CyberLympha®

МОБИЛЬНЫЙ КОМПЛЕКС

контроля защищенности АСУ ТП и проверки реализации требований 187-ФЗ «О безопасности КИИ»

Алексей Комаров
Руководитель практики ИБ АСУ ТП

218.57

СИСТЕМА ЗАЩИТЫ

КИИ ПОСТРОЕНА

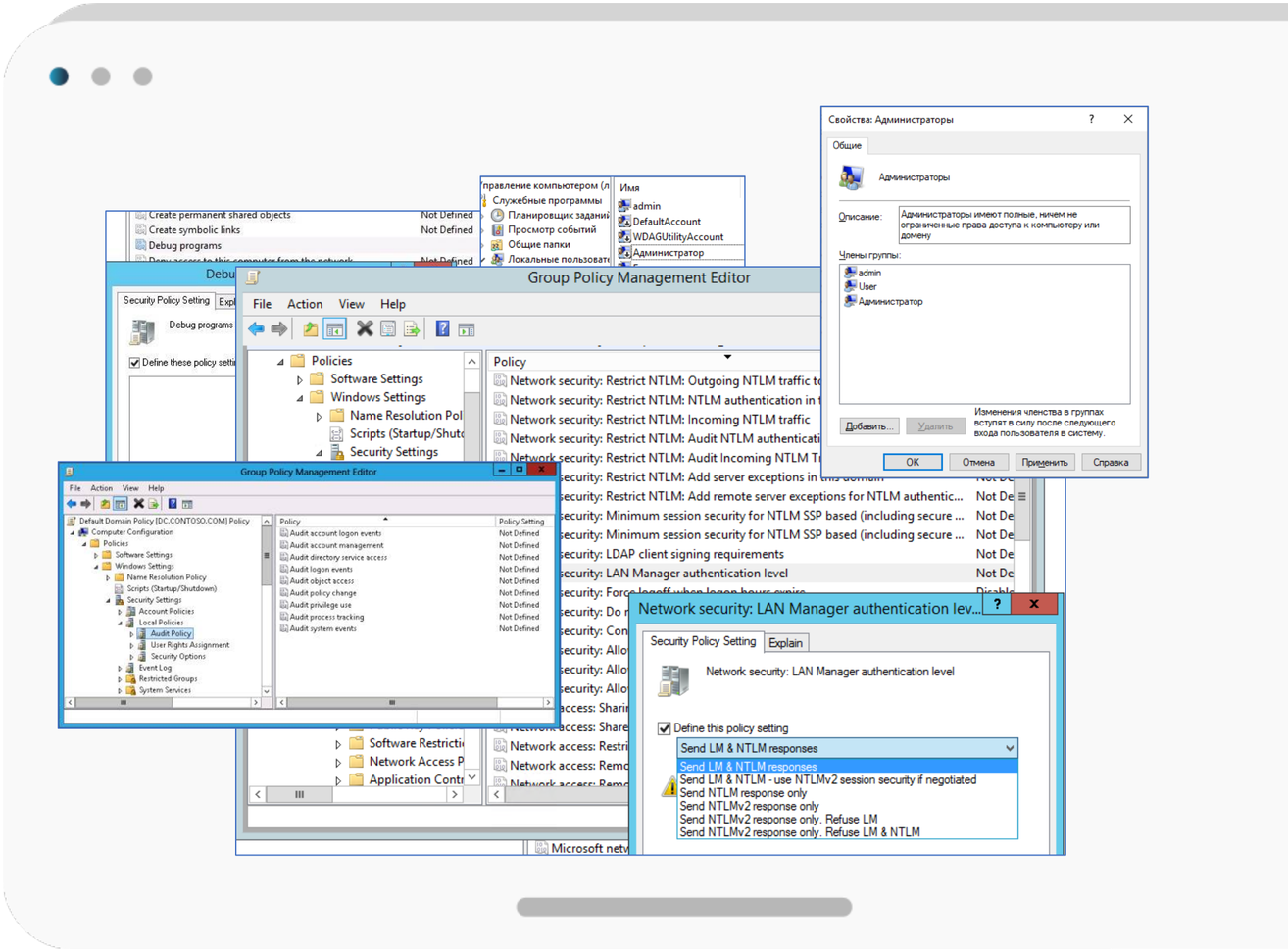
CyberLympha®

ОЖИДАНИЕ vs. РЕАЛЬНОСТЬ

CyberLympha®

- ✓ Защищенная АСУ ТП
- ✓ Реализация технических мер защиты приказов ФСТЭК России
- ✓ Соответствие требованиям 187-ФЗ
- ✓ Реализация отраслевых требований и внутренних нормативных документов
- ✓ Реализация рекомендаций производителей АСУ ТП
- ✓ Соответствие проектным решениям СОИБ КИИ

VS



КОНТРОЛЬ ЗАЩИЩЕННОСТИ **В АСУ ТП**

CyberLympha®

ОСОБЕННОСТИ

- Отсутствие влияния на защищаемые системы и технологические процессы
- Поддержка специального оборудования и ПО
- Поддержка особенностей сетей передачи данных и специализированных протоколов
- Фокусирование на атаках и угрозах, актуальных для промышленных систем автоматизации

ТРЕБОВАНИЯ К ФУНКЦИЯМ

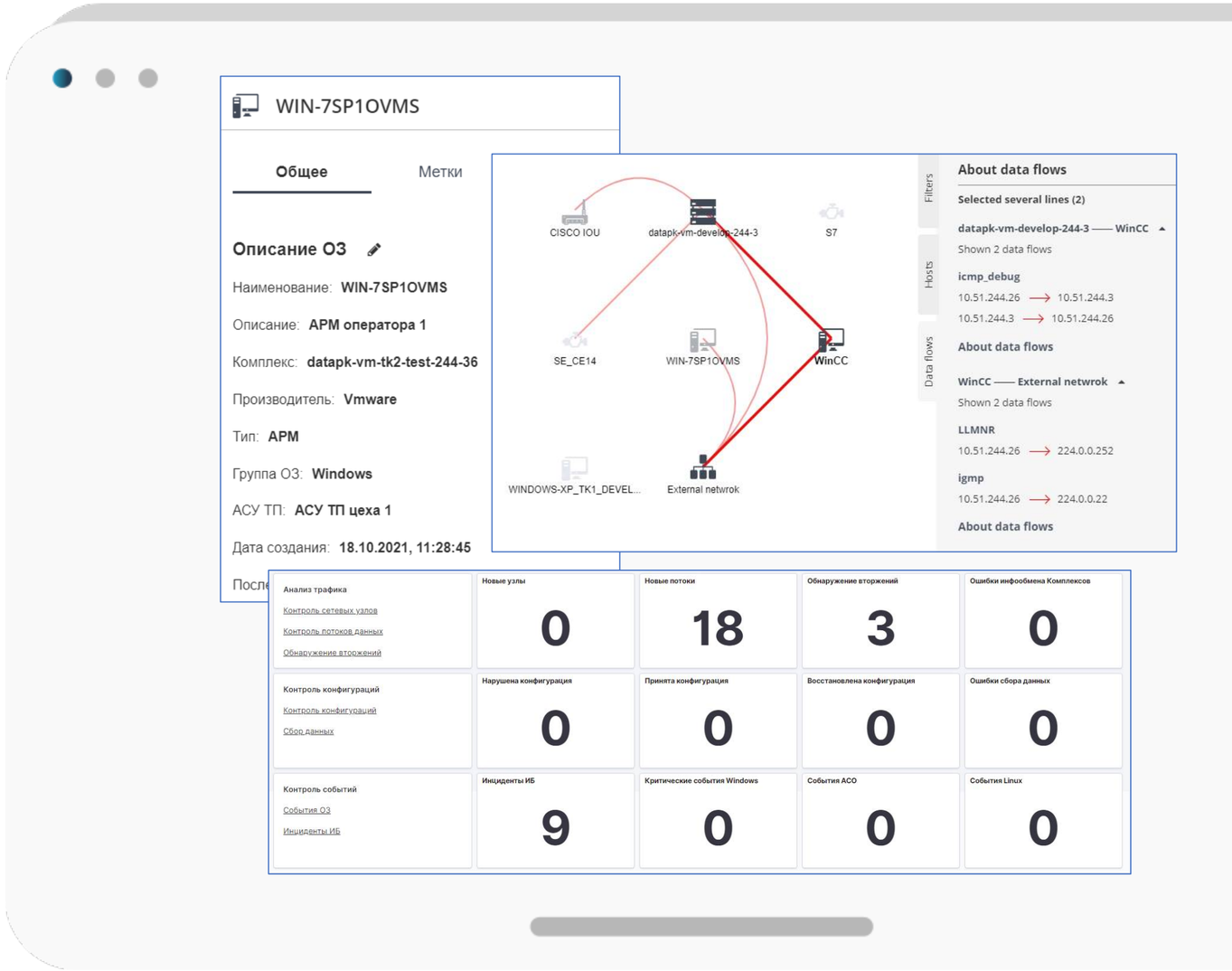
- Контроль реального состояния защищенности АСУ ТП
- Контроль соответствия отраслевым требованиям
- Контроль соответствия требованиям локальных нормативных документов
- Контроль соответствия требованиям регуляторов и законодательства РФ

CL DATAPK. ВАРИАНТЫ КОНТРОЛЯ

CyberLympha®

ПОСТОЯННАЯ РАБОТА НА ЗАЩИЩАЕМОЙ СИСТЕМЕ

- Постоянный аудит защищаемой системы
- Ведение каталога сетевых узлов **с учетом всех атрибутов**
- Ведение каталога сетевых взаимодействий **и управление статусом** информационных потоков
- Выявление уязвимых и запрещенных протоколов
- Выявление уязвимых сетевых узлов – ПО, прошивки
- Выявление небезопасных команд и удаленного управления
- Выявление взаимодействий с внешними сетями, в т. ч. Интернет
- Обнаружение сетевых атак на компоненты АСУ ТП
- **Непрерывный** контроль соответствия политикам безопасности
- **Непрерывный** контроль соответствия рекомендациям вендоров
- **Непрерывное** выявление инцидентов ИБ на базе анализа событий



CL DATAPK. ВАРИАНТЫ КОНТРОЛЯ

CyberLympha®

ПЕРИОДИЧЕСКИЙ КОНТРОЛЬ ОБЪЕКТА

РЕЖИМ ПРОСЛУШИВАНИЯ

- Периодический аудит защищаемой системы
- Ведение каталога сетевых узлов
- Ведение каталога сетевых взаимодействий
- Выявление уязвимых и запрещенных протоколов
- Выявление уязвимых сетевых узлов – ПО, прошивки
- Выявление небезопасных команд и удаленного управления
- Выявление взаимодействий с внешними сетями, в т. ч. Интернет
- Обнаружение сетевых атак на компоненты АСУ ТП

РЕЖИМ ОПРОСА

- Периодический контроль соответствия политикам безопасности
- Периодический контроль соответствия рекомендациям вендоров
- Периодическое выявление инцидентов ИБ на базе анализа событий

SNMP

SSH

WMI Windows Management Instrumentation

ИНСТРУМЕНТЫ ЭФФЕКТИВНОГО КОНТРОЛЯ

CyberLympha®

ПАРАМЕТРЫ БЕЗОПАСНОСТИ ПЛК

Параметр	Значение
Собрано блоков	111/111
Код заказа	6ES7 315-2EH14-0AB0
Версия ОС	37.12.12
Тип модуля	CPU 315-2 PN/DP
Серийный номер	S C-H5D527772016
Наименование ПЛК	S7300/ET200M station_1
Наименование модуля	PLC_1
Состояние ПЛК	S7CpuStatusRun
Количество программных блоков	111
Позиция селектора	RUN-P
Параметры уровня защиты	Write Password
Уровень защиты ЦПУ	Read Only
Переключатель запуска	Unknown / N.A.
Уровень защиты селектора	Can Read/Write

РЕКОМЕНДОВАННЫЕ ПОЛИТИКИ БЕЗОПАСНОСТИ WINDOWS

Настройка	Статус	Должно быть	Имеется
Размер истории паролей	Не соответствует	5	0
Пороговое значение блокировки (попытки)	Соответствует	0	0
Требовать вход в систему для изменения пароля	Соответствует	0	0
Принудительный выход из системы по истечении часа	Соответствует	0	0
Новое имя администратора	Не соответствует	"user_2"	"Administrator"
Новое имя гостя	Не соответствует	"user_1"	"Guest"
Открытый текстовый пароль	Соответствует	0	0
Доступ анониного пользователя к локальной политики LSA	Соответствует	0	0
Включить аккаунт администратора	Не соответствует	0	1
Включить аккаунт гостя	Не соответствует	0	1

РЕКОМЕНДАЦИИ SIEMENS ДЛЯ ПРОМЫШЛЕННОГО ОКРУЖЕНИЯ

Информация о рекомендации в документации Siemens «Recommended security settings for IPCs in industrial environments»	Проверяемый параметр	Соответствует ли рекомендациям Siemens
Раздел 4.2 документации: «Обнаружение пользовательской установки и запроса повышения прав с помощью контроля учетных записей пользователей (UAC)». Параметр: Локальная политика безопасности\Локальные политики\Параметры безопасности\Контроль учетных записей: поведение запроса на повышение прав для обычных пользователей (рекомендуемое значение: «Автоматически отклонять запросы на повышение прав»)	MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\ConsentPromptBehaviorUser	Не соответствует
Раздел 4.4 документации: «Запрет завершения работы системы без выполнения входа в систему». Параметр: Локальная политика безопасности\Локальные политики\Параметры безопасности\Завершение работы: разрешить завершение работы системы без выполнения входа в систему (рекомендуемое значение: «Отключен»)	MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\ShutdownWithoutLogon	Соответствует

ИНСТРУМЕНТЫ ЭФФЕКТИВНОГО КОНТРОЛЯ

CyberLympha®

РАСШИРЕНИЕ ВОЗМОЖНОСТЕЙ

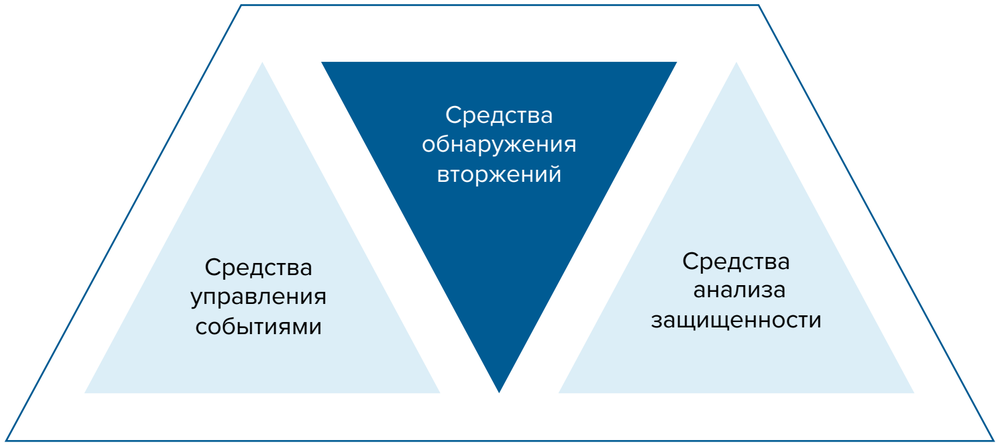
- Готовые и заполненные итоговые документы по результатам контроля
- Управление результатами контроля множества проверяемых объектов
- Расширение сети сенсоров на базе компактных сетевых сенсоров-приманок
- Эмуляция атак на АСУ ТП и оценка реакции подразделений ИБ проверяемых объектов
- Анализ беспроводных сетей

CyberLympha®

CyberLympha

DATAPK

Непрерывный комплексный мониторинг
и анализ состояния информационной безопасности
промышленных систем автоматизации



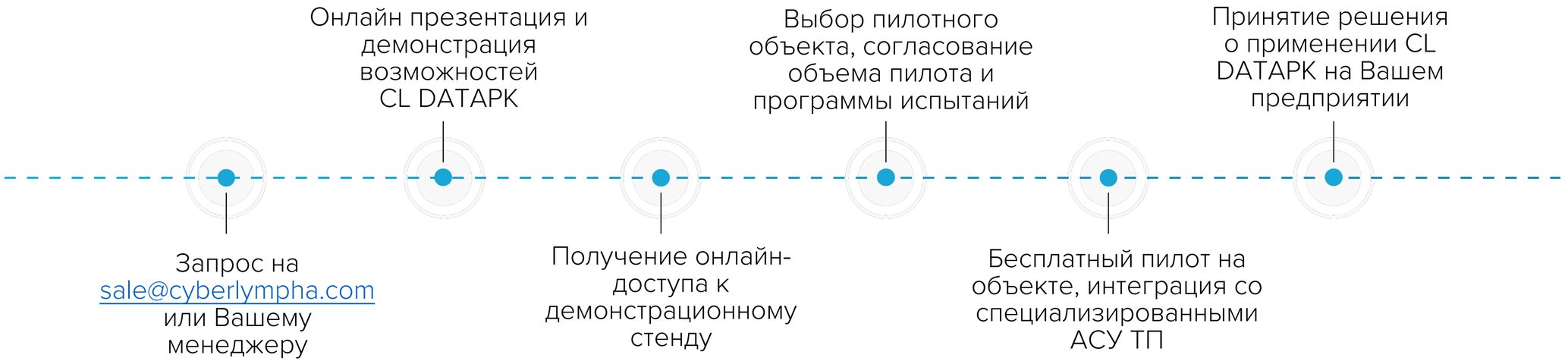
Классы средств защиты информации в соответствии с Приказом №235 ФСТЭК России

- Создан для АСУ ТП и учитывает все требования к средствам защиты информации
- Реализует все необходимые возможности класса промышленных СОВ
- Обладает дополнительным функционалом нескольких классов решений
- Сертифицирован ФСТЭК России
- Защищает значимые объекты КИИ в РФ
- Протестирован производителями АСУ ТП

ПРИМЕНИТЬ CL DATAPK

CyberLympha®

Пилотное внедрение CL DATAPK



CyberLympha®

КОНТАКТЫ

Алексей Комаров

Руководитель практики
ИБ АСУ ТП

CyberLympha®

sale@cyberlympha.ru

CYBERLYMPHA.RU