ПРОТОКОЛ

испытаний Системы анализа и мониторинга состояния информационной безопасности на базе программного комплекса CyberLympha DATAPK совместно с программно-техническим комплексом АСУ ТП «КРУГ-2000»

г. Пенза 03.11.2023

Состав приемочной комиссии

От НПФ «КРУГ»:

Начальник департамента ПО Ревунов Д.С.

Инженер-тестировщик Кашаев М.Д.

От ООО «СайберЛимфа»:

Руководитель направления лаборатории кибербезопасности Ганжа В.В.

Младший инженер лаборатории кибербезопасности Панов К.О.

ЦЕЛИ ИСПЫТАНИЙ:

1. Демонстрация функциональных возможностей Комплекса.
2. Проверка работоспособности Комплекса.
3. Подтверждение отсутствия негативного влияния Комплекса на функционирование автоматизированной системы управления технологическим процессом (АСУ ТП) на базе программно-технического комплекса (ПТК) «КРУГ-2000».
4. Проверка готовности Системы к промышленной эксплуатации совместно с АСУ ТП на базе ПТК «КРУГ-2000».

ИТОГИ ИСПЫТАНИЙ:

Испытания проведены в соответствии с документом «Программа и методика испытаний Системы анализа и мониторинга состояния информационной безопасности на базе программного комплекса CyberLympha DATAPK совместно с программно-техническим комплексом АСУ ТП «КРУГ-2000»».

РЕЗУЛЬТАТЫ ИСПЫТАНИЙ:

Таблица Б.1 – Сведения о результатах проведения испытаний

№ п/п	Наименование испытаний	Результат выполнения испытаний	Сведения о сбоях, отказах, аварийных ситуациях, возникших в ходе испытания	Примечания
1.	Контроль и анализ сетевого трафика. Проверка сетевых объектов на наличие активных сетевых сервисов в пассивном режиме. Автоматизация присвоения статусов для детектируемых сетевых взаимодействий посредством правил	Выполнено		
2.	Контроль целостности защищаемой промышленной сети. Контроль информационных потоков между компонентами АСУ ТП	Выполнено		
3.	Обнаружение сетевых узлов и определение их типа. Инвентаризация сетевых узлов	Выполнено		
4.	Проверка сбора конфигураций. Контроль конфигураций компонентов АСУ ТП и средств защиты информации	Выполнено		
5.	Проверка сбора конфигураций с активного сетевого оборудования. Проверка сетевых объектов на наличие активных сетевых сервисов и служб в режиме запрос-ответ	Выполнено		
6.	Проверка сбора событий. Регистрация, анализ, систематизация и визуализация событий ИБ	Выполнено		
7.	Проверка функции оценки состояния доступности сетевых узлов. Инвентаризация сетевых узлов и отслеживание их жизненного цикла	Выполнено		
8.	Проверка соответствия требованиям ИБ. Обнаружение, анализ уязвимостей компонентов объекта защиты на основе режима «запрос-ответ» и анализа пакетов данных. Формирование отчетов и рекомендаций по устранению выявленных уязвимостей. Проверка соответствия техническим стандартам ИБ	Выполнено		
9.	Проверка службы обнаружения вторжений.	Выполнено		

№ п/п	Наименование испытаний	Результат выполнения испытаний	Сведения о сбоях, отказах, аварийных ситуациях, возникших в ходе испытания	Примечания
10.	Проверка корреляции событий и управления инцидентами ИБ. Регистрация, анализ, систематизация и визуализация событий ИБ.	Выполнено		
11.	Проверка сбора конфигураций с ПЛК.	Выполнено		
12.	Проверка сбора конфигураций с SCADA. Контроль целостности защищаемой промышленной сети.	Выполнено		
13.	Контроль информационных потоков между компонентами АСУ ТП.	Выполнено		
14.	Проверка наличия встроенных механизмов резервного копирования.	Выполнено		
15.	Проверка наличия функционала самодиагностики.	Выполнено		

ЗАКЛЮЧЕНИЕ:

1. Испытания проведены в соответствии с документом «Программа и методика испытаний Системы анализа и мониторинга состояния информационной безопасности на базе программного комплекса CyberLympha DATAPK совместно с программно-техническим комплексом АСУ ТП «КРУГ-2000»».
2. Все тесты Методики завершены успешно.
3. Негативного влияния на функционирование АСУ ТП не выявлено.
4. Считать возможным функционирование Комплекса совместно с АСУ ТП «КРУГ-2000».

Дата	Подпись	ФИО
07.11.2023		Ревунов Д.С.
07.11.2023		Кашаев М.Д.
07.11.2023		Ганжа В.В.
07.11.2023		Панов К.О.