CyberLympha®

Выявление и ликвидация последствий компьютерных инцидентов в 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

3 инновационных разработки

50 сотрудников в штате

5 лет на рынке ИТ

1000 инсталляций

ПРОМЫШЛЕННЫЕ СИСТЕМЫ АВТОМАТИЗАЦИИ

CyberLympha®

Разнообразные системы автоматизации

Старые решения медленно отмирают

…и быстро появляются новые

Нуждаются в эффективных средствах защиты

Растет число атак

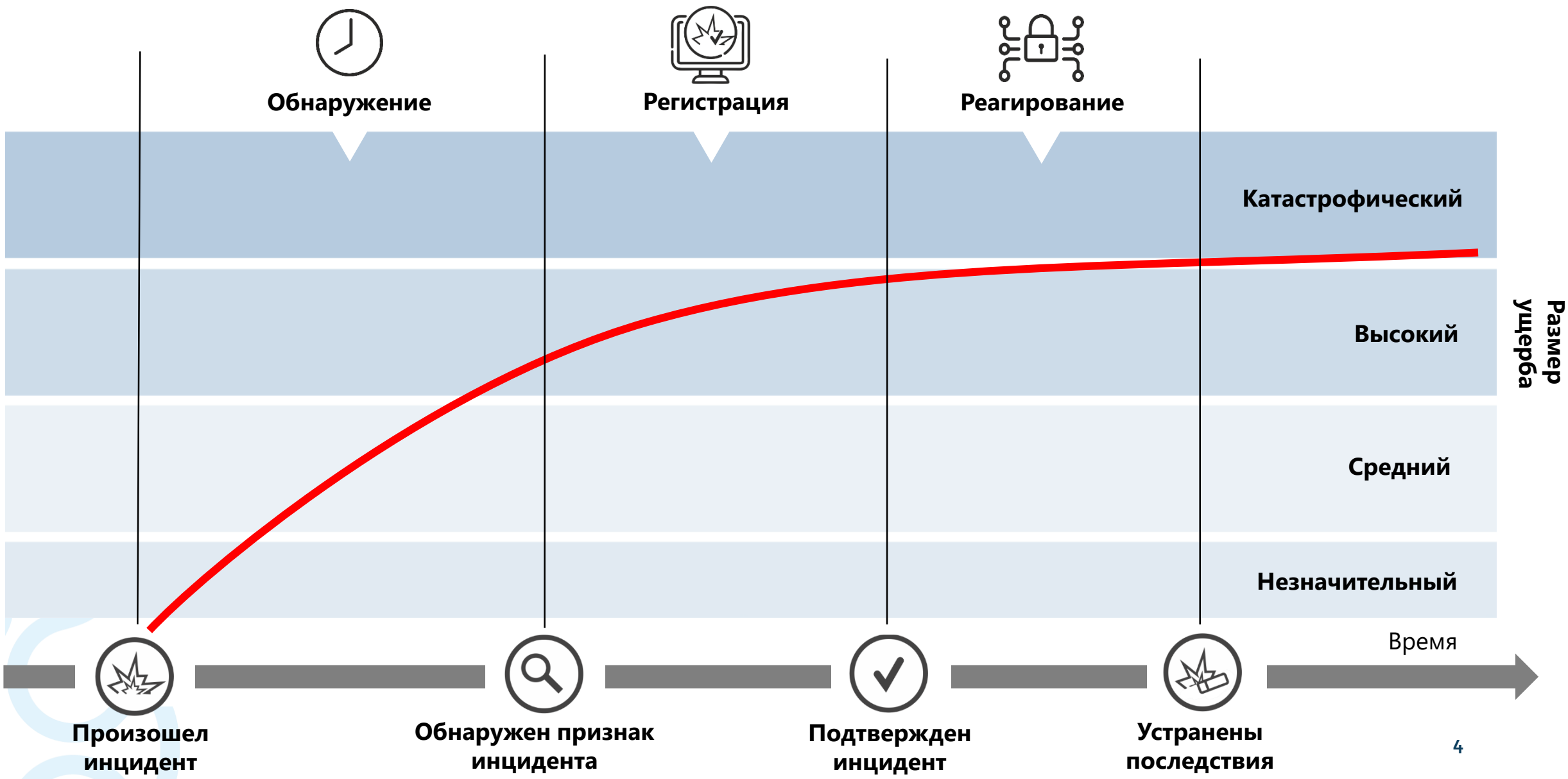
…как и число самих объектов атак

Но их некому настраивать и эксплуатировать

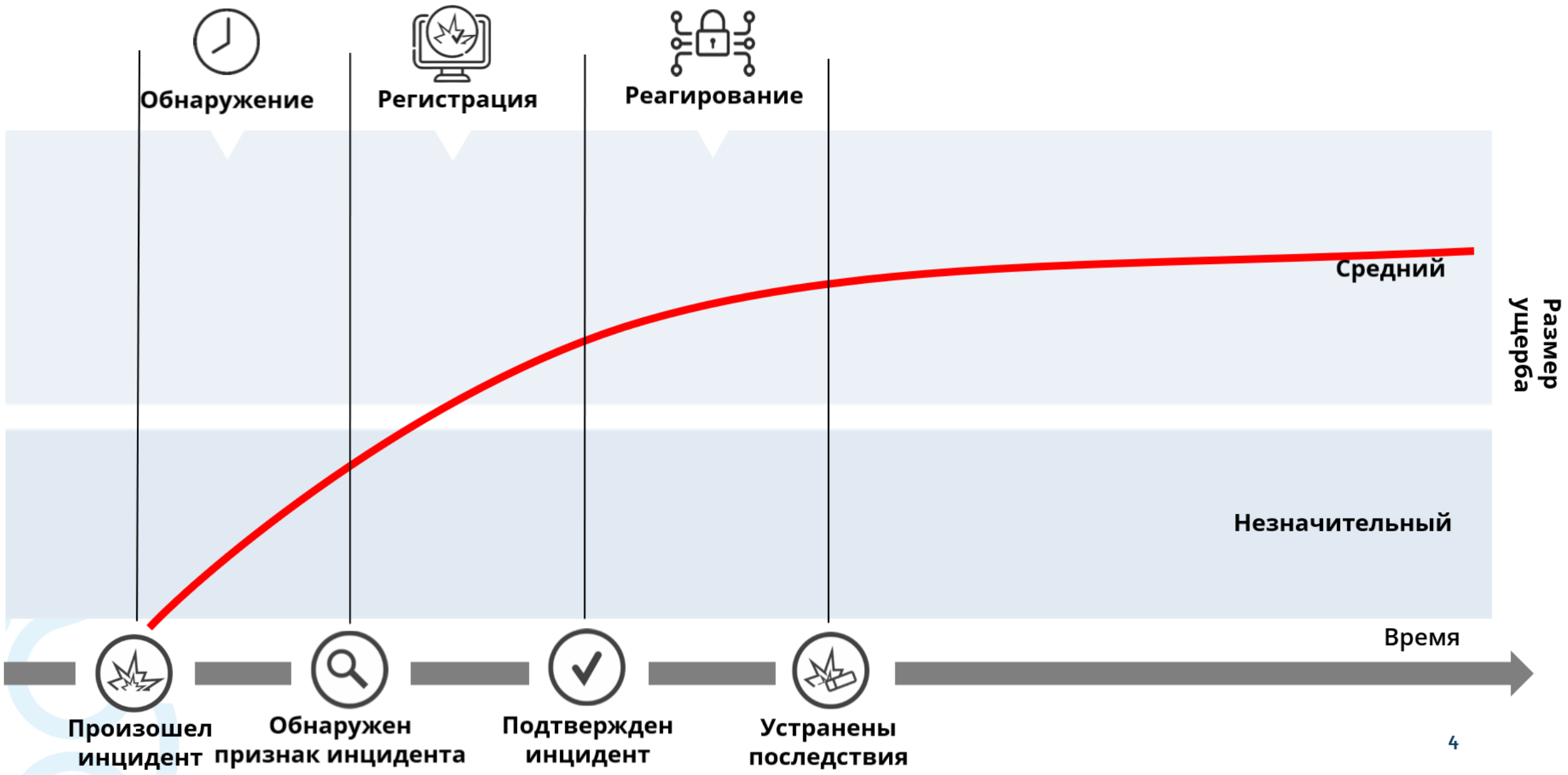
Не хватает квалифицированных кадров для защиты

…на фоне растущей сложности систем

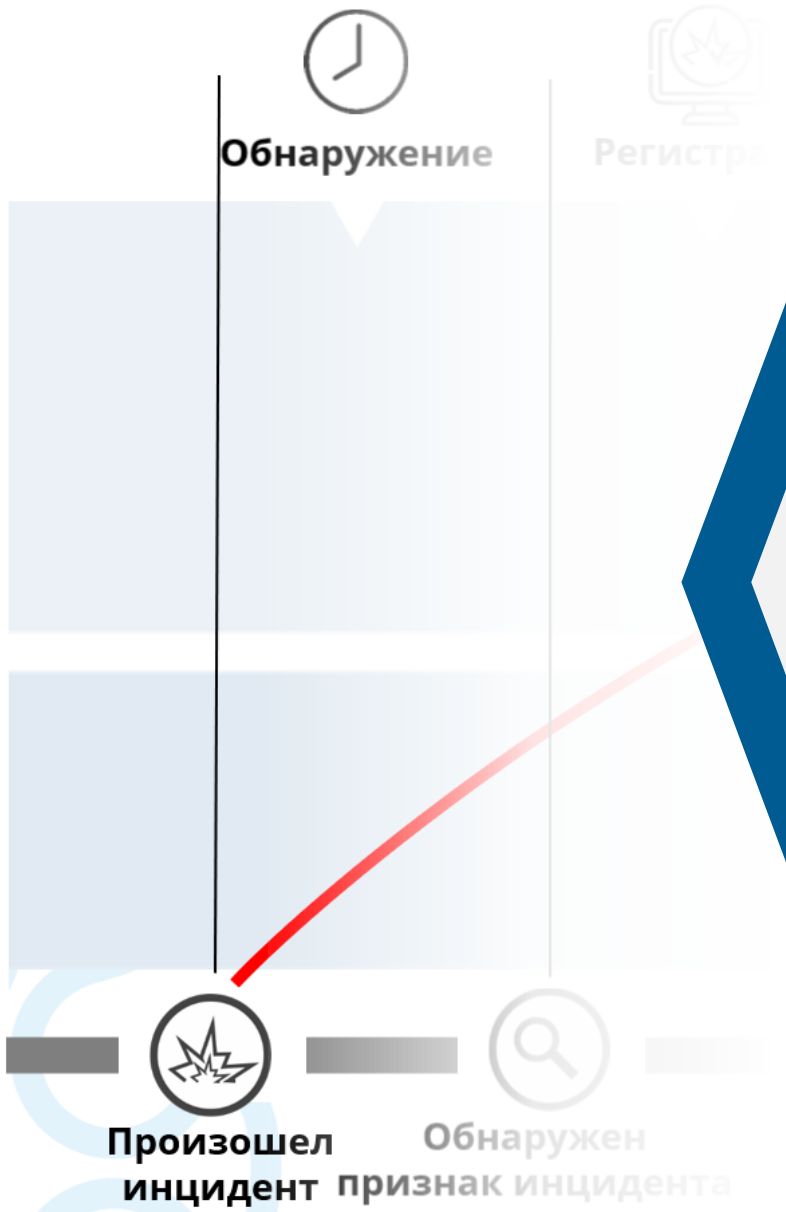
БЫСТРОЕ И ТОЧНОЕ ОПРЕДЕЛЕНИЕ ИНЦИДЕНТОВ ИБ СНИЖАЕТ УЩЕРБ ДЛЯ БИЗНЕСА



БЫСТРОЕ И ТОЧНОЕ ОПРЕДЕЛЕНИЕ ИНЦИДЕНТОВ ИБ СНИЖАЕТ УЩЕРБ ДЛЯ БИЗНЕСА



Платформа CyberLympha

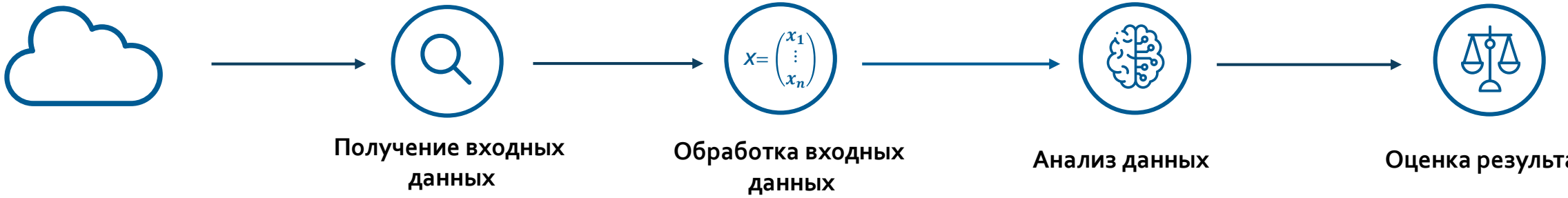


Концепция киберимунной системы с возможностью поэтапного развития адаптируемой системы защиты

CyberLympha DATAPK	Комплекс оперативного мониторинга состояния ИБ и контроля защищенности систем автоматизации
CL Thymus CyberLympha	Выявление и ликвидация последствий компьютерных инцидентов с применением интеллектуальных алгоритмов
ITM CyberLympha	Контроль безотказного функционирования, вычислительных ресурсов и каналов связи

ВЫБОР ОПТИМАЛЬНЫХ ТЕХНОЛОГИЙ

CyberLympha®



Основные варианты реализации	Скорость обнаружения	Точность обнаружения	Гибкость	Сложность реализации
Сигнатурные средства обнаружения	☺	☺	☹	☺
Обнаружение аномалий на основе метаданных и классификации	😐	😐	☺	😐
Обнаружение на базе модели ИБ	☺	☺	☺	☹

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

Подразделения ИБ

Нефть и газ

Металлургия

Энергетика и генерация

Промышленность

Умный город

CyberLympha ITM – IT мониторинг для АСУ ТП

CyberLympha®

Компьютерный инцидент – факт нарушения и (или) прекращения функционирования объекта

- Для предотвращения **умышленных** компьютерных атак уже реализуются комплексные решения
- Для предотвращения отказов и сбоев отсутствует специализированная система защиты

Реализация мер обеспечения безопасности:

- ОДТ.3: Контроль безотказного функционирования средств и систем
- ОДТ.8: Контроль предоставляемых вычислительных ресурсов и каналов связи

Доступность узлов и сервисов →

Показатели производи-тельности →

Нагрузка на каналы связи →

Ошибки функциони-рования →

ITM
CyberLympha

- **Непрерывный мониторинг метрик**
- **Соотнесение данных с пороговыми значениями**
- **Генерация тревог при обнаружении сбоев**
- **Активный сбор с использованием агентов и без них**
- **Безопасность функционирования**
- **Масштабирование и иерархия**

→ Верхнеуровневая информация о состоянии ИТ и сервисов

→ Оповещение о сбоях

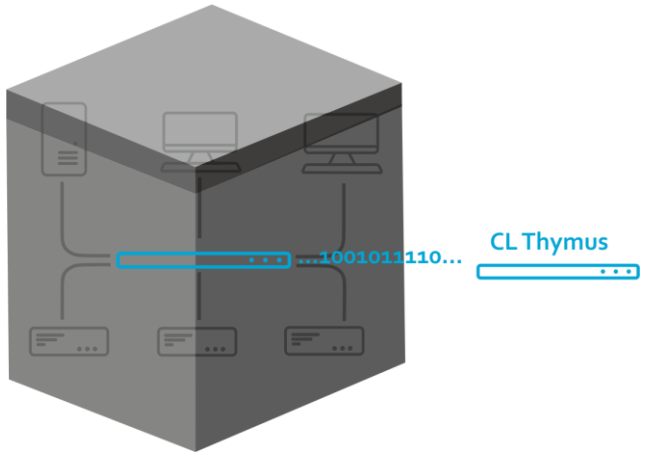
→ Соответствие законодатель-ству

CyberLympha Thymus – Инновационный[1] метод выявления аномалий

CyberLympha®

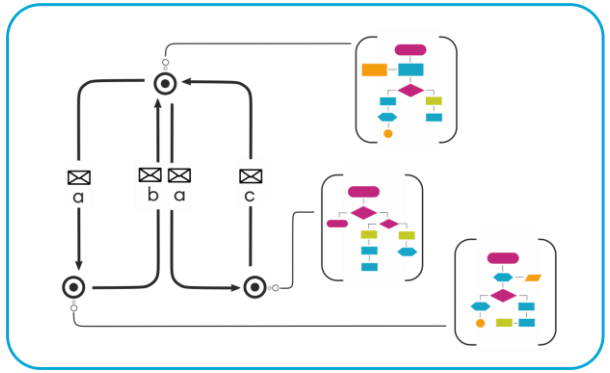
1

CyberLympha Thymus анализирует сетевой трафик защищаемой системы, не обладая никакой дополнительной информацией о ней



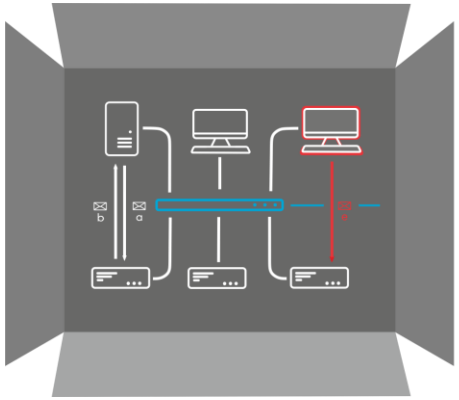
2

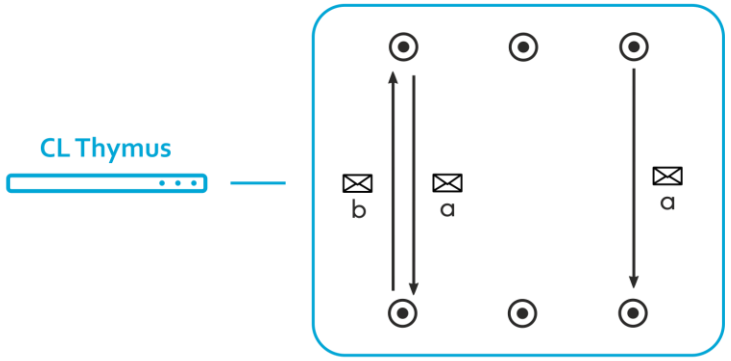
В ходе обучения CyberLympha Thymus определяет структуру протоколов обмена и алгоритм работы отдельных узлов защищаемой системы



3

После завершения обучения CyberLympha Thymus сопоставляет работу защищаемой системы с работой
модели и выявляет несоответствия, которые могут быть признаками инцидента ИБ





CL Thymus CyberLympha

1 - Патент № 2 738 460 на технологию выявления аномалий в работе сети автоматизированной системы

CYBERLYMPHA И СИСТЕМА БЕЗОПАСНОСТИ КИИ

CyberLympha®

СрЗИ от НСД

Средства антивирусной защиты

Средства управления событиями

Средства обнаружения вторжений

Средства анализа защищенности

Межсетевые экраны

Средства защиты каналов передачи данных

Встроенные механизмы защиты АСУ ТП

Подсистемы безопасности конкретных объектов КИИ

Система безопасности объектов КИИ

Планирование

Контроль

Реагирование

Совершенствование

Процессы обеспечения ИБ объекта КИИ

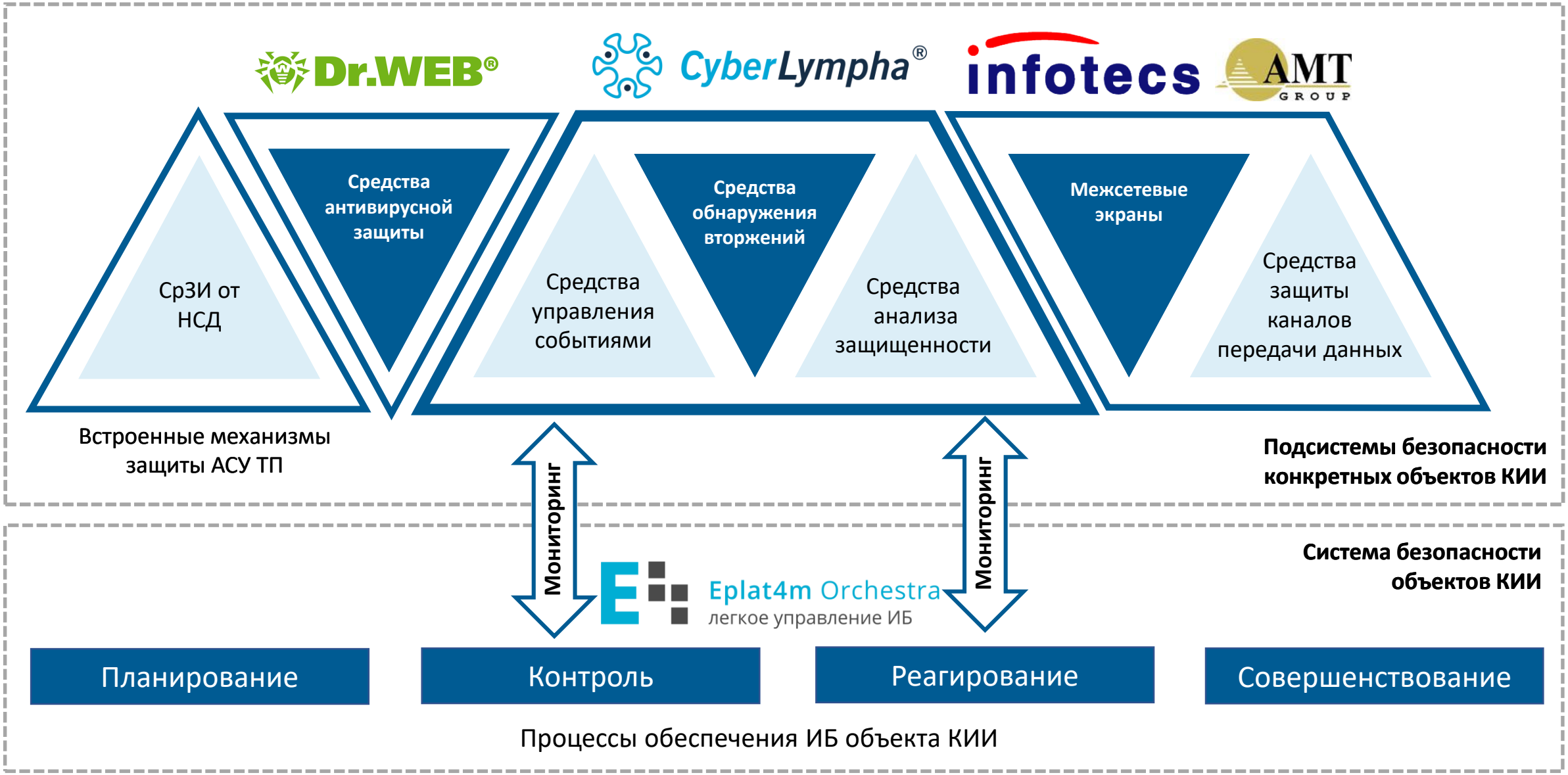
CYBERLYMPHA И СИСТЕМА БЕЗОПАСНОСТИ КИИ

Система безопасности объектов КИИ

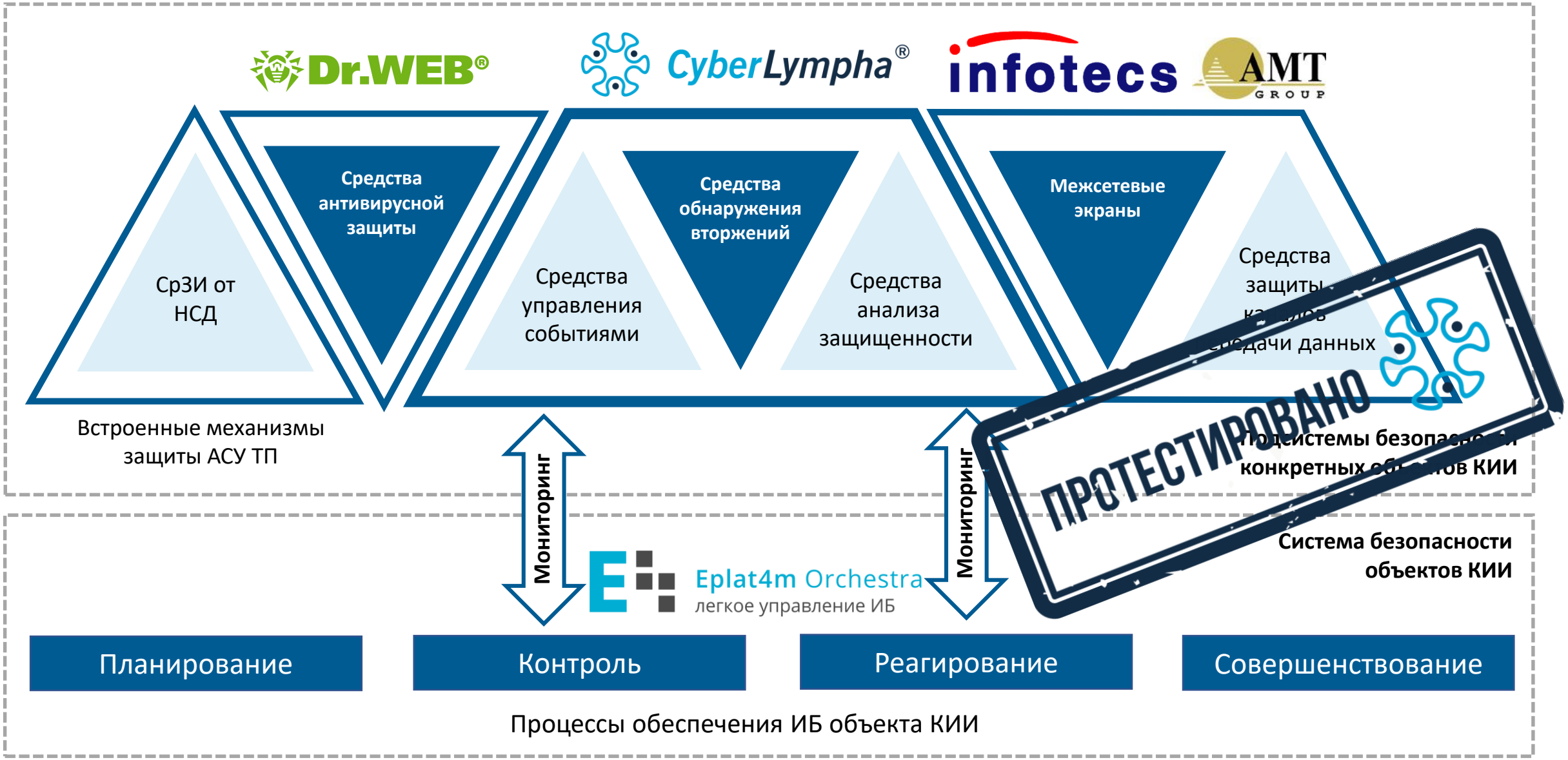
Планирование | Контроль | Реагирование | Совершенствование

Процессы обеспечения ИБ объекта КИИ

CYBERLYMPHA И СИСТЕМА БЕЗОПАСНОСТИ КИИ

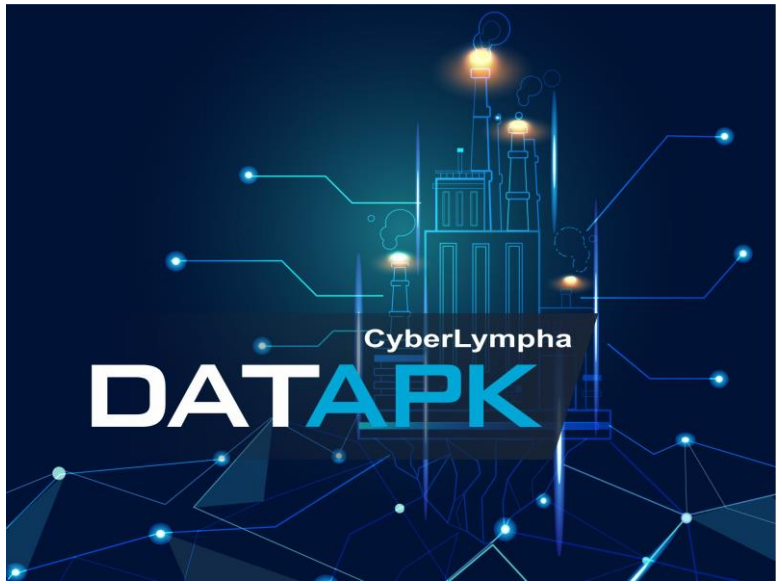


CYBERLYMPHA И СИСТЕМА БЕЗОПАСНОСТИ КИИ



CyberLympha это:

- Современные решения в области кибербезопасности для Заказчиков
- Приглашение партнеров к взаимовыгодному сотрудничеству



Контакты

CyberLympha®

Алексей Шанин

Директор ООО «СайберЛимфа»

cyberlympha.ru