

АКТ ПРОВЕРКИ СОВМЕСТИМОСТИ

Между программными продуктами

Kaspersky Industrial CyberSecurity
продукция компании

АО «Лаборатория Касперского»

Россия, 125212, г. Москва, Ленинградское шоссе, 39А, стр.2

Здесь и далее именуемые как «KICS» и «Лаборатория Касперского»
соответственно

и

программно-техническим комплексом «ИНБРЭС»
продукция компании

ООО «ИНБРЭС»

Россия, 428018, Чувашская республика, г. Чебоксары, ул. Афанасьева, д. 13,
пом.2

Здесь и далее именуемый как ПТК «ИНБРЭС» и «ИНБРЭС» соответственно

ИНБРЭС 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 процессами (далее – АСУ ТП), в которых данные продукты эксплуатируются совместно:

ПТК «ИНБРЭС» является системой автоматизации электростанций и предназначена для выполнения любых задач в области управления. **KICS** является комплексным решением для обеспечения кибербезопасности объектов критической инфраструктуры и объектов промышленной автоматизации.

ИНБРЭС и Лаборатория Касперского провели испытание ПТК «ИНБРЭС» и **KICS** на совместимость в рамках единой информационной системы. 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.

Совместно установлено, что в рамках единой информационной системы продукты ПТК «ИНБРЭС» и **KICS** своей функциональностью, в соответствии с требованиями и руководствами по установке и настройке, обеспечивают выполнение части требований информационной безопасности, предъявляемых к АСУ ТП.

Помимо установки и использования обоих продуктов, для реализации всех требований информационной безопасности в каждом конкретном классе



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 “**Inbres**”

the product of

“Inbres” LLC

13 Afanasiev Str., Cheboksary, 428018, Chuvash Republic, Russia

hereinafter referred to as Software and hardware complex «Inbres» and «Inbres»

respectively.

Inbres 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:

Software and hardware complex **Inbres** is a power plant automation system designed to perform any tasks in the field of control. **KICS** is an integrated cybersecurity solution for critical infrastructure and industrial automation.

Inbres and **Kaspersky Lab** tested software and hardware complex **Inbres** 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.

Jointly established that within the unified information system functionality of software and hardware complex **Inbres** and **KICS** their functionality, according to requirements and installation and control guidelines provides realization of part of information security requirements for industrial control systems.

Besides installing and using both products, other measures may be necessary to complete all information security requirements for each specific class of automated systems.

Original

автоматизированных систем могут быть необходимы другие меры. Фактические принимаемые меры будут зависеть от конкретных требований информационной безопасности, предъявляемых к автоматизированной системе, а также архитектуры АСУ ТП. 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.

Исполнительный директор
АО «Лаборатория Касперского»



А.Г. Тихонов

Технический директор
ООО «ИНБРЭС»



Л.Л. Орлов

Translation

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.