

POSITIVE TECHNOLOGIES

Дмитрий Кузнецов

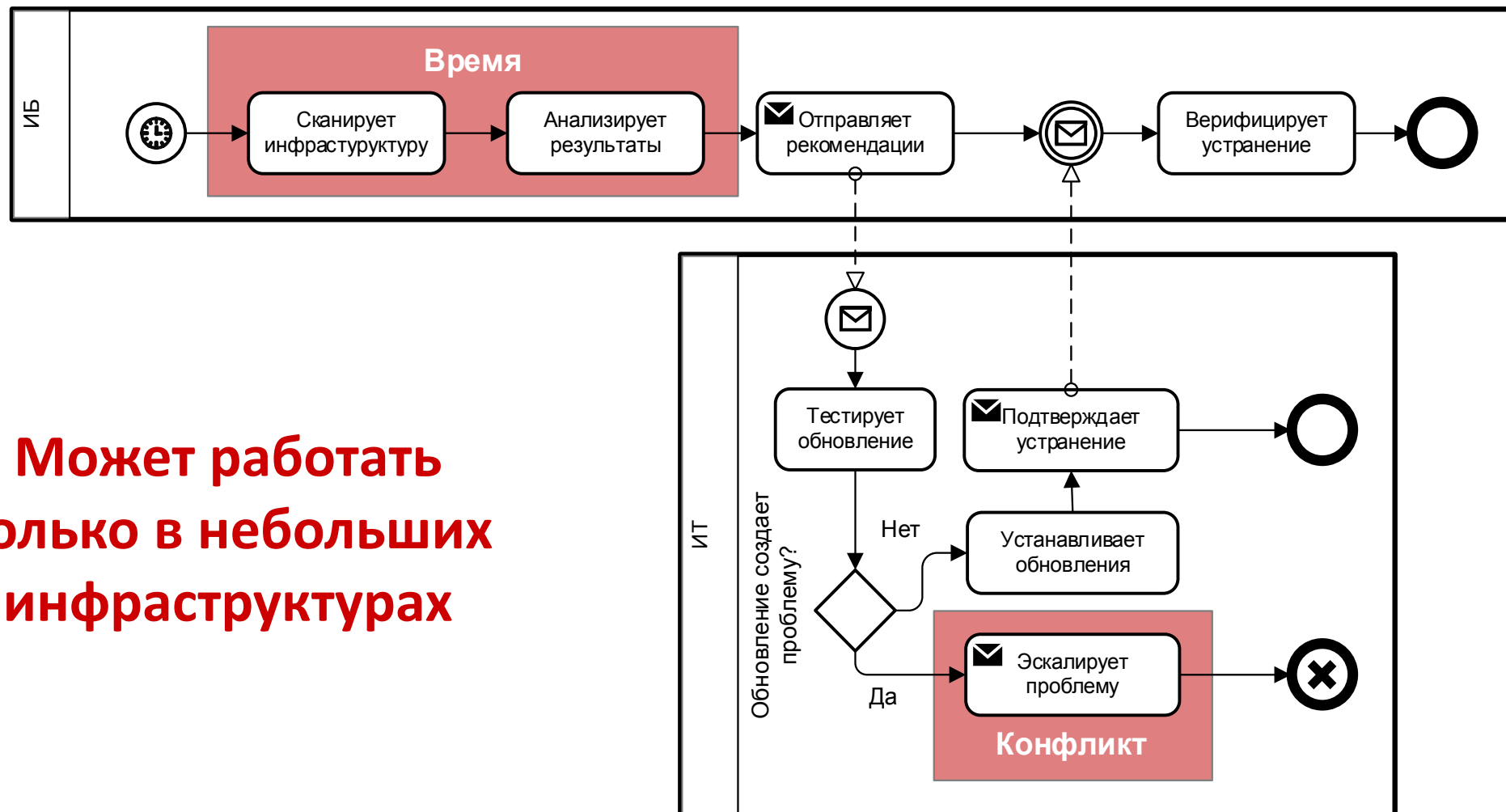
Директор по методологии и стандартизации

dkuznetsov@ptsecurity.com

“Вас много, я один!” или
как не сойти с ума в
процессе менеджмента
уязвимостей



Типичный процесс менеджмента уязвимостей



Может работать только в небольших инфраструктурах

Как его пытаются оптимизировать

Давайте устранять только серьезные уязвимости

Давайте устранять только уязвимости, к которым есть эксплойты

Давайте устранять только удаленно эксплуатируемые уязвимости

Давайте моделировать действия злоумышленника

Менеджмент конфигурации

Нужны строгие правила, как именно должны настраиваться компоненты ИС и как именно должны устанавливаться обновления. Исполнение этих правил – ответственность ИТ.

Менеджмент изменений

Иногда уязвимости ИС обусловлены дизайном ИС, и для их устранения систему нужно модернизировать. И для этого тоже нужны строгие правила.

Мониторинг уязвимостей

Большая часть уязвимостей должна устраняться “автоматически” в рамках менеджмента конфигурации и изменений. Но эти процессы нужно контролировать

- ▶ В вашей инфраструктуре действительно нужны Windows 10, 8 и 7 одновременно?
- ▶ Основные компоненты ИС можно и нужно унифицировать:
 - Операционные системы
 - СУБД
 - CMS
 - Офисные приложения
 - Сетевое оборудование
 - ...
- ▶ Для унифицированных компонентов можно и нужно организовать тестирование и автоматическую установку обновлений. Анализ устранимых ими уязвимостей становится не нужен
- ▶ Для унифицированных компонентов можно и нужно разрабатывать стандарты безопасной настройки. Их применение легко автоматизируется

Что требуется от менеджмента изменений

- ▶ Использование унифицированных компонентов – одно из требований ТЗ
- ▶ Разработка стандартов конфигурации для нестандартных компонентов – обязанность подрядчика
- ▶ Сервисный контракт: подрядчик гарантирует работоспособность ИС после установки обновлений компонентов
- ▶ Первичный анализ уязвимостей и их устранение – обязанность подрядчика
- ▶ Инвентаризация компонентов ИС: что из установленного действительно нужно для работы системы и ее пользователей?

Мониторинг уязвимостей – это...

- ▶ Инвентаризация фактического состава инфраструктуры
- ▶ Контроль соблюдения стандартов конфигурации
- ▶ Контроль установки обновлений
- ▶ Контроль использования запрещенного или отсутствия обязательного ПО
- ▶ Мониторинг оповещений об угрозах и инцидентах
- ▶ Анализ уязвимостей заказного ПО
- ▶ Тестирование на проникновение
- ▶ Препжний “менеджмент уязвимостей” для неунифицированных компонентов

Что в результате ?

- ▶ Отказ от ненужного и трудоемкого анализа найденных уязвимостей
- ▶ Функции подразделения ИБ сведены с контрольным, взаимодействие с ИТ – к отношениям “исполнитель-контролер”
- ▶ Риски отказа ИС в связи с установкой обновлений перенесены на подрядчика
- ▶ Многие задачи мониторинга решаются анализом инвентаризационной информации
- ▶ Устраняются все уязвимости, и сроки их устранения можно ограничить

POSITIVE TECHNOLOGIES

Дмитрий Кузнецов

Директор по методологии и стандартизации

dkuznetsov@ptsecurity.com

Спасибо
за внимание

