

## 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

**Программное обеспечение программно-технического комплекса «UniSCADA»**

продукция компании

**ООО «Релематика»**

428020, Республика Чувашия, г. Чебоксары, пр. И. Яковлева, д. 1

Здесь и далее именуемые как **«UniSCADA»** и **«Релематика»**, соответственно

**Релематика** 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 АСУТП), в которых данные продукты эксплуатируются совместно:

**UniSCADA** является автоматизированной системой управления технологическими процессами и используется в области промышленной автоматизации. **KICS** является комплексным решением для обеспечения кибербезопасности объектов критической инфраструктуры и объектов промышленной автоматизации.

**Релематика** и **Лаборатория Касперского** произвели обширное испытание **UniSCADA** 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.

Установлено совместно, в соответствии с требованиями и руководствами по установке и настройке, в единой информационной среде продукты **UniSCADA** и **KICS** своей функциональностью обеспечивают выполнение части требований информационной безопасности, определенных в Федеральном законе от 26.07.2017 г. № 187-ФЗ «О безопасности критической информационной

инфраструктуры Российской Федерации», в частности Приказа № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» Федеральной Службы по Техническому и Экспортному Контролю Российской Федерации (ФСТЭК) от 25 декабря 2017 г.

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.

Исполнительный директор,  
АО «Лаборатория Касперского»



А.А.Тихонов

Технический директор  
ООО «Релематика»



В.С. Шевелев