НОРНИКЕЛЬ

Создание комплексной системы защиты АСУ ТП крупной промышленной группы

Бадеха Иван Александрович

30 июня 2021 года
ТБ Форум

Группа компаний Норильский никель

НОРНИКЕЛЬ

ГЕОЛОГОРАЗВЕДКА

НОРНИКЕЛЬ

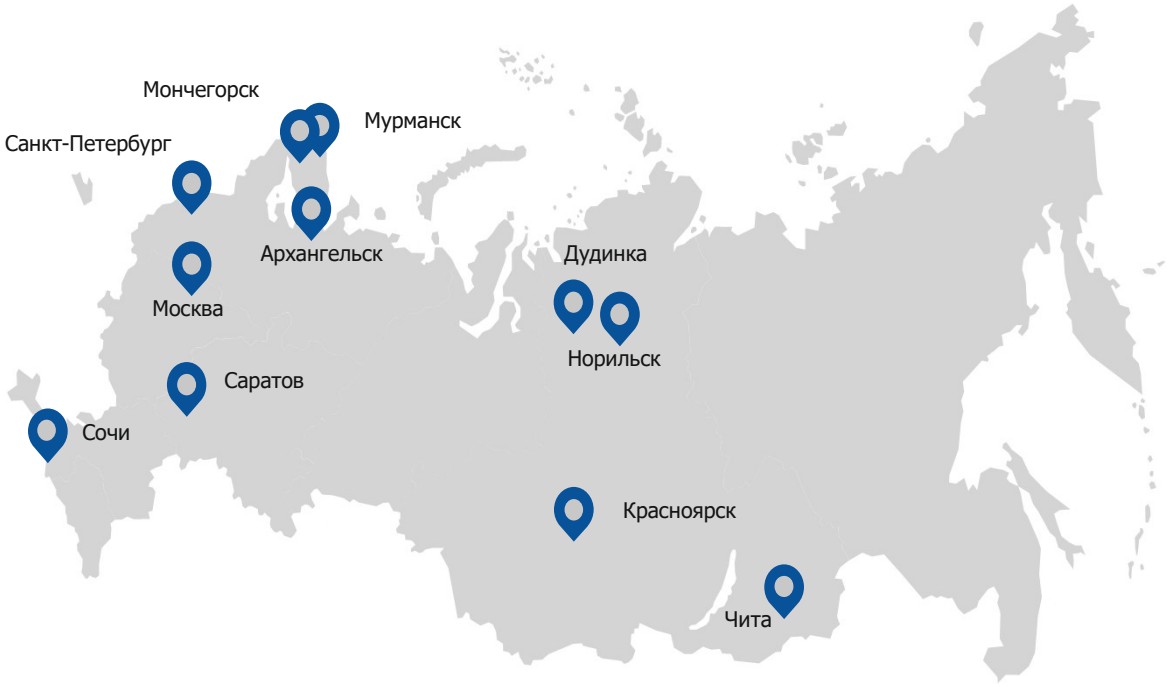
НАУЧНЫЕ КОМПЛЕКСЫ

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
					

Производственный цикл цветных металлов. Критические процессы: металлургия

НОРНИКЕЛЬ

- Обнаружение пожара и оповещение персонала о пожаре
- Контроль наличия в шахте метана
- Измельчение
- Флотация

- Плавка
- Огневое рафинирование меди
- Подготовка шихты в сушильном цехе
- Сушка концентрата
- Окислительно-сульфатизирующий обжиг никелевого шлама

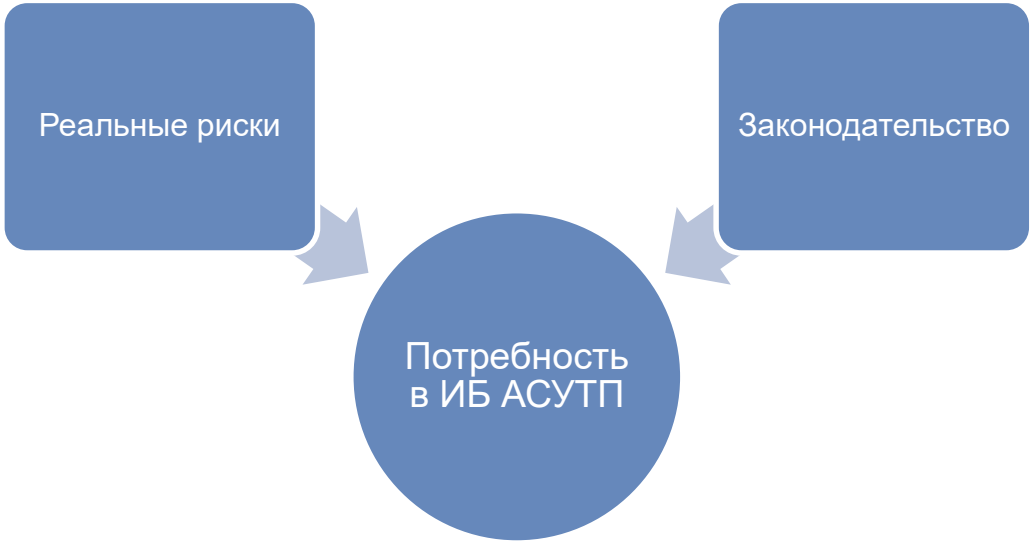
- Электролиз никеля
- Восполнение дефицита никеля
- Синтез тетра-карбонила никеля
- Электролиз кобальта
- Экстракционное отделение кобальта

- Прием, хранение и отправка хлора
- Прием, хранение и выдача соляной кислоты
- Производство элементной серы
- Производство и хранение серной кислоты

- Химводоподготовка
- Очистка газов и печей от пыли
- Фильтрация сливов
- Газоудаление
- Очистка промышленных стоков

- Электропитание цехов
- Управление насосами, импеллерами, воздухонагне тателями, приточная вентиляция и т.п.
- Газоудаление
- Электропитание
- Подача воздуха, кислорода, газов
- Подача воды

Основные драйверы ИБ АСУТП

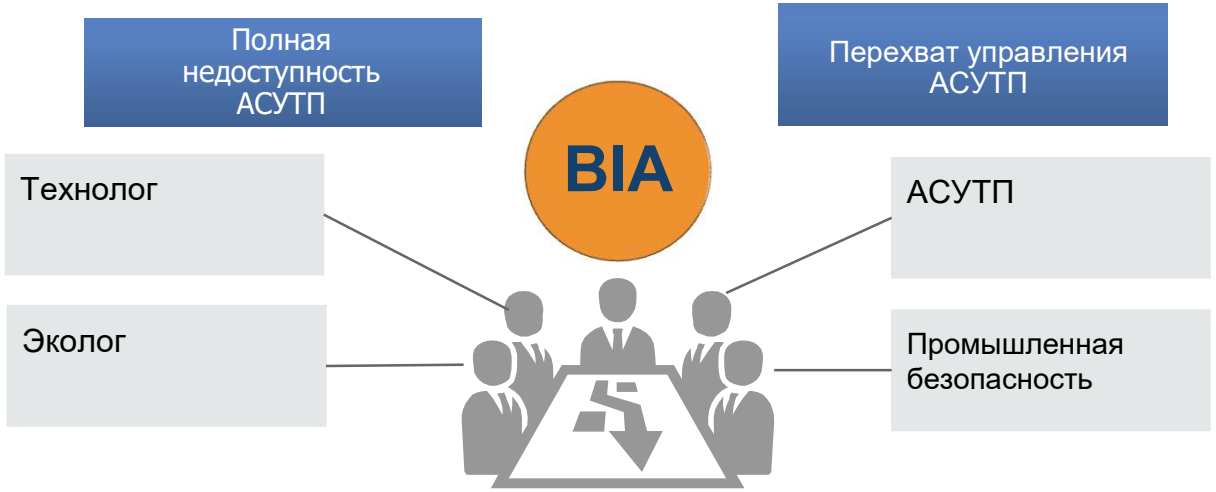


- Риски потери активов сопоставимы со стоимостью активов
- Риски останова сопоставимы с величиной выручки
- Риски нанесения вреда экологии, а также жизни и здоровью людей всегда приоритетны

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

Основные драйверы ИБ АСУТП

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

НОРНИКЕЛЬ

Снижение рисков информационной безопасности АСУ ТП

НОРНИКЕЛЬ

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

Структура системы защиты АСУ ТП предприятия

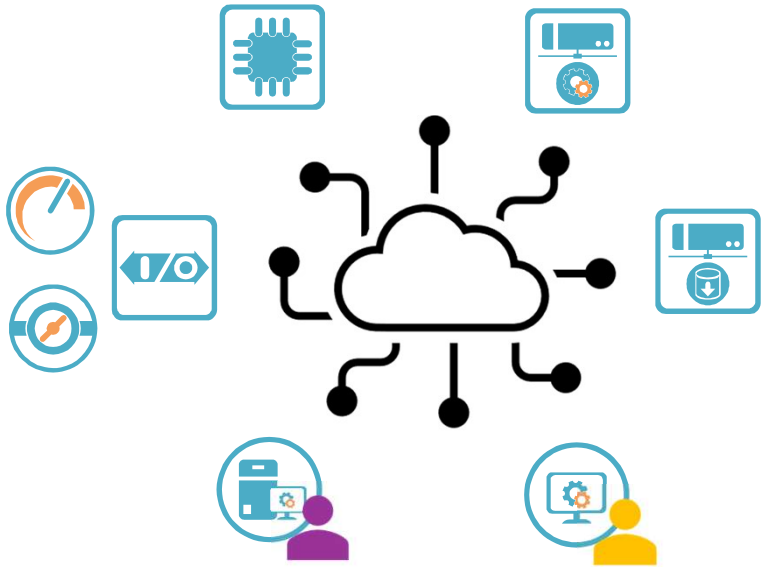
НОРНИКЕЛЬ

Корпоративная сеть

ИТ-сервисы

Информационные активы

Технологическая сеть

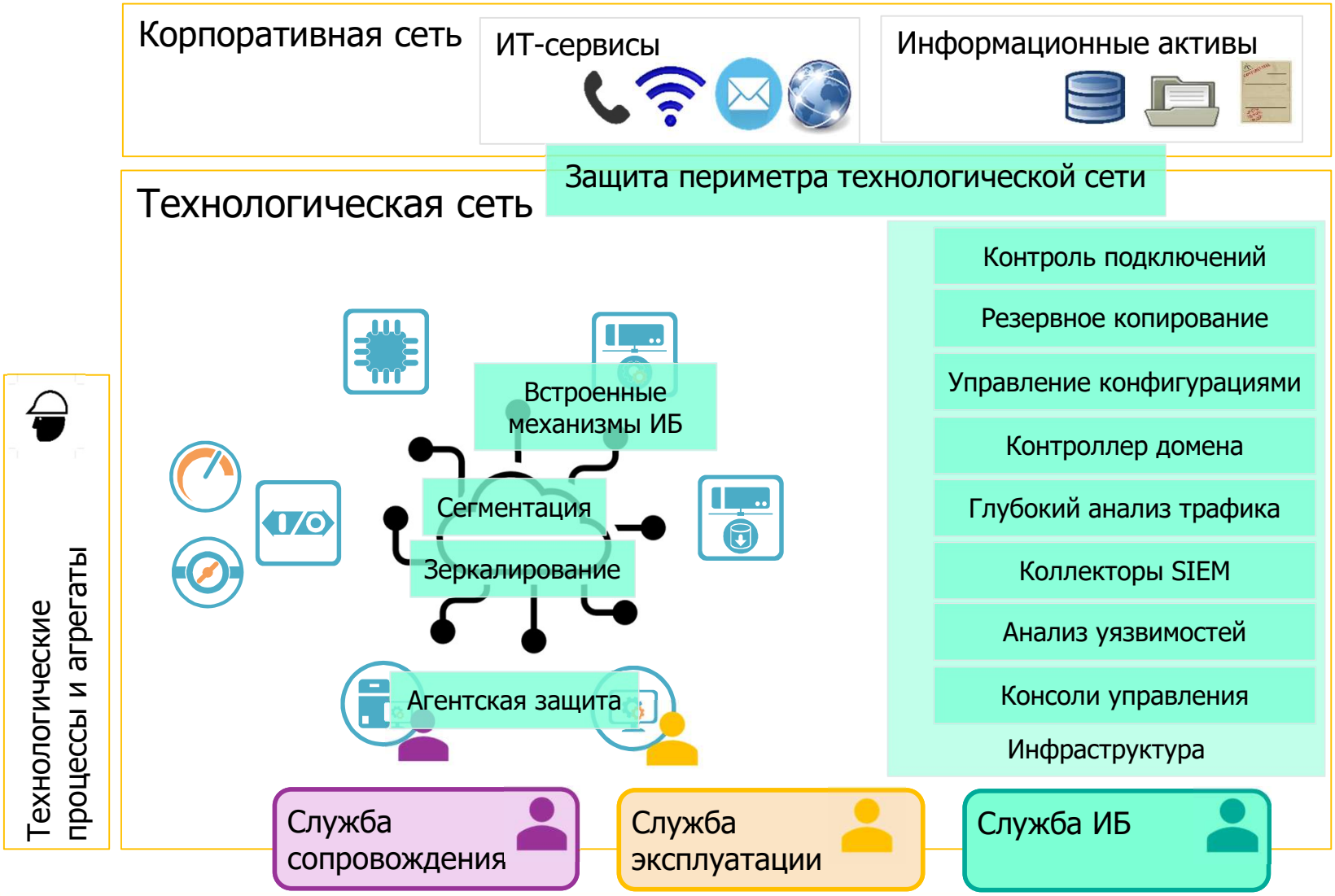


Технологические процессы и агрегаты

Служба сопровождения

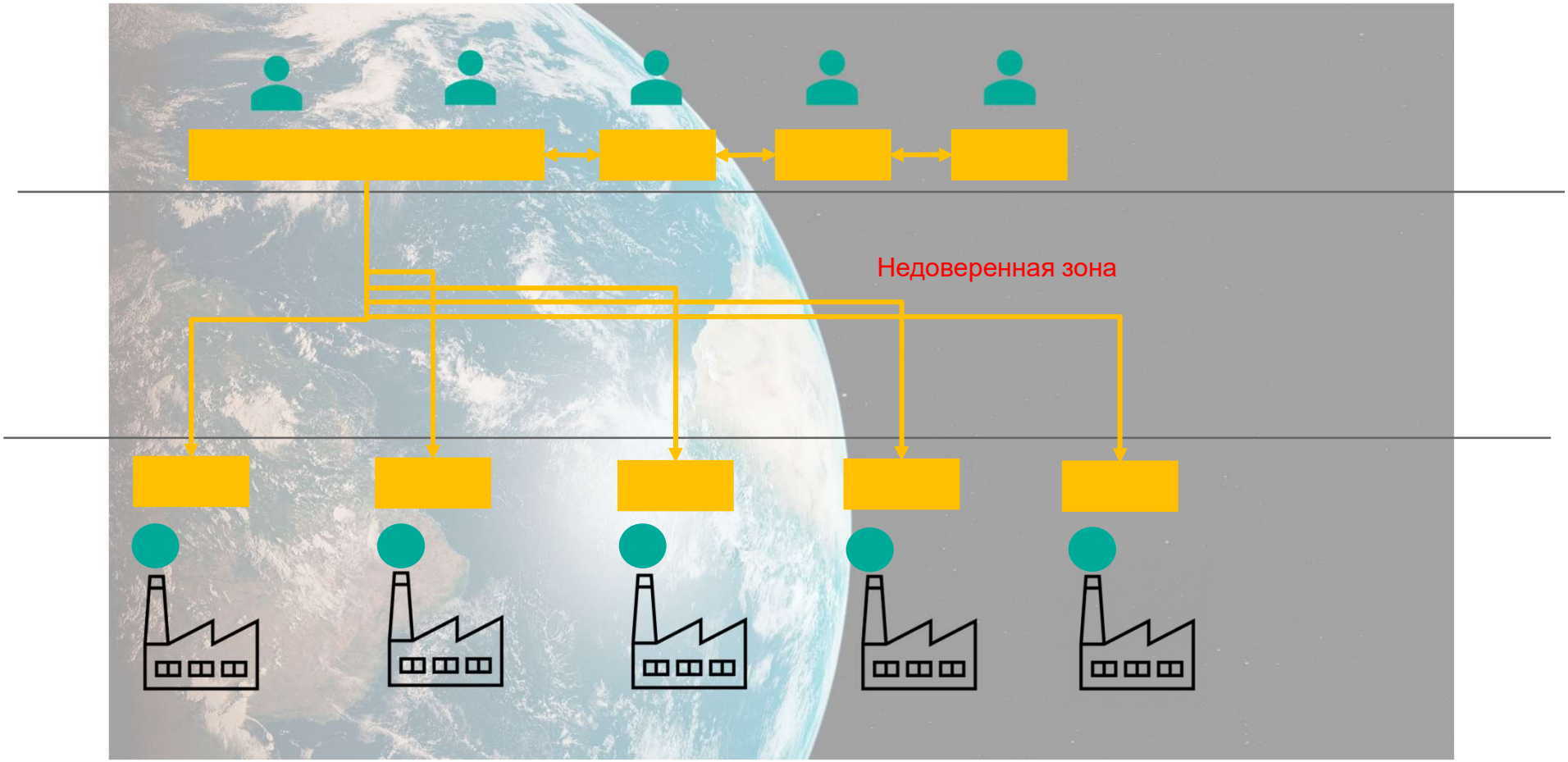
Служба эксплуатации

Структура системы защиты АСУ ТП предприятия



Комплексная система защиты АСУ ТП промышленной группы

Комплексная система защиты АСУ ТП промышленной группы



Базовые принципы создания комплексной системы защиты АСУ ТП

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

Базовые принципы создания комплексной системы защиты АСУ ТП

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

Базовые принципы создания комплексной системы защиты АСУ ТП

НОРНИКЕЛЬ

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

Базовые принципы создания комплексной системы защиты АСУ ТП

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

Базовые принципы создания комплексной системы защиты АСУ ТП

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!

Примеры известных компьютерных атак

НОРНИКЕЛЬ

Кибератака нарушила работу заводов Rheinmetall в трех странах

11:00 / 28 Сентября, 2019

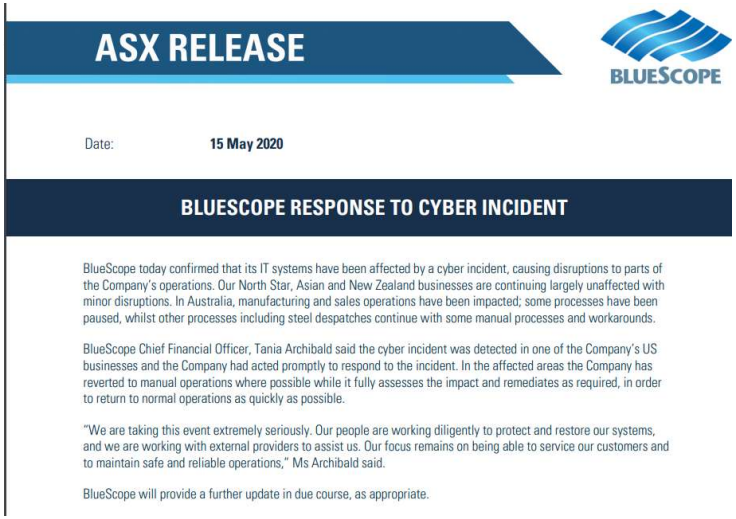
По оценкам компании, период восстановления после атаки займет примерно 2-4 недели, а убытки составят €3 млн - €4 млн в неделю.

https://www.securitylab.ru/news/501458.php

https://www.hydro.com/en/media/on-the-agenda/cyber-attack/

Потери компании Norsk Hydro от кибератаки оцениваются в $75 млн.

https://www.computerweekly.com/news/252467199/Norsk-Hydro-cyber-attack-could-cost-up-to-75m



https://ics-cert.kaspersky.ru/news/2020/05/20/cyber-incidents-in-industrial-enterprises-during-the-first-half-of-may/

https://s3-ap-southeast-2.amazonaws.com/bluescope-corporate-umbraco-media/media/2832/200515-asx-release-bluescope-update-15-may-2020.pdf

Выводы

Технологическая ИТ-инфраструктура относится к наивысшей зоне безопасности. Злоумышленник выбирает для атаки наиболее незащищенный компонент инфраструктуры.

Любая система или компонент, подключаемый к технологической сети, должен соответствовать стандартному уровню безопасности для этой сети.

Цифровизация предприятий должна идти рука об руку с информационной безопасностью и модернизацией инфраструктуры технологических сетей

В проекты по созданию/модернизации технологической ИТ-инфраструктуры и АСУТП должны закладываться требования ИБ. Защитить ПОТОМ будет намного дороже!

Выводы

НОРНИКЕЛЬ

Уязвимое звено системы – персонал

Каждый, кто участвует в процессе обеспечения безопасности, эксплуатации, а также обслуживания и ремонта значимых объектов, своими действиями или бездействием влияет на безопасность

Повышать осведомленность персонала

Добиться понимания, что киберугрозы настолько же опасны, как и угрозы промышленной безопасности

Проводить тестирование процедур реагирования на компьютерные инциденты

Безопасность – не отсутствие угроз, а поддержание непрерывной деятельности предприятий при условии их воздействия

Выводы

Безопасность – не отсутствие угроз, а поддержание непрерывной деятельности предприятий при условии их воздействия

благодаря совместной и слаженной работе подразделений эксплуатации, сопровождения и обеспечения безопасности

ВОПРОСЫ и ОТВЕТЫ