Оценка эффективности мер обеспечения ИБ

Наталья Куканова

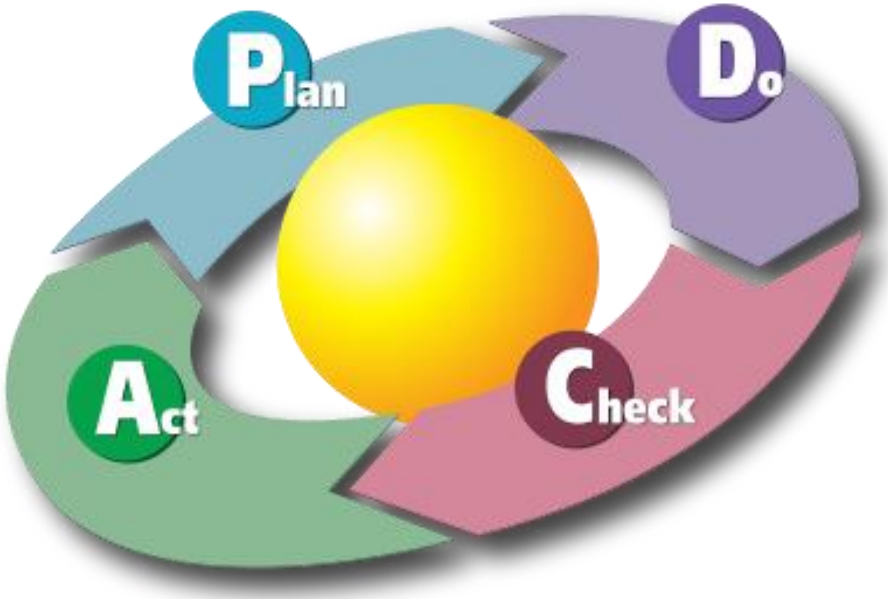
Positive Technologies

POSITIVE TECHNOLOGIES

Цель рассказа

- **Зачем оценивать результативность СУИБ?**
- **Как оценивать результативность СУИБ? Откуда брать данные для анализа?**
- **Что делать с полученными оценками? Как совершенствовать процедуры СУИБ?**

Место процесса в PDCA-модели



- ***Процесс оценки результативности СУИБ находится на этапе "Check" и служит в первую очередь для того, чтобы выявить, насколько результативно и эффективно внедрены процедуры СУИБ, и разработать методики совершенствования, которые будут использованы на этапах "Act" и "Plan".***

Цели оценки результативности СУИБ

- **Правильно ли функционируют процедуры обеспечения ИБ?**
- **Повышается ли уровень защищенности при использовании процедур?**
- **Как много ресурсов (трудовых, материальных и пр.) используется для реализации процедур обеспечения ИБ?**
- **Как устранить выявленные недостатки и улучшить процедуры обеспечения ИБ?**

Как оценить результативность СУИБ?

- **Какие процедуры обеспечения ИБ необходимо оценить?**
- **Какие метрики однозначно показывают, позволяют ли процедуры обеспечения ИБ достичь поставленных целей?**
- **Какие способы сбора данных для расчета метрик выбрать?**
- **Как сформировать отчетность по результатам анализа полученных данных и принятия решений?**
- **Как определить направления совершенствования процедур обеспечения ИБ?**

Что анализировать при оценке результативности?

- **Процедуры обеспечения ИБ реализуются различными механизмами. В процессе оценки результативности процедур необходимо выявить, насколько правильно функционируют эти механизмы.**

Процедура ИБ	Механизмы
Повышение осведомленности пользователей	1. Очные курсы, тесты 2. Дистанционная система обучения 3. Инструктаж при приеме на работу
Управление обновлениями ОС	1. Централизованная система установки обновлений 2. Установка обновлений по расписанию вручную
Контроль доступа. Парольная политика	1. Технические средства обеспечения стойкости паролей 2. Регламентирующие документы 3. Обучение пользователей

Метрики оценки результативности СУИБ

- **Однозначно измеряются, без «экспертного мнения»**
- **Доступны для расчета и анализа (предпочтительно автоматически)**
- **Имеют количественное выражение (деньги, время, пр.)**
- **Понятны и указывают на проблемную область и возможные решения**

- **Процесс определения метрик и их оценки изложен, например, в ISO/IEC 27004**

Пример разработки метрик

Контроль доступа

Цель	Метрика	Источник данных
Минимизация привилегий пользователей	Актуальность матрицы доступа	Аудит
	Соответствие привилегий пользователей матрице доступа	Автоматизированная проверка пользователей АС Аудит
Доступ представляется только авторизованным пользователям	Сложность паролей пользователей	Анализ настроек АС Проверка паролей пользователей
	Учетные записи уволенных сотрудников блокируются	Проверка наличия учетных записей уволенных сотрудников в АС

Пример метрики (ISO/IEC 27004)

Метрика	Система защиты от вредоносного ПО (SPSM)
Требование	10.4.1 [27001:2005]
Цель метрики	Определить результативность средств защиты от вредоносного ПО
Расчет метрики	Формула для расчета: SPSM = ISM / EBSM, где: ISM – сумма инцидентов, связанных с вредоносным ПО EBSM – сумма обнаруженных и блокированных инцидентов, связанных с вредоносным ПО
Частота сбора данных	Ежедневно
Период создания отчета	Ежемесячно
Критерии	Неудовлетворительно: SPSM>0.001 Удовлетворительно: SPSM<0.001
Действия	Если SPSM имеет неудовлетворительное значение, необходим пересмотр данной процедуры обеспечения ИБ
Положительное значение	Значение SPSM должно быть минимальным

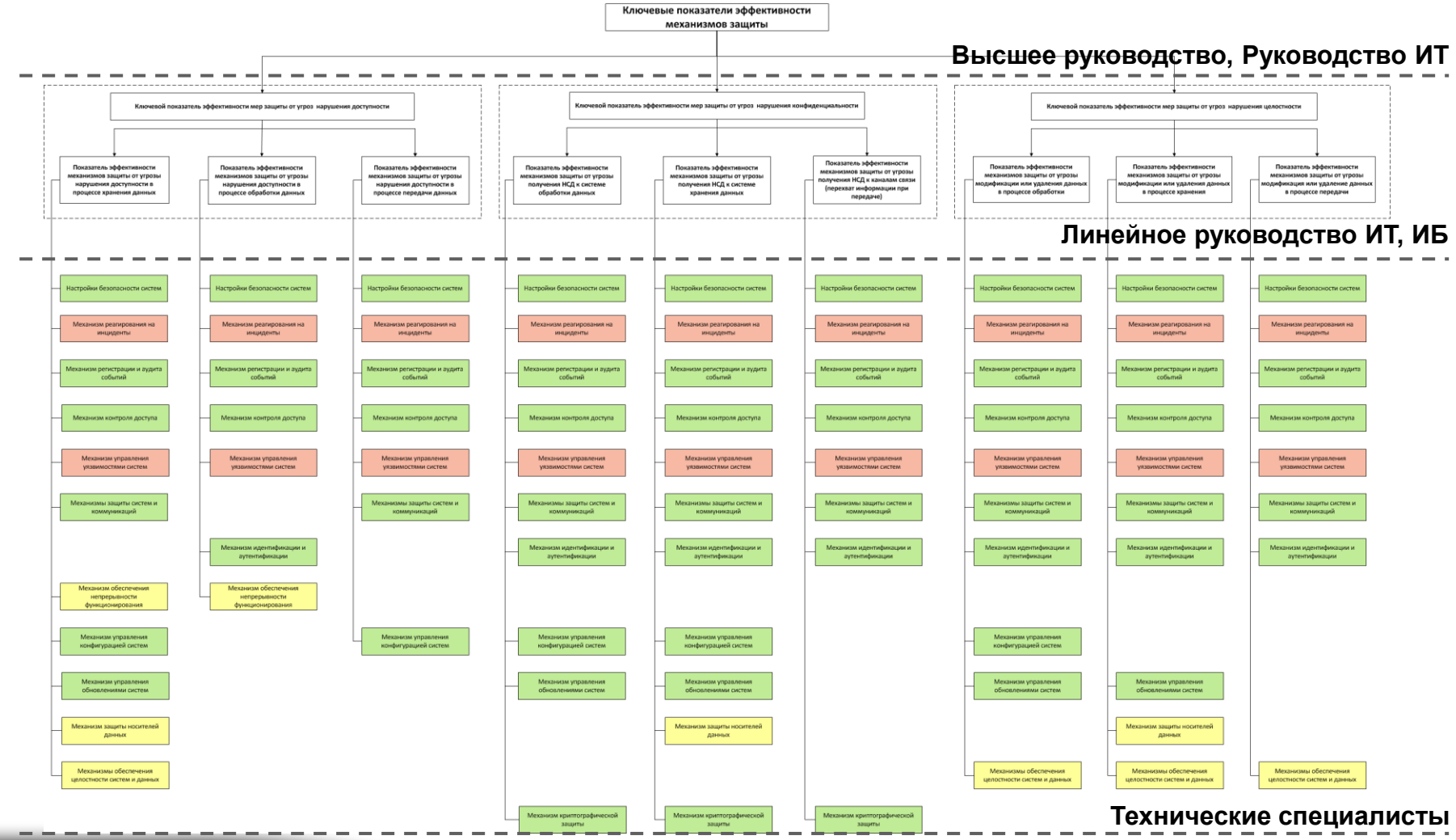
Пример метрики

Процесс	Управление конфигурациями ПО
Требование	Все используемые ОС должны иметь актуальные версии
Метрика	Процент ОС, имеющих актуальную версию (F)
Расчет метрики	Формула расчета: F = (A / B) * 100%, где A – количество ОС, имеющих актуальную версию B – общее количество используемых ОС
Частота сбора данных	Ежемесячно
Период создания отчета	Ежемесячно
Критерии	Неудовлетворительно F<90% Удовлетворительно F>90%
Действия	Если F<90%, необходим пересмотр данной процедуры обеспечения ИБ
Комментарии	Исключения (ресурсы, на которых актуальные версии ОС не могут устанавливаться своевременно) рассматриваются отдельно. Перечень исключений должен быть документирован и утвержден

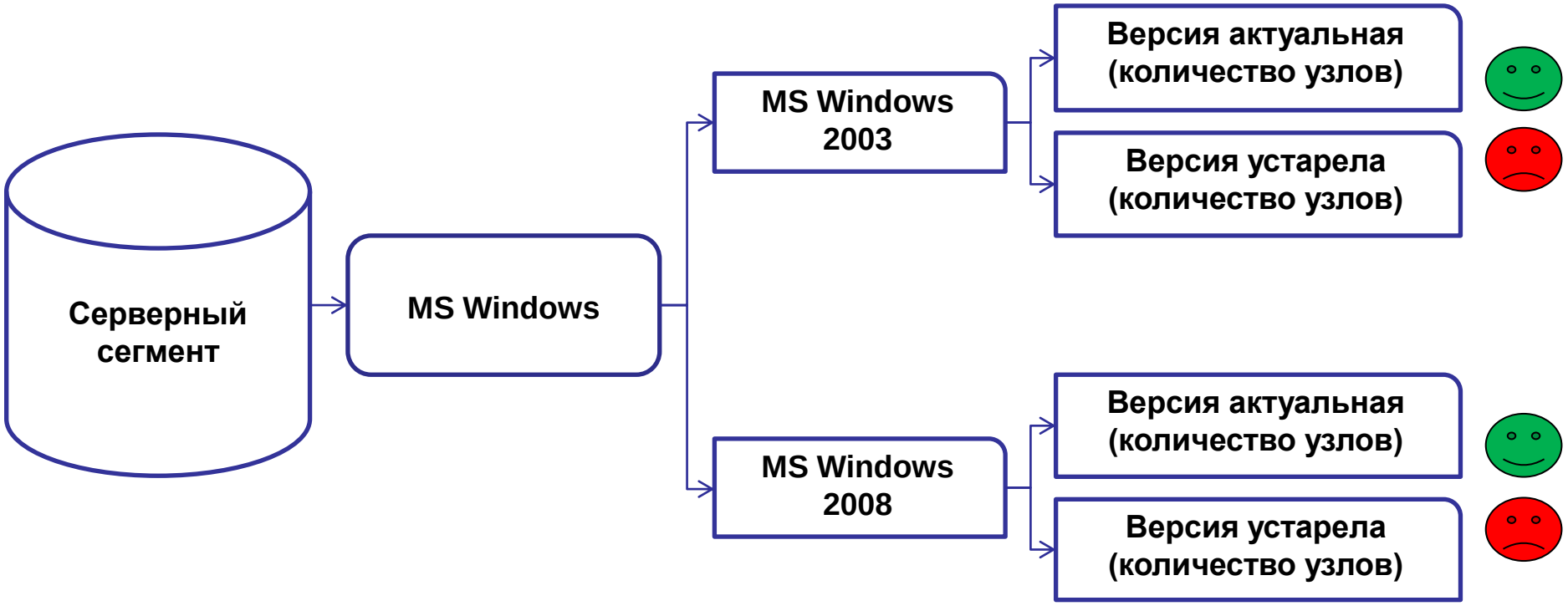
Способы сбора данных

- **Внешние аудиты**
- **Внутренние аудиты, опросы**
- **Анализ инцидентов и событий ИБ**
- **Использование автоматизированных средств**
- **…**

Иерархия метрик

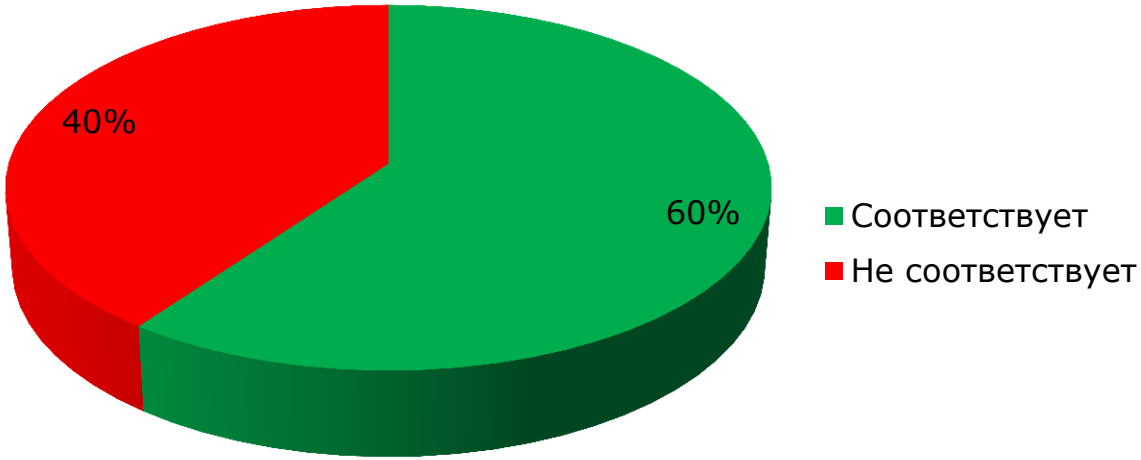


Пример оценки результативности процедур ИБ



Отчет для руководства департамента ИТ

Управление конфигурациями ПО



Отчет для менеджера ИБ

Серверный сегмент

Управление конфигурациями ПО

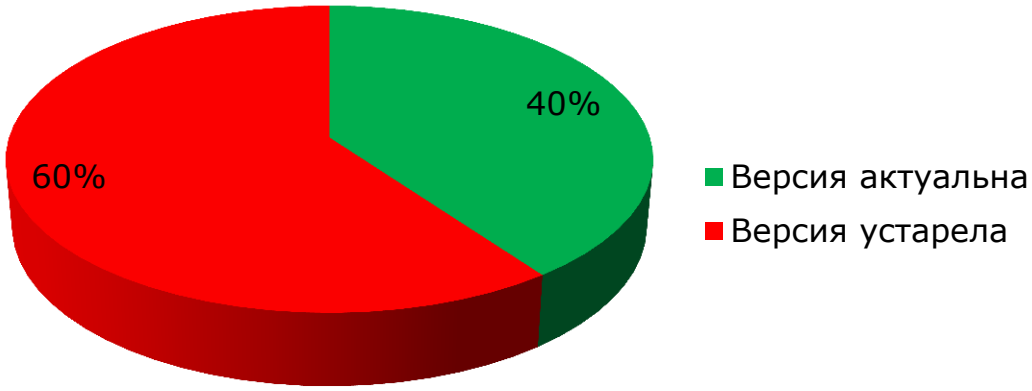
Актуальность версий ПО

Операционные системы

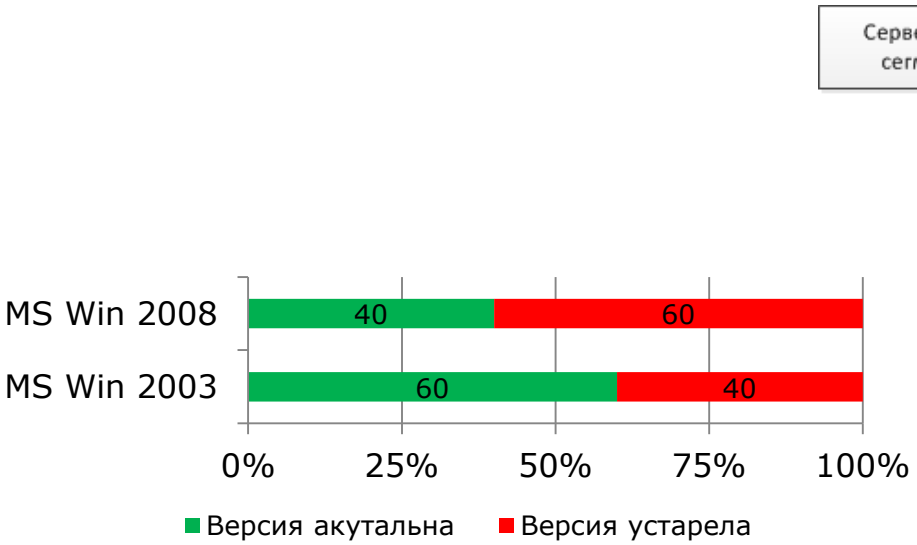
MS Windows

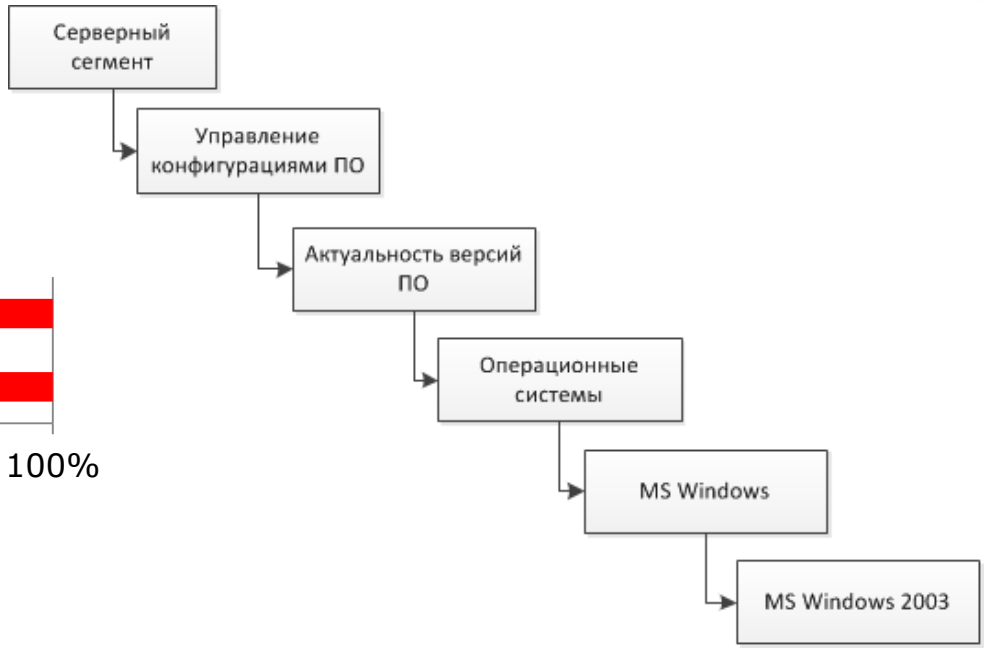
MS Windows 2003

Актуальность версий Windows-систем



Отчет для технического специалиста



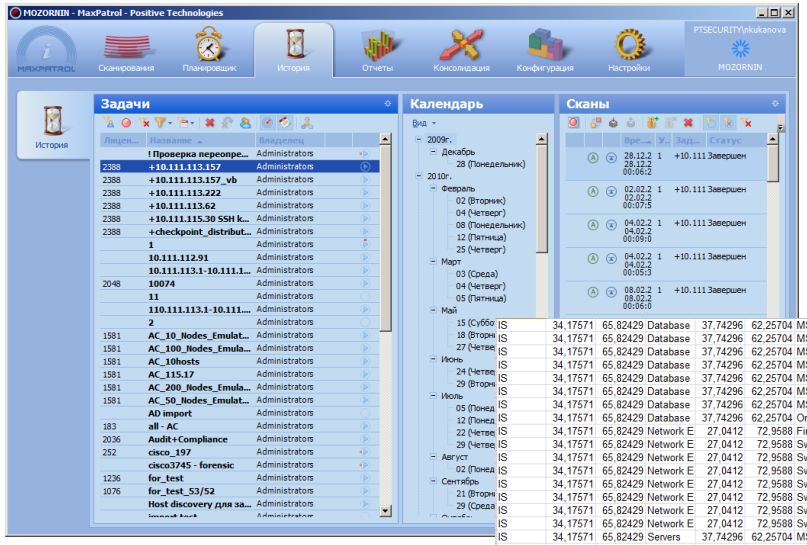


ОС	Перечень узлов с устаревшей версией ОС
MS Windows 2003	192.168.40.100, 192.168.40.153, …
MS Windows 2008	192.168.49.90, 192.168.49.101, …

Примеры метрик

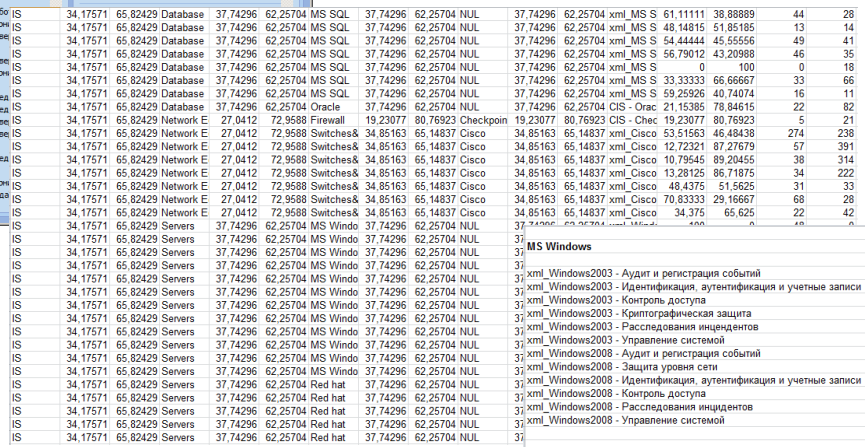
Процедура ИБ	Метрики
Антивирусная защита	Количество и процент рабочих станций с установленным антивирусным пакетом Количество и процент рабочих станций с обновленными антивирусными базами …
Сетевая безопасность	Количество нестандартных серверных портов и приложений на рабочих станциях/серверах …
Управление уязвимостями	Количество и процент систем, содержащих критические уязвимости Количество уязвимостей, возникающих в течение определенного промежутка времени (месяц, квартал, год) Количество уязвимостей, устраняемых в течение определенного промежутка времени (месяц, квартал, год) Количество уязвимостей, требующих устранения …
Управление конфигурациями	Уровень соответствия (несоответствия) различных систем корпоративным и международным стандартам Количество изменений конфигураций различных систем Среднее время (задержка) развертывания критических обновлений …

Использование MaxPatrol для получения данных

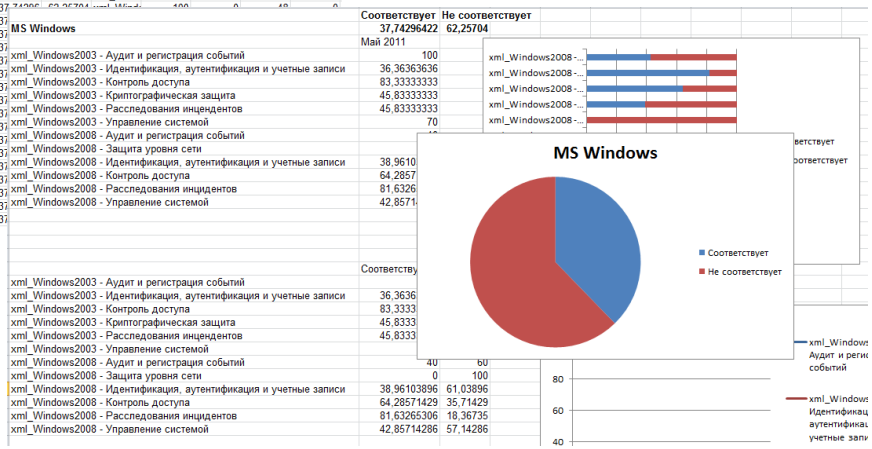


MaxPatrol

XML



MS Excel



Анализ полученных данных

- **Позволяют ли используемые средства обеспечения ИБ достичь поставленных целей? Если нет, то почему?**
- **Какими ресурсами это достигается? Насколько это целесообразно?**
- **Утвержден ли перечень исключений?**
- **Используются ли компенсирующие меры? Достаточно ли существующих мер?**
- **Как устранить выявленные недостатки и улучшить выполнение процедур ИБ?**

Заключение

Оценка результативности процедур обеспечения ИБ позволяет:

- **Определить некачественную реализацию процедур ИБ**
- **Выявить причины возникновения недостатков**
- **Выявить нецелесообразное расходование ресурсов**
- **Своевременно принять меры по улучшению –**

прежде, чем эти недостатки обнаружит и применит злоумышленник

Спасибо за внимание!

Наталья Куканова

Positive Technologies

nkukanova@ptsecurity.ru

POSITIVE TECHNOLOGIES