ПРОТОКОЛ ИСПЫТАНИЙ СОВМЕСТИМОСТИ СИСТЕМЫ ЗАЩИТЫ РАБОЧИХ СТАНЦИИЙ И СЕРВЕРОВ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ INFOWATCH ARMA INDUSTRIAL ENDPOINT LINUX 3.0 С ПТК КРУГ-2000

1. Аннотация

Данный протокол предполагает проведение испытаний на совместимость Infowatch ARMA industrial endpoint linux 3.0 (далее СрЗИ) и ПТК КРУГ-2000 5.1 (далее СПО).

Тестирование проводилось на ЭВМ с установленной ОС Astra Linux Special Edition 1.8.1.6 версия ядра: 6.6.28-1-generic. СПО функционировало в слое совместимости Wine 10.0-1.

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

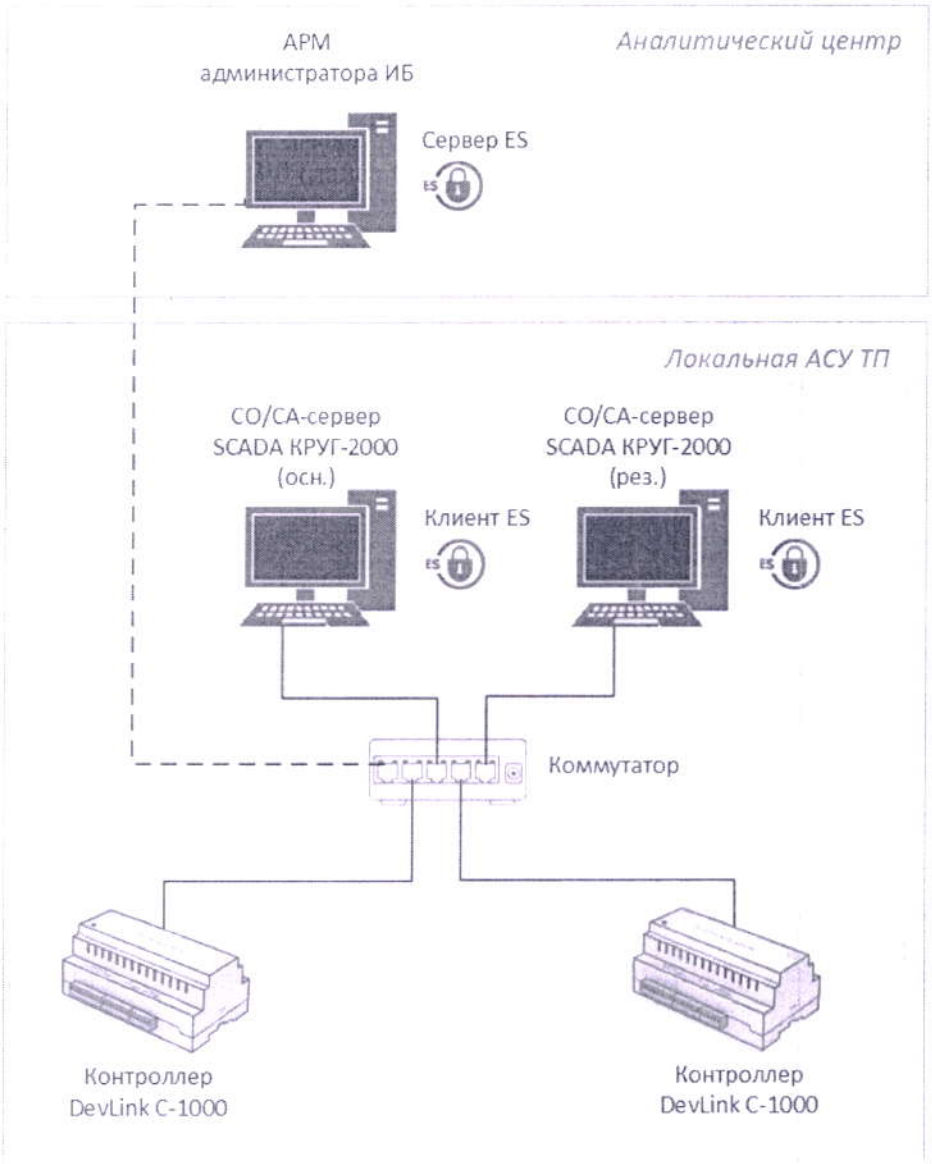

Рисунок 1 – Структурная схема полигона

Состав аппаратного обеспечения (результат выполнения команд *lspci, lscpu, lsblk, lsusb*) предоставлен в Приложении 1.

Список программного обеспечения и сервисов, работающих в ОС (результат выполнения команды *dpkg-query -W -f='${Package} ${Version}\n'*) 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 администратора версия 1 ред. От 03.03.2025» дистрибутив СрЗИ был перенесен на жесткий диск ЭВМ.

После чего была выполнена команда *apt install*. СрЗИ успешно установилось.

Для активации лицензии была выполнена команда *endpoint-cli*.

В предложенном списке был выбран пункт *«2. Осуществить ручное лицензирование»*.

Сформированный ключ был передан в ТП Infowatch, в ответ был получен файл лицензии *license.bin*. После помещения файла лицензии в папку */etc/iwarma-endpoint/* СрЗИ успешно активировалось.

3. Проверка механизма защиты «контроль целостности»

Для проверки механизма защиты «контроль целостности» были выбраны неизменяемые файлы СПО, находящиеся в папке *«/root/.wine-scada-krug-2000/drive_c/Program Files/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 Guardant. В конфигурации СПО токен был добавлен в исключения.

5. Проверка механизма защиты «контроль приложений»

Для проверки механизма защиты «контроль приложений» был включен «Режим обучения» сроком на 10 минут. После чего ЭВМ был перезагружен и запущено СПО. Результатом «Режима обучения» стало формирование «Белого списка» в следующем виде:

Каталоги, установленные по-умолчанию в СрЗИ:

/usr

/root

/lib/systemd/system

Каталог самого СрЗИ:

/etc/iwarma-endpoint

Каталоги ПО, запускаемого ОС:

/home/root

/bpfilter_umh

/etc/X11/fly-dm/Xreset

/etc/X11/fly-dm/Xsession

/etc/X11/fly-dm/Xstartup

/etc/init.d/initialization-profile

Каталог ПО, необходимого для работы токена Guardant:

/opt/guardant/grdcontrol/grdcontrold

А так же каталоги антивирусной защиты Kaspersky Industrial CyberSecurity:

/var/opt/kaspersky/kics/1.5.0.2430_1763736399/opt/kaspersky/kics/shared/kics

/var/opt/kaspersky/kics/1.5.0.2430_1763736399/opt/kaspersky/kics/libexec/kics

/var/opt/kaspersky/kics/1.5.0.2430_1763736399/opt/kaspersky/kics/libexec/kics-gui

/var/opt/kaspersky/kics/1.5.0.2430_1763736399/opt/kaspersky/kics/libexec/launcher

/var/opt/kaspersky/kics/1.5.0.2430_1763736399/opt/kaspersky/kics/libexec/wdserver

/var/opt/kaspersky/kics/1.5.0.2430_1763736399/opt/kaspersky/kics/libexec/kics-gui-launcher

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 серверами не пропадает. В случае отказа основного	

		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 «КРУГ» Прокофов О.В.	Подпись	Дата
Представитель исполнителя Руководитель группы сопровождения и технической поддержки №1 ООО «ИнфоВотч АРМА» Тарарук Ю.О. (Представитель вендора СрЗИ)	Подпись	Дата
Генеральный директор ООО «ИнфоВотч АРМА» Филиппова Е.В. (Представитель вендора СрЗИ)	Подпись	Дата