CyberLympha®

# CyberLympha DATAPK: больше, чем промышленный IDS

**Павел Богданов**

Директор лаборатории кибербезопасности

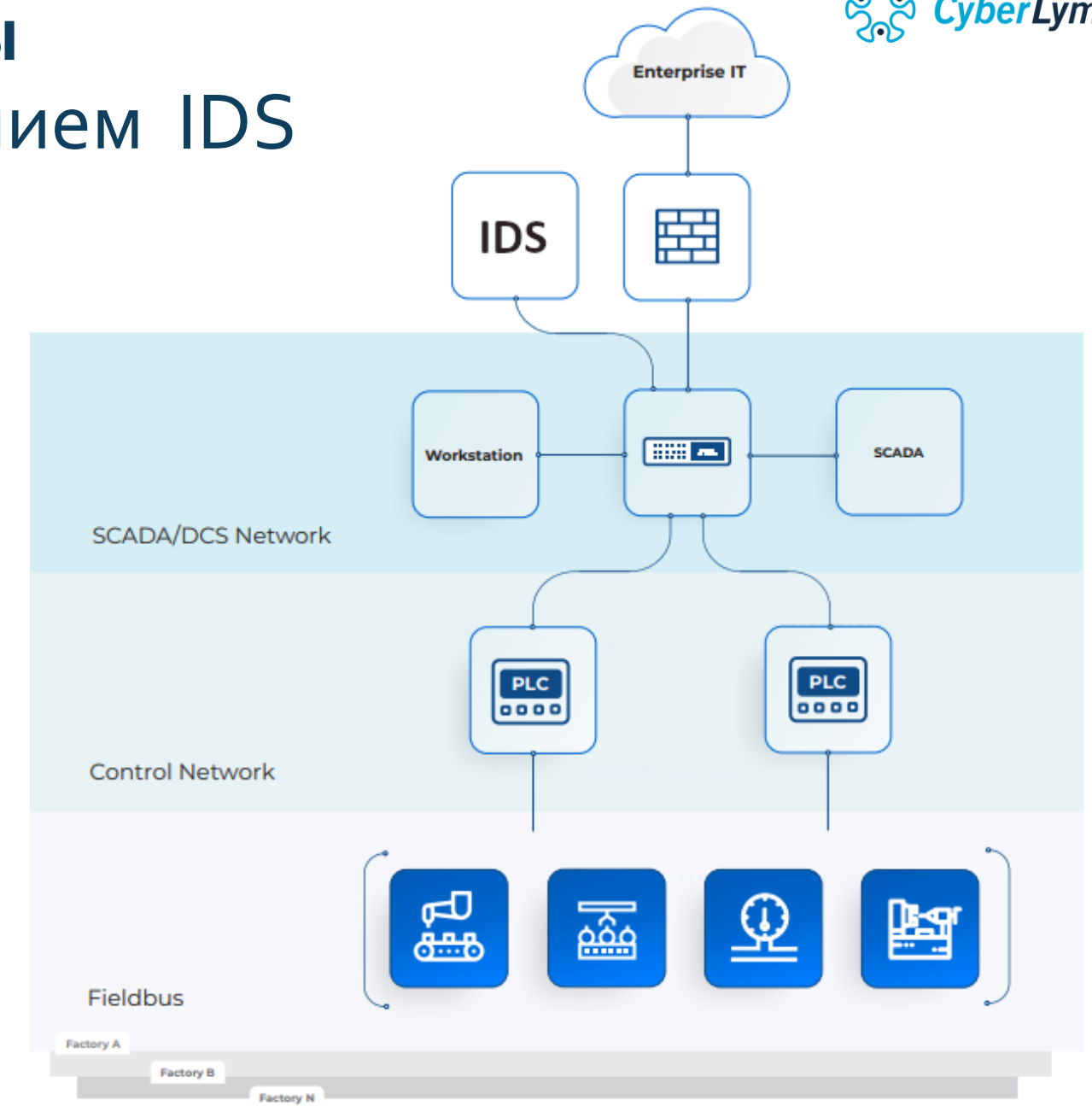
ТБ Форум, 29.09.2021

# **Типовая схема защиты объекта** с использованием IDS

CyberLympha®

## Преимущества решения:

+ Простота интеграции
+ Неинвазивность метода
+ Универсальность подхода



# Мнение **экспертов**

CyberLympha®

## Dale Peterson

ICS security researcher

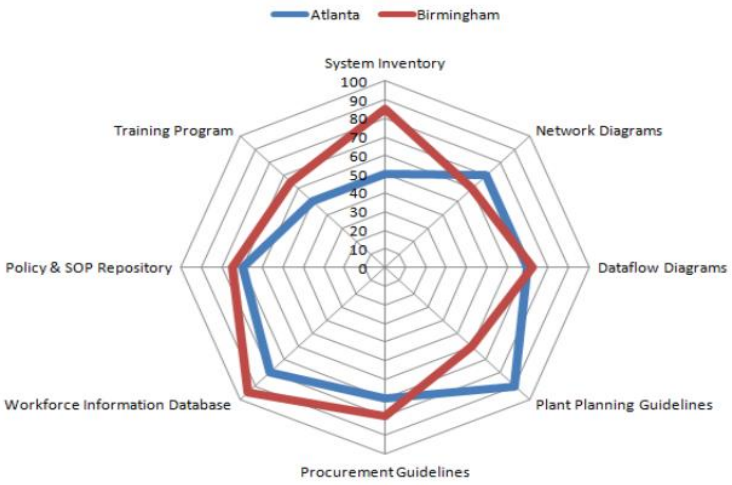
- Passive-only is a phase that will end soon
- You would want to ingest firewall logs, application whitelisting events, Windows, Linux and ICS application security events, switch logs and eventually PLC/controller events
- IDS/IPS is only part of a detection solution. It has proved to be a viable product category and it would be relatively simple to add ICS anomaly detection technology to their sensors and management systems.

https://dale-peterson.com/2018/07/23/the-future-of-the-ics-cyber-security-detection-market/

## Ralph Langner

(OT Security Analyst, создатель RIPE framework)

- ACTIVE discovery — because it's better and cheaper
- Documentation: A cyber system inventory, manifested as a database, stores information on hardware systems, the software running on those systems, network association, and configuration details.




https://www.langner.com/wp-content/uploads/2017/04/The-RIPE-Framework.pdf

# Причины:

CyberLympha®

## Не все угрозы ИБ сетевые

- Подключение съемных устройств
- Нерегламентированные изменения настроек безопасности
- Выключение конечного устройства

## Внедрение шифрования трафика:

Уже сейчас:

- RDP, SSH, HTTPS, …
- OPC UA
- Modbus TLS
- S7CommPlus

В будущем будет становиться больше

## Технологические сложности обеспечения полного покрытия IDS/IPS:

- Обеспечение сбора трафика во всех точках обмена
- Потери пакетов при зеркалированиии трафика
- Ограничения со стороны сетевого оборудования
- Повышение нагрузки на каналы связи (в отдельных случаях реализации)

# Мониторинг **сети**

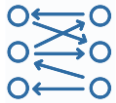
CyberLympha®

## Анализ потоков данных

- Обнаружение сетевых узлов и ведение каталога активов
- Выявление информационных потоков и ведение их базы
- Визуализация карты сети
- Выявление запрещенных коммуникаций и управляющих команд
- Обнаружение вторжений

# Комплексный **мониторинг ИБ**

CyberLympha®



## Анализ потоков данных

- Пассивное получение данных посредством SPAN или зеркальных портов сетевого оборудования
- Визуализация карты сети и потоков
- Выявление и инвентаризация узлов

## Управление конфигурациями

- Безагентный сбор данных
- Использование встроенных механизмов объектов защиты для сбора конфигураций
- Расширение списка поддерживаемых объектов без необходимости доработки CL DATAPK

## Обнаружение инцидентов

- Безагентный сбор данных
- Нормализация, корреляция, визуализация
- Поддержка новых источников событий без необходимости доработки продукта

## Поиск уязвимостей и оценка соответствия

- Безагентный сбор данных
- Поддержка сторонних баз данных определений OVAL (в том числе БДУ ФСТЭК России)

# CyberLympha DATAPK: на страже систем автоматизации

**Защищаемая АСУ ТП**

Сетевой трафик

Конфигурации

События

Анализ защищенности

CyberLympha DATAPK

- **Непрерывный мониторинг отклонений от эталонной модели**
- **Связь данных из различных источников**
- **Пассивный сбор данных**
- **Активный сбор без агентов**
- **Адаптация к защищаемой системе без изменения кода**
- **Широкий функционал в одном устройстве**
- **Масштабирование и иерархия**

Осведомленность о состоянии ИБ АСУ ТП

Выявление инцидентов

Соответствие Законодательству и best practice

**Подразделения ИБ**

**Нефть и газ**

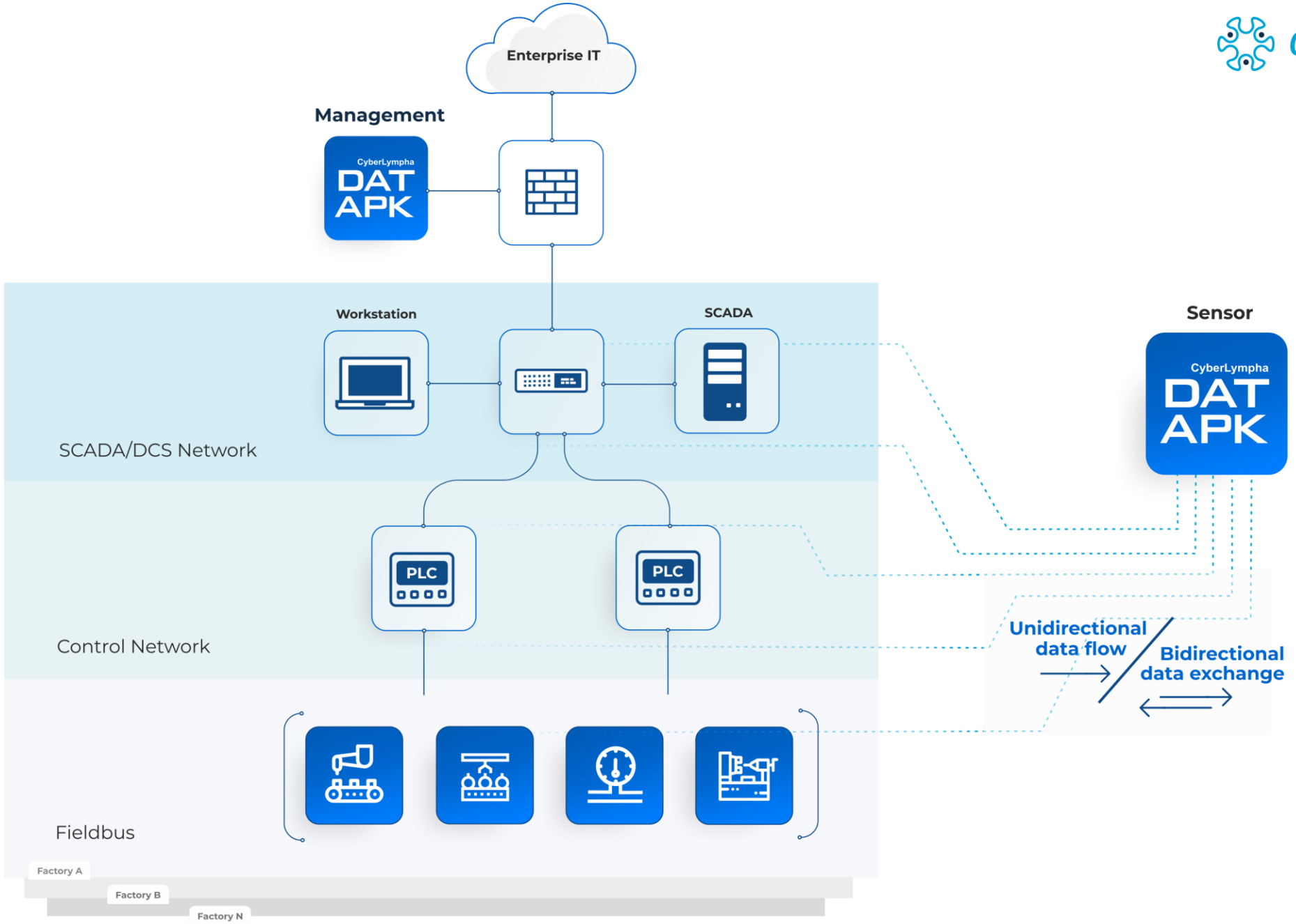
**Металлургия**

**Энергетика и генерация**

**Промышленность**

**Умный город**

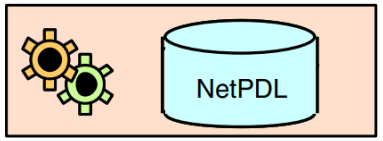
CyberLympha®



# Технологии:

CyberLympha®

## Анализ потоков данных


## Управление конфигурациями





## Обнаружение инцидентов




## Поиск уязвимостей и оценка соответствия

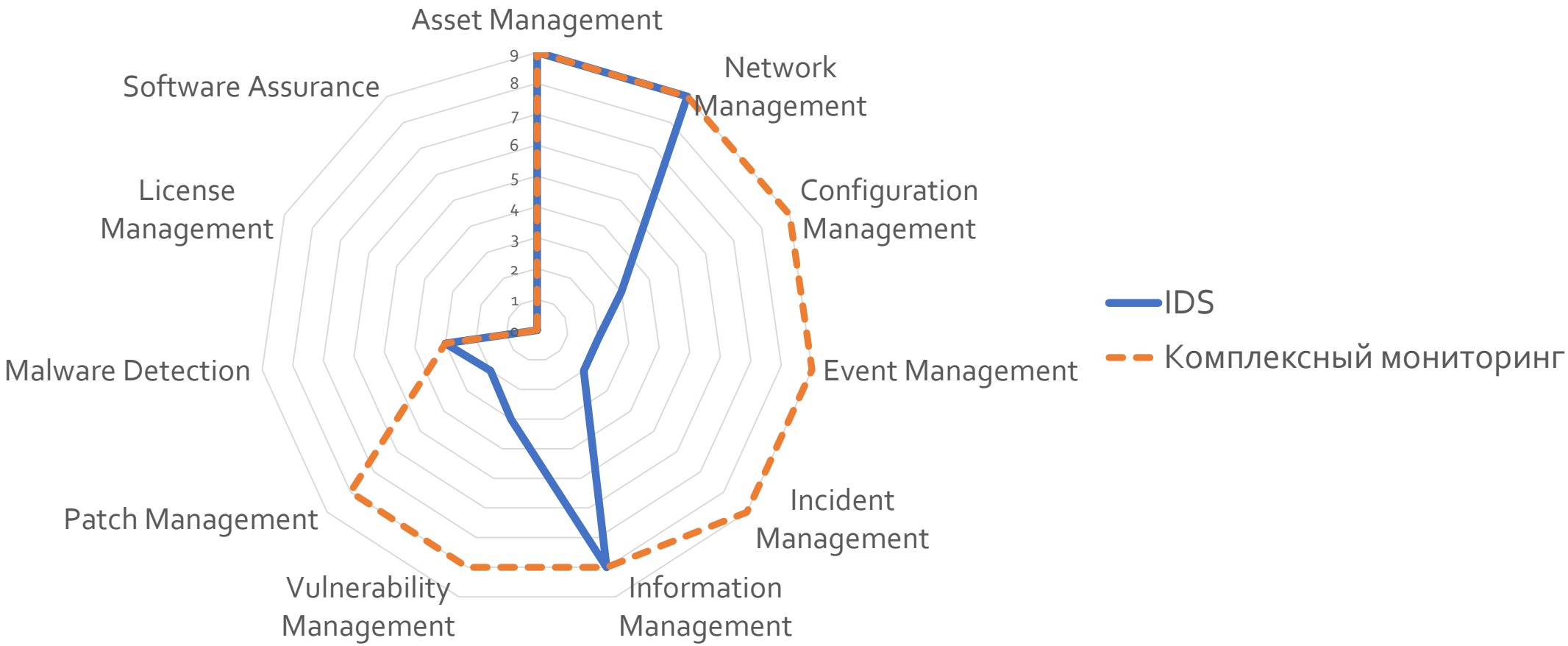

*oval.mitre.org*

# **Интеграция** со смежными системами

## Интеграция со смежными системами:

+ Сбор событий со смежных систем безопасности
+ Контроль конфигурации компонентов смежных систем
+ Обмен данными с системами SIEM, GRC, SoC и системами оркестрации средств защиты
+ Интеграция на основе стандартных протоколов (SMTP, Syslog, API, OPC UA, Rabbit MQ)

# NIST: SP 800-137 «Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations»



# Проект стандарта ГОСТ: Защита информации.
## Мониторинг информационной безопасности

CyberLympha®

**5.1.2 При формировании перечня источников данных следует учитывать необходимость получения следующей информации:**

+ данные о событиях безопасности от средств, осуществляющих регистрацию событий безопасности (источников событий безопасности);
+ данные о результатах выявления (поиска) уязвимостей
+ данные о результатах контроля обновлений программного обеспечения
+ данные о результатах контроля состава программно-технических средств, программного обеспечения и средств защиты информации (инвентаризационных данных)
+ данные о результатах контроля соответствия настроек программного обеспечения и средств защиты информации установленным требованиям безопасности;
+ данные о работоспособности (неотключении) программного обеспечения и средств защиты информации;

✓ информация **о результатах контроля потоков информации;**

+ данные о действиях пользователей и процессов, необходимых для выявления преднамеренного или непреднамеренного нарушения установленных политик безопасности, регламентов работы, фактов запрещенной деятельности, попыток совершения несанкционированного доступа и утечки конфиденциальной информации;

✓ **данные о** новых **угрозах безопасности информации**

# Проект стандарта ГОСТ: Защита информации.
## Мониторинг информационной безопасности

CyberLympha®

**5.1.2 При формировании перечня источников данных следует учитывать необходимость получения следующей информации:**

- ✓ данные о событиях безопасности от средств, осуществляющих регистрацию событий безопасности (источников событий безопасности);
- ✓ данные о результатах выявления (поиска) уязвимостей
- ✓ данные о результатах контроля обновлений программного обеспечения
- ✓ данные о результатах контроля состава программно-технических средств, программного обеспечения и средств защиты информации (инвентаризационных данных)
- ✓ данные о результатах контроля соответствия настроек программного обеспечения и средств защиты информации установленным требованиям безопасности;
- ✓ данные о работоспособности (неотключении) программного обеспечения и средств защиты информации;
- ✓ информация о результатах контроля потоков информации;
- ✓ данные о действиях пользователей и процессов, необходимых для выявления преднамеренного или непреднамеренного нарушения установленных политик безопасности, регламентов работы, фактов запрещенной деятельности, попыток совершения несанкционированного доступа и утечки конфиденциальной информации;
- ✓ данные о новых угрозах безопасности информации

# Результаты

**45+** Корпоративных Заказчиков применяют решения от CyberLympha

**7/10** Крупнейших нефтяных и газовых промышленных компаний России

**6/10** Крупнейших энергетических компаний России

**7/10** крупнейших металлургических компаний России

**7/10** Крупнейших химических компаний России

История коммерческих внедрений с 2017 года

1000+ комплексов CL DATAPK в промышленной эксплуатации

К сожалению мы можем приводить только весьма общие обезличенные данные в силу имеющихся договоренностей с нашими Заказчиками.

# А дальше?

CyberLympha®

## Познакомиться с CL DATAPK

- ✓ Публичное демо решения
- ✓ Стенды в лабораториях кибербезопасности
- ✓ Пилотное внедрение на Вашем предприятии

## Приобрести CL DATAPK

- ✓ Запрос на info@cyberlympha.com

## Изучить CL DATAPK в деталях

- ✓ Официальные курсы обучения в авторизованном учебном центре IT-Cloud

CyberLympha
DATAPK

# Контакты

CyberLympha®


## Павел Богданов

**Директор лаборатории кибербезопасности**

**8 800 350 31 85**

**info@cyberlympha.com**


**cyberlympha.ru**