НОРНИКЕЛЬ

Процесс обеспечения соответствия требованиям законодательства в области защиты КИИ в Группе компаний «Норильский никель»

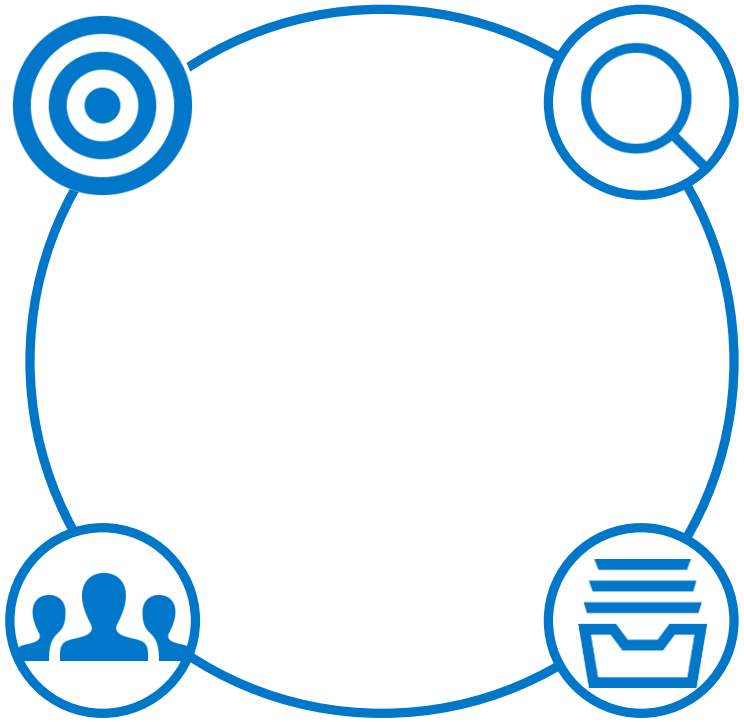
Игорь Железняк / ДЗИ

Версия 1.0, 08.02.2024

Норникель и КИИ

Металлургия
Горно-добывающая промышленность
Энергетика
ТЭК
Транспорт
Связь
Медицина
Наука

~20
Предприятий

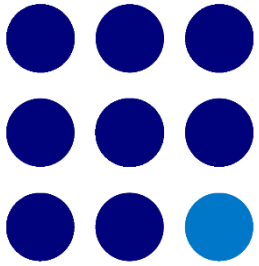


Есть значимые объекты КИИ

Риск, связанный с обеспечением безопасности ЗОКИИ – управляется на уровне Корпоративного управления рисками

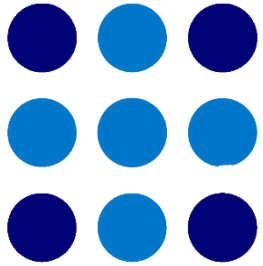
Большая часть значимых объектов КИИ - АСУТП

Защита КИИ в рамках БП ДЗИ



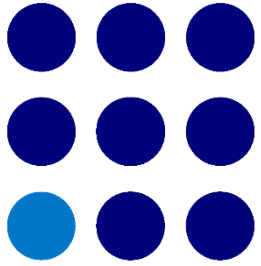
БП 1 уровня

Информационная безопасность



БП 2 уровня

1. Управление информационными активами и рисками ИБ
2. Управление комплаенсом в области ИБ
3. Управление архитектурой ИБ
4. Управление контролем ИБ
5. Управление проектной экспертизой в части ИБ
6. Управление эксплуатацией СЗИ
7. Управление инцидентами ИБ
8. Управление уязвимостями ИБ
9. Управление портфелем проектов в области ИБ



БП 3 уровня

1.1 Управление рисками ИБ
1.2 Управление непрерывностью ИБ
2.1 Обеспечение комплаенса в области защиты КИИ
2.2 Повышение осведомленности в области ИБ
2.2 Управление взаимоотношениями с регуляторами по вопросам ИБ
3.1 Формирование и обесп. целевой архитектуры ИБ
4.1 Оценка и контроль выполнения требований ИБ
5.1 Адаптация и контроль выполнения требований ИБ в рамках ИТ-проектов
6.1 Управление конфигурацией и обновлениями СЗИ
6.2 Управление ключевой информацией (криптография)
7.1 Выявление и обработка инцидентов ИБ
7.2 Расследование инцидентов ИБ
8.1 Анализ защищенности и выявление уязвимостей ИБ
9.1 Управление проектной деятельностью в области ИБ

ЛНА по защите КИИ

Методика обеспечения безопасности значимых объектов КИИ

Унифицированные мероприятия по обеспечению комплаенса в области защиты КИИ

1. Анализ угроз ЗОКИИ
2. Планирование мероприятий по защите ЗОКИИ
3. Создание системы защиты ЗОКИИ
4. Реагирование на компьютерные атаки и взаимодействие с ГосСОПКА
5. Обеспечение отказоустойчивости ЗОКИИ и реагирование на нештатные ситуации
6. Повышение осведомленности персонала в части защиты КИИ
7. Контроль защищенности

Стандарт обеспечения информационной безопасности на стадиях жизненного цикла ИС и АСУТП

Системообразующий локальный нормативный акт для функции ИБ в Группе «Норникель»

Набор требований ИБ для ИС/АСУТП в зависимости от результатов их классификации

Все ИС и АСУТП в Группе компаний «Норильский никель» должны соответствовать требованиям данного Стандарта

Порядок управления доступом

Порядок управления инцидентами ИБ

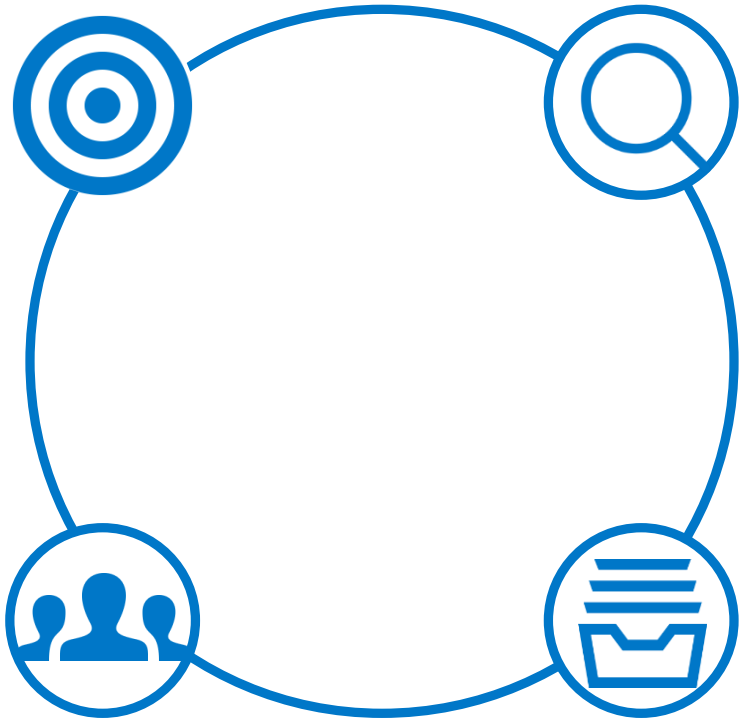
Порядок управления уязвимостями ИБ

Регламент повышения осведомленности персонала в области ИБ

И др.

Категорирование ОКИИ

Категорирование в ГК «Норникель» – это процесс



Практика – 2 вида категорирования

1) Категорирование по ПП-127
2) Предварительное категорирование в рамках проектной экспертизы

Экспертиза и автоматизация

1) Экспертиза проектных команд
2) База знаний по результатам предварительного категорирования
3) Реестры ЗОКИИ и предварительного категорирования
4) Набор типовых форм (шаблонов)

Предварительное категорирование в рамках проектной экспертизы

~300 ИТ-проектов за 2 года

Организация работ

План мероприятий по обеспечению безопасности ЗОКИИ

1) План на каждом предприятии, у которого есть ЗОКИИ
2) План согласовывается с Директором ДЗИ и утверждается Генеральным директором предприятия

Методологический подход

1) Чек-лист для фиксации информации
2) Типовая форма (шаблон) документированной информации

Управление мотивацией

Цели выполнения Плана – в КПЭ всех заинтересованных в рамках ИБ-вертикали

Основные участники

1) Отдел безопасности КИИ
2) Подразделения или специалисты по ИБ на предприятиях
3) Технологические подразделения и ИТ

Взаимодействие с регуляторами

Взаимодействие с регуляторами по вопросам ИБ – это процесс

Регуляторы

1) ФСТЭК России
2) НКЦКИ
3) ФСБ России
4) Отраслевые регуляторы (Минпромторг, Митранс, Минэнерго)
5) другие

~150 Запросов/писем в 2023г.

Экспертиза и автоматизация

1) Реестр запроса регуляторов по вопросам ИБ
2) База знаний по обработке запросов
3) Специалисты с высшим юридическим образованием

Письма УФСТЭК по СФО «о мерах по защите ИИ РФ»

~20% Уязвимостей/угроз актуальны для предприятий Группы

Импортозамещение

Целевой ландшафт СЗИ

В 2022-2023 гг. выполнена работа по анализу СЗИ, сравнению и тестированию

Все СЗИ для защиты ЗОКИИ – соответствуют требованиям ПП-1912

Проекты по импортозамещению

ДЗИ выполняет проекты по импортозамещению СЗИ

Программа проектов до 2030г.

Тренды

- **Импортозамещение**
- **Перечни типовых ОКИИ**
- **Запросы регуляторов по теме ИБ**

Благодарю за внимание!