Управление соответствием техническим стандартам с помощью MaxPatrol

Наталья Куканова
Positive Technologies
nkukanova@ptsecurity.ru

Цель рассказа

- **Как разработать грамотные технические стандарты для обеспечения ИБ?**
- **Как обеспечить контроль над их выполнением с помощью MaxPatrol?**
- **Как проанализировать результаты проверок и принять решения?**

Формирование технических стандартов

Зачем нужны технические стандарты?

Любые организационные и процессные меры обеспечения безопасности опираются на техническую реализацию.

Выполнение технических требований:

- **Защита корпоративной сети, снижение рисков ИБ**
- **Индикатор, насколько хорошо функционируют процессы ИБ**
- **Индикатор, выполнены ли требования регуляторов**

Как создать правильный технический стандарт? Миссия НЕ выполнима?

- **Инвентаризация ИТ-ресурсов**
- **Категоризация ИТ-ресурсов**
- **Анализ рисков ИБ**
  - определение угроз и уязвимостей
  - анализ существующих контрмер
- **Определение требований к ИБ и защитных мер**
- **Формирование технических стандартов**

Как создать правильный технический стандарт? Миссия выполнима!

- **Инвентаризация ИТ-ресурсов**
  - перечень узлов и технологических платформ
- **Ранжирование ИТ-ресурсов**
- **Выбор соответствующих лучших практик, анализ внутренних регламентов**
- **Формирование технических стандартов**

Ранжирование ИТ-ресурсов

- **По ценности для Компании:**
  - Mission Critical (Высокий)
  - Business Critical (Средний)
  - Operational (Низкий)

- **По инфраструктурным функциям:**
  - Ключевые инфраструктурные объекты (корневые маршрутизаторы и пр.)
  - Серверы
  - Рабочие станции

Best practice.
Опыт ~~поколений~~ Positive Technologies

- **CIS (Center for Internet Security, http://www.cisecurity.org/)**
- **STIGs (Defense information systems agency, http://disa.mil) – 2012 год**
- **PT (Исследовательский центр Positive Technologies, https://ptsecurity.ru)**

Приоритезация требований

Важные требования необходимо контролировать и соблюдать более тщательно.

Методы приоритезации требований:

- **Оценка экспертов**
- **CVSS (Common Vulnerability Scoring System, http://www.first.org/cvss)**

Кастомизация требований

Перечень требований и проверяемые значения зависят от конфигурации ИС, применяемой политики ИБ, взаимосвязей между системами, бизнес-процессов, построенных в компании.

Параметры, требущие изменения в зависимости от объекта применения:

- **Перечень требований стандарта**
- **Значения требований**
- **Тексты требований**

Структура технических стандартов

- **Ранжированные ИТ-ресурсы**
  - **Технологические платформы (ОС, СУБД, прикладное ПО, сетевые устройства)**
    - **Технические стандарты**
      - **Важные и второстепенные требования**

Реализация контроля над соответствием стандартам с помощью MaxPatrol

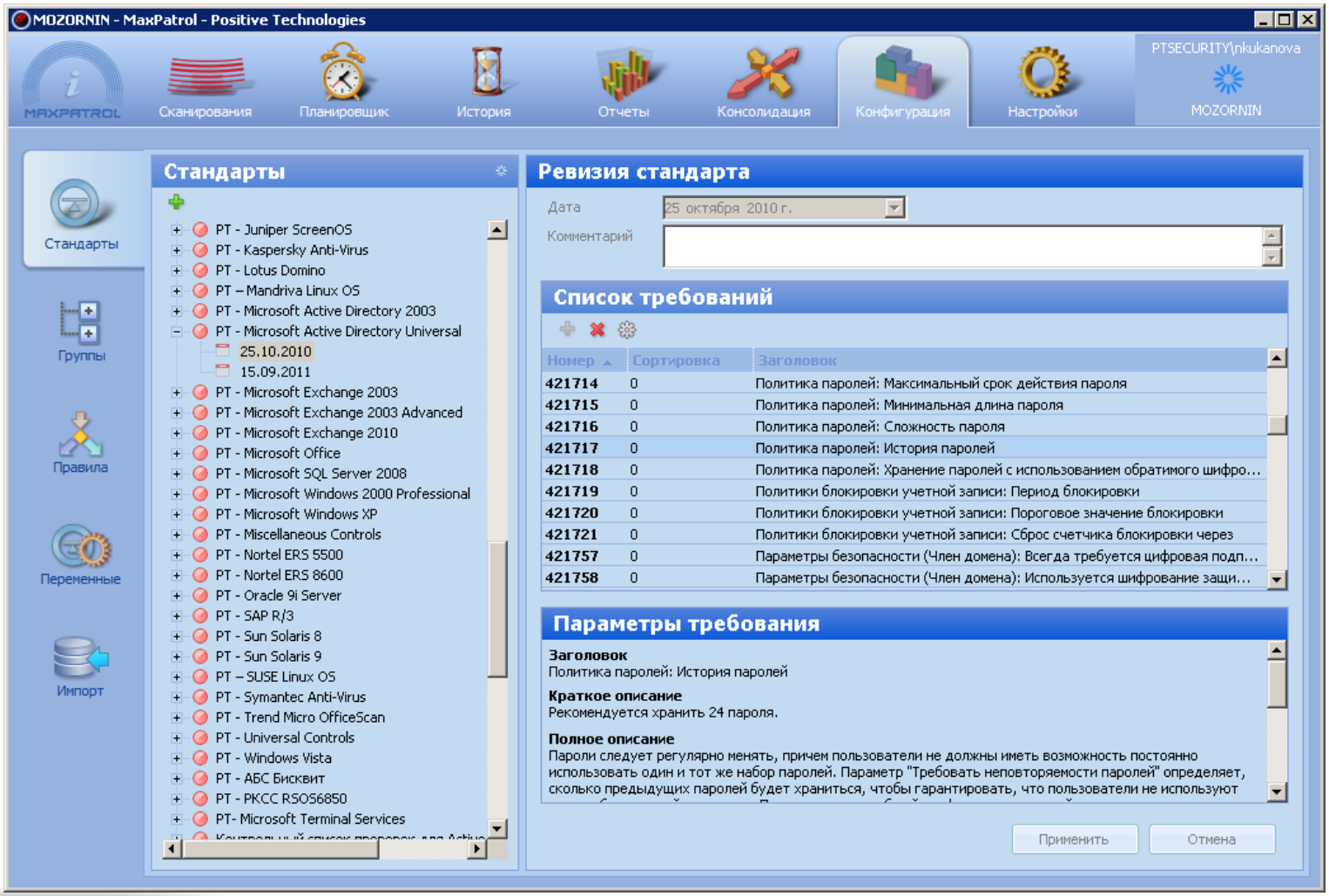
Что уже сделано?

- **Перечни узлов и тех.платформ, которые необходимо проверять, с учетом их ранжирования**
- **Стандарты для тех.платформ с учетом их критичности**
- **Перечни, значения и тексты требований**

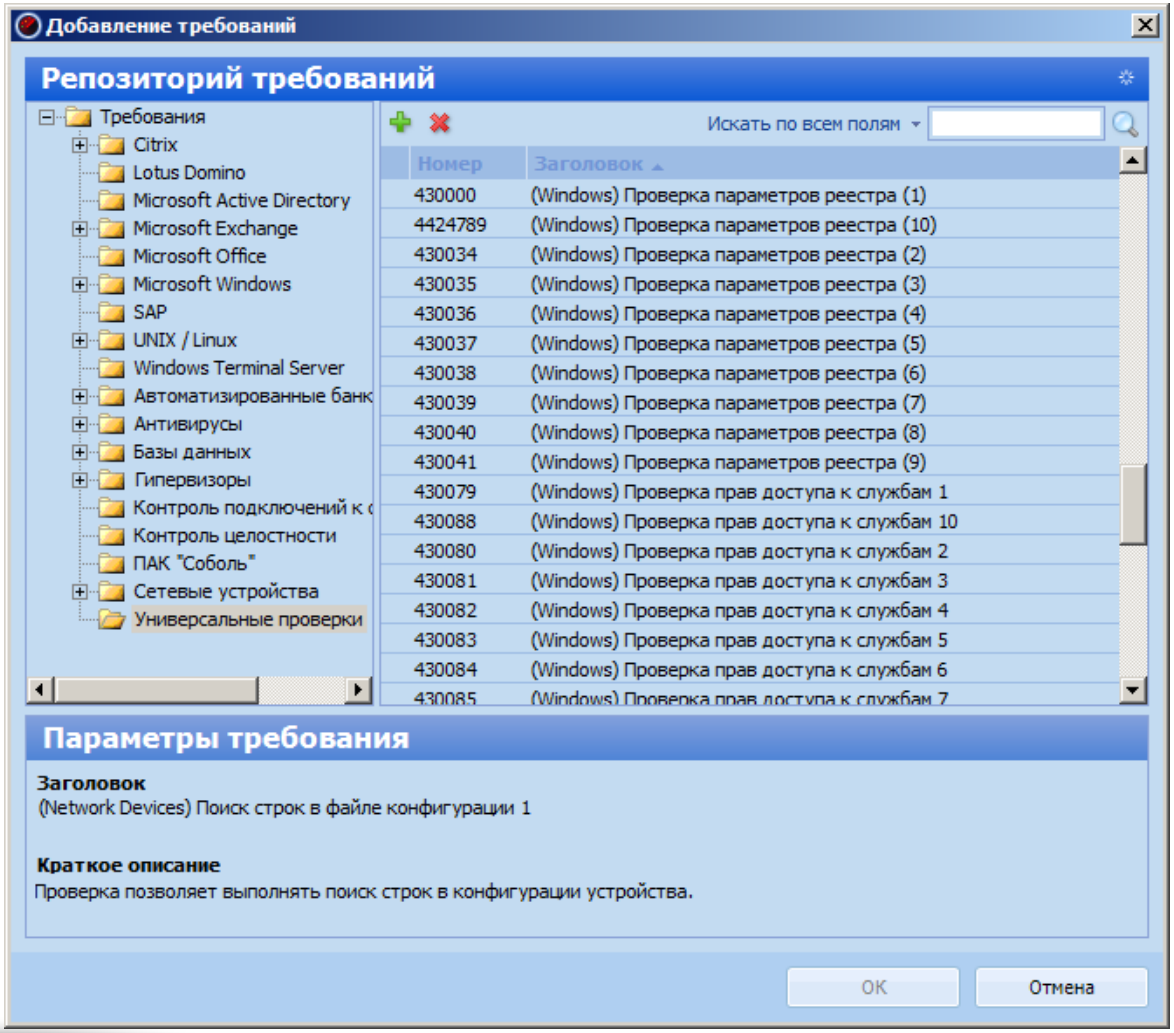
Что нужно сделать?

- **Выбрать перечень требований**
- **Изменить тексты требований и проверяемые значения**
- **Настроить режимы сканирования**
- **Настроить необходимые отчеты**
- **Настроить расписание формирования отчетов и доставку**

Создание технических стандартов. Выбор требований.



Создание технических стандартов. Выбор требований. Универсальные проверки.

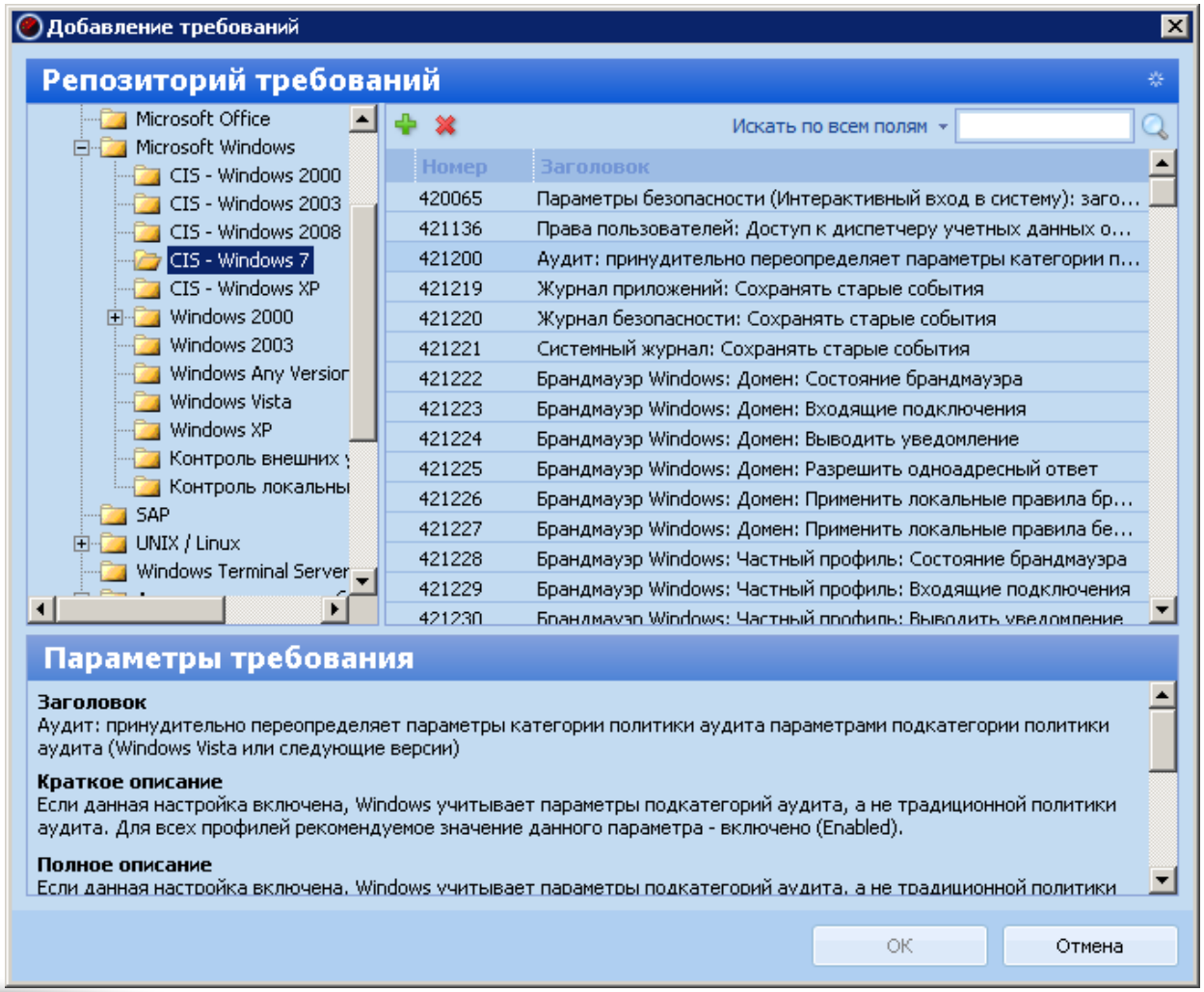


Создание технических стандартов. Применимость требований.

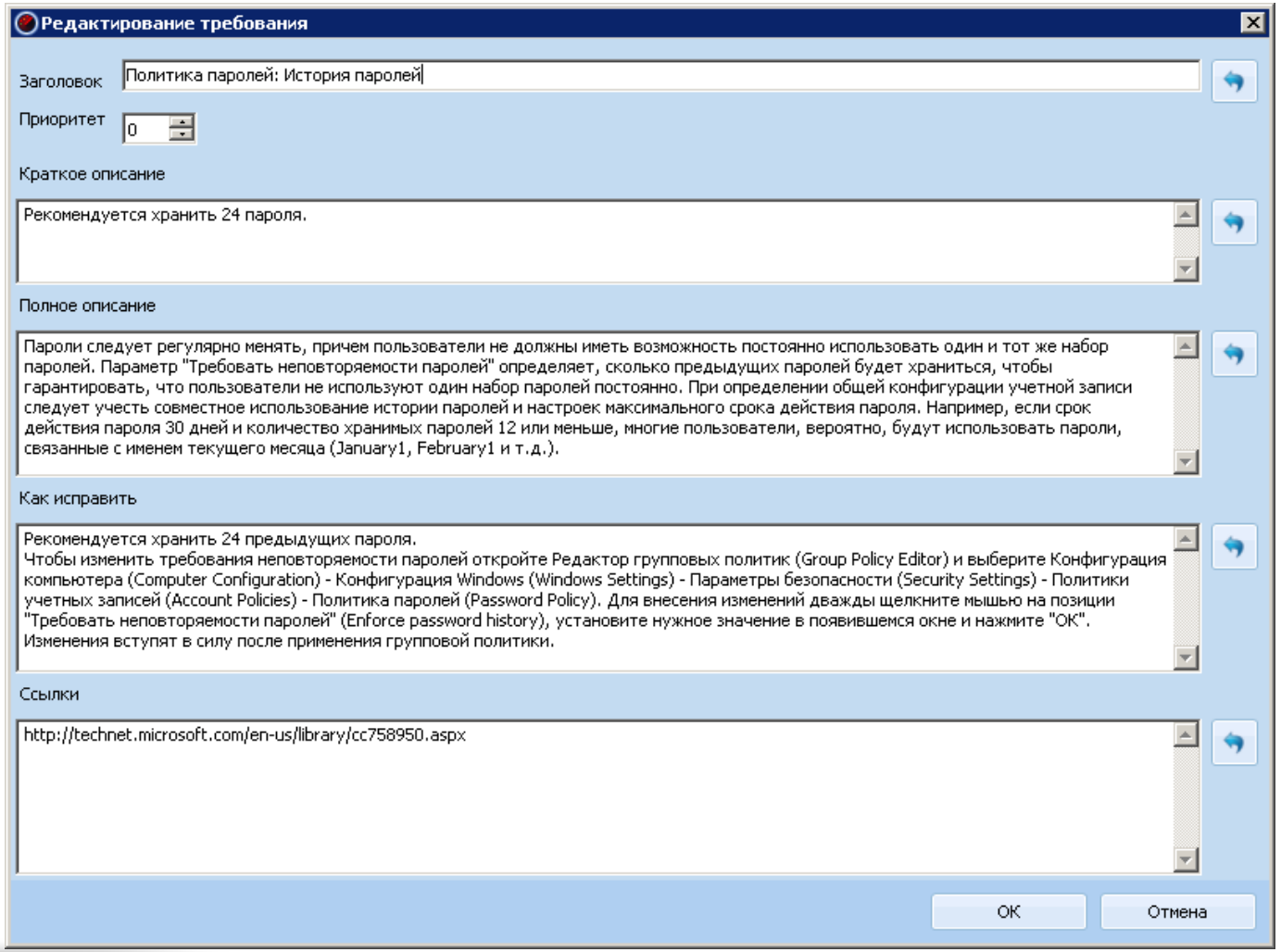
- **Требования стандартов применяются к соответствующим тех.платформам** (определение тех.платформы осуществляется MaxPatrol в режиме аудита)

- **Требования могут применяться ко всем платформам производителя** (например, все MS Windows) **или к конкретным версиям** (например, MS Windows 7)

Создание технических стандартов. Применимость требований.



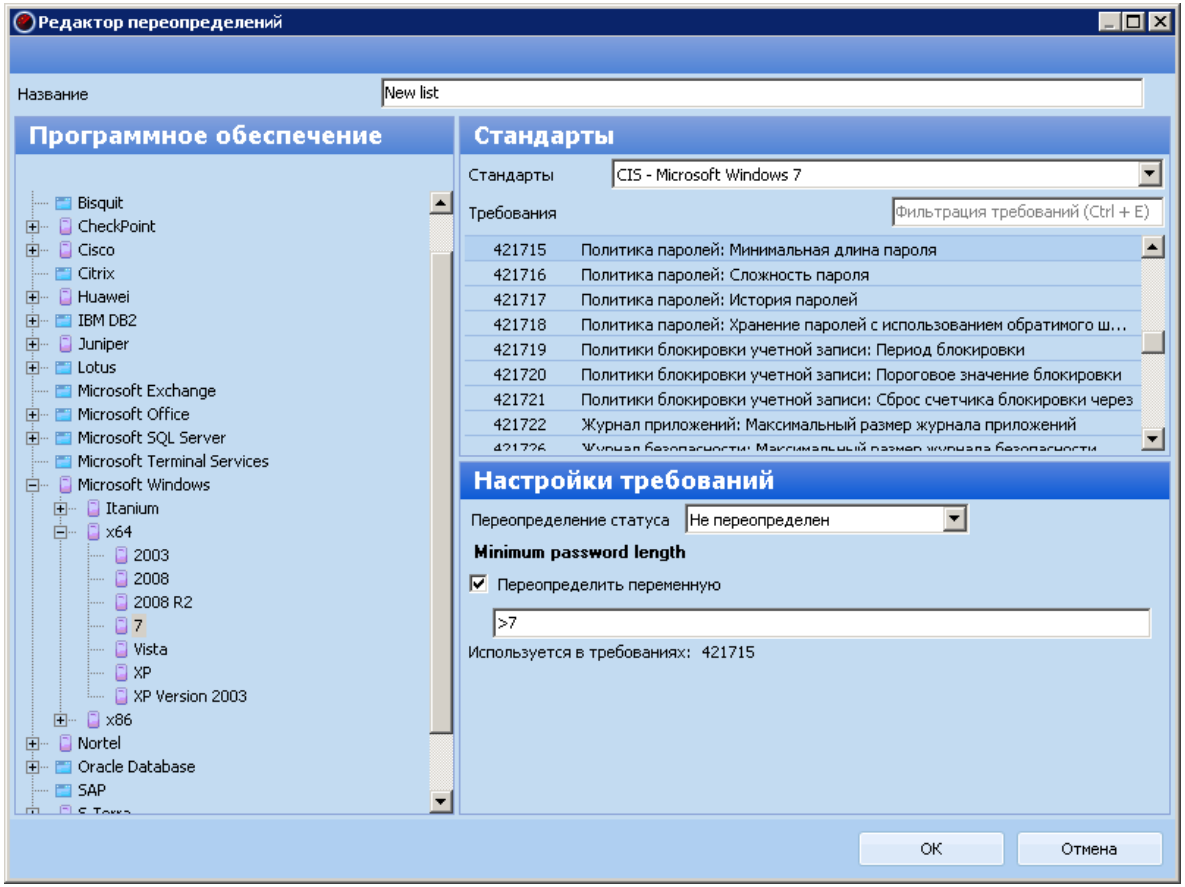
Создание технических стандартов. Изменение текстов требований.



Создание технических стандартов. Применимость значений требований.

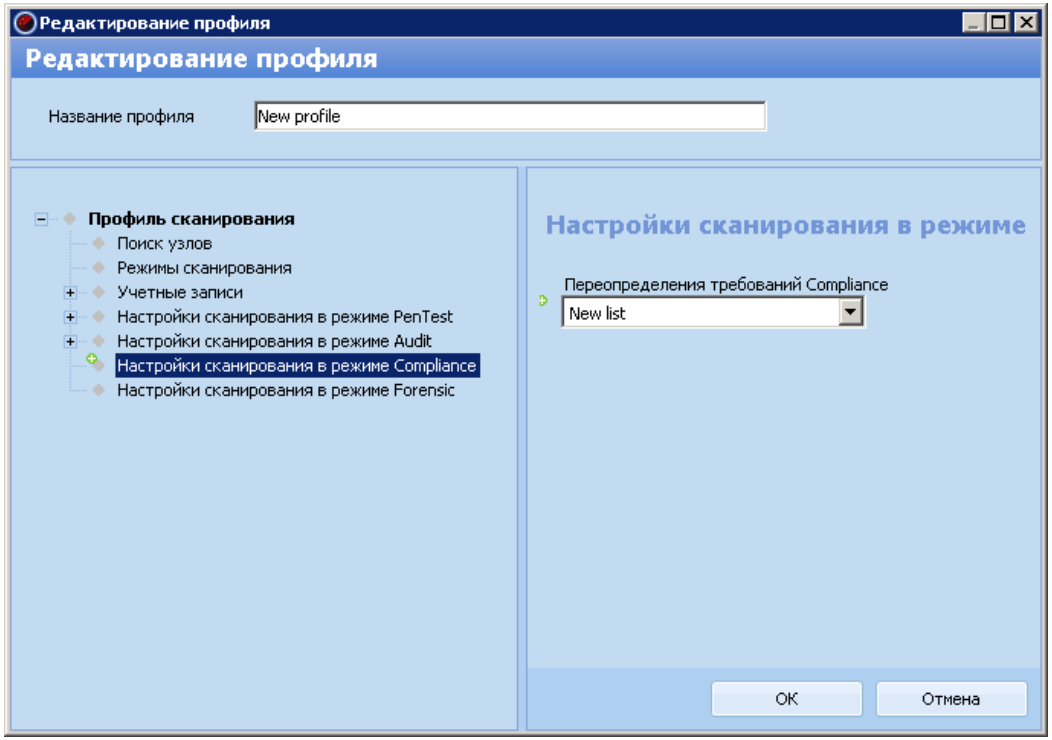
Новые значения требований могут применяться:

- **Ко всем платформам производителя (например, все MS Windows)**
- **К конкретным версиям (например, MS Windows 7)**



Формирование профилей и задач сканирования

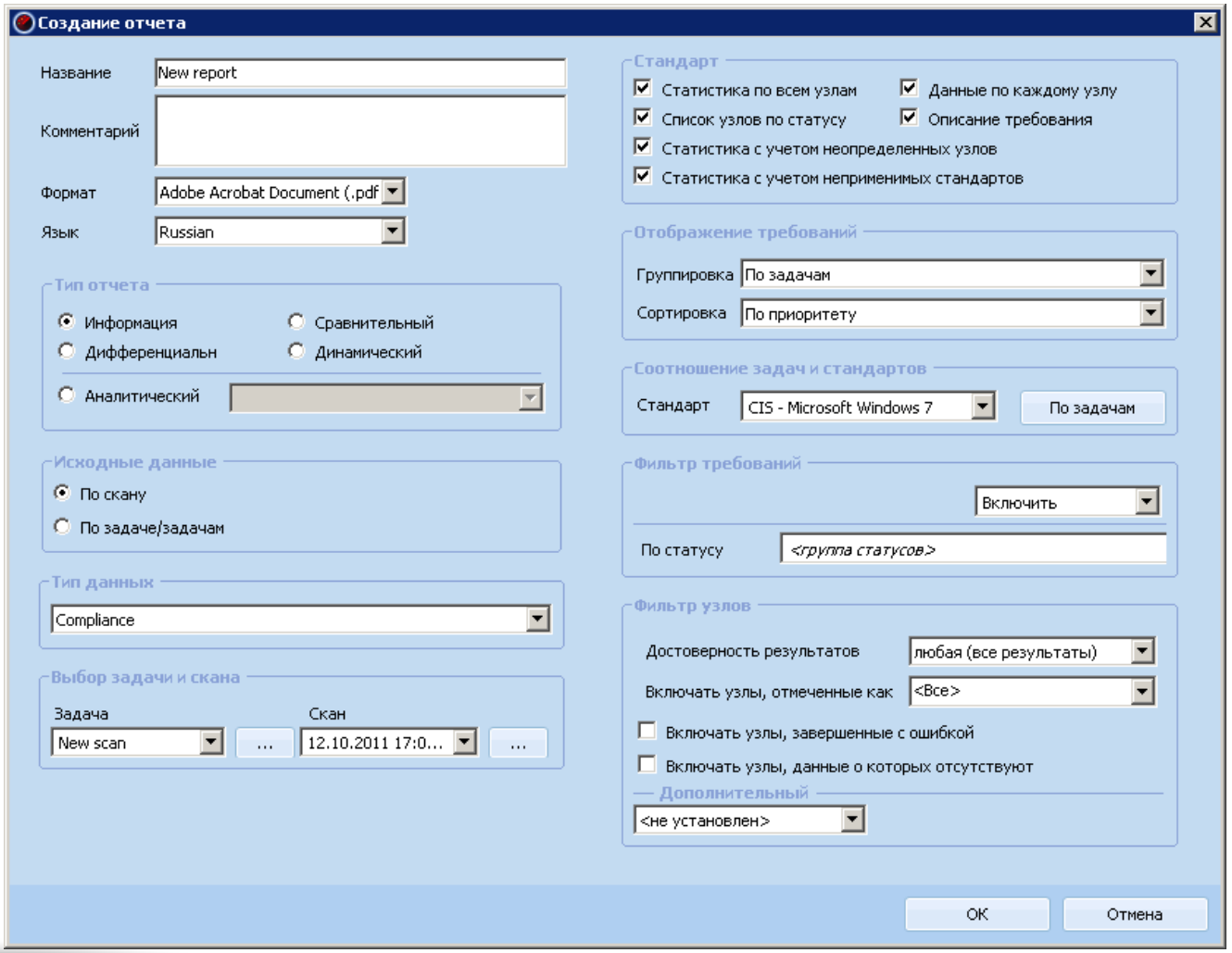
- **При формировании профилей сканирования необходимо указать, какие переопределения будут применены при сканировании объектов**



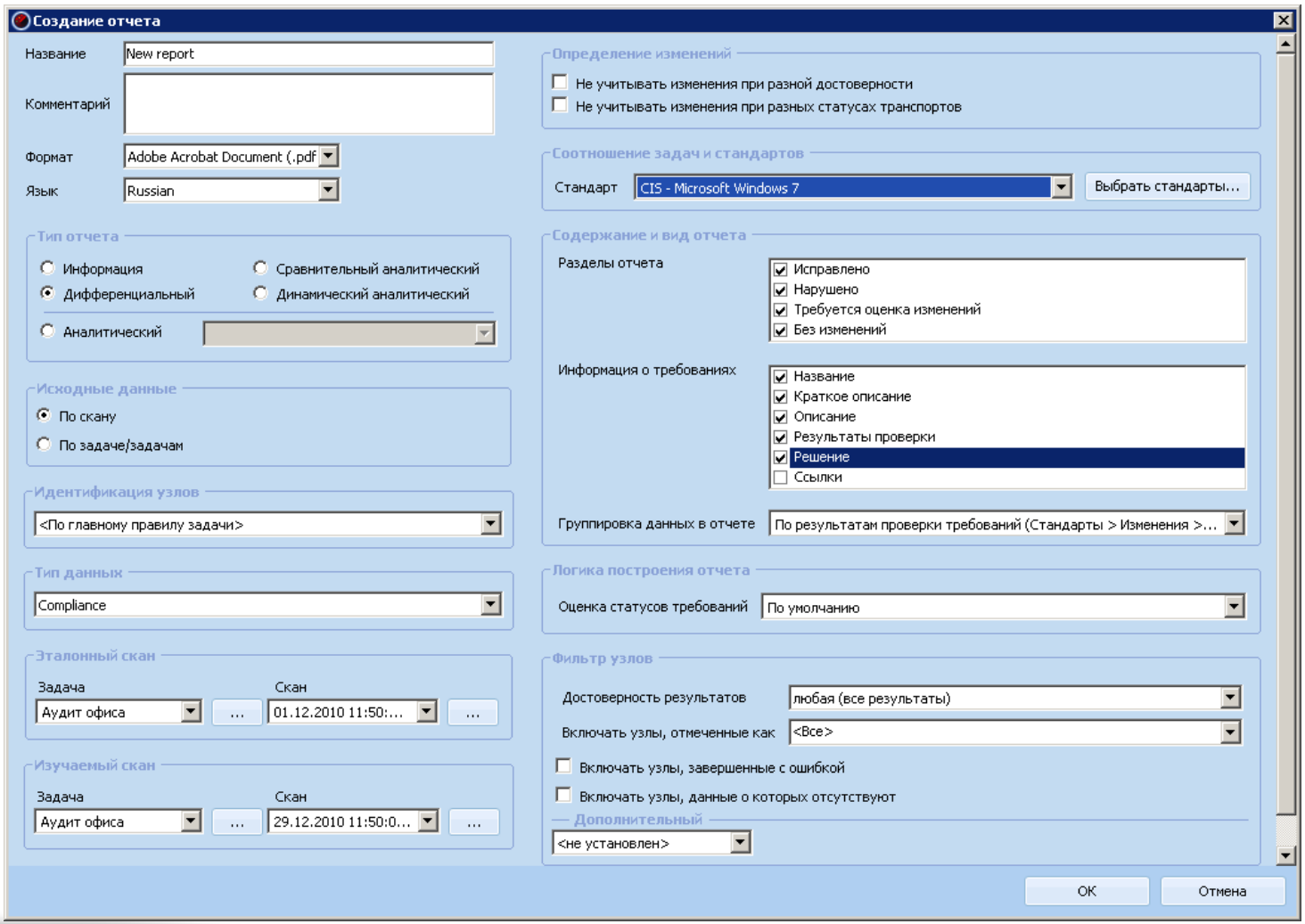
Формирование отчетов

- **Целевая аудитория отчетов:**
  - Менеджмент ИТ и ИБ
  - Специалисты ИБ (контроль)
  - Администраторы ИТ и ИБ (исполнение)
- **В зависимости от целевой аудитории могут меняться:**
  - Данные, представленные в отчете
    - Высокоуровневый отчет
    - Подробный отчет
  - Частота формирования отчета
  - Информационный и дифференциальный отчеты

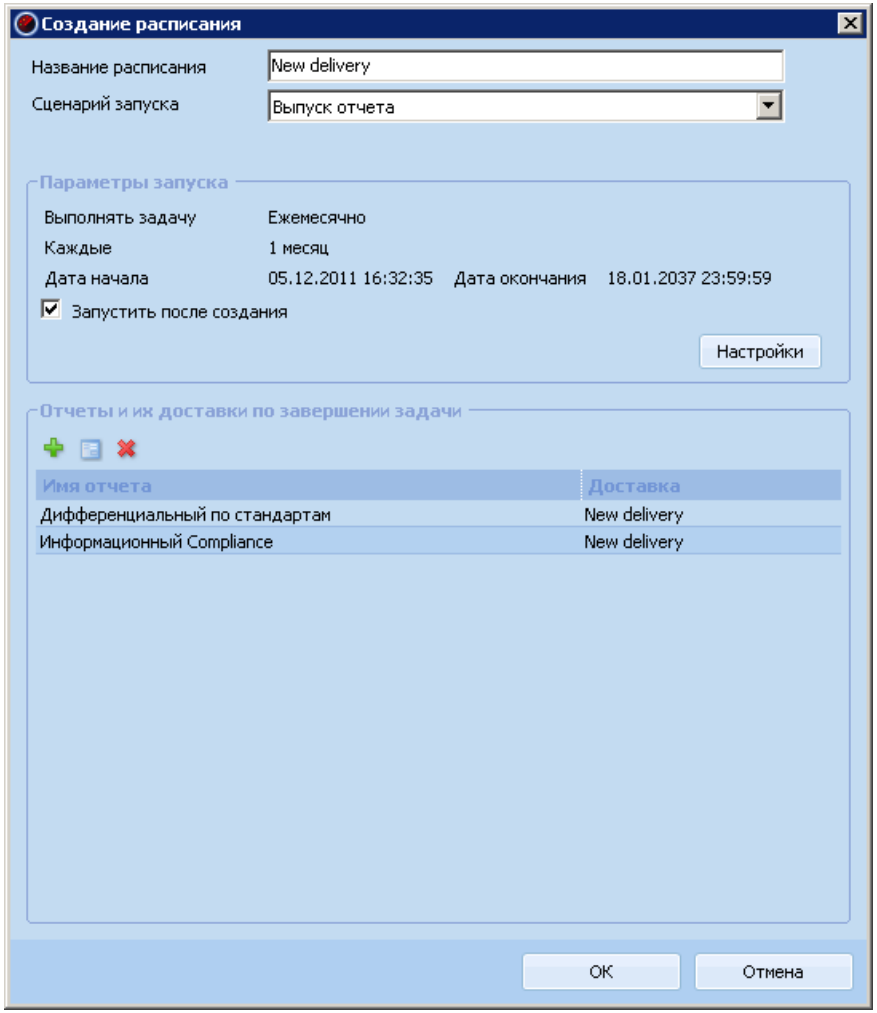
Формирование отчетов



Формирование отчетов. Дифференциальный отчет по стандартам



Формирование расписаний и доставки отчетов

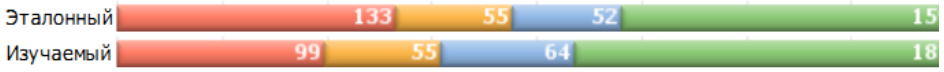


Пример отчета

10.111.114.9

Задача: AC_50_Nodes_Emulated
IP: 10.111.114.9 **FQDN:** **NetBIOS:**
OS: Operating System: Windows XP Pro Service Pack 2 → Operating System: Windows 7

Статистика по статусам требований



- Исправлено
  - Не соответствует → Соответствует

PT - Microsoft Office

Для Access 2003 для обработки макросов установлен Высок безопасности защиты от макросов

ID: 301528

Описание

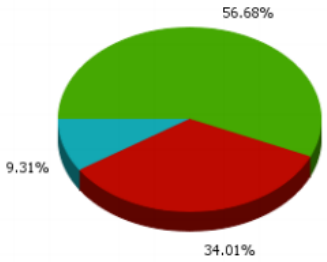
Для Access 2003 для обработки макросов установлен Высокий уровень безопасности защит макросов.

Результаты проверки

Access 2007: Default level (2)
Access 2003: Default level (2)

Access: Default level (3)

узел	задача	начало	конец	время
localhost	Audit+Compliance	24.06.2011 11:05:35	24.06.2011 11:10:56	00:05:21



Статус	Количество проверок	Доля проверок
Не проверялось	0	0%
Соответствует	140	56.68%
Не соответствует	84	34%
Неприменимо	23	9.31%
Не определено	0	0%
Итого:	247	100%

Другие системные требования: Включить брандмауэр для Интернет-подключений

ID: 421907

Краткое описание

Необходимость в использовании брандмауэра для Интернет-подключений (Internet Connection Firewall) определяется системным администратором.

Требование

Необходимость в использовании брандмауэра для Интернет-подключений (Internet Connection Firewall) определяется системным администратором.
Брандмауэр Windows доступен только когда система напрямую связана с Интернетом, и не имеет отношения к локальным (LAN) соединениям. Брандмауэр также доступен при работе с коммутируемым доступом и совместными интернет-подключениями.
При включении брандмауэр Windows блокирует входящий трафик, за исключением трафика, который проходит через порт, который явно открыт. Брандмауэр Windows обычно не требуется во внутренних сетях, т.к. в них брандмауэр уже существует между клиентом и внешней сетью. Брандмауэр Windows поддерживает аудит.

Результаты проверки

Настройки требования

Имя	Значение по умолчанию	Пользовательское значение
Windows Firewall Status	1	1

Требование	Текущее
1	0

Анализ результатов и принятие решений

Менеджмент ИТ и ИБ

- **Получает Отчеты о соответствии стандартам и Дифференциальные отчеты о соответствии стандартам (без технических подробностей)**
- **Анализирует, насколько конфигурация тех.платформ соответствует требованиям**
- **Дает указание администраторам ИТ и ИБ исправить ситуацию, специалистам ИБ – помочь и проконтролировать**

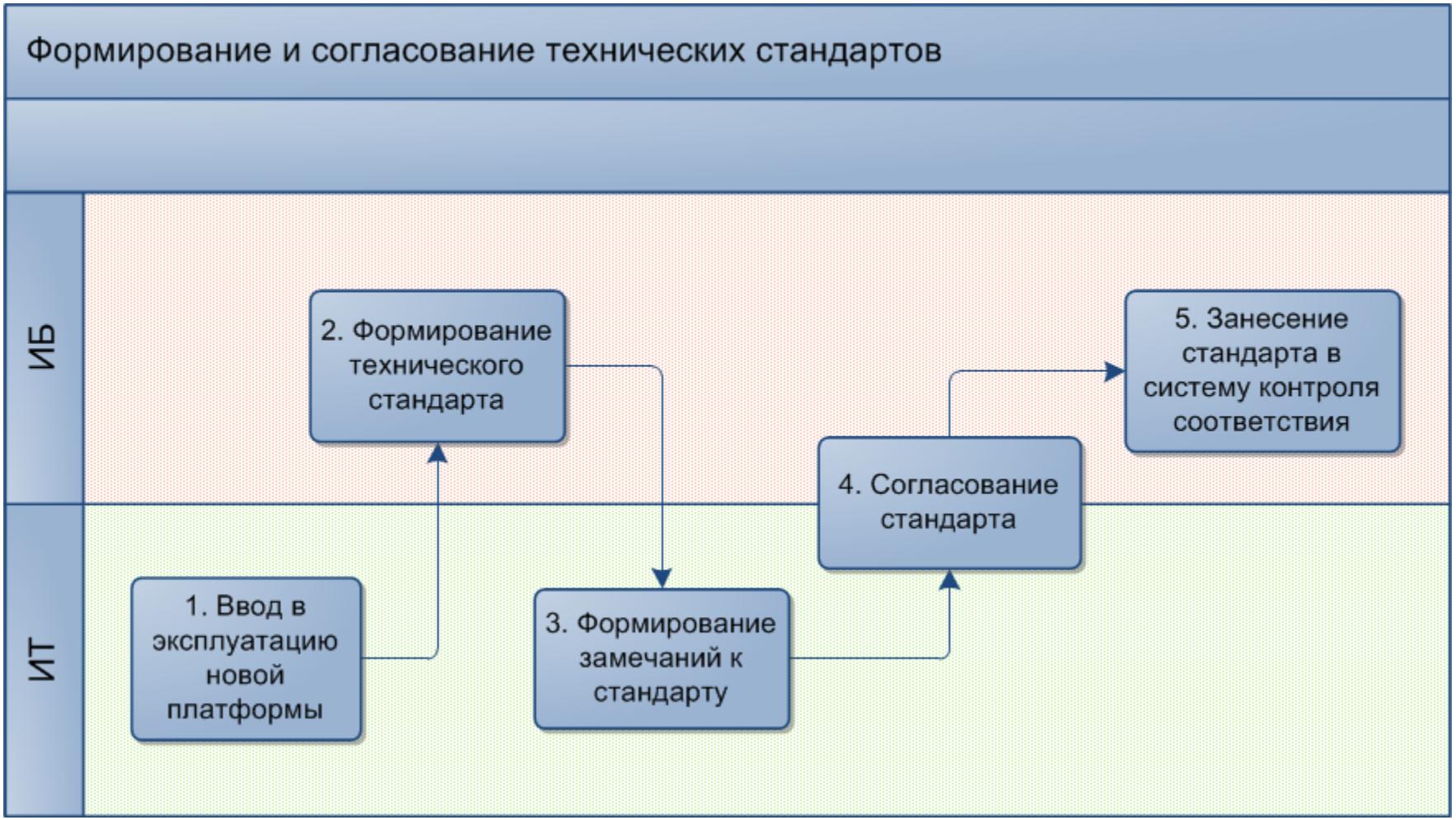
Администраторы ИТ и ИБ

- **Получают детальные Отчеты о соответствии стандартам**
- **Получают указание от Менеджмента ИТ и ИБ устранить выявленные несоответствия либо аргументировать невозможность устранения**
- **Формируют план устранения несоответствий с описанием причин и сроков устранения несоответствий, причин невозможности устранения несоответствий**

Специалисты ИБ

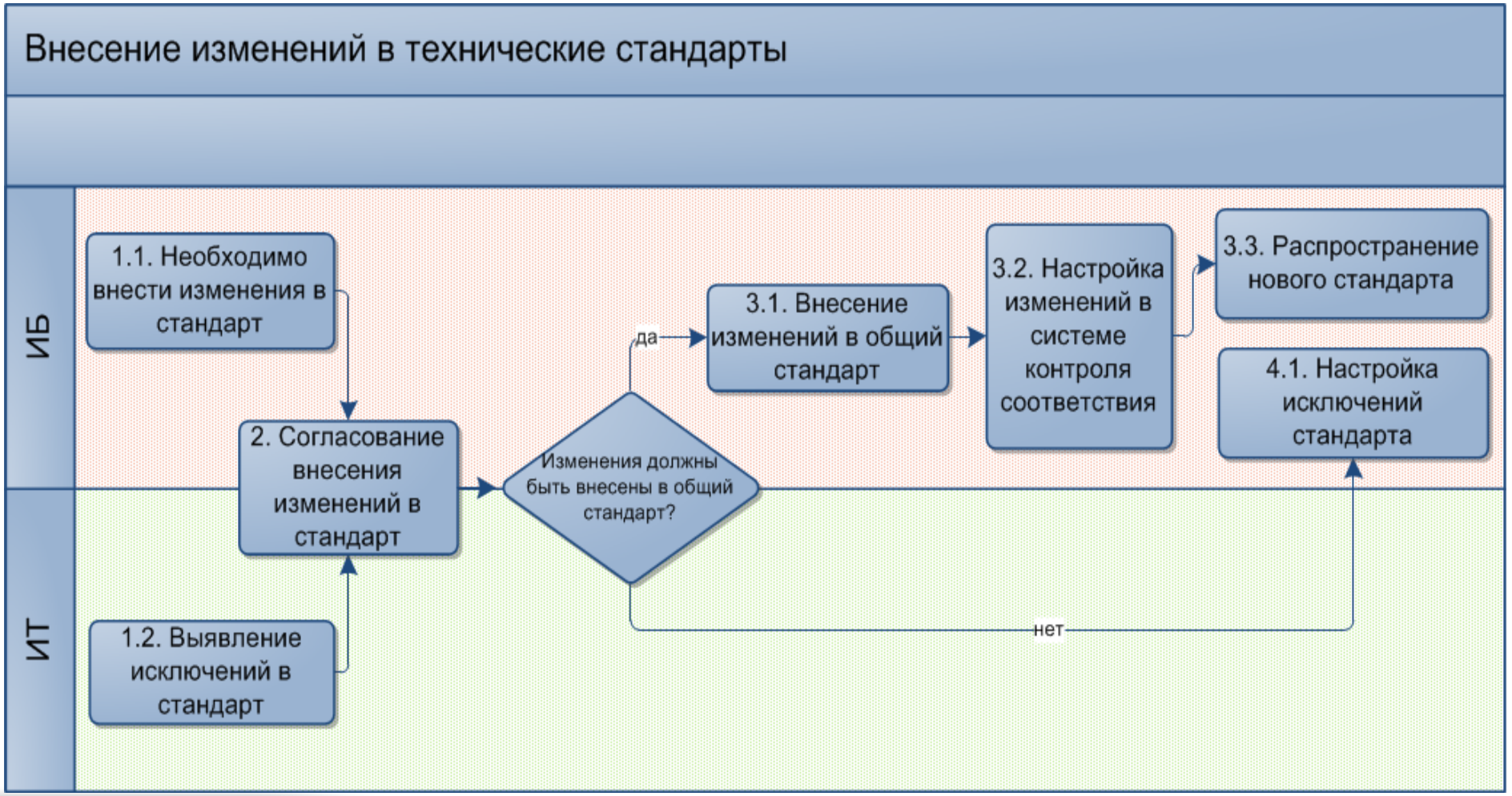
- **Получают детальные Отчеты о соответствии стандартам и Дифференциальные отчеты о соответствии стандартам**
- **Согласуют сроки устранения несоответствий, а также перечень несоответствий, не подлежащих устранению**
- **Контролируют своевременность и качество приведения конфигураций тех.платформ в соответствие стандартам**

Процесс приведения в соответствие стандартам



Процесс приведения в соответствие стандартам

Процесс приведения в соответствие стандартам



Управление соответствием техническим стандартам

- **Технические стандарты разработаны с учетом особенностей инфраструктуры Компании**
- **Контроль над соблюдением технических стандартов осуществаляется автоматизированным средством MaxPatrol**
  - Нет человеческого фактора
  - Снижены затраты ресурсов
  - Используется база знаний MaxPatrol
- **Анализ результатов осуществляется на основе достоверных и своевременных данных**
- **Устранение несоответствий легко организовано и контролируемо**

Спасибо за внимание!

Наталья Куканова
Positive Technologies
nkukanova@ptsecurity.ru

POSITIVE TECHNOLOGIES