



Ключевые показатели для достижения киберзащищенности АСУ ТП

 Казаков Дмитрий Валентинович

 16.10.2024





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

Череповецкий металлургический комбинат – основной актив компании «Северсталь».

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



Что делать?



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

Как формулируем

Определяем KPI по ИБ АСУ ТП с 2020 года.

Количество пунктов растёт (в KPI 2023 29 показателей, в KPI 2024 – 33).

Для каждого определяются минимальное, базовое и амбициозное значение.

Формируем цели, учитывая текущие значения, для новых показателей – экспертная оценка.

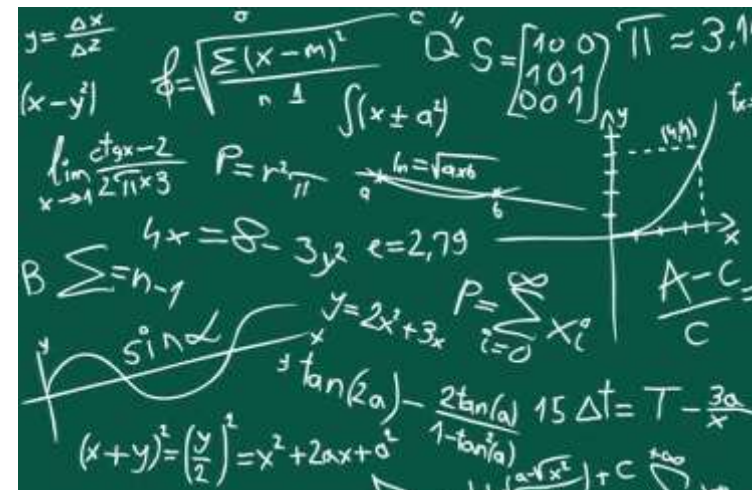
Назначается вес показателя от 1 до 4.

Сводный показатель рассчитываем по формуле.

Результаты

Итоговая защищённость 2023 **102%**.

(По показателям направления КИИ **117%**).



Кто виноват?



Документ

по достижению сводного показателя защищенности АСУ ТП
подписывают руководители управлений «Инфоком» и профильной службы УИБ.
Утверждает ИТ-директор.

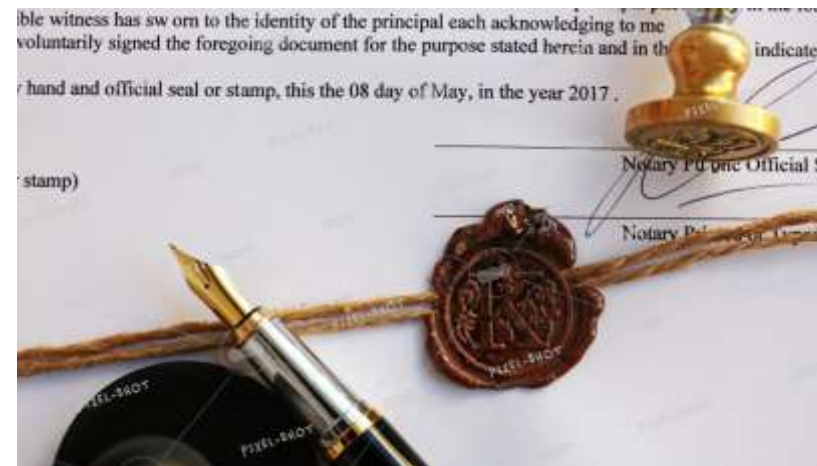
Непосредственные исполнители

Группы ответственных:

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

Как это работает

Есть ответственные за каждый пункт,
за некоторые показатели совместная ответственность нескольких групп.
УИБ разделяет ответственность с руководителями ИТ-подразделений.
От выполнения KPI зависит годовое вознаграждение.



Группы KPI



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 KPI



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)

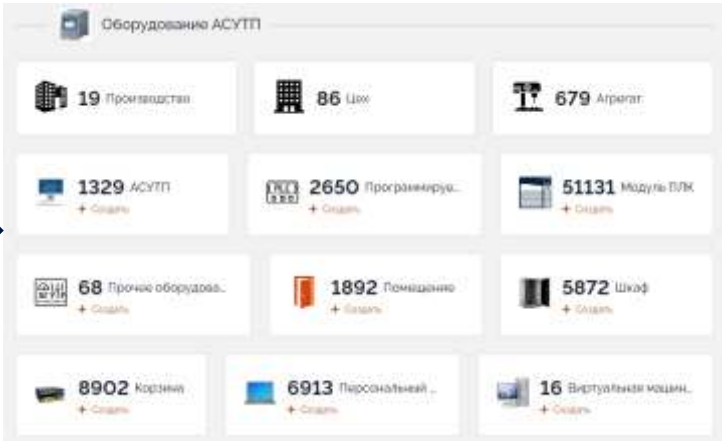
Учёт оборудования – выполнена амбиция!



№	Показатель	KPI 2022	Мин.	База	Амбиция	KPI 2023
1	% ВМ 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 – ВМ 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 ВМ (техподдержка предоставила)
Выпуск регламента, прописана ответственность

Перспектива

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



Описание КЕ Камера-ПК4 АПР

Служебная информация

АСУТП ☒ КИИ ☐ Бэкап требуется ☒

Другой вариант (указать в примечании)

Имеется единый образ

Имеется резервный компьютер

Переустановка ОС

Перспективы KPI по ИБ



- 01 Тираж** на другие предприятия «Севергрупп» и не только по АСУ ТП.
Статус 2024: выполнено на части предприятий и по КСПД. Дополнительно: 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.
Важна точная группировка показателей по командам ответственных для справедливого вознаграждения.
Требуется дополнительных усилий.





КРІ по
кибербезопасности –
всем в годовые цели!

