

ПРОТОКОЛ ИСПЫТАНИЙ СОВМЕСТИМОСТИ
СИСТЕМЫ ЗАЩИТЫ РАБОЧИХ СТАНЦИЙ
И СЕРВЕРОВ АВТОМАТИЗИРОВАННЫХ
СИСТЕМ УПРАВЛЕНИЯ
ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ
INFOWATCH ARMA INDUSTRIAL ENDPOINT WINDOWS 2.7.2
С ПТК КРУГ2000

1. Аннотация

Данный протокол предполагает проведение испытаний на совместимость Infowatch ARMA industrial endpoint windows 2.7.2 (далее СрЗИ) и системы диспетчерского управления и сбора данных Круг2000 4.4 СПО 9 (далее СПО).

Тестирование проводилось на ЭВМ с установленной ОС Windows 10 Pro Версия 21H2 Сборка ОС 19044.1766

В тестировании обмена с нижним уровнем использовалась СРВК DevLink C-1000 (S23) версии 8.1

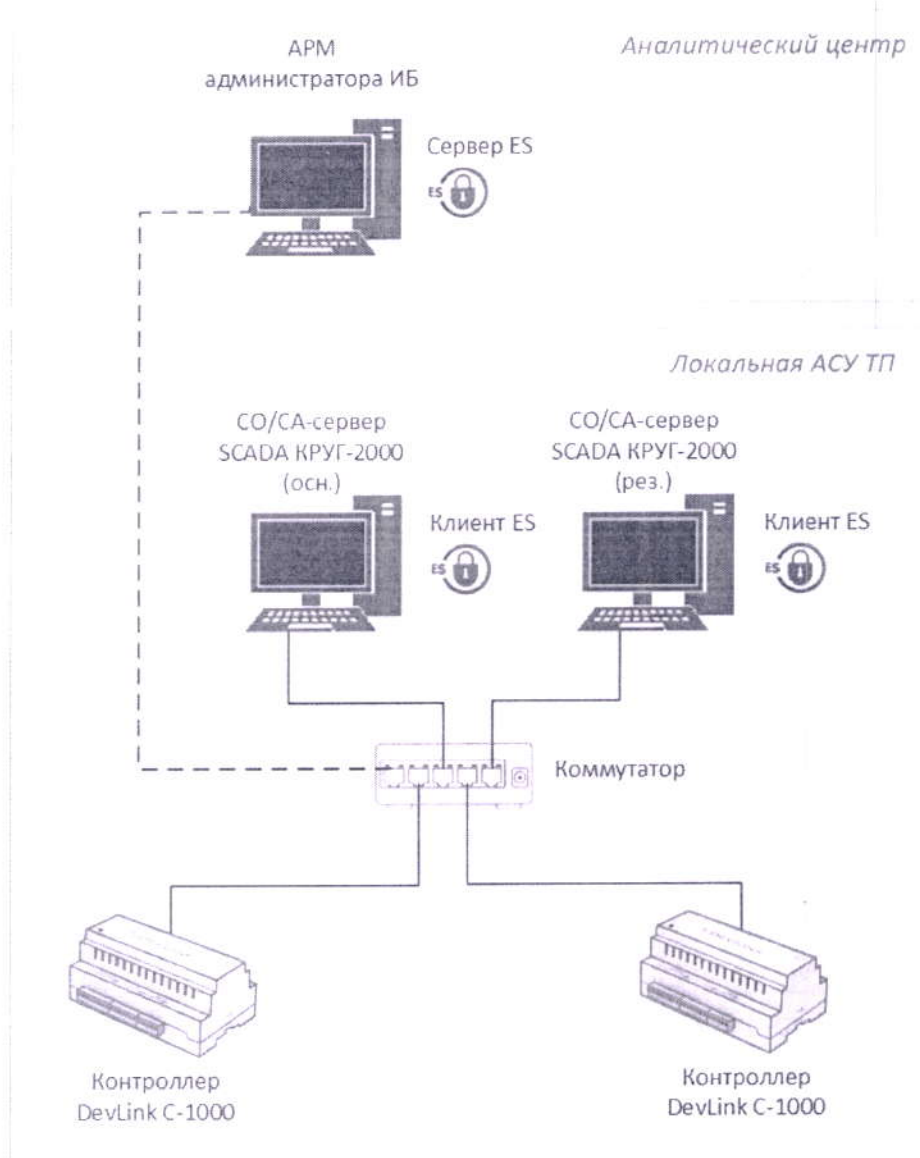


Рисунок 1 – Структурная схема полигона

Состав аппаратного обеспечения предоставлен в Приложении 1.

Список программного обеспечения и сервисов, работающих в ОС предоставлен в Приложении 2.

Обязательным условием успешности пройденных проверок будет невмешательство в работу системы СПО.

В протокол входят следующие пункты, подлежащие проверке:

1. установка, запуск и активация лицензии СрЗи;
2. проверка механизма защиты «контроль целостности»;
3. проверка механизма защиты «контроль устройств»;
4. проверка механизма защиты «контроль приложений».

2. Установка, запуск и активация лицензии СрЗИ.

Согласно «Руководству пользователя версия 15 ред. от 16.09.2024» установка проводилась под локальной учетной записью «Администратор».

ЭВМ был перезагружен. Запущен графический интерфейс и проведена активация лицензии с доступом в интернет.

СрЗИ успешно активировалось.

3. Проверка механизма защиты «контроль целостности»

Для проверки механизма защиты «контроль целостности» были выбраны неизменяемые файлы СПО, находящиеся в папке «*C:\Program Files (x86)\Krug2000*» (исполняемые файлы .exe, файлы библиотек .dll, файлы конфигурации .config и тд), полный список файлов и папок контролируемых механизмом защиты «контроль целостности» предоставлен в Приложении 3.

4. Проверка механизма защиты «контроль устройств»

Для проверки механизма защиты «контроль устройств» был включен контроль подключенных USB устройств, запрещен доступ на чтение и запись CD/DVD. Так же были запрещены все типы USB устройств.

Для получения лицензии СПО используется USB-токен SafeNet USB SuperPro/UltraPro. В конфигурации СПО токен был добавлен в исключения.

5. Проверка механизма защиты «контроль приложений»

Для проверки механизма защиты «контроль приложений» был включен «Режим обучения». Результатом «Режима обучения» стало формирование «Белого списка» в следующем виде:

Каталоги, установленные по-умолчанию в СрЗИ:

C:\Program Files (x86)\ARMA Industrial Endpoint

C:\Windows

Каталоги ПО, запускаемого ОС:

C:\Program

Files\WindowsApps\Microsoft.ScreenSketch_10.1907.2471.0_x64__8wekyb3d8bbwe

C:\Program Files (x86)\ARMA Industrial Endpoint\front

C:\Windows\SystemApps\MicrosoftWindows.Client.CBS_cw5n1h2txyewy

C:\Windows\ImmersiveControlPanel

C:\Windows\SystemApps\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy

C:\Program

Files\WindowsApps\Microsoft.WindowsStore_11910.1002.5.0_x64__8wekyb3d8bbwe

C:\Program Files (x86)\Common Files\SafeNet Sentinel\Sentinel Keys Server

C:\Windows\System32\oobe

C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static

C:\Program Files\Realtek\Audio\HDA

C:\Windows\SystemApps\Microsoft.Windows.Search_cw5n1h2txyewy

C:\Windows\SystemApps\ShellExperienceHost_cw5n1h2txyewy

C:\Windows\System32\wbem

C:\Program Files (x86)\Common Files\SafeNet Sentinel\Sentinel Protection Server\WinNT

C:\Windows\System32

C:\Program Files (x86)\Common Files\SafeNet Sentinel\Sentinel Security Runtime

C:\Program Files (x86)\Krug2000

6. Результаты испытаний:

№	Название испытания	Результат испытания	Замечания
1	Установка, запуск и активация лицензии СрЗИ на целевой ОС	СрЗИ установлено, ошибок в процессе установки нет. СрЗИ успешно активировано.	
2	Проверка механизма защиты СрЗИ «контроль целостности»	Механизм защиты СрЗИ «контроль целостности» включен. Выбраны файлы и папки СПО, подлежащие защите. СПО функционирует в штатном режиме.	
3	Проверка механизма защиты СрЗИ «контроль устройств»	Механизм защиты СрЗИ «контроль устройств» включен. Токен Guardant с лицензией СПО добавлен в исключения. СПО функционирует в штатном режиме.	
4	Проверка механизма защиты СрЗИ «контроль приложений»	Механизм защиты СрЗИ «контроль приложений» включен. Выбраны программы и сервисы СПО и ОС, разрешенные к запуску. СПО и ОС функционируют в штатном режиме.	
5	Проверка механизма резервирования Серверов АБД	Механизм защиты СрЗИ включен. Связь между	

		сервера, резервный сменит статус.	
6	Проверка передачи данных с нижним уровнем	Механизм защиты СрЗИ включен. Связь между серверами и контроллером не «рвется». Значения переменных и атрибутов передаются. Протокол событий с контроллера на сервера передается.	

Представитель заказчика
 Генеральный директор
 ООО НПФ "КРУИ" Ч
 Прудков О.В.

Представитель исполнителя

Руководитель группы сопровождения и
 технической поддержки №1

ООО «ИнфоВотч АРМА»

Тарарук Ю.О.

(Представитель вендора СрЗИ)

Генеральный директор

ООО «ИнфоВотч АРМА»

Филиппова Е.В.

(Представитель вендора СрЗИ)

Подпись

Подпись

Подпись

Подпись

Дата

Дата

Дата

Дата