




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**



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>)



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, требующие изменения в зависимости от объекта применения:

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



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.

The screenshot displays the MOZORNIN - MaxPatrol - Positive Technologies interface. The top navigation bar includes icons for MAKPATROL, Сканирования, Планировщик, История, Отчеты, Консолидация, Конфигурация, Настройки, and MOZORNIN. The main window is divided into two panes: 'Стандарты' (Standards) and 'Ревизия стандарта' (Standard Review).

Стандарты

- PT - Juniper ScreenOS
- PT - Kaspersky Anti-Virus
- PT - Lotus Domino
- PT - Mandriva Linux OS
- PT - Microsoft Active Directory 2003
- PT - Microsoft Active Directory Universal
 - 25.10.2010
 - 15.09.2011
- PT - Microsoft Exchange 2003
- PT - Microsoft Exchange 2003 Advanced
- PT - Microsoft Exchange 2010
- PT - Microsoft Office
- PT - Microsoft SQL Server 2008
- PT - Microsoft Windows 2000 Professional
- PT - Microsoft Windows XP
- PT - Miscellaneous Controls
- PT - Nortel ERS 5500
- PT - Nortel ERS 8600
- PT - Oracle 9i Server
- PT - SAP R/3
- PT - Sun Solaris 8
- PT - Sun Solaris 9
- PT - SUSE Linux OS
- PT - Symantec Anti-Virus
- PT - Trend Micro OfficeScan
- PT - Universal Controls
- PT - Windows Vista
- PT - ABC Висквит
- PT - PKCC RS056850
- PT - Microsoft Terminal Services

Ревизия стандарта

Дата: 25 октября 2010 г.

Комментарий:

Список требований

Номер	Сортировка	Заголовок
421714	0	Политика паролей: Максимальный срок действия пароля
421715	0	Политика паролей: Минимальная длина пароля
421716	0	Политика паролей: Сложность пароля
421717	0	Политика паролей: История паролей
421718	0	Политика паролей: Хранение паролей с использованием обратимого шифро...
421719	0	Политики блокировки учетной записи: Период блокировки
421720	0	Политики блокировки учетной записи: Пороговое значение блокировки
421721	0	Политики блокировки учетной записи: Сброс счетчика блокировки через
421757	0	Параметры безопасности (Член домена): Всегда требуется цифровая подп...
421758	0	Параметры безопасности (Член домена): Используется шифрование защи...

Параметры требования

Заголовок
Политика паролей: История паролей

Краткое описание
Рекомендуется хранить 24 пароля.

Полное описание
Пароли следует регулярно менять, причем пользователи не должны иметь возможность постоянно использовать один и тот же набор паролей. Параметр "Требовать неповторяемости паролей" определяет, сколько предыдущих паролей будет храниться, чтобы гарантировать, что пользователи не используют

Применить Отмена

Создание технических стандартов. Выбор требований. Универсальные проверки.

Добавление требований

Репозиторий требований

Искать по всем полям

Номер	Заголовок
430000	(Windows) Проверка параметров реестра (1)
4424789	(Windows) Проверка параметров реестра (10)
430034	(Windows) Проверка параметров реестра (2)
430035	(Windows) Проверка параметров реестра (3)
430036	(Windows) Проверка параметров реестра (4)
430037	(Windows) Проверка параметров реестра (5)
430038	(Windows) Проверка параметров реестра (6)
430039	(Windows) Проверка параметров реестра (7)
430040	(Windows) Проверка параметров реестра (8)
430041	(Windows) Проверка параметров реестра (9)
430079	(Windows) Проверка прав доступа к службам 1
430088	(Windows) Проверка прав доступа к службам 10
430080	(Windows) Проверка прав доступа к службам 2
430081	(Windows) Проверка прав доступа к службам 3
430082	(Windows) Проверка прав доступа к службам 4
430083	(Windows) Проверка прав доступа к службам 5
430084	(Windows) Проверка прав доступа к службам 6
430085	(Windows) Проверка прав доступа к службам 7

Параметры требования


Заголовок
(Network Devices) Поиск строк в файле конфигурации 1


Краткое описание
Проверка позволяет выполнять поиск строк в конфигурации устройства.

OK Отмена



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.

Добавление требований

Репозиторий требований

Искать по всем полям

Номер	Заголовок
420065	Параметры безопасности (Интерактивный вход в систему): заго...
421136	Права пользователей: Доступ к диспетчеру учетных данных о...
421200	Аудит: принудительно переопределяет параметры категории п...
421219	Журнал приложений: Сохранять старые события
421220	Журнал безопасности: Сохранять старые события
421221	Системный журнал: Сохранять старые события
421222	Брандмауэр Windows: Домен: Состояние брандмауэра
421223	Брандмауэр Windows: Домен: Входящие подключения
421224	Брандмауэр Windows: Домен: Выводить уведомление
421225	Брандмауэр Windows: Домен: Разрешить одноадресный ответ
421226	Брандмауэр Windows: Домен: Применить локальные правила бр...
421227	Брандмауэр Windows: Домен: Применить локальные правила бе...
421228	Брандмауэр Windows: Частный профиль: Состояние брандмауэра
421229	Брандмауэр Windows: Частный профиль: Входящие подключения
421230	Брандмауэр Windows: Частный профиль: Выводить уведомление

Параметры требования

Заголовок
Аудит: принудительно переопределяет параметры категории политики аудита параметрами подкатегории политики аудита (Windows Vista или следующие версии)

Краткое описание
Если данная настройка включена, Windows учитывает параметры подкатегорий аудита, а не традиционной политики аудита. Для всех профилей рекомендуемое значение данного параметра - включено (Enabled).

Полное описание
Если данная настройка включена, Windows учитывает параметры подкатегорий аудита, а не традиционной политики

OK Отмена



Создание технических стандартов. Изменение текстов требований.

Редактирование требования

Заголовок

Приоритет

Краткое описание

Полное описание

Пароли следует регулярно менять, причем пользователи не должны иметь возможность постоянно использовать один и тот же набор паролей. Параметр "Требовать неповторяемости паролей" определяет, сколько предыдущих паролей будет храниться, чтобы гарантировать, что пользователи не используют один набор паролей постоянно. При определении общей конфигурации учетной записи следует учесть совместное использование истории паролей и настроек максимального срока действия пароля. Например, если срок действия пароля 30 дней и количество хранимых паролей 12 или меньше, многие пользователи, вероятно, будут использовать пароли, связанные с именем текущего месяца (January1, February1 и т.д.).

Как исправить

Рекомендуется хранить 24 предыдущих пароля.
Чтобы изменить требования неповторяемости паролей откройте Редактор групповых политик (Group Policy Editor) и выберите Конфигурация компьютера (Computer Configuration) - Конфигурация Windows (Windows Settings) - Параметры безопасности (Security Settings) - Политики учетных записей (Account Policies) - Политика паролей (Password Policy). Для внесения изменений дважды щелкните мышью на позиции "Требовать неповторяемости паролей" (Enforce password history), установите нужное значение в появившемся окне и нажмите "ОК". Изменения вступят в силу после применения групповой политики.

Ссылки

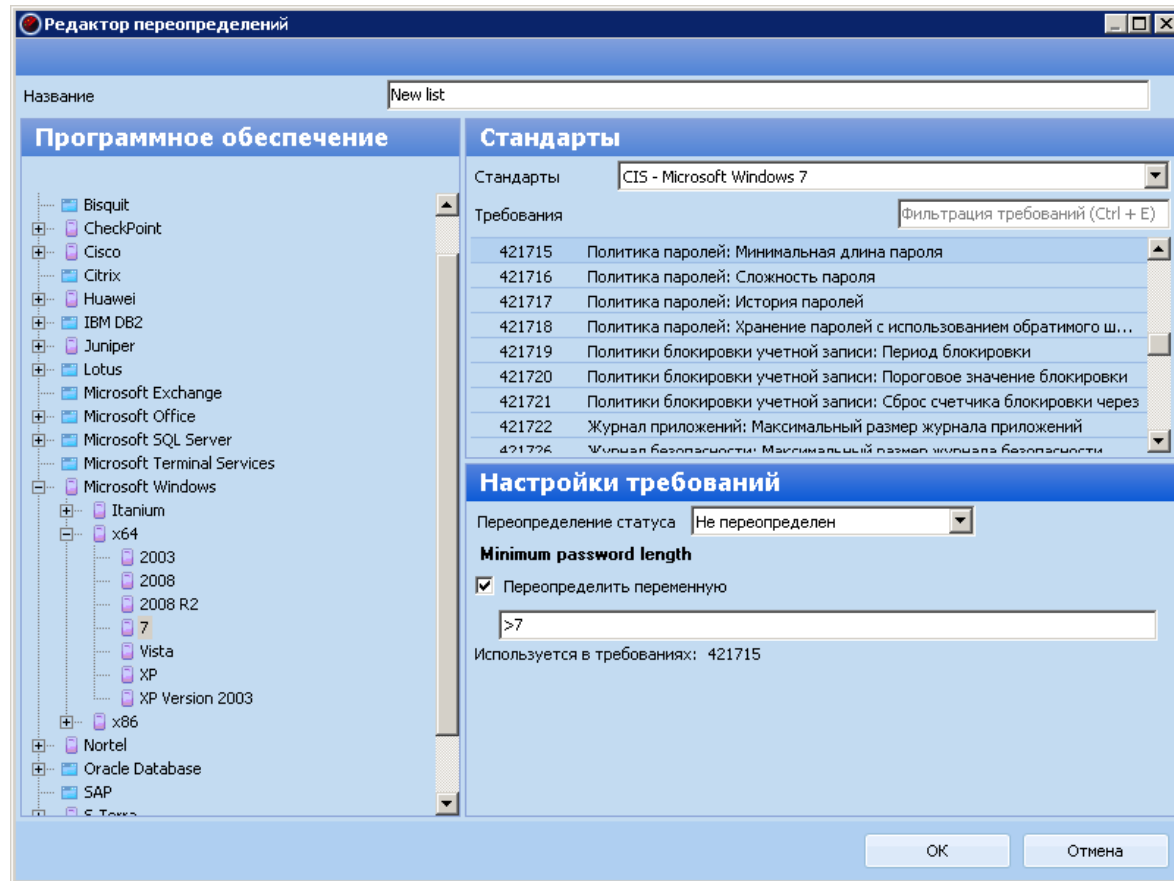
OK Отмена



Создание технических стандартов. Применимость значений требований.

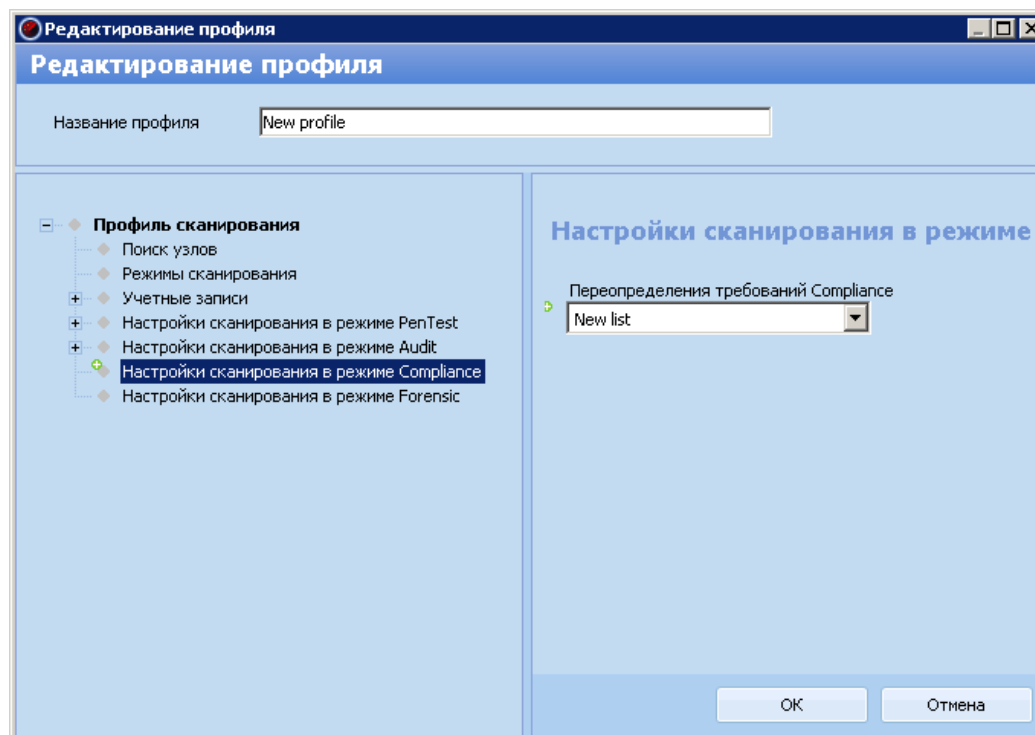
Новые значения требований могут применяться:

- 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

Создание отчета

Название:

Комментарий:

Формат:

Язык:

Тип отчета

Информация Сравнительный
 Дифференциальный Динамический
 Аналитический

Исходные данные

По скану
 По задаче/задачам

Тип данных

Выбор задачи и скана

Задача: ... Сканы: ...

Стандарт

Статистика по всем узлам Данные по каждому узлу
 Список узлов по статусу Описание требования
 Статистика с учетом неопределенных узлов
 Статистика с учетом неприменимых стандартов

Отображение требований

Группировка:
Сортировка:

Соотношение задач и стандартов

Стандарт:

Фильтр требований

По статусу:

Фильтр узлов

Достоверность результатов:
Включать узлы, отмеченные как:
 Включать узлы, завершенные с ошибкой
 Включать узлы, данные о которых отсутствуют

Дополнительный

OK Отмена



Формирование отчетов. Дифференциальный отчет по стандартам

Создание отчета

Название:

Комментарий:

Формат:

Язык:

Тип отчета

Информация Сравнительный аналитический
 Дифференциальный Динамический аналитический
 Аналитический

Исходные данные

По скану
 По задаче/задачам

Идентификация узлов

Тип данных

Эталонный скан

Задача: Скан:

Исследуемый скан

Задача: Скан:

Определение изменений

Не учитывать изменения при разной достоверности
 Не учитывать изменения при разных статусах транспортов

Соотношение задач и стандартов

Стандарт:

Содержание и вид отчета

Разделы отчета

- Исправлено
- Нарушено
- Требуется оценка изменений
- Без изменений

Информация о требованиях

- Название
- Краткое описание
- Описание
- Результаты проверки
- Решение
- Ссылки

Группировка данных в отчете:

Логика построения отчета

Оценка статусов требований:

Фильтр узлов

Достоверность результатов:

Включать узлы, отмеченные как:

Включать узлы, завершенные с ошибкой
 Включать узлы, данные о которых отсутствуют

Дополнительный



Формирование расписаний и доставки отчетов

Создание расписания

Название расписания:

Сценарий запуска:

Параметры запуска

Выполнять задачу: Ежемесячно
Каждые: 1 месяц
Дата начала: 05.12.2011 16:32:35 Дата окончания: 18.01.2037 23:59:59
 Запустить после создания

Отчеты и их доставки по завершении задачи

+ - ×

Имя отчета	Доставка
Дифференциальный по стандартам	New delivery
Информационный Compliance	New delivery



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 Высокий уровень безопасности защиты от макросов

ID: 301528

Описание

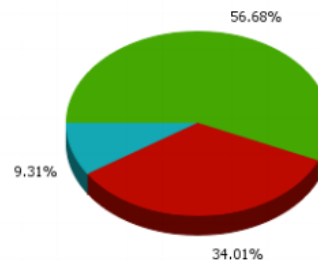
Для Access 2003 для обработки макросов установлен Высокий уровень безопасности защиты от макросов.

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






-  **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

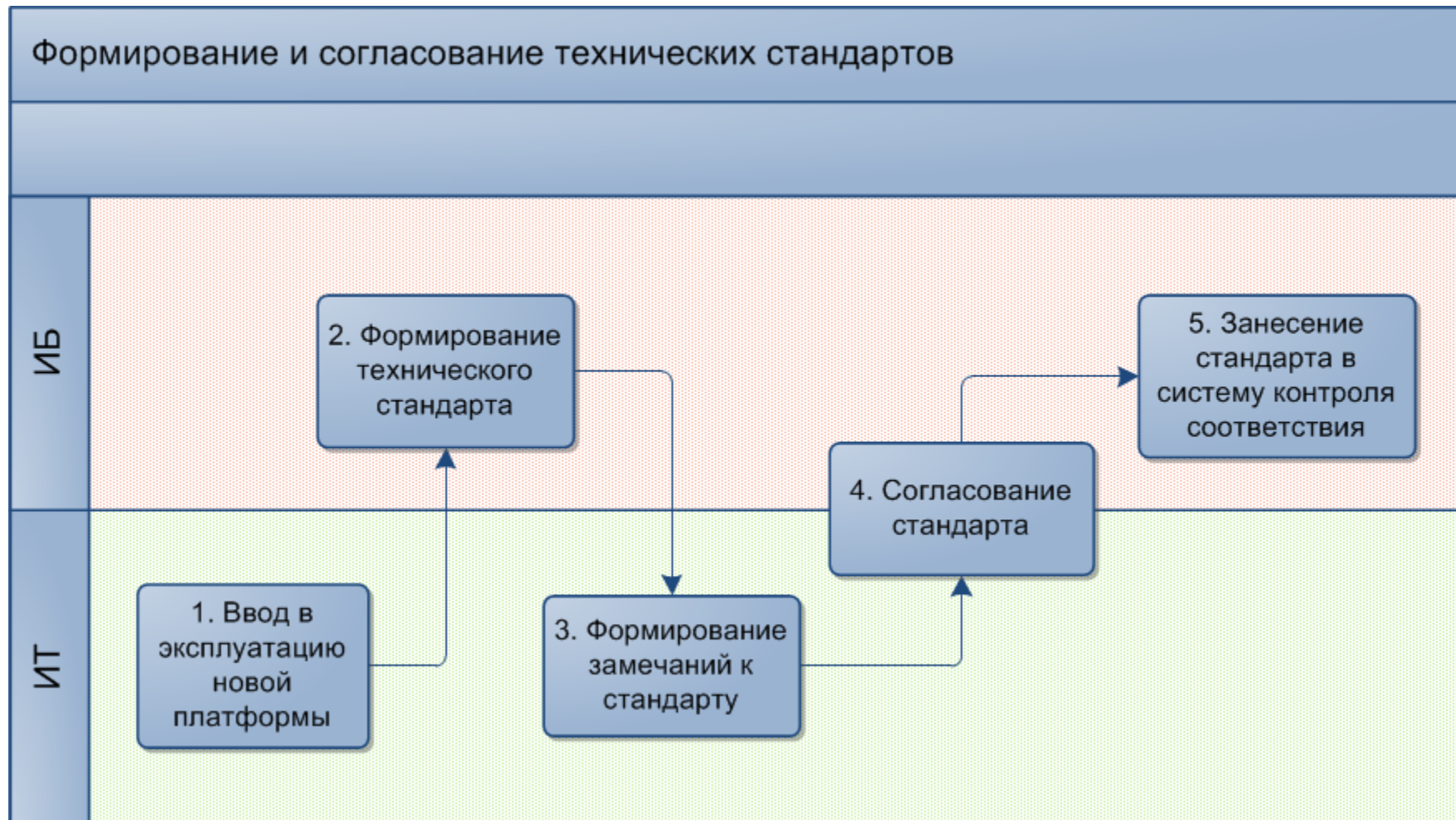
-  **Получают детальные Отчеты о соответствии стандартам**
-  **Получают указание от Менеджмента ИТ и ИБ устранить выявленные несоответствия либо аргументировать невозможность устранения**
-  **Формируют план устранения несоответствий с описанием причин и сроков устранения несоответствий, причин невозможности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



-  **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



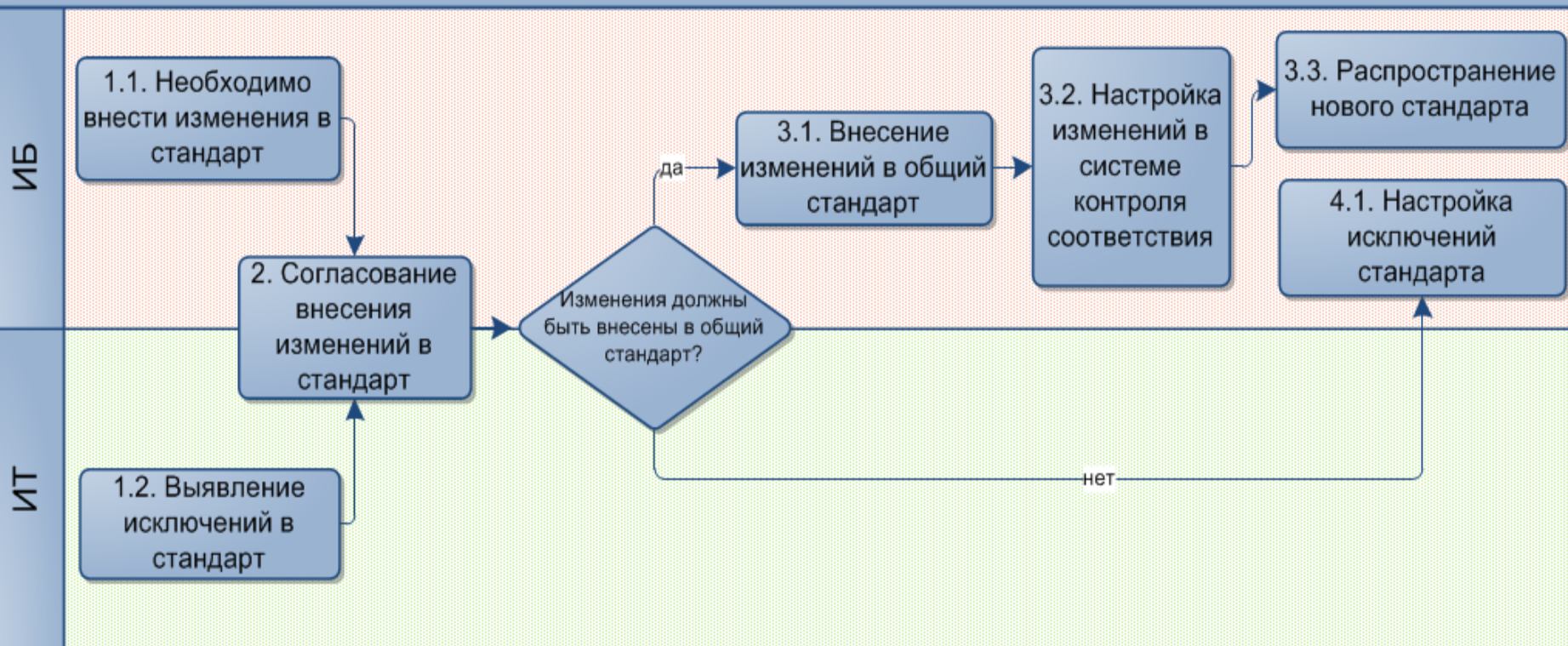
Процесс приведения в соответствие стандартам

Контроль соответствия техническим стандартам





Процесс приведения в соответствие стандартам


Внесение изменений в технические стандарты




Управление соответствием техническим стандартам

-  **Технические стандарты разработаны с учетом особенностей инфраструктуры Компании**

-  **Контроль над соблюдением технических стандартов осуществляется 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