kaspersky

Kaspersky Industrial Cybersecurity Conference 2021

Дмитрий Хоменко

Директор департамента информационной безопасности, ООО «ПРОМТЕХ», Россия

#KasperskyICS

Чат конференции: https://kas.pr/kicscon

ПРОМТЕХ

Практические подходы к реализации систем кибербезопасности на промышленных объектах КИИ для существующих и вновь проектируемых ОТ/АСУТП

Реализация проекта для
ООО «ПГ «Фосфорит»

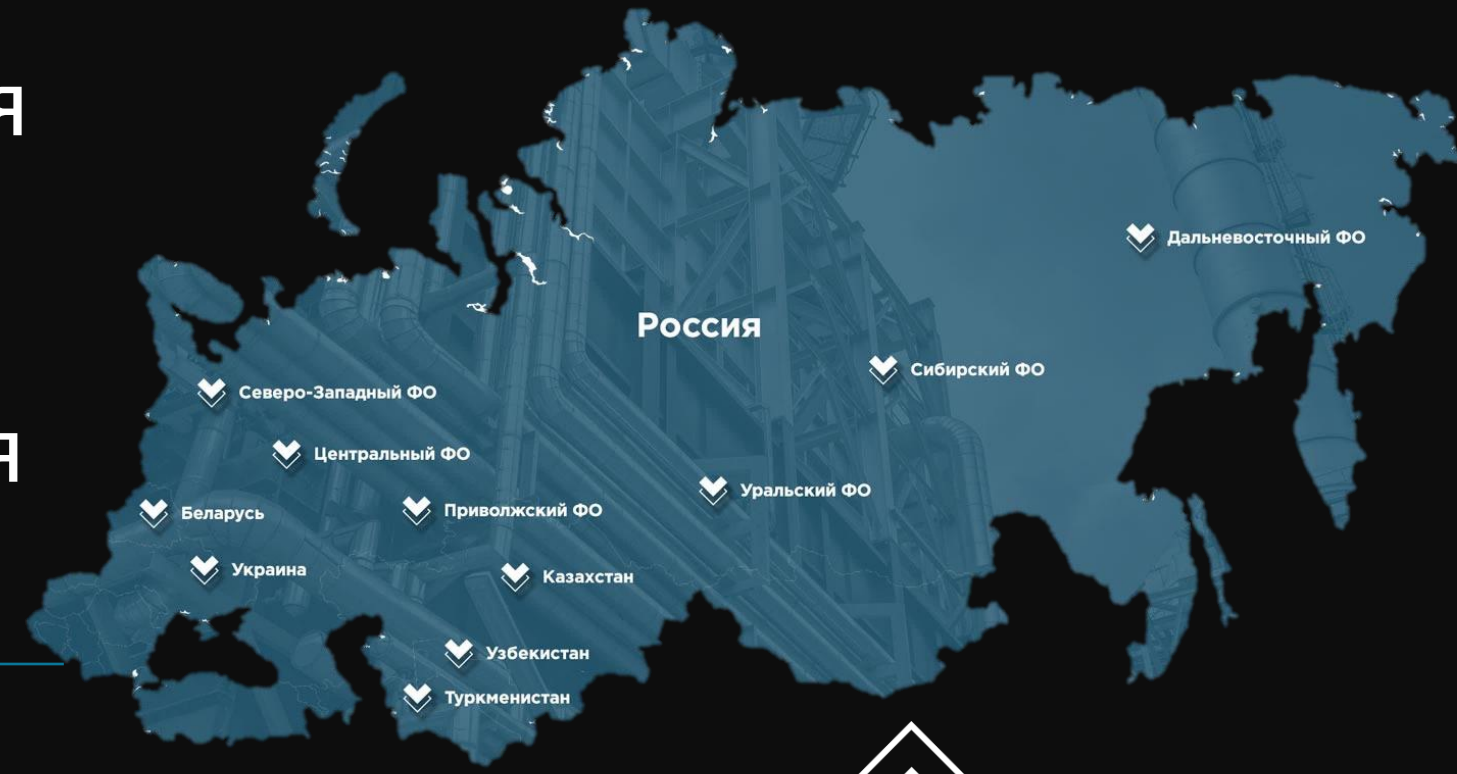
Дмитрий Хоменко

Директор департамента
информационной безопасности
ООО «Промтех»

Промтех – на рынке промышленной автоматизации более 25 лет

Отрасли:

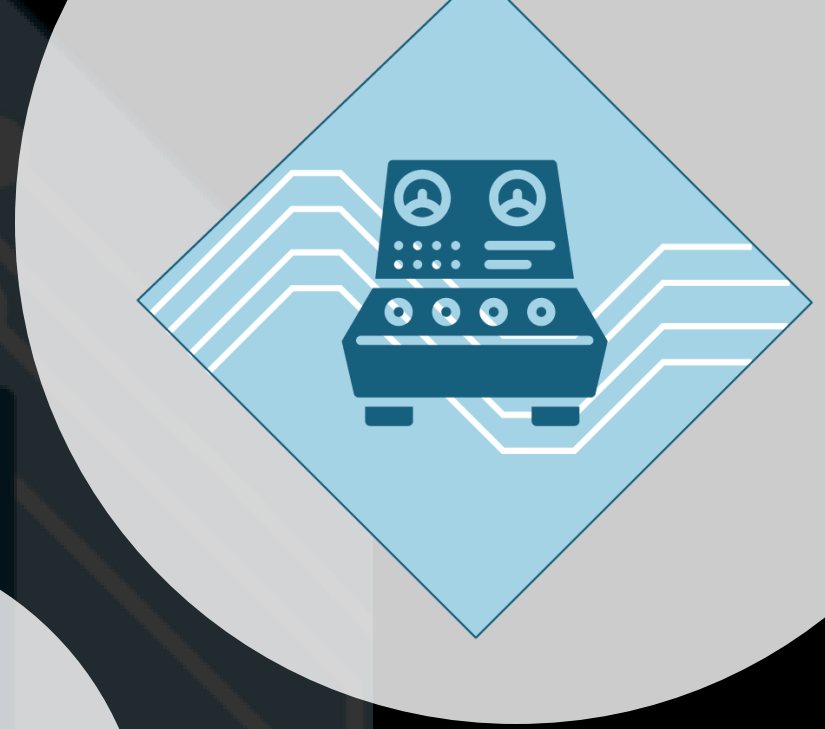
- ✓ Горнодобывающая
- ✓ Химическая
- ✓ Нефтехимическая
- ✓ Металлургическая

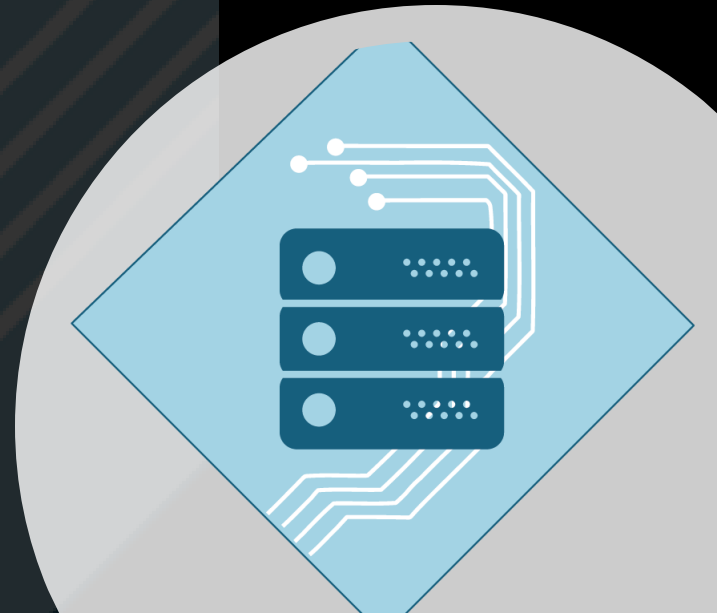


ПРОМТЕХ

Основные направления деятельности

- ✓ **Комплексные решения** в области создания автоматизированных систем управления технологическими процессами и диспетчеризации предприятий промышленного сектора;
- ✓ **Производство и поставка оборудования**;
- ✓ **Сервис и комплексная техническая поддержка** автоматизированных систем управления технологическими процессами;
- ✓ **Обеспечение информационной безопасности** АСУТП и систем диспетчеризации.





Преимущества внедрения СЗИ

1. Повышение уровня защищенности АСУТП, что позволит предотвратить случайные и злонамеренные действия нарушителей

2. Снижение убытков, связанных с потерей информации, поломкой и простоем оборудования, нарушением технологических процессов, репутационными потерями

3. Уменьшение влияния человеческого фактора на реализацию возможных угроз ИБ АСУТП и эксплуатацию уязвимостей ПТК АСУТП

4. Создание единого защищенного информационного пространства предприятия

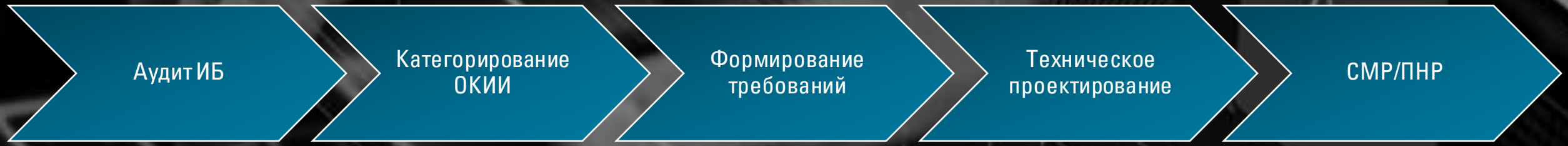
5. Отсутствие влияния СЗИ АСУТП на возможности масштабирования производства

6. Возможность мгновенного принятия решений на основе полученной и обработанной информации СЗИ АСУТП

7. Увеличение отказоустойчивости подсистем АСУТП, а также возможность восстановления работы ПТК АСУТП в кратчайшие сроки

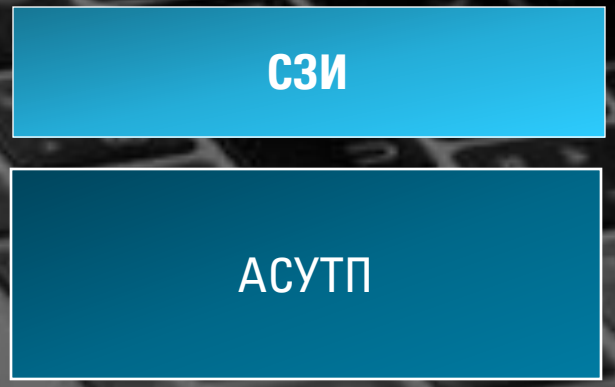
8. Соответствие предприятия требованиям регуляторов РФ и локальным нормативным документам Компании. Привлекательность для инвесторов.

Этапы внедрения СЗИ

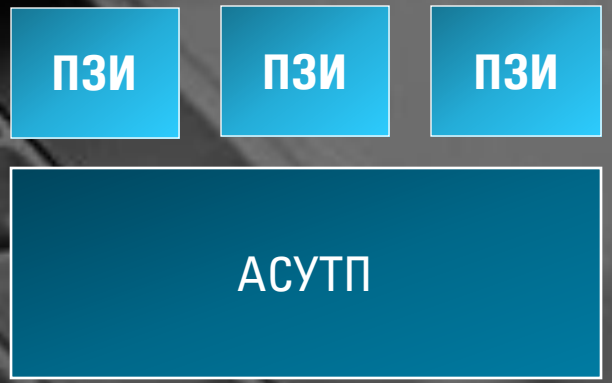


Подходы к внедрению СЗИ

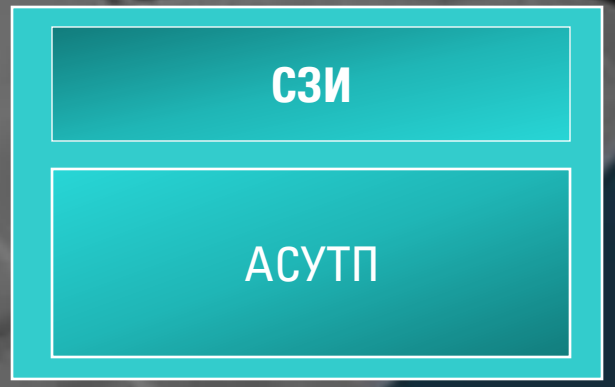
Комплексный



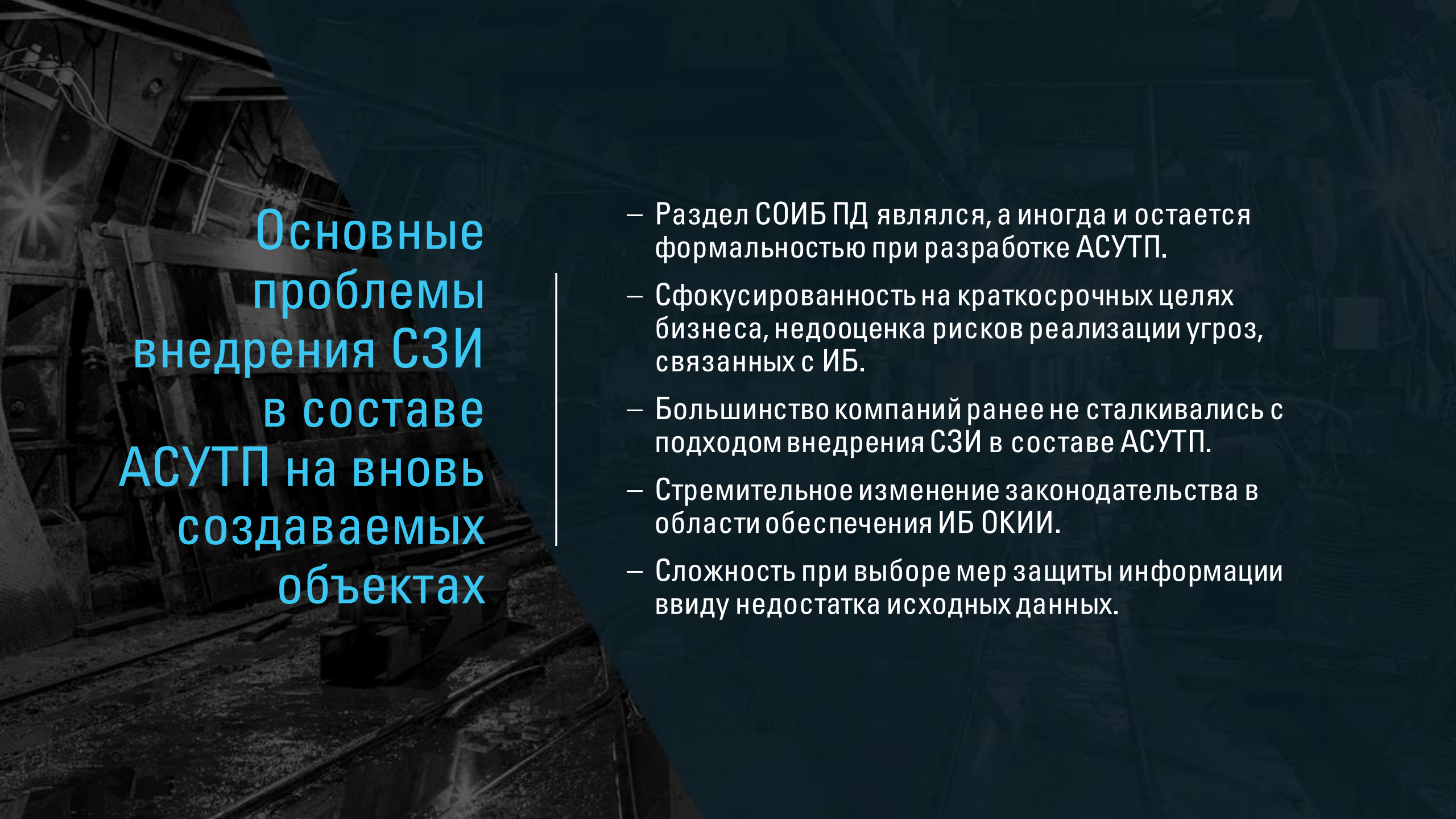
Фрагментарный



В составе АСУТП



Комплексный	Фрагментарный
Преимущества: ✓ Включает организационную, документальную и техническую часть; ✓ Обеспечивает высокий уровень информационной безопасности на объекте внедрения.	**Преимущества:** ✓ Гибкость; ✓ Точечные решения против конкретных угроз; ✓ Стоимость реализации.
Недостатки: – Сложность и стоимость реализации; – Нехватка резервных мощностей на существующем оборудовании; – Попытки адаптации корпоративных подходов к обеспечению ИБ в промышленном сегменте; – Организация работ подрядчиков на объекте, контроль и время реакции на необходимые действия.	**Недостатки:** – Неполная информированность о возможных угрозах и рисках, – Отсутствие единой защищенной среды предприятия.



Основные проблемы внедрения СЗИ в составе АСУТП на вновь создаваемых объектах

- Раздел СОИБ ПД являлся, а иногда и остается формальностью при разработке АСУТП.
- Сфокусированность на краткосрочных целях бизнеса, недооценка рисков реализации угроз, связанных с ИБ.
- Большинство компаний ранее не сталкивались с подходом внедрения СЗИ в составе АСУТП.
- Стремительное изменение законодательства в области обеспечения ИБ ОКИИ.
- Сложность при выборе мер защиты информации ввиду недостатка исходных данных.

Ключевые **преимущества** подхода к внедрению СЗИ в составе АСУТП на вновь создаваемых объектах

- ✓ Оптимальный состав оборудования и ПО, необходимый для успешного внедрения СЗИ АСУТП, в том числе и резервные мощности, в случае изменения конфигурации в дальнейшем;
- ✓ Параллельное проектирование совместно с департаментами автоматизации и программирования в составе рабочих групп;
- ✓ Независимость от подрядчиков и субподрядчиков, контроль процесса выполнения работ и транслирование требований до старта проекта;
- ✓ Отсутствие необходимости останавливать производство или добычу при изменении состава или функционала СЗИ в будущем;
- ✓ Формирование культуры обеспечения ИБ с самого начала эксплуатации объекта автоматизации;
- ✓ Соответствие требованиям Стандартов организации(либо их разработка), международных стандартов, законодательства.

Реализация проекта для ООО «ПГ «Фосфорит»

ПРОМТЕХ EuroChem

EuroChem
MINERAL AND CHEMICAL COMPANY

ООО ПГ «Фосфорит»

- ✓ Один из ведущих производителей серной и фосфорной кислот, сложных комплексных удобрений и кормовых фосфатов на Северо-Западе России.
- ✓ Работает под управлением минерально-химической компании «ЕвроХим» – крупнейшего российского производителя агрохимикатов и химических продуктов, входящего в первую тройку европейских и десятку мировых лидеров отрасли.
- ✓ Продукция Предприятия – аммофос, сульфоаммофос, дефторированный фосфат –поставляется в 45 регионов Российской Федерации от Калининградской области до Приморского края, в Азербайджан, Беларусь, Украину и более чем в 70 стран дальнего зарубежья.

СЗИ ОКИИ ООО «ПГ «Фосфорит»

Разработка проектного решения СЗИ ОКИИ проводилась:

- ✓ в полном соответствии с нормативно-правовыми актами и методическими документами в области обеспечения безопасности значимых объектов критической информационной инфраструктуры, устанавливающими порядок разработки, внедрения и эксплуатации СЗИ;
- ✓ с учетом используемых технологий и структурно-функциональных характеристик ОКИИ и особенностей их функционирования;
- ✓ с перспективой дальнейшего развития/модернизации СЗИ ОКИИ.

Детальный состав технических и организационных мер защиты, используемых при разработке СЗИ ОКИИ, согласно требованиям Федерального закона № 187-ФЗ от 26 июля 2017 г. и его подзаконных актов, определялся на основании:

1. категории значимости объекта КИИ;
2. актуальных угроз информационной безопасности;
3. требований к мерам и средствам защиты информации, применяемых для значимых объектов КИИ;
4. требований к защите информации при информационном взаимодействии значимых объектов КИИ с иными объектами КИИ и/или информационными системами.

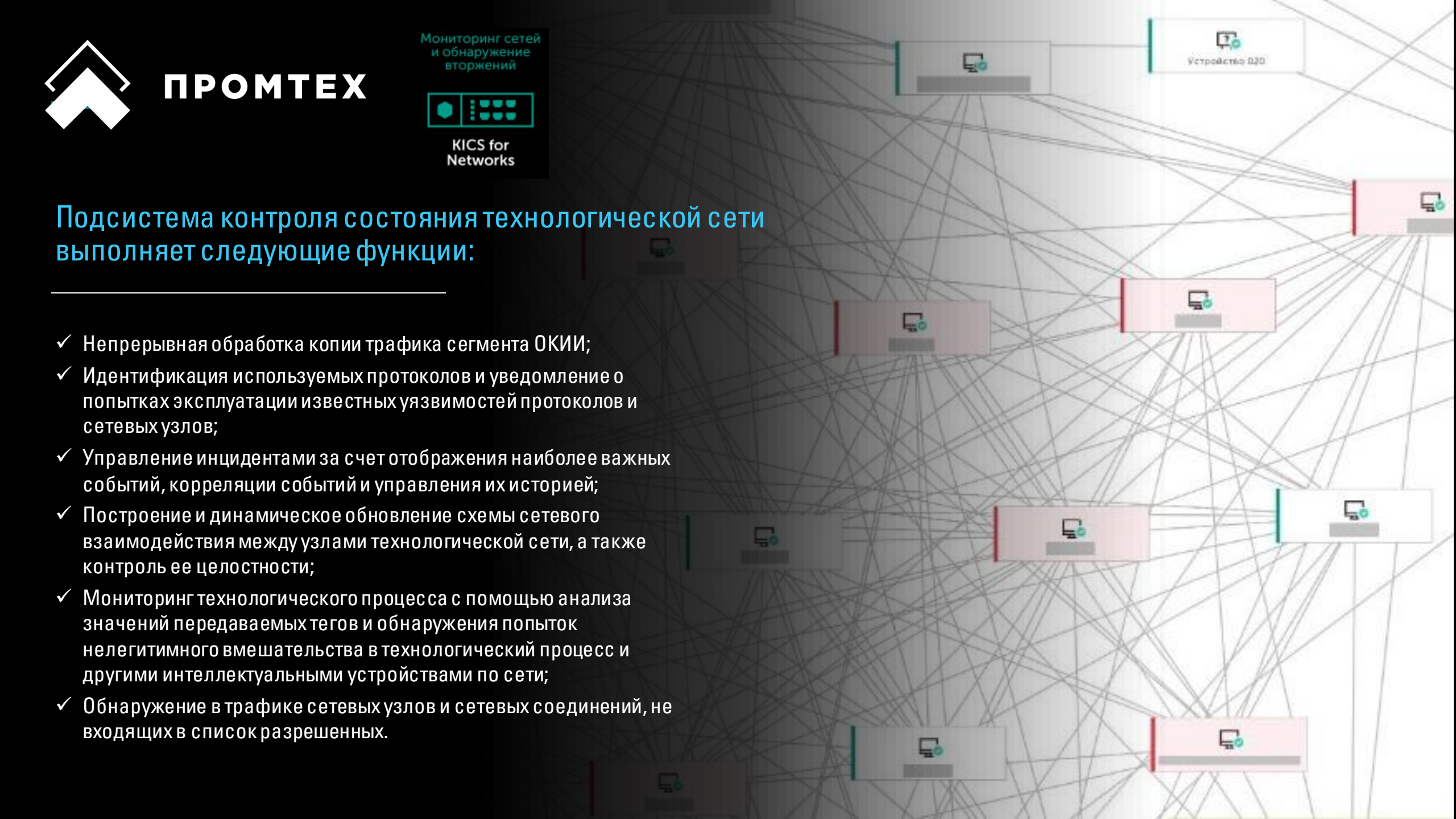
ПРОМТЕХ

Мониторинг сетей и обнаружение вторжений

KICS for Networks

Подсистема контроля состояния технологической сети выполняет следующие функции:

- ✓ Непрерывная обработка копии трафика сегмента ОКИИ;
- ✓ Идентификация используемых протоколов и уведомление о попытках эксплуатации известных уязвимостей протоколов и сетевых узлов;
- ✓ Управление инцидентами за счет отображения наиболее важных событий, корреляции событий и управления их историей;
- ✓ Построение и динамическое обновление схемы сетевого взаимодействия между узлами технологической сети, а также контроль ее целостности;
- ✓ Мониторинг технологического процесса с помощью анализа значений передаваемых тегов и обнаружения попыток нелегитимного вмешательства в технологический процесс и другими интеллектуальными устройствами по сети;
- ✓ Обнаружение в трафике сетевых узлов и сетевых соединений, не входящих в список разрешенных.



Помимо стандартного функционала антивируса выделяются особые функции, учитывающие специфику АСУТП:

- ✓ Работа антивируса в неблокирующем режиме
- ✓ Отказ от установки файлового антивируса
- ✓ Антивирусная проверка с разными уровнями безопасности для разных зон
- ✓ Контроль запуска программ
- ✓ Быстрое создание белого списка программ
- ✓ Контроль устройств
- ✓ Защита от шифрования файлов на общих сетевых ресурсах
- ✓ Мониторинг файловых операций (контроль целостности произвольных файлов на диске)
- ✓ Мониторинг целостности файлов на основе эталона
- ✓ Контроль целостности проектов ПЛК
- ✓ Установка и удаление продукта без перезагрузки ОС
- ✓ Обновление продукта без перезагрузки ОС
- ✓ Управление потребляемыми ресурсами
- ✓ Интеграция со сторонними системами

Спасибо за внимание!

С уважением,
Дмитрий Хоменко
Директор департамента информационной безопасности

Тел.: +7 (926) 091-74-32
E-mail: D.Homenko@promtex.ru Site: www.promtex.ru

ПРОМТЕХ

Рекомендую к прочтению:

Industrial Control Systems: Pentesting Industrial Networks

Author: Paul Smith

Job title: ICS CyberSecurity Specialist

Professional qualifications:

- ✓ Pentest with Hak5,
- ✓ SANS Global Industrial Cyber Security Professional,
- ✓ Department of Homeland Security(DHS) Control Systems Cyber Security Advanced Training