



Уязвимости и инструменты защиты технологических сетей

Алексей Анастасьев
aanastasev@ptsecurity.ru

ptsecurity.com

20 лет спустя...

6 Oct 2020 | 2020, Podcast



Dale Peterson @digitalbond · Sep 30

Are we past the air gap myth? What percentage of ICS asset owners still believe they have an air gap?



105 votes · Final results

Глобальные вызовы



- **Экономические**

Рост конкуренции, снижение спроса

- **Технологические**

Индустрия 4.0

- **Геополитические**

Санкции, закон о КИИ, импортозамещение

Может ИБ подождет? До сих пор без нее обходились же как-то?

«Готовь сани летом»

РТ



Цифровая трансформация инфраструктуры и процессов

Объект защиты постоянно меняется в ответ на бизнес вызовы.

Новые технологии – новые риски и уязвимости.



Кратный ежегодный прирост кибератак

Ежегодный прирост числа кибератак по разным оценкам колеблется в диапазоне 100%-2000%.

До 40% всех кибератак приходится на промышленность.



Высокий дефицит экспертизы в ИБ

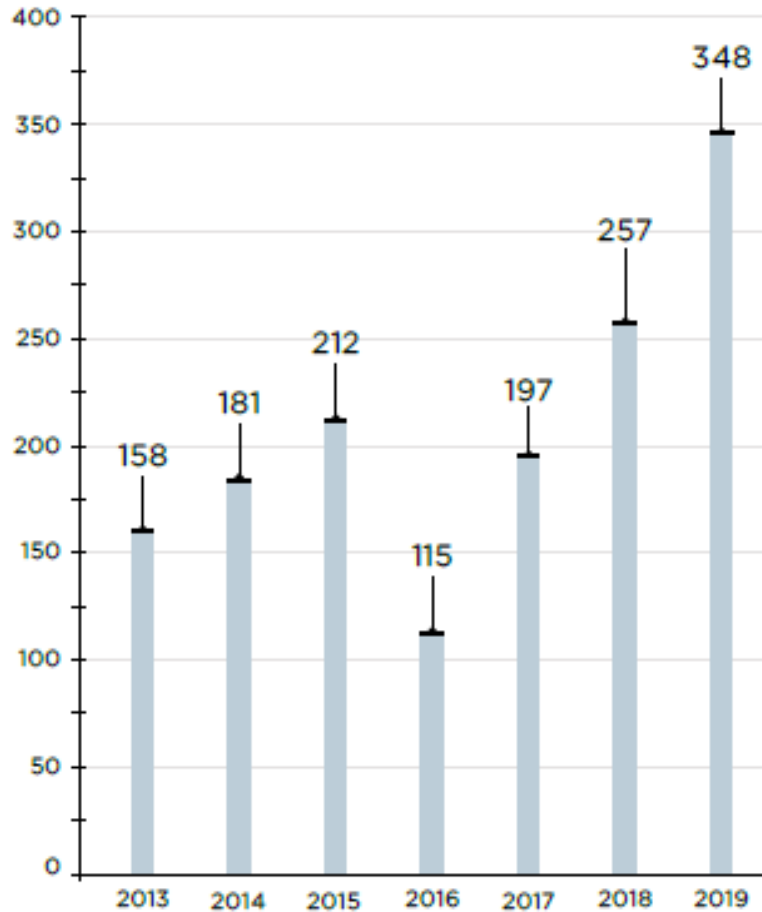
Сложность и количество кибератак растет.

Специалистов, способных создать эффективную систему защиты, катастрофически не хватает.

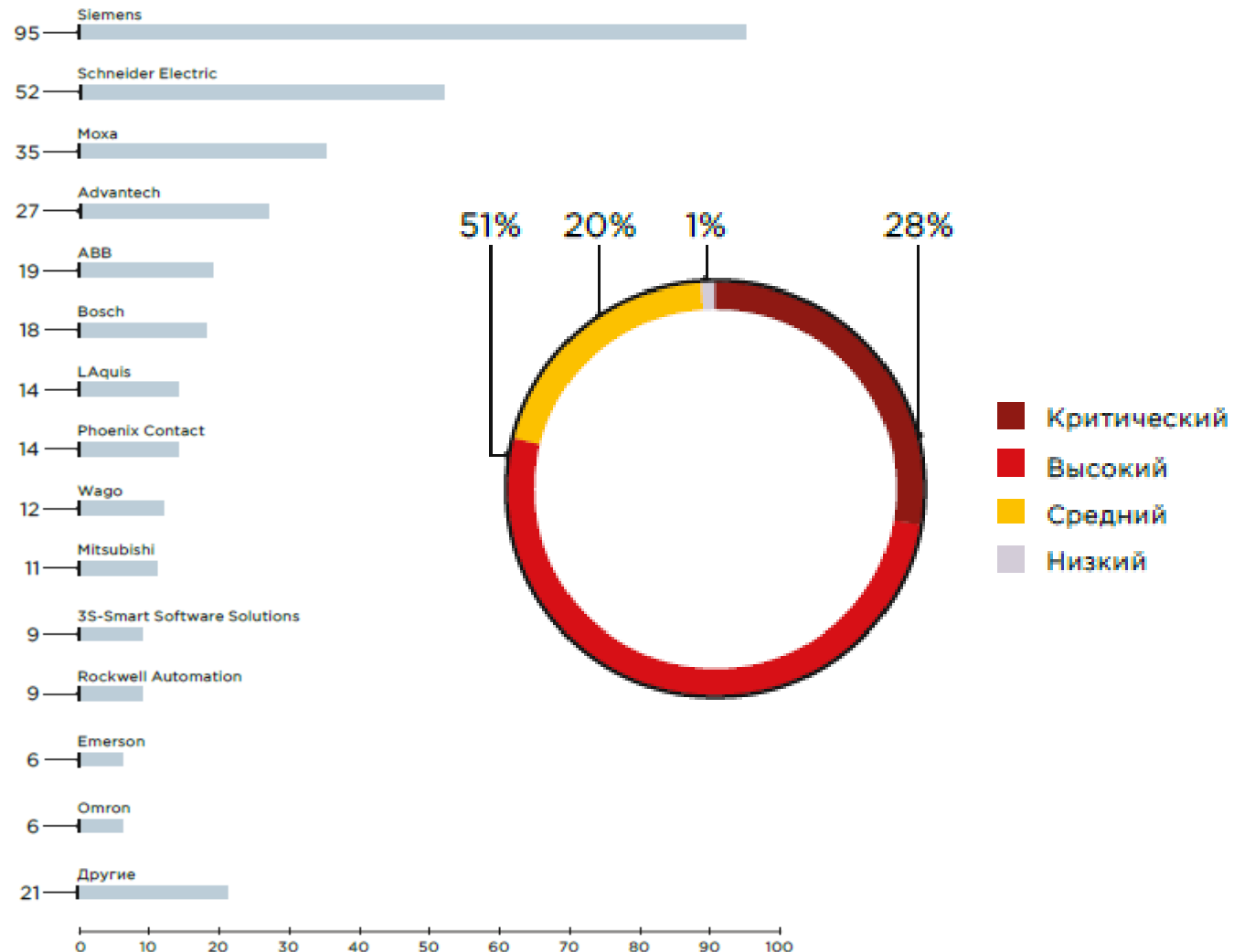
Уязвимость АСУ ТП



Количество опубликованных уязвимостей АСУ ТП:



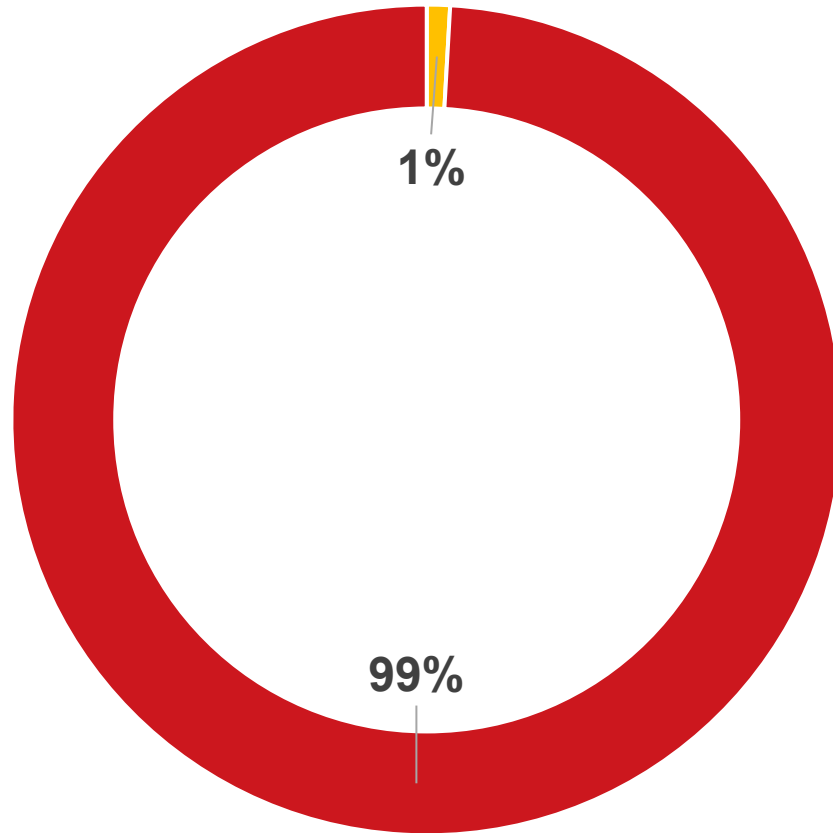
Распределение по вендорам и критичности:



Насколько продвинулись?



Емкость рынка промышленных NTA России > 1 трлн. руб.



- Реализовано проектов 2016-2020гг.
- Предстоит реализовать до 2020г

Путь к практической кибербезопасности

01 Сценарный анализ и определение ущерба

Практический семинар с разбором сценариев реализации масштабных кибератак и анализом их последствий



02 Верификация киберрисков и последствий

Формирование реестра возможных рисков кибербезопасности и их проверка путем имитации действий злоумышленников



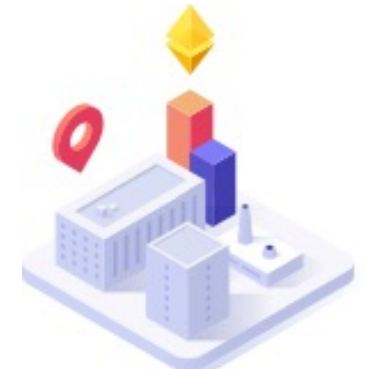
03 Формирование программы кибертрансформации

Определение целевого состояния и роадмапа результативной системы кибербезопасности



04 Киберучения и повышение устойчивости

Киберучения и внедрение мер, исключающих критичные для бизнеса риски



Платформа Positive Technologies



Технологии:

- **Промышленный сегмент** – ISIM, MS, MP8
- **Корпоративн. сегмент** – VM, NAD, WAF, AI
- **SOC** - MP SIEM
- **ГосСОПКА** - PT Ведомственный Центр

Экспертные сервисы и консалтинг:

- Тесты на проникновение
- Оценка уровня защищенности
- Управление уровнем защищенности
- Расследование инцидентов
- Консультации экспертов

Обучение:

- Учебные курсы
- Сертификация



Спасибо за внимание!

Алексей Анастасьев
aanastasev@ptsecurity.com

ptsecurity.com