
# Ландшафт угроз для систем промышленной автоматизации

Петухов Алексей

Руководитель направления KICS
Alexey.Petukhov@kaspersky.com
Tel: +7 (963) 686 07 83

## ICS-CERT

**Данные об угрозах, Специальные отчеты**

Kaspersky®
Threat Intelligence

**Тренинг по тесту на проникновение**

Kaspersky®
Security Awareness

**Тренинг по поиску уязвимостей**

Kaspersky®
Security Awareness

## (ICS) SOC

**Услуга по мониторингу и реагированию**

Kaspersky®
Managed Protection

**Интеграция с SIEM**

**Тренинг по расследованиям**

Kaspersky®
Security Awareness

**Реагирование на инциденты**

Kaspersky®
Incident Response

## Площадка/Предприятие

**Тесты на проникновение**

Kaspersky®
Security Assessment

**Защита конечных узлов Мониторинг сетей**

KICS
for Nodes

KICS
for Networks

**Повышение осведомленности**

Kaspersky®
Security Awareness

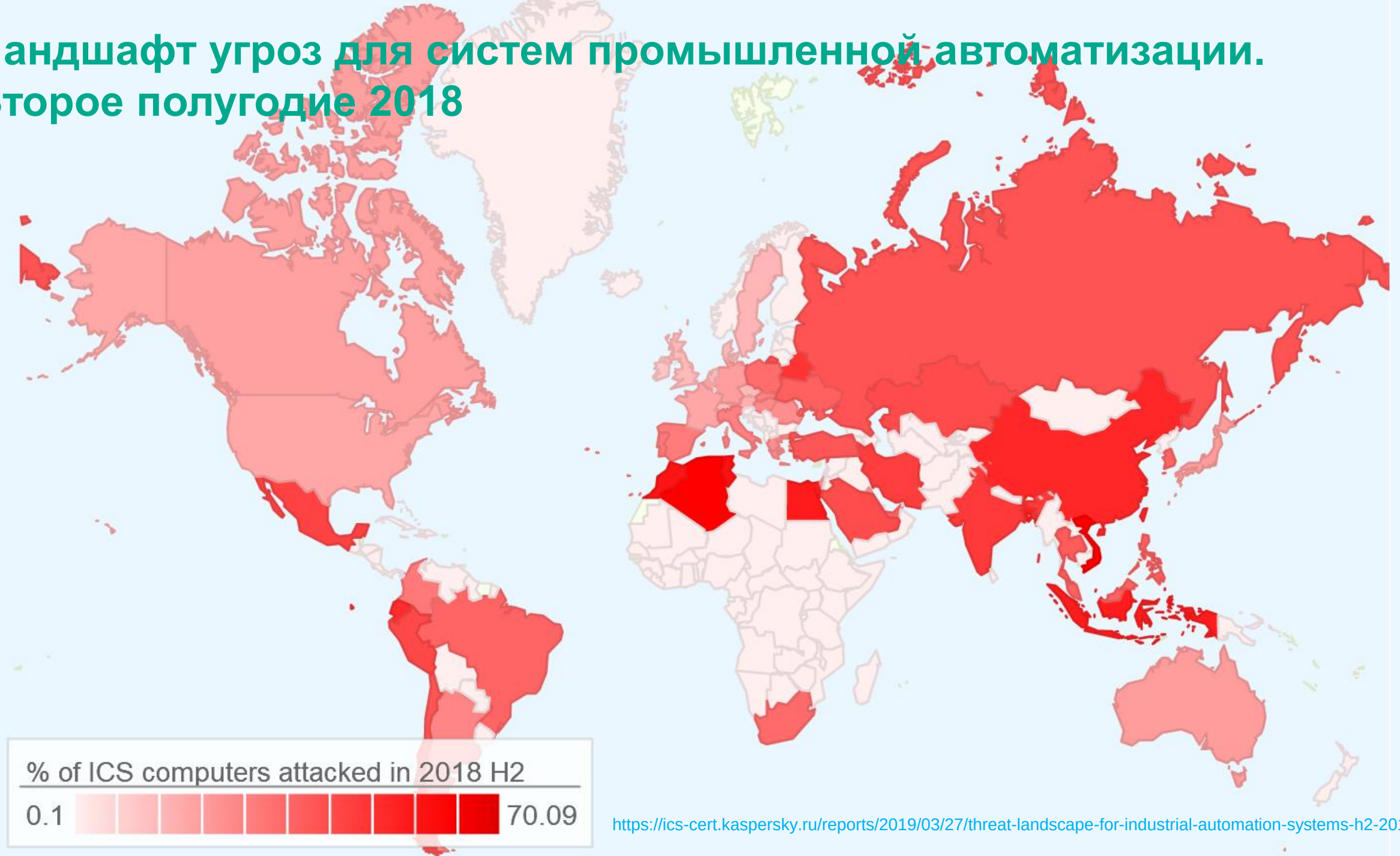
**Реагирование на инциденты**

Kaspersky®
Incident Response

10 YEARS JETSECURITY CONFERENCE 2019

KASPERSKY lab

# Ландшафт угроз для систем промышленной автоматизации. Второе полугодие 2018



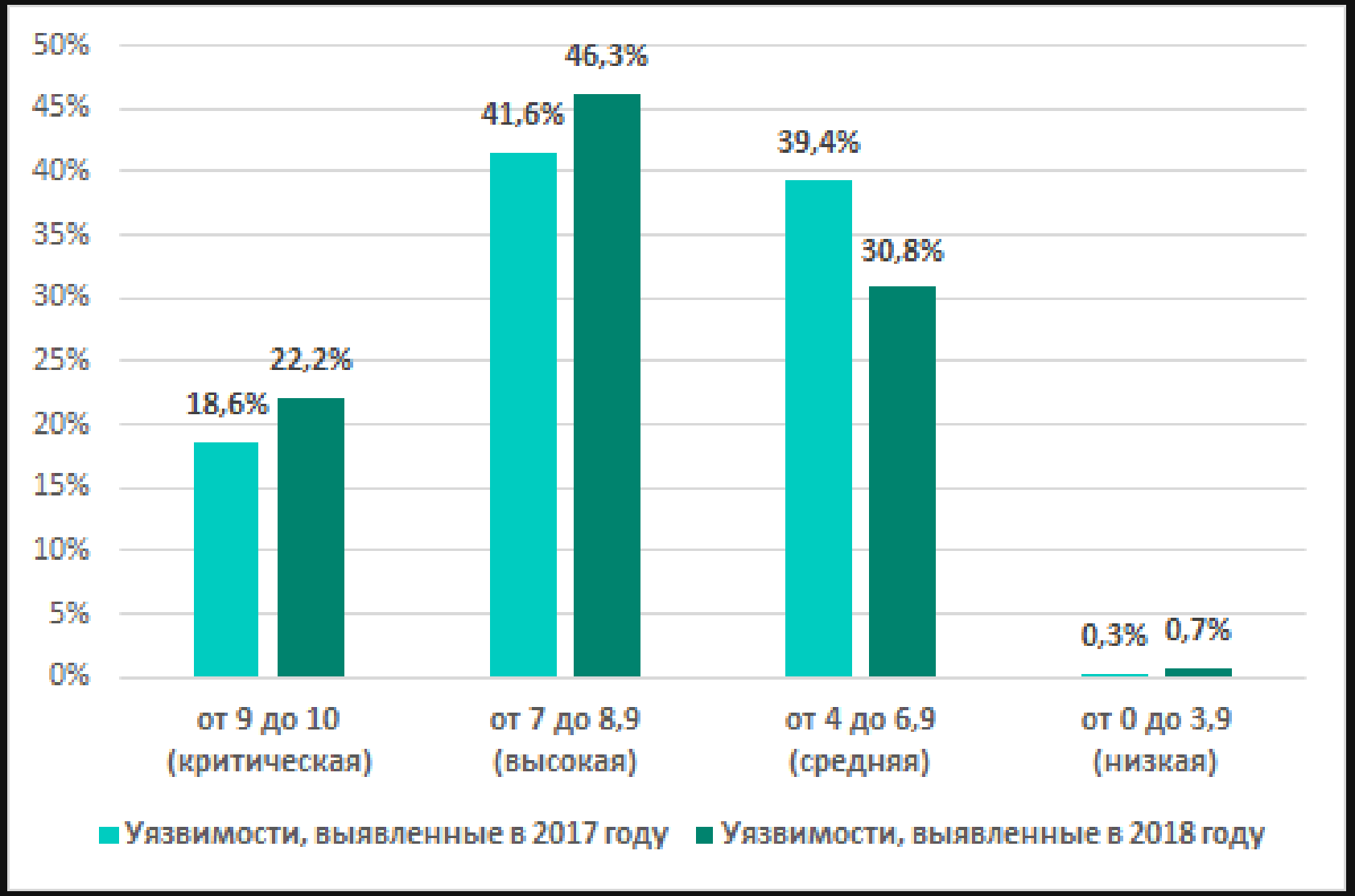

https://ics-cert.kaspersky.ru/reports/2019/03/27/threat-landscape-for-industrial-automation-systems-h2-2018/

# Количество и степень риска выявленных уязвимостей

**415**

**обнаруженных уязвимостей**

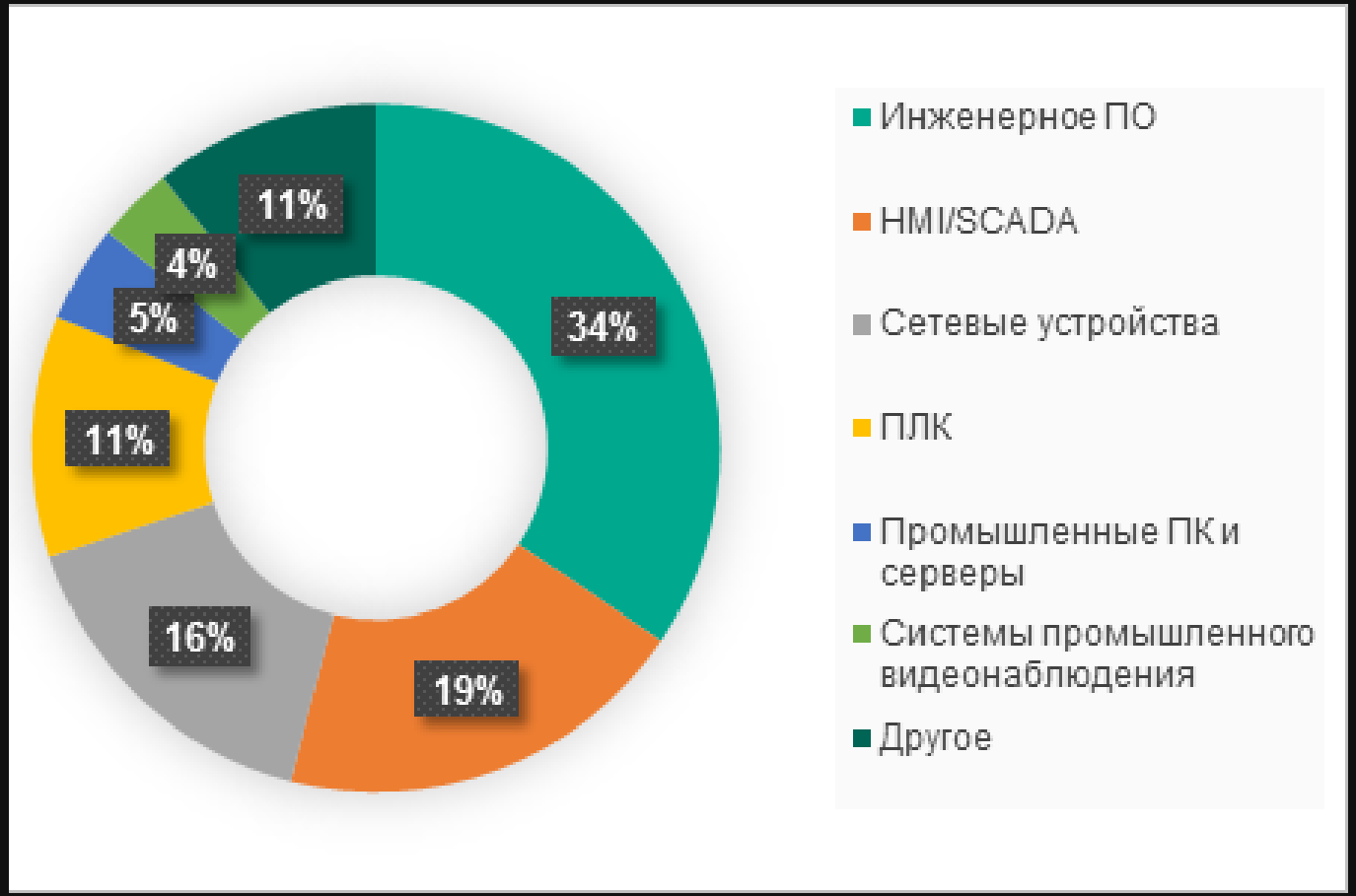
(vs 322 в 2017)



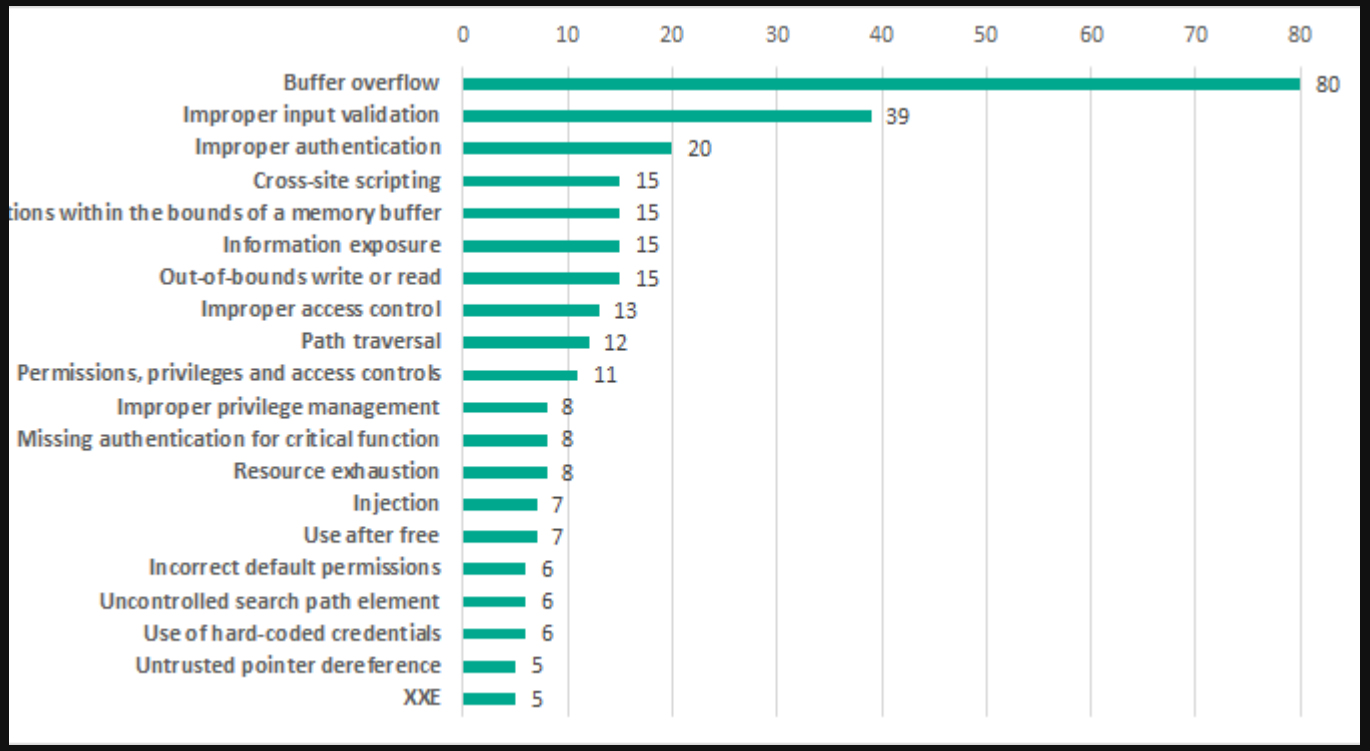
# Распределение уязвимостей

## Критичность 10 баллов

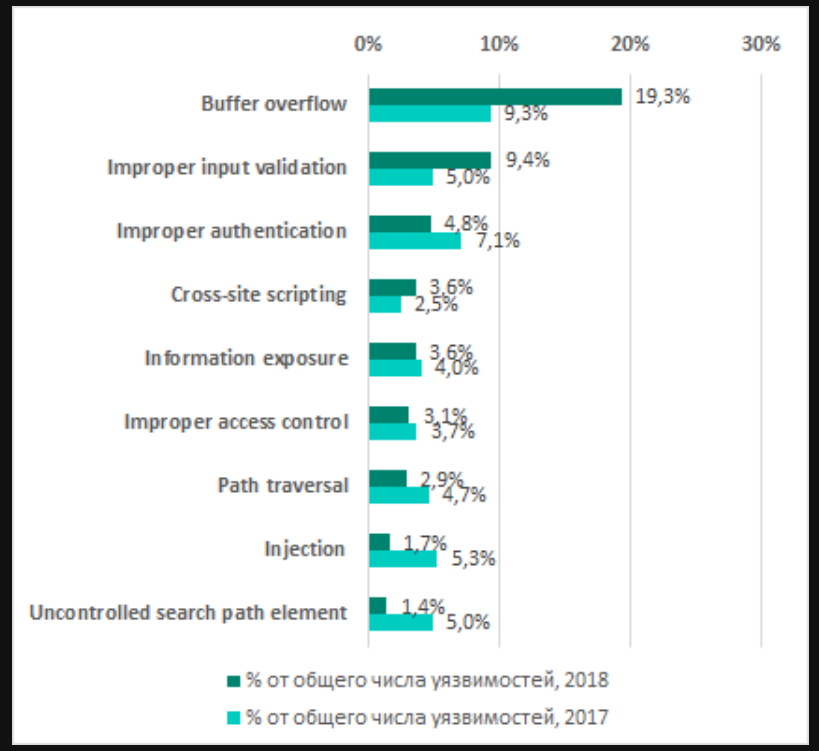
Siemens TIM 1531 IRC Modules
Siemens SINUMERIK Controllers
Circontrol CirCarLife
NUUO NVRmini2 and NVRsolo
Emerson AMS Device Manager
Rockwell Automation RSLinx Classic
Schneider Electric U.motion Builder
Martem TELEM-GW6/GWM



# Типы выявленных уязвимостей

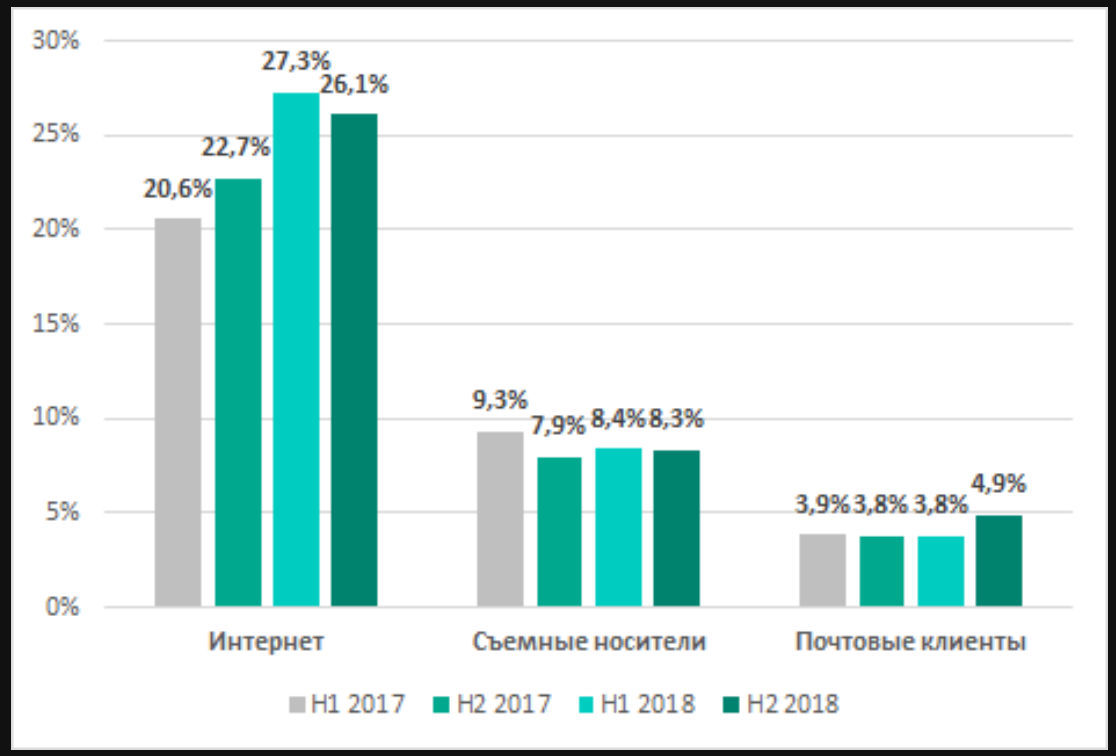



Наиболее распространенные типы уязвимостей. Уязвимости, опубликованные в 2018 году

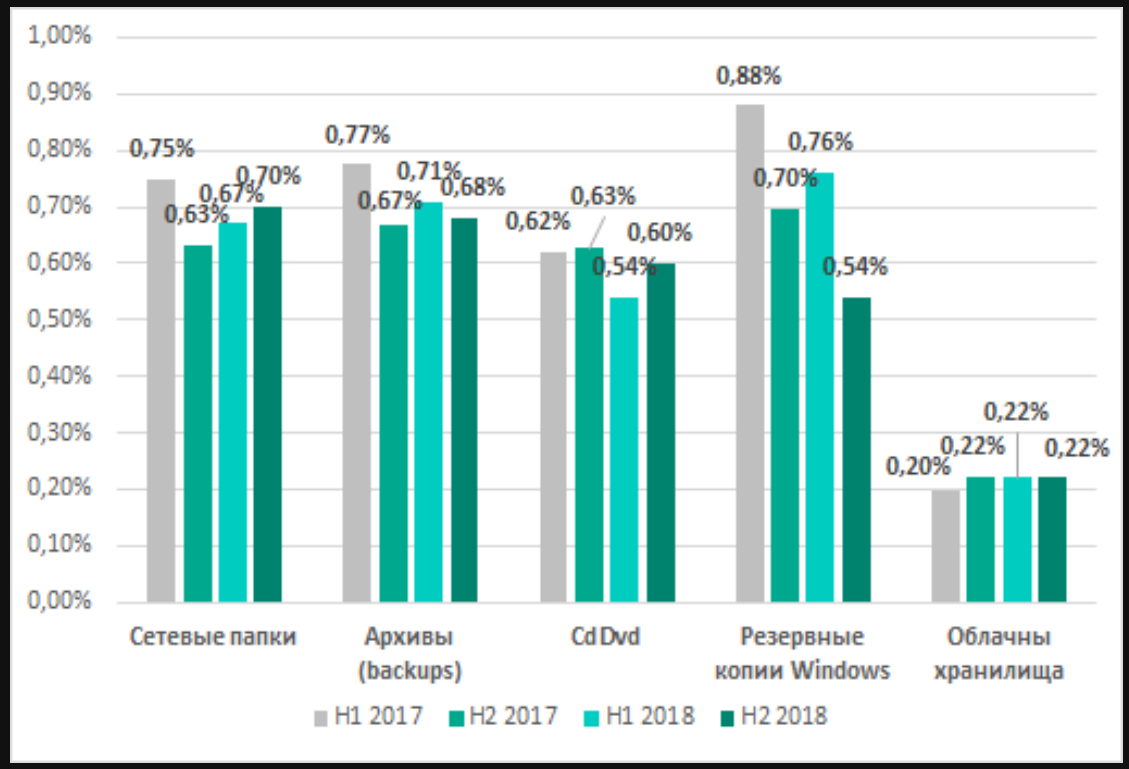



Процент уязвимостей различных типов от общего числа уязвимостей, сравнение 2018 года с 2017 годом

# Источники заражения

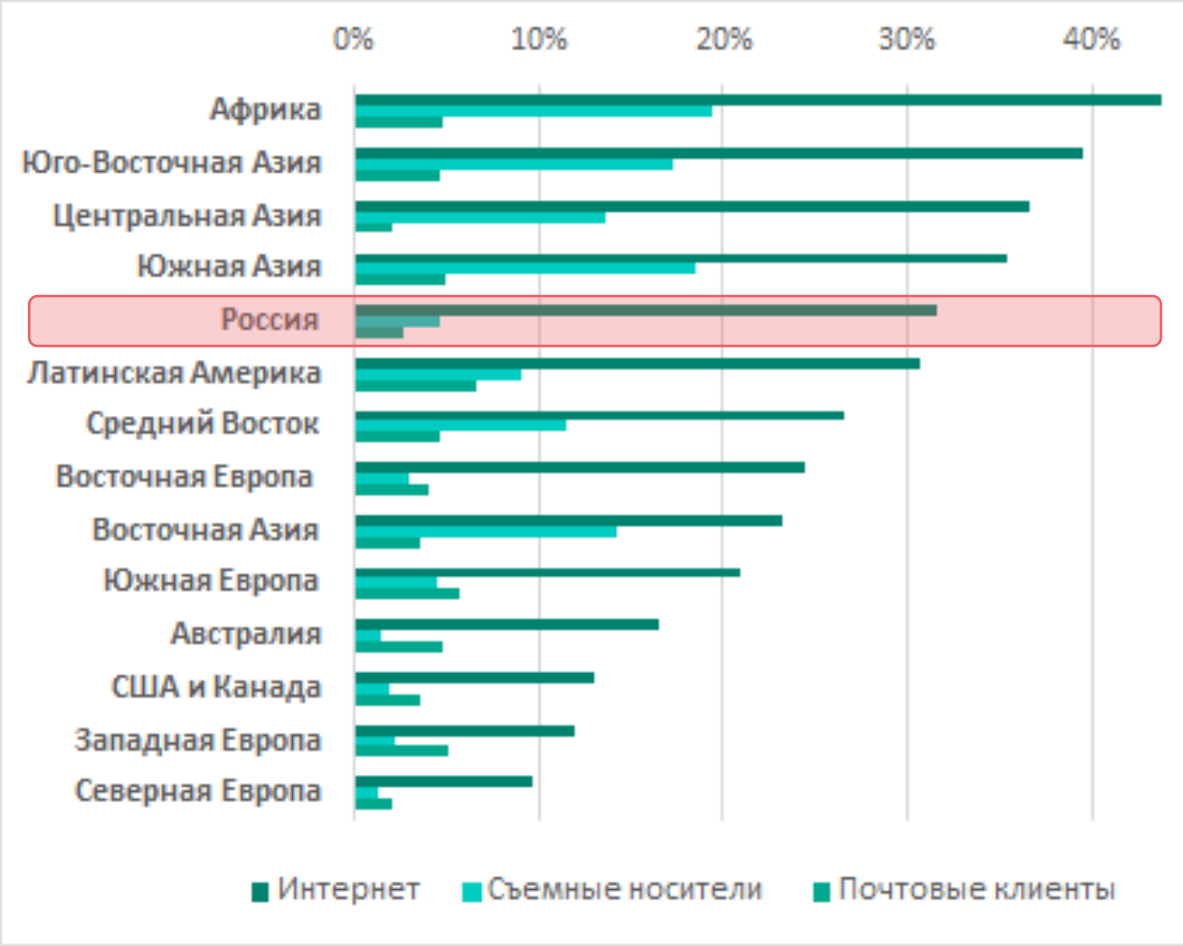



Основные источники угроз, заблокированных на компьютерах АСУ*, по полугодиям

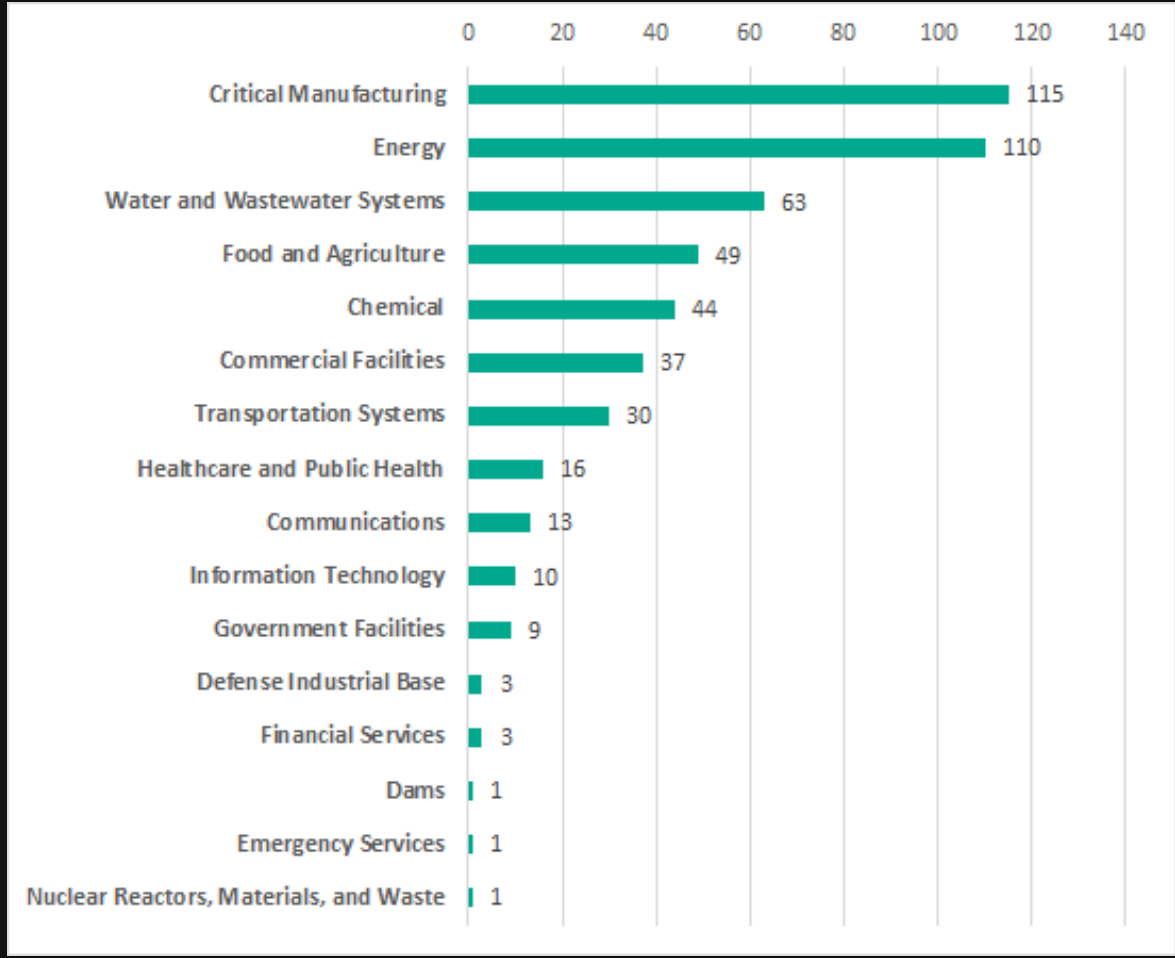



Минорные источники угроз, заблокированных на компьютерах АСУ, по полугодиям

## Основные источники угроз в регионах




## Анализ по отраслям



# Крупные кибератаки 2018/2019

# Целевые кибератаки

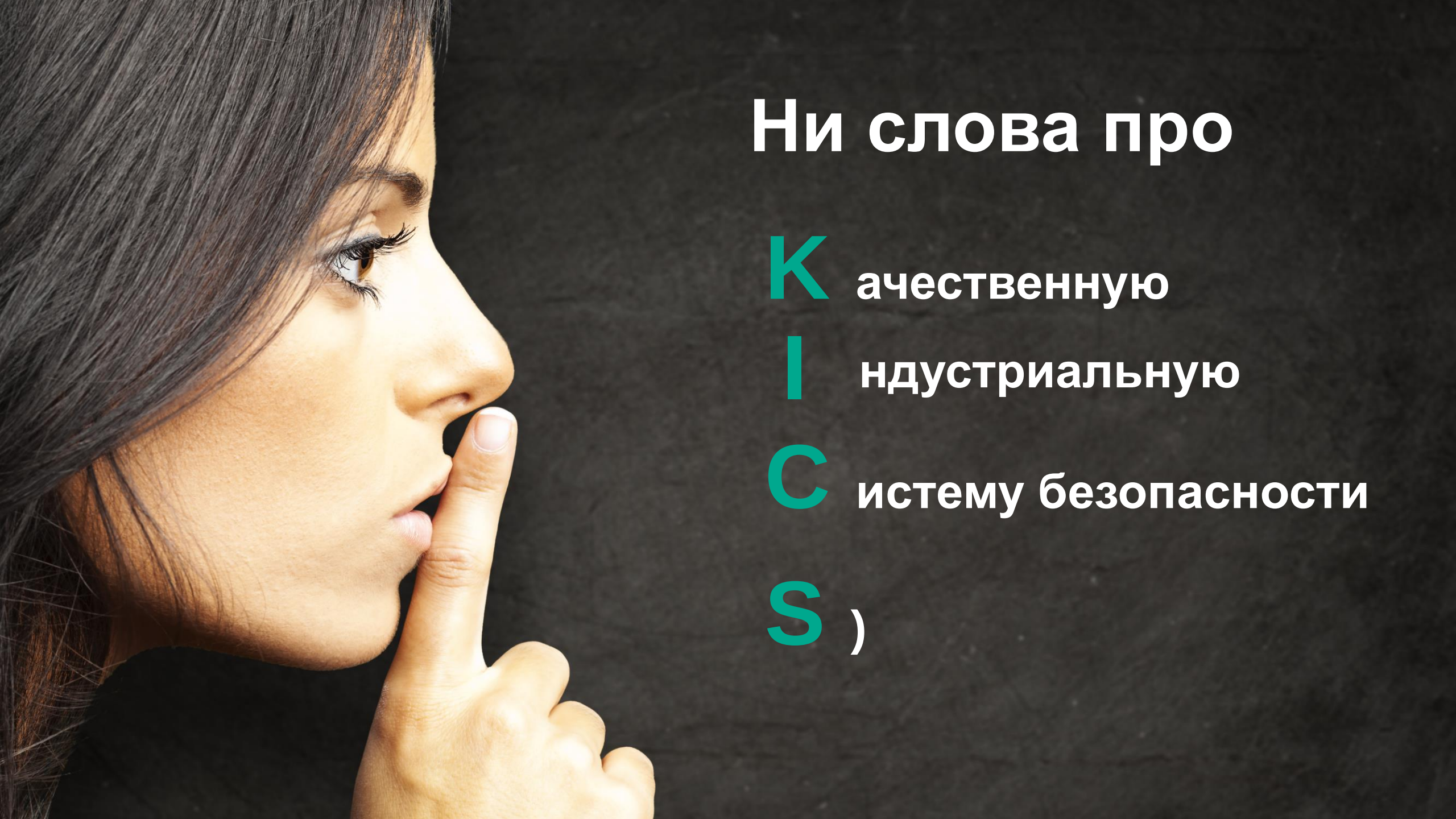
Президент **Мадуро** заявил, что **после кибератак США использовали диверсантов и даже ЭМИ-оружие**, электромагнитные импульсы которого препятствовали восстановлению нормальной работы сети. По его словам, случившееся возгорание и взрыв на одной из крупнейших подстанций – точно дело рук диверсантов.

Оппозиция и сами США уверяют, что «режим» сам всё и испортил-отключил. Такие заявления очень похожи на украинские сказки о том, как жители Донбасса сами себя обстреливают. Но хорошо известно, что у американцев в методичке по организации «цветных майданов» сказано **о диверсиях против[end_short_text] энергетики страны**.

Так что кибератаки, скорее всего, действительно были. Это стало возможным по следующим причинам – станции и оборудование сетей, в том числе **компьютерные системы управления** в стране, оснащены в основном американским, реже французским и иным оборудованием. Всё это закупалось или при марионеточных режимах, или в начале эры Чавеса. Тогда никаких санкций США не было и в помине – отношения с Вашингтоном были нормальными. А сейчас местные спецслужбы не смогли обеспечить нормальной защиты от проникновения в эти сети вражеских хакеров. Американцы, достаточно хорошо знающие, что они туда поставили, смогли преодолеть защиту.

http://argumenti.ru/society/2019/03/605319?typelink=openlink


S. GÄRTNER
the production people, and from technical customer service.
Hydro
HYDRO


Ни слова про
Качественную
Индустриальную
Систему безопасности
(ICS)

10 YEARS JETSECURITY CONFERENCE 2019

# СПАСИБО ЗА ВНИМАНИЕ!

Петухов Алексей

Руководитель направления KICS
Alexey.Petukhov@kaspersky.com
Tel: +7 (963) 686 07 83

KASPERSKY lab