Original

АКТ ПРОВЕРКИ СОВМЕСТИМОСТИ

Между программными продуктами

Kaspersky Industrial Cyber Security
продукция компании

АО «Лаборатория Касперского»
Россия, 125212, г. Москва, Ленинградское шоссе, 39А, стр.2

Здесь и далее именуемый как «KICS» и «Лаборатория Касперского»,соответственно

и

SCADA NPT Expert
продукция компании

ООО «ЭнергопромАвтоматизация»
195273, г. Санкт-Петербург, Пискаревский пр., д. 63, лит. Б

Здесь и далее именуемые как «SCADA NPT Expert» и «ЭнергопромАвтоматизация», соответственно

Испытания проведены компанией

ООО «Интеллектуальные Сети»
428020, Россия, г. Чебоксары, ул. Пристанционная, 1/9

Здесь и далее именуемое как «Интеллектуальные Сети»

ЭнергопромАвтоматизация и **Лаборатория Касперского** настоящим актом заявляют о возможности совместного использования упомянутых программных продуктов в единой информационной системе, о совместимости этих программных продуктов, позволяющей добиться выполнения определенных требований информационной безопасности автоматизированных систем управления технологическими процессом (далее АСУ ТП), в которых данные продукты эксплуатируются совместно:

SCADA NPT Expert и **KICS** являются программными продуктами, используемыми в автоматизации цифрового полигона филиала ПАО «РусГидро» - «Нижегородская ГЭС». SCADA NPT Expert является автоматизированной системой управления технологическим процессом. KICS является комплексным инструментом обеспечения информационной безопасности АСУ ТП.

ЭнергопромАвтоматизация и **Интеллектуальные Сети** произвели испытание **SCADA NPT Expert** и **KICS** на совместимость в рамках единой информационной системы на Нижегородской ГЭС (в рамках научно-исследовательских, опытно-конструкторских и технологических работ по расширению цифрового полигона

Translation

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

SCADA NPT Expert

the product of

“EnergyindustryAutomatization” LLC
Lit. B, 63 Piskarevsky Ave., St.-Petersburg, 195273, Russia

hereinafter referred to as «SCADA NPT Expert» and «EnergyindustryAutomatization» respectively

Tests are carried out by the company

“Intellectual Networks” LLC

1/9 Pristantcionnaya str., Cheboksary, 428020, Russia

EnergyindustryAutomatization 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 mutually run:

SCADA NPT Expert and **KICS** are software products used in automation of digital polygon of branch of PJSC "RusHydro" Nizhny Novgorod HPP. **SCADA NPT Expert** is the automated process control system. **KICS** an integrated cybersecurity solution for critical infrastructure and industrial automation.

EnergyindustryAutomatization and **Kaspersky Lab** tested **SCADA NPT Expert** and **KICS** compatibility within unified information system at Nizhny Novgorod HPP (within the framework of research, experimental design and technological works on expansion of the digital polygon of the Nizhny Novgorod HPP).

Original

Нижегородской ГЭС). В результате испытаний было выявлено, что с учетом их индивидуальных требований к среде продукты могут быть использованы в рамках единой информационной системы. Проведенные испытания не выявили каких-либо проблем совместимости между продуктами.

Установлено совместно, в соответствии с требованиями и руководствами по установке и настройке, в единой информационной среде продукты **SCADA NPT Expert** и **KICS** своей функциональностью обеспечивают выполнение части требований информационной безопасности, определенных в Приказе № 31 «*Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды*» Федеральной Службы по Техническому и Экспортному Контролю Российской Федерации (ФСТЭК) от 14 Марта, 2014.

Помимо установки и использования обоих продуктов, для реализации всех требований информационной защищенности в каждом конкретном классе автоматизированных систем могут быть необходимы другие меры. Фактические принимаемые меры будут зависеть от конкретных требований информационной безопасности предъявляемых к объекту защиты, а также архитектуры АСУ ТП объекта. Такие меры могут, помимо прочего, включать в себя установку и использование других программных или аппаратных продуктов, соответствующее конфигурирование продуктов и создание или корректировку организационных процессов.

Управляющий директор,
Россия и страны СНГ
АО «Лаборатория Касперского» Земков С.А.

Руководитель департамента
оперативно-диспетчерских и
технологических задач
ООО «ЭнергопромАвтоматизация» Лобанов С.В.

Директор
ООО «Интеллектуальные Сети» Никандров М.В.

Translation

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.

Besides installing and using both products, other measures may be necessary to complete all information security requirements for each specific class of automated systems. The actual measures taken should depend on the specific information security requirements for the object, as well as the APCS architecture of the object. Such measures may include, but are not limited to, installation and implementation of other software or hardware products, appropriate product configuration, and creation or adjustment of organizational processes.