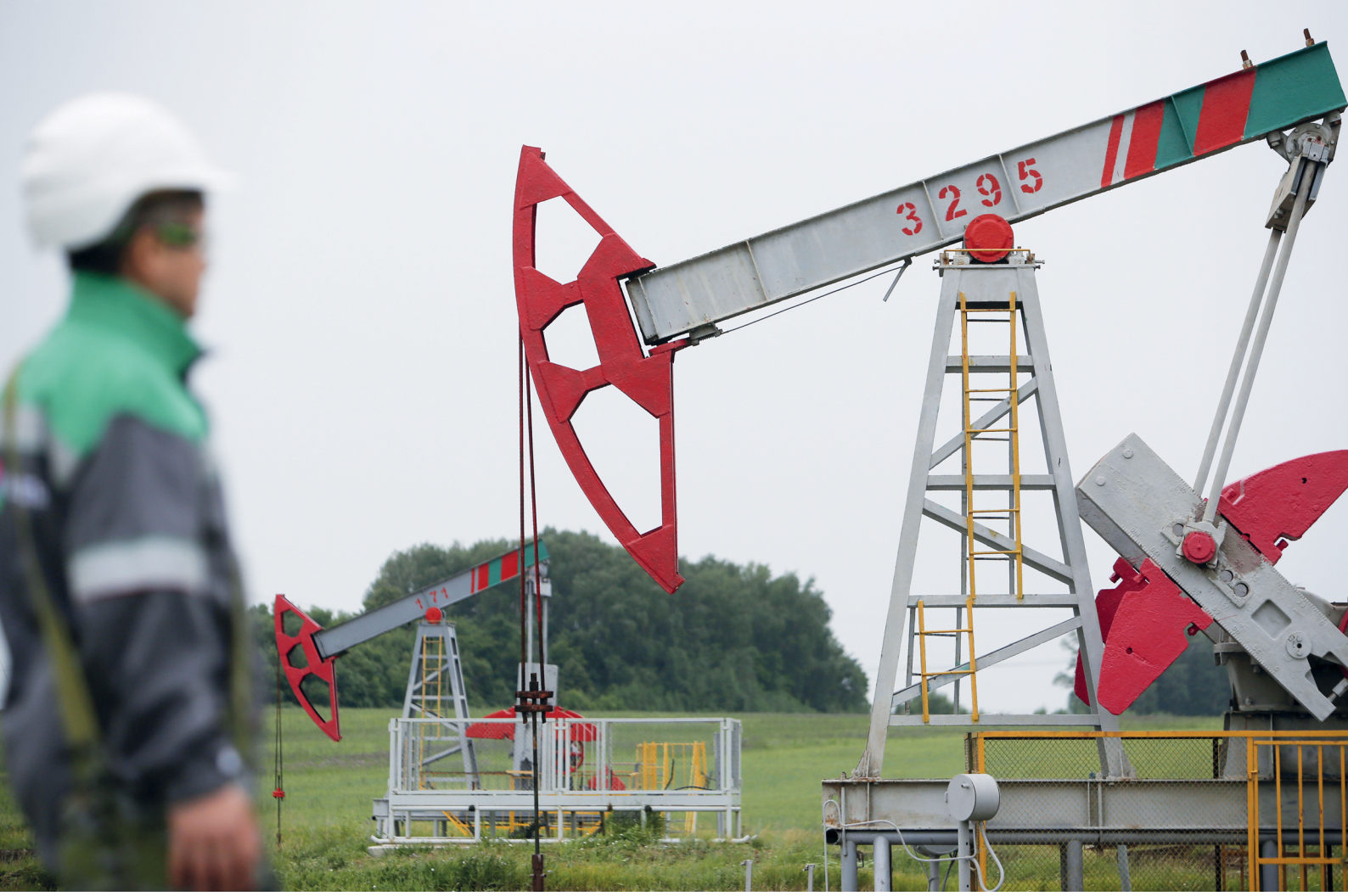


TATNEFT

Tackling cyber security to build a global energy business

kaspersky

Kaspersky Industrial CyberSecurity

Tatneft

https://www.tatneft.ru/?lang=en

Oil & Gas

- Founded in 1950
- More than 80 fields
- Proprietary refining capacity
- Uses Kaspersky Industrial Cybersecurity / Advanced Training

Tatneft is one of Russia's largest energy companies, carrying out oil production at more than 80 fields across Russia

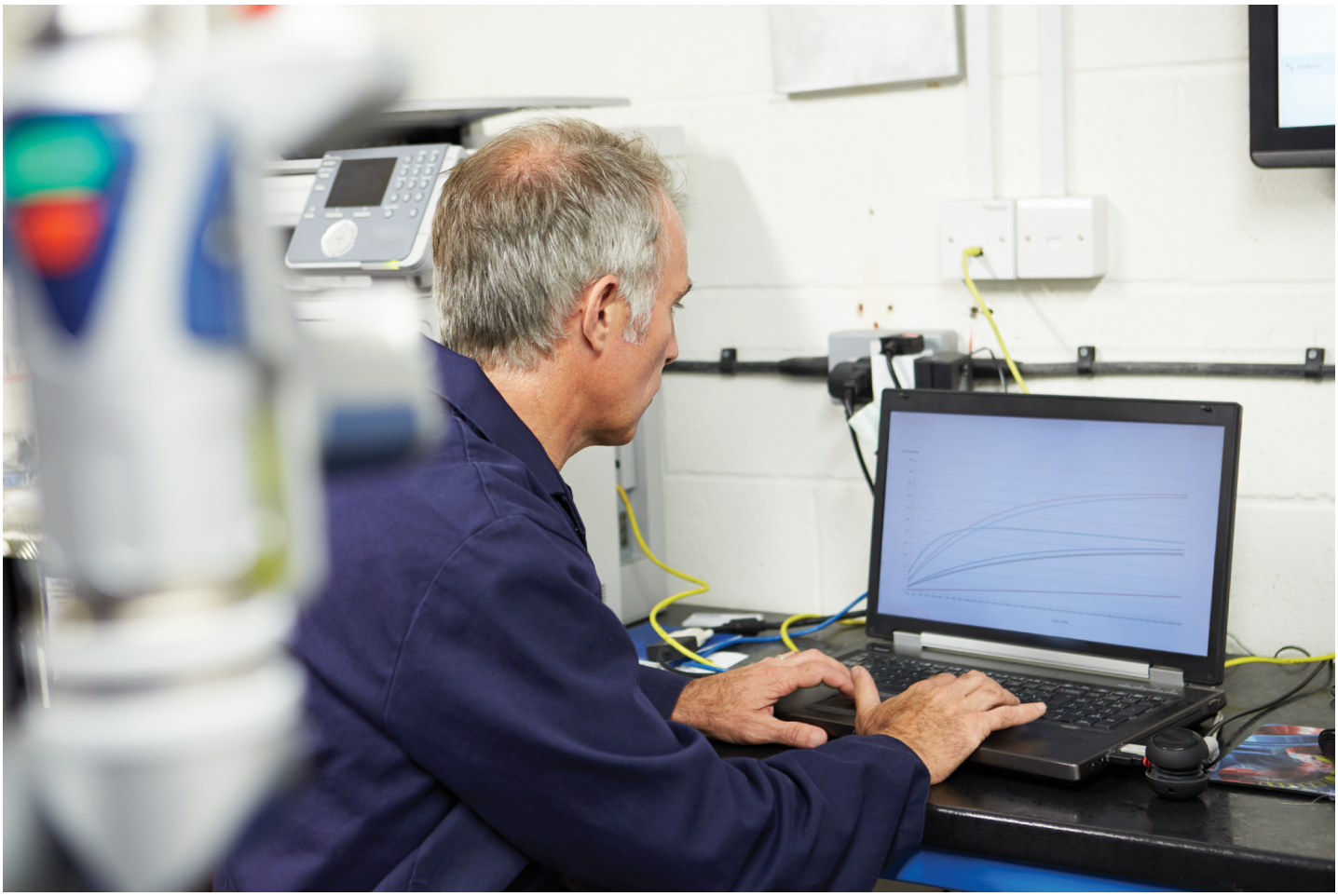
The company's industrial operations include oil and gas production, oil refining, petrochemicals, tires, and a national network of filling stations. All segments are growing, and each is supported by a range of Tatneft services.

The oil refining business is focused on the manufacture of high-quality products, in high-tech, efficient and environmentally friendly facilities.

Objective

Oil extraction and refining requires a forensic approach to safety. Incidents can impact not only production, but the surrounding area.

"The automation of technological processes is one of the keys to developing the business," says Aleksey Bespalov, Head of the Information Technology Department at Tatneft OJSC. "The transfer of labor-intensive and complex tasks to automated control systems allows us to create a technological advantage and reduce the cost of production. Our strategic vision requires safety measures as well as cybersecurity to be taken into consideration."



> **“We expect to raise awareness of possible threats. Kaspersky training will help our managers in the field to re-evaluate possible risks and adjust workflows based on modern standards of cybersecurity.”**

Aleksey Bespalov,
Head of the Information Technology Department, Deputy Head Engineer

“Cybersecurity risks are much higher at industrial companies than they are at family-run businesses or even corporate manufacturers,” says Andrey Suvorov, Head of Critical Infrastructure Protection Business Development at Kaspersky.

Incidents caused by cyber attacks aimed at automated command and control systems can directly affect safe production. In Russia, the need to ensure cybersecurity at a production facility is governed by Decree No. 31 of 14 March 2014 and monitored by the Federal Service for Technical and Export Control (FSTEC). Any automated technological process has a cyber-physical element and, as a result of this process, is a physical event.

“The responsibility for security lies with the person who is in charge of the technological process,” says Bespalov. “It is the duty of employees to follow the continuity of the process. They are a key part of the system.”

Kaspersky Solution

The growing number of industrial cybersecurity incidents worldwide confirms the risk of unsecured access to industrial entities through open networks. Hacking communities have been encouraged to exploit these vulnerabilities.

In response, Tatneft has assigned managers to participate in specialized Kaspersky Lab Industrial Security training. “Within the framework of the training,” says Bespalov, “experts at Kaspersky have demonstrated the possible cyber threat scenarios and vectors of attack on industrial facilities. They've shared their knowledge of cybersecurity incidents obtained from analyzing security incidents at industrial companies worldwide.”

A significant feature of the Kaspersky Industrial Cybersecurity training is that it is based on real facts and events. In the case of serious security incidents or a suspected targeted attack, the Kaspersky experts are called in to analyze the situation. Taftnet participants are given the opportunity to become acquainted with deep expertise in the field of industrial cybersecurity.

“We expect to raise awareness of the threat scenarios which will help managers in the field to re-evaluate possible risks and adjust workflows accordingly,” says Bespalov.

Security
Reduces the risk of cyber attacks on automated industrial command and control systems

Human factor
Up to 80% of all cyber incidents at industrial facilities stem from human error

Expertise
Kaspersky Industrial Cybersecurity trainings are built on real-world experience of investigating industrial cyber incidents. It includes the expertise of the field team that responds to industrial threats

Projections

Andrey Suvorov from Kaspersky says management training is only the first step in raising industrial cybersecurity. The next steps include training programs for other staff and the introduction of specialized cyber protection for automated command and control systems.

Taftnet management is considering broadening the training, including specialized training programs for engineers directly responsible for the technological process.

“Kaspersky is our trusted partner in cyberspace. We welcome the opportunity to develop the protection of our industrial facilities,” concludes Bespalov.

Kaspersky Industrial CyberSecurity

Kaspersky Industrial CyberSecurity is a portfolio of technologies and services designed to secure operational technology layers and elements of your organization - including SCADA servers, HMIs, engineering workstations, PLCs, network connections and even engineers - without impacting on operational continuity and the consistency of industrial process.

Learn more at www.kaspersky.com/ics

Kaspersky ICS CERT:
https://ics-cert.kaspersky.com
Cyber Threats News:
www.securelist.com

#Kaspersky
#BringontheFuture

www.kaspersky.com



* World Leading Internet Scientific and Technological Achievement Award at the 3rd World Internet Conference

** China International Industry Fair (CIIF) 2016 special prize