CyberLympha®

Зачем нужен SOC для АСУ ТП?

Алексей Шанин

Директор ООО «СайберЛимфа»

О КОМПАНИИ

CyberLympha®

Резидент инновационного фонда Сколково

Собственная лаборатория кибербезопасности и исследовательский центр

Технологические и бизнес-партнеры

Платформа обнаружения компьютерных атак и аномалий CyberLympha

Поставка современных решений в области кибербезопасности на российский и международные рынки

Sk Участник

О КОМПАНИИ

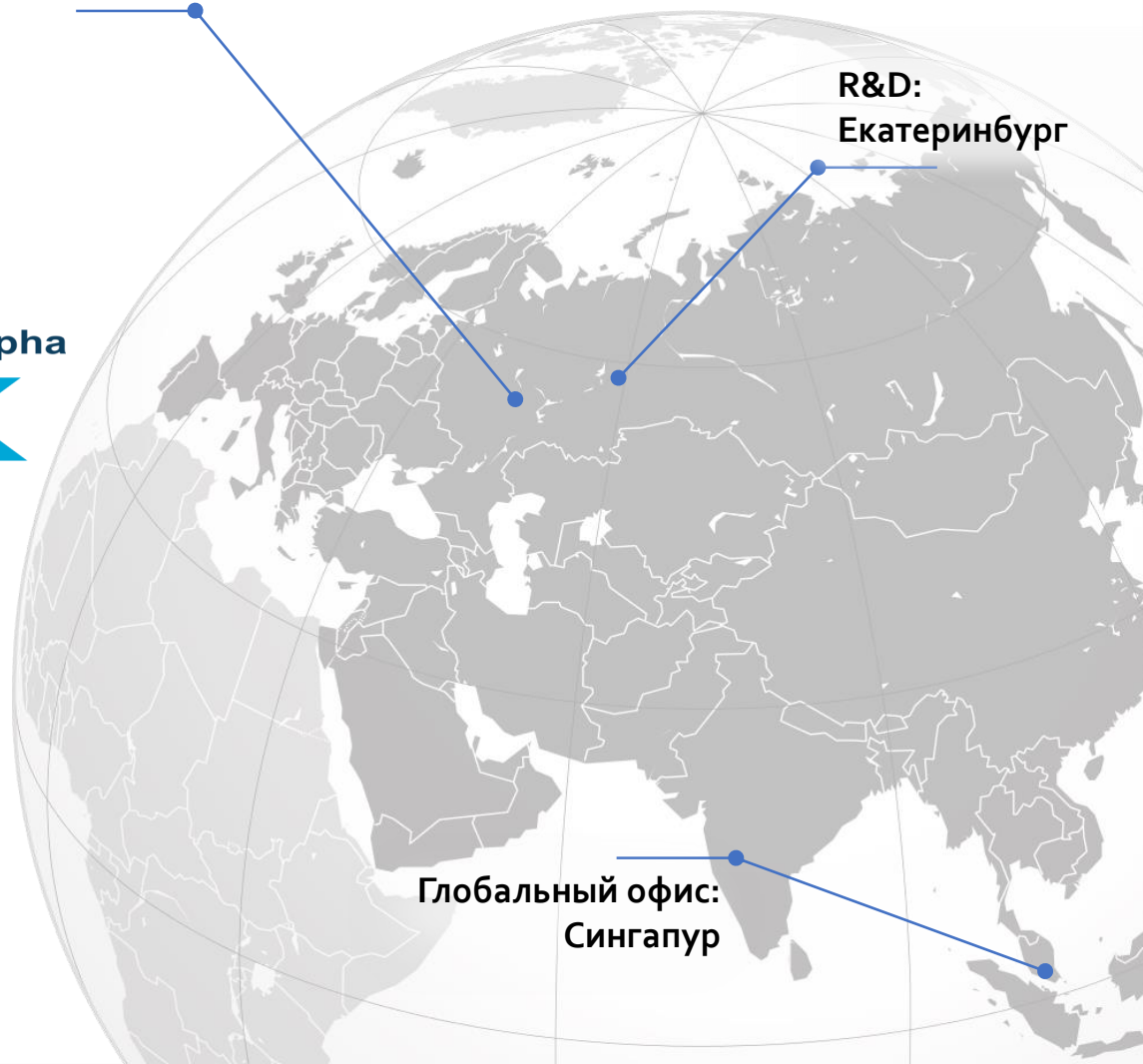
CyberLympha®

- Нефть и газ
- Энергетика и генерация
- Металлургия
- Умный город
- Промышленность

CLThymus CyberLympha

CyberLympha DATAPK

ITM CyberLympha



ПРОМЫШЛЕННЫЕ СИСТЕМЫ АВТОМАТИЗАЦИИ

CyberLympha®

Разнообразные системы автоматизации

Старые решения медленно отмирают

…и быстро появляются новые

Нуждаются в эффективных средствах защиты

Растет число атак

…как и число самих объектов атак

Но их некому настраивать и эксплуатировать

Не хватает квалифицированных кадров для защиты

…на фоне растущей сложности систем

SecOps в АСУ ТП

CyberLympha®

Оперативный режим

- Обновление ПО
- Обновление сигнатур
- Изоляция и останов
- Установка агентов
- Получение данных

Технологический останов

- Длительность
- Фокус персонала
- Тестирование работоспособности
- Откат к рабочей конфигурации

SecOps - объединение усилий команды ИТ-подразделений, подразделений разработки услуг и команды ИБ для построения стабильной, безопасной и надежной ИТ-инфраструктуры предприятия

Мониторинг ИБ: задачи

Инвентаризация

Состояние
защищенности

Инциденты ИБ

Законодательство

Мониторинг ИБ: задачи

- Инвентаризация
- Состояние защищенности
- Инциденты ИБ
- Законодательство

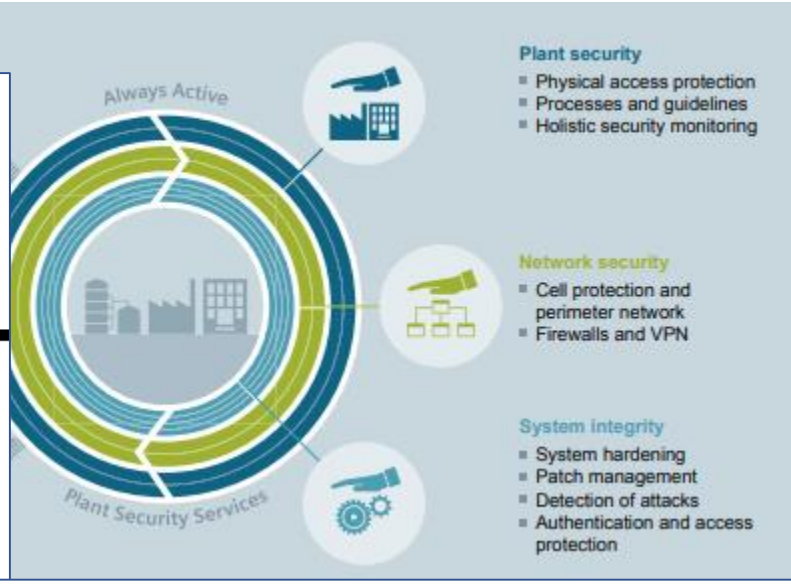
НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р (проект, окончательная редакция)

Защита информации

МОНИТОРИНГ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Общ



NIST Special Publication 800-137

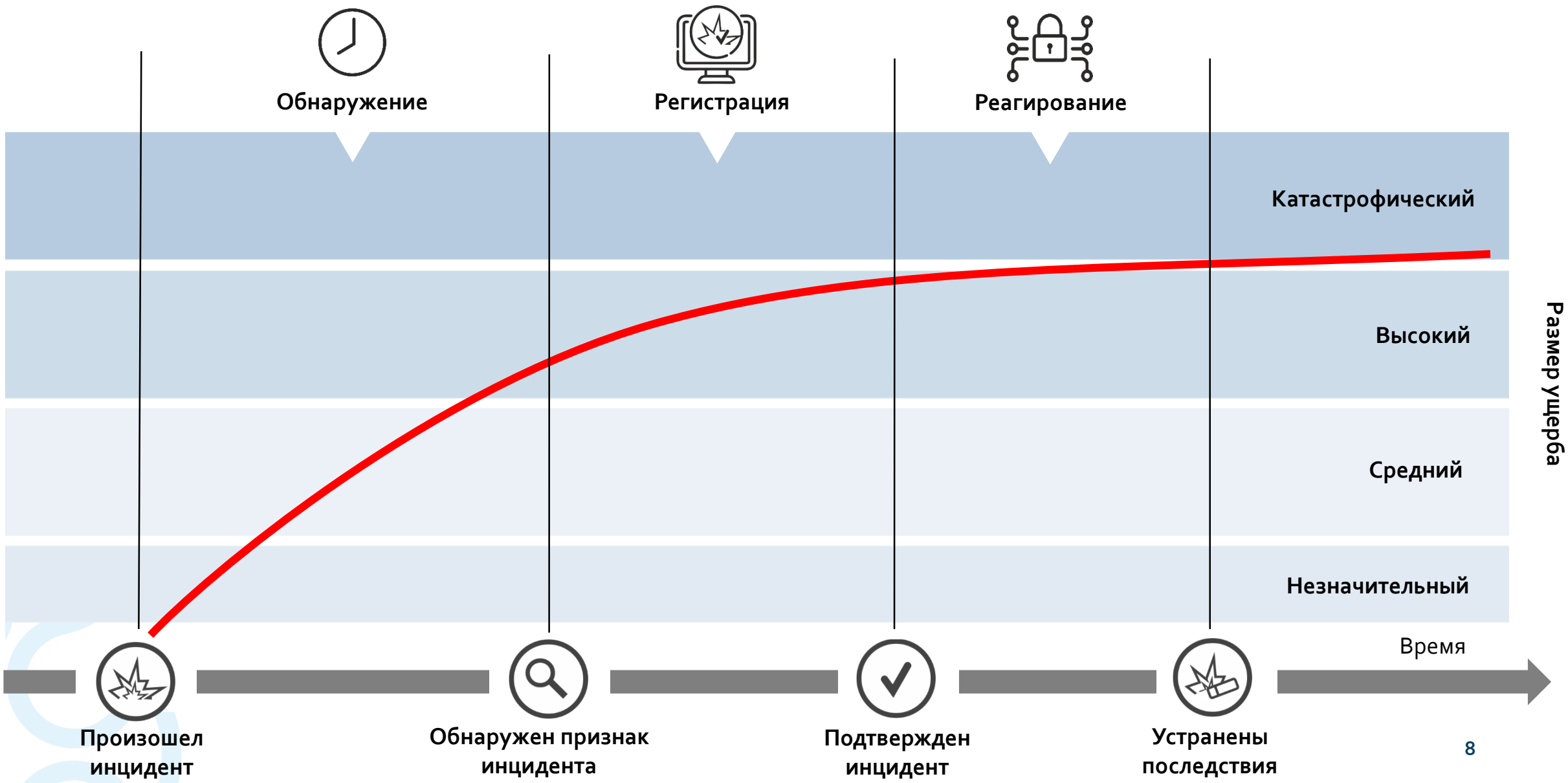
Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

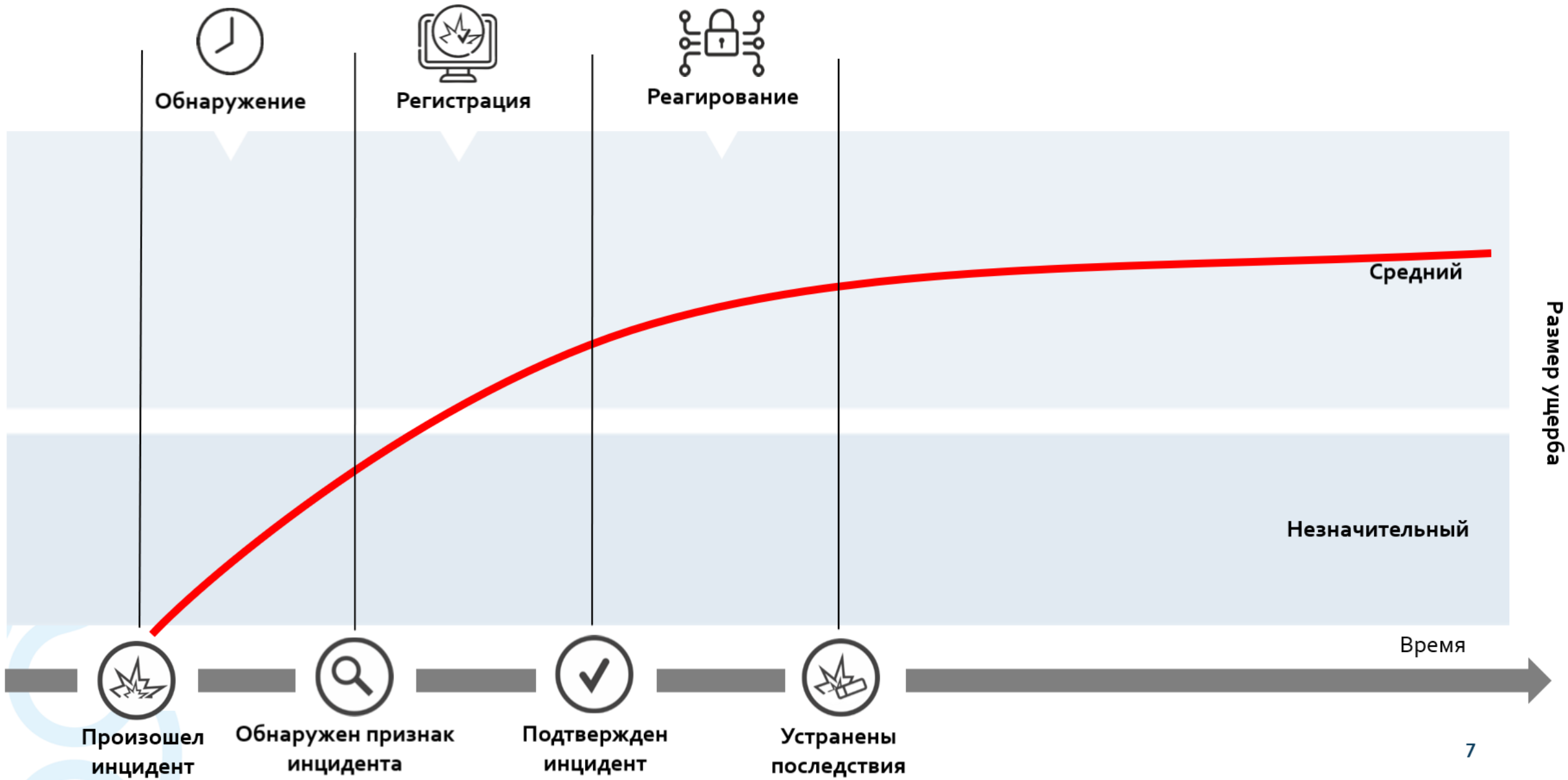
Kelley Dempsey
Nirali Shah Chawla
Arnold Johnson
Ronald Johnston
Alicia Clay Jones
Angela Orebaugh
Matthew Scholl
Kevin Stine

- Федеральный закон "О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 N 187-ФЗ
- Приказ ФСТЭК России от 14.03.2014 N 31
- Приказ ФСТЭК России от 21.12.2017 N 235
- Приказ ФСТЭК России от 25.12.2017 N 239

МОНИТОРИНГ ИБ ВО ВРЕМЕНИ

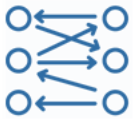


МОНИТОРИНГ ИБ ВО ВРЕМЕНИ



Комплексный мониторинг ИБ

CyberLympha®



Сетевой трафик

Анализ сети IDS/DPI

События

Управление событиями и инцидентами

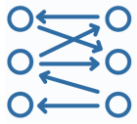
Контроль конфигураций и compliance

Состояние активов

Анализ уязвимостей

Комплексный мониторинг ИБ

CyberLympha®



Сетевой трафик

Продукт A

Анализ сети IDS/DPI

Продукт C

Контроль конфигураций и compliance

Состояние активов

События

Управление событиями и инцидентами

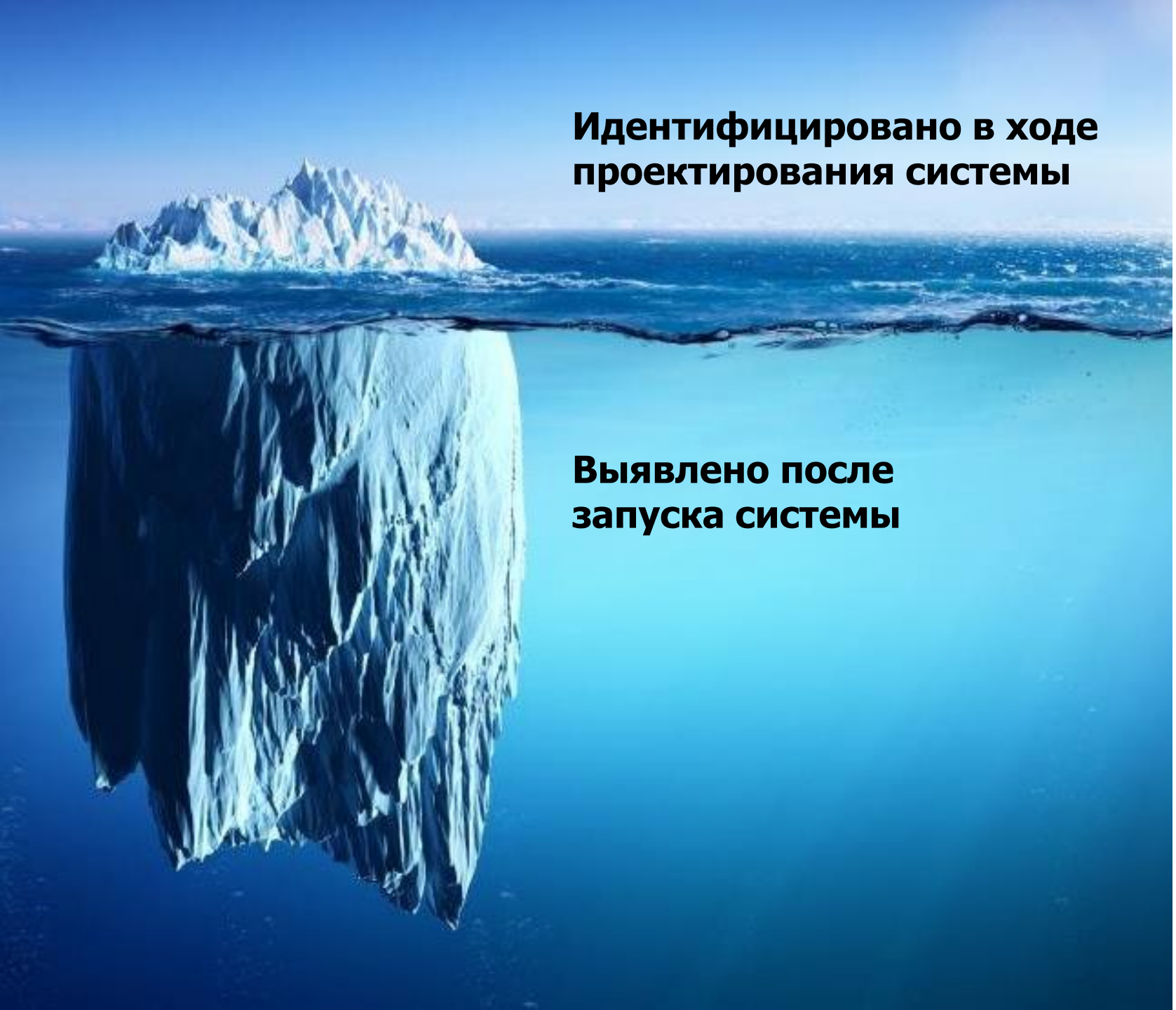
Продукт B

Анализ уязвимостей

Продукт D

Комплексный мониторинг ИБ

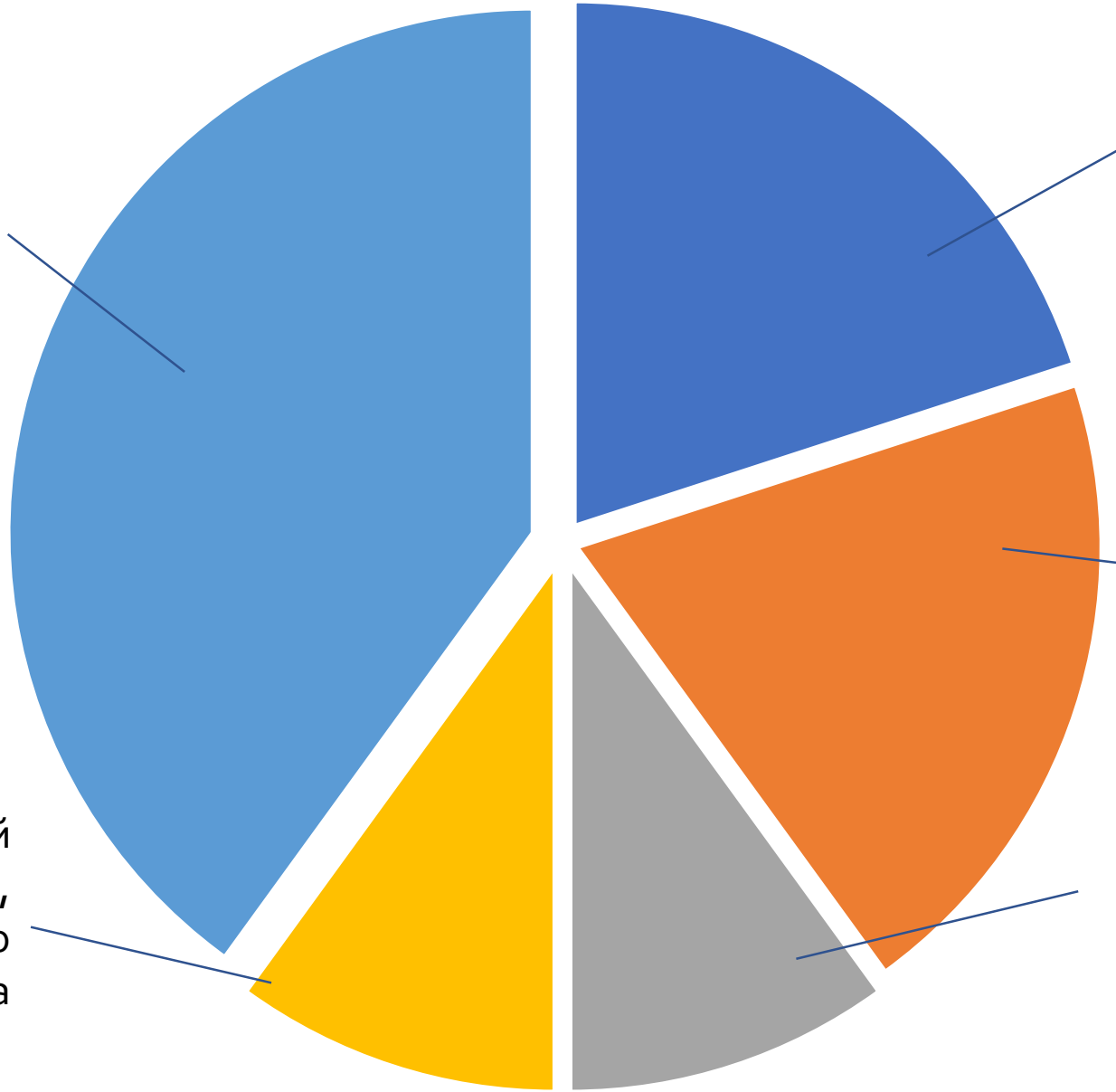
CyberLympha®



CyberLympha®

- Множество неизвестных узлов
- Расположение узлов неизвестно
- Неизвестные взаимодействия между узлами и сетями
- Отсутствие безопасной конфигурации
- Не настроен аудит
- Отсутствуют учетные данные

Данные с реального объекта



~ 40% неизвестный трафик специального ПО АСУ ТП

~ 20% трафик известный службе автоматизации

~ 20% стандартный служебный трафик сети

~ 10% известный служебный трафик, легитимность которого должна быть уточнена

~ 10% трафик, которого не должно быть (нарушения политики)

Нужен ли SOC в АСУ ТП?

CyberLympha®

Инциденты ИБ:

- Предупреждение
- Выявление
- Расследование
- Ликвидация

Субъекты КИИ:

- Наличие подразделения
- Безопасный канал ГосСОПКА

Мировые практики: Singapore OT Security Masterplan

CyberLympha®

OT CYBERSECURITY DETECTION AND MONITORING CAPABILITIES

A critical aspect of strengthening the OT cybersecurity posture in Singapore involves constant, robust monitoring of network activities within CII, and swift and decisive responses in the event anomalous activity is detected. This requires putting in place Security Operations Centres (SOCs) at the sectoral level to oversee, monitor and coordinate cybersecurity efforts between Government agencies and CII owners.

Mr Ngiam Shih Chun
Chief Executive, Energy Market Authority, Singapore's energy industry regulator

"The power system is a complex and critical network. With digitalisation and the rising trend of cyber threats, the Energy Market Authority will need to work closely with CSA to strengthen the reliability and resilience of our systems."

All CII sectors who operate OT systems are developing or have in place sectoral SOCs suited toward their respective operating environments, with three examples highlighted below:

- Since 2017, the Energy Market Authority (EMA) has collaborated with CSA on two systems to strengthen the cybersecurity of the power sector. This included a Sectoral Detection & Early Warning System (SDEWS) to detect cyber-attacks. The SDEWS analyses and monitors security logs sent from the power sector's CII for anomalous behaviour in the OT environment. Complementing this is the Cyber Threat Detection System (CTDS) that detects cyber anomalies in the OT network. These systems help EMA safeguard our power systems and ensure a reliable supply of electricity and gas for Singapore.
- The Maritime and Port Authority of Singapore (MPA) operationalised and officially launched the Maritime Cybersecurity Operations Centre (MSOC) in May 2019. The MSOC conducts round-the-clock detection, monitoring, and correlation and analysis of data activities across all maritime CII. This has helped to strengthen the maritime cybersecurity posture in Singapore against potential IT and OT cyber-attacks. Besides possessing the capability to detect and analyse anomalous activities and cyber threats in the IT environment, the MSOC is also able to respond to cybersecurity incidents by employing and integrating advanced OT technology solutions. In addition, MPA is in the process of linking the MSOC and the Port Operations Control Centre (POCC) to respond to cyber-physical incidents in a more holistic and timely manner.
- The Public Utilities Board (PUB) is also leveraging the expertise and infrastructure offered by the cybersecurity industry, and has subscribed to Managed Security Services for its SOC operations. This allows PUB to monitor and analyse its cybersecurity posture, as well as provide the cyber situational awareness and anticipate cyber threats. As part of PUB's capability development roadmap, it will also be harnessing new technologies to enhance cybersecurity resilience for the water sector.

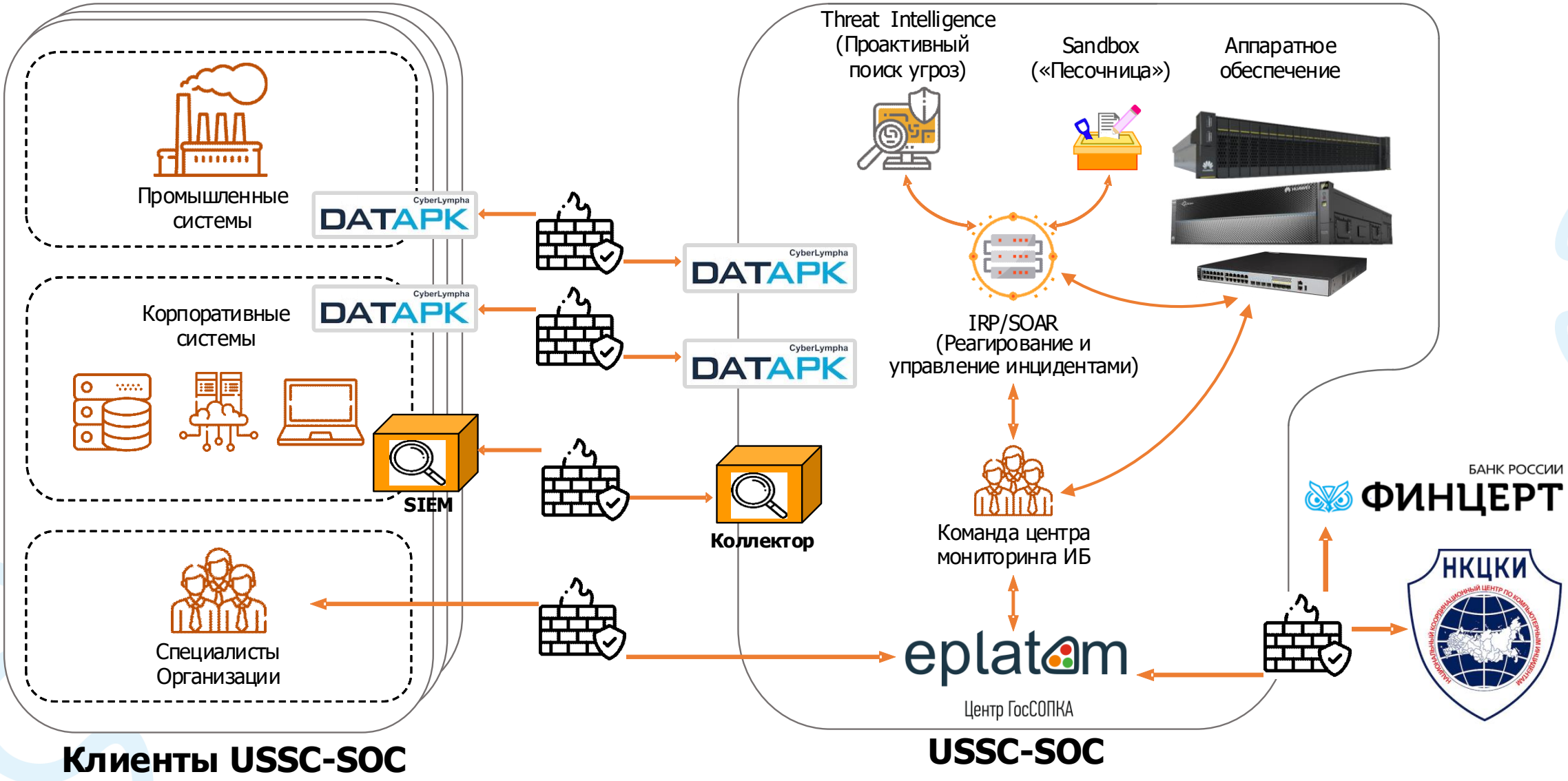
Собственный SOC

CyberLympha®

Собственный SOC
Срок запуска
Капитальные вложения и инфраструктура
Актуальный контент
Проблема кадров
Лицензия ФСТЭК России

Любой SOC
Действия по реагированию
Регламентные работы

Как это работает? USSC-SOC



Как это работает? USSC-SOC

CyberLympha®

Обеспечивает SOC:

- Правила нормализации событий
- Правила обнаружения инцидентов
- Сигнатуры обнаружения вторжений
- Определения уязвимостей

USSC-SOC

CL DATAPK в центре обработки данных USSC-SOC

CyberLympha DATAPK

CL DATAPK защищаемого объекта

Принимает SOC:

- Обнаруженные объекты защиты
- Потоки данных
- Карты сетевого взаимодействия
- Собранные конфигурации
- События
- Выявленные инциденты ИБ
- Результаты проверок на уязвимости

А дальше?

Познакомиться с CL DATAPK

- ✓ Публичное демо решения
- ✓ Пилотное внедрение на Вашем предприятии

Познакомиться с USSC-SOC

- ✓ Пилотное внедрение на Вашем предприятии

Приобрести CL DATAPK

- ✓ Запрос на sale@cyberlympha.ru

Изучить CL DATAPK в деталях

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

Контакты

CyberLympha®

Алексей Шанин

Директор ООО «СайберЛимфа»

cyberlympha.ru