Автопентест и управление рисками ИБ

Валерий Филин
Технический директор

План

- Типовой процесс управления рисками ИБ
- Применимые инструменты анализа защищенности
- Ключевые отличия автоматизированного пентеста

Управление рисками ИБ

Процессы ИБ

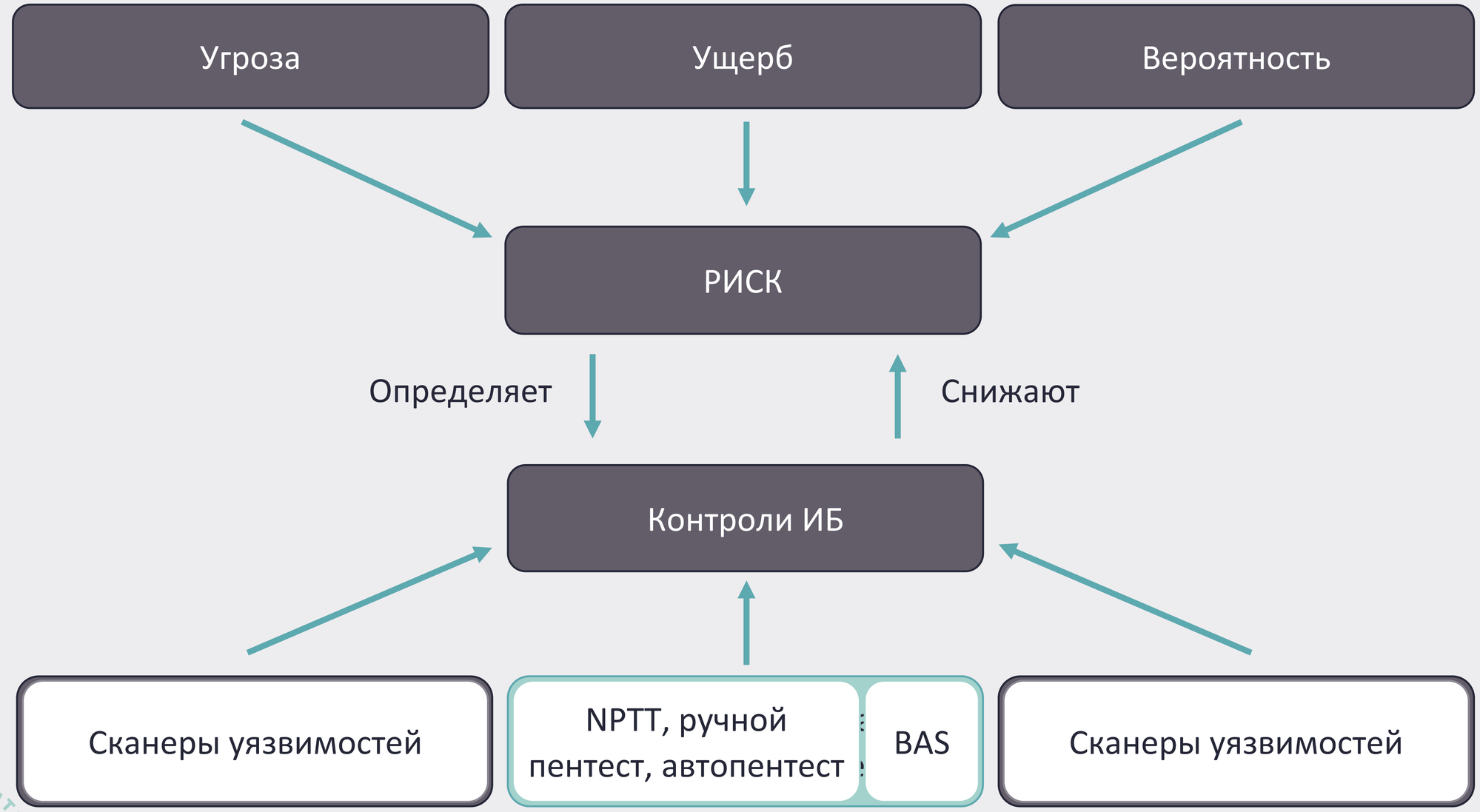
Области автоматизации

- **Управление рисками ИБ**
- Управление уязвимостями
- Управление изменениями
- Управление доступом
- Реагирование на инциденты
- Защита данных

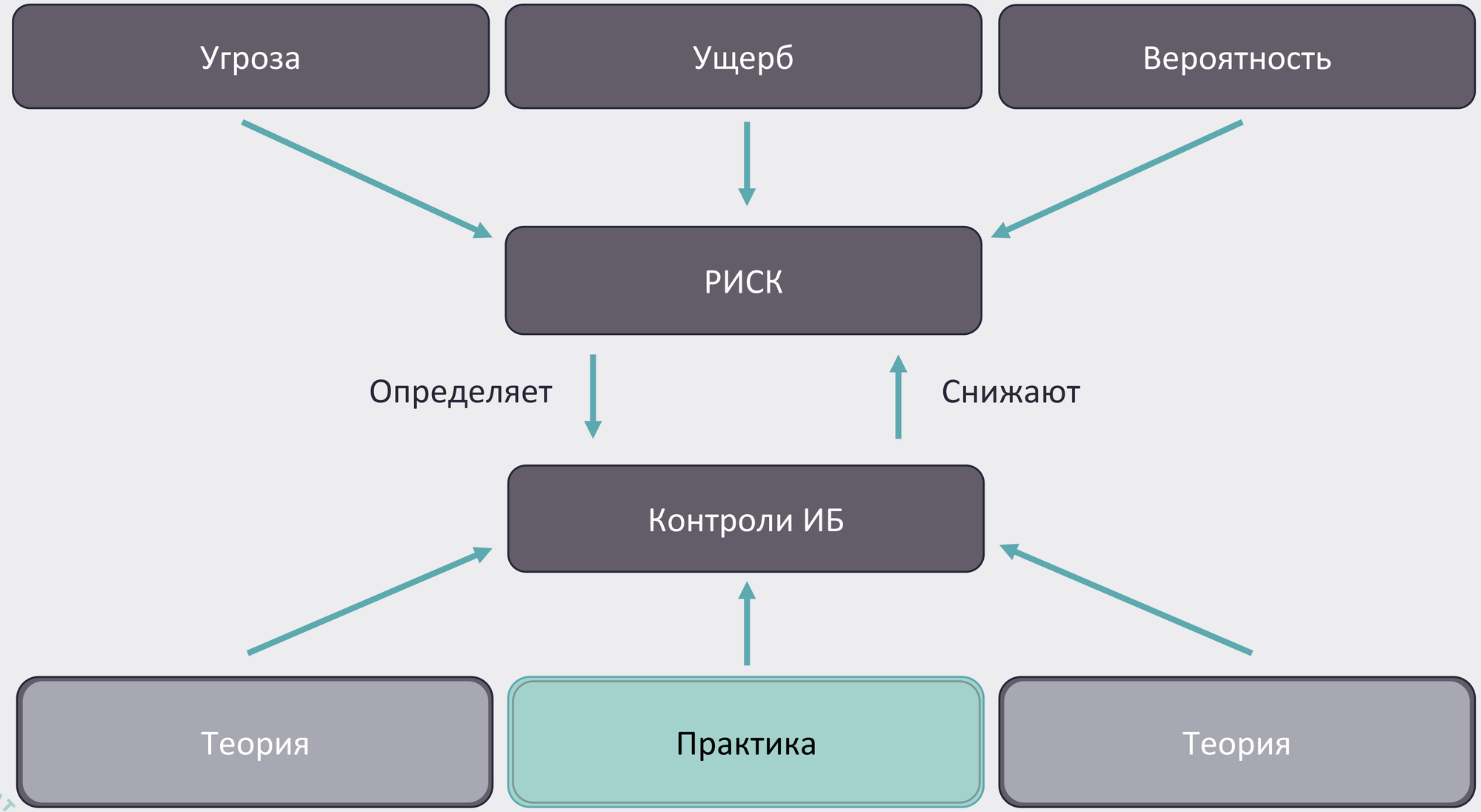
Управление рисками ИБ

Варианты проверки контролей ИБ

Решения анализа защищенности

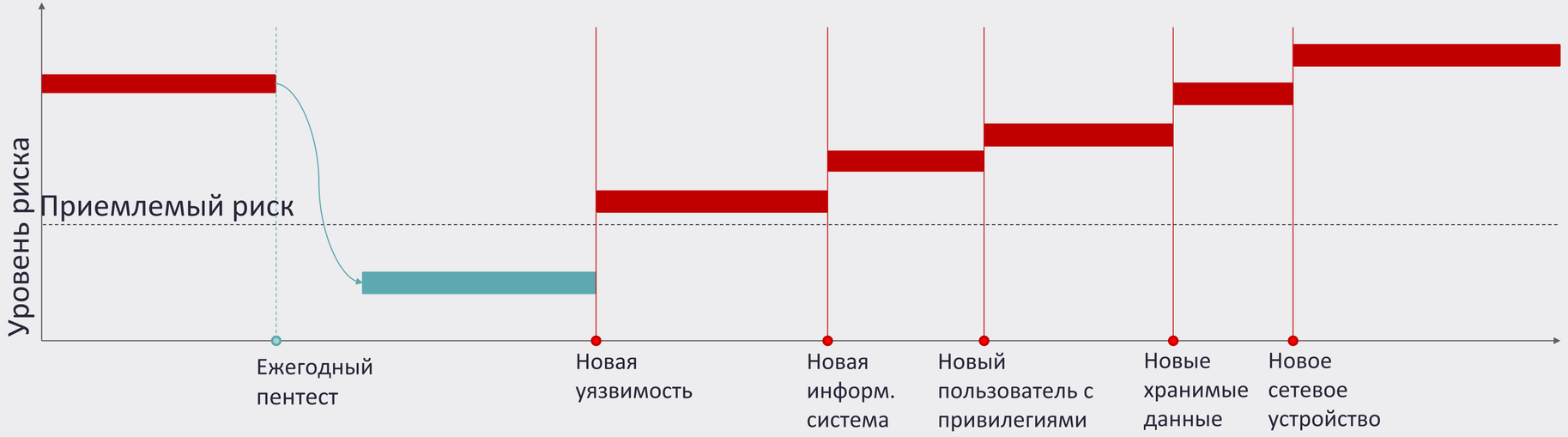


Разница между подходами

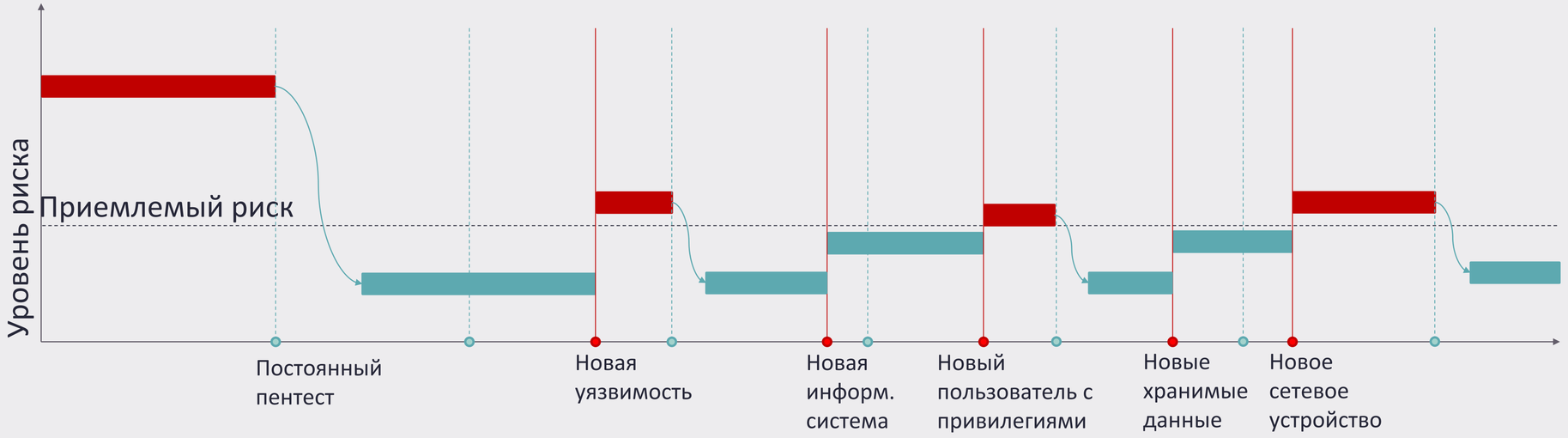


Важность непрерывного тестирования

Изменение уровня риска в случае ежегодного пентеста

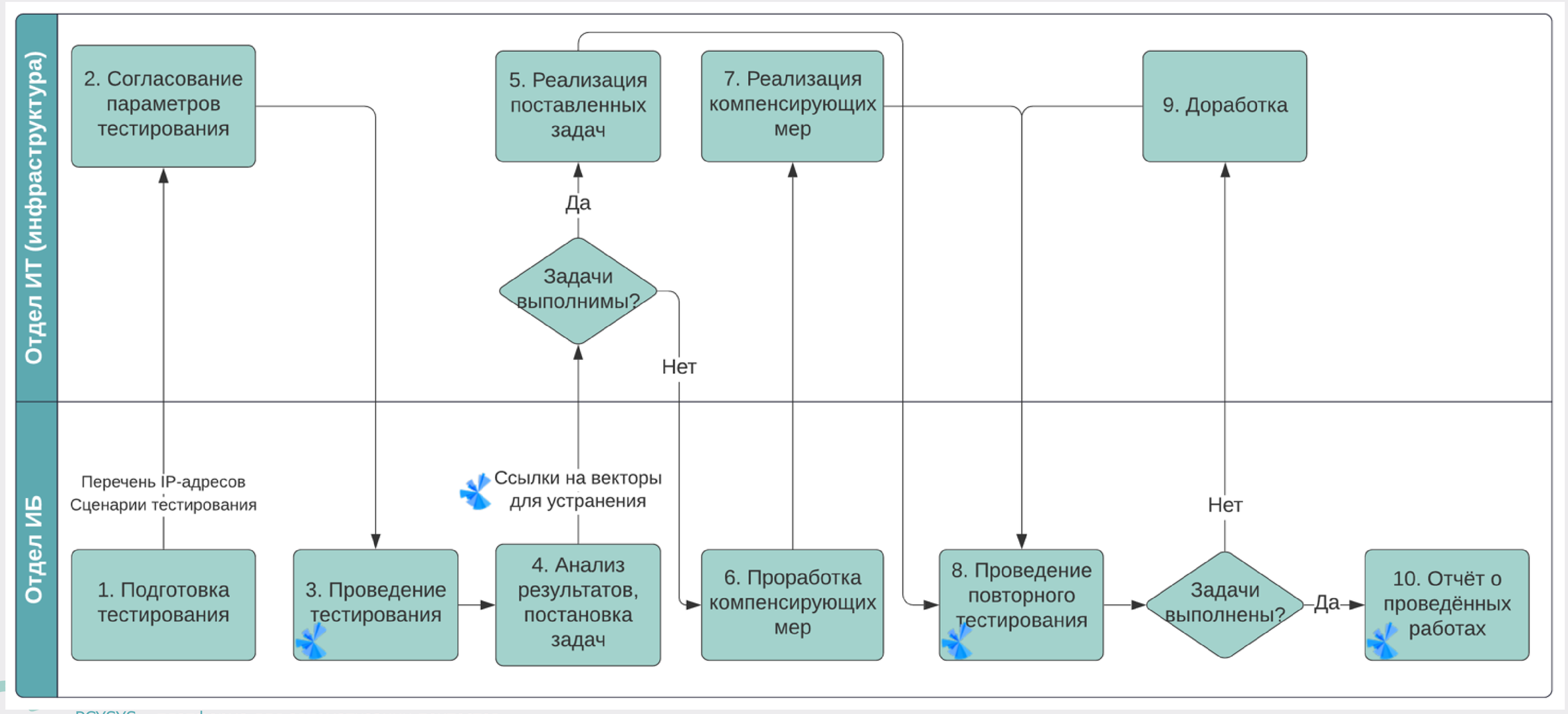


Изменение уровня риска в случае постоянного пентеста



Управление рисками/уязвимостями

Через автоматизацию пентеста



Отличия автопентеста от других решений

Автопентест vs Сканер уязвимостей

Возможности	Авто-ПТ	Сканер
• Соответствие требованиям регуляторов	✗	✓
• Теоретическая оценка риска	✗	✓
• Практическая оценка защищенности (фокус на реальных угрозах)	✓	✗
• Полные векторы атак	✓	✗
• Быстрые ценные результаты	✓	✗
• Экономический эффективный подход	✓	✗

https://citum.ru/blog/tpost/2uxlg0tvo1-gartner-ne-pitaites-ispravit-vsyo-sosred

Автопентест vs Ручной пентест

Возможности	Авто-ПТ	Ручной пентест
• Соответствие требованиям регуляторов (382-П)	✗	✓
• Тестирование веб-приложений	✗	✓
• Непрерывная оценка защищенности	✓	✗
• Тестирование в произвольном масштабе	✓	✗
• Быстрые ценные результаты	✓	✗
• Экономический эффективный подход	✓	✗

Автопентест vs Network PT Tools

Возможности	Авто-ПТ	NPTT
• Тестирование веб-приложений	✗	✓
• Тестирование собственных кастомных приложений	✗	✓
• Непрерывная оценка защищенности	✓	✗
• Тестирование в произвольном масштабе	✓	✗
• Быстрые ценные результаты	✓	✗
• Экономический эффективный подход	✓	✗

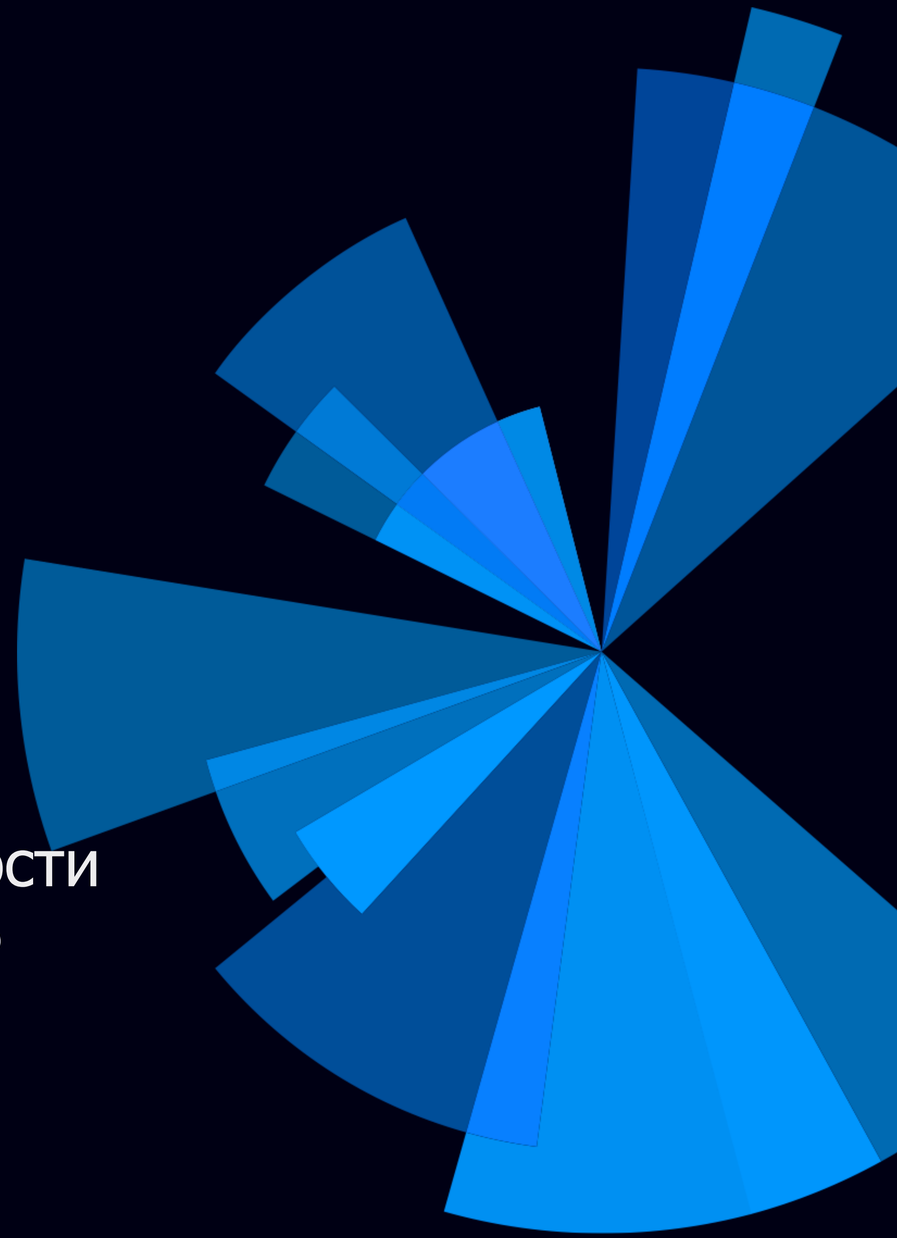
Автопентест vs Breach and Attack Simulation

Возможности	Авто-ПТ	BAS
• Тестирование периметра	✗	✓
• Тестирование настроек индивидуальных средств ИБ	✗	✓
• Практическая оценка защищенности (фокус на реальных угрозах)	✓	✗
• Анализ сети в произвольном масштабе	✓	✗
• Тестирование сети с учетом всех внедренных средств ИБ	✓	✗
• Без доступа в Интернет и разглашения информации	✓	✗

Выгоды PenTera

- Бизнес:
  - Экономически эффективное повышение защищенности сети
- ИТ/ИБ:
  - Практическая проверка безопасности сети
  - Приоритеты на основе реальных угроз
  - Снижение затрат на анализ защищенности
  - Снижение затрат на повышение защищенности
  - Эффективная коммуникация между ИТ и ИБ

https://citum.ru/blog/tpost/t0n118adt1-gartner-pcysys-cool-vendor-2020



Есть вопросы?

Мы готовы ответить:
vfilin@citum.ru
+7(903)765-3862