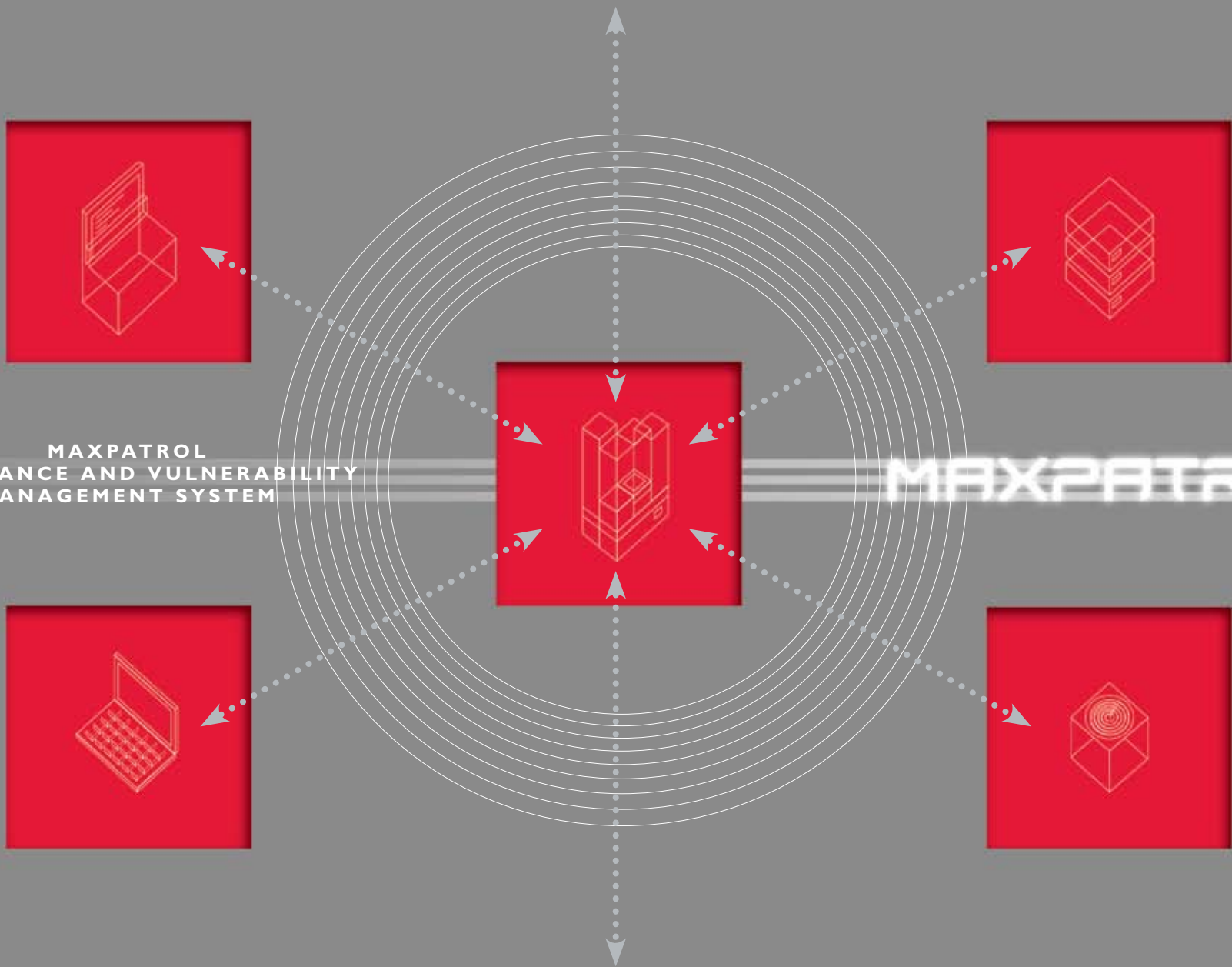


MAXPATROL  
COMPLIANCE AND VULNERABILITY  
MANAGEMENT SYSTEM

MAXPATROL





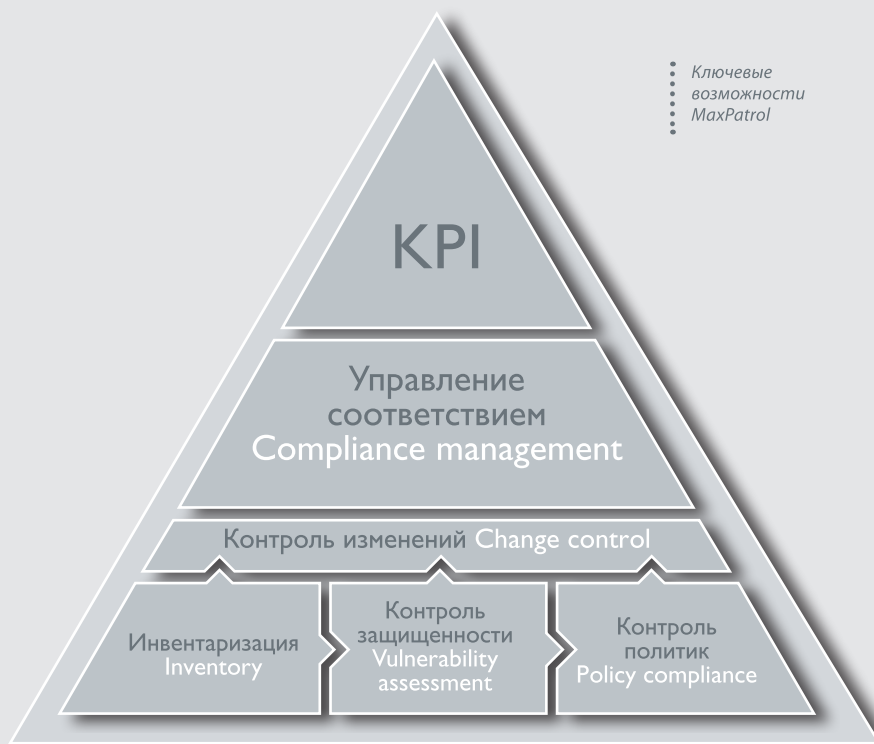


Система контроля защищенности и соответствия стандартам MaxPatrol разработана компанией Positive Technologies. Основой для создания MaxPatrol послужил профессиональный сканер безопасности XSpider и десятилетний опыт экспертов компании Positive Technologies, полученный в ходе его разработки, внедрения и эксплуатации в ведущих российских и зарубежных компаниях. В результате в системе MaxPatrol реализованы общемировые передовые технологии, а также учтены особенности российского рынка.

MaxPatrol - единственный продукт на мировом рынке, в котором объединены механизмы системных проверок, тестирования на проникновение, контроля соответствия стандартам в сочетании с поддержкой анализа сетевого оборудования, операционных систем, СУБД, прикладных и ERP-систем, веб-приложений.

Использование MaxPatrol позволяет сформировать непротиворечивые корпоративные стандарты, автоматизировать процессы инвентаризации, контроля изменений, управления уязвимостями и контроля соответствия, оценивать эффективность ИТ и ИБ-процессов с помощью ключевых показателей эффективности (KPI).

# КОНТРОЛЬ ЗАЩИЩЕННОСТИ И СООТВЕТСТВИЯ СТАНДАРТАМ



## Ключевые возможности

- Проактивная защита корпоративных ресурсов с помощью автоматического мониторинга ИБ;
- Автоматизация процессов контроля соответствия отраслевым и международным стандартам;
- Оценка эффективности подразделений ИТ и ИБ с помощью расширяемого набора метрик безопасности и KPI;
- Снижение затрат на аудит и контроль защищенности, подготовку ИТ и ИБ-проектов;
- Автоматизация процессов инвентаризации ресурсов, управления уязвимостями, контроля соответствия политикам безопасности и контроля изменений;
- Комплексный анализ сложных систем, включая сетевое оборудование Cisco, Nortel, Juniper, Huawei, платформ Windows, Linux, Unix, СУБД Microsoft SQL, Oracle, приложений Active Directory, Microsoft Exchange, Lotus, SAP/R3 и веб-службы собственной разработки;
- Встроенная поддержка основных стандартов, таких как ГОСТ ИСО/МЭК 17799, ГОСТ ИСО/МЭК 27001, SOX (Sarbanes-Oxley Act), PCI DSS (Payment Card Industry Data Security Standard), NSA (National Security Agency), NIST (National Institute of Standards and Technologies), CIS (Center for Internet Security);
- Максимальная автоматизация процессов, снижающая трудозатраты и позволяющая оперативно контролировать состояние защищенности систем;
- Поддержка базы знаний командой профессиональных экспертов.

Поддержание в актуальном состоянии данных о существующих информационных активах, поиск и исправление брешей в защите и проверка соответствия корпоративным, отраслевым и международным стандартам современных гетерогенных, многоуровневых информационных систем является непростой задачей. Быстрый ввод в эксплуатацию новых компонентов, изменяющийся набор платформ и приложений, аутсорсинг ИТ, постоянно трансформирующиеся угрозы безопасности еще больше усложняют этот процесс.

Система MaxPatrol позволяет автоматизировать и централизовать процессы поиска уязвимостей, контроля состояния ИБ и соответствия стандартам в информационных системах любого масштаба, что дает возможность своевременно получать полную картину состояния защищенности как всей системы, так и отдельных узлов.

### Автоматизация мониторинга информационной безопасности

Система MaxPatrol обеспечивает автоматизацию таких важных задач управления ИТ и ИБ, как инвентаризация ресурсов, управление уязвимостями, контроль соответствия политикам безопасности и контроль изменений.

Зачастую процедуры инвентаризации, оценки защищенности и контроля политик

безопасности проводятся нерегулярно или с большими промежутками. Это приводит к тому, что информация теряет актуальность, и ситуация выходит из-под контроля. Комплексный подход и интеллектуальные средства автоматизации, реализованные в системе MaxPatrol, обеспечивают минимизацию трудозатрат, необходимых для решения задач мониторинга ИБ, что позволяет своевременно обнаруживать проблемы и, как следствие, – повышать защищенность информационной системы.

Используя обширную и постоянно обновляемую базу знаний MaxPatrol, специалисты могут оперативно создавать эталонные шаблоны конфигураций систем, отслеживать системы, несоответствующие требованиям политик безопасности, и эффективно устранять обнаруженные недочеты.

### Комплексное многоплатформенное решение

В отличие от традиционных, узкоспециализированных сканеров безопасности, в системе MaxPatrol реализованы функции анализа сетевого оборудования, операционных систем, приложений, баз данных и веб-приложений. Такой подход позволяет с помощью одного инструмента контролировать защищенность сложных информационных систем, использующих сетевое оборудование Cisco, Nortel, Juniper, Huawei, платформ Windows, Linux, Unix, СУБД Microsoft SQL, Oracle, приложений Active Directory, Microsoft Exchange, Lotus, SAP/R3 и веб-службы собственной разработки.

# КОНТРОЛЬ ЭФФЕКТИВНОСТИ ПРОЦЕССОВ ИБ

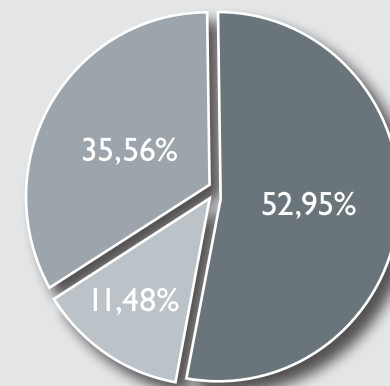
В большинстве компаний многие из распространенных средств защиты уже используются или находятся на этапе внедрения. Трудно представить корпоративную сеть, в которой механизмы межсетевого экранирования, антивирусной защиты или установки обновлений не были бы реализованы в том или ином виде. В связи с этим, одним из наиболее важных моментов становится оценка эффективности существующих процессов ИБ с помощью метрик безопасности. Расширяемый набор метрик, входящих в MaxPatrol, позволяет контролировать текущее состояние и динамику изменений распространенных процессов ИБ. В ходе внедрения набор метрик может быть адаптирован под нужды заказчика. Так, например, при внедрении решений класса DLP или контроля за действиями пользователей, можно отслеживать количество и процент рабочих станций, на которых установлен агент системы. Данная простая метрика даёт возможность эффективно контролировать внедрение проекта, а возможность рассчитать её значение для различных групп компьютеров и подразделений – проводить анализ работы ИТ и ИБ-специалистов. Важной характеристикой метрик безопасности является то, что они измеряются в абсолютных значениях (количество узлов, изменений и несоответствий), что позволяет легко спроецировать их на трудозатраты или перевести в денежное выражение.

- Соответствие
- корпоративным
- стандартам,
- Центральный регион,
- 2009 год, июнь



По узлам

Статус	Кол-во
Не проверялось	0
Соответствует	0
Не соответствует	213
Неприменимо	0
Не определено	0
Итого:	213

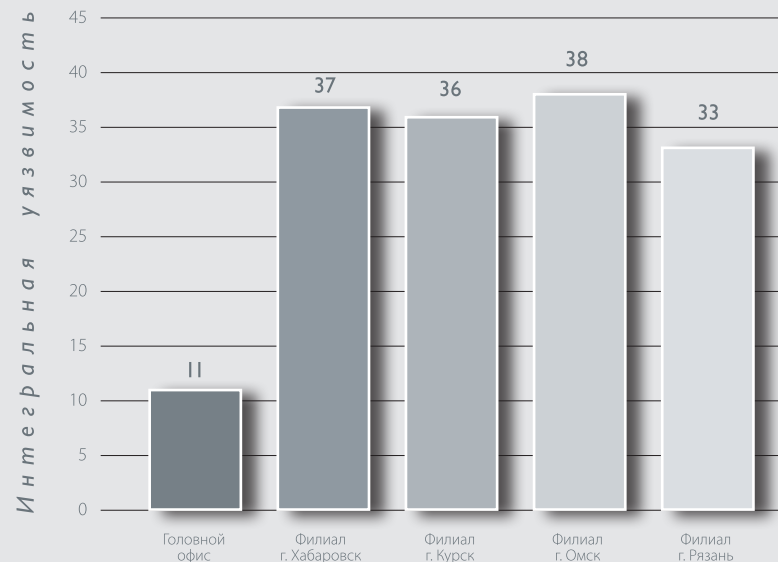


По требованиям

Статус	Кол-во
Не проверялось	0
Соответствует	319
Не соответствует	475
Неприменимо	103
Не определено	0
Итого:	897

## Ниже приведены популярные метрики, контролируемые с помощью MaxPatrol:

- Количество и процент рабочих станций с установленным антивирусным пакетом;
- Количество и процент рабочих станций с обновленными антивирусными базами;
- Количество нестандартных серверных портов и приложений на рабочих станциях/серверах;
- Среднее время (задержка) развертывания критических обновлений;
- Количество и процент систем, содержащих критические уязвимости;
- Процент охвата систем корпоративными и международными стандартами;
- Уровень соответствия (несоответствия) различных систем корпоративным и международным стандартам;
- Количество и процент рабочих станций/серверов, работающих с системами сбора и корреляции событий безопасности;
- Количество уязвимостей, выявляемых в течение определенного промежутка времени (месяц, квартал, год);
- Количество уязвимостей, устраняемых в течение определенного промежутка времени (месяц, квартал, год);
- Количество уязвимостей, требующих устранения;
- Среднее время устранения уязвимостей для различных подразделений;
- Количество изменений конфигураций различных систем.



• Интегральная  
• уязвимость,  
• 2009 год, 3 квартал

# ОЦЕНКА ЗАЩИЩЕННОСТИ

Система MaxPatrol основана на базе профессионального сканера уязвимости XSpider. Существующие в XSpider механизмы контроля были значительно дополнены за счет добавления модулей анализа безопасности баз данных и системных проверок.

Сочетание в одном продукте функций сетевых и системных сканеров, а также средств оценки защищенности СУБД и веб-приложений, позволяет получать максимально достоверную картину защищенности сети.

## Сетевой сканер

Основой MaxPatrol является высокопроизводительный сетевой сканер, который быстро и эффективно обнаруживает сетевые узлы, открытые порты, идентифицирует операционную систему и серверные приложения. Распределенная архитектура позволяет размещать сканирующий модуль в непосредственной близости от объекта сканирования, что дает возможность снижать нагрузку на магистральные каналы связи.

## Тестирование на проникновение

Эвристические механизмы анализа выявляют уязвимости в сетевых службах и приложениях, работая с минимальным уровнем привилегий (режим тестирования на проникновение – penetration testing), давая оценку

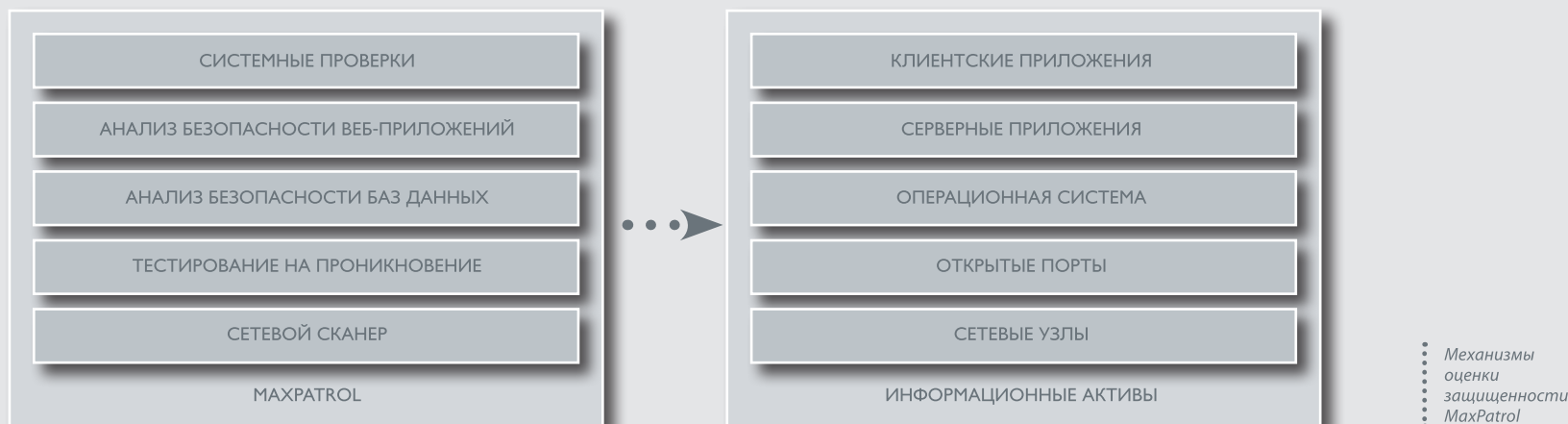
защищенности сети со стороны злоумышленника. Экспертами разработаны интеллектуальные алгоритмы и механизмы поиска уязвимостей, эффективность которых доказана независимыми исследованиями ([http://www.itsecurity.ru/news/reliase/2008/12\\_22\\_08.htm](http://www.itsecurity.ru/news/reliase/2008/12_22_08.htm)). Они максимально приближены к тем, которые используются реальными нарушителями, что позволяет не только идентифицировать ошибки в эксплуатации систем, но и обнаруживать новые, ещё неизвестные уязвимости реализации сетевых приложений.

## Анализ безопасности баз данных

Специализированные модули позволяют получить экспертную оценку защищенности популярных СУБД, таких как Microsoft SQL Server 2000/2005, Oracle 9i,10g. Проверки затрагивают все аспекты безопасности СУБД, такие как:

- настройки сетевого взаимодействия;
- система аутентификации;
- механизмы разграничения доступа;
- права и привилегии пользователей;
- управление обновлениями.





Анализ безопасности СУБД «изнутри» выявляет уязвимости, которые либо невозможно, либо крайне сложно идентифицировать методами тестирования на проникновение.

## Анализ безопасности веб-приложений

Модуль анализа безопасности веб-приложений идентифицирует уязвимости в наследуемых приложениях и приложениях собственной разработки. Эвристические механизмы позволяют обнаруживать большинство типичных ошибок, допускаемых при разработке веб-приложений: внедрение операторов SQL (SQL Injection), межсайтовое выполнение сценариев (Cross-Site Scripting, XSS) и др.

В создание модуля анализа безопасности веб-приложений внесли вклад признанные эксперты отрасли, участники международной организации Web Application Security Consortium ([www.webappsec.org](http://www.webappsec.org)), что позволило обеспечить высокое качество сканирования.

## Системные проверки

При наличии доступа к механизмам удаленного управления узлом модуль сканирования может использовать их для глубокой проверки безопасности

операционной системы и приложений. Данный метод позволяет с минимальным использованием ресурсов получить комплексную оценку защищенности, а также провести анализ параметров, недоступных в режиме теста на проникновение.

База знаний включает в себя системные проверки для большинства распространенных операционных систем: линеек Windows, Linux и Unix, а также специализированного оборудования, такого как маршрутизаторы и коммутаторы Cisco IOS, межсетевые экраны Cisco PIX и Cisco ASA и сетевое оборудование других производителей.

В отличие от классических системных сканеров, MaxPatrol не требует развертывания программных модулей на узлах, что упрощает эксплуатацию и снижает совокупную стоимость владения. Все проверки проводятся удаленно с использованием встроенных механизмов удаленного администрирования. При поддержке узлом нескольких протоколов (например, Telnet и SSH) MaxPatrol выбирает наиболее безопасный из них, что обеспечивает защиту конфиденциальных данных при передаче по сети.

# КОНТРОЛЬ ПОЛИТИК БЕЗОПАСНОСТИ

Настраиваемые под требования заказчика модули анализа для различных операционных систем и приложений позволяют проводить автоматическую проверку на соответствие техническим стандартам безопасности, а также рекомендациям производителей и передовому опыту в отрасли. Наглядная картина соответствия требованиям политик может быть сформирована как для СУИБ заказчика в целом, так и для отдельных подразделений, узлов и приложений.

Консолидация результатов анализа системы всевозможными модулями даёт возможность контролировать политики различной степени сложности. Так, политика безопасности веб-приложения может включать в себя требования по отсутствию уязвимостей типа SQL Injection, требования по настройке операционной системы, базы данных, веб-сервера Apache, настройке межсетевого экрана Cisco PIX и других компонентов, развернутых на нескольких узлах. Система MaxPatrol позволяет проверить все эти параметры в рамках одной сессии сканирования, проанализировав результаты работы модулей анализа безопасности веб-приложений, баз данных и системных проверок.

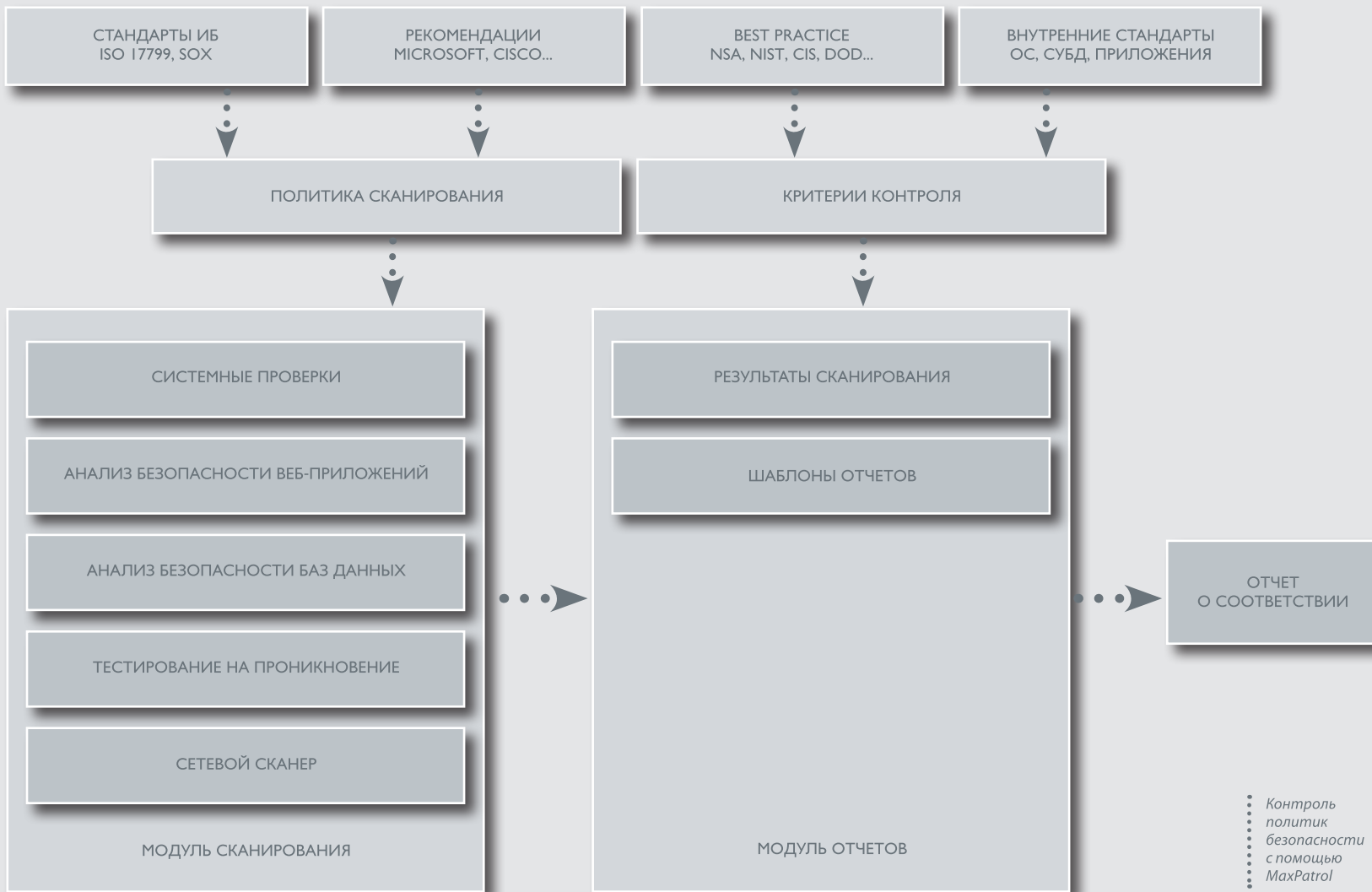
Система MaxPatrol содержит ряд готовых политик, основанных на рекомендациях производителей программ и активного сетевого оборудования, компетентных организаций, таких как NSA, NIST, CIS, DoD (Department of Defense) и т.д. Архитектура системы адаптирует проверки под конкретные требования, добавляя их для новых приложений и формируя на основе технических регламентов заказчика. Это позволяет в любой момент времени иметь актуальную информацию об узлах, состоянии которых

нарушает политику безопасности, и оперативно устранять несоответствия.

Использование MaxPatrol облегчает процесс внедрения требований, полученных из передового опыта в области ИТ и ИБ, таких как COBIT, ITIL. Многие задачи (High Level Objectives), обозначенные в COBIT, могут быть автоматизированы с помощью MaxPatrol:

- *AI6 Manage Changes;*
- *AI7 Install and Accredited Solutions and Changes;*
- *ME1 Monitor and Evaluate IT Processes;*
- *ME2 Monitor and Evaluate Internal Control;*
- *ME3 Ensure Regulatory Compliance;*
- *ME4 Provide IT Governance;*
- *DS4 Ensure Continuous Service;*
- *DS5 Ensure Systems Security;*
- *DS8 Manage Service Desk and Incidents;*
- *DS9 Manage the Configuration;*
- *DS10 Manage Problems*

Комплексный подход к поиску уязвимостей позволяет MaxPatrol за одно сканирование проводить проверку на соответствие сложным стандартам безопасности. Ниже приведен анализ функций MaxPatrol с точки зрения проверки на соответствие PCI DSS.



... Контроль  
... политик  
... безопасности  
... с помощью  
... MaxPatrol

# КОНТРОЛЬ ПОЛИТИК БЕЗОПАСНОСТИ

ТРЕБОВАНИЯ PCI DSS	ВОЗМОЖНОСТИ MAXPATROL
1. Разработка и поддержка стандарта межсетевого экранирования	Механизмы MaxPatrol позволяют осуществлять проверку таких требований, как: <ul style="list-style-type: none"><li>● контроль разрешенных сетевых портов;</li><li>● контроль разрешенных сетевых служб;</li><li>● контроль небезопасных протоколов;</li><li>● анализ правил межсетевых экранов;</li><li>● контроль соответствия настроек маршрутизаторов;</li><li>● контроль конфигурации рабочих станций.</li></ul>
2. Отказ от использования стандартных настроек для паролей и других параметров защиты	Контроль использования стандартных паролей и параметров защиты, используя механизмы тестирования на проникновение и аудита. Контроль соответствия техническим требованиям. Обнаружение небезопасных протоколов удаленного управления.
3. Защита данных держателей банковских карт во время хранения	Контроль наличия и конфигурации средств шифрования данных. Поиск важной информации в СУБД, приложениях и файловой системе с помощью регулярных выражений.
4. Шифрование данных держателей банковских карт при передаче по открытым сетям	Контроль конфигурации беспроводных устройств, межсетевых экранов.
5. Использование и регулярное обновление антивирусных систем	Механизмы аудита и контроля соответствия позволяют своевременно обнаруживать системы, нарушающие правила антивирусной защиты.
6. Разработка и поддержка защищенных систем и приложений	Механизмы аудита и тестирования на проникновение позволяют своевременно обнаруживать отсутствие обновлений ПО. Механизмы анализа веб-приложений и СУБД позволяют выявлять уязвимости приложений.



ТРЕБОВАНИЯ PCI DSS	ВОЗМОЖНОСТИ MAXPATROL
7. Минимизация прав доступа к данным держателей банковских карт	Механизмы контроля соответствия дают возможность проверять настройку механизмов разграничения доступа.
8. Использование индивидуального разграничения доступа	Механизмы контроля соответствия позволяют проверять настройки системы аутентификации, такие как: <ul style="list-style-type: none"><li>● метод аутентификации (пароль, токены, биометрия);</li><li>● использование небезопасных протоколов аутентификации;</li><li>● контроль сложности и времени смены пароля;</li><li>● истекшие и неиспользуемые учетные записи.</li></ul>
9. Отслеживание и мониторинг доступа к сетевым ресурсам и данным держателей банковских карт	MaxPatrol позволяет контролировать настройки механизмов протоколирования и аудита для ОС, сетевого оборудования и приложений.
10. Регулярное тестирование безопасности систем и процессов	Использование механизмов тестирования на проникновение MaxPatrol является достаточным условием для соответствия требованиям по сканированию и тестированию защитных механизмов. Эффективные механизмы сканирования позволяют быть готовыми к тестам на проникновения и проверкам ASV.
11. Поддержка политики информационной безопасности, затрагивающей сотрудников и подрядчиков	Система MaxPatrol может использоваться для реализации механизмов инвентаризации, проверки технических политик безопасности и др.

# ИНВЕНТАРИЗАЦИЯ АКТИВОВ И КОНТРОЛЬ ИЗМЕНЕНИЙ



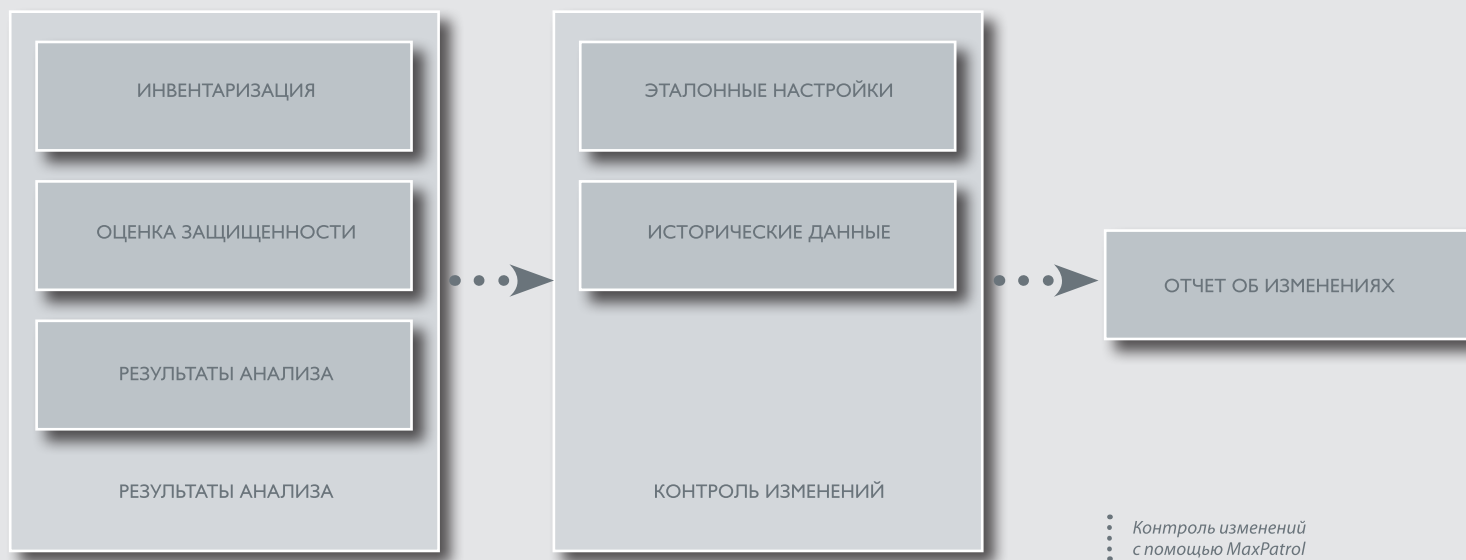
Инвентаризация и контроль изменений в постоянно изменяющихся и растущих информационных системах без использования средств автоматизации становятся практически невыполнимыми задачами. Но, с другой стороны, наличие актуальных данных об ИС необходимо для эффективного функционирования системы управления ИБ.

## Непрерывная инвентаризация

Автоматизированная инвентаризация информационных активов является важным компонентом системы управления ИТ и ИБ. Высокопроизводительный сетевой сканер и уникальные методы определения версий приложений, реализованные в

MaxPatrol, дают возможность оперативно собирать информацию о существующих элементах ИТ-инфраструктуры и отслеживать происходящие изменения. Функции инвентаризации, основанные на системных проверках, дают возможность минимизировать сетевой трафик и воздействие на системы, что позволяет чаще проводить сканирования и получать более актуальную информацию. Использование в ходе инвентаризации модулей анализа СУБД и приложений добавляют возможности контроля таких параметров, как учетные записи и группы пользователей, объекты баз данных.

Результаты инвентаризации могут быть использованы для контроля изменений или документирования состояния системы или отдельных узлов.



## Своевременное отслеживание изменений

Контроль изменений является одним из основополагающих моментов современных подходов к управлению информационной инфраструктурой, таких как ITIL, COBIT. Для оценки эффективности предпринятых мер и планирования развития ИТ и ИБ требуется не только знать текущее состояние системы, но и иметь возможность сравнить его с состоянием, к примеру, на прошлой неделе, в прошлом месяце.

Механизмы формирования отчетов в MaxPatrol дают возможность отслеживать изменения состояния всей информационной системы, отдельных ее

подразделений и узлов. Примерами событий, контролируемых с помощью этого механизма, являются: появление новых сетевых узлов и служб, переустановка операционной системы, изменение аппаратной конфигурации.

Однако возможности MaxPatrol не ограничиваются только отслеживанием изменений в инвентаризационной информации. Существуют возможности отслеживать изменения в параметрах безопасности систем, полученных в результате оценки защищенности и контроля политик безопасности. Это позволяет контролировать и оперативно реагировать на изменения в системе, которые могут приводить к нарушению требований безопасности и являться причиной инцидентов.



# МОНИТОРИНГ ЗАЩИЩЕННОСТИ СИСТЕМ ЛЮБОГО МАСШТАБА

## Распределенная архитектура

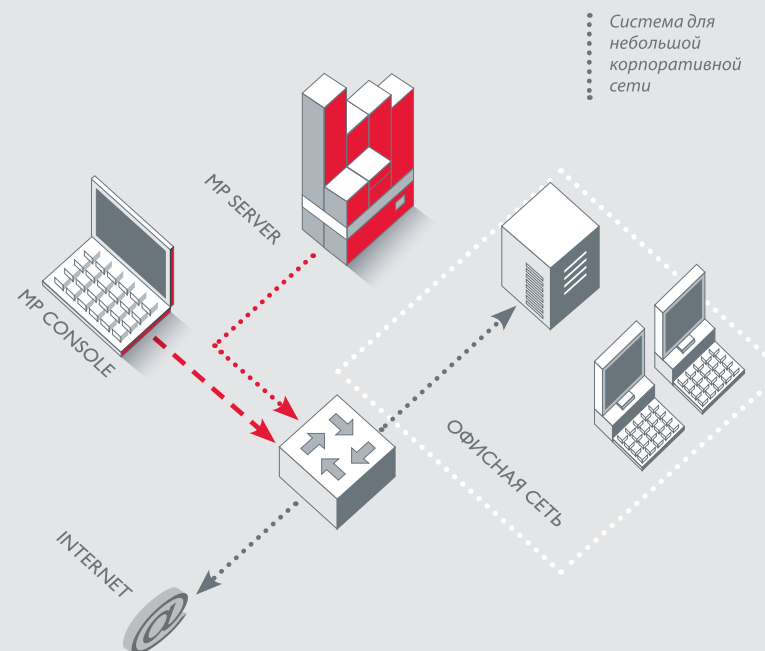
Система MaxPatrol построена на основе трехуровневой архитектуры, что обеспечивает высокое масштабирование и позволяет производить внедрения в компаниях любых размеров. В качестве хранилища информации может использоваться как внутренняя база данных, так и корпоративная СУБД. При внедрении учитываются иерархия СУИБ и пропускная способность каналов связи, что позволяет использовать систему с максимальной эффективностью. В зависимости от ситуации могут быть использованы различные дистрибутивы и наборы компонентов системы, что даёт возможность строить систему мониторинга состояния информационной безопасности в соответствии с потребностями заказчика.

## Система для небольшой корпоративной сети

Система мониторинга информационной безопасности для небольшого офиса содержит минимальное количество компонентов.

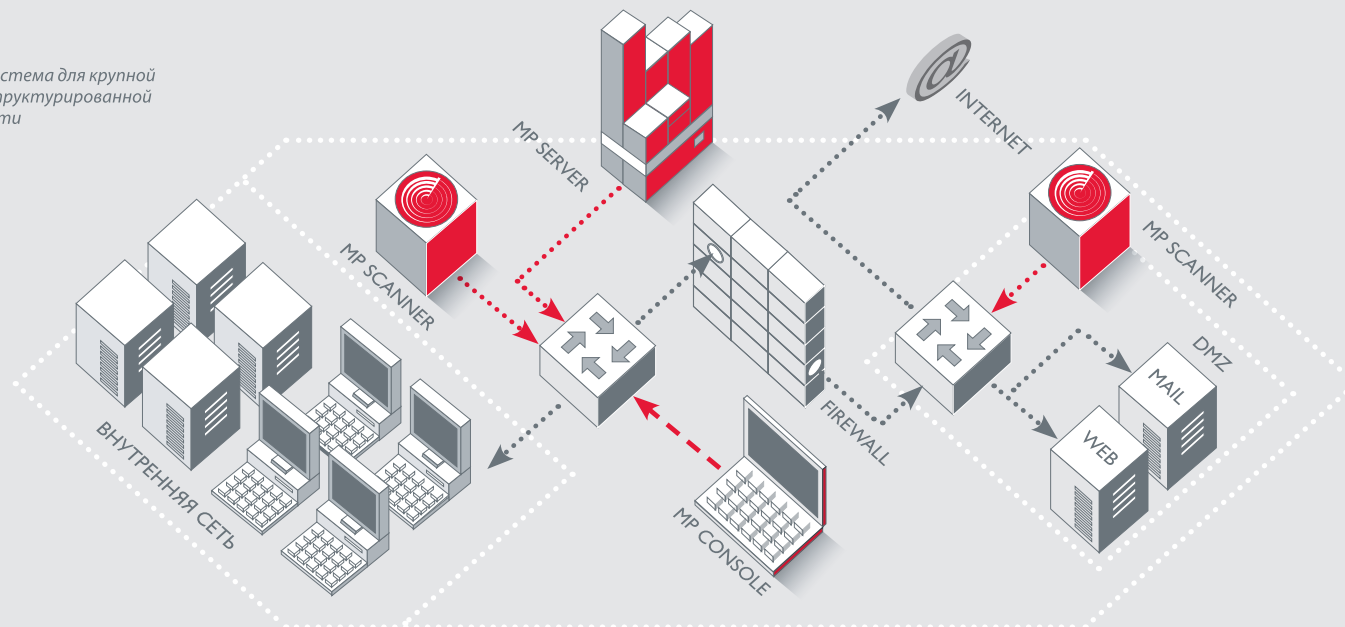
Для небольшой системы достаточно одного MP Server. Его можно установить и на одном из серверов компании, хотя следует иметь в виду, что сканер может отрицательно повлиять на производительность сервера.

Обновления MaxPatrol в такой системе загружаются непосредственно из Интернета.





Система для крупной структурированной сети



## Система для крупной структурированной сети

В крупной компании сканирование можно осуществлять одновременно снаружи и изнутри. Для большой сети целесообразно в дополнение к MP Server установить несколько дополнительных сканеров, чтобы увеличить скорость и эффективность сканирования.

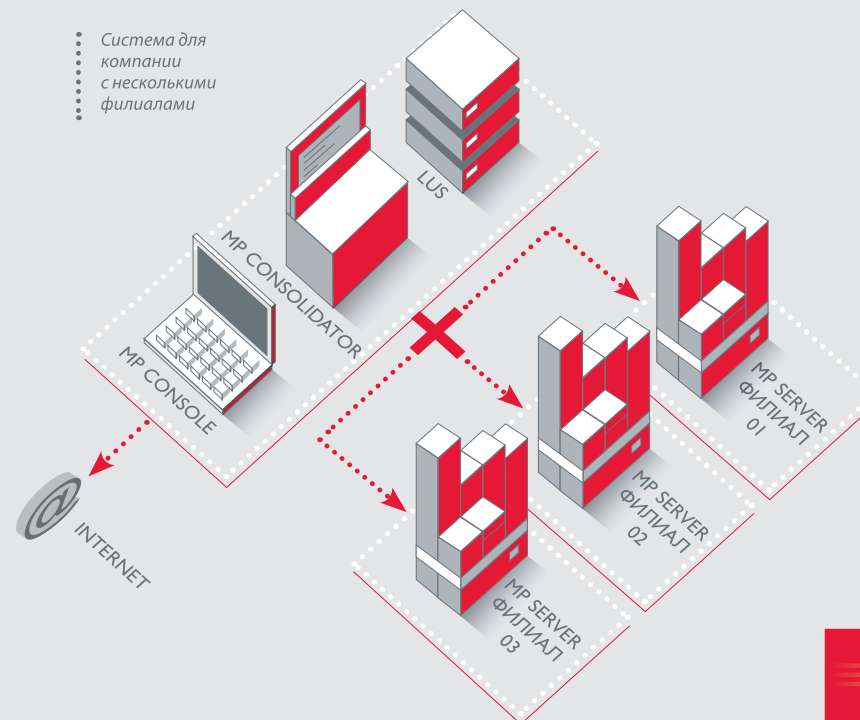
## Система для компании с несколькими филиалами

Для крупной многофилиальной корпорации оптимальной является следующая схема развёртывания системы MaxPatrol:

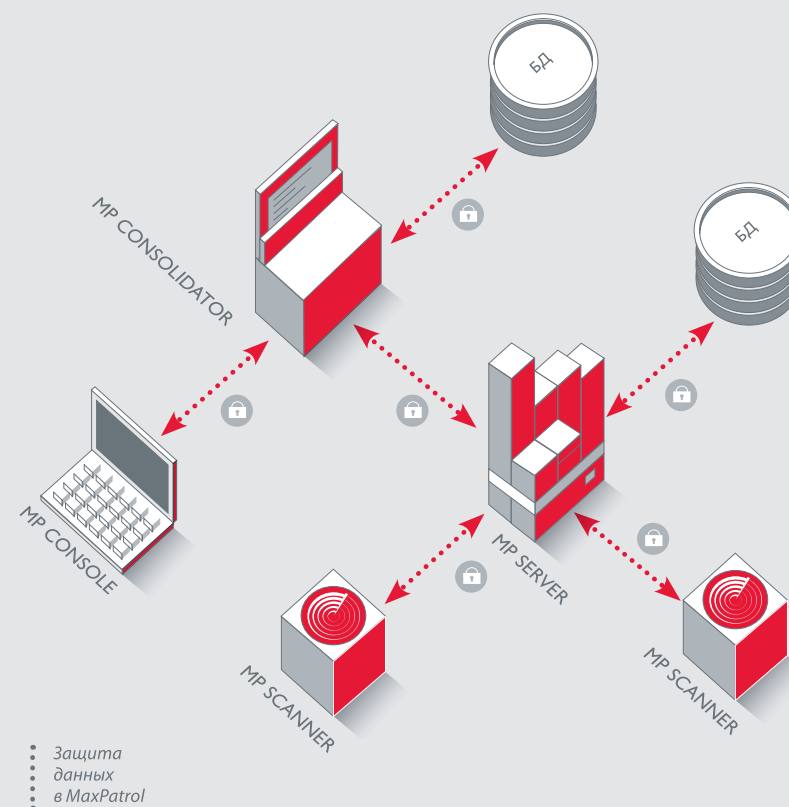
- в каждом филиале устанавливается свой MP Server с одним или несколькими сканерами;
- в центральном офисе устанавливается сервер консолидации и сервер обновлений, собирающие информацию от филиалов;
- связь с филиалами при этом может быть как постоянной, так и периодической.

При такой конфигурации обновления модулей MaxPatrol можно получать напрямую из Интернета или (если Интернет-подключение недоступно или ограничено) установить в центральном сегменте локальный сервер обновлений MaxPatrol.

Система для компании с несколькими филиалами



# БЕЗОПАСНОСТЬ MAXPATROL



Учитывая высокие требования к конфиденциальности информации, обрабатываемой системой, в MaxPatrol реализованы мощные механизмы обеспечения безопасности.

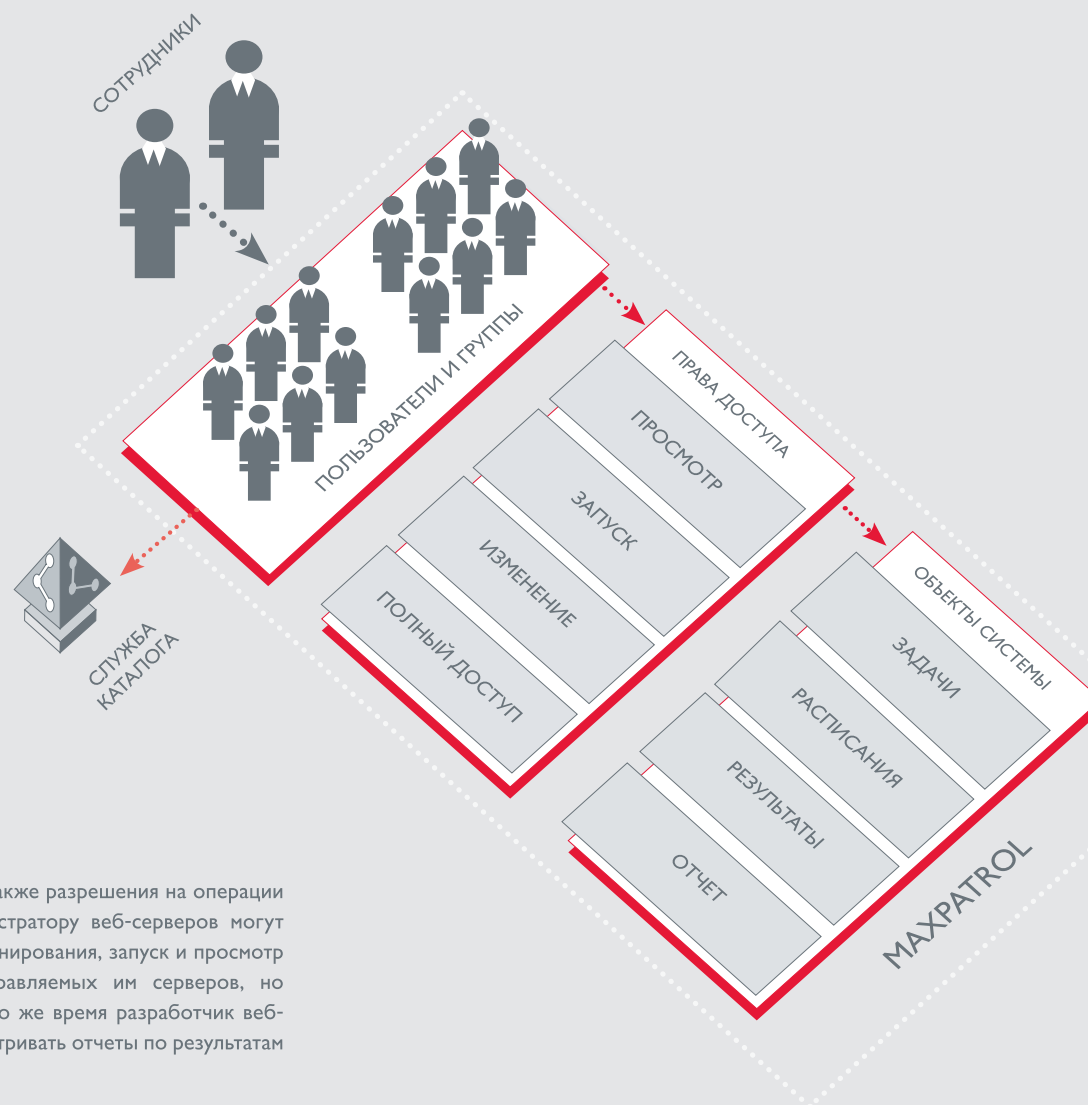
## Защита данных

При передаче и хранении используются криптографические методы защиты, обеспечивающие конфиденциальность и целостность важной информации, такой как пароли пользователей, привилегии на доступ и т. д. Предусмотрена возможность использования сертифицированных реализаций отечественных криптографических алгоритмов.

Защита трафика обеспечивается с помощью цифровых сертификатов и протокола SSL/TLS, являющегося промышленным стандартом, что обеспечивает высокую совместимость и защиту данных. Поддерживается интеграция с существующей инфраструктурой открытых ключей (PKI).

## Разграничение доступа

Гибкая система разграничения прав доступа дает возможность производить мониторинг информационной безопасности на различных уровнях иерархии (например, на уровне администраторов, менеджеров ИТ и ИБ-подразделения, директора по ИБ). Для каждого из пользователей системы можно задать список



- Разграничение
- доступа
- в MaxPatrol

заданий, которые он может выполнять в системе, а также разрешения на операции над конкретными объектами системы. Так, администратору веб-серверов могут быть делегированы права на изменение профиля сканирования, запуск и просмотр результатов задачи по оценке защищенности управляемых им серверов, но запрещено изменять список сканируемых узлов. В то же время разработчик веб-приложений будет иметь возможность только просматривать отчеты по результатам сканирования.

Разрешения могут назначаться на уровне MaxPatrol Server или MaxPatrol Consolidator. Такой подход позволяет адаптировать систему разграничения доступа практически под любую иерархию управления системой ИБ.

# АВТОМАТИЗАЦИЯ ПРОЦЕССОВ ИБ

В системе контроля защищенности и соответствия стандартам безопасности MaxPatrol заложен ряд возможностей, которые упрощают и автоматизируют процессы, связанные с обеспечением ИБ.

## Контроль актуальных угроз безопасности

Интеллектуальные возможности MaxPatrol разрабатываются при активном участии команды консультантов и экспертов по информационной безопасности компании Positive Technologies. Уникальный опыт, полученный в ходе аудитов безопасности, тестов на проникновение и оценки защищенности веб-приложений, позволяет постоянно повышать качество механизмов MaxPatrol и контролировать их эффективность в реальных условиях. База знаний системы MaxPatrol постоянно обновляется, что обеспечивает выявление и оперативное устранение актуальных угроз безопасности.

## Анализ рисков

Использование для оценки степени риска, связанной с уязвимостью, универсальной системы Common Vulnerability Scoring System (CVSS), позволяет применять отчеты MaxPatrol в качестве исходных данных для различных методик анализа рисков.

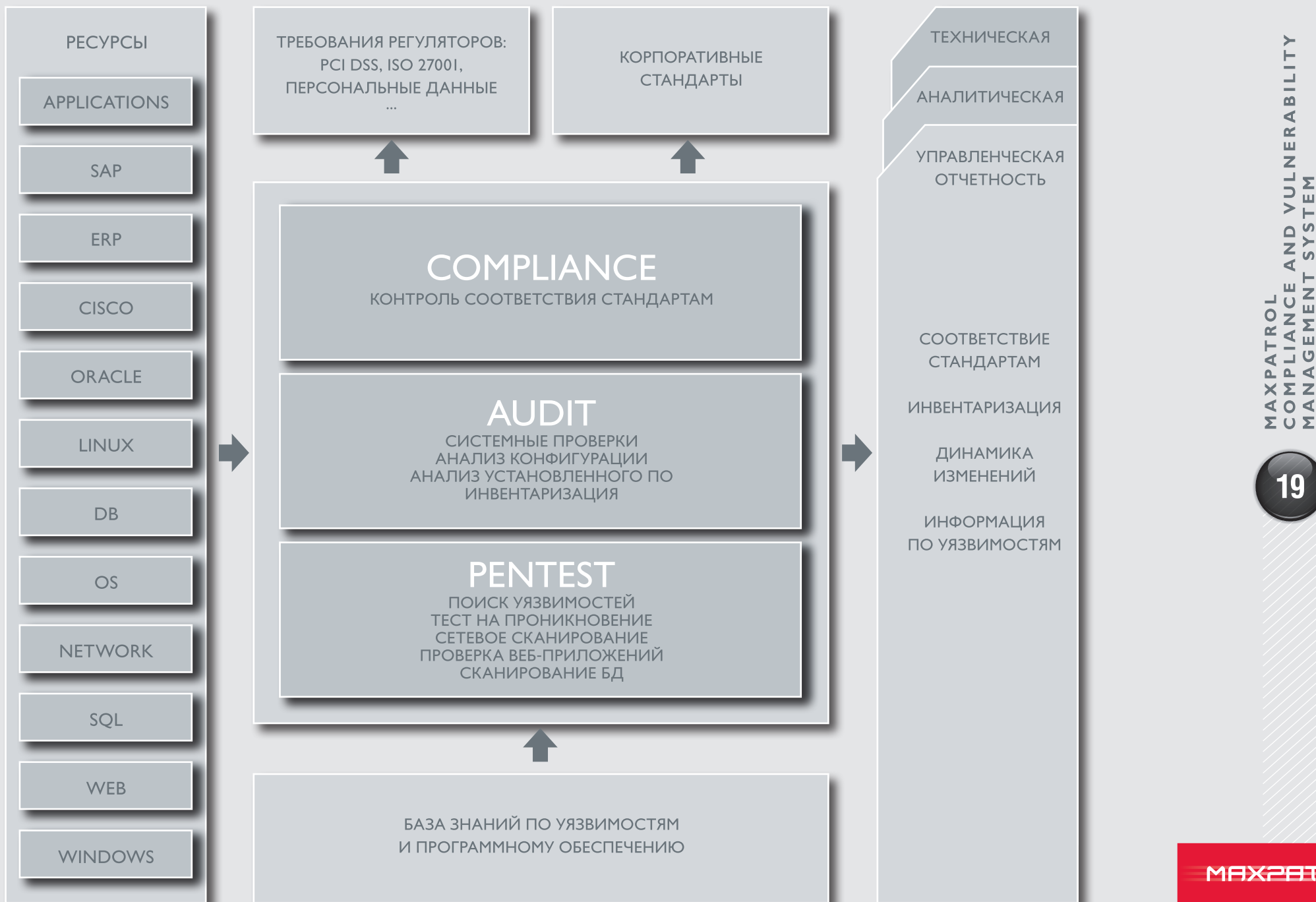
Значение, получаемое в результате расчета CVSS, учитывает такие параметры,

как последствия использования, сложность эксплуатации уязвимости, наличие «эксплойта», доступность информации об исправлении и т. д. Путем нормализации значение CVSS может быть приведено к другим системам оценки риска, связанного с уязвимостью, например, к классической трехуровневой «светофорной» оценке или к пятиуровневому рейтингу, принятому в стандарте PCI DSS. Функция переназначения уровня риска, связанного с уязвимостью, дает возможность определять приоритеты по устранению проблемы для разных групп узлов.

## Генерация и доставка отчетов

Мощный модуль отчетов позволяет создавать их на основе стандартных и собственных шаблонов. Возможность создания собственных отчетов позволяет предоставлять информацию системы в максимально удобном и отвечающем конкретным задачам виде. Результаты могут сохраняться в различных форматах, а также доставляться конечному пользователю с использованием транспортов HTTP, E-mail и т. д.

Модуль отчетов позволяет включать в себя как результаты, полученные непосредственно в ходе сканирования, так и информацию, полученную из множества источников и задач, включая данные истории сканирований. Например, отчет об оперативности устранения уязвимостей по подразделениям компании строится на основе данных истории сканирования по множеству узлов.



# АВТОМАТИЗАЦИЯ ПРОЦЕССОВ ИБ

## Автоматизация процессов

Мощный модуль управления задачами полностью автоматизирует логику работы системы: от обнаружения новых узлов до анализа защищенности, составления отчетов и реагирования на обнаружение нарушений требований ИБ.

В ходе внедрения логика работы системы может быть адаптирована под внутренние процессы в компании заказчика.

Например, в случае обнаружения нового сетевого узла система уведомляет администратора сети, автоматически запускает процесс сканирования этого компьютера в режиме тестирования на проникновение и передает результаты сканирования по электронной почте ответственному лицу.

## Консолидация событий и управление обновлениями

Интеграция с системами управления обновлениями и системами консолидации и корреляции событий ИБ (netForensics, ArcSight, Cisco MARS) позволяют использовать MaxPatrol в качестве основы для построения корпоративной системы управления уязвимостями.

# СЦЕНАРИИ ВНЕДРЕНИЯ MAXPATROL

Система MaxPatrol спроектирована таким образом, чтобы приносить максимальную отдачу в различных ситуациях. Ниже приведено несколько возможных сценариев внедрения системы контроля защищенности и соответствия стандартам.

## Повышение уровня зрелости

На определенном этапе существующий уровень системы менеджмента ИБ перестает удовлетворять требованиям бизнеса. Информационная система может развиваться эволюционно или по заранее обозначенному плану. Вне зависимости от этого, для качественного перехода на новый уровень зрелости требуется серьезная подготовка. Примером подобного перехода может стать внедрение международных и отраслевых стандартов.

Большинство ИТ и ИБ-стандартов содержит в своей основе набор проблемных областей или защитных механизмов, влияющих как на бизнес-процессы, так и на технические аспекты инфраструктуры, на основе которых планируются вносимые изменения.

Перефразируя классический цикл Деминга-Шухарта (PDCA: Plan-Do-Check-Act), можно выделить следующие этапы реализации задачи:

- *определение требований к новой информационной инфраструктуре;*
- *оценка соответствия существующего положения дел выработанным требованиям;*
- *выработка мер по улучшению уровня соответствия;*
- *устранение несоответствий.*

Система MaxPatrol может эффективно применяться на каждом из этих этапов. Обширная база знаний стандартов и уязвимостей может использоваться для формирования требований к различным информационным системам и приложениям. В ходе внедрения заказчик может определить собственные требования к информационным системам и процессам мониторинга информационной безопасности или использовать наработки из имеющейся базы знаний системы.

Механизм создания собственных списков соответствия позволяет разбить процесс повышения уровня зрелости на этапы, что дает возможность сконцентрироваться на ключевых задачах. Подробные описания проблем и рекомендации по устранению позволяют эффективно бороться с обнаруженными несоответствиями. Аналитические отчеты на основе истории сканирования и функции расчета численных метрик (KPI) играют незаменимую роль в ходе оценки динамики эффективности состояния системы менеджмента информационной безопасности.

# СЦЕНАРИИ ВНЕДРЕНИЯ MAXPATROL

Таким образом, применение MaxPatrol в этом случае даёт возможность:

- сформулировать требования к информационной инфраструктуре;
- регламентировать и автоматизировать процессы аудита систем;
- в кратчайшие сроки внедрить принятые технические стандарты;
- использовать объективные численные метрики (KPI) для оценки эффективности ведения проекта.

## Слияния и поглощения

Слияния и поглощения часто приводят к серьезному падению уровня информационной безопасности. Объединение информационных систем различного уровня, использующих разные подходы и инфраструктурные решения, не проходит безболезненно. Зачастую перед ИТ- и ИБ-подразделениями ставится задача максимально быстро и эффективно «подтянуть» присоединяемую систему до принятого в компании уровня. Существует множество подходов к решению этой задачи – от полной перестройки инфраструктуры до интеграции существующих решений без ощутимых изменений. Но в любом случае, задачи определения наиболее проблемных мест, оценка текущей готовности и отслеживание развития проекта являются важнейшими моментами процесса слияния ИТ-инфраструктур различных компаний.

Механизмы тестирования на проникновения и аудита системы MaxPatrol позволяют оперативно оценить текущее состояние ИТ и ИБ присоединяемой компании, идентифицировать наиболее уязвимые узлы и системы. Автоматизация изменений может применяться для сбора и поддержания в актуальном состоянии информации о ресурсах системы, что является необходимым условием любого проекта.

Функции контроля соответствия дают наглядное представление о различиях между требованиями, предъявляемыми к конфигурации и защите систем, и сложившейся ситуацией. Механизмы контроля и анализа изменений используются для оценки эффективности ведения проекта.

Таким образом, применение MaxPatrol в случае слияний и поглощений даёт возможность:

- поддерживать в актуальном состоянии информацию по активам системы;
- оперативно проводить технические аудиты ИТ и ИБ;
- получать оперативную техническую и управленческую информацию;
- в кратчайшие сроки внедрить принятые технические стандарты;
- использовать объективные численные метрики (KPI) для оценки прогресса проекта.





## Эволюционное развитие и повышение эффективности

В настоящее время многие компании достигли высокого уровня развития систем менеджмента ИТ и ИБ. Доказательством этого факта является увеличение количества компаний, получивших признание в рамках тех или иных отраслевых стандартов.

Одной из важнейших задач, стоящих перед любой системой менеджмента, в том числе и системой менеджмента ИТ и ИБ, является постоянное самосовершенствование и повышение эффективности процессов. Однако контроль и развитие невозможны без наличия актуальных и оперативных данных о текущем положении дел.

Система MaxPatrol позволяет автоматизировать многие периодические задачи по инвентаризации, техническому аудиту, контролю соответствия и изменений в информационных системах. Автоматизация процессов позволяет снизить затраты на выполнение данных задач. Более того, использование технических средств дает возможность проводить проверки гораздо чаще, что положительно сказывается на актуальности используемой менеджментом информации. Фактически, время и трудозатраты на проверки ручным и автоматизированным методом могут отличаться в десятки и сотни раз.

Получение точных и объективных данных об уязвимостях и расхождениях с требованиями стандартов дает возможность использовать результаты MaxPatrol в формировании метрик эффективности процессов ИБ.

Таким образом, применение MaxPatrol в этом случае позволяет:

- *регламентировать и автоматизировать процессы аудита систем;*
- *снизить трудозатраты и повысить эффективность процессов мониторинга и контроля изменений;*
- *отказаться от субъективных экспертных оценок в пользу однозначных воспроизводимых результатов;*
- *использовать объективные численные метрики (KPI) для оценки и повышения эффективности системы менеджмента ИБ.*

### **Positive Technologies – одна из ведущих российских компаний в области информационной безопасности**

Основные направления деятельности компании – разработка системы контроля защищенности и соответствия стандартам MaxPatrol и сканера безопасности XSpider; предоставление консалтинговых и сервисных услуг в области информационной безопасности; развитие специализированного портала Securitylab.ru.

Positive Technologies – это команда высококвалифицированных разработчиков, консультантов и экспертов, которые обладают большим практическим опытом, являются членами международных организаций и активно участвуют в развитии отрасли.



