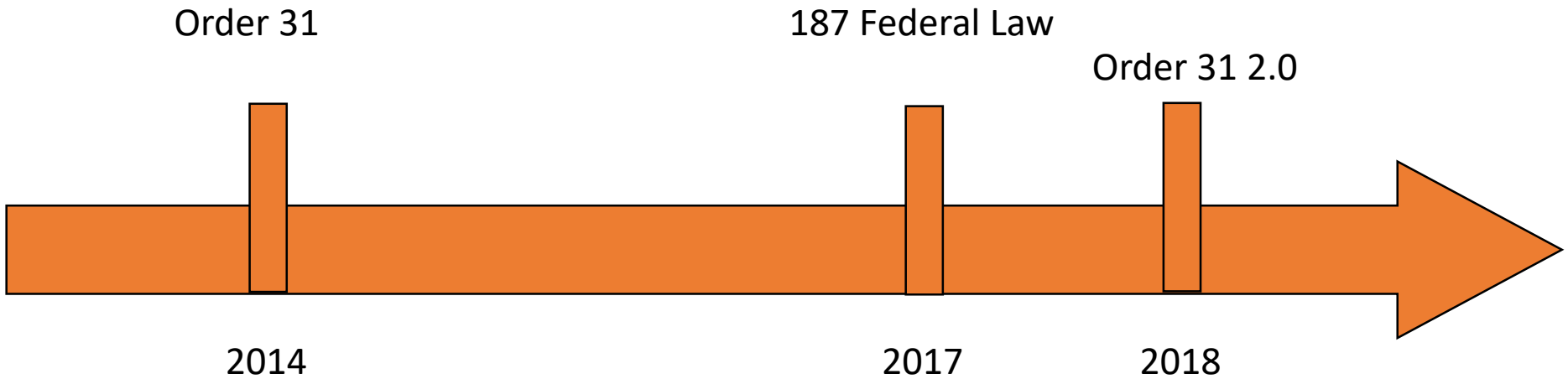
Ensuring cybersecurity of industrial control systems: Life after the Federal Law on critical information infrastructure

Dmitry Avramenko
Head of the competence center for information security of the industrial control systems

What will be discussed?

Before and after



All clear

The new Law, the new beginning…

It's too bad?

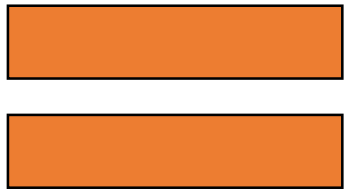
A lot of work has been done…

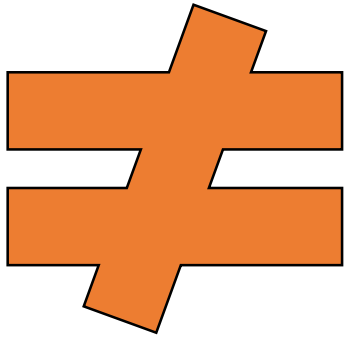
0. Object of protection

Starting point

- For process control systems "conducted" work on the 31 Order
- Owner – CII subject
- ICS provides automation of the critical process and 127-GD "gets" into the significant objects of CII

ICS = CII object?





1. Formation of requirements

Threat analysis and threat model development

Update the existing threat model:

- Object of protection changed (?)
- Sources of threats
- Methodical documents of FSTEC

Requirements

Update the existing Technical Requirement:

- Object of protection changed (?)
- Requirement changed (?)

2. Building cybersecurity system

Documentation

- Adjusting an existing project (?)
- Centralized project (?)

Integration and conformity assessment

- Configuring existing security features
- Centralized management of security features
- Analysis and correlation of cybersecurity events

3. Organizational structure

Is change inevitable?

- What is now?
- What is required by law?
- Organizational and administrative documentation
- New employee?

Cybersecurity forces

- Updating Organizational and administrative documentation
- The order №235 FSTEC (section II)
- Requirements of the FSB

Overall results

- Don't start over, but continue
- Updating cybersecurity system (31 order) = cybersecurity system (187 Federal law)
- Building organizational processes

Thank you!