РЕШЕНИЯ «ЛАБОРАТОРИИ КАСПЕРСКОГО» ДЛЯ ЗАЩИТЫ ИНДУСТРИАЛЬНОЙ СЕТИ

Алексей Лафицкий

СОДЕРЖАНИЕ

КИБЕР УГРОЗЫ

СПЕЦИФИКА АСУТП

РЕШЕНИЯ «ЛАБОРАТОРИИ КАСПЕРСКОГО»

КИБЕР УГРОЗЫ

СПЕЦИФИКА АСУТП

РЕШЕНИЯ «ЛАБОРАТОРИИ КАСПЕРСКОГО»

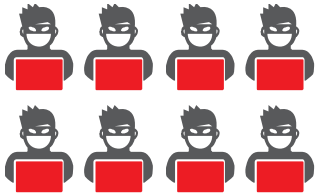
KASPERSKY lab

АТАКИ НА ИНДУСТРИАЛЬНЫЕ ОБЪЕКТЫ

Тенденция увеличения количества инцидентов в АСУ ТП (ICS-CERT):

2012

198 инцидента

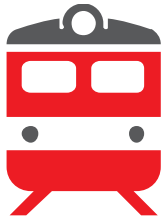


2013

~400 инцидентов

Чаще атакуют:

Нефте-Газ, Энергетика (Гидро и Атом)



Транспорт

Цель – получить доступ к SCADA и PLC

KASPERSKY lab

КИБЕР УГРОЗЫ ПО ВЕРТИКАЛЯМ

19%

Другие

6% Транспорт
5% Связь
4% Водоснабжение
3% Здания, Склады
1% Почта

17%

Производство

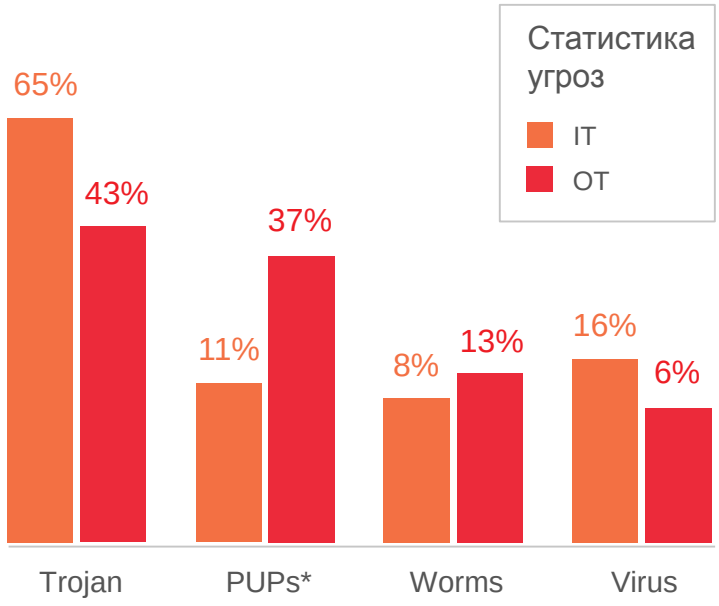
64%

Энергетика

Источник: ICS-CERT, 2013

KASPERSKY lab

ЧТОБЫ СТАТЬ ЖЕРТВОЙ НЕ НУЖНО БЫТЬ ЦЕЛЬЮ



Источник: Kaspersky Security Network

***PUPs — Potentially unwanted programs**

Рядовое вредоносное ПО

Многие АСУ не обновляются и уязвимы даже для старых угроз, таких как Kido

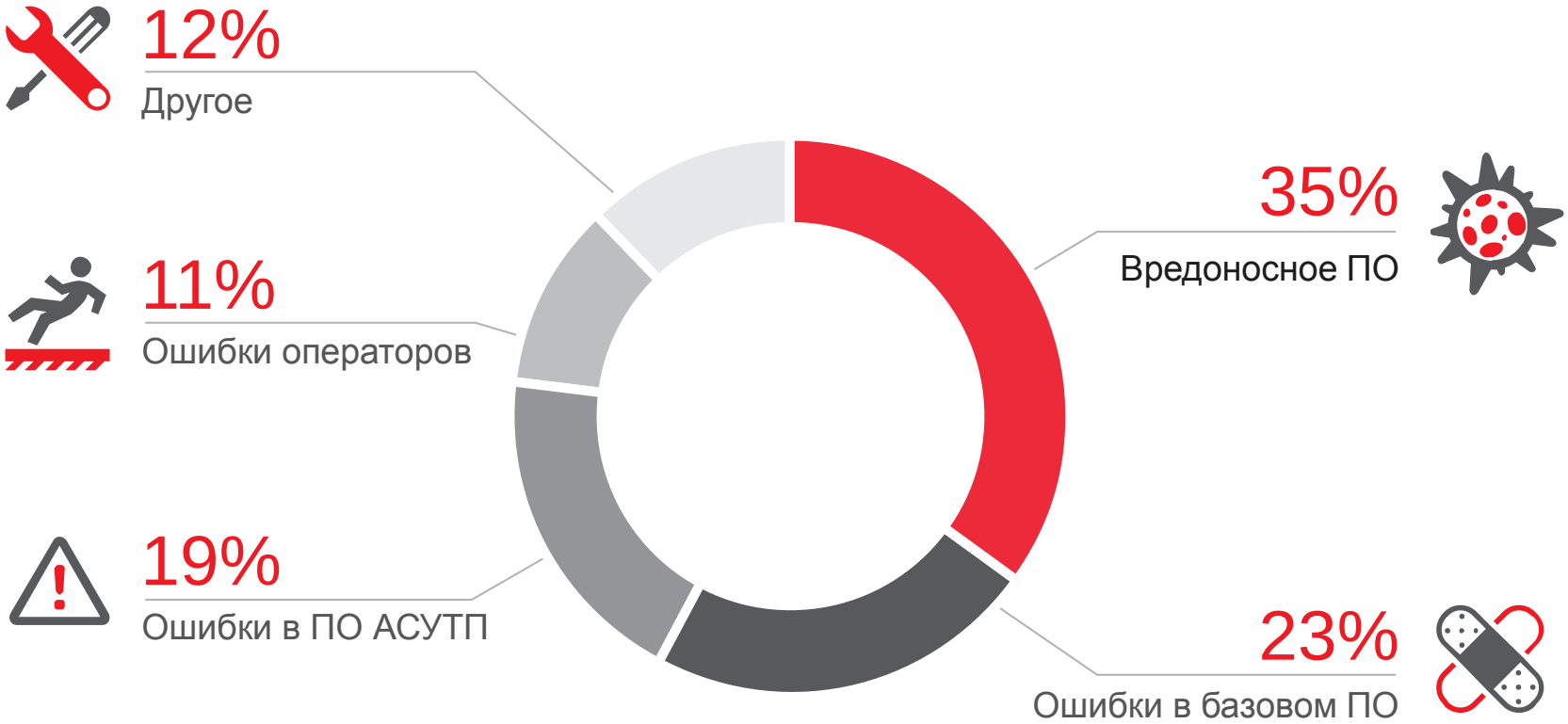
Таргетированые атаки (APT)

Duqu, Flame, Gauss, Energetic Bear, Epic Turla

Кибер-оружие

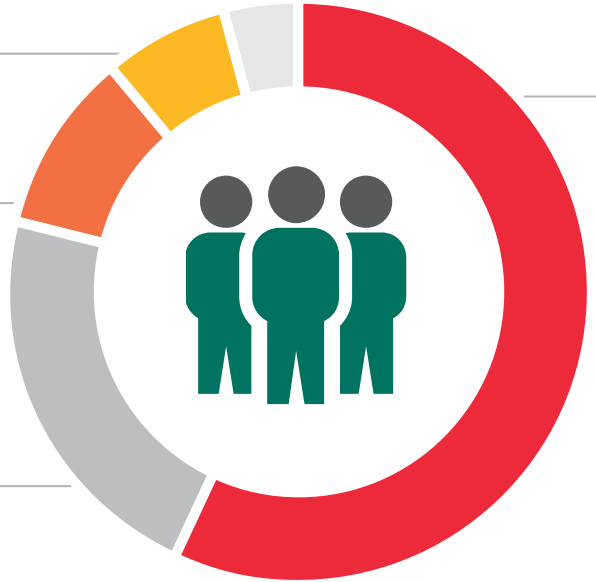
Stuxnet

ПРИЧИНЫ ИНЦИДЕНТОВ



Источник: RISI Annual Summary 2013

ЧЕЛОВЕЧЕСКИЙ ФАКТОР



4%
Зарубежные исполнители

7%
Бывшие сотрудники

10%
Внешние подрядчики

22%
Текущие сотрудники

57%
нарушение регламента

Source: RISI Annual Summary 2013

KASPERSKY lab

ВРЕМЯ ПРОСТОЯ В РЕЗУЛЬТАТЕ ИНЦИДЕНТА

Источник: RISI Annual Summary 2013

КИБЕР
УГРОЗЫ

**СПЕЦИФИКА
АСУТП**

РЕШЕНИЯ
«ЛАБОРАТОРИИ
КАСПЕРСКОГО»

РАЗЛИЧИЕ В ПОДХОДАХ

АСУТП

1. Доступность
2. Целостность
3. Конфиденциальность

Corporate Network

1. Конфиденциальность
2. Целостность
3. Доступность

- «Офисная» информационная безопасность – это защита данных.
- Промышленная кибербезопасность – это защита непрерывности процесса и управления

KASPERSKY lab

КИБЕР
УГРОЗЫ

СПЕЦИФИКА
АСУТП

РЕШЕНИЯ «ЛАБОРАТОРИИ КАСПЕРСКОГО»

КОМПЛЕКСНОЕ РЕШЕНИЕ ДЛЯ АСУ ТП

LEVEL 4

Business planning and logistics

ERP

LEVEL 3

Manufacturing Operations management

MES

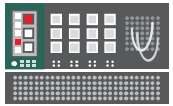
LEVEL 2, 1

Batch Control.

Continuous Control.

Discrete Control.

SCADA



ПЛК / РЗА

LEVEL 0

Physical

Полевые устройства

KASPERSKY lab

ЗАЩИТА РАБОЧИХ СТАНЦИЙ, HMI И СЕРВЕРОВ

LEVEL 4

Business planning and logistics

ERP

LEVEL 3

Manufacturing Operations management

MES

LEVEL 2, 1

Batch Control.

Continuous Control.

Discrete Control.

SCADA

ПЛК / РЗА

LEVEL 0

Physical

Полевые устройства

РАБОЧИЕ СТАНЦИЙ, HMI И СЕРВЕРЫ

ВЕКТОРЫ АТАК

- Уязвимое ПО (OS, SCADA, и т.д.) используемые в технологических сетях
- Доступ к ERP/MES системам или Интернет
- Неконтролируемое использование приложений операторами / инженерами
- Неавторизованное подключение 3G модемов/точек доступа
- Неконтролируемое использование внешних устройств (USB, SATA, и т.д.)
- Доступ контрагентов/подрядчиков к технологическим площадкам, возможные неконтролируемые действия

KASPERSKY lab

KASPERSKY INDUSTRIAL CYBER SECURITY

- Разработано специально для применения в среде АСУ ТП
  - Оптимизированное потребление ресурсов
  - Политика обновлений адаптированная к требованиям АСУ ТП
  - Передача уведомлений операторам АСУ ТП (МЭК 60870-5-104, OPC 2.0 DA)
  - Протестировано на совместимость с ПО АСУ ТП
- Обеспечение замкнутой среды (белые списки)
  - Контроль запуска приложений
  - Контроль внешних устройств
- Проактивная / сигнатурная антивирусная защита
- Обнаружение уязвимостей программной среды
- Контроль целостности проектов ПЛК

ТЕХНОЛОГИЧЕСКАЯ СЕТЬ

LEVEL 4

Business planning and logistics

ERP

LEVEL 3

Manufacturing Operations management

MES

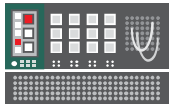
LEVEL 2, 1

Batch Control.

Continuous Control.

Discrete Control.

SCADA



ПЛК / РЗА

LEVEL 0

Physical

Полевые устройства

ЗАЩИТА ТЕХНОЛОГИЧЕСКОЙ СЕТИ

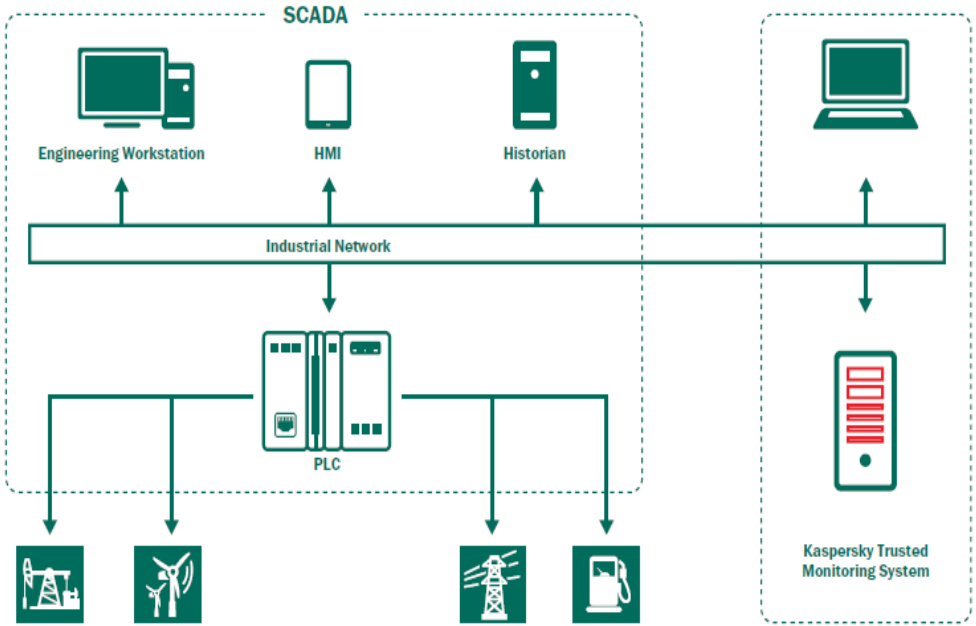
ВЕКТОРЫ АТАК

- Неконтролируемые действия контрагентов/подрядчиков на технологических площадках;
- Доступ к ERP/MES системам или Интернет
- **Несанкционированное подключение устройств к сети;**
- **Нелегитимное переконфигурирование устройств;**
- **Отправка нелегитимных управляющих команд, нарушающих ТП;**

KASPERSKY lab

KASPERSKY INDUSTRIAL CYBER SECURITY

- Пассивный анализ трафика без влияния на АСУ ТП
- Мониторинг целостности сети
- Анализ сетевого трафика на уровне логики технологического процесса
- Поддержка различных индустриальных протоколов
- Поддержка различных ПЛК / РЗА и ПО АСУ ТП



ОСНОВНЫЕ ЗАДАЧИ

- **Контроль целостности сети**
  - Идентификация устройств в сети.
  - Идентификация «легитимных» сетевых коммуникаций
  - Обнаружение новых устройств в режиме реального времени.
  - Уведомление о подключении новых устройств.
- **Контроль целостности PLC**
  - Оповещение о попытках изменениях PLC.
  - Обнаружение команд на переконфигурирование (остановку / перезагрузку / пр).

- **Обнаружение сетевых аномалий**
  - Детектирование нелегитимных команд и сетевого трафика, выводящих из строя системы управления (SCADA, HMI, PLC).

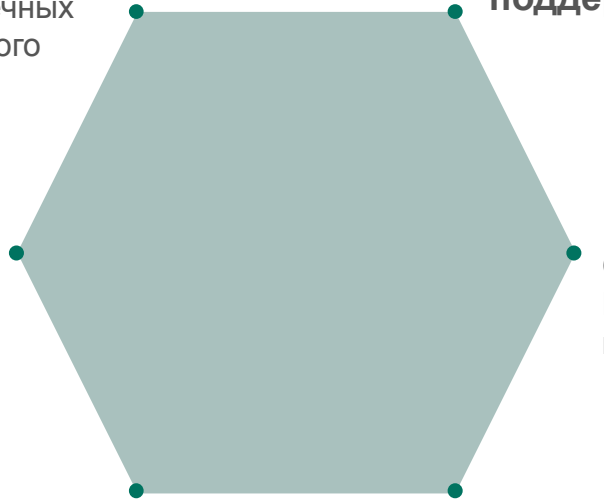
- **Обнаружение управляющих команд, приводящих к нарушению технологического процесса**
  - Обнаружение команд, устанавливающих недопустимые/нежелательные значения ключевых параметров управления технологическим процессом

СТРУКТУРА КОМПЛЕКСНОГО ПРЕДЛОЖЕНИЯ

Технологии защиты АСУ ТП
контроль целостности конечных узлов, сети, технологического процесса

Обслуживание и техническая поддержки

Для регулирующих органов
Консультирование и экспертиза по разработке отраслевых стандартов и регулирующих документов



Профессиональные сервисы
Обучение Оценка защищённости Раннее оповещение Расследование инцидентов Управляемая защита

Для интеграторов
Оценка информационной безопасности, Разработка безопасной архитектуры, Раннее оповещение

Для разработчиков
Embedded security (KOS, KSS, KSH) Разработка безопасной архитектуры

СПАСИБО