



Ключевые показатели для достижения киберзащищенности АСУ ТП

 Казаков Дмитрий Валентинович

 12.04.2024





«Северсталь» – вертикально-интегрированная горнодобывающая и сталелитейная компания.

Череповецкий металлургический комбинат – основной актив компании «Северсталь».

«Северсталь-инфоком» — центр информационных и коммуникационных технологий компании «Северсталь».





KPI по информбезопасности для ПАО «Северсталь»

KPI (англ. key performance indicators) – ключевые показатели эффективности.

KPI по ИБ АСУ ТП с 2020 года. В KPI 2023 29 показателей, в KPI 2024 обсуждается 35.

Определяется минимальное, базовое и амбициозные значения.

Учитывается текущее значение. Для новых показателей – экспертная оценка.

Назначается вес показателя от 1 до 4, расчёт по формуле.

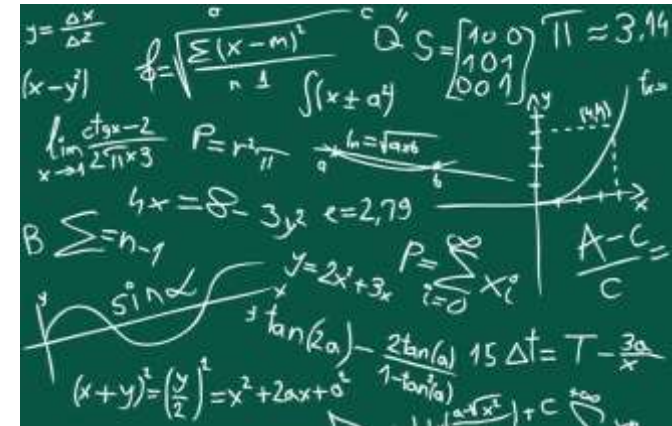
Итоговая защищённость 2023 **102%**. По показателям направления КИИ **117%**.

Группы ответственных:

- направление КИИ
- автоматизация L1 и L2
- сетевые специалисты
- ответственные за ИТ-оборудование
- администраторы БД
- разработчики ПО

За некоторые показатели совместная ответственность.

УИБ разделяет ответственность с руководителями ИТ-подразделений.





Группы КРІ



Управление активами



Эффективность работы СЗИ



Управление уязвимостями



Мониторинг ИБ



Резервное копирование



Защищенность критичных хостов АСУ ТП



Защищенность СУБД



Управление ПО



Безопасная разработка ПО



Защищенность инфраструктуры



Пример группы КРІ



Управление активами – сколько ИТ-устройств занесено в CMDB (систему учёта) в соответствии с инструкциями (проверка по обязательным полям)

- 01** % виртуальных машин и гипервизоров
- 02** % физических ПК и серверов
- 03** % активного сетевого оборудования (коммутаторов)
- 04** % ПЛК (контроллеров)

Учёт оборудования – выполнена амбиция!



№	Показатель	KPI 2022	Мин.	База	Амбиция	KPI 2023
1	% VM и гипервизоров, занесенных в CMDB в соответствии с инструкцией	98,22%	98%	99%	100%	100%
2	% физических ПК и серверов, занесенных в CMDB в соответствии с инструкцией	98,22%	98%	99%	100%	100%

Что позволило достичь результата

Новая категория в CMDB – VM на ПК

Командная работа

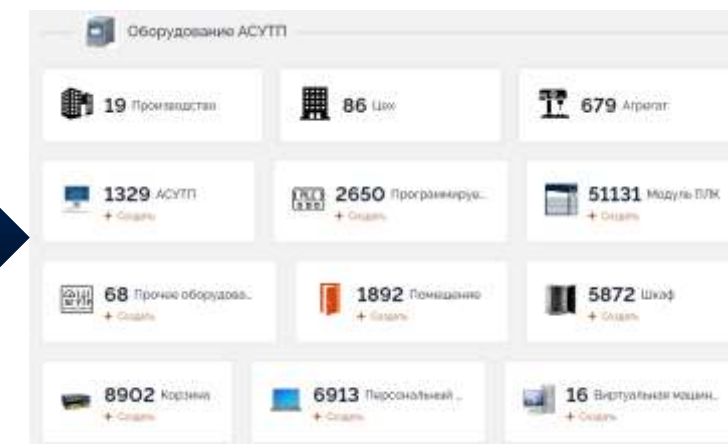
Высокое внимание к показателю руководителей УТА

Перспектива показателя

Необходимо поддерживать

Точечные несоответствия проще исправить

Готовы к введению новых полезных полей



Антивирусная защита – рекорд!



№	Показатель	KPI 2022	Мин.	База	Амбиция	KPI 2023
7	% АВЗ на хостах Windows, работающих без ошибок	97,40%	97%	98%	99%	99,20%

Что позволило достичь результата

Справились с проблемными:

- меняли ОС
- выводили из эксплуатации
- применяли разные продукты и версии антивируса

Перспектива показателя

Достижение аналогичных значений для Linux



Резервное копирование – сильный результат



№	Показатель	KPI 2022	Мин.	База	Амбиция	KPI 2023
17	% физических хостов АСУ ТП из CMDB, имеющих резервную копию или план восстановления	82,15%	90%	95%	98%	97,43%
18	% виртуальных хостов АСУ ТП из CMDB, имеющих резервную копию или план восстановления	76,60%	90%	95%	98%	95,55%

Что позволило достичь результата

Инструменты (в том числе новый), см. скриншот ниже
 Инициатива группы КИИ (в том числе заявки)
 Решение по клонированным VM (техподдержка предоставила)
 Выпуск регламента, прописана ответственность

Перспектива

Чтобы добиться 100%, при вводе в работу сразу делать бэкап



Другой вариант (указать в примечании)

Имеется единый образ

Имеется резервный компьютер

Переустановка ОС

Описание КЕ Камера-ПК4 АПР

Служебная информация

АСУТП

КИИ

Бэкап требуется



Перспективы КРІ по ИБ

- 01** Тираж на другие предприятия «Севергрупп» и не только по АСУ ТП.
Статус: выполнено на части предприятий.
Для ИТ-функции введен общий показатель «Киберкультура».

- 02** Ежегодный пересмотр (добавление, удаление, повышение планки).
Выполняется.

- 03** Добавление в годовые цели максимальному количеству сотрудников, влияющих на показатели.
В работе.

- 04** Наиболее точная группировка показателей по командам ответственных.
В работе.





КРІ по
кибербезопасности –
всем в годовые цели!

