



НОРНИКЕЛЬ

Создание комплексной системы защиты АСУ ТП крупной промышленной группы

Бадеха Иван Александрович

08 апреля 2021 года
ТБ Форум

ГЕОЛОГОРАЗВЕДКА



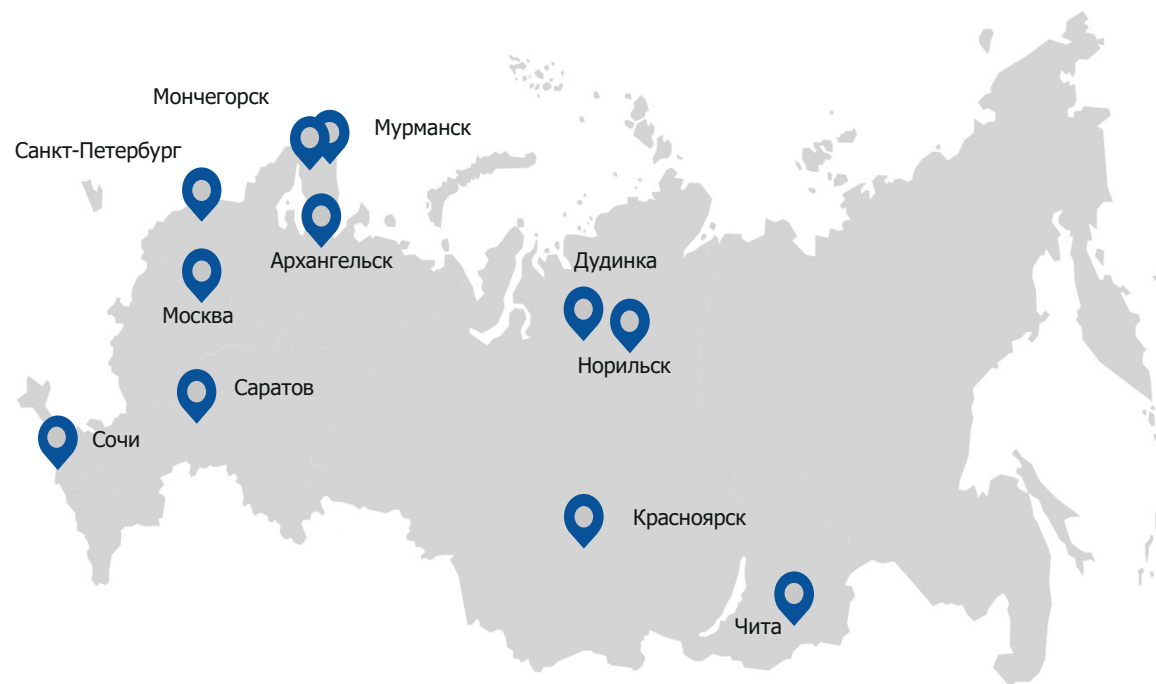
**НАУЧНЫЕ
КОМПЛЕКСЫ**

ПРОИЗВОДСТВО

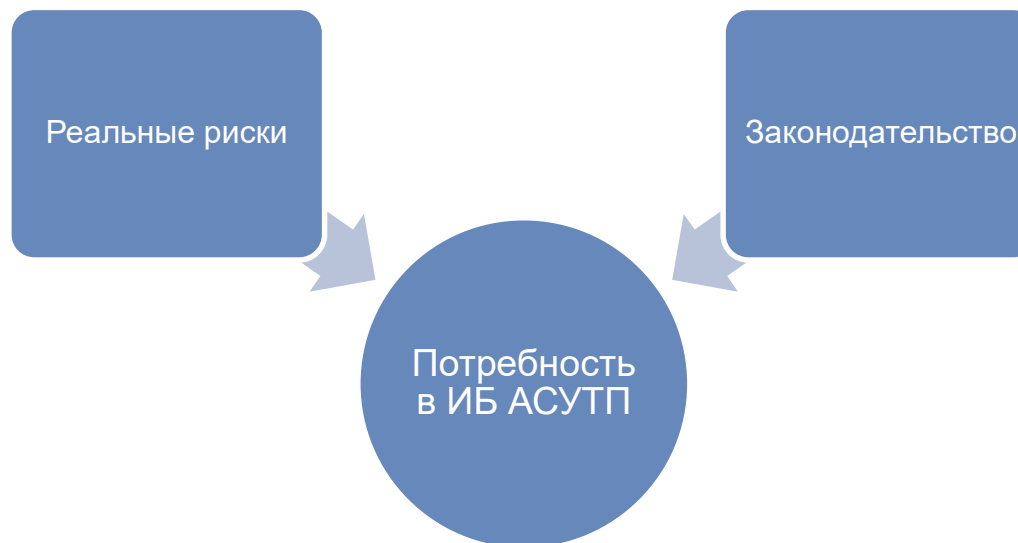
СБЫТОВАЯ СЕТЬ

ТРАНСПОРТ

ЭНЕРГЕТИКА



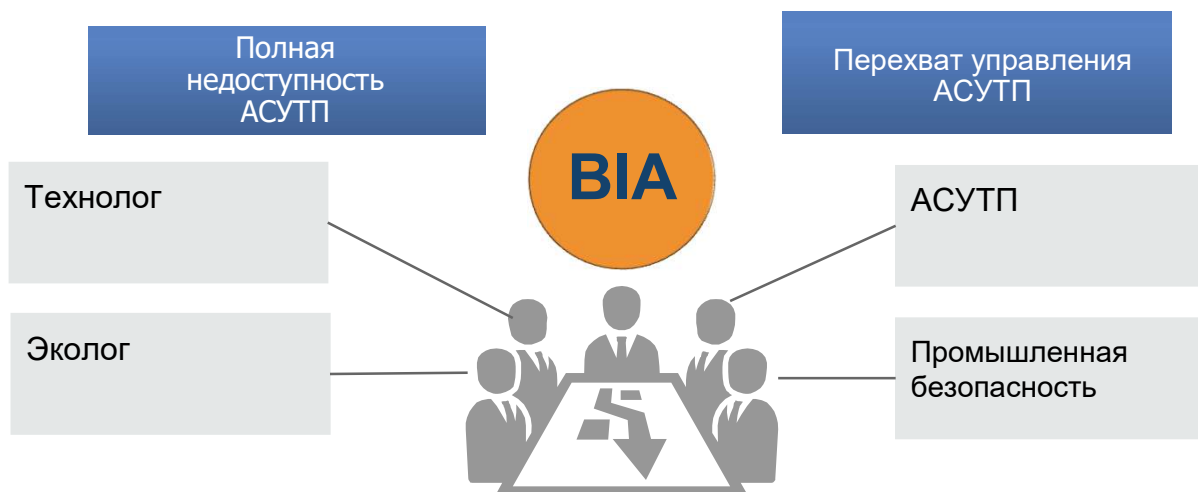
Добыча 	Обогащение 	Производство 	Энергетика 	Транспорт 	Продажа 
Вентиляция	Дробление	Плавка концентрата	Добыча и транспортировка газа	Порты, аэропорты	Стратегия и управление
Спуск техники	Измельчение и классификация	Конвертирование штейна	Гидроэлектростанции	Суда речного и морского типа	Сбыт
Подъем продукции	Флотация	Анодная плавка	Топливо-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
					



- Риски потери активов сопоставимы со стоимостью активов
- Риски останова сопоставимы с величиной выручки
- Риски нанесения вреда экологии, а также жизни и здоровью людей всегда приоритетны

- Полноценная законодательная и нормативная база формируется начиная с июля 2017 года

Снижение 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 производительности	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

Снижение рисков информационной безопасности АСУ ТП



Реализация 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

Корпоративная сеть

ИТ-сервисы



Информационные активы



Технологическая сеть

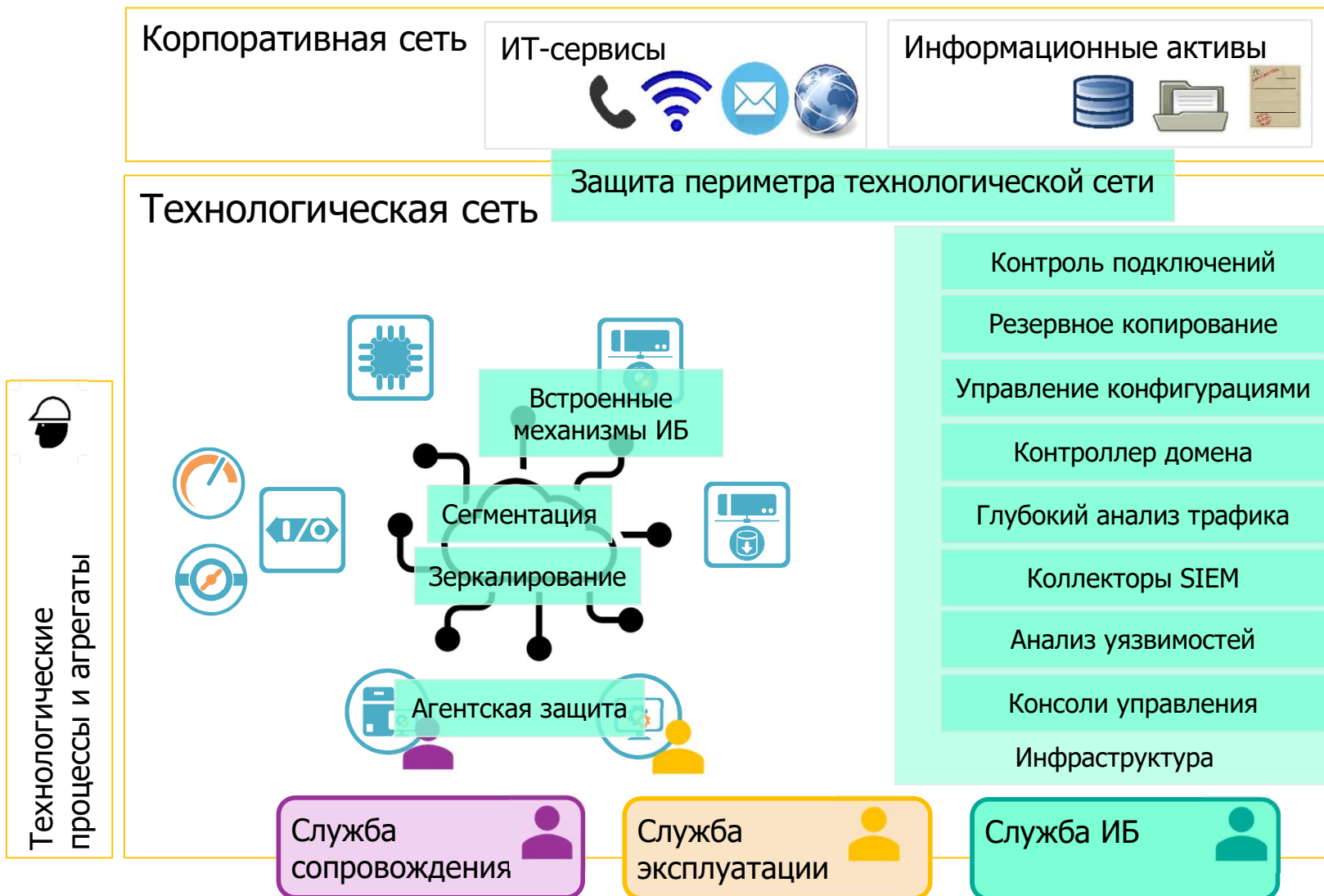


Технологические процессы и агрегаты



Служба сопровождения

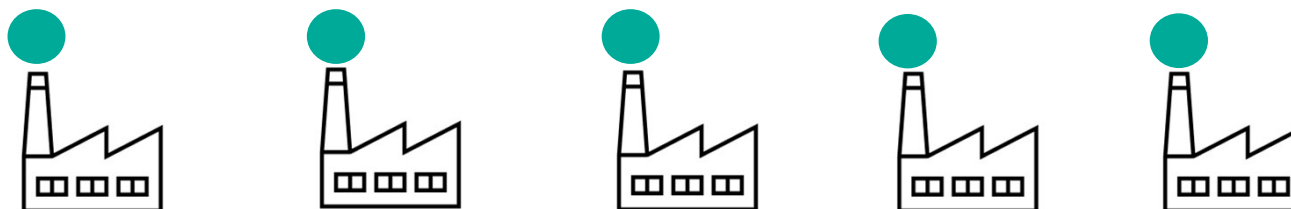
Служба эксплуатации



Комплексная система защиты АСУ ТП промышленной группы



- Управление доступом
- Среда взаимодействия участников процесса
- Средства управления и мониторинга
- Инфраструктура для тестирования обновлений



1. 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

2. 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

3. 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

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



5. 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!

ВОПРОСЫ и ОТВЕТЫ