STATEMENT OF COMPATIBILITY

between
Kaspersky Industrial CyberSecurity
the product of
AO “Kaspersky Lab”
39A/2 Leningradskoe Shosse,
Moscow, 125212, the Russian Federation
hereinafter referred to as “KICS” and “Kaspersky” respectively
and
Software and hardware complex “KRUG-2000” (SCADA KRUG-2000 version 4.2 minimum)
the product of
“SPC KRUG” LLC
1 Germana Titova Str., Penza, 440028, Russia
hereinafter referred to as “KRUG-2000” and “SPC KRUG“ respectively.

SPC KRUG and Kaspersky Lab hereby declare the possibility of mutual apply of the mentioned software products in unified information system, compatibility of these software products, allowing to meet certain information security requirements for automated process control systems (hereinafter referred to as APCS), these products are operated.

KRUG-2000 is a software and hardware complex for creation of automated process control systems. KICS is an integrated cybersecurity solution for critical infrastructure and industrial automation.

SPC KRUG and Kaspersky Lab conducted extensive testing of the KRUG-2000 and KICS compatibility within unified information system. Tests proved the possibility of use the products in unified information system, taking into account their individual environmental requirements. The tests have not revealed any compatibility problems in products.
Installed together, according to requirements and installation and control guidelines, in the unified information environment, OIK Dispatcher NT products and KICS their functionality ensure that some information security requirements are met, Specified in Order No. 31 “About approval of Requirements to ensure information protection in automated systems of control of production and technological processes at critical objects, potentially dangerous objects, as well as objects that pose increased danger to human life and health and to the environment” of the Federal Service for Technical and Export Control of the Russian Federation” (FSTEC) “of March 14, 2014 with regard to anti-virus protection and intrusion detection (items VI, VII of Appendix No. 2 to the order).