

# MaxPatrol 8

POSITIVE TECHNOLOGIES

[ptsecurity.ru](http://ptsecurity.ru)

**Positive Technologies:**

---

в цифрах и фактах

Каждый год

**200+**

аудитов безопасности корпоративных систем

**200+**

обнаруженных уязвимостей нулевого дня

### Главные продукты

MaxPatrol	MaxPatrol SIEM
PT ISIM	PT Application Firewall



**15**

лет исследований и экспертизы

**150+**

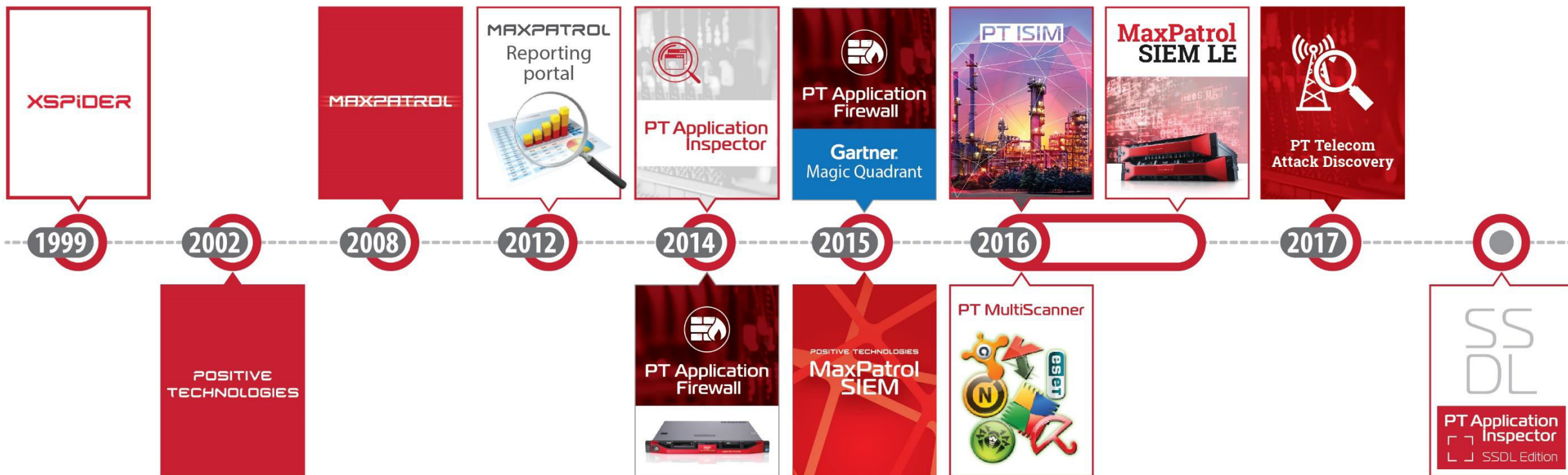
уязвимостей нулевого дня в системах SCADA

**30+**

обнаруженных уязвимостей нулевого дня в Mobile Telco

**500+**

исследований безопасности мобильных и веб-приложений



## Финансы, страхование



## Телекоммуникации



## Промышленность, энергетика



## Госсектор



ФНС



МВД



Минобороны



ФСТЭК



ПФР



ГОЗНАК



ФТС

**MaxPatrol 8.**

---

Контроль защищенности  
и соответствия стандартам

Каждую **вторую** систему может взломать неквалифицированный хакер

73%

Защита периметра  
**не останавливает**  
проникновение

96%

Атак могли быть  
предотвращены  
**стандартными**  
решениями

87%

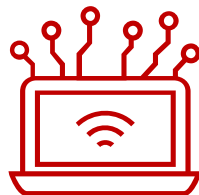
Инцидентов стали  
успешными **из-за**  
**серьезных ошибок**  
в конфигурации

73%

Атак **не требовали**  
высокой  
квалификации  
нарушителей



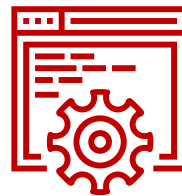
**Слабые  
пароли**



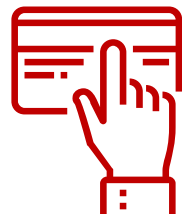
**Небезопасные  
беспроводные сети**



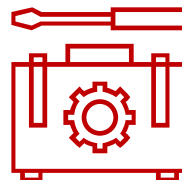
**Уязвимости  
веб-приложений**



**Программное  
обеспечение**



**Социальная  
инженерия**



**Ошибки в настройках:**

- сетевого оборудования
- систем защиты периметра
- веб-приложений
- баз данных





- Требуется наличие узкопрофильных специалистов
- Длительное время обслуживания каждого компонента ИС
- Высокая роль человеческого фактора



- + Использует единые подходы для анализа всех компонентов ИС
- + Производится на регулярной основе автоматически
- + Формирует унифицированную отчетность

1

Инвентаризация  
и контроль конфигураций

2

Комплексная  
оценка защищенности

3

Автоматизация  
контроля соответствия требованиям

4

Технические  
и высокоуровневые отчеты

5

Ежедневно обновляемая  
база знаний





**MaxPatrol 8.**

---

Особые сценарии использования



## ERP



NetWeaver™



R/3



R/3  
ENTERPRISE



## АСУ ТП



SIEMENS



invenSys



Rockwell  
Automation



Schneider  
Electric



## ТЕЛЕКОМ



HUAWEI

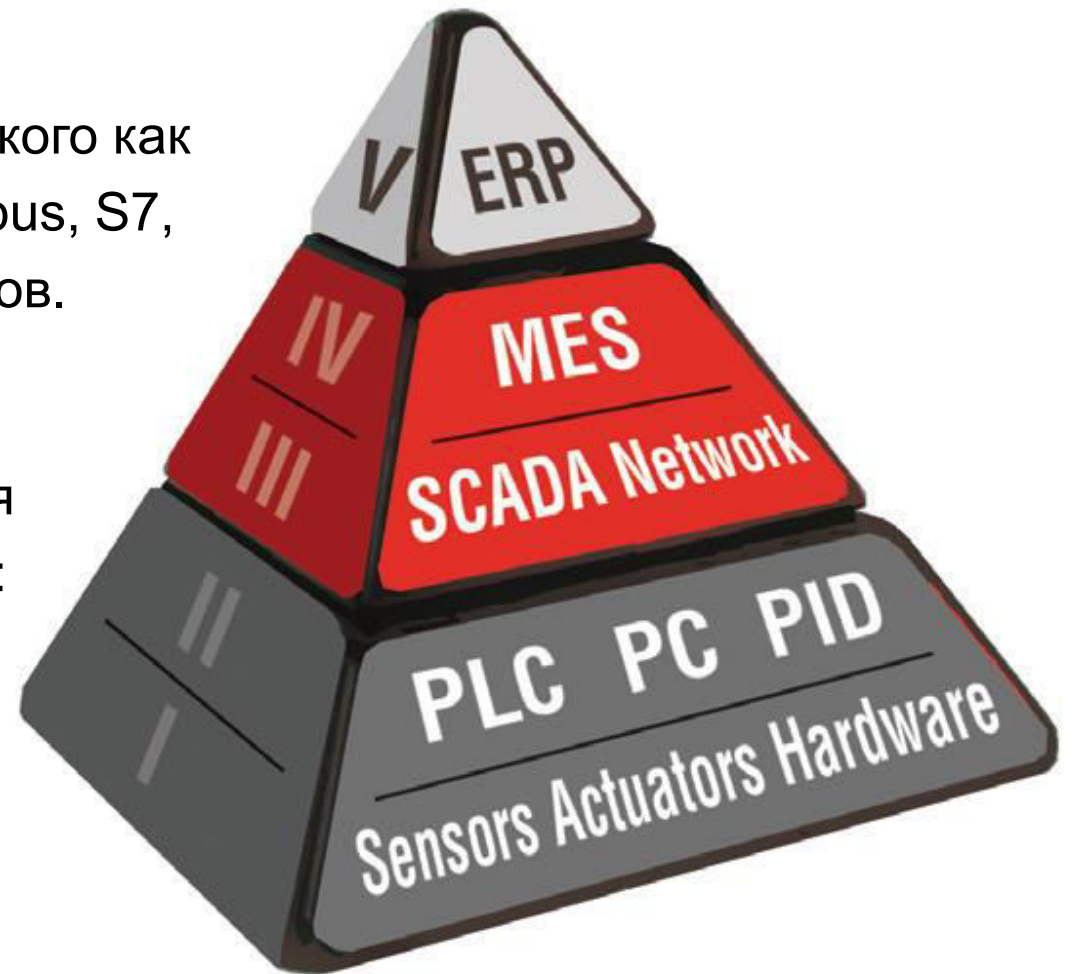


ERICSSON



**MaxPatrol** имеет встроенные проверки для специализированного сетевого оборудования, такого как Cisco Connected Grid, реализует поддержку Modbus, S7, DNP3, IEC104 и других промышленных протоколов.

База знаний содержит более **30 000** проверок на уязвимости и требования по безопасности для *HMI/SCADA, PLC, RTU* ведущих производителей: **Siemens, Schneider Electric, Rockwell Automation, ABB.**



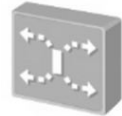
1

## УСТРАНЕНИЕ ПЕТЕЛЬ КОММУТАЦИИ HUAWEI

Статус	IP	Стр. ID	Полное описание
Соответствует	10.176.71.196	436196	Включить Loopback-detection на интерфейсах S33/S53-UNI, S33/S53-UNI и S33/S53-ext-UNI
Соответствует	10.176.71.198		
Соответствует	10.176.71.199		
Соответствует	10.176.71.200		
Соответствует	10.176.71.201		
Соответствует	10.176.71.202		
Соответствует	10.176.71.203		
Не соответствует	10.176.71.204		Технические требования, которые переопределены пользователем
Не соответствует	10.176.71.205		Включить Loopback-detection на интерфейсах S33/S53-UNI, S33/S53-UNI и S33/S53-ext-UNI
Не соответствует	10.176.71.206		
Не соответствует	10.176.71.207		
Не соответствует	10.176.71.208		
Не соответствует	10.176.71.209		
Не соответствует	10.176.71.210		
Не соответствует	10.176.71.223		loopback-detect enable
Соответствует	10.176.71.225		
Соответствует	10.176.71.226		
Соответствует	10.176.71.227		
Соответствует	10.176.71.228		
Соответствует	10.176.71.229		
Соответствует	10.176.71.230		
Соответствует	10.176.71.231		
Соответствует	10.176.71.234		

Название блока	Значение	Несоответствие	Статус
interface Auh0/0/1	link-protocol ppp undo shutdown		Входит в список исключений
interface GgabitEthernet10/0/0	speed auto duplex auto undo shutdown		Входит в список исключений
interface GgabitEthernet11/0/0	carrier up-hold-time 10000 description BSC_OAM_1c7919348_BEZERV_T77419948 undo shutdown set flow-stat interval 30 mtu 9600 l2 binding vsi BSC_DAM undo don trust upstream default trust 8021p	loopback-detect enable	Не соответствует требованию
interface GgabitEthernet11/0/1	carrier up-hold-time 10000 description BSC_OAM_Beloreck_1C7910932 undo shutdown set flow-stat interval 30 mtu 9600 l2 binding vsi BSC_OAM_Beloreck_1C7923386 undo don loopback-detect enable trust upstream not_6_7 trust 8021p undo ltp enable		Соответствует требованию



GGSN



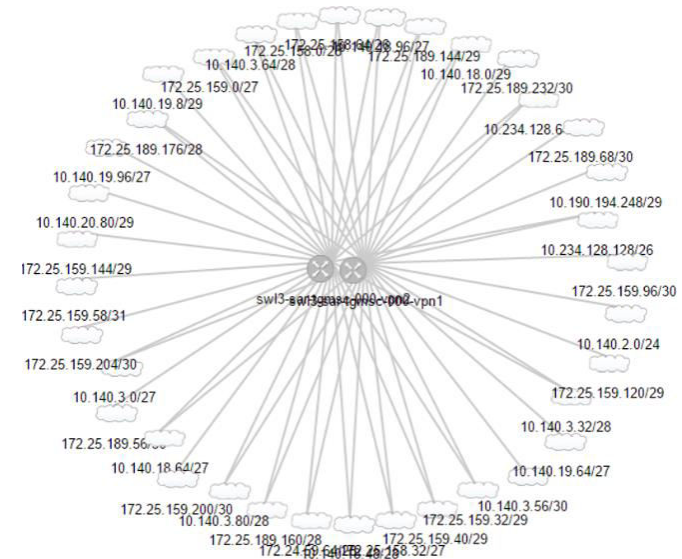
RNC



Node B

2

## ПОСТРОЕНИЕ ТОПОЛОГИИ МЕН-СЕТЕЙ



3

## КОНТРОЛЬ СООТВЕТСТВИЯ LOW LEVEL DESIGN

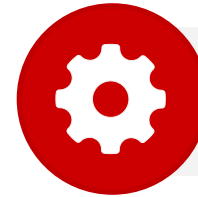
4

## АУДИТ МЕН-СЕТЕЙ



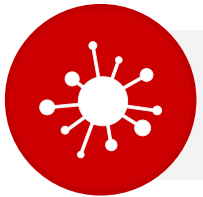
## СООТВЕТСВИЕ ТРЕБОВАНИЯМ ТЕХНИЧЕСКИХ СТАНДАРТОВ

- для прикладного
- для системного
- для сетевого
- для пользовательского уровней



## ИНВЕНТАРИЗАЦИЯ КОМПОНЕТОВ СИСТЕМЫ

- серверы приложений SAP
- серверы СУБД
- рабочие станции
- сетевое оборудование
- средства защиты



## ВЫЯВЛЕНИЕ И УСТРАНЕНИЕ ТЕХНИЧЕСКИХ УЯЗВИМОСТЕЙ

- SAP R/3 и SAP R/3 Enterprise;
- SAP NetWeaver AS ABAP;
- SAP NetWeaver AS JAVA;
- Бизнес модулей SAP
- SAPRouter



## АНАЛИЗ КОНФИГУРАЦИЙ СИСТЕМЫ И ЕЕ КОМПОНЕТОВ

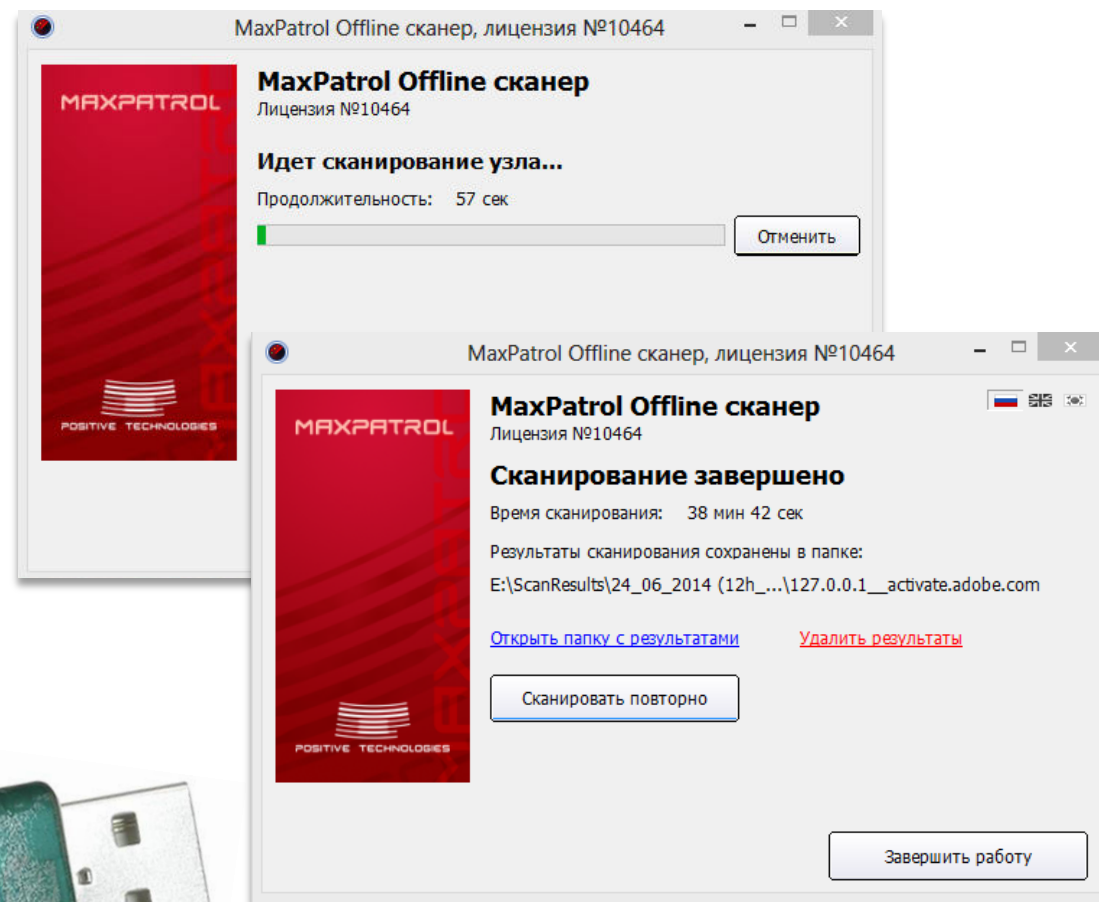
- системные параметры
- бизнес модули (ERP, HR, MM)
- сервисы SAP системы
- настройки шифрования
- неиспользуемые RFC-соединения
- статус учетных записей и критичные полномочия



Компонент **offline-сканер** предназначен для сканирования узлов, изолированных от локальной сети.

Он позволяет произвести полноценное сканирование Windows-систем в режимах **pentest, audit, compliance, forensic**.

Сканирующий **offline-модуль** размещается на специализированном USB-носителе.



# 1000+

СИСТЕМ,  
с которыми умеет работать **MaxPatrol 8**, среди них:

## Операционные системы



## Базы данных



## Сетевое оборудование



## Инфраструктурные приложения



## Решения виртуализации

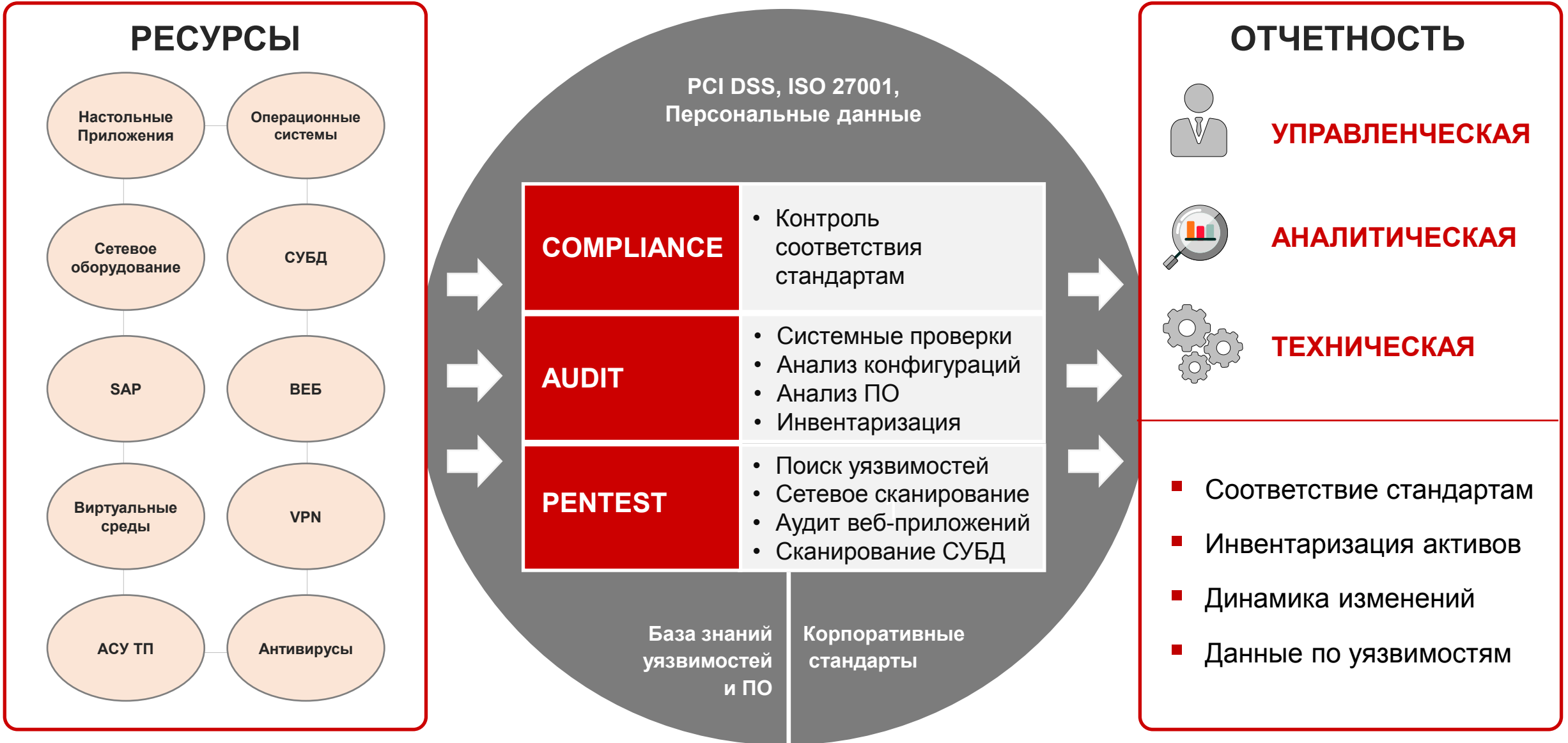


## Настольные приложения

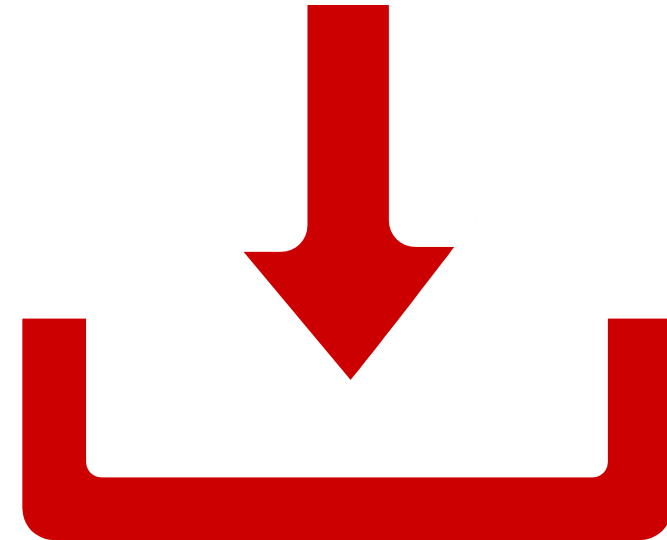


## Средства безопасности





- Анализ в режиме «черного ящика»
- Определяет уязвимости:
  - путем анализа сообщений (баннеров)
  - используя логику работы эксплойтов
  - эвристическими методами
- Анализирует веб-приложения
- Перебирает пароли
- Диагностирует сетевые службы



The screenshot displays a Pentest tool interface on the left and a browser window on the right. The tool interface includes a 'Навигатор' (Navigator) pane with a tree view of scanned services, a 'Сводная/узлы' (Summary/Nodes) pane, and an 'Информация' (Information) pane. The 'Информация' pane shows a critical vulnerability: 'Выполнение произвольного кода' (Arbitrary code execution) with ID 8339, CVE-2015-0240, and f5tec: BDU:2015-10377. The browser window shows the SecurityFocus article 'Samba 'TALLOC\_FREE()' Function Remote Code Execution Vulnerability' with tabs for 'info', 'discussion', 'exploit', 'solution', and 'references'. The article text includes a red box highlighting the available exploit and proof-of-concept code: `./data/vulnerabilities/exploits/72711.rb` and `./data/vulnerabilities/exploits/72711.py`.

**Навигатор**

- Сортировка - Узел - Журнал
- 445 / tcp - Microsoft DS
  - Выполнение произвольного кода
  - Атака "на понижение" (BADLOCK)
  - Удаленное управление реестром
- 22 / tcp - SSH
- 53 / tcp - DNS
- 139 / tcp - NetBIOS samba
- 8080 / tcp - HTTP
- 110 / tcp - POP3
- 143 / tcp - IMAP
- 993 / tcp - IMAP SSL
- 995 / tcp - POP3 SSL
- 10000 / tcp - HTTP SSL
- 80 / tcp - HTTP
- System
- 53 / udp - DNS
- 137 / udp - NetBIOS Name
- 23 / tcp
- 1723 / tcp - PPTP
- 1521 / tcp - Oracle Listener
- 139 / tcp - NetBIOS samba
- 25 / tcp - SMTP
- 443 / tcp - HTTP SSL
- 445 / tcp - Microsoft DS
- System
- 137 / udp - NetBIOS Name
- 20005 / tcp - HTTP
- 80 / tcp - HTTP
- 8009 / tcp - Apache JServ Protocol
- 5432 / tcp - PostgreSQL
- PostgreSQL
- Повышение привилегий

**Информация**

Серьезная уязвимость  
**Выполнение произвольного кода**  
ID: 8339  
CVE: CVE-2015-0240  
f5tec: BDU:2015-10377

**Краткое описание**  
Уязвимость позволяет атакующему выполнить произвольный код.

**Описание**  
Уязвимость существует в реализации сервера Netlogon в smbд в Samba (в версиях 3.5.x и 4.1.17, а также в 4.2.x до 4.2.0rc5) из-за освобождения неинициализированного указателя уязвимости позволяет злоумышленникам, действующим удаленно, выполнить произвольные сформированных пакетов Netlogon, использующих ServerPasswordSet RPC API, например `_netr_ServerPasswordSet` в `rpc_server/netlogon/srv_netlog_nt.c`.

**Как исправить**  
Для устранения уязвимости необходимо установить последнюю версию продукта, соответствующую используемой платформе. Необходимую информацию можно получить по адресу:  
<https://www.samba.org/>  
<https://access.redhat.com/articles/1346913>

**Ссылки**  
<https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0240>  
<https://www.nccgroup.trust/en/blog/2015/03/exploiting-samba-cve-2015-0240-on-ubuntu-1204-and-debian-7-32-bit/>  
<https://securityblog.redhat.com/2015/02/23/samba-vulnerability-cve-2015-0240/>  
<https://www.samba.org/samba/security/CVE-2015-0240>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0240>

**CVSS**  
Базовая оценка: **10** (AV:N/AC:L/Au:N/C:C/I:A/C)   
AV:N данная уязвимость может эксплуатироваться удаленно  
AC:L для эксплуатации уязвимости не требуются особые условия  
Au:N для эксплуатации уязвимости проходить аутентификацию не требуется  
C:C эксплуатация уязвимости влечет полное разглашение конфиденциальных данных

**SecurityFocus™**

info discussion exploit solution references

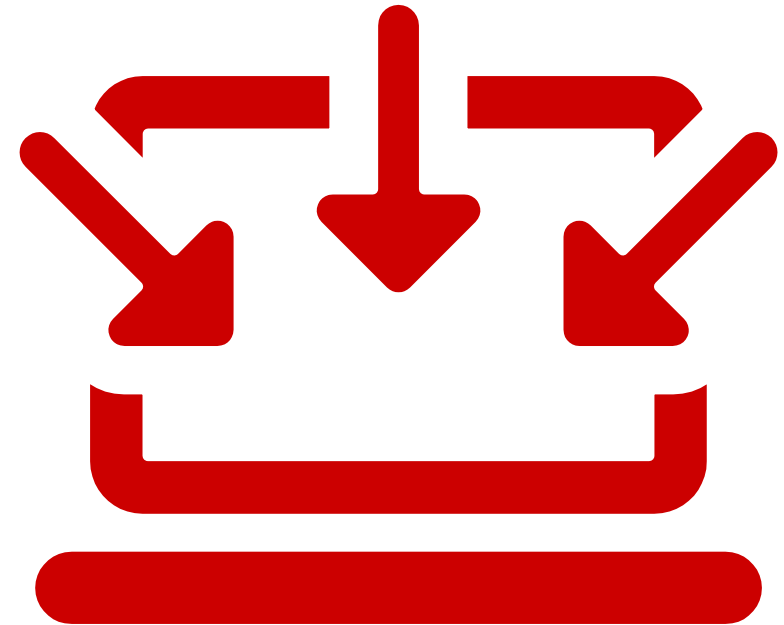
**Samba 'TALLOC\_FREE()' Function Remote Code Execution Vulnerability**

The following exploit and prof-of-concept code are available:

- `./data/vulnerabilities/exploits/72711.rb`
- `./data/vulnerabilities/exploits/72711.py`

Privacy Statement  
Copyright 2010, SecurityFocus

- Не требует установки агента
- Использует стандартные протоколы удаленного доступа
  - Инвентаризация аппаратного и программного обеспечения
  - Проверки наличия обновлений безопасности
  - Выявление наличия уязвимостей и ошибок конфигураций
  - Анализ конфигурации
  - Контроль учетных записей
  - Контроль изменений



The screenshot displays the Positive Technologies Audit interface. On the left is a 'Навигатор' (Navigator) pane showing a tree view of system components. The right pane, titled 'Информация' (Information), displays details for a specific vulnerability. A red box highlights the vulnerability title and its ID, CVE, and publication date. Another red box highlights the 'Краткое описание' (Brief description) section. Below that, the 'Описание' (Description) section provides a detailed explanation of the vulnerability. The 'Как исправить' (How to fix) section offers a link to the manufacturer's recommendations. The 'Ссылки' (Links) section provides additional references. The 'CVSS' section shows the base and temporal scores along with their components.

**Навигатор**

- Сортировка ▾ Узел ▾ Журнал
- 192.168.53.20
  - Microsoft .NET Framework
  - Microsoft Internet Explorer
  - Microsoft JScript
  - Microsoft Pragmatic General Multicast
  - Microsoft VBScript
  - Microsoft Windows
  - Microsoft Windows Media
    - Удаленное выполнение кода в Windows Media Player, связанное с DataObject
    - Удаленное выполнение кода, связанное с видеodeкодером WMV
    - Удаленное выполнение кода, связанное с обработкой мультимедиа
    - Удаленное выполнение кода, связанное с обработкой мультимедиа
  - Microsoft XML Core Services
    - 3.0
    - 6.0
      - Уязвимость в MSXML XSLT
        - Разглашение информации, связанное с MSXML
        - Уязвимость, связанная с URI сущности MSXML
  - Quartz.dll (DirectShow)
  - Remote Desktop Connection Client
    - Небезопасная загрузка библиотек в Remote Desktop
    - Повышение привилегий, связанное с обходом каталога
    - Удаленное выполнение кода, связанное с элементом управления ActiveX удаленных рабочих столов
    - Подмена данных узла сеансов удаленных рабочих столов
  - Windows Media Center
  - Windows Defender
  - Hardware Information
    - Информация о BIOS
    - Информация о CPU
    - Информация о жестких дисках
    - Информация о материнской плате
    - Информация о памяти
    - Информация о сетевых картах
  - Network Configuration
    - MAC-адрес сканируемого адаптера
    - Доступные сетевые подключения
    - Открытые порты по прослушиваемым адресам
    - Список открытых портов
  - Operating System
    - Список процессов

**Информация**

Серьезная уязвимость  
**Удаленное выполнение кода в Windows Media Player, связанное с DataObject**  
ID: 413741  
CVE: CVE-2015-1728  
fstec: BDU:2015-12135  
Дата публикации: 09.06.2015

**Краткое описание**  
Уязвимость позволяет злоумышленнику получить полный контроль над системой.

**Описание**  
Уязвимость, позволяющая удаленно выполнить код, существует в Windows Media Player и связана с обработкой специально сформированных DataObjects. Эксплуатация данной уязвимости позволяет злоумышленнику, действующему удаленно, получить полный контроль над системой; после чего он может устанавливать программы, просматривать, изменять или удалять данные, а также создавать новые учетные записи с полными правами пользователя. Пользователи, права которых в системе ограничены, менее подвержены данной уязвимости, чем пользователи, работающие с правами администратора. Для эксплуатации данной уязвимости пользователь должен открыть специально сформированный DataObject в Windows Media Player.

**Как исправить**  
Используйте рекомендации производителя:  
<http://technet.microsoft.com/security/bulletin/ms15-057>

**Ссылки**  
MS (15-057): <http://technet.microsoft.com/security/bulletin/ms15-057>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1728>

**CVSS**  
Базовая оценка: 9.3 (AV:N/AC:M/Au:N/C:I/C/A:C)  
Временная оценка: 6.9 (AV:N/AC:M/Au:N/C:I/C/A:C/E:U/RL:OF/RC:C)  
AV:N данная уязвимость может эксплуатироваться удаленно  
AC:M для эксплуатации уязвимости нужна дополнительная информация или нестандартная конфигурация уязвимого ПО  
Au:N для эксплуатации уязвимости проходить аутентификацию не требуется

The screenshot displays the Positive Technologies Audit interface. The top navigation bar includes icons for PenTest, Audit, Compliance, and Сводная/узлы. The main interface is divided into three panels: Навигатор (Navigator), Информация (Information), and another Information panel on the right.

**Навигатор (Navigator):** Shows a tree view of the scanned system. The selected node is "Cisco ASA" under IP "192.168.52.10". A red arrow points to the vulnerability "Выполнение произвольного кода" (Arbitrary code execution) with ID 186302 and CVE-2016-2108.

**Информация (Information) - Left Panel:** Displays details for the selected vulnerability:

- Серьезная уязвимость** (Critical vulnerability)
- Выполнение произвольного кода** (Arbitrary code execution)
- ID: 186302
- CVE: CVE-2016-2108
- Краткое описание** (Brief description): Уязвимость позволяет злоумышленнику выполнить произвольный код.
- Описание** (Description): Уязвимость в реализации ASN. 1 в OpenSSL позволяет злоумышленнику (недостаточное заполнение буфера и ошибку при работе с памятью).
- Как исправить** (How to fix): Используйте рекомендации производителя: <https://tools.cisco.com/security/center/content/CiscoSecurityAdvisories>
- Ссылки** (Links): <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2108>
- CVSS** (CVSS): Базовая оценка: **10** (AV:N/AC:L/Au:N/C:C/I:C/A:C)

**Информация (Information) - Right Panel:** Displays details for the selected vulnerability:

- Серьезная уязвимость** (Critical vulnerability)
- Уведомление безопасности usn-3061-1** (Security advisory usn-3061-1)
- ID: 1003455
- CVE: CVE-2016-6515
- Ubuntu: USN-3061-1
- Описание** (Description): Уведомление безопасности об уязвимостях openssl
- Как исправить** (How to fix): Проблема может быть решена обновлением операционной системы до следующих версий пакетов:  
Ubuntu 16.04 LTS:  
openssl-server - 1:7.2p2-4ubuntu2.1  
Ubuntu 14.04 LTS:  
openssl-server - 1:6.6p1-2ubuntu2.8  
Ubuntu 12.04 LTS:  
openssl-server - 1:5.9p1-5ubuntu1.10
- Ссылки** (Links):  
<http://www.ubuntu.com/usn/usn-3061-1/>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6210>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6515>
- CVSS** (CVSS): Базовая оценка: **7.8** (AV:N/AC:L/Au:N/C:N/I:N/A:C)  
AV:N данная уязвимость может эксплуатироваться удаленно  
AC:L для эксплуатации уязвимости не требуются особые условия  
Au:N для эксплуатации уязвимости проходить аутентификацию не требуется  
C:N эксплуатация уязвимости не затрагивает конфиденциальные данные системы  
I:N эксплуатация уязвимости не затрагивает целостность системы  
A:C при успешной эксплуатации злоумышленник может сделать систему полностью недоступной
- Критерии возникновения уязвимости** (Vulnerability occurrence criteria): Красным отмечены подтвержденные критерии.



- Более **150** встроенных стандартов
- Автоматическое определение соответствия применимым стандартам
- Поддержка высокоуровневых стандартов и требований регуляторов
  - 152-ФЗ «О персональных данных»
  - СТО БР ИББС
  - PCI DSS
  - ISO 27001/27002
  - Приказы ФСТЭК 17, 21, 31
- Контроль выполнения собственных корпоративных правил безопасности



Audit
Compliance
Сводная/узлы

**Навигатор**

Узел > Журнал

- all
- 192.168.52.150
- 192.168.52.232

**Стандарты**

- [421265] Службы терминалов: Не разрешать перенаправление дисков
- [421267] Службы терминалов: Запретить сохранение паролей
- [421268] Связь через Интернет: Отключение загрузки драйверов принтера по протоколу HTTP
- [421269] Связь через Интернет: Отключить веб-публикацию в списке задач для файлов и папок
- [421270] Связь через Интернет: Отключить загрузку из Интернета для мастеров веб-публикаций и заказа отпечатков
- [421271] Связь через Интернет: Отключить печать по протоколу HTTP
- [421272] Связь через Интернет: Отключить обновление информационных файлов «Помощника по поиску»
- [421273] Связь через Интернет: Отключить участие в программе улучшения поддержки пользователей Windows Messenger
- [421284] Дополнительные настройки безопасности: Отключить автозапуск
- [421294] Политики пользователя: Парольная защита заставки
- [421295] Политики пользователя: Применить указанную заставку
- [421298] MSS: (DisableIPSourceRouting IPv6) Уровень защиты исходной IP-маршрутизации (защита от подделки пакетов)
- [421715] Политика паролей: Минимальная длина пароля
- [421720] Политики блокировки учетной записи: Пороговое значение блокировки
- [421722] Журнал приложений: Максимальный размер журнала приложений
- [421726] Журнал безопасности: Максимальный размер журнала безопасности
- [421731] Системный журнал: Максимальный размер системного журнала
- [421736] Параметры безопасности (Сетевой доступ): Не разрешать перечисление учетных записей SAM анонимными пользо
- [421737] Параметры безопасности (Сетевой доступ): Не разрешать перечисление учетных записей SAM и общих ресурсов а
- [421741] Параметры безопасности (Учетные записи): Переименование учетной записи администратора
- [421742] Параметры безопасности (Учетные записи): Переименование учетной записи гостя
- [421755] Параметры безопасности (Контроллер домена): Требования цифровой подписи для LDAP-сервера
- [421763] Параметры безопасности (Интерактивный вход в систему): Не отображать последнее имя пользователя
- [421765] Параметры безопасности (Интерактивный вход в систему): Текст сообщения для пользователей при входе в систе
- [421766] Параметры безопасности (Интерактивный вход в систему): Заголовок сообщения для пользователей при входе в о
- [421767] Параметры безопасности (Интерактивный вход в систему): Количество предыдущих подключений к кэш (в случае
- [421768] Параметры безопасности (Интерактивный вход в систему): Заранее напоминать пользователям об истечении срока
- [421771] Параметры безопасности (Интерактивный вход в систему): Действия при извлечении смарт-карты
- [421772] Параметры безопасности (Клиент сети Microsoft): Использовать цифровую подпись (всегда)
- [421780] Параметры безопасности (Сетевой доступ): Разрешать применение разрешений "Для всех" к анонимным пользовате
- [421781] Параметры безопасности (Сетевой доступ): Разрешать анонимный доступ к именованным каналам
- [421788] Параметры безопасности (Сетевая безопасность): Принудительный выход из сеанса по истечении допустимых час
- [421789] Параметры безопасности (Сетевая безопасность): Уровень проверки подлинности LAN Manager
- [421791] Параметры безопасности (Сетевая безопасность): Минимальная безопасность сеанса для клиентов на базе NTLM SS
- [421792] Параметры безопасности (Сетевая безопасность): Минимальная безопасность сеанса для серверов на базе NTLM SS
- [421808] Параметры безопасности (MSS): (DisableIPSourceRouting) Уровень защиты исходной IP-маршрутизации (защита от п
- [421822] Параметры безопасности (MSS): Процент заполнения журнала событий безопасности, при достижении которого вы
- [421866] Права пользователей: Доступ к компьютеру из сети (SeNetworkLogonRight)
- [421868] Права пользователей: Добавление рабочих станций к домену (SeMachineAccountPrivilege)
- [421869] Права пользователей: Настройка квот памяти для процесса (SeIncreaseQuotaPrivilege)
- [421870] Права пользователей: Разрешить локальный вход в систему (SeInteractiveLogonRight)
- [421871] Права пользователей: Разрешить вход в систему через службу терминалов (SeRemoteInteractiveLogonRight)
- [421872] Права пользователей: Архивирование файлов и каталогов (SeBackupPrivilege)
- [421874] Права пользователей: Изменение системного времени (SeSystemTimePrivilege)
- [421880] Права пользователей: Отказ в доступе к компьютеру из сети (SeDenyNetworkLogonRight)
- [421881] Права пользователей: Отказ во входе в качестве пакетного задания (SeDenyBatchLogonRight)
- [421882] Права пользователей: Отказ во входе в качестве службы (SeDenyBatchLogonRight)
- [421883] Права пользователей: Отключить локальный вход (SeDenyInteractiveLogonRight)
- [421886] Права пользователей: Принудительное удаленное завершение (SeRemoteShutdownPrivilege)
- [421887] Права пользователей: Создание журналов безопасности (SeAuditPrivilege)
- [421888] Права пользователей: Имитация клиента после проверки подлинности (SeImpersonatePrivilege)
- [421890] Права пользователей: Загрузка и выгрузка драйверов устройств (SeLoadDriverPrivilege)
- [421900] Права пользователей: Замена маркера уровня процесса (SeAssignPrimaryTokenPrivilege)

**Информация**

Не соответствует

**Параметры безопасности (Сетевая безопасность): Уровень проверки подлинности LAN Manager**

ID: 421789

**Краткое описание**

Рекомендуется использовать максимально допустимый для сети предприятия уровень проверки подлинности LAN Manager.

**Полное описание**

Когда один компьютер пытается установить соединение с другим компьютером и пройти проверку подлинности, он обычно отправляет базовый хэш LAN Manager и более безопасный NTLM-хэш. Раскрываемый параметр позволяет более тонко настроить поведение компьютера, проходящего аутентификацию. Возможны следующие варианты значений параметра:

- "Отправлять LM и NTLM ответы" (Send LM & NTLM responses)
- "Отправлять LM и NTLM - использовать сеансовую безопасность NTLMv2 при согласовании" (Send LM & NTLM - Use NTLMv2 session security if negotiated)
- "Отправлять только NTLM ответ" (Send NTLM response only)
- "Отправлять только NTLMv2 ответ" (Send NTLMv2 response only)
- "Отправлять только NTLMv2 ответ, отказывать LM" (Send NTLMv2 response only/refuse LM)
- "Отправлять только NTLMv2 ответ, отказывать LM и NTLM" (Send NTLMv2 response only/refuse LM & NTLM)

Стандартная (и самая слабая в отношении безопасности) опция - "Отправлять LM и NTLM ответы" (send LM & NTLM responses). Использование NTLM становится неэффективным, поскольку данные отправляются параллельно по обоим протоколам. Чтобы обеспечить более высокий уровень защищенности сетевой проверки подлинности, необходимо настроить уровень проверки подлинности LAN Manager как "Отправлять только NTLMv2 ответ, отказывать LM и NTLM" (Send NTLMv2 response only).

Выбор такого значения опции может негативно сказаться на возможности обмена данными с другими компьютерами Windows, если только это изменение не применено в масштабе всей сети. Если пройти проверку с использованием указанного уровня проверки подлинности LM не удастся, следует вернуться к уровню "Отправлять LM и NTLM - использовать сеансовую безопасность" (Send LM & NTLM - Use NTLMv2 session security if negotiated) и снова попытаться пройти сетевую проверку подлинности. Рекомендуется использовать уровень проверки подлинности LAN Manager "Отправлять только NTLMv2 ответ, отказывать LM" (Send NTLMv2, refuse LM). Для систем с повышенными требованиями к безопасности рекомендуемый уровень - "Отправлять только NTLMv2 ответ, отказывать LM и NTLM" (Send NTLMv2, refuse LM and NTLM). В целях совместности используйте уровень "Отправлять только NTLMv2 ответ" (Send NTLMv2).

Для профилей настольных и переносных компьютеров Enterprise в системах Windows 7 рекомендуемое значение - "Отправлять только NTLMv2-ответ. Отказывать LM" (Send NTLMv2 response only, Refuse LM). Для профилей настольных и переносных компьютеров SSUF рекомендуемое значение - "Отправлять только NTLMv2-ответ. Отказывать LM и NTLM" (Send NTLMv2 response only, Refuse LM & NTLM).

**Результаты проверки**

Требование	Текущее значение
5	1

**Настройки требования**

Имя	Значение по умолчанию	Пользовательское значение
Network security: LAN Manager authentication level	5	5

**Как исправить**

Чтобы настроить уровень проверки подлинности LAN Manager, откройте Редактор групповых политик (Group Policy Editor) и выберите "Конфигурация компьютера" (Computer Configuration) - "Конфигурация Windows" (Windows Settings) - "Параметры безопасности" (Security Settings) - "Локальные политики" (Local Policies) - "Параметры безопасности" (Security Options), для внесения изменений дважды щелкните мышью на позиции "Сетевая безопасность: Уровень проверки подлинности LAN Manager" (Network security: LAN Manager authentication level), установите нужное значение в появившемся окне и нажмите "ОК". Изменения вступят в силу после применения групповой политики.

The screenshot displays the Compliance module of the Positive Technologies software. The interface is divided into three main sections: a navigation pane on the left, a central list of standards, and an information pane on the right.

**Навигатор (Navigation):** Shows a tree view with 'Узел Журнал' and 'all' under the IP addresses 192.168.52.150 and 192.168.52.232.

**Стандарты (Standards):** A list of 30 security standards for CIS — Microsoft Windows 2012 R2, each with a green plus icon indicating compliance. The standards include:

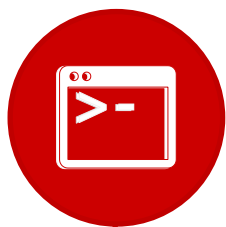
- [420214] Удаленный вызов процедур (RPC): Проверка RPC-клиентов сопоставителя конечных точек
- [421136] Права пользователей: Доступ к диспетчеру учетных данных от имени доверенного вызывающего
- [421200] Аудит: Принудительно переопределяет параметры категории политики аудита параметрами подкатегории полити
- [421219] Журнал приложений: Сохранять старые события
- [421220] Журнал безопасности: Сохранять старые события
- [421221] Системный журнал: Сохранять старые события
- [421240] Обновления Windows: Не отображать параметр "Установить обновления и завершить работу" в диалоговом окне "З
- [421241] Обновления Windows: Не выполнять автоматическую перезагрузку при автоматической установке обновлений, есл
- [421246] Контроль учетных записей: Обнаружение установки приложений и запрос на повышение прав
- [421247] Контроль учетных записей: Повышать права для UIAccess-приложений только при установке в безопасных местах
- [421248] Контроль учетных записей: Все администраторы работают в режиме одобрения администратором
- [421249] Контроль учетных записей: Переключение к безопасному рабочему столу при выполнении запроса на повышение пр
- [421250] Контроль учетных записей: При сбоях записи в файл или реестр виртуализация в размещении пользователя
- [421251] Контроль учетных записей: Разрешить UIAccess-приложениям запрашивать повышение прав, не используя безопас
- [421252] Права пользователей: Изменение метки объекта
- [421254] Права пользователей: Создание символических ссылок
- [421257] MSS: Отключить автоматический вход в систему
- [421260] Сетевая безопасность: Разрешить LocalSystem использовать нулевые сеансы
- [421262] Сетевая безопасность: разрешить использование сетевых удостоверений в запросах проверки подлинности PKU2U
- [421282] Дополнительные настройки безопасности: Предложение удаленной помощи
- [421283] Дополнительные настройки безопасности: Запрос удаленной помощи
- [421296] Политики пользователя: Таймаут экранной заставки
- [421297] Политики пользователя: Включить заставку
- [421713] Политика паролей: Минимальный срок действия пароля
- [421714] Политика паролей: Максимальный срок действия пароля
- [421716] Политика паролей: Настроить сложность пароля
- [421717] Политика паролей: История паролей
- [421718] Политика паролей: Хранение паролей с использованием обратимого шифрования
- [421719] Политики блокировки учетной записи: Период блокировки
- [421721] Политики блокировки учетной записи: Сброс счетчика блокировки через
- [421735] Параметры безопасности (Сетевой доступ): Разрешить трансляцию анонимного SID в имя

**Информация (Information):** A summary report for CIS — Microsoft Windows 2012 R2, version 1.1.0, for host 192.168.52.150 / DC\_01 / DC\_01.lab.local. It includes a 3D pie chart showing compliance status:

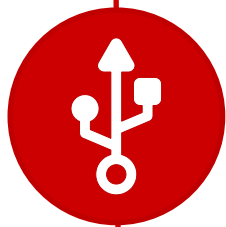
Статус	Процент
Соответствует (Green)	48.10%
Не соответствует (Red)	48.52%
Неприменимо (Blue)	3.38%

**Параметры сканирования (Scan Parameters):**

Начало сканирования:	02.03.2017 20:59:44
Завершение сканирования:	02.03.2017 21:35:23
Профиль:	[Demo][AC] Windows
Сканер:	MP-SCN-01
Версия сканера:	25067



**Контроль  
установленного ПО**



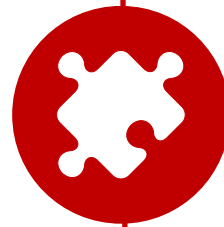
**Контроль подключенных  
USB-устройств**



**Контроль  
сетевых настроек**



**Контроль  
парольной политики**



**Контроль  
целостности**



**Контроль  
средств защиты**

## Дифференциальные отчеты – уведомление об изменениях в инфраструктуре:

1

Смена  
пароля

192.168.1.4  
IP: 192.168.1.4 FQDN: NetBIOS:  
OS: Cisco IOS: 12.3(4)T2

Список учетных записей

MaxPatrol

Алгоритм шифрования пароля	secret 5 → password 0
Пароль	\$1\$B/V1\$<removed>g. → e<removed>d
Уровень привилегий	1 (значение по умолчанию)
Дополнительные атрибуты	

2

Модификация  
списков контроля  
доступа

Списки доступа

101

Тип	extended
Интерфейсы (линии)	не задан(а)
Правила фильтрации	10 permit ip 192.168.200.0 0.0.0.255 192.168.201.0 0.0.0.255 → 10 permit ip 192.168.200.0 0.0.0.255 host 192.168.201.1 20 permit tcp any 10.0.0.0 0.255.255.255

3

Изменение  
контрольных  
сумм файлов

1

Хранилище	nvrn:
Имя файла	startup-config
Размер файла	11060 → 10883
Контрольная сумма	380809eb05eac69a3cea21be67bb7cb2 → a5f03bb24e8c6b2b196c99325585207f







1

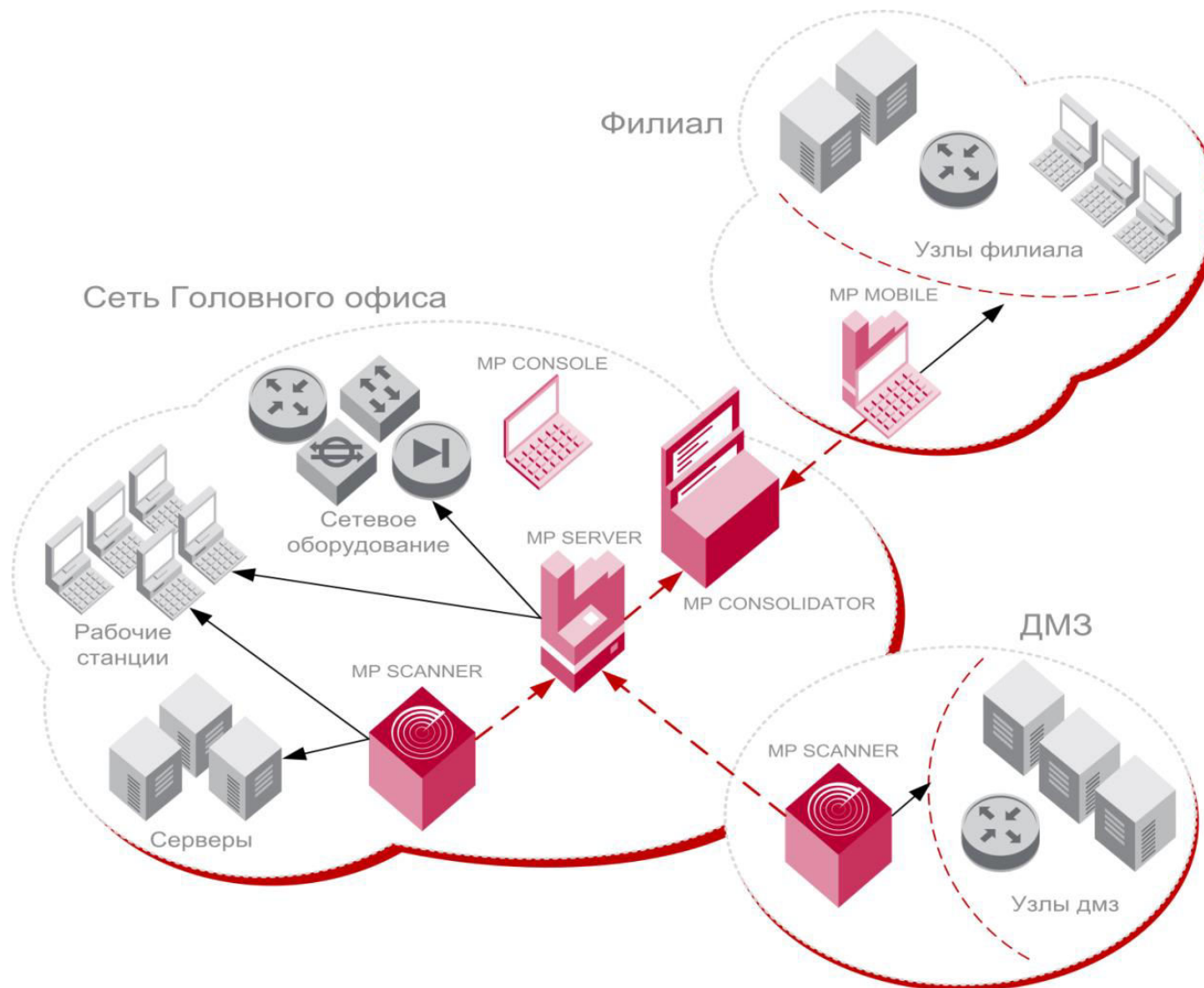
Хранилище	system:
Имя файла	running-config
Размер файла	11060 → 10883
Контрольная сумма	380809eb05eac69a3cea21be67bb7cb2 → a5f03bb24e8c6b2b196c99325585207f

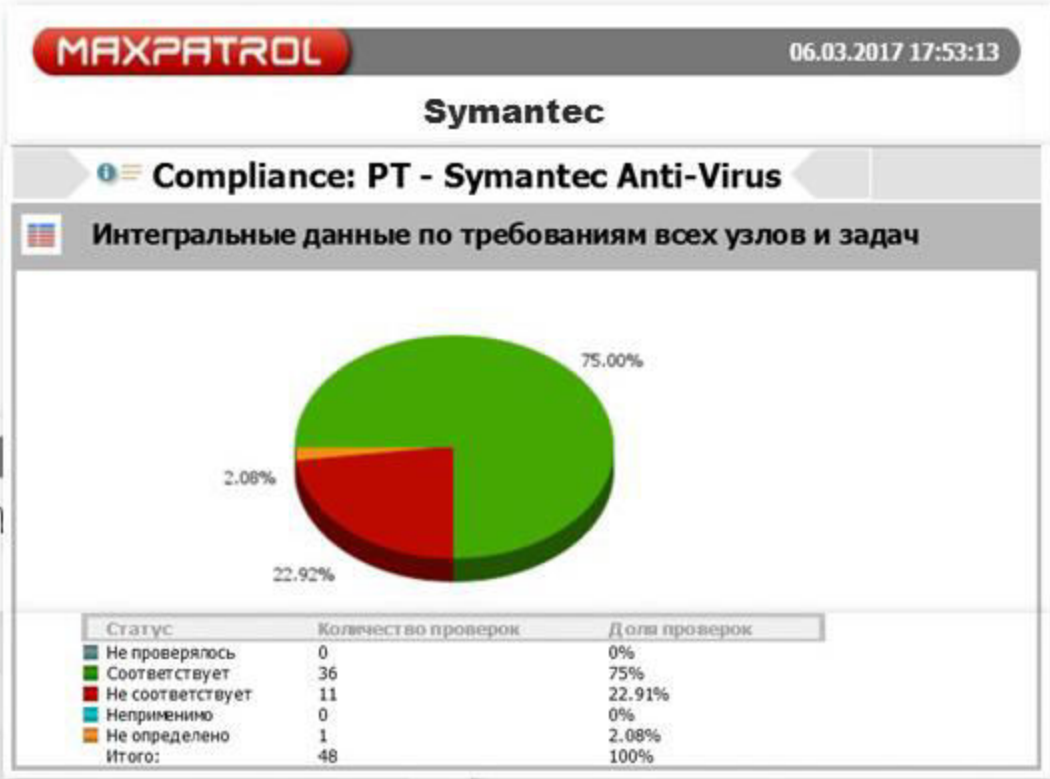
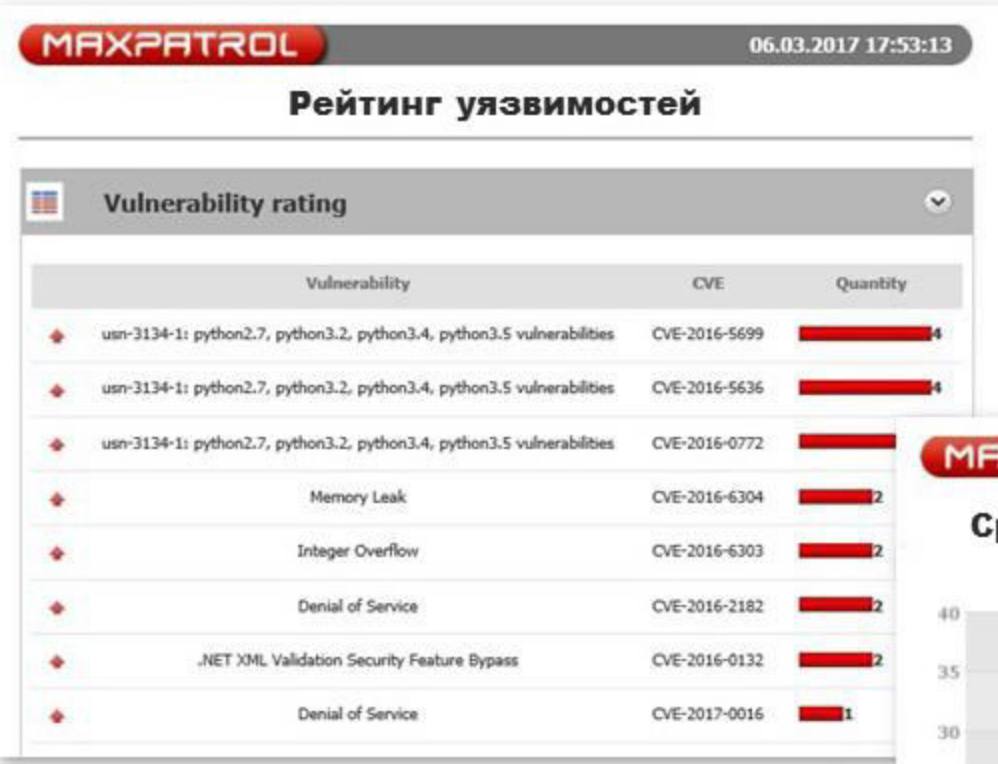
- Управление активами
- Help Desk системы
- Управление рисками
- Управление установкой исправлений
- SIM/SIEM
- IDM



## КОМПОНЕНТЫ

-  **MP Server**
-  **MP Scanner**
-  **MP Consolidator**
-  **MP Console**
-  **MP Mobile Server**
-  **MP Local Update Server**



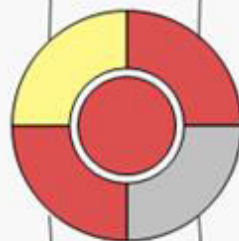




## Показатели информационной безопасности инфраструктуры за Q3

### Контроль защищенности

Обнаружено High уязвимостей	● 29,3%
Обнаружено Medium уязвимостей	● 41,7%
Количество уязвимостей больше, чем в Q2, на	● -
Количество узлов с High уязвимостями	● 49,3%
Количество узлов с Medium уязвимостями	● 26,6%
Количество уязвимых узлов выросло с Q2 на	● -



### Контроль эффективности ИБ

Устранено уязвимостей	● -
План сканирования узлов выполнен на	● 29,3%
Количество просканированных узлов выросло с Q2 на	↓ -38,4%
Заданная регулярность сканирования узлов соблюдена на	● 50,4%
План ввода в эксплуатацию компонентов МР выполнен на	● 23,4%
Работоспособность компонентов МР за период	—

### Управление активами

Количество узлов с запрещенным ПО	● 3,7%
Количество узлов с обязательным ПО	● 16,7%
Соблюдение лицензионной политики	—
Использование запрещенного оборудования	—

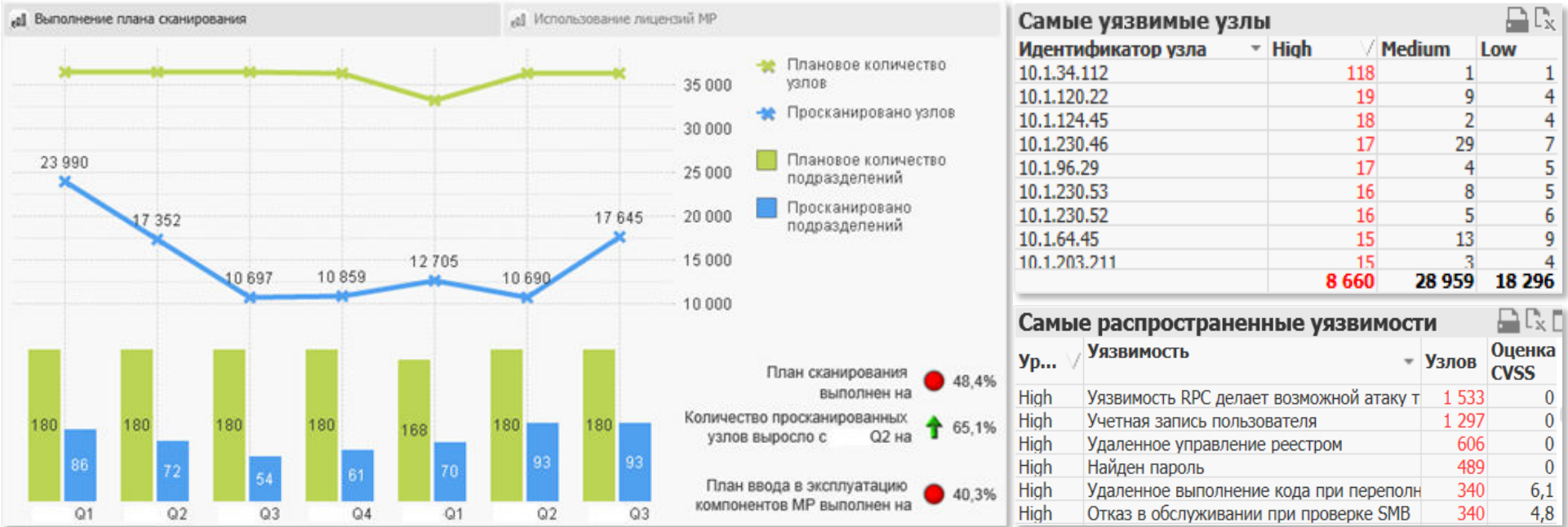
### Соответствие стандартам

### Подразделение

- ⊖ Управление по Архангельской области
- Управление по Архангельской области
- Подразделение № 31
- Подразделение № 1
- Подразделение № 7
- ⊕ Управление по Астраханской области
- ⊕ Управление по Брянской области
- ⊕ Управление по г.Москве
- ⊕ Управление по г.Санкт-Петербургу

### Статус





### Обнаруженные уязвимости

ID	Уязвимость	Оценка CVSS	Подраз	Узлы	Распространение	Идентификатор уязвимости
412022	High	Уязвимость RPC делает возможной атаку типа "отказ в обслуживании"	(+2) ↑	72	1533 (+561)	CVE-2007-2228
1205	High	Учетная запись пользователя	(+8) ↑	59	1297 (+1 166)	-
6015	High	Найдены учётные записи	8,7 (-1) ↓	49	293 (+120)	-
1066	High	Удаленное управление реестром	(+1) ↑	66	606 (+332)	-
412205	High	Удаленное выполнение кода при переполнении SMB-буфера	6,1	48	340 (+59)	CVE-2008-4834

Применение MaxPatrol 8 позволяет выполнить ряд **требований регуляторов**:

- **Приказ ФСТЭК №17 от 11.02.2013г.**  
«Об утверждении требований о защите информации, не составляющей государственную тайну»
- **Приказ ФСТЭК №21 от 18.02.2013г.**  
«Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»
- **Приказ ФСТЭК №31 от 14.03.2014г.**  
«Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а так же объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды»

Применение MaxPatrol 8 позволяет выполнить ряд **требований регуляторов**:

- **РС БР ИББС – 2.6-2014.**

«Рекомендации в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации.

Обеспечение информационной безопасности на стадиях жизненного цикла автоматизированных банковских систем»

- **Payment Card Industry Data Security Standard (PCI DSS v3.2).**

«Требования и процедуры аудита безопасности»

- **ISO/IEC 27001/27002.**

«Системы менеджмента информационной безопасности», «Свод рекомендуемых правил для управления информационной безопасностью»



Автоматизация  
поиска и устранения  
уязвимостей



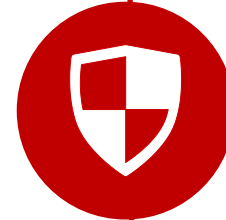
Стандарты  
ИБ для ИС  
и прикладного ПО



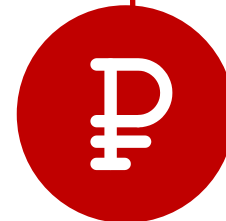
Оптимизация  
использования  
средств защиты



Регулярная оценка  
эффективности работы  
отделов ИТ и ИБ



Повышения уровня  
защищенности ИС



Сокращение  
финансовых  
затрат

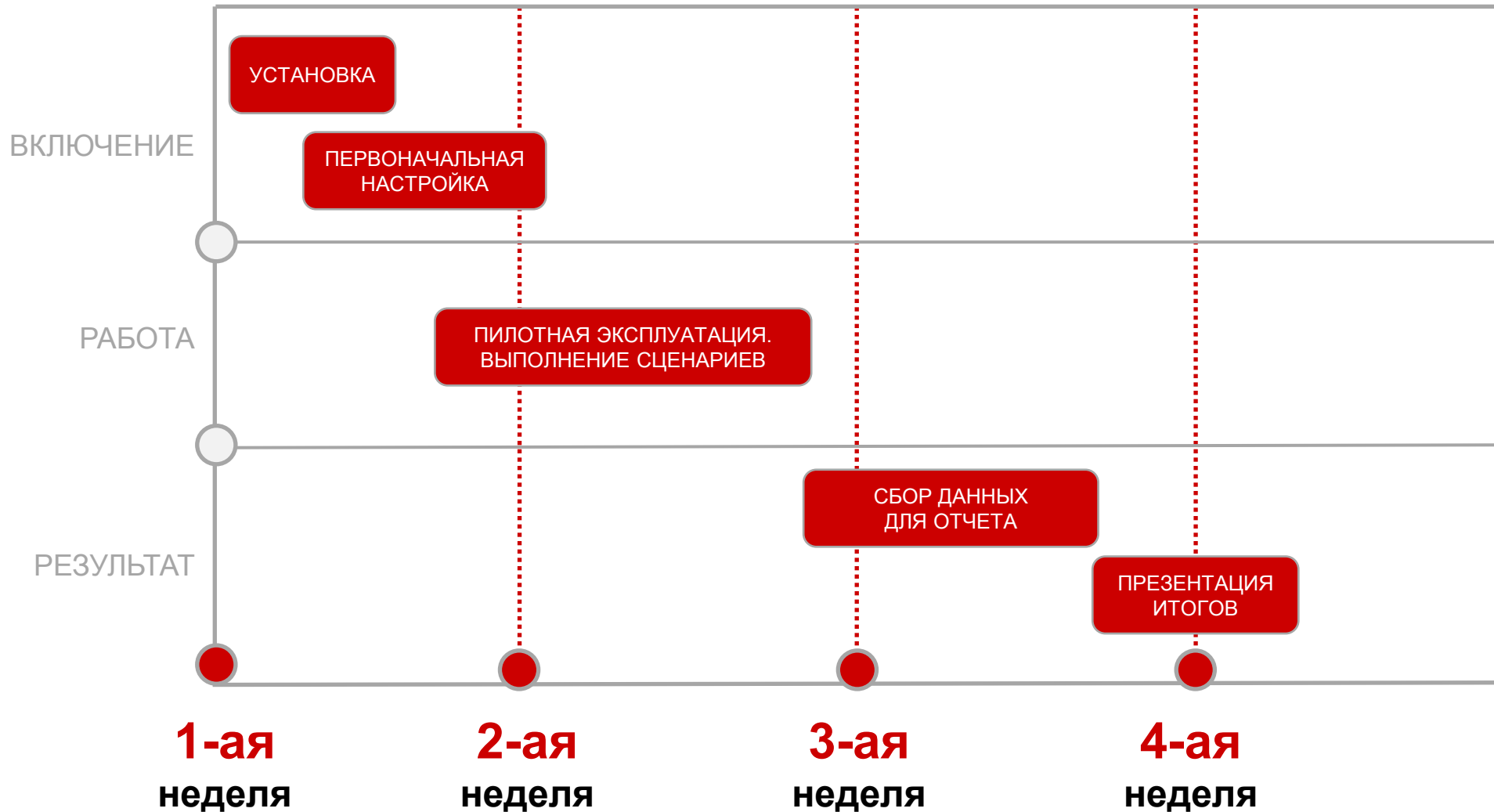
**MaxPatrol 8.**

---

Пилотный проект

- **Полностью** заполнена анкета
- Получено коммерческое и техническое одобрение от РТ
- Составлен план пилота
- Назначена дата начала проекта









Спасибо за внимание!

POSITIVE TECHNOLOGIES

[ptsecurity.ru](http://ptsecurity.ru)