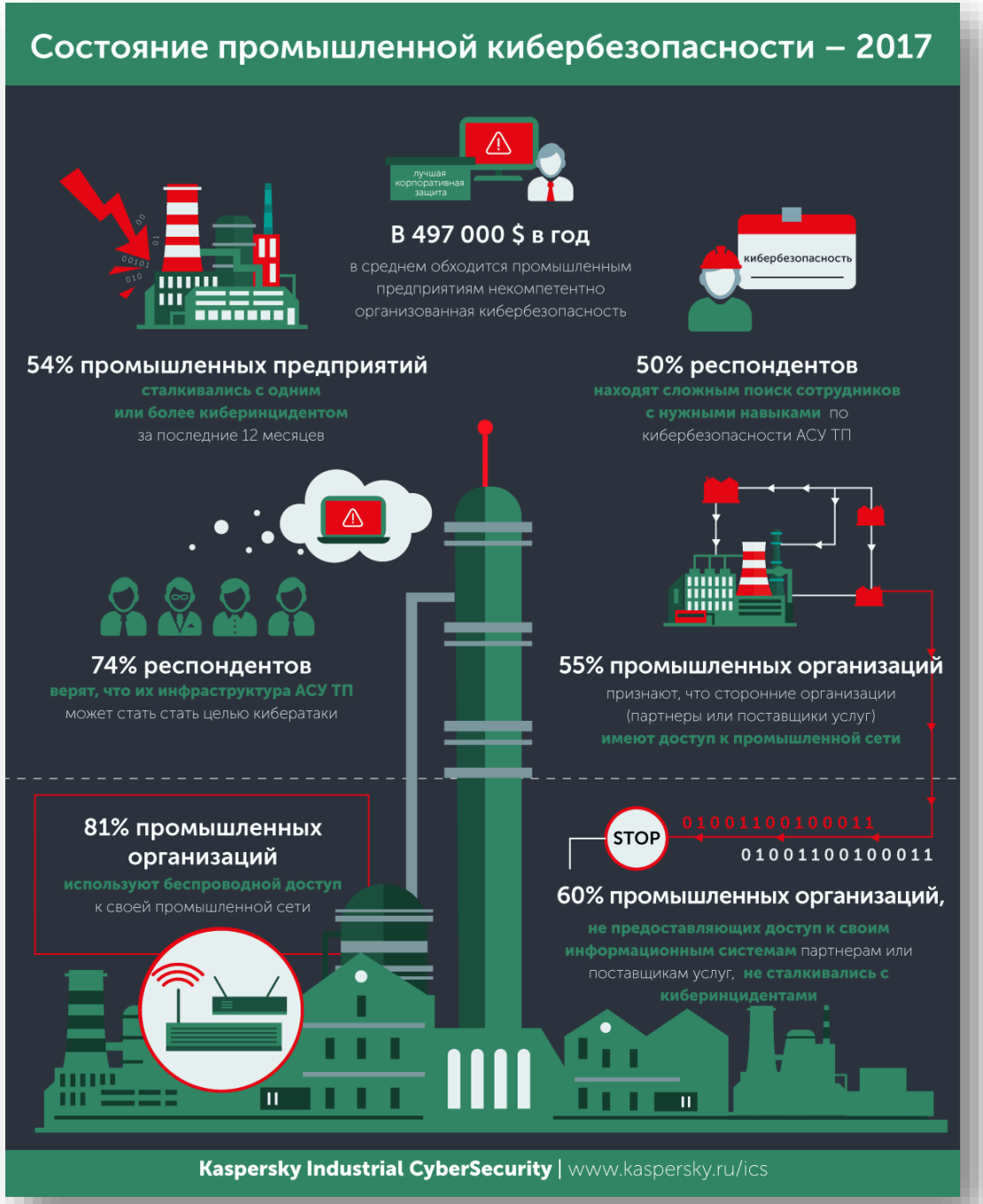
Результаты глобального исследования Лаборатории Касперского о состоянии промышленной кибербезопасности в различных отраслях

KASPERSKY lab

Цель исследования

1. Общее понимание проблем безопасности АСУ ТП в мире
2. Обзор мер безопасности АСУ ТП
3. Обзор инцидентов безопасности в АСУ ТП

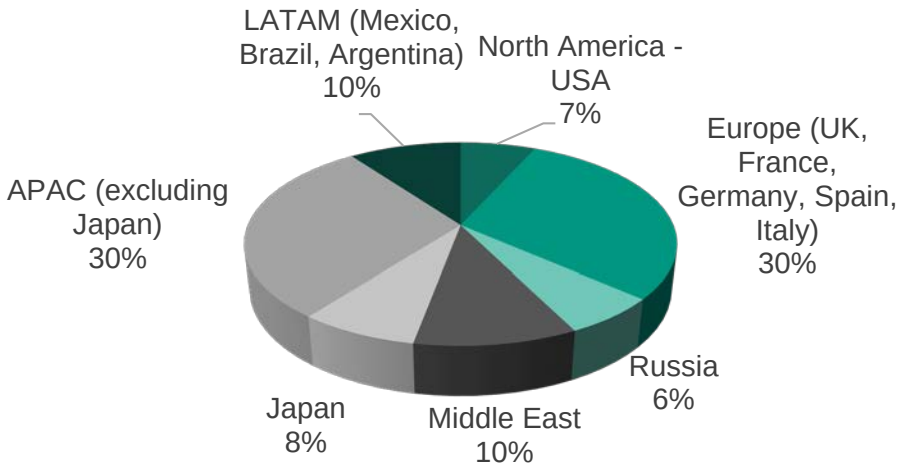
https://blog.kaspersky.ru/ics-report-2017/17812/



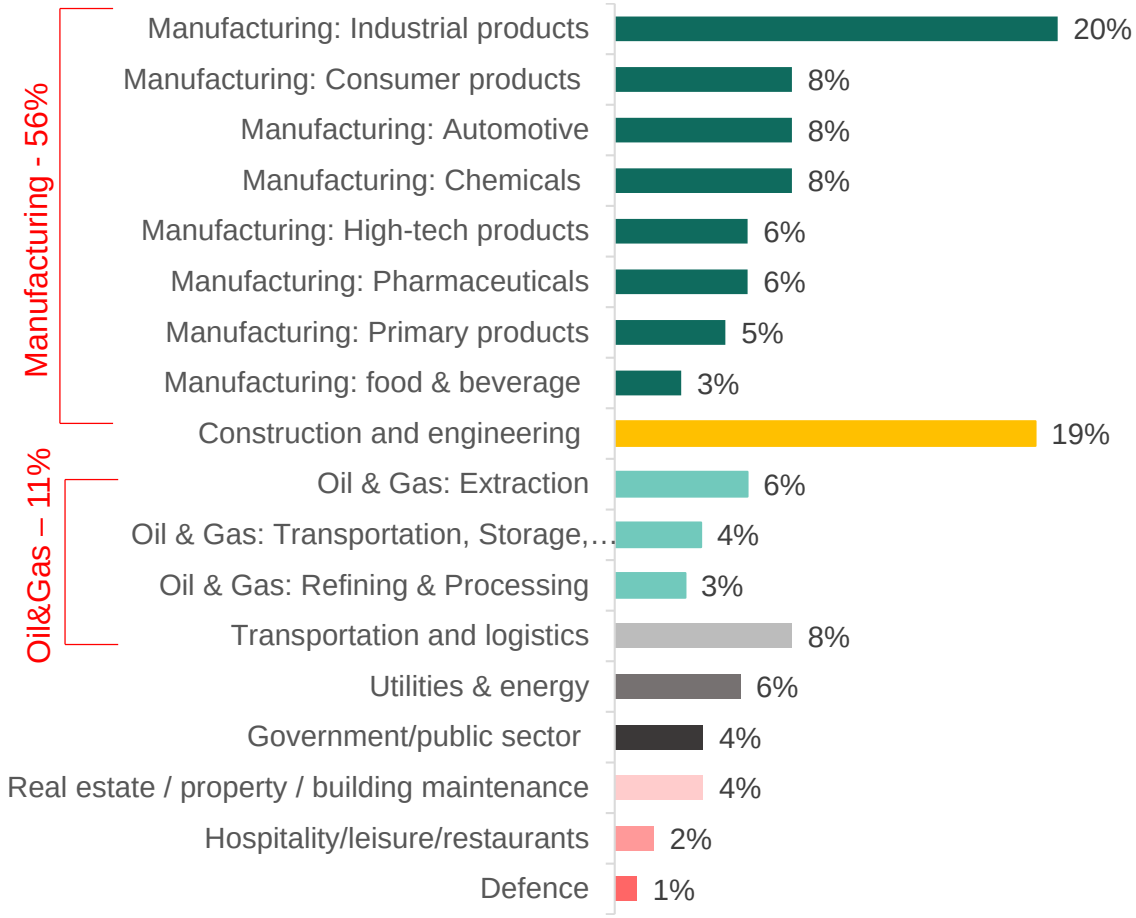
Профиль респондентов

359 Interviews across **21** countries

- North America
- Latin America
- Europe
- Middle East
- APAC



56% of the sample are Manufacturing companies



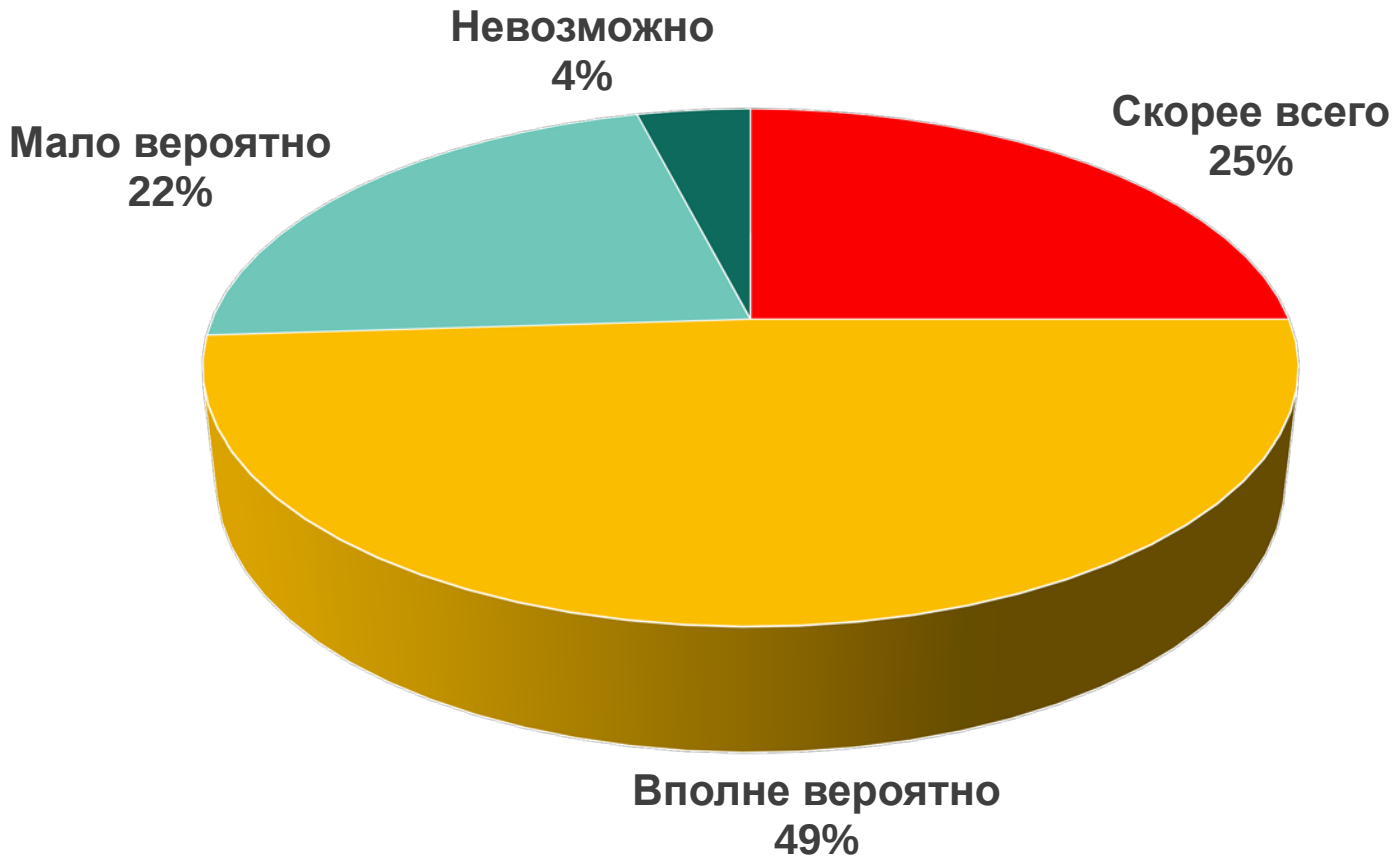
*Total greater than 100% as multiple answers possible

Безопасность АСУ ТП понимание проблемы

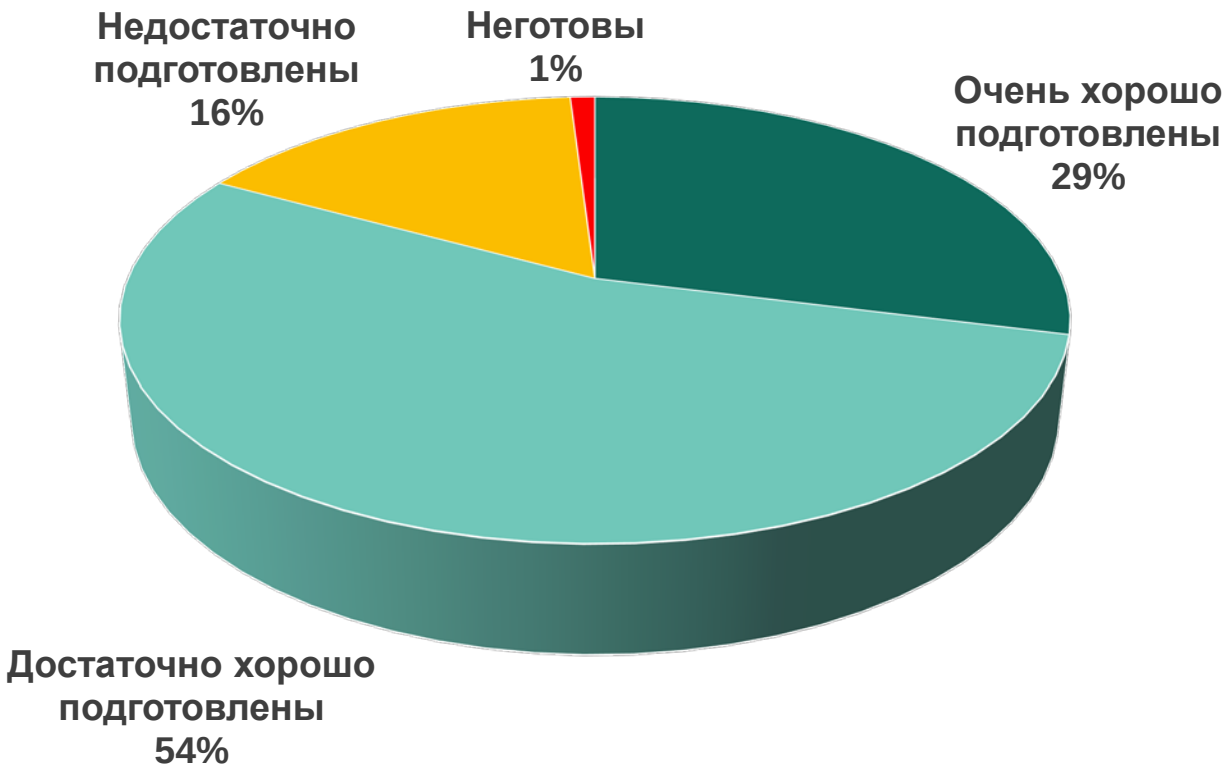
KASPERSKY lab

Проблемы управления кибербезопасностью АСУ ТП

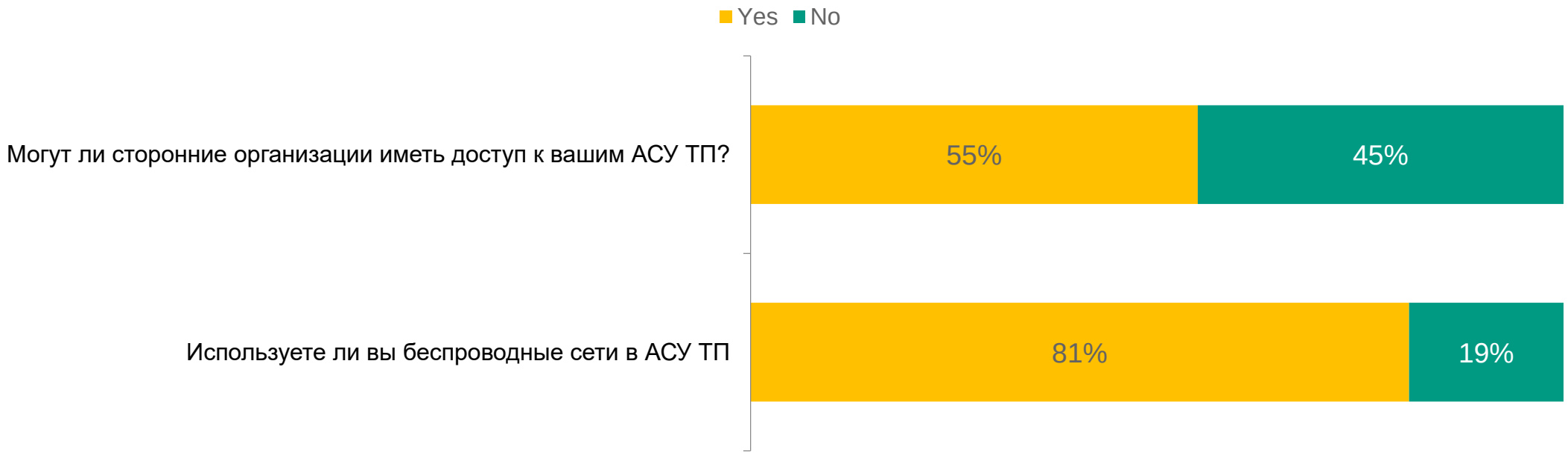
75% компаний прогнозируют кибератаки на АСУ ТП в будущем. Вероятность увеличивается с размером компании



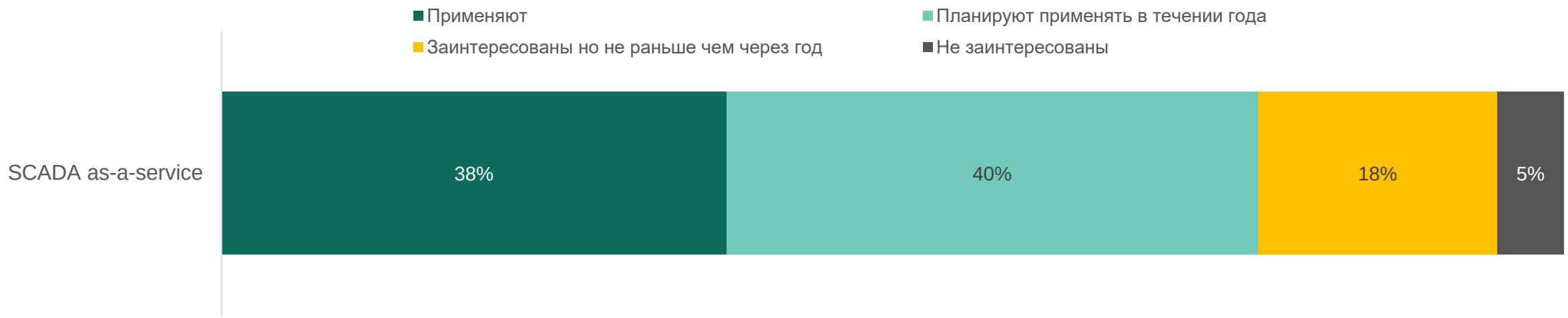
Однако большинство компаний считают себя подготовленными против кибератак на АСУ ТП



Технологические сети во многих компаниях под риском кибератак в результате наличие внешнего доступа



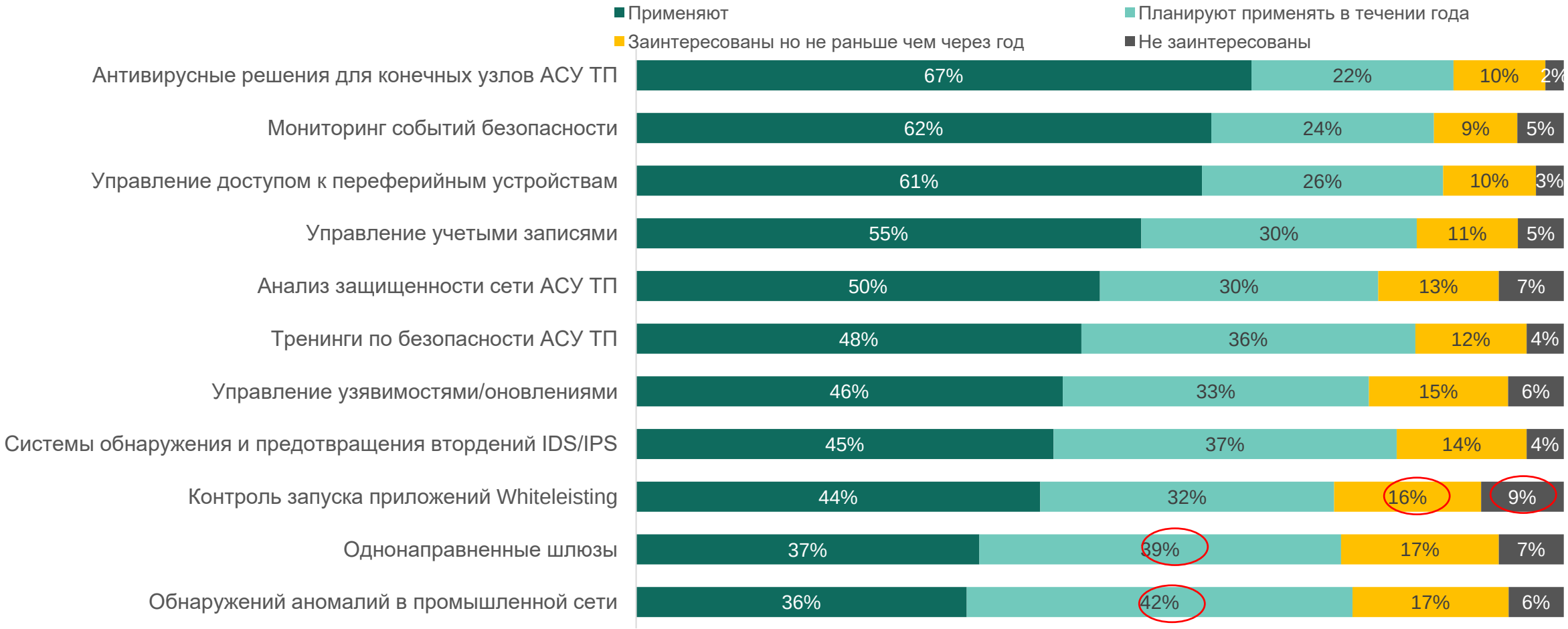
Большое количество опрошенных признают выгоды SCADA as-a-service



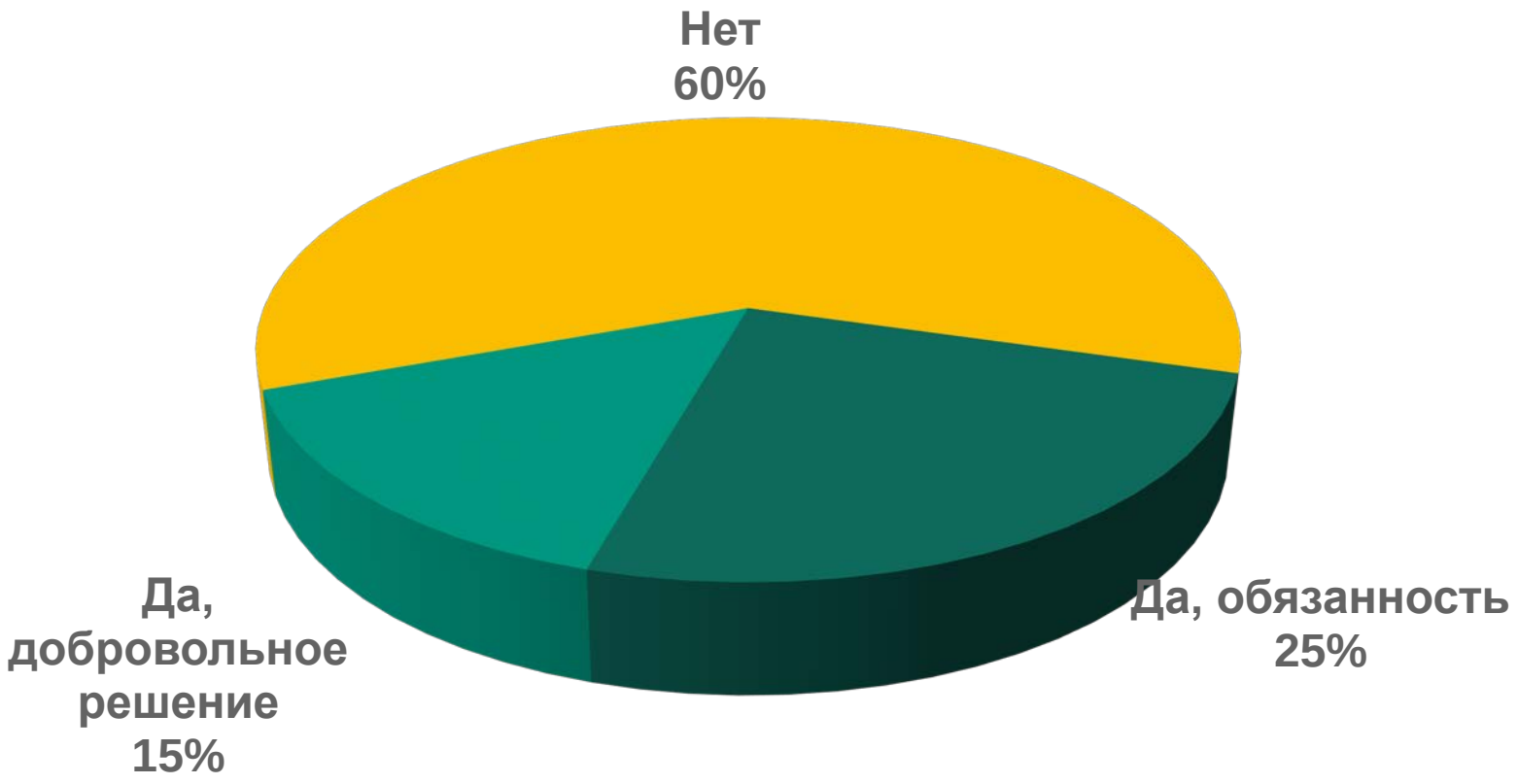
Текущие и планируемые меры безопасности АСУ ТП

KASPERSKY lab

Применяемы и планируемые меры безопасности АСУ ТП, антивирусная защита наиболее распространена



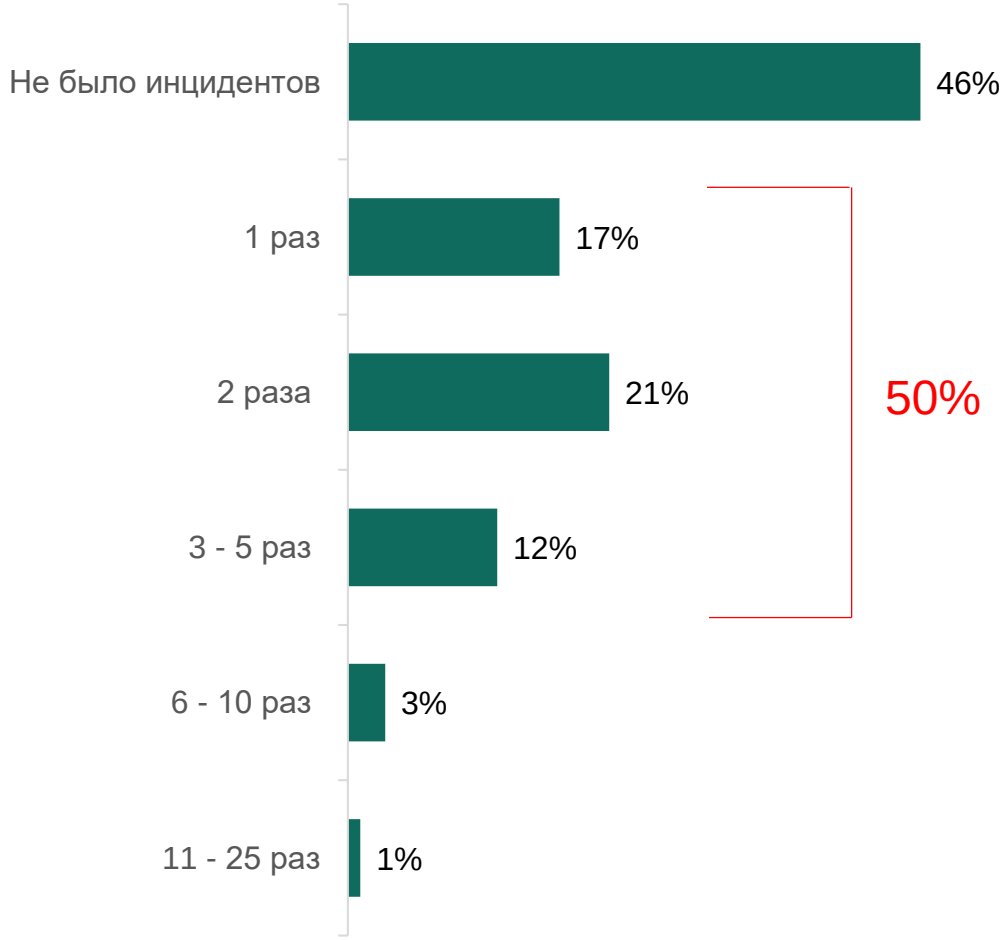
В основном компании не приводят кибербезопасность АСУ ТП в соответствии с нормами и стандартами



Обзор инцидентов безопасности АСУ ТП

KASPERSKY lab

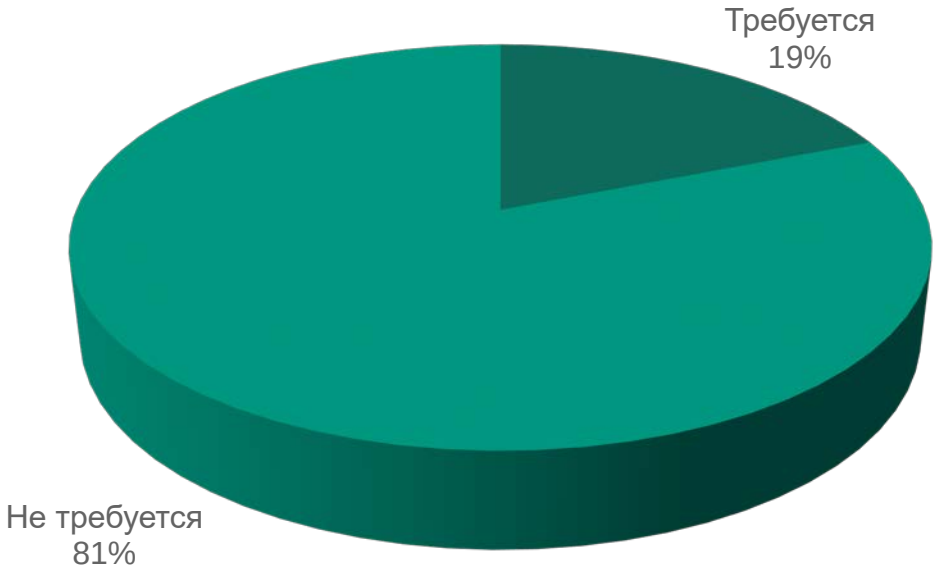
Половина опрошенных испытала от 1 до 5 инцидентов кибербезопасности в АСУ ТП за 12 месяцев

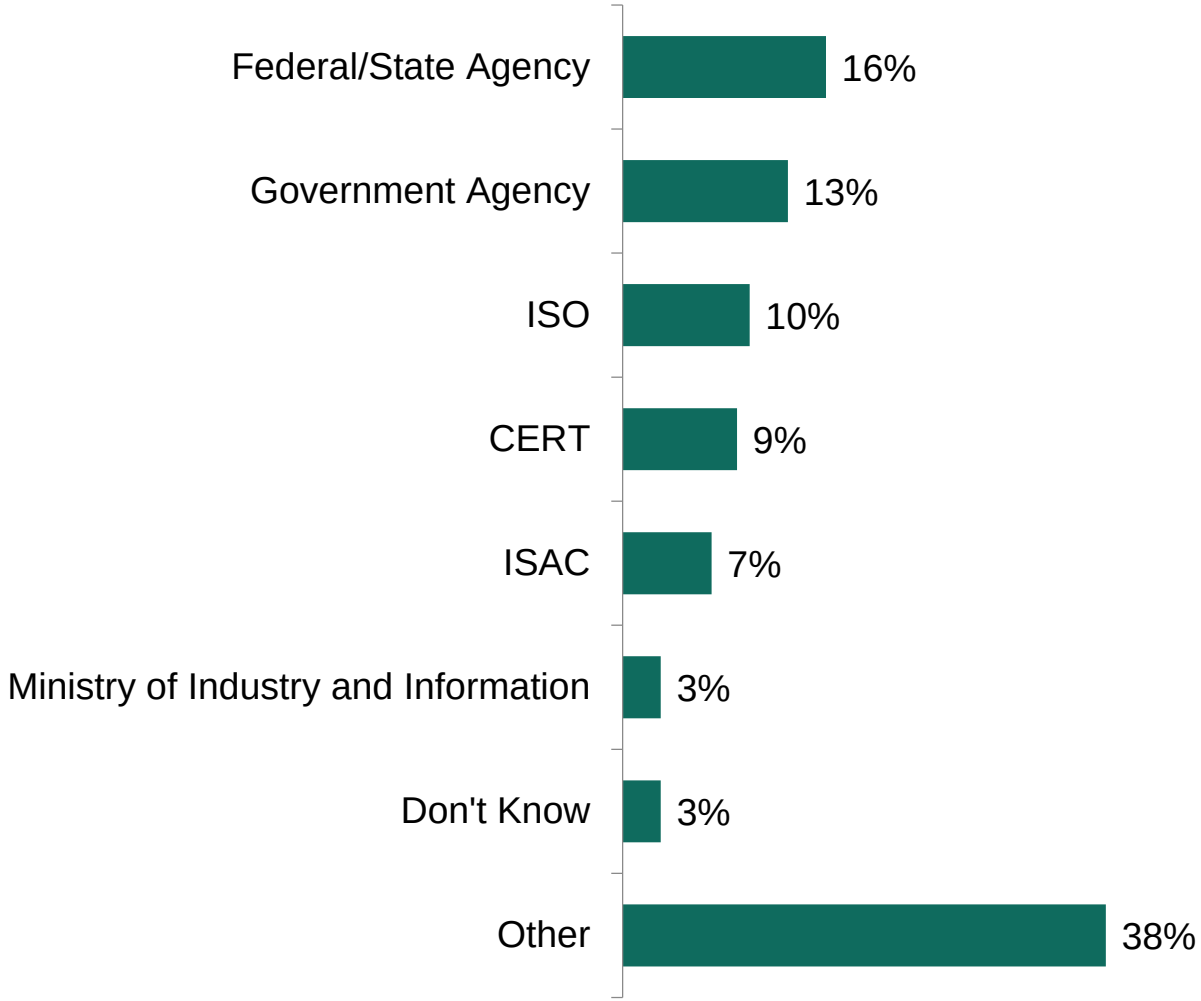


Компании опасаются больше всего заражения обычным вредоносным ПО – эта же угроза являлась причиной реальных инцидентов за год

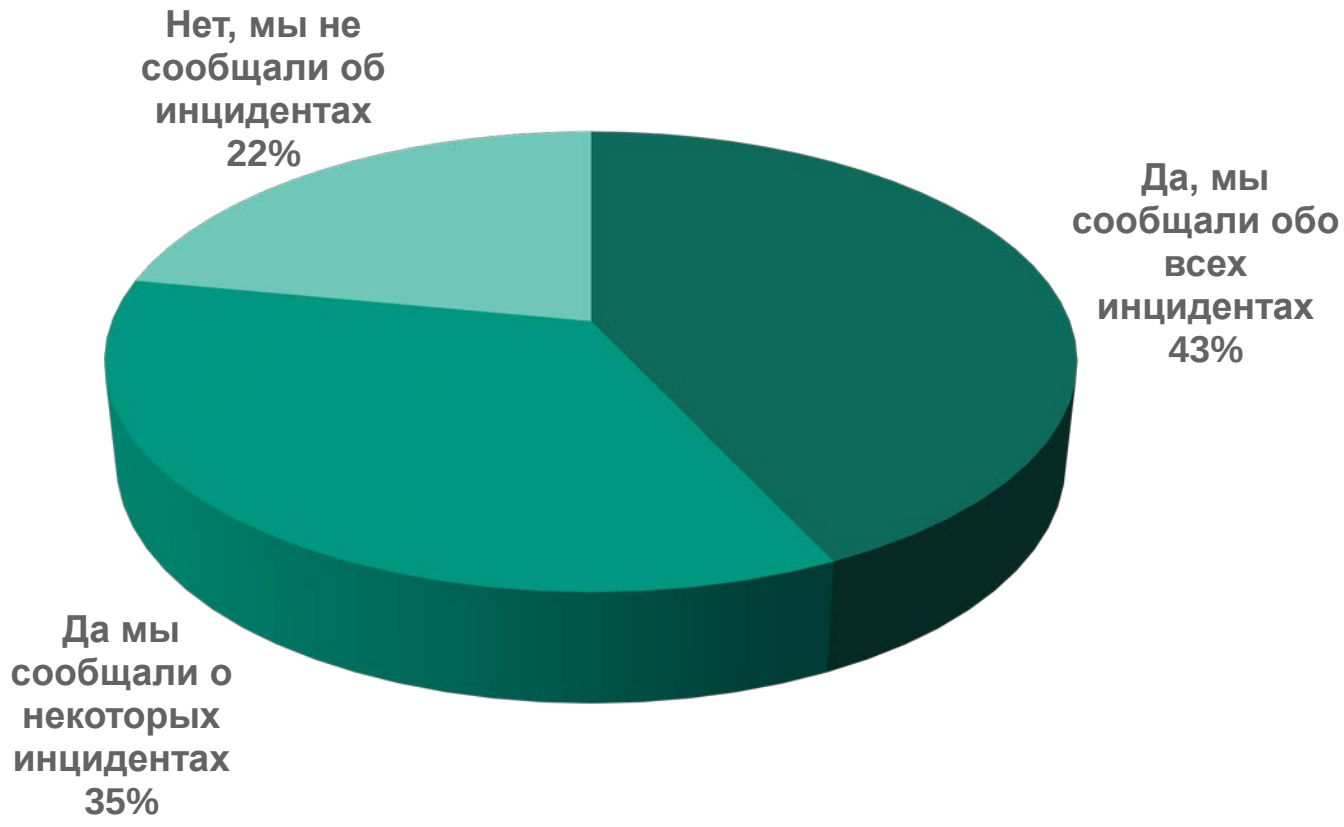
Средние финансовые потери вызванные последствиями киберинцидентов в АСУ ТП составили более $92,000 за 12 месяцев

В основном, большинство опрошенных не обязаны сообщать об инцидентах безопасности АСУ ТП регуляторам



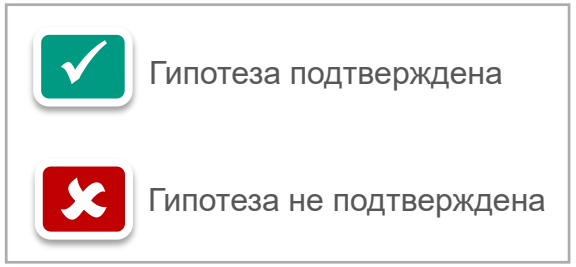


Однако когда происходит инцидент безопасности АСУ ТП, с основном компании сообщают о них, даже если они не обязаны

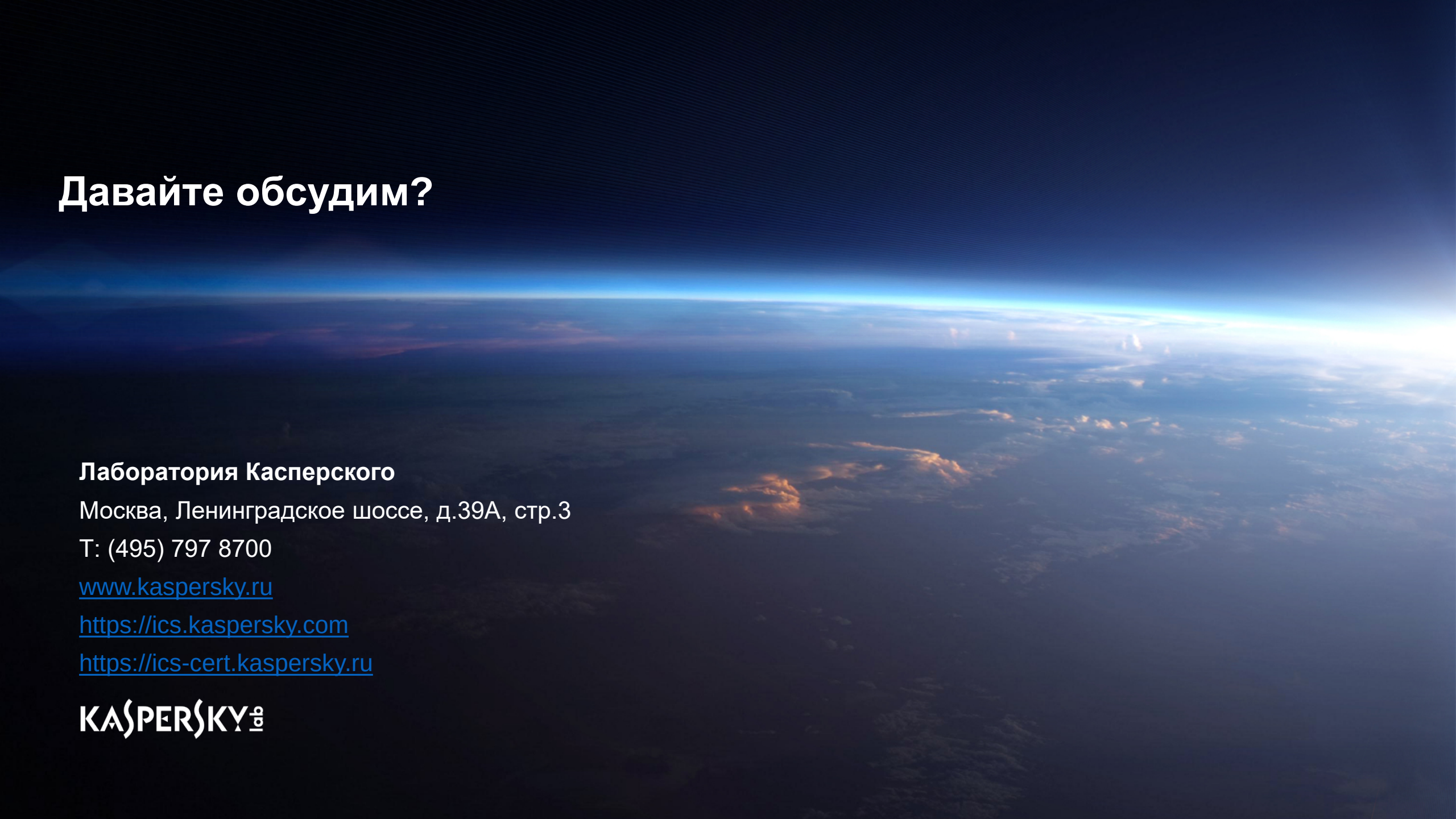


Проверка исходных гипотез

1. Изоляция сетей не помогает остановить кибератаки
2. Угрозы блокировщиков / вымогателей актуальна и высока для сегмента АСУ ТП
3. Инциденты в АСУ ТП не сообщаются в регулирующие организации
4. Внешние организации (вендоры, поставщики услуг) имеют доступ к сети АСУ ТП
5. Относительно высокое применение беспроводных сетей в АСУ ТП
6. Многие компании планируют использовать облачные услуги SCADA as-a-service
7. Существует дефицит профессионалов безопасности АСУ ТП
8. Программы обучения и повышения осведомленности безопасности АСУ ТП не применяются
9. Мониторинг сетей АСУ ТП применяется редко



Давайте обсудим?



Лаборатория Касперского

Москва, Ленинградское шоссе, д.39А, стр.3

T: (495) 797 8700

www.kaspersky.ru

https://ics.kaspersky.com

https://ics-cert.kaspersky.ru

KASPERSKY lab


БУДЬ БДИТЕЛЕН!
СЛЕДИ ЗА ТЕМ, ЧТО ПРОИСХОДИТ В ПРОМЫШЛЕННОЙ СЕТИ!
ИСПОЛЬЗУЙ СОВРЕМЕННЫЕ СИСТЕМЫ МОНИТОРИНГА
И ВИЗУАЛИЗАЦИИ КИБЕРБЕЗОПАСНОСТИ
KASPERSKY lab
Kaspersky Industrial CyberSecurity
© АО «Лаборатория Касперского», 2017.