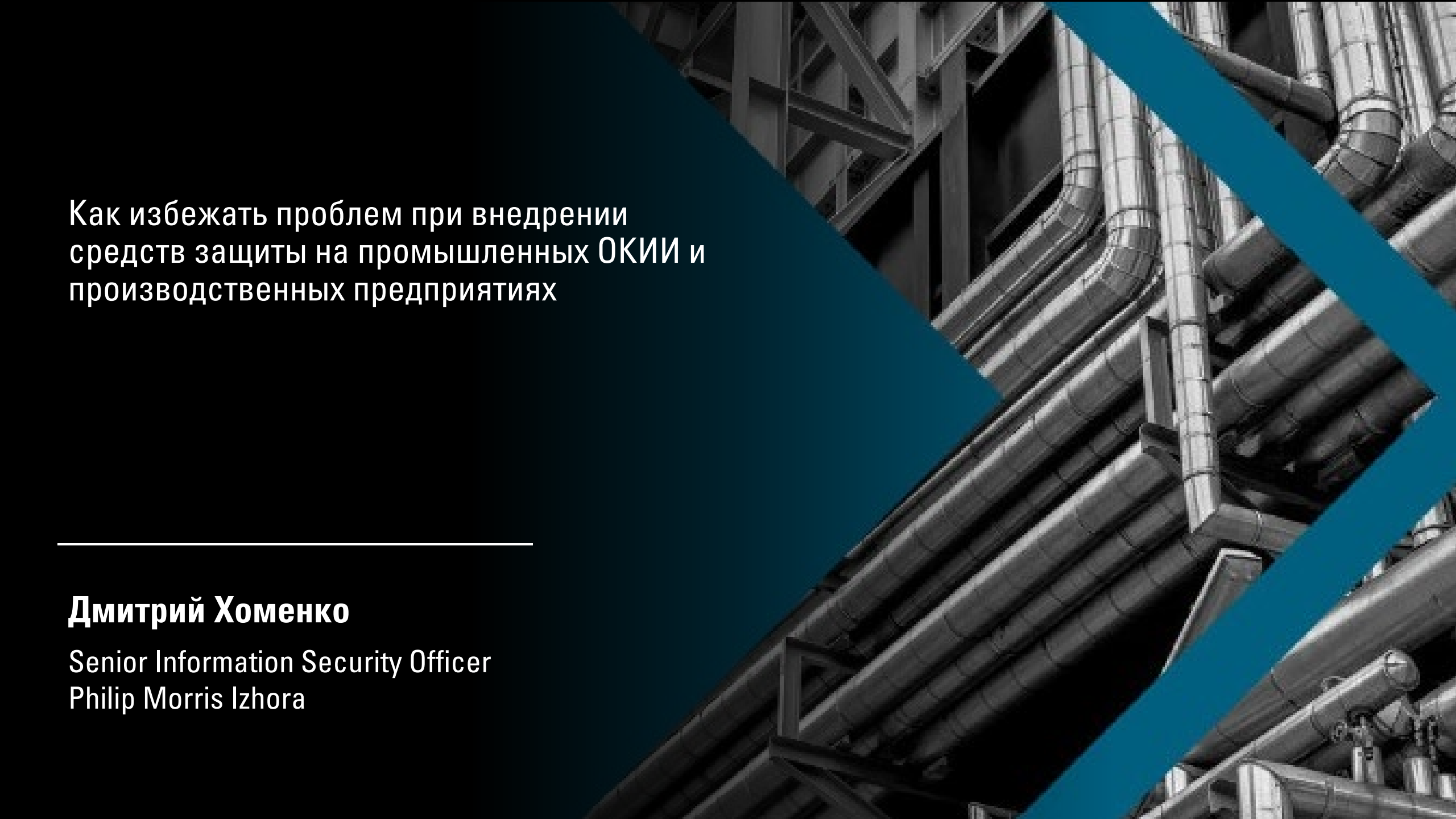
Как избежать проблем при внедрении средств защиты на промышленных ОКИИ и производственных предприятиях



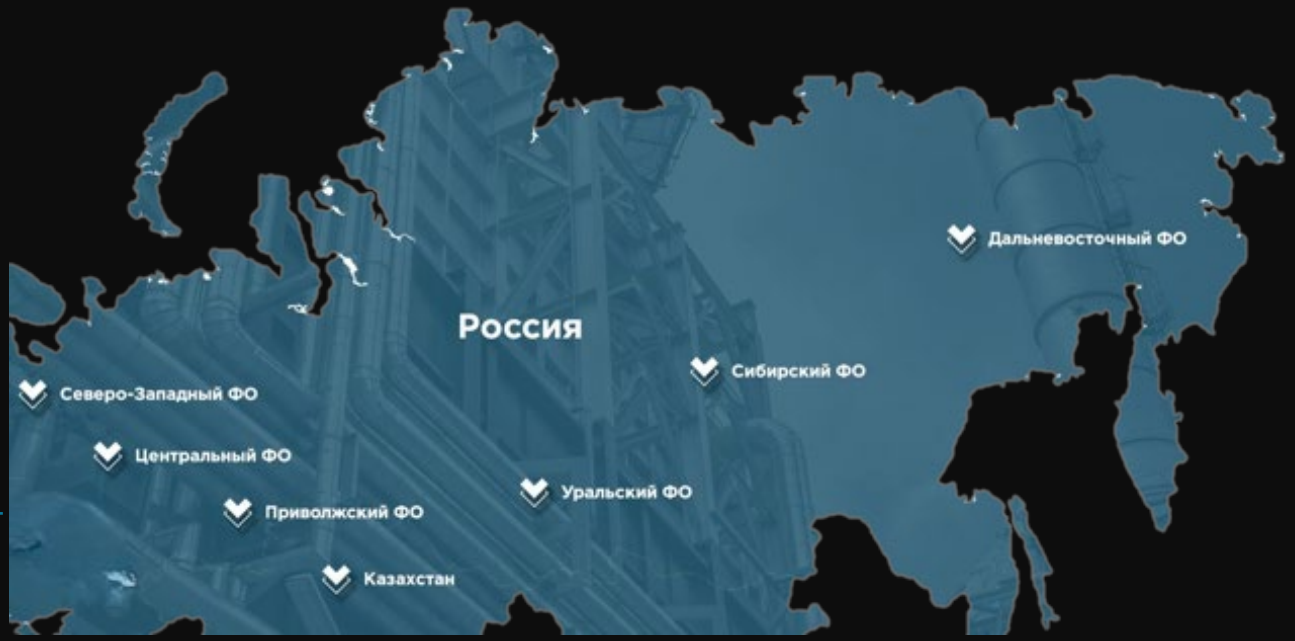
Дмитрий Хоменко

Senior Information Security Officer
Philip Morris Izhora

Опыт проектирования и внедрения средств защиты на ОКИИ и промышленных предприятиях

Отрасли:

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



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

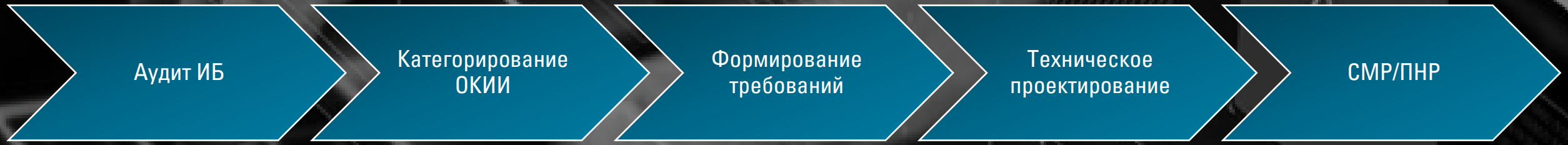
5. Отсутствие влияния СЗИ АСУТП на возможности масштабирования производства

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

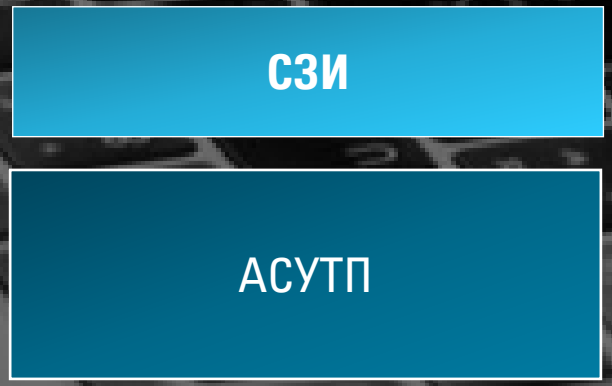
8. Соответствие предприятия требованиям регуляторов РФ и локальным нормативным документам Компании. Привлекательность для инвесторов.

Этапы внедрения СЗИ

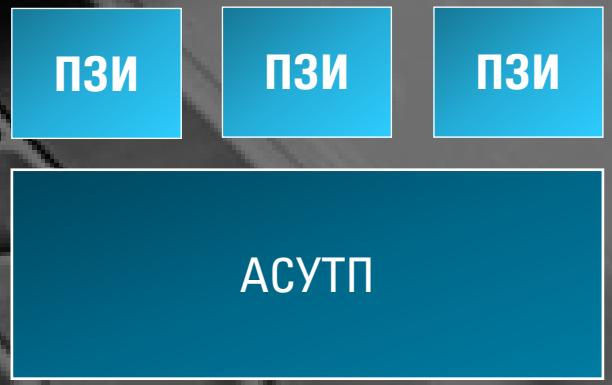


Подходы к внедрению СЗИ

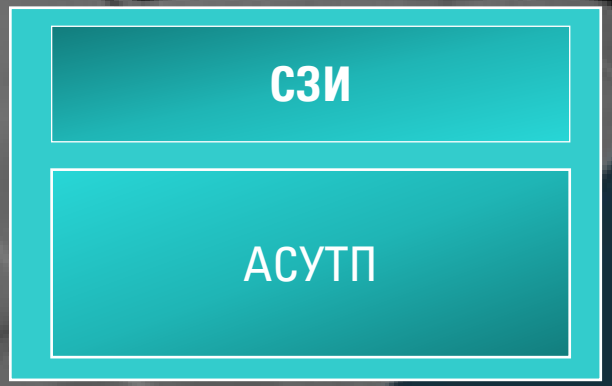
Комплексный



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; – Проблемы с последующей интеграцией решений; – Защита бюджета для следующих итераций.

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 и компетенций.

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.

Разработка проектного решения СЗИ для ОКИИ и производственных предприятий

Разработка проектного решения СЗИ должна проводиться:

- ✓ в полном соответствии с нормативно-правовыми актами и методическими документами в области обеспечения безопасности значимых ОКИИ, международными стандартами, устанавливающими порядок разработки, внедрения и эксплуатации СЗИ + best practices;
- ✓ с учетом используемых технологий и структурно-функциональных характеристик объекта защиты и особенностей его функционирования;
- ✓ с перспективой дальнейшего развития/модернизации СЗИ.

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.

Подготовка/планирование

- ✓ Бизнес – зачем ему это (законодательство, риски, репутация, и т.д.);
- ✓ Брифинг для руководителей/директоров направлений;
- ✓ Брифинг для ИТ;
- ✓ Брифинг для начальников цехов/производственных линий/участков;
- ✓ Брифинг для инженеров по автоматизации/электронщиков/специалистов по диспетчеризации, и т.д.;
- ✓ Выделение ресурсов (люди, время, тестовые зоны);
- ✓ Постоянный контакт с вендорами (чьи решения внедряете);
- ✓ Пилотирование решений и подготовка к ним;
- ✓ Серьезный подход к выбору подрядчика;
- ✓ Проектирование, внедрение и последующее сопровождение.

Спасибо за внимание!

С уважением,
Дмитрий Хоменко

E-mail: DmitriyHomenko87@yandex.ru