по сетевым каналам с низкой пропускной способностью	Установить в удаленных сегментах сети дополнительные компоненты MaxPatrol Scanner или использовать offline-сканирование

2.2. Требования к программному обеспечению

2.2.1. Требования к операционной системе

Система MaxPatrol разработана для функционирования на базе операционных систем Windows. В настоящее время поддерживаются следующие ОС:

- Microsoft Windows XP SP 3 (x86) и выше;
- Microsoft Windows Server 2003 SP 2 (x86, x64) и выше;
- Microsoft Windows Vista SP 2 (x86,x64) и выше;
- Microsoft Windows Server 2008 SP 2 (x86, x64) и выше;
- Microsoft Windows 7 (x86,x64) и выше;
- Microsoft Windows Server 2008 R2 (x64) и выше;
- Microsoft Windows 8 (x86,x64) и выше;
- Microsoft Windows 8.1 (x86,x64)

- Microsoft Windows Server 2012 (x64);
- Microsoft Windows Server 2012 R2 (x64, x86).

Список совместимых систем постоянно расширяется. Актуальную информацию можно получить в службе технической поддержки (https://support.ptsecurity.com).

Выбирая операционную систему, следует учитывать, что при ряде проверок система MaxPatrol интенсивно использует стек протоколов TCP/IP операционной системы. В связи с этим развертывание MaxPatrol на пользовательских версиях ОС (например, Windows XP) снижает эффективность сканирования большого количества узлов. В частности, уменьшается производительность сканера портов и ряда других механизмов PenTest. Тип ОС минимально влияет на работу механизмов Audit и Compliance.

2.2.2. Требования к прикладному программному обеспечению

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

- Microsoft Internet Explorer 7.0 и выше;
- Microsoft .NET Framework Version 4.0.

На ОС Microsoft Windows 8.1 для выпуска XML-отчетов необходима установка Microsoft .NET Framework Version 3.5. Это требуется для корректной работы внешней утилиты Saxon, которая является XSLT-процессором.

Получить дистрибутивы данных программ можно на сайте компании Microsoft (www.microsoft.com).

> **Примечание**: при установке и обновлении системы инсталлятор проверяет наличие обновления Windows Installer 4.5 Redistributable и устанавливает его в случае отсутствия.

2.2.3. Требования к СУБД

В зависимости от требований к производительности могут использоваться корпоративные либо бесплатные редакции СУБД Microsoft SQL Server.

В составе дистрибутива MaxPatrol имеется инсталлятор СУБД Microsoft SQL Server 2008 R2 SP1 редакции Express Edition (далее по тексту - встроенная база). При использовании встроенной базы данных существует ограничение на объем хранимых результатов сканирования — 10 ГБ. Использование встроенной базы данных в промышленных системах не рекомендуется.

> **Внимание!** Указанная версия встроенной базы данных не совместима с операционными системами Microsoft Windows XP, Microsoft Windows 8 и Microsoft Windows 8.1.

Также существует возможность использования внешней СУБД, такой как Microsoft SQL Server редакции Standard и Enterprise следующих версий:

- Microsoft SQL Server 2005 SP4 и старше;
- Microsoft SQL Server 2008 SP3 и старше;
- Microsoft SQL Server 2008 R2 SP1 и старше;
- Microsoft SQL Server 2012 и старше;
- Microsoft SQL Server 2014.

Список совместимых систем постоянно расширяется. Актуальную информацию можно получить в службе технической поддержки (https://support.ptsecurity.com).

В Табл. 7 приведены значения размеров одного результата сканирования для типовых систем в зависимости от режима сканирования.

Таблица 7. Размер результата сканирования при разных режимах сканирования, КБ

Операционная система	PenTest	Audit	Compliance
Windows 7 Workstation	64	832	1024
Windows 2008 R2 Server	704	1664	1088
FreeBSD	64	88	512
Cisco IOS	64	128	640

В Табл. 8 представлено сравнение возможностей программных продуктов MS SQL 2008 Standard и Enterprise.

Таблица 8. Возможности программных продуктов MS SQL 2008 Standard и Enterprise

	SQL Server 2008 Enterprise Edition	SQL Server 2008 Standard Edition
Число процессоров	Столько, сколько поддерживает ОС	4
Масштабируемость и производительность	В полной мере	Ограничено
Высокий уровень доступности (схема сетевой готовности)	В полной мере	Ограничено
Повышенная безопасность	В полной мере	Ограничено
Хранилища данных	В полной мере	Недоступно
Бизнес-аналитика	В полной мере	Ограничено
Повышенная управляемость	В полной мере	Недоступно

Сравнение доступно также на сайте Microsoft: http://www.microsoft.com/sqlserver/2008/ru/ru/compare-std-ent.aspx

2.3. Требования к сетевой инфраструктуре

Перед установкой компонентов MaxPatrol необходимо удостовериться, что сетевая инфраструктура, в которой они будут функционировать, соответствует ряду требований.

2.3.1. Сетевые транспорты

Все параметры сетевой архитектуры тесно связаны с понятием транспорта. Система MaxPatrol реализует концепцию сканирования узлов без применения заранее установленных агентов. Для глубокой проверки программного обеспечения и конфигураций в режимах Audit и Compliance используются протоколы удаленного управления, позволяющие получать доступ к настройкам анализируемых ОС и приложений. Характеристики основных транспортов MaxPatrol приведены в Табл. 9.

Транспорт — это набор сетевых протоколов, используемых системой MaxPatrol для проведения сканирования в режимах Audit и Compliance.

Различные транспорты применимы к различным типам систем. При этом один и тот же тип систем может быть просканирован с использованием различных транспортов. В этом случае выбор транспорта обуславливается его возможностями, скоростью работы, сетевым трафиком. Влияние могут оказывать и дополнительные характеристики, такие как распространенность транспорта и его защищенность.

Таблица 9. Транспорты MaxPatrol

Транспорт	Системы	Возможности	Скорость	Нагрузка	Защищенность
WMI	Windows 2000 и выше	+	+	-	±
NetBIOS	Windows	-	-	+	±
LDAP	Active Directory	-	+	-	±
SSH	Unix, Linux, Cisco, CheckPoint SPLAT	+	+	+	+
Telnet	Unix, Linux, Cisco, CheckPoint SPLAT	+	+	-	-
Oracle	Oracle Database	+	+	±	±
MS SQL	Microsoft SQL Server	+	+	±	±
SAP DIAG	SAP NetWeaver	±	-	+	±
SAP RFC	SAP NetWeaver	±	+	±	±
Remote Engine	Windows 2000 и выше	+	+	-	±

+ максимальное значение;
- минимальное значение;
± значение зависит от настроек.

При использовании транспорта Remote Engine на сканируемый узел загружается модуль, который выполняет часть проверок локально. Это позволяет снизить нагрузку на сеть и повысить скорость сканирования при медленном соединении.

Транспорты используют различные сетевые протоколы. Список протоколов и стандартных сетевых портов приводится в Табл. 10.

Таблица 10. Сетевые протоколы, используемые транспортами

Транспорт	Протокол	Сетевые порты	Примечание
WMI	DCE/RPC	135, >1024	Номера портов RPC присваиваются автоматически[1]
NetBIOS	CIFS/SMB	445 TCP/UDP	Поддерживаются устаревшие клиенты (137-139 TCP/UDP)

Таблица 10. Сетевые протоколы, используемые транспортами

Транспорт	Протокол	Сетевые порты	Примечание
LDAP	LDAP	389,636 TCP	
SSH	SSH	22 TCP	Стандартный порт. Может быть изменен
Telnet	Telnet	23 TCP	Стандартный порт. Может быть изменен
Telnet	SAP AS Java	50008-59908 TCP	В зависимости от экземпляра
Oracle	SQL Net	1521 TCP	Стандартный порт. Может быть изменен
MS SQL	Microsoft SQL Server SMB	1433 TCP 445 TCP	В зависимости от настроек сервера
SAP DIAG	SAP DIAG	3200—3299 TCP	В зависимости от экземпляра
SAP RFC	SAP RFC	3300—3399 TCP	В зависимости от экземпляра
Remote Engine	CIFS/SMB DCE/RPC	445 TCP/UDP 135, >1024	Поддерживаются устаревшие клиенты (137-139 TCP/UDP). Номера портов RPC присваиваются автоматически[1]

Внимание! Набор поддерживаемых транспортов расширяется по мере совершенствования механизмов аудита. Для получения актуальной информации обратитесь в службу технической поддержки.

Использование различных транспортов порождает различную нагрузку на тестируемую систему и сеть. В Табл. 11 дана информация о нагрузке на сеть, возникающей при сканировании узлов в режиме Audit и Compliance при использовании различных транспортов. Данные приведены для случая использования MP Scanner на двухъядерном процессоре.

Таблица 11. Средняя нагрузка на сеть по отношению к объекту сканирования, КБ/с

	WMI	NetBIOS	SSH	Telnet
1 узел	130	250	15	5
Объем трафика на узел, КБ	60 000	80 000	1 500	500

2.3.2. Сетевое взаимодействие компонентов

Компоненты системы MaxPatrol используют сеть для синхронизации и репликации данных, удаленного управления и других задач. По умолчанию система использует сетевой порт 2002/TCP для передачи данных.

1. Номера портов RPC присваиваются автоматически, диапазон 1024 — 65535 обычно используются для ОС Windows 2000/XP/2003, а диапазон 49152 — 65535 — для ОС Windows Vista/2008.

Многоуровневая архитектура системы MaxPatrol дает возможность масштабирования внедрения по различным признакам. Расположение MP Scanner в непосредственной близости от объекта сканирования позволяет проводить оценку защищенности с минимальной нагрузкой на магистральные каналы связи. В Табл. 12 представлена информация об объеме данных, передаваемых между MP Scanner и сканируемым объектом, между MP Scanner и MP Server в ходе передачи результатов сканирования, между MP Server и MP Console в ходе просмотра результатов, а также между MP Server и MP Consolidation Server в ходе консолидации данных. Указана пиковая нагрузка на сеть, которая возникает при выполнении указанных операций.

Таблица 12. Средняя нагрузка на сеть при выполнении операций MaxPatrol, КБ/с

	MP Scanner — объект	MP Scanner - MP Server	MP Server - MP Consolidation Server	MP Server - MP Console
1 узел	До 100 (Windows), до 15 (другие системы)	4,5	2	18
10 узлов	До 1000 (Windows), до 150 (другие системы)	18	20	180

Как видно из Табл. 13, трафик между компонентами MaxPatrol значительно меньше, чем объем передаваемых данных между MP Scanner и объектом сканирования.

Таблица 13. Средний объем трафика на узел, КБ

MP Scanner — объект	MP Scanner - MP Server	MP Server - MP Consolidation Server	MP Server - MP Console
До 130 000 (Windows), до 10 000 (другие системы)	225	200	275

Примечание. Передача данных между MP Server и MP Consolidation Server может происходить как в режиме реального времени, так и в указанный интервал минимальной загрузки сети. К данному типу взаимодействия не предъявляется требование высокой оперативности.

При генерации отчетов объем трафика между MP Server и MP Console может достигать достаточно серьезных объемов (в зависимости от типа отчета и анализируемых временных интервалов). В связи с этим при генерации отчетов рекомендуется использовать канал с пропускной способностью не менее 2 Мб/с.

В Табл. 14 приводится информация о нагрузке на канал связи, возникающей при сканировании узлов в режимах PenTest, Audit и Compliance для различных информационных систем.

Таблица 14. Нагрузка на канал связи между сканером MaxPatrol и объектом сканирования

Режим сканирования	Информационная система	Время сканирования, мин:сек	Средняя скорость передачи данных, Кбит/сек
PenTest	Windows 2003 SP2	7:00	24
PenTest	Suse 9	5:49	23,2
PenTest	Cisco IOS	59:10	5,84
PenTest	S-Terra VPN Gate 1000	34:13	7,89
PenTest	CheckPoint 2200	37:20	32,52
PenTest	Windows Server 2012	31:30	35,75
PenTest	Windows Server 2008	43:54	44,18
Audit и Compliance	Windows 2003 SP2	10:00	272
Audit и Compliance	Suse 9	10:00	10,4
Audit и Compliance	Cisco IOS	12:07	17,38
Audit и Compliance	S-Terra VPN Gate 1000	4:19	0,95
Audit и Compliance	CheckPoint 2200	3:07	2,95
Audit и Compliance	Windows Server 2012	9:10	231,27
Audit и Compliance	Windows Server 2008	9:04	219,55

В Табл. 15 приведена информация о влиянии транспорта Remote Engine при сканировании Windows-систем на объем трафика и нагрузку на канал связи.

Таблица 15. Влияние транспорта Remote Engine при сканировании Windows-систем на объем трафика и нагрузку на канал связи

Система	Объем трафика		Нагрузка на канал		Средний размер пакета, МБ
	Получено, МБ	Передано, МБ	Получено, пакетов	Передано, пакетов	
Windows 2003 (без использования транспорта Remote Engine)	40,87	31,79	195423	190871	0,000188095
Windows 2003 (с использованием транспорта Remote Engine)	19,9	8,91	57651	52768	0,000260873

Таблица 15. Влияние транспорта Remote Engine при сканировании Windows-систем на объем трафика и нагрузку на канал связи

Система	Объем трафика		Нагрузка на канал		Средний размер пакета, МБ
	Получено, МБ	Передано, МБ	Получено, пакетов	Передано, пакетов	
Windows 7 (без использования транспорта Remote Engine)	55,8	56,71	263537	260105	0,000214861
Windows 7 (с использованием транспорта Remote Engine)	32,46	12	60539	56831	0,000378802

2.3.3. Используемые привилегии

Поскольку MP Scanner использует для анализа систем протоколы удаленного управления, он должен проходить аутентификацию и авторизацию на сканируемом узле. Учетные записи, с которыми осуществляется сканирование, можно указать в профиле сканирования. В Табл. 16 дана информация о необходимых правах для используемых учетных записей.

Существует возможность настроить конкретные системы на сканирование с использованием других учетных записей, не требующих высоких привилегий (см. *Руководство администратора,* раздел *Список проверяемых объектов для различных систем*).

Таблица 16. Используемые MaxPatrol привилегии

Система	Привилегии	Стандартные права
Windows	WMI Remote Enable DCOM Remote Launch DCOM Remote Activation	Administrators
	Remote Registry	
	System Shares	
Linux	Read System Files	root
	Execute System Commands	
Solaris	Read System Files	root
	Execute System Commands	
Cisco Router Cisco Switch	Show commands Dir Verify	Level 15
CheckPoint	cat $FWDIR/conf/*	expert
Oracle Database	Select from system tables	DBA

Таблица 16. Используемые MaxPatrol привилегии

Система	Привилегии	Стандартные права
Microsoft SQL Server	Select from system tables	System Administrator (sa)
	Execution of system procedures	
SAP NetWeaver	SA38 (Reports)	SAP_ALL
	SE16 (Tables)	
	SM04 (Sessions Info)	

2.3.4. Взаимодействие со средствами защиты

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

2.3.4.1. Межсетевые экраны

Межсетевые экраны (МЭ) осуществляют фильтрацию трафика и могут блокировать доступ к сетевым портам, на которых работают протоколы удаленного управления, используемые MaxPatrol при проведении сканирования. Для решения этой проблемы можно использовать два подхода: открытие сетевых портов, используемых сканером на МЭ, или размещение MP Scanner «за» межсетевым экраном в непосредственной близости от объекта сканирования (см. Рис. 4). В последнем случае межсетевой экран должен разрешать взаимодействие между MP Server и MP Scanner по порту 2002/TCP.

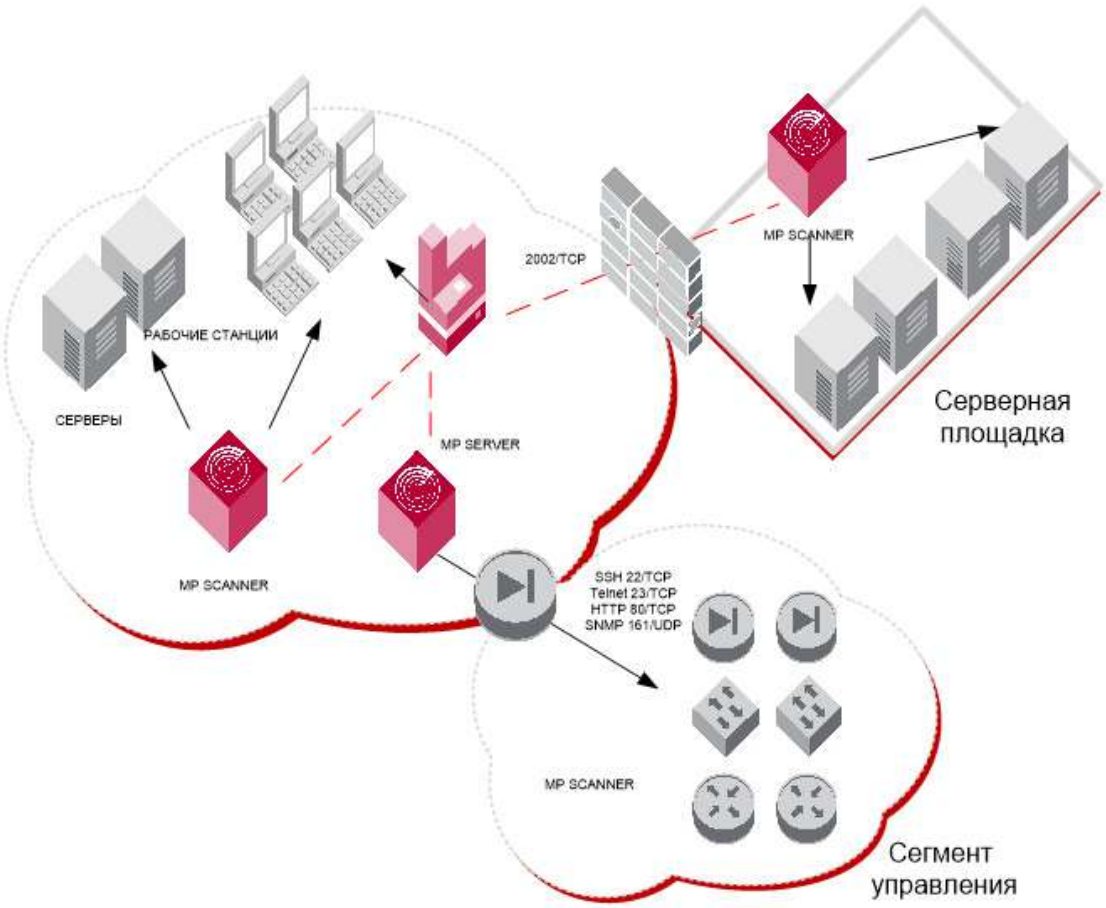

Рис. 4 – Использование дополнительных сканеров для работы через межсетевой экран

Примечание: Взаимодействие между компонентами не зависит от направления соединения. Система MaxPatrol спроектирована таким образом, что направление TCP-соединения не является определяющим критерием. При установлении канала связи между MP Server и MP Scanner соединение может настраиваться как исходящее на MP Server или как исходящее на MP Scanner. В первом случае инициатором TCP-сессии будет MP Server, а во втором – MP Scanner.

Если между компонентами системы присутствует межсетевой экран, работающий в режиме сервера-посредника (proxy), то в настройках соединения необходимо указать тип протокола, а также учетную запись и пароль. Система поддерживает следующие типы proxy: HTTP (Connect), Socks4 и Socks5 (см. Рис. 5).

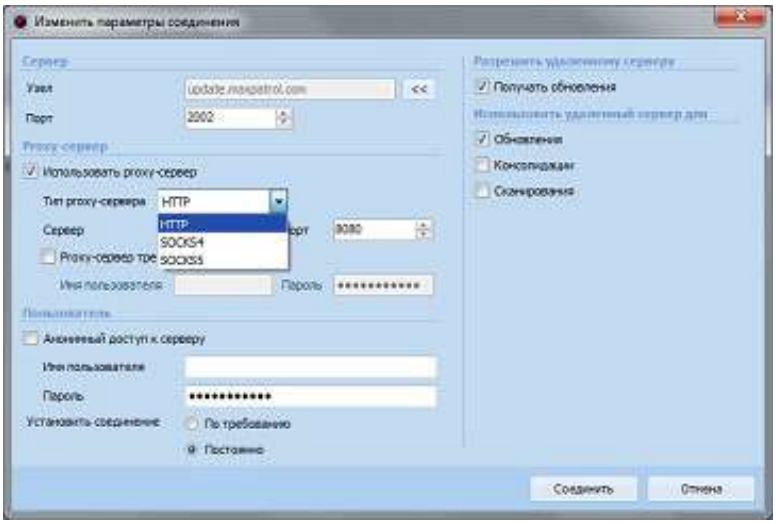

Рис. 5 – Настройка proxy-сервера в свойствах соединения

При сканировании через МЭ необходимо, чтобы на нем были открыты порты, соответствующие типу используемого транспорта. Информация об используемых транспортах и соответствующих сетевых портах приведена в Табл. 10.

Оптимальной ситуацией с точки зрения достоверности и скорости сканирования является отсутствие межсетевого экрана между объектом сканирования и MP Scanner.

2.3.4.2. 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, результат сканирования веб-приложения через межсетевой экран, 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. К примеру, фильтр протокола RPC в Microsoft Internet Security and Acceleration Server (ISA) 2004/2006 по умолчанию блокирует WMI-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* (см. Рис. 6).

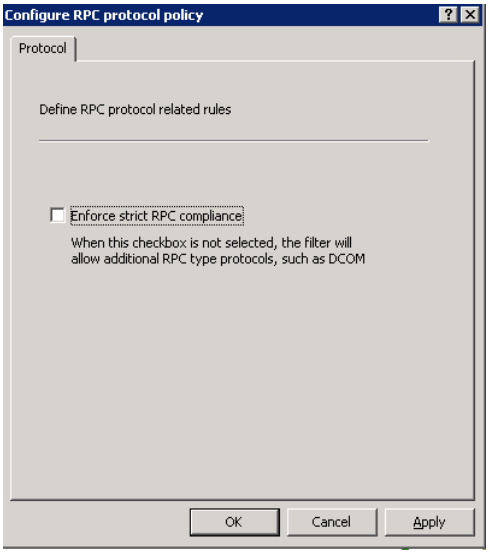

Рис. 6 – Отключение проверки RPC в Microsoft ISA Server 2004/2006

В некоторых средствах защиты нельзя отключить фильтрацию прикладных протоколов для отдельных узлов. В таких случаях рекомендуется выносить сканер за МЭ.

2.3.4.3. Системы обнаружения и предотвращения атак

Системы обнаружения и 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 системы MaxPatrol. В связи с этим рекомендуется вносить узлы, на которых установлен MP Scanner, в список исключений системы обнаружения атак.

2.3.4.4. 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 MP Scanner, 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* (см. Рис. 7). Кроме того, необходимо убедиться, что отключен параметр *Computer Configuration — Administrative Templates — Network — Network Connections — Windows Firewall — Domain Profile —Windows Firewall: Do not allow exceptions.*

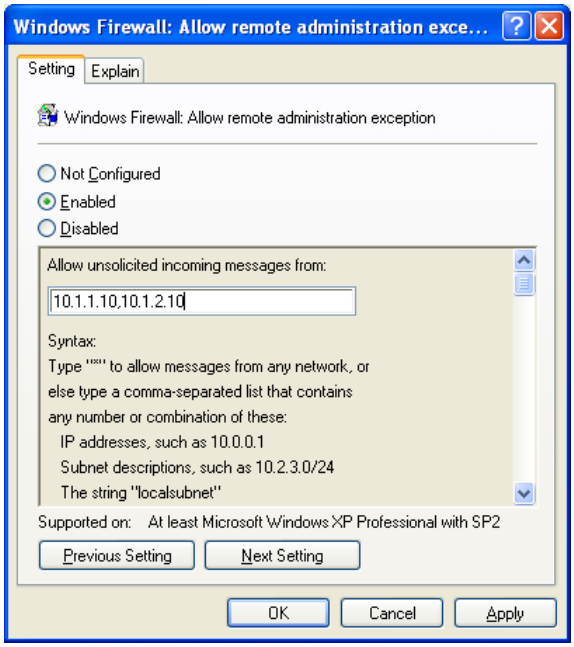

Рис. 7 – Настройка исключений в Windows Firewall

3. Подготовка к установке

Убедитесь, что технические характеристики системы соответствуют минимальным требованиям, описанным в главе Требования к системе.

3.1. Подготовка внешней базы данных

3.1.1. Создание учетных записей

Для повышения безопасности системы необходимо запускать службы SQL Server от имени учетной записи с ограниченными правами. Для реализации подобного запуска можно использовать две учетные записи:

1. служба SQL Server будет запускаться от имени учетной записи 1 (например, SVC-SQL);
2. MaxPatrol будет обращаться к службе SQL Server от имени учетной записи 2 (например, SVC-MPSQL).

Создайте такие учетные записи в операционной системе сервера баз данных. Для них достаточно прав пользователя операционной системы, дополнительных прав не требуется.

3.1.2. Установка и настройка СУБД Microsoft SQL Server 2008 R2

Для установки Microsoft SQL Server 2008 R2 можно выполнить следующие действия:

1. Запустите установку SQL Server 2008 R2.
2. В левой части окна выберите *Installation,* в правой части – перейдите по ссылке *New installation or add features…* (см. Рис. 8).

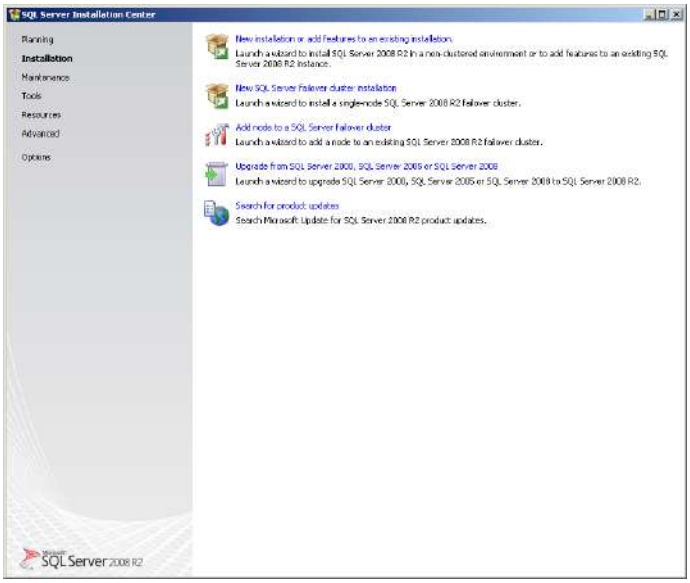

Рис. 8 – Установка Microsoft SQL Server 2008

3. Нажмите *OK* в окне *Setup Support Rules*.

4. Нажмите *Next* в следующем окне. Затем включите опцию *I accept the license terms* и продолжайте установку (см. Рис. 9).

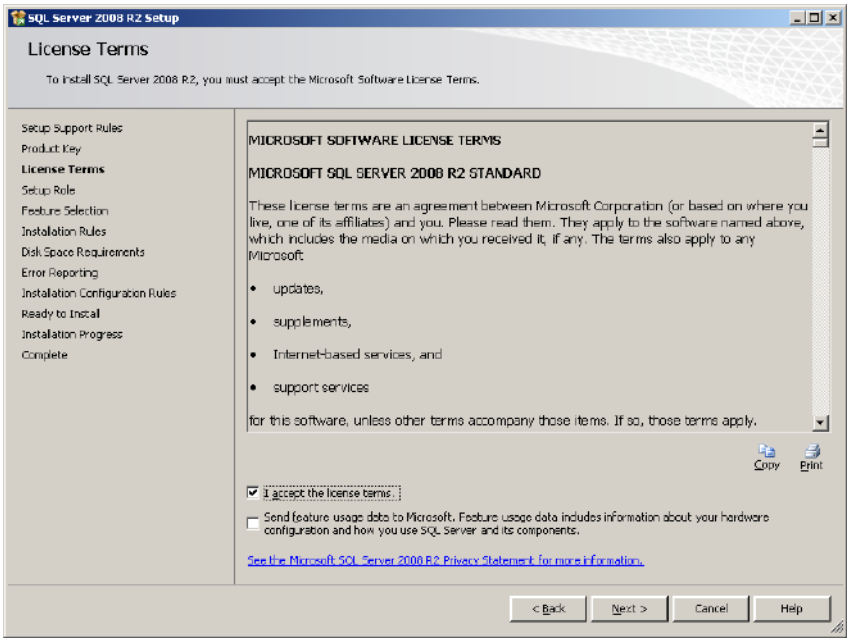

Рис. 9 – Окно *License Terms*

5. Когда появится окно *Setup Role*, выберите *SQL Server Feature Installation* и нажмите *Next* (см. Рис. 10).

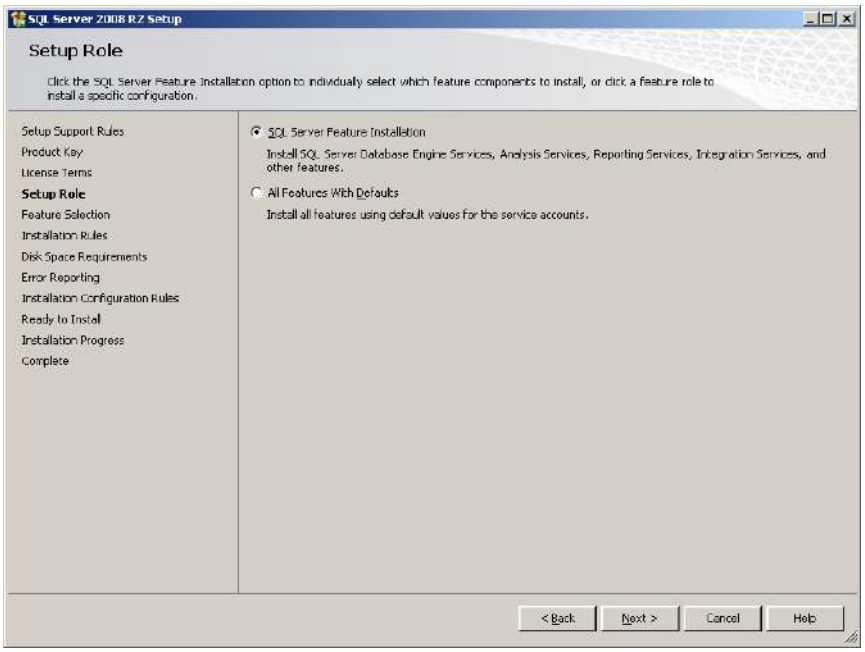

Рис. 10 – Окно *Setup Role*

6. Выберите устанавливаемые компоненты:

- Database Engine Services;

- Client Tool Connectivity;
- Management Tools.

Нажмите Next, чтобы продолжить установку (см. Рис. 11).

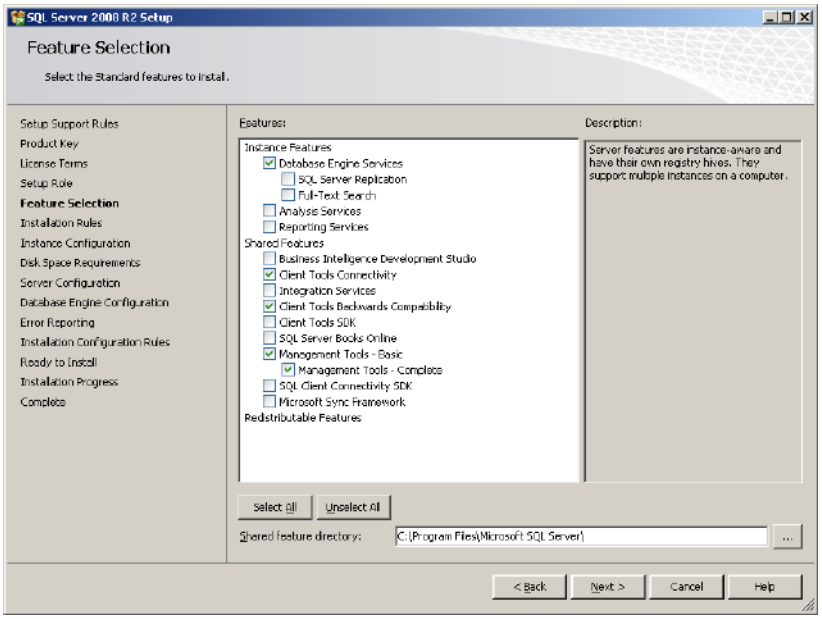

Рис. 11 – Окно выбора устанавливаемых компонентов

7. В окне *Server Configuration* выберите учетную запись, от имени которой будут работать службы SQL Server (см. Рис. 12).

Здесь следует выбрать учетную запись 1.

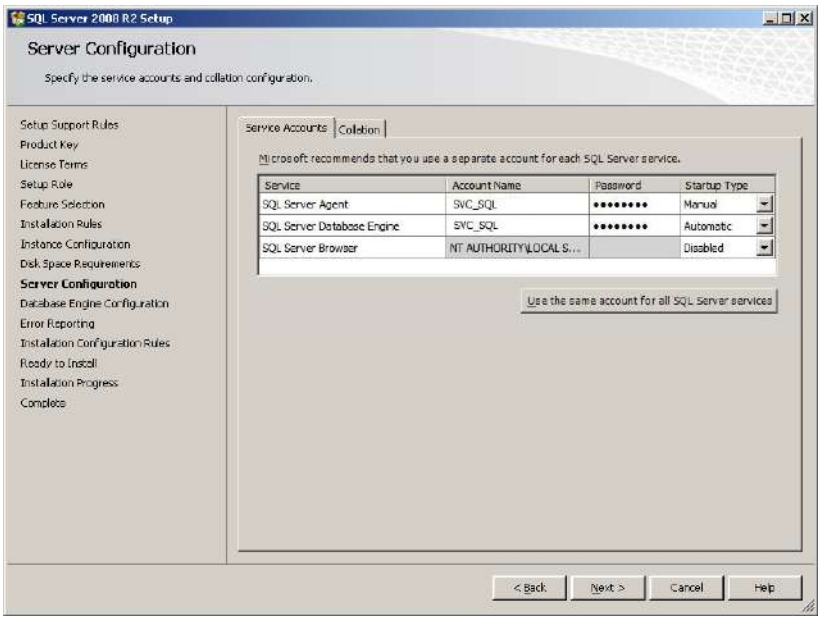

Рис. 12 – Окно выбора учетной записи

8. В окне *Database Engine Configuration* выберите режим аутентификации Windows (см. Рис. 13).

Примечание. Проверка подлинности Windows включена по умолчанию; она обеспечивает более высокий уровень безопасности, чем проверка подлинности SQL Server, так как использует протокол безопасности Kerberos, реализует проверку сложности и надежности паролей, поддерживает блокировку учетных записей по истечении срока пароля. Соединение, установленное с помощью проверки подлинности Windows, иногда называется доверительным соединением (SQL Server доверяет учетным данным, предоставляемым Windows).

9. Укажите учетные записи, которые в последствии будут обладать правами администратора SQL-сервера. Нажмите Next (см. Рис. 13).

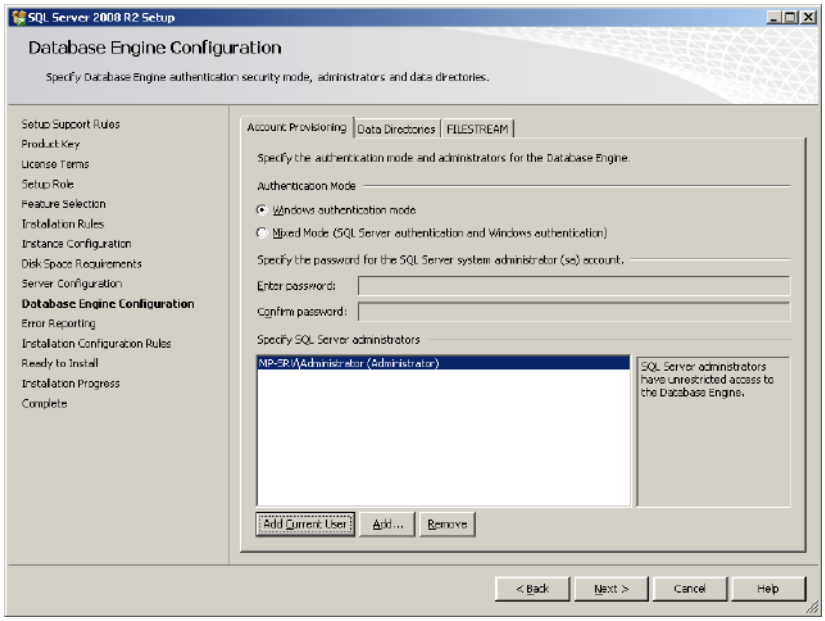

Рис. 13 – Окно выбора режима аутентификации

10. Продолжите установку. Затем нажмите Close для завершения.

3.1.3. Создание базы данных для MaxPatrol

На сервере базы данных создайте БД для MaxPatrol. Сервисную учетную запись, с правами которой MaxPatrol будет обращаться к БД, назначьте владельцем БД MaxPatrol. Для этого средствами SQL Server Management Studio подключитесь к SQL-серверу с правами администратора SQL-сервера и создайте БД для MaxPatrol (см. Рис. 14, Рис. 15).

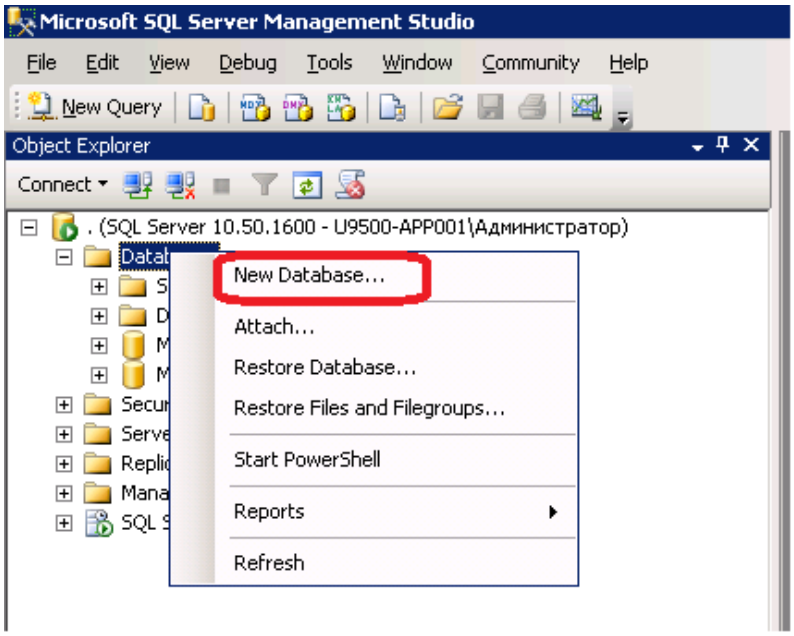

Рис. 14 – Создание БД

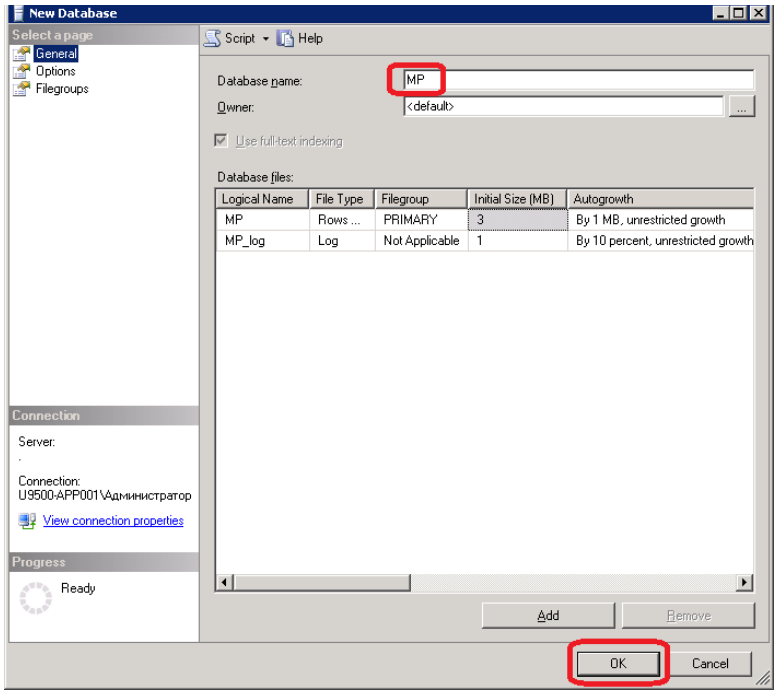

Рис. 15 – Имя новой БД

Затем добавьте вторую сервисную учетную запись в список пользователей БД (см. Рис. 16 и Рис. 17).

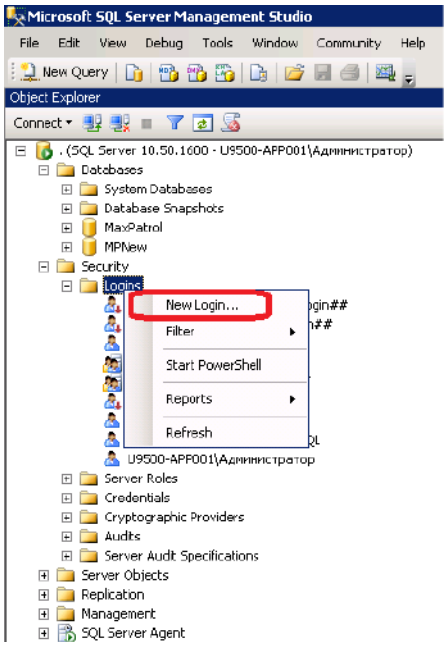

Рис. 16 – Добавление сервисной учетной записи

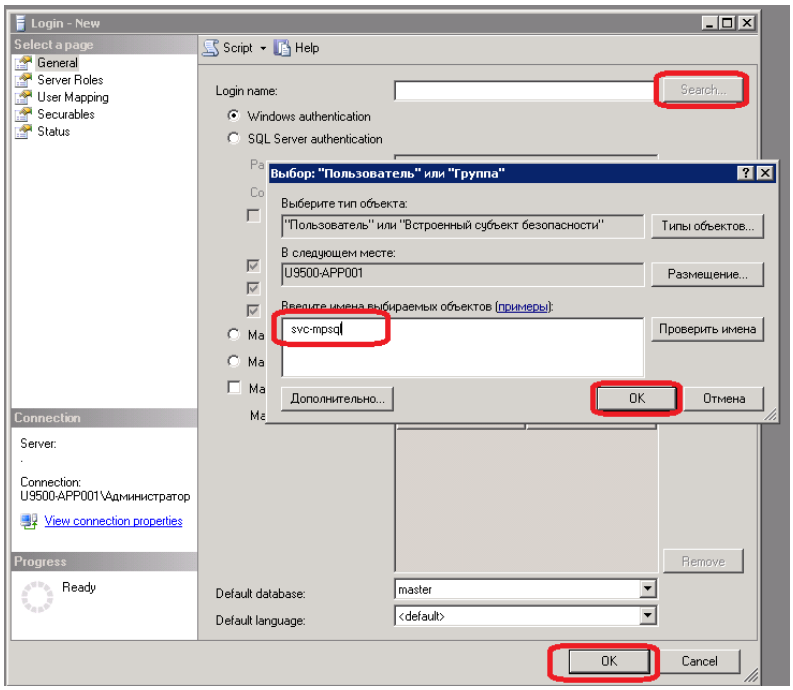

Рис. 17 – Выбор пользователя

Назначьте сервисную учетную запись владельцем БД MaxPatrol (см. Рис. 18) и завершите создание базы данных на SQL-сервере.

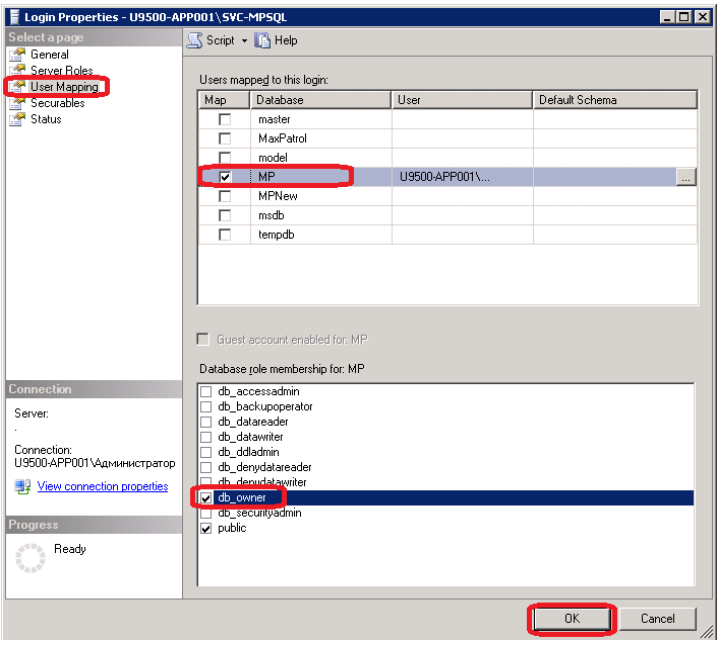

Рис. 18 – Назначение сервисной учетной записи владельцем БД

3.2. Получение дистрибутива

Дистрибутив MaxPatrol можно получить на CD-диске в рамках поставки или загрузить с сервера обновлений. В последнем случае предоставляется гиперссылка с ограниченным сроком действия, например:

http://update.maxpatrol.com/downloads/21A50617-565D-4CCD-851F-0C25A3DAB9F1/MaxPatrol-3385-100411.exe

Дистрибутив системы MaxPatrol представляет собой один исполняемый файл, имя которого формируется следующим образом:

MaxPatrol-<номер лицензии>-<дата сборки в формате ММДДГГ>.exe

Этот файл содержит мастер установки, компоненты системы и одну лицензию.

Дистрибутив может содержать следующие типы лицензий:

- Server – сервер MaxPatrol Server;
- Scanner – сканер MaxPatrol Scanner;
- LUS – локальный сервер обновлений MaxPatrol Local Update Server;
- Consolidator – сервер консолидации MaxPatrol Consolidator;
- Mobile Server – сервер MaxPatrol Mobile Server.

Несколько лицензий могут быть установлены на одном компьютере (кроме Server и Mobile Server, а также Scanner, поскольку лицензия Server подразумевает функциональность сканера).

Мастер установки позволяет установить на компьютер серверные компоненты системы MaxPatrol в соответствии с приобретенной лицензией. Вы можете установить неограниченное количество клиентских рабочих мест MP Console, так как эти рабочие места не лицензируются.

4. Установка системы

Мастер установки позволяет выбрать компонент, который требуется установить на конкретном узле: это может быть MaxPatrol Server, MaxPatrol Console или оба компонента сразу. Выбирая опцию «Установка сервера», следует помнить, что управление системой MaxPatrol осуществляется через консоль, которая может быть установлена как на данном узле, так и на другом узле при условии возможности соединения с MaxPatrol Server.

Внимание! Для установки системы MaxPatrol необходимо обладать правами локального администратора.

4.1. Установка сервера

Чтобы установить на узле MaxPatrol Server, выполните следующие действия:

1. Запустите мастер установки MaxPatrol и нажмите *Далее* в окне приветствия.
2. В окне лицензионного соглашения выберите пункт «Я принимаю условия соглашения».
3. В окне «Выбор каталога установки» выберите каталог установки.
4. В окне «Выбор типа установки» выберите пункт «Полная установка».
5. В следующем окне укажите каталог в меню «Пуск», где будут созданы ярлыки для программы MaxPatrol.
6. В окне «Настройка сервера» укажите имя сервера, номер используемого TCP-порта и сертификат открытого ключа (см. Рис. 19).

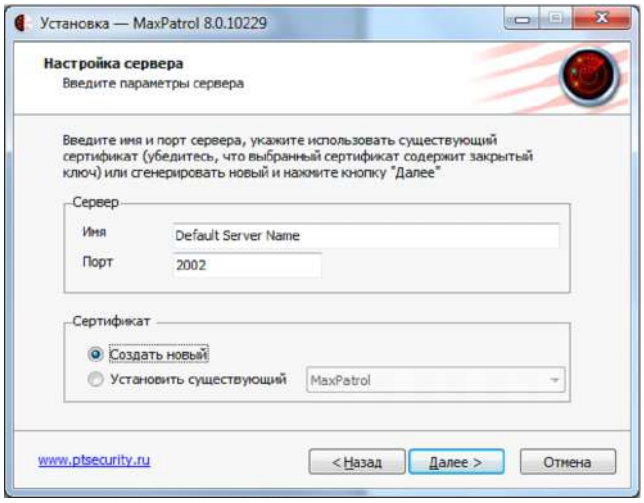

Рис. 19 – Окно настроек сервера

Имя сервера будет использоваться для идентификации экземпляра MaxPatrol Server в рамках системы, поэтому желательно использовать понятное мнемоническое наименование.

Цифровой сертификат требуется для аутентификации взаимодействующих сторон и защиты передаваемых данных. В зависимости от выбранного сценария

развертывания может использоваться как сертификат, выданный внешним или корпоративным удостоверяющим центром, так и самоподписанный сертификат, который создается на этапе установки системы. При нажатии кнопки *Далее* на экран выводится идентификатор выбранного сертификата (fingerprint) (см. Рис. 20).

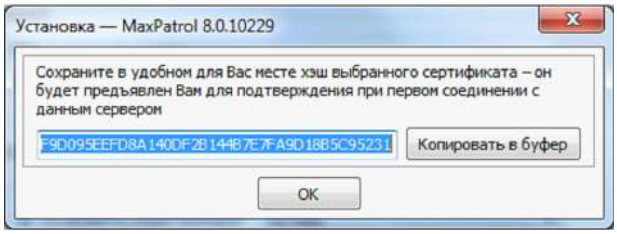

Рис. 20 – Идентификатор сертификата

Если используется самоподписанный сертификат, то при первой попытке установить соединение потребуется вручную подтвердить его подлинность. После установки сертификат может быть изменен на вкладке «Настройки» в MaxPatrol Console.

7. В окне «Ввод пароля администратора» задайте пароль учетной записи, которая будет обладать правами администратора и иметь максимальные привилегии по отношению к данному экземпляру MaxPatrol Server. Имя этой учетной записи фиксировано – Administrator.

Примечание: используйте сложный пароль.

8. В следующем окне выберите тип базы данных, которая будет использоваться MaxPatrol Server для хранения результатов сканирования (см. раздел Требования к СУБД).
При выборе встроенной базы данных не требуется указывать дополнительные параметры.
При выборе внешней базы данных под управлением MS SQL Server, которая должна быть предварительно настроена (см. раздел Подготовка внешней базы данных), необходимо указать:

• Для случая, когда СУБД установлена на том же сервере, где разворачивается MP (см. Рис. 21):

- Имя сервера: . (точка);
- Windows-аутентификация;
- Отключить опцию «Использовать текущие учетные данные»;
- Имя входа и пароль: указать сервисную учетную запись (SVC-MPSQL) и ее пароль;

Имя БД: выбрать БД MaxPatrol.

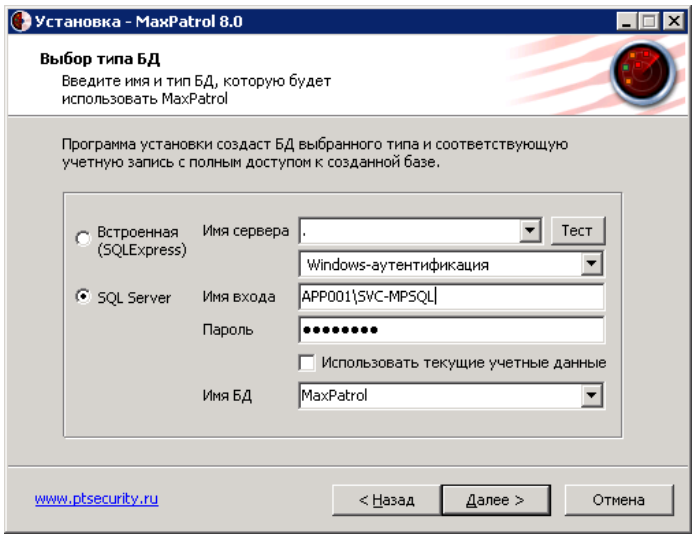

Рис. 21 – Указание параметров СУБД, установленной на сервере с MaxPatrol

- Для случая, когда СУБД установлена на удаленном сервере (см. Рис. 22):
  - Имя сервера: IP-адрес, либо DNS-имя удаленного сервера БД;
  - Windows-аутентификация;
  - Отключить опцию «Использовать текущие учетные данные»;
  - Имя входа и пароль: если используется учетная запись ОС (не доменная), то следует обратить внимание на имя сервера (учетная запись указывается в формате имя сервера\имя учетной записи);
  - Имя БД: выбрать БД MaxPatrol.

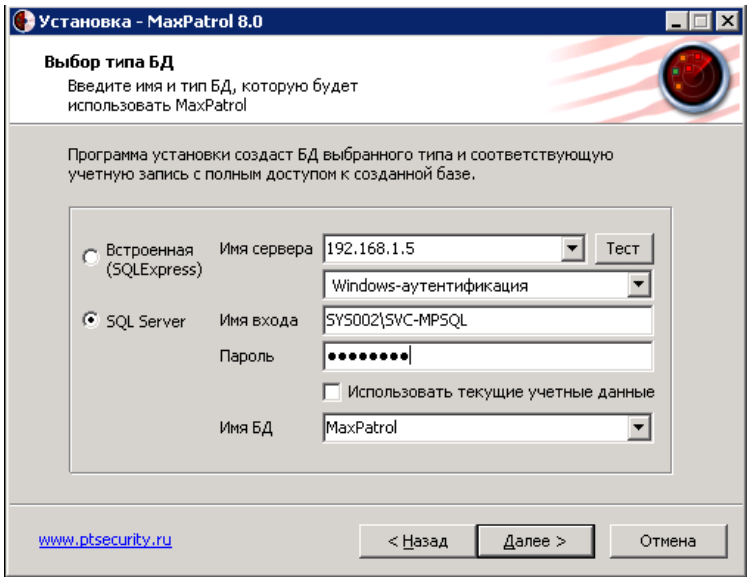

Рис. 22 – Указание параметров СУБД, установленной на удаленном сервере

Нажмите *Далее*.

Внимание! В дальнейшем можно изменить параметры доступа к базе данных с помощью вкладки «Настройки» в MaxPatrol Console.

9. При выборе внешней БД мастер установки предложит создать новую базу данных либо подключиться к существующей. Введите соответствующие данные в открывшемся диалоговом окне и нажмите *OK*.

10. Следующие два шага – проверка системы на соответствие минимальным требованиям (подробнее см. Требования к системе) и подтверждение выбранных настроек. Нажмите *Установить*, чтобы запустить процесс установки MaxPatrol Server.

Внимание! По окончании установки проверьте дату и время на сервере, поскольку они имеют большое значение для функционирования системы.

4.2. Установка сканера

Компонент MaxPatrol Scanner (MP-SCN) является дополнительным компонентом, который подключается к MP Server и работает под его управлением. Сканер используется в качестве элемента масштабирования, например, при необходимости сканирования большого количества сетевых объектов за определенный промежуток времени.

Установка MaxPatrol Scanner аналогична установке MaxPatrol Server. После установки, активации лицензии и обновления следует подключить MaxPatrol Scanner к MaxPatrol Server. Для этого на сканере необходимо создать системную учетную запись для подключения к серверу и настроить соединение с MaxPatrol Server:

1. Запустите консоль управления MaxPatrol: «Пуск» (Start) – «Программы» (Programs) – Positive Technologies – MaxPatrol – MaxPatrol.

2. В параметрах соединения укажите сетевое имя или IP-адрес MaxPatrol Scanner, а также пароль учетной записи *Administrator*, заданный при установке.

3. Переключитесь на закладку «Настройки» – «Пользователи» и нажмите на кнопку *Добавить пользователя* (см. Рис. 23). Создаваемый пользователь должен входить в группу *Administrators*.

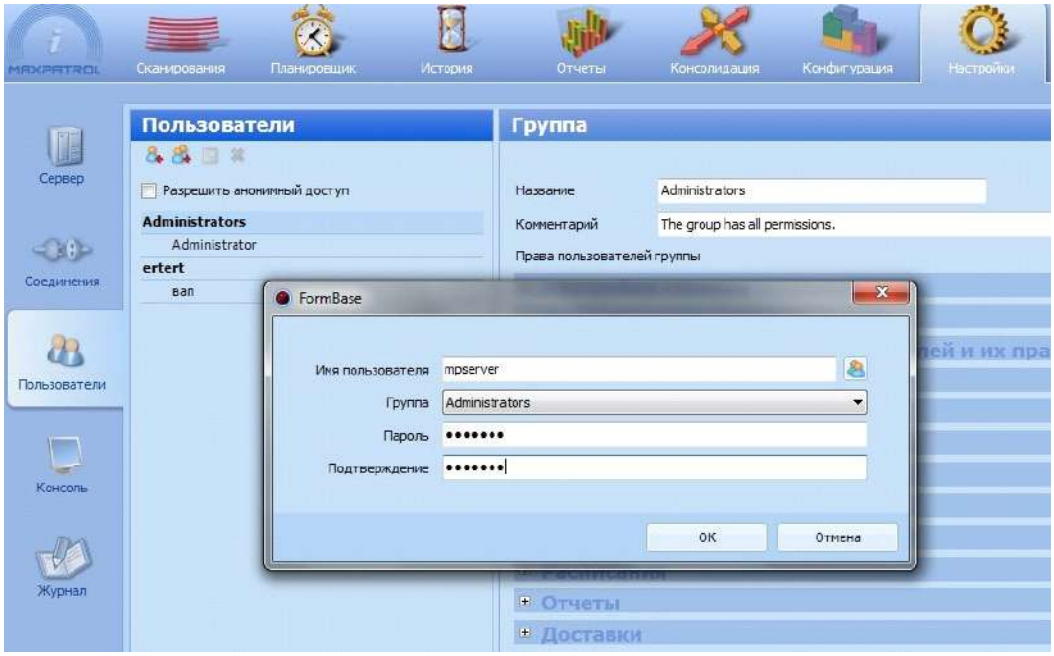

Рис. 23 – Добавление пользователя

4. Соединитесь с экземпляром MaxPatrol Server, к которому планируется подключить сканер: на закладке «Настройки» - «Соединения» нажмите кнопку *Добавить новое соединение* (см. Рис. 24).

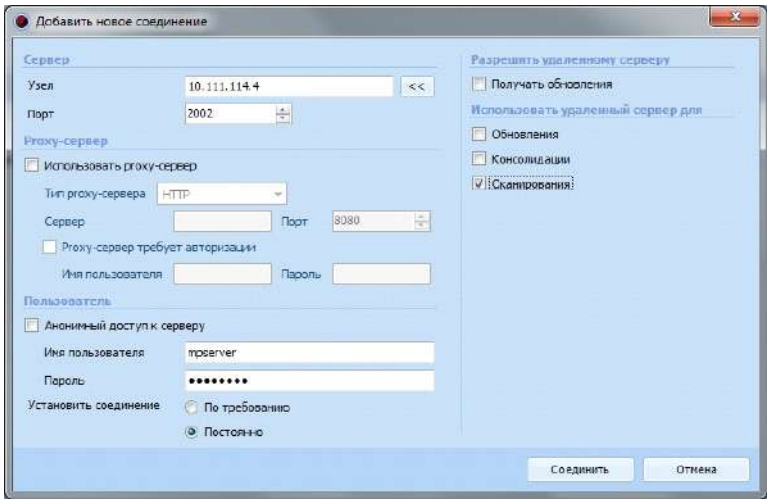

Рис. 24 – Настройка соединения сервера со сканером

5. В поле «Сервер» – «Узел» укажите IP-адрес или сетевое имя подключаемого сканера. В разделе «Пользователь» отключите опцию «Анонимный доступ к серверу» и укажите имя пользователя и пароль для учетной записи, созданной на сканере. Выберите режим постоянного соединения («Установить соединение» – «Постоянно»). Укажите опцию «Использовать удаленный сервер для» – «Сканирования» и нажмите кнопку *Соединить*.

6. Переключитесь на закладку «Сканирование» – «Сканеры» и нажмите на кнопку ✚ (*Добавить*). Укажите в списке подключенный сканер и нажмите *OK* (см. Рис. 25).

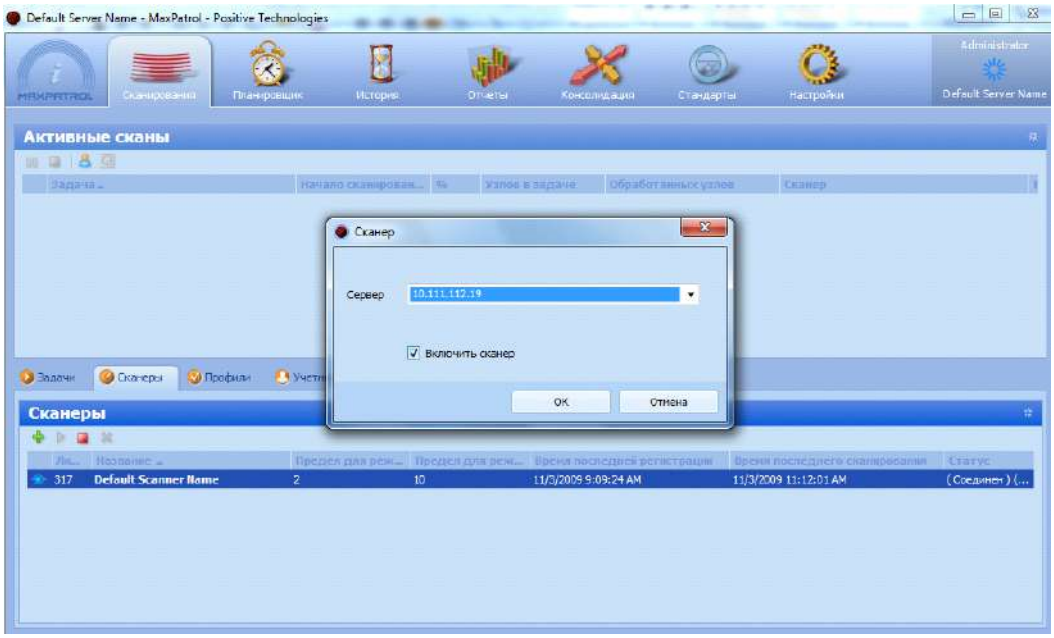

Рис. 25 – Подключение сканера

Если операция прошла успешно, сканер появится в списке доступных сканеров.

Настройка обновления MaxPatrol Scanner проводится аналогично настройкам обновления других компонентов.

4.3. Защита установки

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

5. Первый запуск

При запуске системы MaxPatrol появляется окно «Соединение», где требуется указать адрес сервера, а также имя учетной записи и пароль. По умолчанию в системе существует пользователь *Administrator*, пароль которого задается в процессе установки.

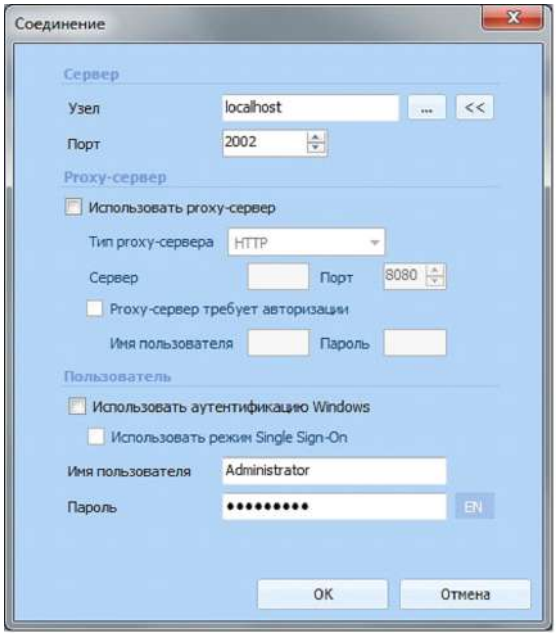

Рис. 26 – Соединение с сервером MaxPatrol

При первом подключении компоненты MaxPatrol автоматически пытаются пройти активацию на глобальном сервере обновлений *update.maxpatrol.com*. При этом используются стандартные настройки (прямое подключение, порт *2002/TCP*).

Если подключение к сети Интернет ограничено (запрещено использование порта 2002/TCP или используется прокси-сервер), следует отказаться от автоматической активации и изменить настройки подключения к серверу обновлений. Подробные инструкции см. в разделе Первоначальное подключение к серверу обновлений.

Посмотреть информацию о продукте можно, нажав пиктограмму *i* в верхнем левом углу консоли и выбрав в контекстном меню пункт «О программе MaxPatrol». В открывшемся окне указана версия консоли, информация о текущем сервере, а также ссылка на руководство администратора, расположенное на сайте технической поддержки (см. Рис. 27).

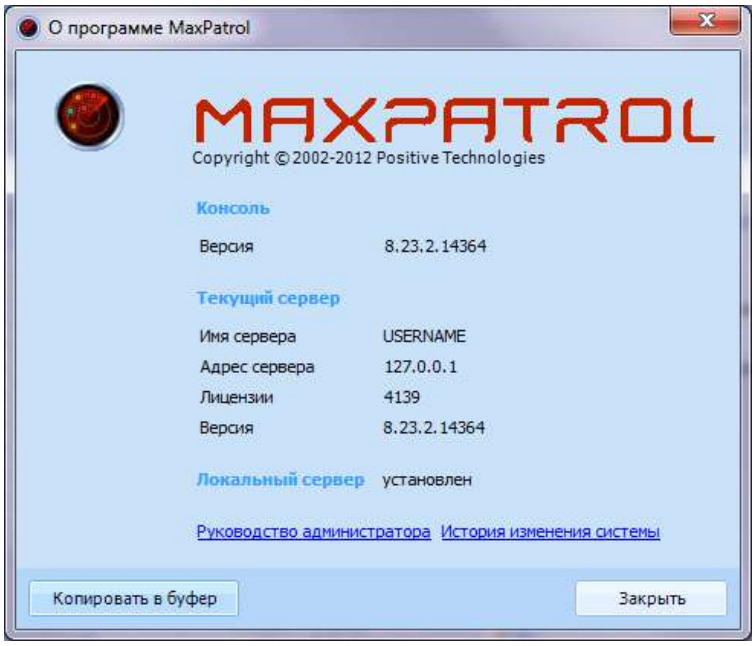

Рис. 27 – Окно информации о программе MaxPatrol

6. Первоначальная настройка

6.1. Планирование системы обновления

Система обновлений является важным компонентом MaxPatrol. Еженедельно обнаруживаются и устраняются десятки уязвимостей, и команда Positive Technologies делает все возможное, чтобы поддерживать базу знаний в актуальном состоянии.

Выпускаемые обновления отличаются по объему и частоте выхода. Политика обновлений продуктов линейки MaxPatrol представлена в Табл. 17.

Таблица 17. Политика обновлений MaxPatrol

Тип обновления	Описание	Объем, МБ					Период
		MP Server (PAC)	MP Server (PA)	MP Server (P)	MP LUS	MP Scanner (PAC)	
Оперативные обновления	Содержат информацию о срочных или критических уязвимостях	~3,7	~3,7	~3,7	~3,7	~9	По мере необходимости
Плановые обновления базы знаний	Содержат информацию о новых уязвимостях, ошибках и стандартах	~93	~94	~93	~92	~95	Еженедельно
Новые выпуски ПО (релизы)	Содержат новые версии программного обеспечения MaxPatrol	~402	~395	~395	~393	~395	Ежемесячно, по мере выхода
Оперативное исправление ошибок ПО	Содержат исправления ошибок программного обеспечения MaxPatrol	~4,5	~4,5	~4,5	~4,5	~10	В случае обнаружения критических ошибок

Основным компонентом системы обновлений являются серверы Positive Technologies, которые расположены по адресу update.maxpatrol.com. Эти серверы ожидают соединения на портах 443/TCP и 2002/TCP.

В ходе планирования системы обновления решаются следующие вопросы:

- эффективное использование пропускной способности каналов связи;
- адаптация под сетевую инфраструктуру и средства защиты;
- реализация обновлений в сетях, отключенных от интернета.

Основным инструментом, позволяющим управлять топологией обновлений, является локальный сервер обновлений MaxPatrol Local Update Server (MP LUS). Серверы MP LUS могут объединяться в цепочки, что позволяет реализовывать структуру обновлений произвольной сложности.

Можно выделить два основных варианта реализации системы обновления:

- топология Online – для сетей с подключением к интернету;
- топология Offline – для сетей без подключения к интернету.

MP LUS может управлять поступающими обновлениями, что позволяет устанавливать на серверы только те обновления, которые отвечают внутренней политике безопасности. Администраторы MP LUS используют систему фильтрации, указывая для поступающего пакета статус одобрения.

6.1.1. Топология Online

Данный вариант обновления подходит для систем, имеющих прямое подключение к интернету или подключение к интернету через межсетевые экраны различных типов.

Пример сложной топологии обновления дан на Рис. 28.

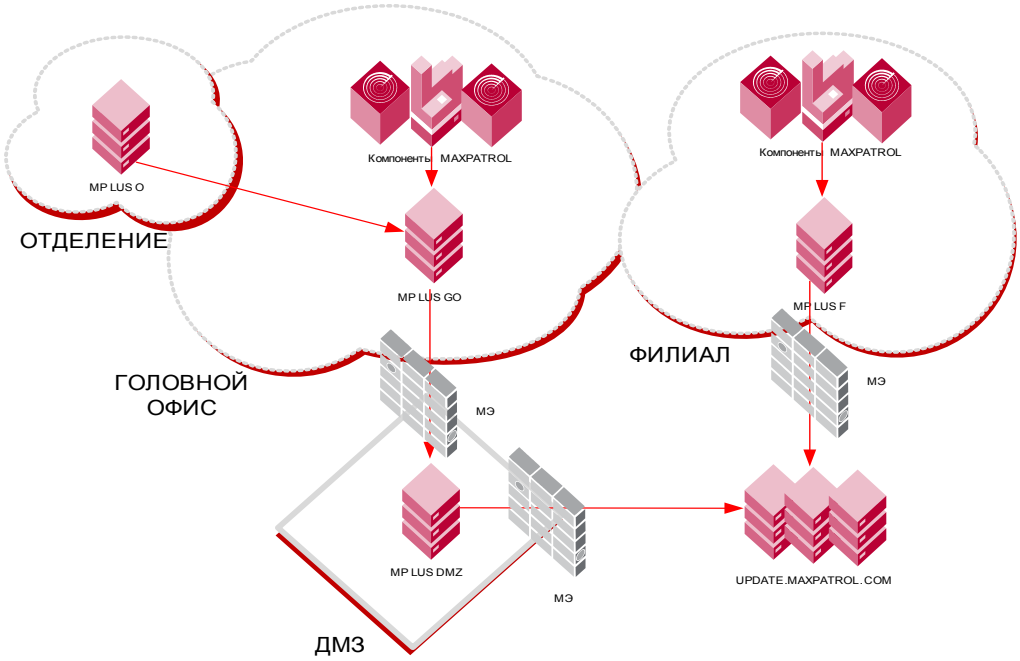

Рис. 28 – Топология Online

Сервер MP LUS DMZ получает обновления от сервера обновлений компании Positive Technologies. Полученные обновления передаются на сервер MP LUS GO, который используется для обновления компонентов MaxPatrol в головном офисе. В отделении, не имеющем собственного подключения к интернету, установлен MP LUS O, который

загружает новые версии с MP LUS GO. В филиале установлен MP LUS F, который подключается непосредственно к серверам обновлений Positive Technologies.

Протокол обновлений, который используется компонентами MaxPatrol и MP LUS, может использовать произвольный TCP-порт, указанный в настройках системы. Стандартный порт – 2002/TCP. Серверы LUS поддерживают следующие типы межсетевых экранов:

- трансляция сетевых адресов (NAT/PAT);
- HTTP-connect proxy;
- Socks4 proxy;
- Socks5 proxy.

При необходимости может быть задействована аутентификация на межсетевом экране с использованием методов Basic, NTLM и Negotiate.

6.1.2. Топология Offline

Данный вариант подходит для систем, которые не имеют прямого подключения к интернету.

Пример такой топологии обновления приведен на Рис. 29.

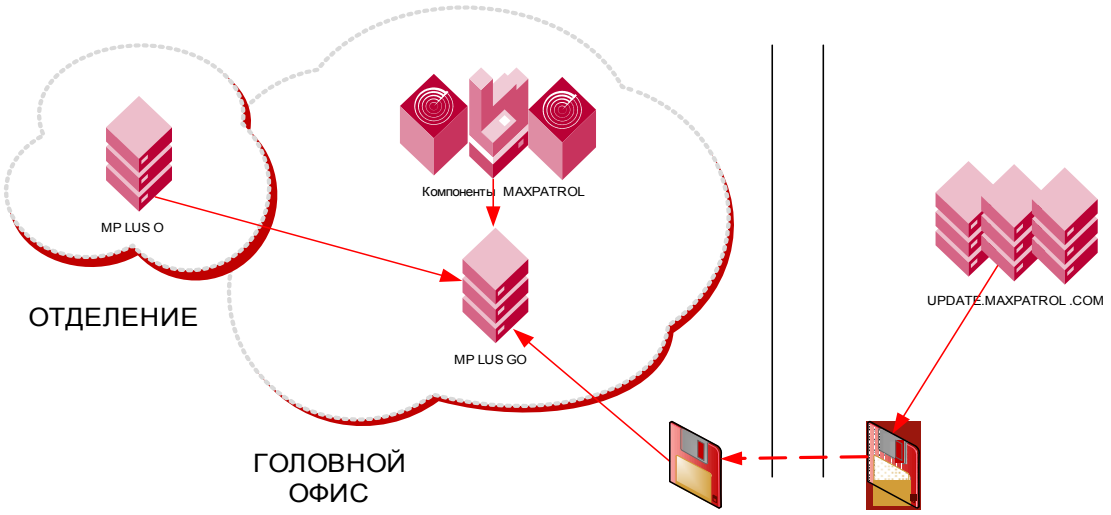

Рис. 29 – Топология Offline

Поскольку рассматриваемая сеть не имеет прямого подключения к интернету, в головном офисе размещается MP LUS. Обновления для системы загружаются с серверов обновления Positive Technologies и доставляются каким-либо offline-методом, например, с использованием внешних носителей информации. Комплект обновлений инсталлируется на MP LUS, а затем его получают нижестоящие серверы обновлений и компоненты MaxPatrol.

6.2. Первоначальное подключение к серверу обновлений

При первом подключении консоли система MaxPatrol автоматически пытается подключиться к глобальному серверу обновлений *update.maxpatrol.com*. При этом используются стандартные настройки (прямое подключение, порт *2002/TCP*).

Вы можете изменить настройки подключения к серверу обновлений, например, в случае если подключение к сети Интернет ограничено (запрещено использование порта 2002/TCP или используется прокси-сервер). Для этого выполните следующие действия:

1. Запустите консоль управления: «Пуск» (Start) – «Программы» (Programs) – Positive Technologies – MaxPatrol – MaxPatrol.

2. В появившемся окне укажите адрес сервера, имя учетной записи и пароль. По умолчанию в системе существует пользователь *Administrator*, пароль которого задается в процессе установки.
Если система предложит провести автоматическую активацию лицензии, то следует отказаться.

3. В открывшемся окне консоли перейдите на вкладку «Настройки» – «Соединения».

4. По умолчанию в окне присутствует только одно соединение с сервером *update.maxpatrol.com*, порт *2002/TCP*. Для изменения настроек выделите соединение, щелкните правой кнопкой мыши и в появившемся контекстном меню выберите пункт «Изменить»:

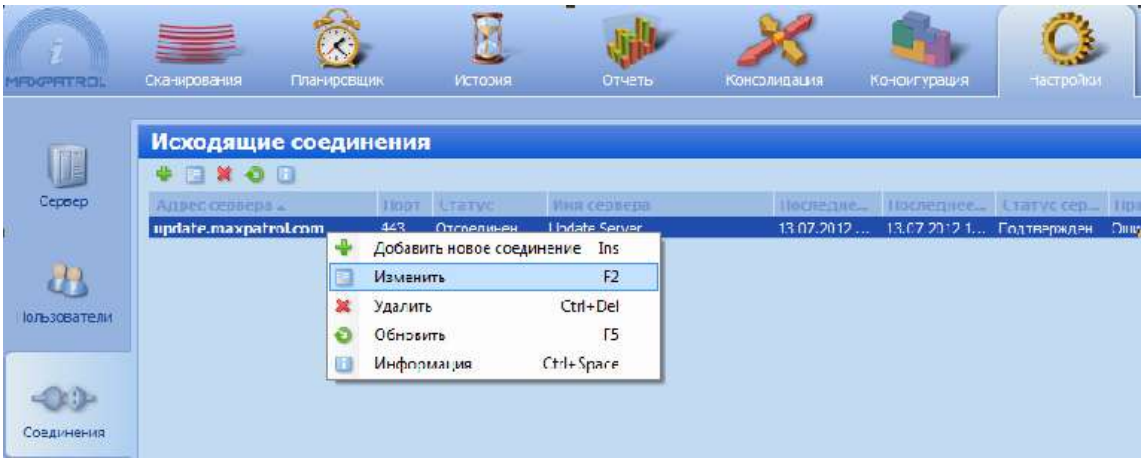

Рис. 30 – Контекстное меню соединения

5. В открывшемся окне «Редактирование соединения» (см. Рис. 31) можно указать номер TCP-порта (2002, 443), а также параметры прокси-сервера (тип, имя и номер порта, учетную запись для аутентификации).
Чтобы система использовала данное соединение для обновления и привязки

лицензии, активируйте опции «Анонимный доступ к серверу» и «Использовать удаленный сервер для» – «Обновления».

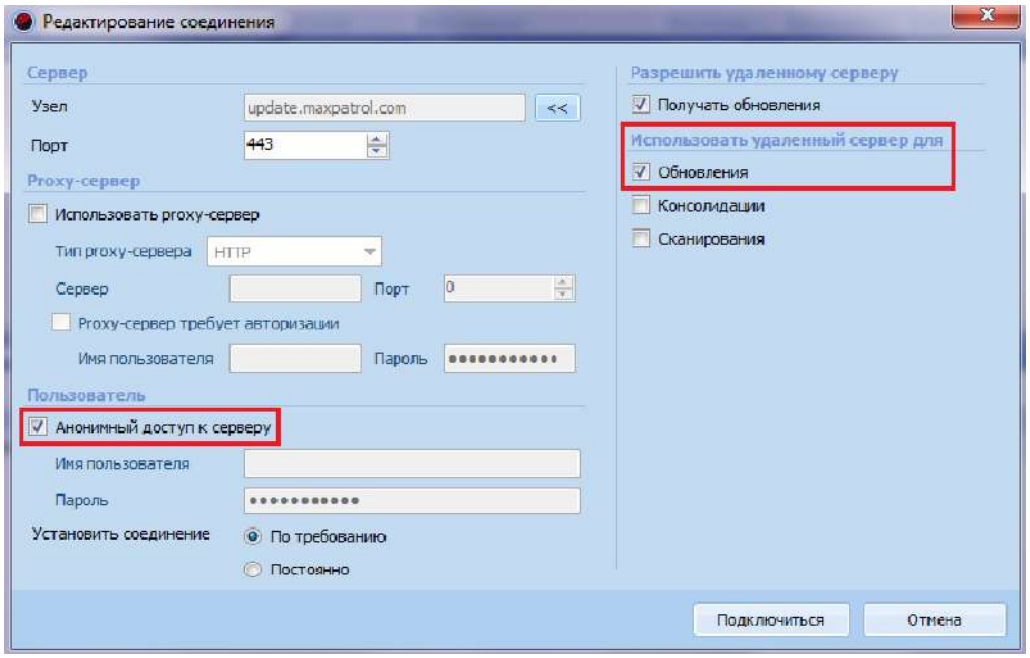

Рис. 31 – Редактирование соединения

Примечание: сервер MaxPatrol автоматически определяет доступные методы аутентификации (Basic, NTLM, NTLMv2) и использует наиболее безопасный из них.

6. После нажатия кнопки *Подключиться* система попытается подключиться к указанному серверу. Если сервер использует самоподписанный или недоверенный сертификат, то появится сообщение с идентификатором сертификата и просьбой подтвердить его корректность.

Проверить корректность подключения можно в окне информации о соединении, нажав кнопку в панели инструментов (см. Рис. 32).

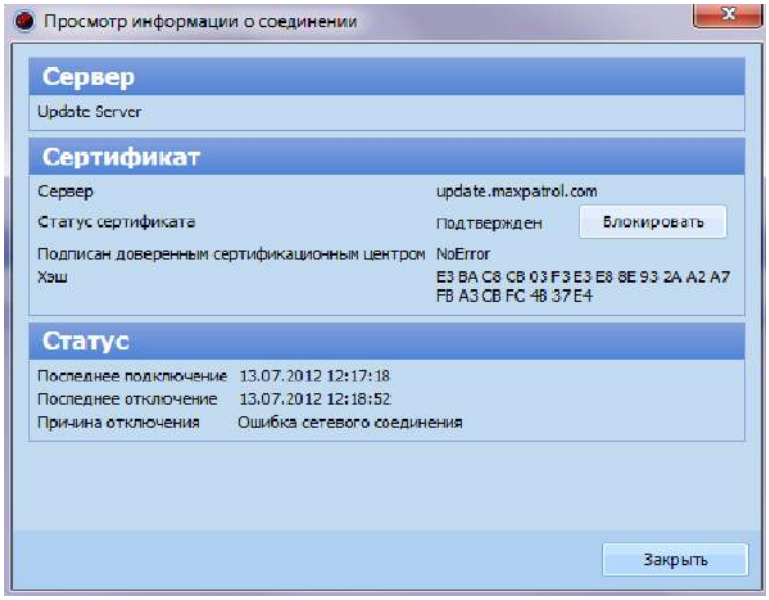

Рис. 32 – Информация о соединении

7. После успешного подключения к серверу обновления перейдите на вкладку «Настройки» – «Сервер» и в панели «Обновления» нажмите *Изменить*. Укажите созданное соединение в окне «Настройки обновления».

6.3. Настройка расписания обновлений

MaxPatrol Console позволяет обновлять систему MaxPatrol вручную или автоматически, согласно установленному расписанию обновлений. Для корректной работы системы автоматического обновления необходимо наличие соединения с сервером обновлений (update.maxpatrol.com).

Для обновления вручную переключитесь на вкладку «Настройки» – «Сервер» и нажмите ссылку *Проверить* в панели «Обновления». Если на сервере обновлений есть более новые сборки продукта, установленная версия MaxPatrol обновится.

Внимание! В ходе обновления консоль потеряет соединение с сервером и в течение нескольких минут не сможет подключиться к системе.

Если обновление не выполняется, убедитесь, что в поле «Сервер обновлений» указано корректное соединение, это соединение подключено, а в его свойствах выбрана опция «Использовать удаленный сервер для» – «Обновления» («Настройки» – «Соединения»– пункт «Информация» контекстного меню).

Для настройки расписания автоматических обновлений переключитесь на вкладку «Настройки» – «Сервер» и нажмите кнопку *Изменить* в панели «Обновления». В области «Расписание» открывшегося диалогового окна можно настроить частоту и время автоматических обновлений (см. Рис. 33).

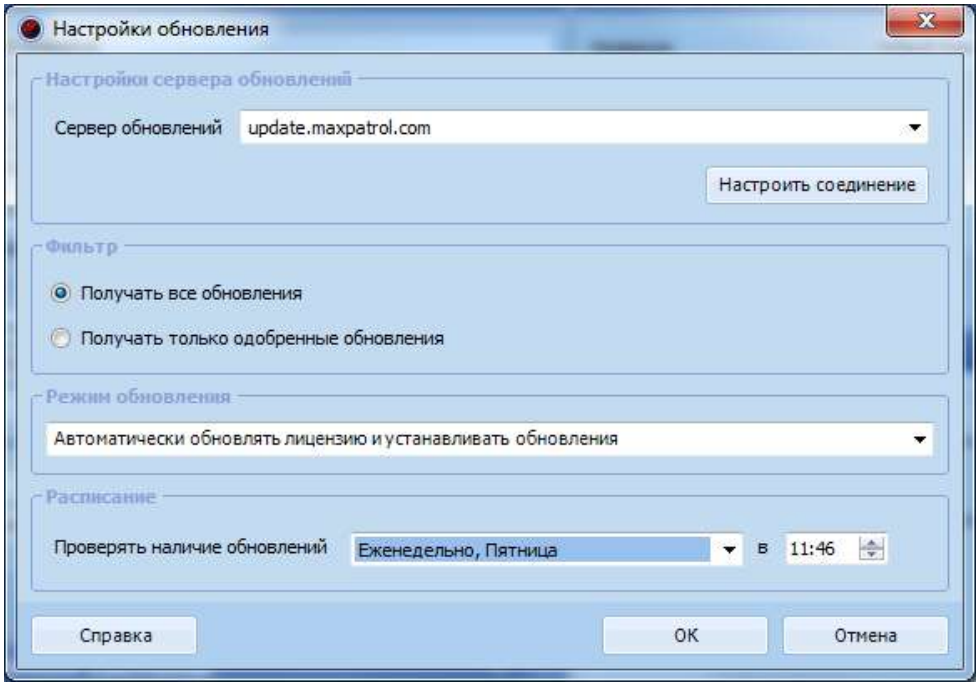

Рис. 33 – Настройка расписания обновлений

После обновления и подключения к системе может потребоваться обновление консоли. В этом случае консоль выдаст соответствующее предупреждение и автоматически установит обновления.

6.4. Активация лицензии

Поставляемая в дистрибутиве лицензия не привязана к конкретному компьютеру. Это позволяет запускать и конфигурировать серверные компоненты. Для использования основных функций компонентов MaxPatrol (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.

Компоненты MaxPatrol автоматически пытаются пройти активацию на глобальном сервере обновлений *update.maxpatrol.com* при первом подключении консоли. При этом используются стандартные настройки (прямое подключение, порт 2002/TCP).

6.4.1. Offline-активация и обновление лицензий

Для активации лицензий MaxPatrol на серверах, которые находятся в изолированных от сети Интернет сегментах, необходимо в такой изолированный сегмент сети установить сервер MP-LUS (MaxPatrol Local Update Server) и активировать его, а затем провести процедуру активации компонентов.

Активация лицензий в режиме offline происходит по следующему алгоритму:

- активировать MP-LUS (действие выполняется один раз);
- сгенерировать запрос на активацию компонента напрямую или подключив соответствующий компонент к MP-LUS;
- получить ответ от сервера https://service.maxpatrol.com;

Примечание. Для выполнения операции требуется подключение к сети Интернет и наличие учетной записи для авторизации. Получить учетную запись можно, зарегистрировавшись на сайте технической поддержки (https://support.ptsecurity.com) и отправив заявку с темой «Получение учетной записи для offline-активации лицензий MaxPatrol». Учетные данные будут переданы на указанный в заявке электронный адрес.

- активировать компонент.

6.4.1.1. Активация сервера обновлений MaxPatrol в изолированной сети

Для использования сервера MP-LUS (MaxPatrol Local Update Server) с возможностью активации компонентов MaxPatrol в изолированной сети требуется сначала активировать его лицензию.

Чтобы активизировать сервер обновления MaxPatrol в режиме Offline, выполните следующее:

1. Подключитесь к MP-LUS через консоль при запуске или настройте соединение в процессе работы, как показано на Рис. 34. В окне «Соединение» укажите имя или IP-адрес узла, на котором находится компонент, а также имя пользователя и пароль для подключения к этому узлу.

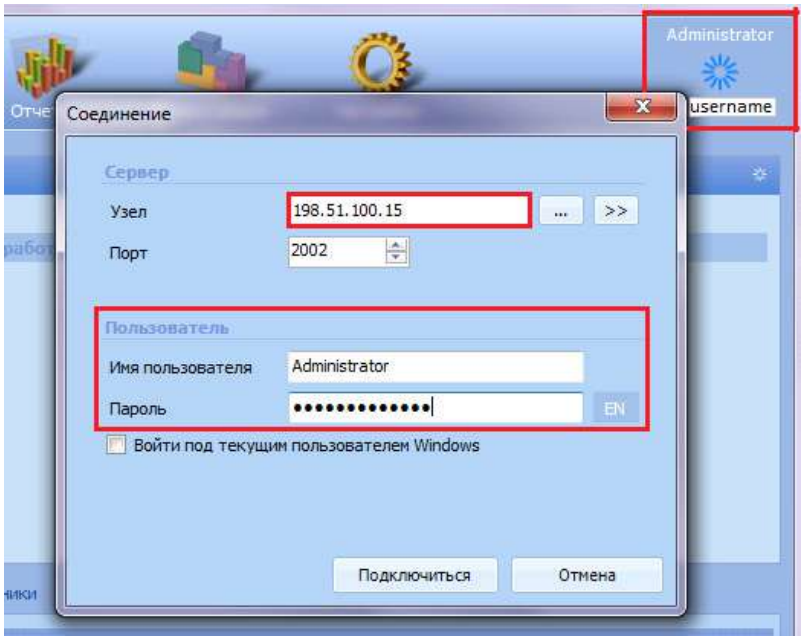

Рис. 34 – Подключение к компоненту MaxPatrol

2. Перейдите на вкладку «Настройки» – «Сервер» и включите опцию «Режим обновления Offline» (см. Рис. 35). Нажмите *Применить*.

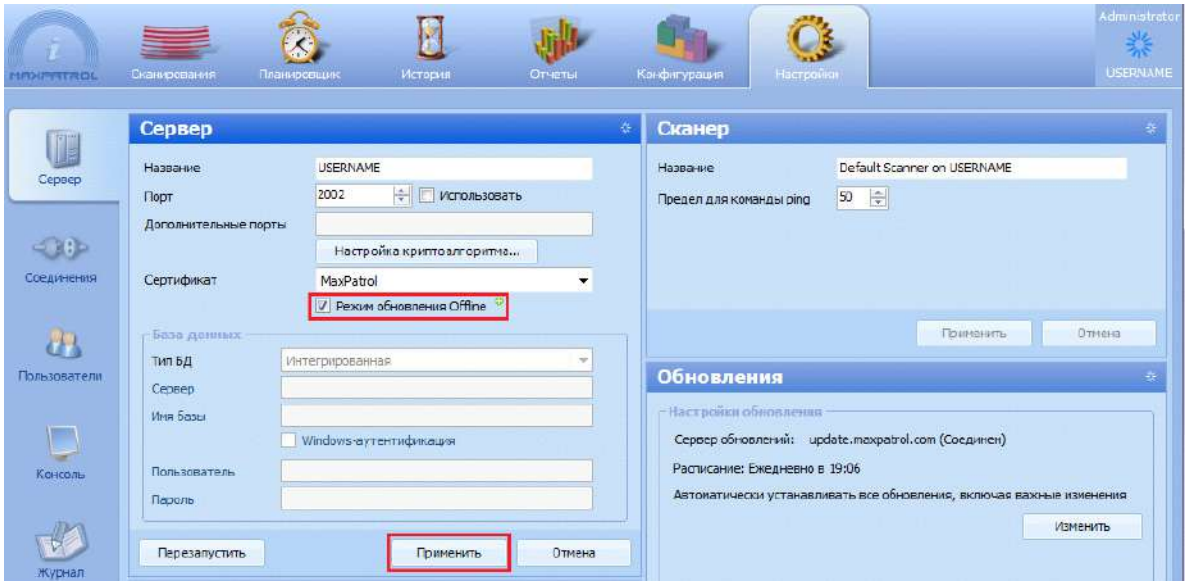

Рис. 35 – Включение режима обновления Offline

3. В панели «Лицензия» нажмите кнопку  («Сформировать запрос на активацию лицензии») и сохраните на съемный носитель файл OFR с запросом на активацию лицензии.

4. Загрузите файл запроса через интерфейс offline-активации лицензий https://service.maxpatrol.com (см. Рис. 36) или отправьте его в службу поддержки Positive Technologies другим способом.

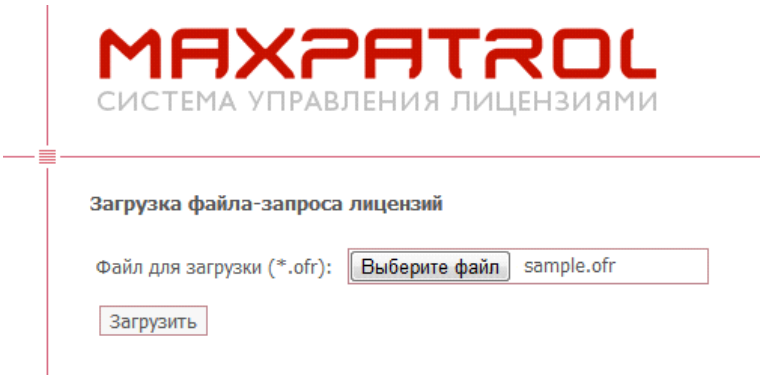

Рис. 36 – Загрузка файла запроса

Примечание: для выполнения операции требуется подключение к сети Интернет и наличие учетной записи для авторизации. Получить учетную запись можно, зарегистрировавшись на сайте технической поддержки (https://support.ptsecurity.com) и отправив заявку с темой «Получение учетной записи для offline-активации лицензий MaxPatrol». Учетные данные будут переданы на указанный в заявке электронный адрес.

5. После обработки запроса появится соответствующее сообщение и ссылка для скачивания файла ответа OFL (см. Рис. 37).

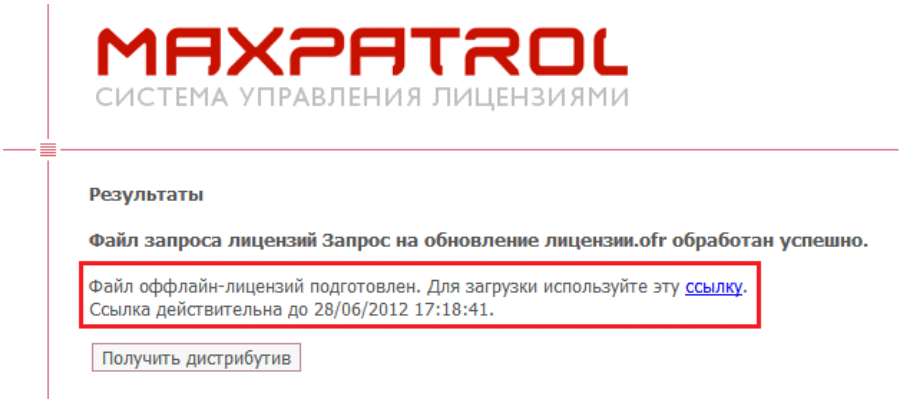

Рис. 37 – Получение файла ответа

Если вы отправляли запрос по электронной почте, OFL-файл будет выслан на обратный адрес.

6. Скачайте файл OFL; его имя соответствует имени файла запроса OFR.

7. Загрузите файл-ответ через консоль MaxPatrol, используя кнопку («Импортировать лицензию в режиме offline») на панели «Настройки» – «Сервер».

8. Сервер обновлений готов к работе.

6.4.1.2. Активация компонентов MaxPatrol в изолированной сети

Активация компонентов системы MaxPatrol в изолированной сети может проводиться двумя способами:

- через локальный сервер обновлений MaxPatrol (лицензия локального сервера должна давать возможность работать в режиме Offline);
- через специальный веб-интерфейс на сайте https://service.maxpatrol.com (активируемая лицензия должна давать возможность работать в режиме Offline).

6. 4. 1. 2. 1. ***Активация компонентов MaxPatrol в изолированной сети через локальный сервер обновлений MaxPatrol***

Для активации выполните следующие действия:

1. Подключите требующие активации компоненты MaxPatrol к серверу MP-LUS и убедитесь, что в панели «Сервер» включена опция «Режим обновления Offline» (вкладка «Настройки» – «Сервер»).

2. В панели «Лицензия» нажмите кнопку («Сформировать запрос на активацию лицензии») для активации лицензии.

Если требуется обновление лицензии, нажмите кнопку («Сформировать запрос на обновление лицензии).

3. Сервер MP-LUS зарегистрирует запрос на активацию или обновление. Подключитесь к серверу MP-LUS через консоль (см. Рис. 36) и сохраните на

съемный носитель файл(ы) OFR с запросом на активацию или обновление лицензии с помощью кнопки («Сформировать запрос на активацию лицензии») или («Сформировать запрос на обновление лицензии») на панели «Лицензии» вкладки «Настройки» – «Сервер».

4. Загрузите файл запроса через интерфейс offline-активации лицензий https://service.maxpatrol.com или отправьте его в Службу поддержки Positive Technologies другим способом.

Примечание: для выполнения операции требуется подключение к сети Интернет и наличие учетной записи для авторизации. Получить учетную запись можно, зарегистрировавшись на сайте технической поддержки (https://support.ptsecurity.com) и отправив заявку с темой «Получение учетной записи для offline-активации лицензий MaxPatrol». Учетные данные будут переданы на указанный в заявке электронный адрес.

5. После обработки появится соответствующее сообщение и ссылка для скачивания файла-ответа OFL (см. Рис. 37).

6. Скачайте файл OFL; его имя соответствует имени файла запроса OFR.

7. Загрузите файл-ответ через консоль MaxPatrol, используя кнопку («Импортировать лицензию в режиме offline») на панели «Настройки» – «Сервер».

8. Ваш компонент MaxPatrol готов к работе.

6. 4. 1. 2. 2. ***Активация компонентов MaxPatrol в изолированной сети через веб-интерфейс***

Для активации выполните следующие действия:

1. Подключитесь к нужному компоненту MaxPatrol через консоль как показано на Рис. 29. Убедитесь, что в панели «Сервер» включена опция «Режим обновления Offline» (вкладка «Настройки» – «Сервер»).

2. В панели «Лицензия» нажмите кнопку («Сформировать запрос на активацию лицензии») для активации лицензии. Если требуется обновление лицензии, нажмите кнопку («Сформировать запрос на обновление лицензии»).

3. Сохраните на съемный носитель файл(ы) OFR.

4. Загрузите файл запроса через интерфейс offline-активации лицензий https://service.maxpatrol.com (см. Рис. 36) или отправьте его в Службу поддержки Positive Technologies другим способом.

Примечание: для выполнения операции требуется подключение к сети Интернет и наличие учетной записи для авторизации. Получить учетную запись можно, зарегистрировавшись на сайте технической поддержки (https://support.ptsecurity.com) и отправив заявку с темой «Получение учетной записи для offline-активации лицензий MaxPatrol». Учетные данные будут переданы на указанный в заявке электронный адрес.

5. После обработки появится соответствующее сообщение и ссылка для скачивания файла-ответа OFL (см. Рис. 37).

6. Скачайте файл OFL; его имя соответствует имени файла-запроса OFR.

7. Загрузите файл-ответ через консоль MaxPatrol, используя кнопку («Импортировать лицензию в режиме offline») на панели «Настройки» – «Сервер».

8. Ваш компонент MaxPatrol готов к работе.

6.4.2. Активация лицензии с ограниченным доступом к сети Интернет

В случае если подключение к сети Интернет ограничено (запрещено использование порта 2002/TCP или используется прокси-сервер), следует отказаться от автоматической активации и изменить настройки подключения к серверу обновлений.

Для этого выполните следующее:

1. Запустите консоль управления: Пуск (Start) – Программы (Programs) – Positive Technologies – MaxPatrol – MaxPatrol.

2. В появившемся окне (см. Рис. 26) укажите адрес сервера, имя учетной записи и пароль. По умолчанию в системе существует пользователь *Administrator*, пароль которого задается в процессе установки.

Если система предложит провести автоматическую активацию лицензии, то следует отказаться.

3. В открывшемся окне консоли перейдите на вкладку «Настройки» – «Соединения».

4. В окне по умолчанию будет присутствовать только одно соединение с сервером update.maxpatrol.com, порт 2002/TCP. Для модификации настроек выделите соединение, щелкните правой кнопкой мыши и в появившемся контекстном меню выберите пункт *Изменить* (см. Рис. 31).

5. В открывшемся окне редактирования соединения можно указать номер TCP-порта (2002, 443), а также параметры прокси-сервера (тип, имя и номер порта, учетную запись для аутентификации).

Чтобы система использовала данное соединение для обновления и привязки лицензии, активируйте опции «Анонимный доступ к серверу» и «Использовать удаленный сервер для» – «Обновления» (см. Рис. 32).

Примечание: сервер MaxPatrol автоматически определяет доступные методы аутентификации (Basic, NTLM, NTLMv2) и использует наиболее безопасный из них.

6. После нажатия кнопки *Подключиться* система попытается подключиться к указанному серверу. Если сервер использует самоподписанный или недоверенный сертификат, то появится сообщение с идентификатором сертификата и просьбой подтвердить его корректность.

Проверить корректность подключения можно в окне информации о соединении (см. Рис. 32), нажав кнопку в панели инструментов.

7. После успешного подключения к серверу обновления перейдите на вкладку «Настройки» – «Сервер» и в панели «Обновления» нажмите *Изменить*. Укажите созданное соединение в окне «Настройки обновления».

8. В панели «Лицензии» щелкните правой кнопкой мыши на нужной лицензии и выберите пункт *Активировать*. Если лицензия на продукт одна, нажмите кнопку (*Активировать лицензию*).

Успешность активации можно проверить в окне информации о лицензии, нажав кнопку в панели инструментов.

7. Обновление системы

Система MaxPatrol может обновляться как с помощью консоли, так и с помощью мастера установки. Отличие между этими способами в том, что в первом случае система обновляется до последней сборки, доступной на сервере обновлений, а во втором – до той версии, установочный файл которой запущен. Последний способ также применяется в случаях, когда требуется обновить список лицензий или набор их функциональных возможностей.

Подробнее о том, как обновить систему, используя MaxPatrol Console, см. раздел Настройка расписания обновлений.

Для обновления системы с помощью мастера установки, выполните следующие действия:

1. Выйдите из консоли MaxPatrol, если она открыта.
2. Запустите мастер установки MaxPatrol и нажмите *Далее* в окне приветствия.
3. В окне «Выбор типа установки» выберите пункт «Полная установка».

Если у вас есть обновленные или дополнительные лицензии, появится запрос на замену использующихся (см. Рис. 38). Нажмите *Да* или *Нет* в зависимости от целей обновления.

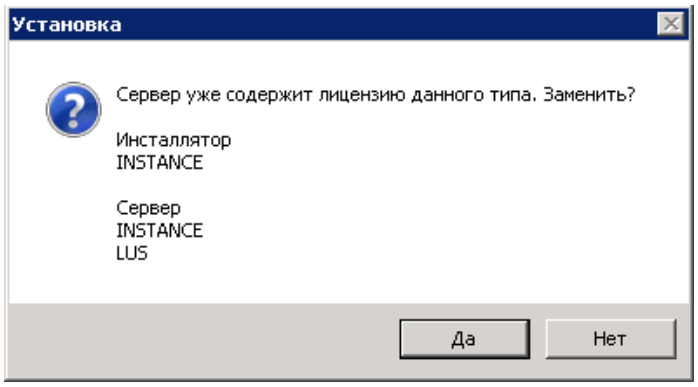

Рис. 38 – Запрос на замену лицензии

4. В окне «Выбор действия» выберите «Обновить MaxPatrol» и нажмите *Далее*.
5. Следующие два шага – проверка системы на соответствие минимальным требованиям (подробнее см. Требования к системе) и подтверждение выбранных настроек. Нажмите *Установить*, чтобы установить обновления системы MaxPatrol.

8. Переустановка системы

Переустановка системы MaxPatrol может понадобиться в случаях, когда ее нормальное функционирование было нарушено; например, вследствие удаления системных файлов.

Для переустановки системы выполните следующие действия:

1. Выйдите из консоли MaxPatrol, если она открыта.
2. Запустите мастер установки MaxPatrol и нажмите *Далее* в окне приветствия.
3. В окне «Выбор типа установки» выберите пункт «Полная установка».

   Если у вас есть обновленные или дополнительные лицензии, появится запрос на замену использующихся (см. Рис. 38). Выберите подходящий вариант ответа.

4. В окне «Выбор действия» выберите «Переустановить MaxPatrol» и нажмите *Далее*.
5. Если появится запрос на использование файлов данных предыдущей установки, нажмите *Да*, чтобы применить использовавшиеся ранее настройки (см. Рис. 39).

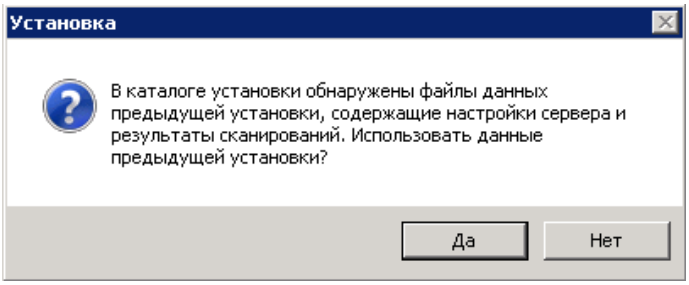

Рис. 39 – Запрос на использование данных предыдущей установки

6. Следующие два шага – проверка системы на соответствие минимальным требованиям (подробнее см. Требования к системе) и подтверждение выбранных настроек. Нажмите *Установить*, чтобы переустановить систему MaxPatrol.

9. Удаление системы

Для удаления системы выполните следующие действия:

1. Выйдите из консоли MaxPatrol, если она открыта.
2. Запустите мастер установки MaxPatrol и нажмите *Далее* в окне приветствия.
3. В окне «Выбор типа установки» выберите пункт «Полная установка».
Если у вас есть обновленные или дополнительные лицензии, появится запрос на замену использующихся (см. Рис. 40). Выберите подходящий вариант ответа.
4. В окне «Выбор действия» выберите «Удалить MaxPatrol» и нажмите *Далее*.
5. Мастер установки запросит подтверждение действия. Нажмите *Да*.

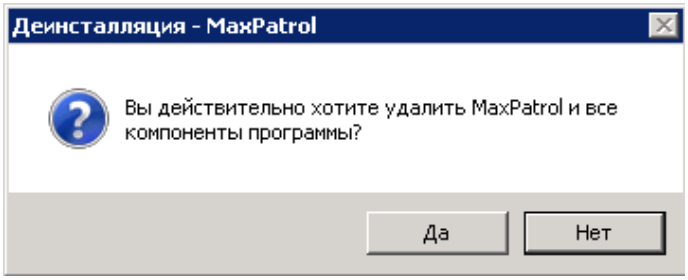

Рис. 40 – Запрос на удаление системы

6. В появившемся окне «Деинсталляция MaxPatrol» укажите, какие компоненты системы требуется удалить и нажмите *Далее*.
7. В случае успешного завершения операции появится соответствующее сообщение.

10. Использование системы в виртуальной среде

Система контроля защищенности и соответствия стандартам MaxPatrol может использоваться в виртуальной среде с привязкой к электронным ключам eToken.

Использование ключа eToken обеспечивает лицензионную защиту компонентов MaxPatrol при работе в виртуальном окружении. На текущий момент такая возможность официально реализована только для виртуальных машин VMware ESXI 4.1, Workstation версии 6.0 и выше, а также для виртуальных машин Hyper-V и KVM-технологии виртуализации для Linux-систем (ядро 2.6.18 и выше).

Внимание! Для виртуальных машин Hyper-V и KVM-технологии виртуализации для Linux-систем (ядро 2.6.18 и выше) рекомендуется подключение ключа eToken в виртуальную машину средствами DigiAnyWhere.

При использовании других виртуальных машин эта возможность 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, Workstation версии 6.0 и выше, а также на виртуальных машинах Hyper-V и KVM-технологиях виртуализации для Linux-систем (ядро 2.6.18 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 MaxPatrol на виртуальной машине.

Допускается использование только ключей eToken, выданных ЗАО «Позитив Текнолоджиз». Для каждого модуля ПО MaxPatrol в случае установки на виртуальный сервер в комплект поставки включается индивидуальный ключ eToken.

Возможны несколько вариантов развертывания системы MaxPatrol:

- Каждый компонент системы MaxPatrol устанавливается на отдельную виртуальную машину. В этом случае для каждого модуля выдается свой ключ eToken.
- Несколько модулей системы MaxPatrol устанавливаются на одну виртуальную машину. В этом случае выпускается один ключ eToken на одну виртуальную машину. Одного ключа достаточно для защиты всех компонентов, установленных на одной виртуальной машине.
- При необходимости изменения размещения модулей системы MaxPatrol (например, объединения нескольких модулей MaxPatrol на одной виртуальной машине или разделения компонентов, установленных на одной виртуальной машине, на несколько машин) необходимо обратиться в службу технической поддержки компании ЗАО «Позитив Текнолоджиз». Сотрудники технической поддержки помогут заново инициализировать ключ eToken и провести повторную активацию компонентов MaxPatrol. В случае необходимости будет сформирован дополнительный ключ eToken.

Внимание! Повторную активацию необходимо проводить на всех компонентах MaxPatrol, привязанных к исходному ключу eToken.

10.1. Порядок использования MaxPatrol с eToken

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

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

Ключ eToken передается клиенту в безвозмездное пользование. 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 авторизованных партнеров (за контактами необходимо обратиться в службу технической поддержки) и передает разработчику для его инициализации. Получение ключа eToken после инициализации осуществляется за счет клиента и с использованием его ресурсов.

Клиенты, которые ранее приобрели систему MaxPatrol и у которых есть необходимость перейти на использование MaxPatrol 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 MaxPatrol с аппаратного сервера в виртуальную среду).

10.2. Установка компонентов системы с использованием eToken

После получения дистрибутива и ключа eToken можно приступить к развертыванию MaxPatrol в виртуальном окружении. Алгоритм развертывания следующий:

1. Подготовьте виртуальную машину на базе VMware ESXI 4.1 или Workstation версии 6.0 и выше.

   При настройке аппаратных ресурсов VMware необходимо руководствоваться требованиями из раздела Требования к аппаратному обеспечению.

2. Установите MaxPatrol из полученного дистрибутива.

   Примечание: Процесс установки необходимо проводить при отключенном ключе eToken.

3. 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 MaxPatrol). По умолчанию Setup Log расположен в каталоге *C:|Program Files|Positive Technologies|MaxPatrol\server|Logs. Если MaxPatrol* устанавливается в каталог,

отличный от указанного, то журнал событий расположен в каталоге *<путь_к_каталогу_MaxPatrol>\server\Logs*.

4. Подключите полученный ранее ключ eToken к USB-порту сервера VMware.

5. В разделе *Settings* созданной виртуальной машины последовательно подключите USB controller и USB device. Если к VMware подключено несколько электронных ключей, выберите ключ, полученный от ЗАО «Позитив Текнолоджиз».

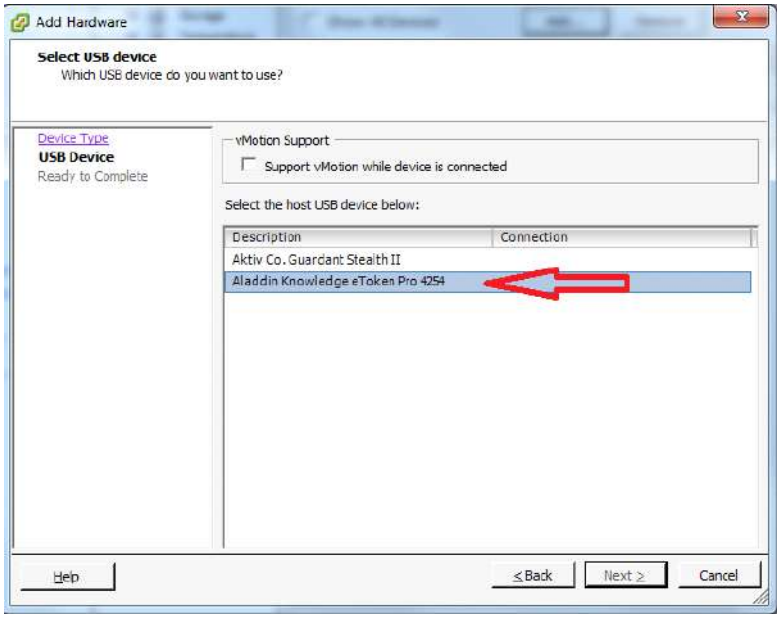

Рис. 41 – Выбор электронного ключа

6. Запустите консоль MaxPatrol. Перейдите на вкладку «Настройки» – «Сервер» и активируйте лицензию MaxPatrol (подробнее см. раздел Настройка расписания обновлений).

В процессе активации проверяется наличие подключенного ключа eToken и действительной лицензии. Для сохранения работоспособности MaxPatrol требуется наличие постоянно подключенного ключа eToken. В случае отключения ключа eToken MaxPatrol блокирует возможность работы с системой до подключения ключа eToken.

10.3. Перенос компонентов MaxPatrol с аппаратного сервера в виртуальную среду

Для переноса компонентов MaxPatrol с аппаратного сервера на виртуальную машину выполните следующие действия:

1. Конвертируйте аппаратный сервер в виртуальную среду с помощью утилиты VMware Converter (http://downloads.vmware.com/d/info/datacenter_downloads/vmware_vcenter_converter_standalone/4_0).

2. Подробно процесс конвертирования описан в документе «VMware vCenter Converter Documentation» на сайте производителя VMware.

Примечание: 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 Converter.

3. По окончании процесса конвертирования используйте полученный ранее дистрибутив MaxPatrol с поддержкой eToken для повторной установки системы на виртуальной машине.

Внимание! Процесс установки должен происходить без подключенного ключа eToken.

4. В ходе установки используйте следующие параметры:

- режим установки «Переустановить MaxPatrol»;
- использование данных предыдущей установки (нажмите *Да)*.

5. После завершения процесса установки подключите полученный ключ eToken к USB-порту сервера VMware.

В разделе *Settings* созданной виртуальной машины проверьте доступность USB controller и подключите USB device (eToken). Если к VMware подключено несколько электронных ключей, выберите ключ, полученный от ЗАО «Позитив Текнолоджиз».

6. Запустите консоль MaxPatrol. Перейдите на вкладку «Настройки» – «Сервер» и активируйте лицензию MaxPatrol (подробнее см. раздел Активация лицензии).

В процессе активации проверяется наличие подключенного ключа eToken и действительной лицензии. Для сохранения работоспособности MaxPatrol требуется наличие постоянно подключенного ключа eToken. В случае отключения ключа eToken MaxPatrol блокирует возможность работы с системой до подключения ключа eToken.

10.4. 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 запись об устройстве USB Token появится в разделе Universal Serial Bus Controllers.

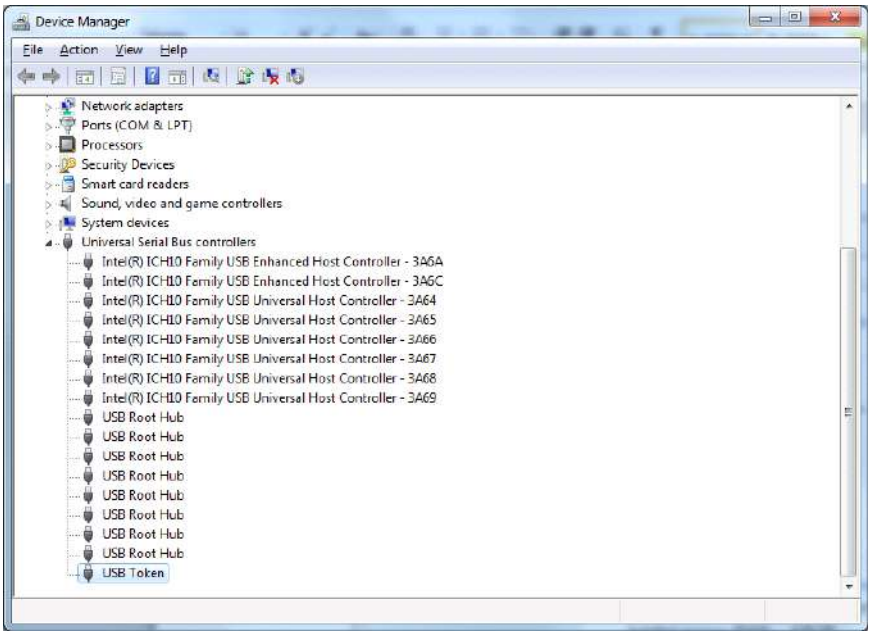

Рис. 42 – Диспетчер устройств Windows

В случае отсутствия устройства USB Token, проверьте журнал Setup Log на наличие ошибок. Журнал Setup Log расположен в каталоге установки MaxPatrol. Стандартный каталог: *C:\Program Files\Positive Technologies\MaxPatrol\server\Logs*. Если MaxPatrol установлен в каталог, отличный от указанного, то журнал событий расположен в каталоге *<путь_к_каталогу_MaxPatrol>\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...
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 MaxPatrol необходимо убедиться, что ключ eToken подключен и распознается системой.

При возникновении ошибок, связанных с подключением и настройкой eToken, следует обратиться в службу технической поддержки компании ЗАО «Позитив Текнолоджиз» (https://support.ptsecurity.com). 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|MaxPatrol|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, при помощи командной строки запустите утилиту *dxdiag.exe* и на вкладке *System* выберите *Save All Information.* Полученный файл журнала следует отправить в службу технической поддержки компании ЗАО «Позитив Текнолоджиз».

Примечание: компания ЗАО «Позитив Текнолоджиз» обеспечивает техническую поддержку решений, которые базируются только на виртуальных машинах VMware ESXI 4.1 и Workstation версии 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 обеспечения.

11. Приложение. Типовые варианты развертывания

В данном разделе рассматриваются несколько примеров развертывания и приводятся основные подходы, используемые при внедрении MaxPatrol.

Можно выделить следующие основные задачи, которые необходимо решить при выборе варианта развертывания:

- масштабирование с точки зрения производительности сканирования;
- эффективное использование пропускной способности каналов связи;
- адаптация к сетевой инфраструктуре и средствам защиты;
- адаптация к структуре управления информационной безопасностью.

Задачи масштабирования с точки зрения производительности, как правило, решаются с помощью использования дополнительных сканеров MP Scanner. Сканеры, работающие под управлением MP Server, позволяют распределять нагрузку по сканированию различных групп узлов. Добавление нового сканера дает практически линейное увеличение производительности. Количество узлов, обрабатываемых одним сканером, зависит от пропускной способности каналов связи и производительности системы, но в общем случае можно использовать число в 1000 узлов на один сканер в качестве приемлемого значения при решении задач непрерывного мониторинга ИБ.

Для обеспечения эффективного использования пропускной способности каналов связи применяются дополнительные сканеры MP Scanner. Как правило, сканеры располагаются в непосредственной «сетевой близости» от сканируемого объекта, в то время как управляющий MP Server может использовать для связи с MP Scanner слабый канал связи. Объем передаваемого трафика между MP Server и MP Scanner на несколько порядков меньше объема трафика, передаваемого между MP Scanner и объектом.

Адаптация к сетевой инфраструктуру и средствам защиты, как правило, решается использованием дополнительных сканеров.

11.1. Минимальная конфигурация

Минимальный вариант конфигурации для развертывания системы предполагает установку одного сервера MP Server со встроенным сканером MP Scanner и консолью управления MP Console. Такой вариант является основным для MaxPatrol Mobile Server (за исключением возможности работы с внешним сервером консолидации). Пример такой системы представлен на Рис. 43.

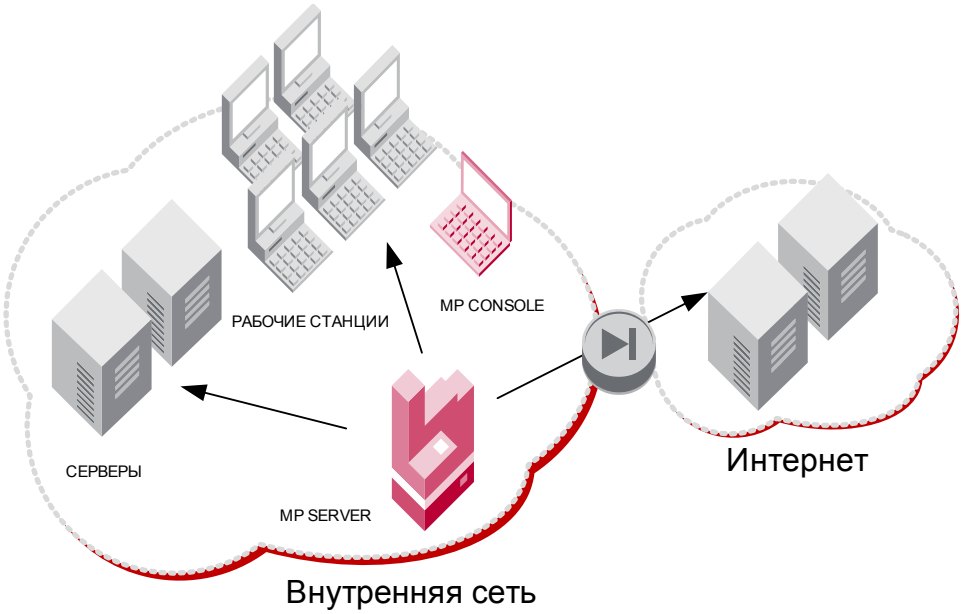

Рис. 43 – Минимальный вариант конфигурации для развертывания MaxPatrol

В таком варианте планирование развертывания практически не требуется. Аппаратные требования совпадают с минимальными требованиями, за исключением объема жесткого диска для хранения результатов. Поскольку MP Server и MP Scanner размещаются на одном компьютере, учет трафика между этими компонентами не требуется. Для защиты трафика консоли используются самоподписанные сертификаты, создаваемые в процессе установки системы. Модель разграничения доступа зависит от требований СУИБ, но в большинстве случает достаточно простой одноуровневой модели.

Информация о планировании минимальной инсталляции приведена в Табл. 17.

Таблица 18. Планирование минимального развертывания

	Требования
Аппаратные требования	Минимальные. Жесткий диск для результатов
Сетевая инфраструктура	10—100 МБ до объекта сканирования
Средства защиты	Средства защиты не препятствуют доступу сканера к объекту сканирования
Система безопасности	Самоподписанные сертификаты. Одноуровневое разграничение доступа
Использование СУБД	Промышленная СУБД

11.2. Конфигурация с несколькими сканерами

Конфигурация с несколькими сканерами может использоваться при развертывании MaxPatrol в сетях среднего размера. Пример подобной конфигурации приведен на Рис. 44.

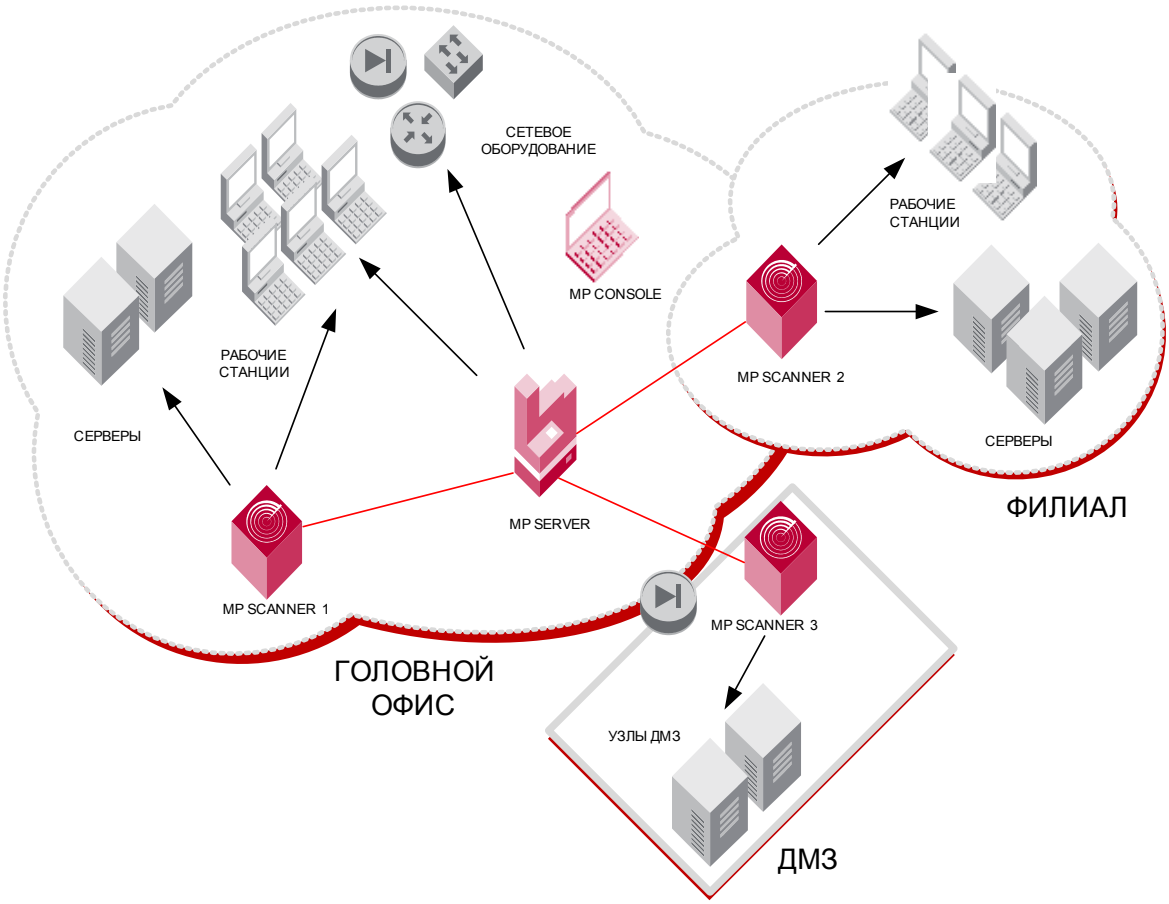

Рис. 44 – Конфигурация с несколькими сканерами

Необходимость использования нескольких сканеров определяется следующими требованиями:

- масштабирование (необходимо проводить сканирование большого количества узлов);
- пропускная способность (сеть, в которой находятся сканируемые узлы, соединена со сканером каналами связи с низкой пропускной способностью);
- требования топологии. Особенности логической и физической топологии определяют необходимость размещения сканеров в определенных сетевых сегментах. Типичные причины: вынос управляющих интерфейсов в отдельную виртуальную сеть (VLAN) или использование средств защиты.

Информация о планировании инсталляции с несколькими сканерами приведена в Табл. 19.

Таблица 19. Планирование конфигурации с несколькими сканерами

	Общие	MP Server	MP Scanner
Критерии выбора	Масштабирование, пропускная способность, топология		
Аппаратные требования	Минимальные	Жесткий диск для результатов	Дополнительные требования к процессору
Использование СУБД	Внешняя	В зависимости от объемов сканирования	Используется СУБД сервера
Сетевая инфраструктура	10-100 МБ до объекта сканирования	Пропускная способность канала между сервером и сканерами	
Средства защиты	Не должны препятствовать доступу сканера к объекту сканирования	Не должны блокировать обмен данными по порту 2002/TCP между сервером и сканерами	
Система безопасности	Зависит от требований СУИБ. Единая база учетных записей и структура разграничения доступа на MP Server		

11.3. Конфигурация с несколькими серверами

Конфигурация с несколькими серверами используется в ходе масштабных внедрений MaxPatrol. Такой вариант обладает максимальной гибкостью с точки зрения масштабирования, управления и разграничения доступа.

Вариант с несколькими серверами выбирается в случае, если система управления информационной безопасностью крайне децентрализована. Например, в случае, если региональные подразделения ИБ полностью самостоятельны, и в задачи центра входит только функция контроля результатов сканирования. В этом случае все функции по управлению сканированием реализуются на базе серверов MP Server, расположенных в различных филиалах, а сервер консолидации MP Consolidation Server, установленный в центре, сохраняет данные по истории сканирований из всех филиалов.

Пример подобной конфигурации приведен на Рис. 45.

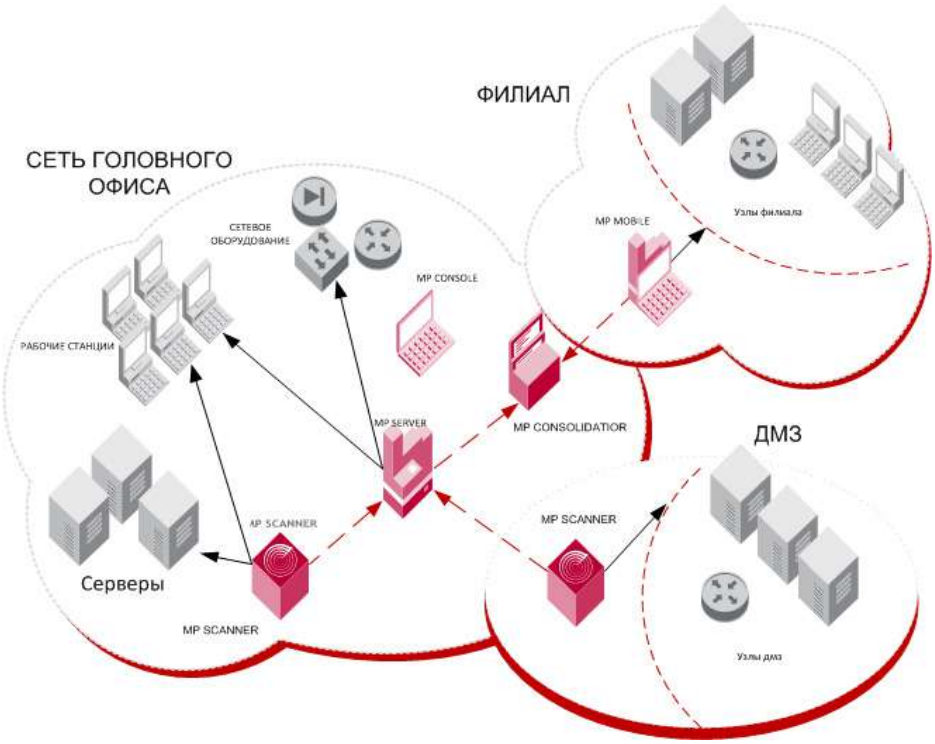

Рис. 45 – Конфигурация с несколькими серверами

Обратной стороной гибкости является необходимость учета большего количества переменных при планировании развертывания. Объем жесткого диска для компонентов MP Consolidation Server и MP Server должен рассчитываться, исходя из планируемых объемов сканирования. При расчете этого значения для MP Consolidation Server следует суммировать объем всех работающих с ним MP Server и умножить на поправочный коэффициент 1,3.

Для работы MP Consolidation Server потребуется использование промышленной СУБД.

Модель разграничения доступа определяется требованиям СУИБ на уровне MP Server и MP Consolidation Server. Каждый MP Server содержит собственную независимую базу данных учетных записей и групп, которые могут использоваться для разграничения доступа на элементы системы (задачи, отчеты и т. п.).

Информация о планировании инсталляции с несколькими серверами приведена в Табл. 20.

Таблица 20. Планирование конфигурации с несколькими серверами

	MP Consolidation Server	MP Server	MP Scanner
Критерии выбора	• Адаптация к структуре управления ИТ и ИБ; • использование нескольких MP Server (например, MP Mobile Server); • масштабирование; • пропускная способность; • топология		
Аппаратные требования	Жесткий диск для результатов	Жесткий диск для результатов	Дополнительные требования к процессору
Использование СУБД	Промышленная СУБД		Используется СУБД сервера
Сетевая инфраструктура	Пропускная способность канала между серверами, сканерами и сервером консолидации		
Средства защиты	Не должны препятствовать доступу сканера к объекту сканирования и блокировать обмен данными по порту 2002/TCP между сервером и сканерами и серверами консолидации		
Система безопасности	Многоуровневая. Отдельные механизмы разграничения доступа для каждого сервера MP Server и сервера консолидации		

11.4. Конфигурация с несколькими консолидаторами

В случае масштабных внедрений существует возможность выстраивать цепочку серверов консолидации MP Consolidation Server. Использование такой архитектуры может понадобиться, если сеть является распределенной, и у нее сложная структура управления. Например, используется трехуровневая структура головной офис – филиал – подразделение, в рамках каждого Подразделения функционирует собственная служба ИБ, и требуется установка MaxPatrol Server. Сотрудникам филиала нужно иметь централизованный доступ к результатам сканирования во всех подразделениях филиала, поэтому в филиале устанавливается сервер консолидации. Этот MP Consolidation Server, в свою очередь, передает результаты серверу консолидации, расположенному в головном офисе, что обеспечивает централизованную отчетность в рамках всей компании. Пример подобной конфигурации дан на Рис. 46.

Обратной стороной гибкости является необходимость учета большого количества переменных при планировании развертывания. Объем жесткого диска для компонентов MP Consolidation Server и MP Server должен рассчитываться, исходя из планируемых объемов сканирования. При расчете этого значения для MP Consolidation Server следует суммировать объем диска, необходимый для всех работающих с ним MP Server, и умножить на поправочный коэффициент 1,3.

Для работы MP Consolidation Server потребуется использование промышленной СУБД. Для серверов MP Server также требуется использование промышленной СУБД.

Исключения могут составлять варианты развертывания системы для изучения или тестирования продукта. В этом случае допускается использование встроенной БД.

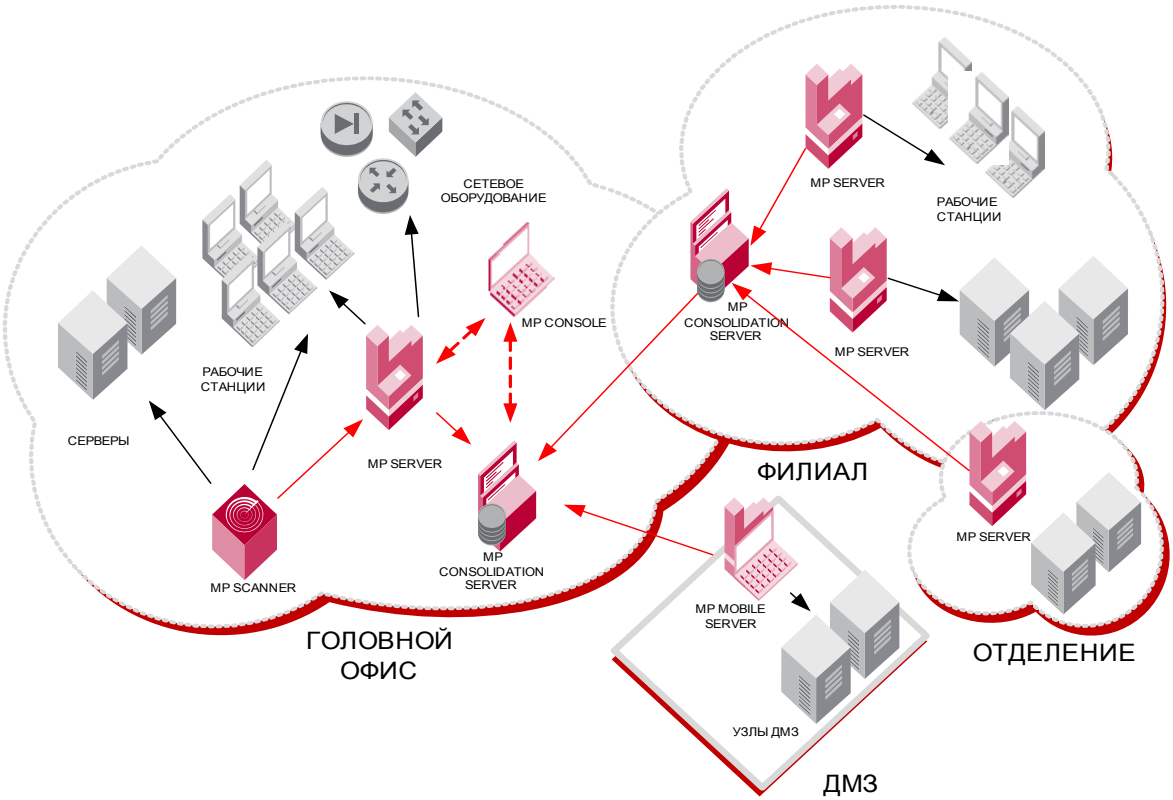

Рис. 46 – Конфигурация с несколькими консолидаторами

Модель разграничения доступа определяется требованиям СУИБ на уровне MP Server и MP Consolidation Server. Каждый MP Server содержит собственную независимую базу данных учетных записей и групп, которые могут использоваться для разграничения доступа к элементам системы (задачи, отчеты и т. п.).

Информация о планировании инсталляции нескольких серверов консолидации приведена в Табл. 21.

Таблица 21. Планирование конфигурации с несколькими серверами консолидации

	MP Consolidation Server	MP Server	MP Scanner
Критерии выбора	• Адаптация под структуру управления ИТ и ИБ; • масштабирование; • пропускная способность; • топология		
Аппаратные требования	Жесткий диск для результатов	Жесткий диск для результатов	Дополнительные требования к процессору

Таблица 21. Планирование конфигурации с несколькими серверами консолидации

	MP Consolidation Server	MP Server	MP Scanner
Использование СУБД	Промышленная СУБД		Используется СУБД сервера
Сетевая инфраструктура	Пропускная способность канала между серверами, сканерами и сервером консолидации		
Средства защиты	Не должны препятствовать доступу сканера к объекту сканирования и блокировать обмен данными по порту 2002/TCP между сервером и сканерами и серверами консолидации		
Система безопасности	Многоуровневая. Отдельные механизмы разграничения доступа для каждого сервера MP Server и сервера консолидации		