НОРНИКЕЛЬ

Создание комплексной системы защиты АСУ ТП промышленной группы предприятий

Бадеха Иван Александрович

16 июля 2020 года
ТБ форум

Группа компаний Норильский никель

НОРНИКЕЛЬ

ГЕОЛОГОРАЗВЕДКА

НОРНИКЕЛЬ

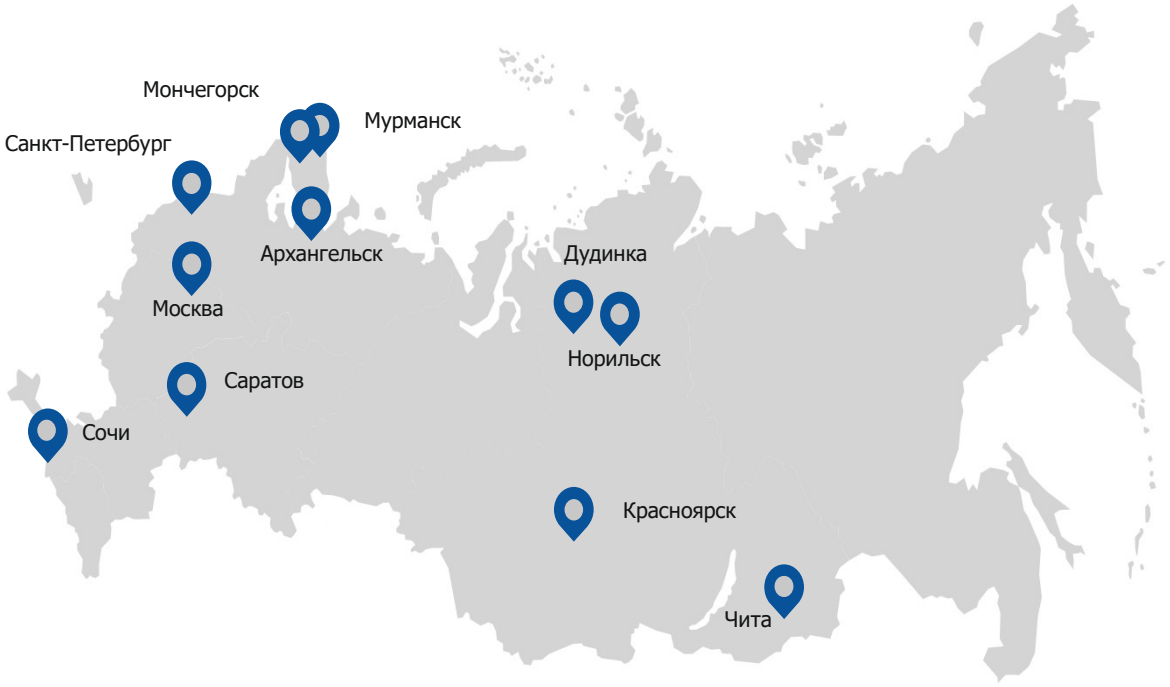
НАУЧНЫЕ КОМПЛЕКСЫ

ПРОИЗВОДСТВО

СБЫТОВАЯ СЕТЬ

ТРАНСПОРТ

ЭНЕРГЕТИКА



Производственный цикл

НОРНИКЕЛЬ

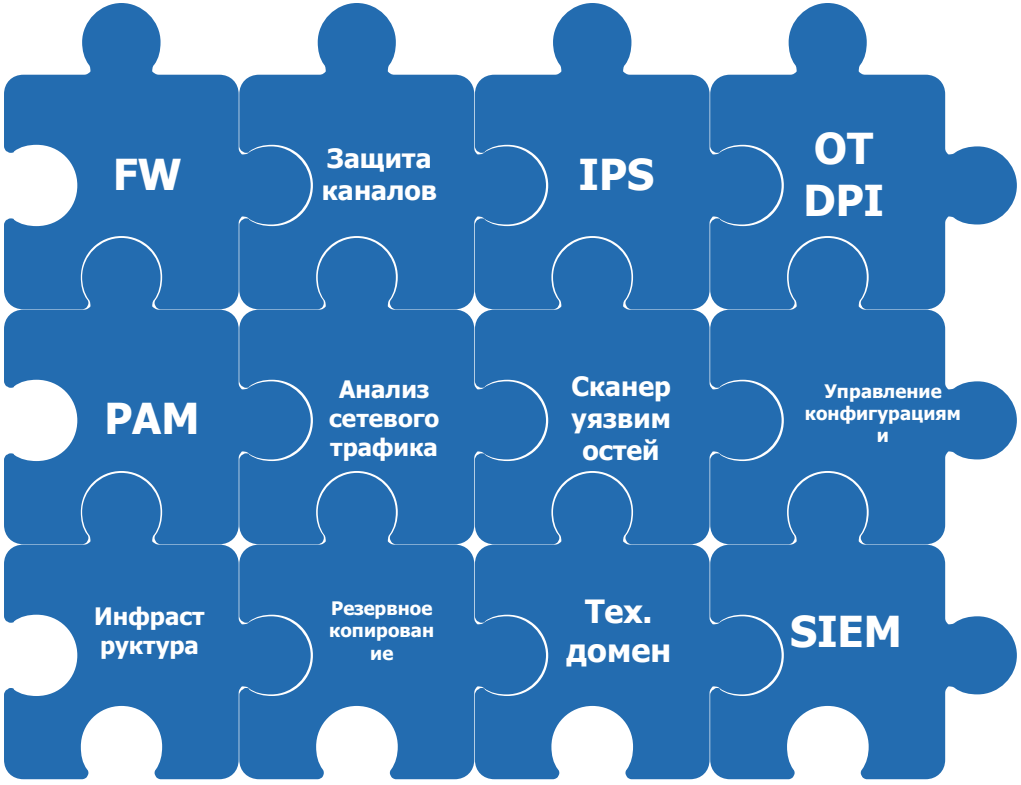
Добыча	Обогащение	Производство	Энергетика	Транспорт	Продажа
Вентиляция	Дробление	Плавка концентрата	Добыча и транспортировка газа	Порты, аэропорты	Стратегия и управление
Спуск техники	Измельчение и классификация	Конвертирование штейна	Гидроэлектро-станции	Суда речного и морского типа	Сбыт
Подъем продукции	Флотация	Анодная плавка	Топливно-энергетические ресурсы	Самолеты и вертолеты	Снабжение запасами
Позиционирование техники и людей	Сгущение и сушка	Электролиз	Электроснабжение	Железные дороги	Экономика и финансы
Сигнализации	Транспортировка на завод	Вспомогательные процессы	Водоснабжение	Промышленная техника	Кадры и социальная политика
					

Комплексная система защиты АСУ ТП группы промышленных предприятий

НОРНИКЕЛЬ

Converged Plantwide Ethernet (CPwE) Design and Implementation Guide

Deploying Industrial Firewalls within a Converged Plantwide Ethernet Architecture

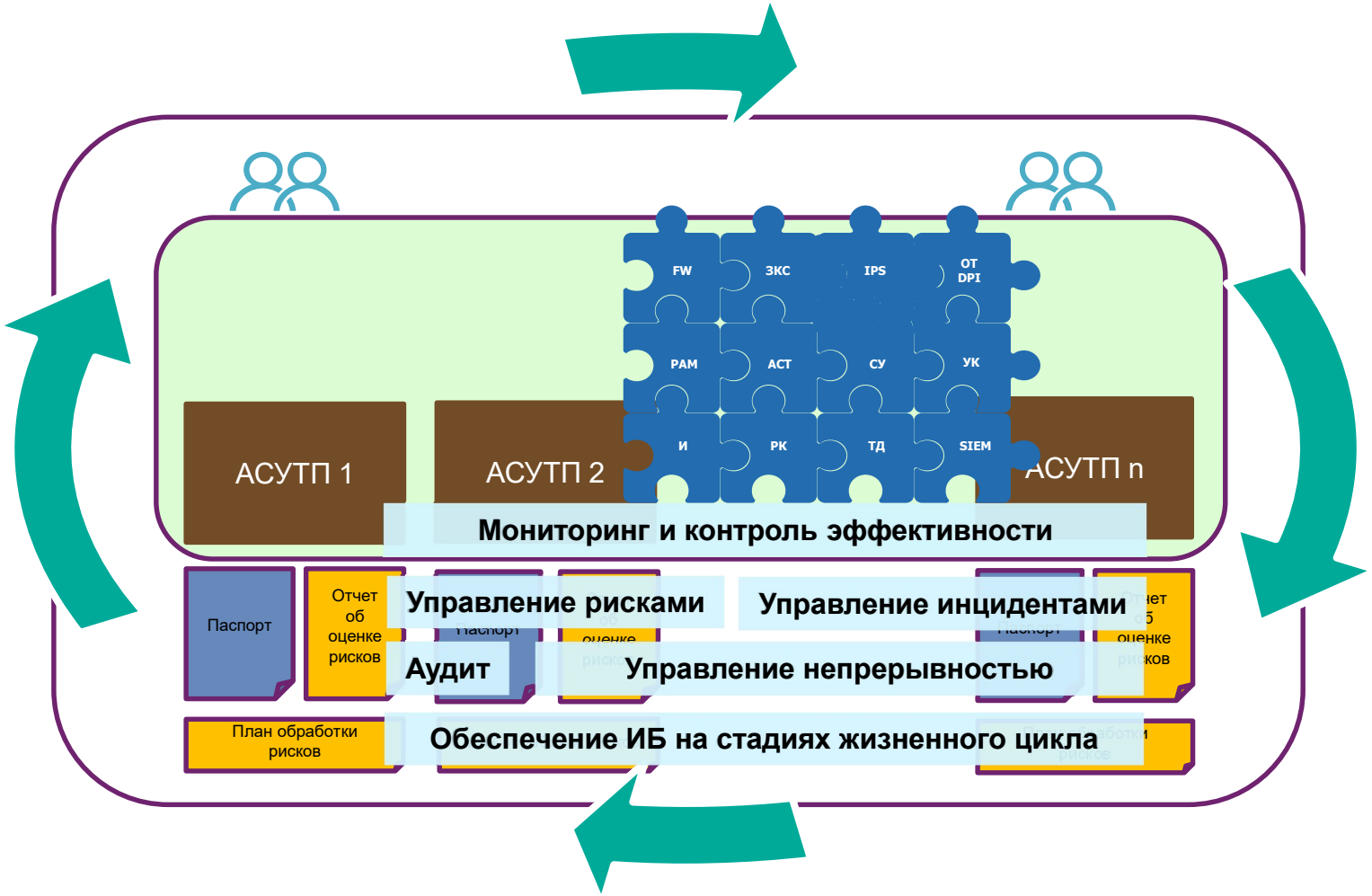


ISA/IEC 62443

Guide to Industrial Control Systems (ICS) Security

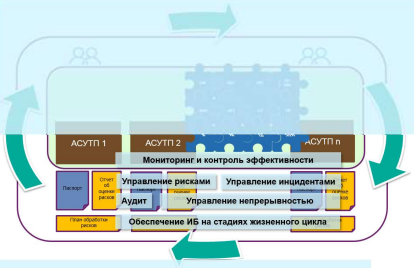
NIST National Institute of Standards and Technology U.S. Department of Commerce

Комплексная система защиты АСУ ТП группы промышленных предприятий

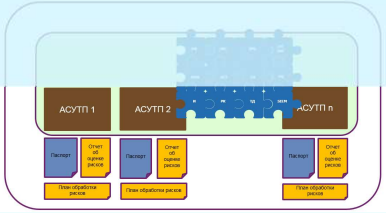


Комплексная система защиты АСУ ТП группы промышленных предприятий

НОРНИКЕЛЬ

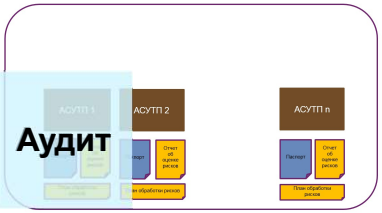


Мониторинг и контроль эффективности

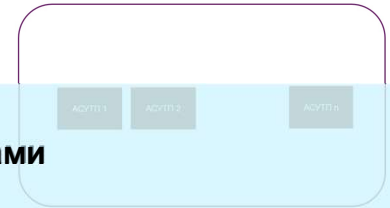


Управление рисками

Управление непрерывностью



Аудит



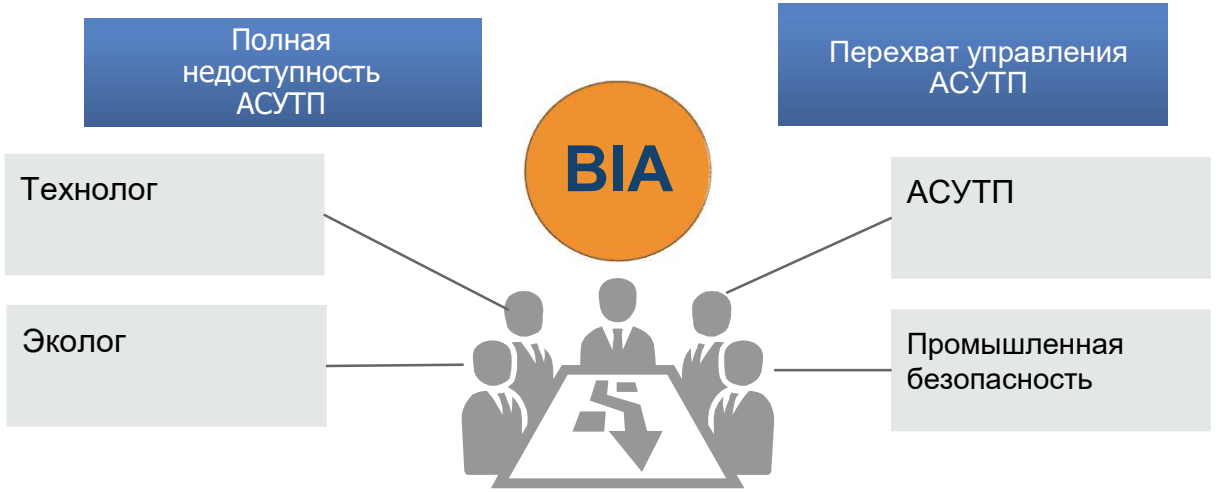
Управление инцидентами

Обеспечение ИБ на стадиях жизненного цикла

Предпосылки создания комплексной системы защиты АСУ ТП

1. Система создается с целью:

а. снижения рисков информационной безопасности АСУ ТП



Оценка воздействия на цели Компании в различных сферах

Финансовая сфера						Окружающая среда / экология	Охрана труда и промышленная безопасность
Стоимость закупки оборудования	Период восстановления производительности (вер.)	Период восстановления производительности (макс.)	Относительное снижение производитель-ности	Иные финансовые потери (штрафные санкции, возмещение убытка и т.д.)	Воздействие на финансовый результат	Воздействие на окружающую среду / экологию	Воздействие на жизнь и здоровье людей

Предпосылки создания комплексной системы защиты АСУ ТП

НОРНИКЕЛЬ

1. **Система создается с целью:**
   a. **снижения рисков информационной безопасности АСУ ТП**

Предпосылки создания комплексной системы защиты АСУ ТП

НОРНИКЕЛЬ

1. **Система создается с целью:**
   a. **снижения рисков информационной безопасности АСУ ТП**

Предпосылки создания комплексной системы защиты АСУ ТП

2. Система создается с целью:
b. реализации требований законодательства РФ

- **Федеральный закон от 26.07.2017 N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»**
- **Постановление Правительства РФ** от 08.02.2018 N 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений»
- **Приказ ФСТЭК России** от 21.12.2017 N 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования»
- **Приказ ФСТЭК России** от 25.12.2017 N 239 (ред. от 09.08.2018) «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»
- **Приказ ФСБ России** от 24.07.2018 № 366 «О Национальном координационном центре по компьютерным инцидентам»
- **Приказ ФСБ России** от 24.07.2018 № 367 «Об утверждении Перечня информации, представляемой … и Порядка представления информации...»
- **Приказ ФСБ России** от 24.07.2018 № 368 «Об утверждении Порядка обмена информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры Российской Федерации...»

Критическая информационная инфраструктура

Персональные данные

Государственная тайна

Коммерческая тайна

Инсайдерская информация

НОРНИКЕЛЬ

3. Технологический сегмент ИТ-инфраструктуры – зона повышенного уровня безопасности

Система строится таким образом, что компрометация любого компонента корпоративного сегмента ИТ-инфраструктуры не приводит к угрозе воздействия на технологический сегмент, в котором размещаются АСУ ТП

Система реализует два или более эшелона защиты по каждому вектору возможной атаки

НОРНИКЕЛЬ

4. Устойчивость к недоступности каналов связи

Процессы эксплуатации системы не должны прерываться при недоступности каналов связи

Система должна поддерживать возможность локального реагирования на компьютерные инциденты в технологическом сегменте ИТ-инфраструктуры при нарушении функционирования каналов связи

Базовые принципы создания комплексной системы защиты АСУ ТП

НОРНИКЕЛЬ

5. Эксплуатация системы – зона компетенции службы ИБ

Службы автоматизации должны получать систему как сервис – вместе с обслуживанием и эксплуатацией

Система должна быть управляемой, требуется централизация точек управления и мониторинга

Эффективное использование компетенций по эксплуатации системы защиты достигается созданием единой инфраструктуры управления комплексной системой защиты АСУ ТП

Базовые принципы создания комплексной системы защиты АСУ ТП

6. Чем более управляемой становится система, тем она должна становиться более защищенной

Базовые принципы создания комплексной системы защиты АСУ ТП

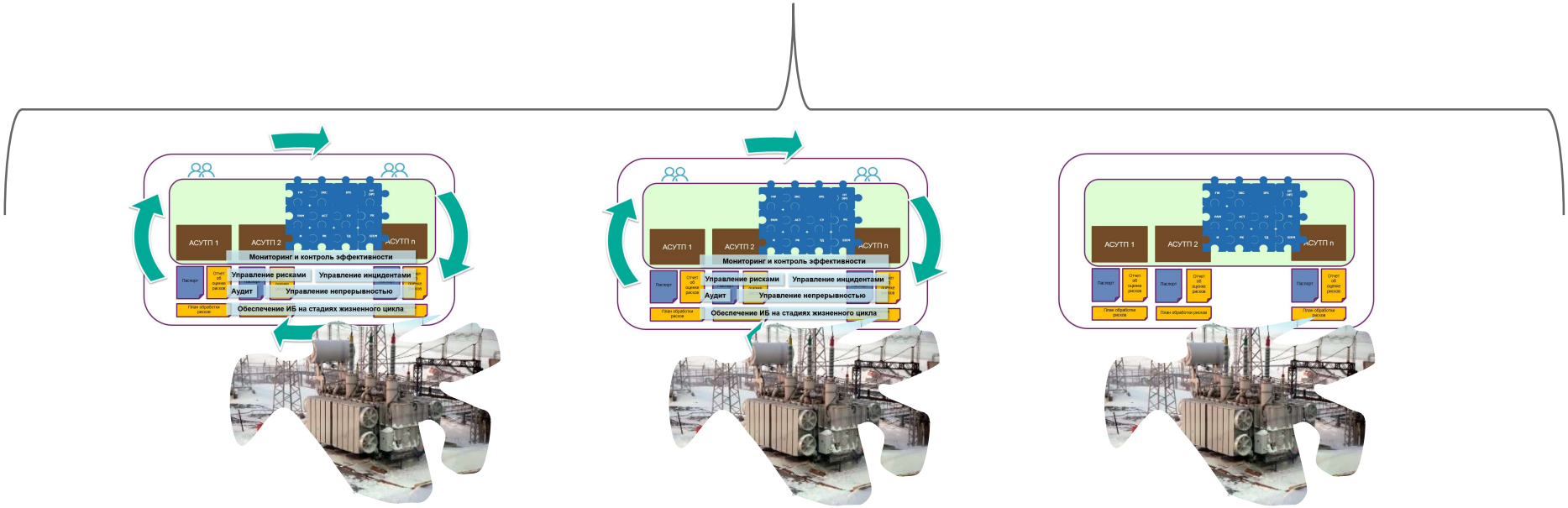
7. Отсутствие негативного влияния на технологические процессы

Система строится таким образом, чтобы исключить негативное воздействие на АСУ ТП

Производственные риски не являются априори более приоритетными по сравнению с рисками ИБ!

Верхнеуровневая структура комплексной системы защиты АСУТП

- Удобный и безопасный доступ к управлению компонентами системы защиты АСУТП
- Обмен сообщениями и информацией
- Централизованный безопасный сервис обновлений и безопасного обмена данными между службами эксплуатации
- Централизованный мониторинг функционирования систем защиты АСУТП



Выводы


Предпосылки создания системы
Базовые принципы создания системы
Архитектура технологической ИТ-инфраструктуры
Архитектура комплексной системы защиты АСУ ТП

ВОПРОСЫ и ОТВЕТЫ