SECURITM

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Управление процессами ИБ через метрики

Николай Казанцев,
CEO SECURITM

securitm.ru

SECURITM решает проблему деградации систем защиты

Меры
Учет организационных и технических мероприятий

Задачи
Таск-менеджер для операционной работы

Риски
Управление ИБ на базе риск-ориентированного подхода

Каталоги
БДУ ФСТЭК,
MITRE ATT@CK

RPA
Robotic process automation
автоматизация задач

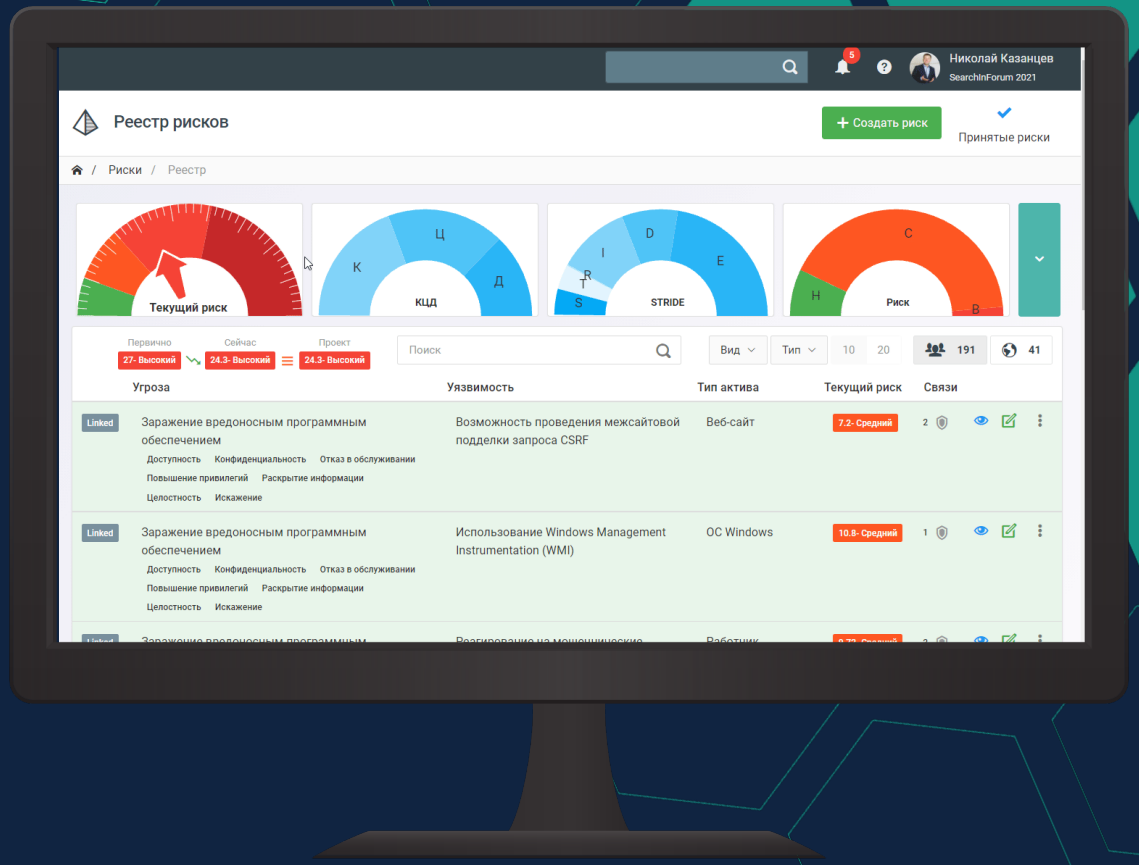
Метрики
Конструктор метрик для процессов ИБ

Опросы
Сбор сведений с работников и контрагентов, Service Desk

Уязвимости
Агрегатор отчетов от сканеров безопасности

Требования
Соответствие требованиям регуляторики и стандартов по ИБ

Активы
Учет и управление любыми типами активов



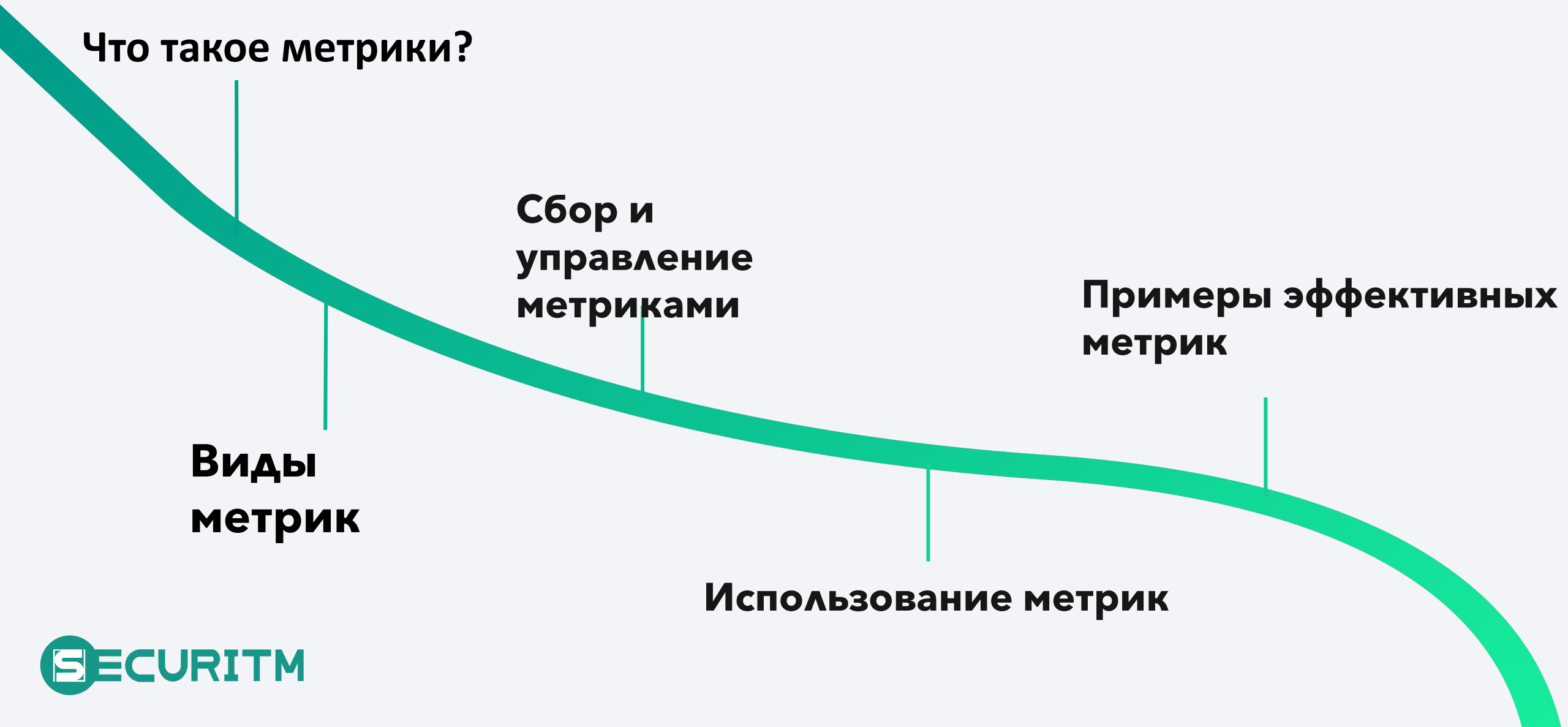
SECURITM

> 3000 пользователей

Открытая цена

Бесплатная **Community** версия

О чем?



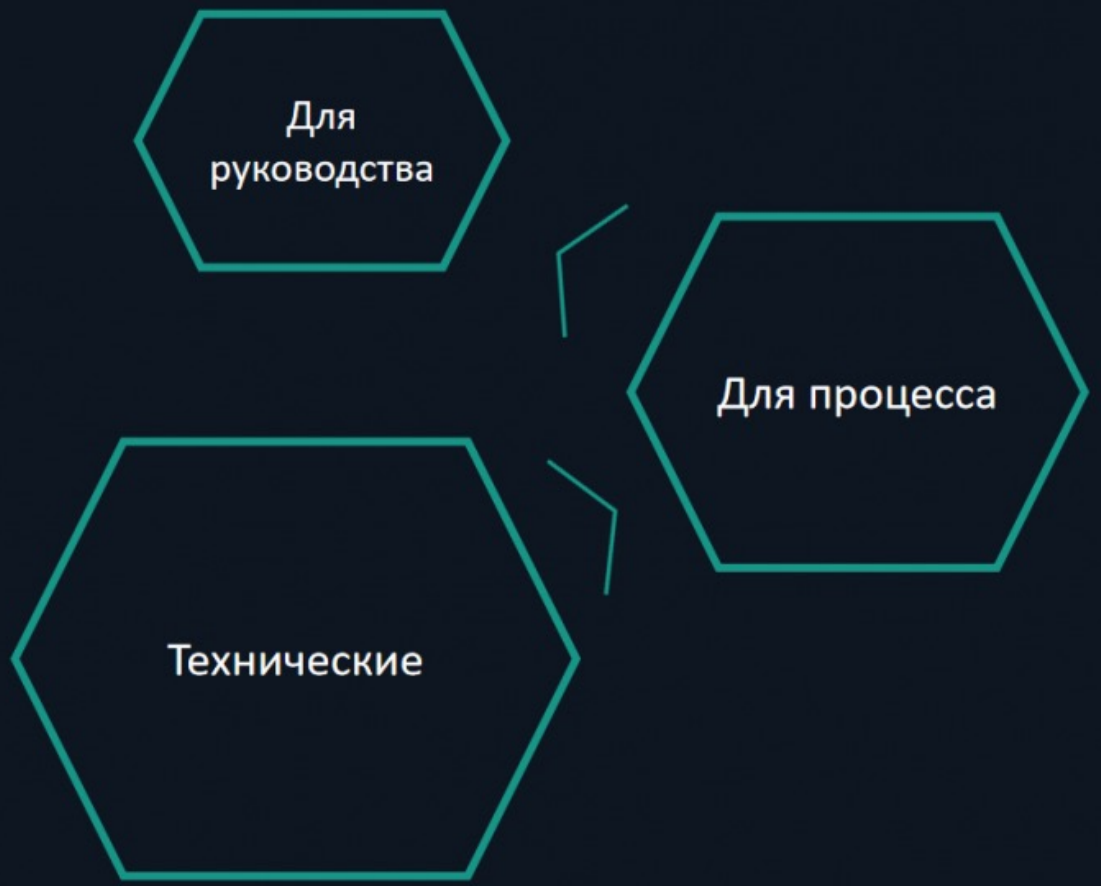
SECURITM

Что такое метрики?

Метрики – это количественные и/или качественные показатели, используемые для оценки эффективности систем и процессов.

- Метрика должна иметь цель и быть эффективной

Для чего метрики ИБ?



SECURITM

Для чего вы используете метрики ИБ?

Анонимный опрос

22% Показать руководству

38% Контролировать процессы

7% Оценить соответствие

9% Посчитать риски

24% А для чего их еще можно использовать - узнаете на вебинаре

45 голосов

❤️ 4 🔥 4 👍 2

207 15:15

Прокомментировать

Метрики бывают разные

Полезные

Уровень/процент соответствия

Процент АРМ с установленным СЗИ

Процент контрагентов с NDA

Количество обученных сотрудников

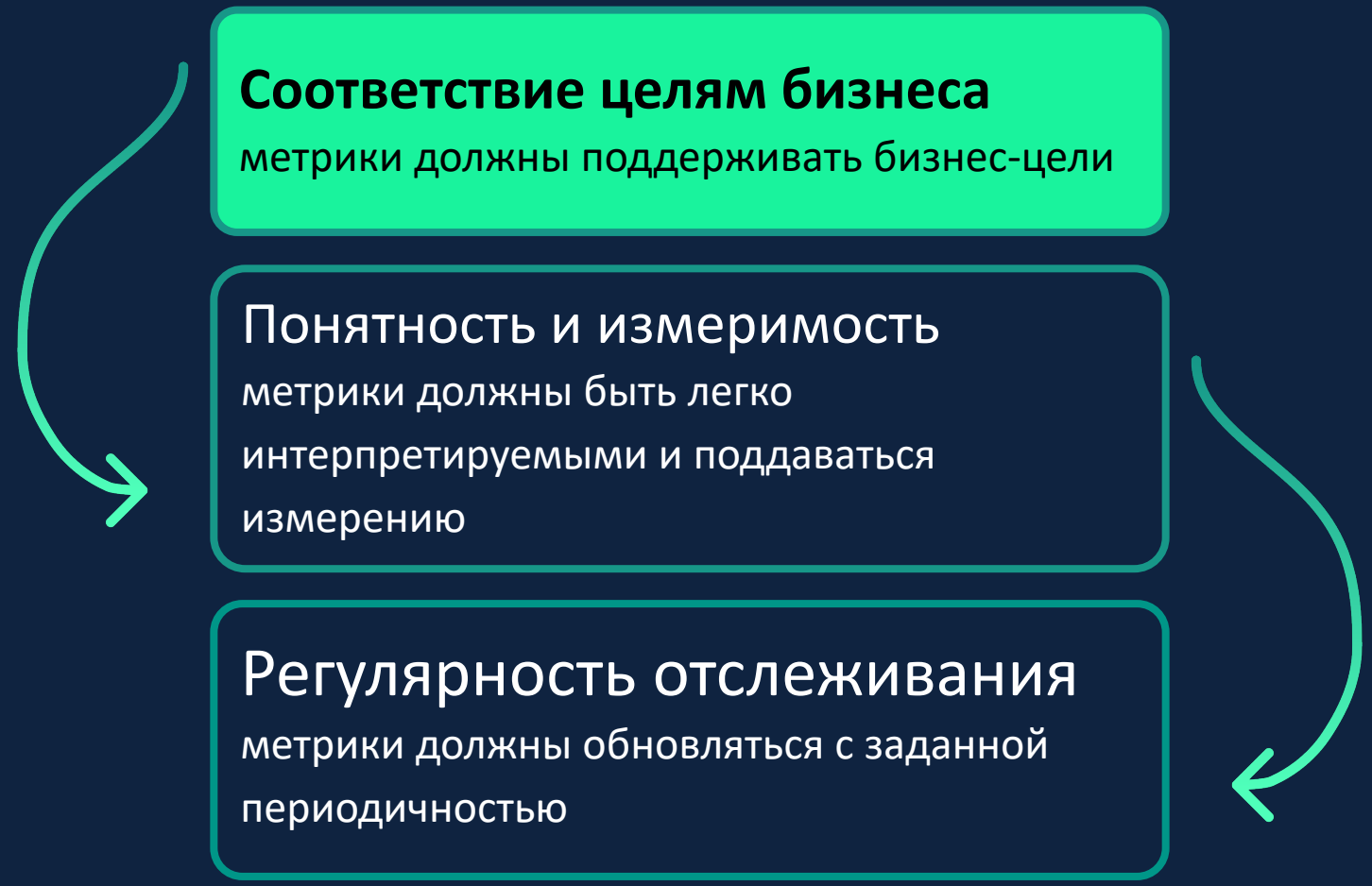
Бесполезные

Количество заблокированных СПАМ писем

Количество отраженных вирусных атак

Количество проверенных договоров

Как выбрать метрики?



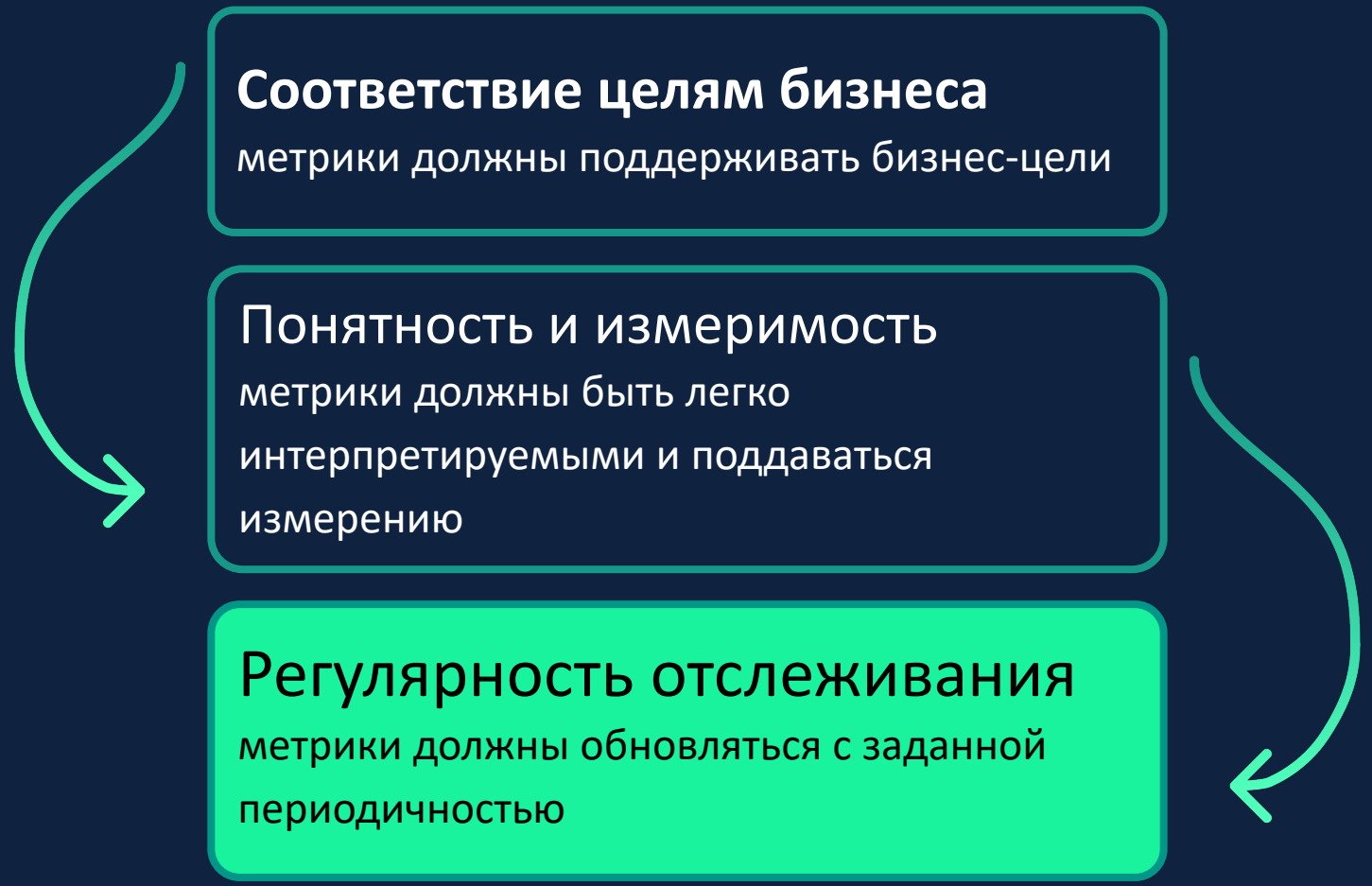
Как выбрать метрики?

Соответствие целям бизнеса
метрики должны поддерживать бизнес-цели

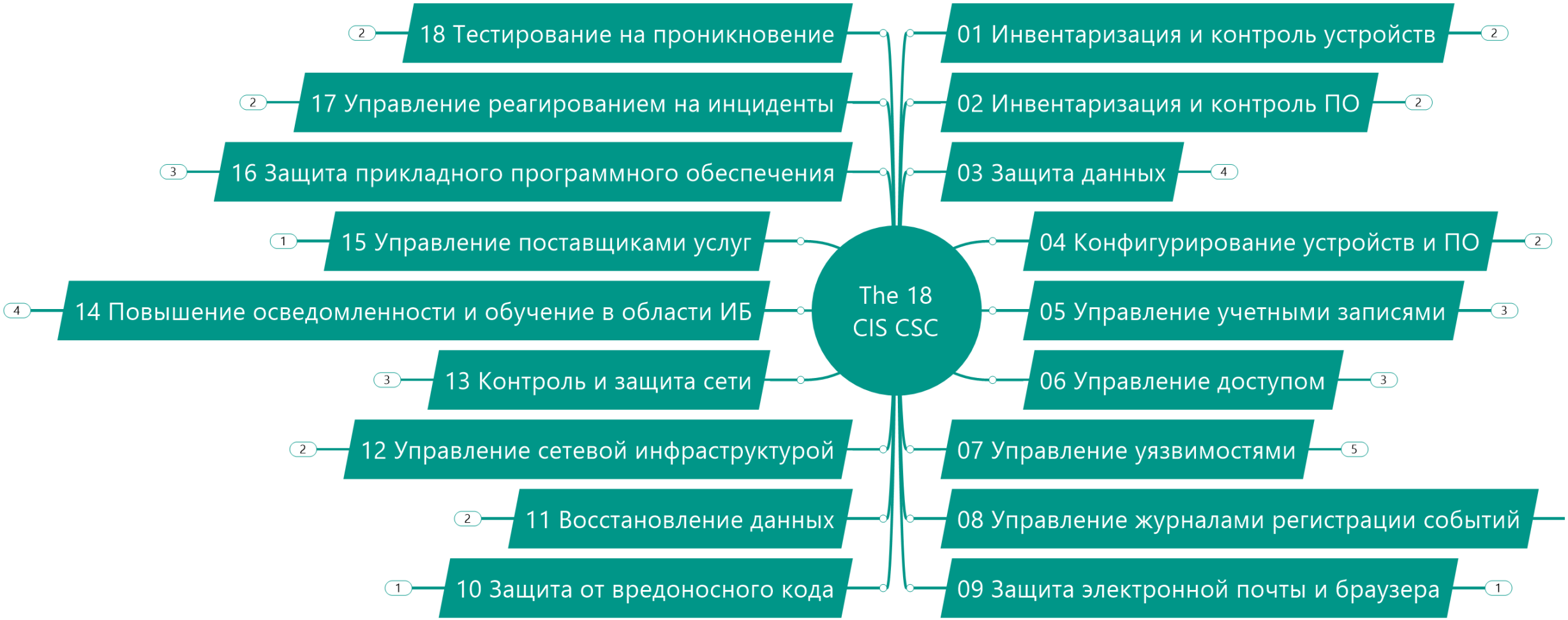
Понятность и измеримость
метрики должны быть легко интерпретируемыми и поддаваться измерению

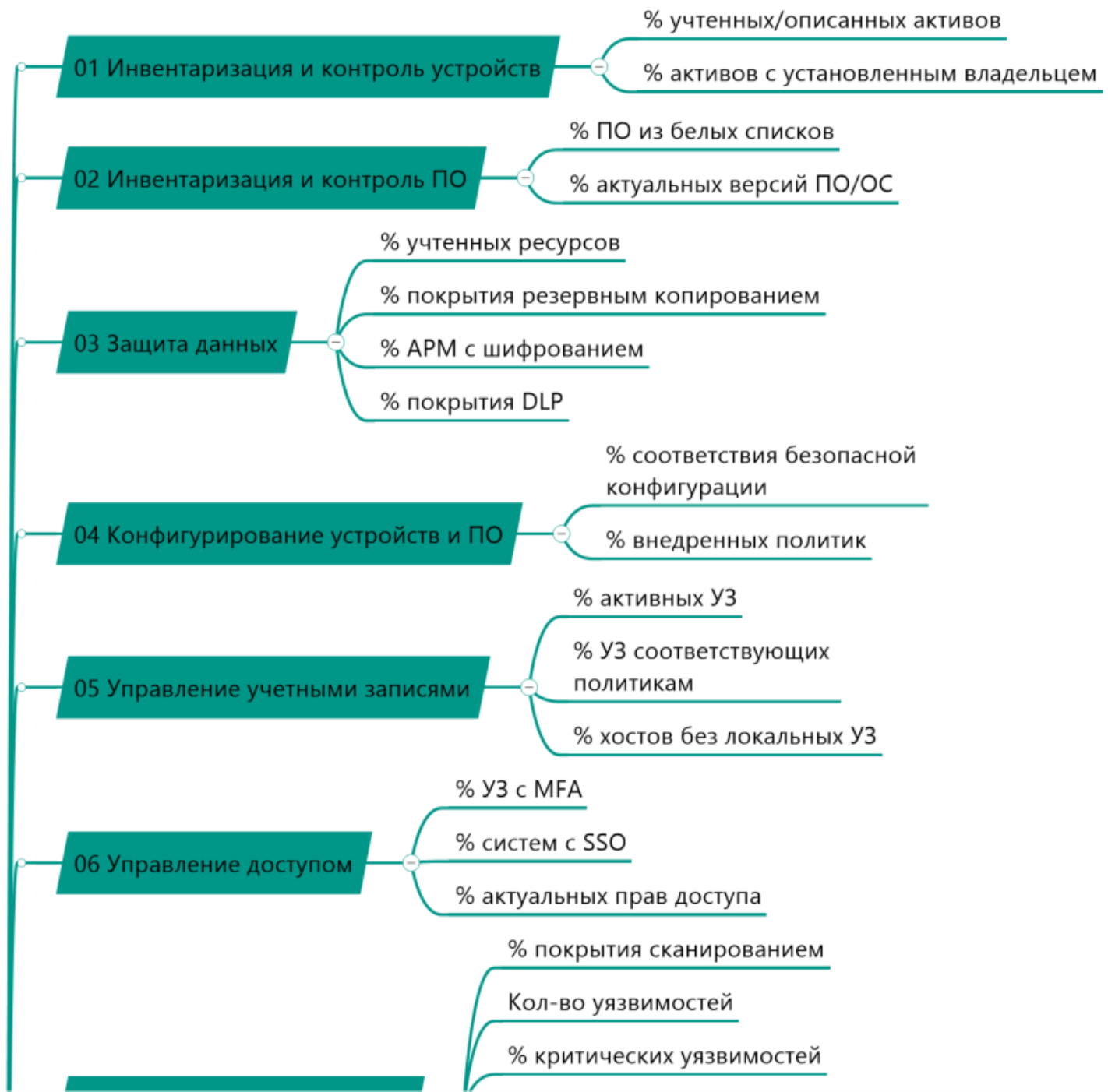
Регулярность отслеживания
метрики должны обновляться с заданной периодичностью

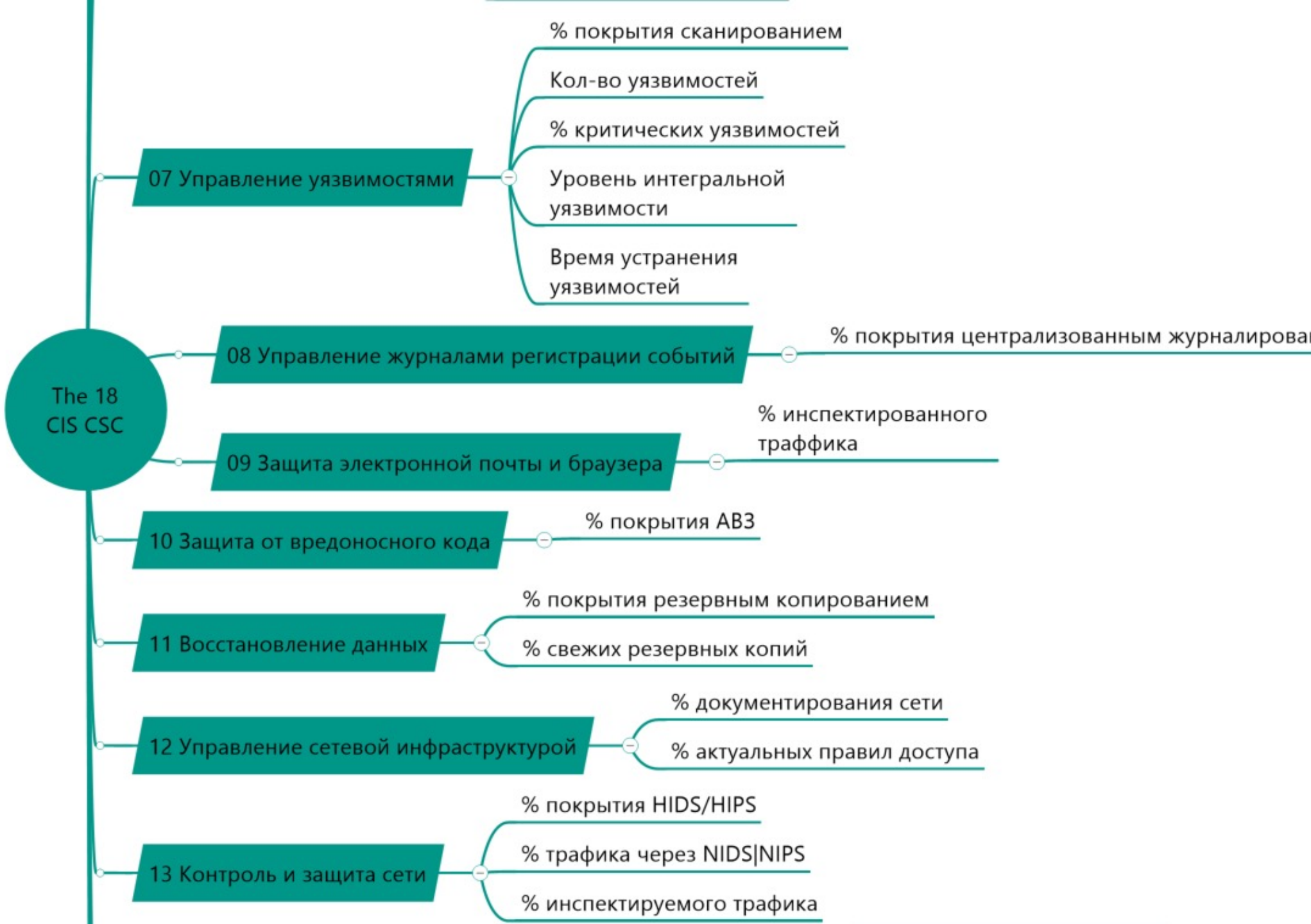
Как выбрать метрики?

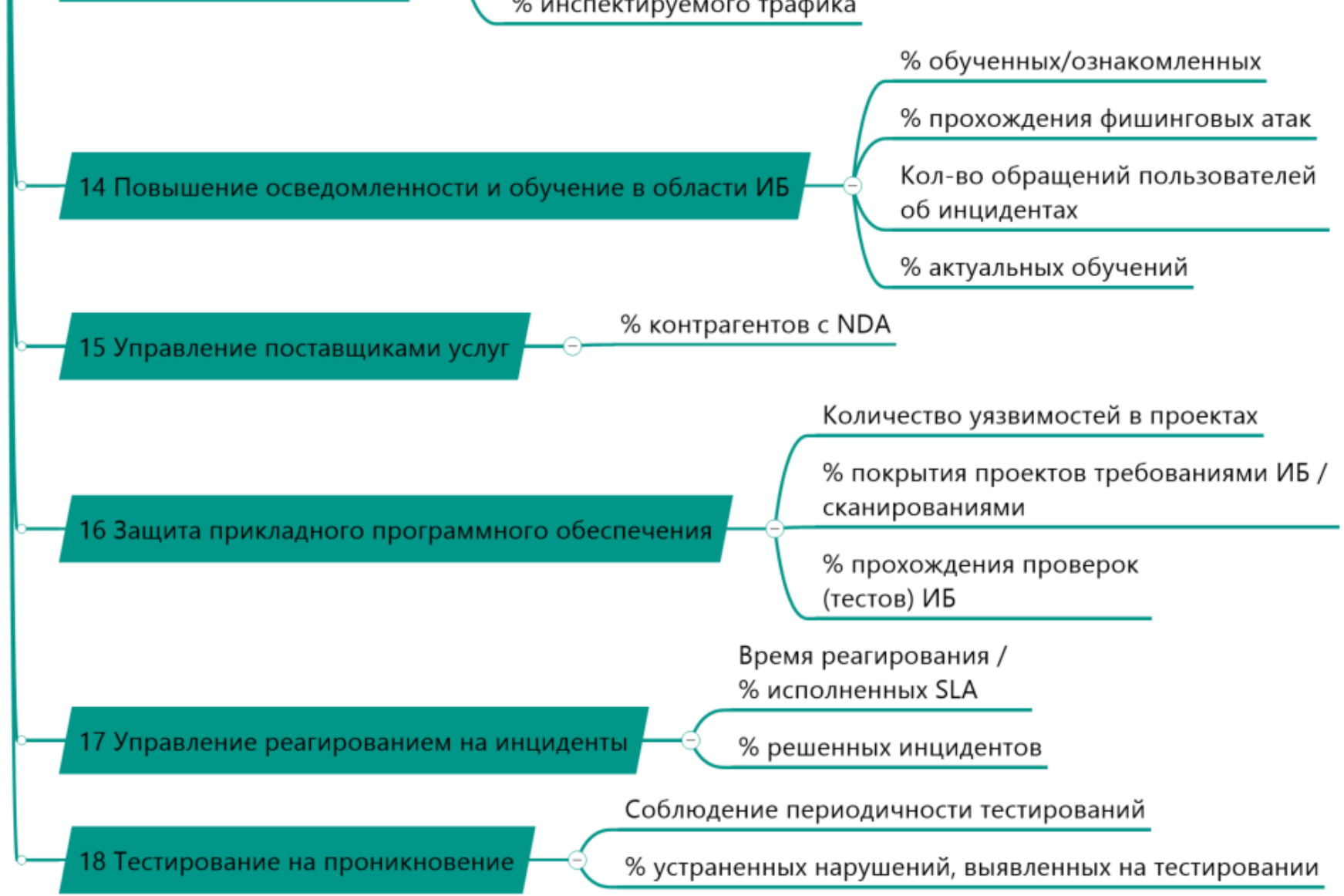


Метрики по процессам




01 Инвентаризация и контроль устройств
% учтенных/описанных активов
% активов с установленным владельцем
02 Инвентаризация и контроль ПО
% ПО из белых списков
% актуальных версий ПО/ОС
03 Защита данных
% учтенных ресурсов
% покрытия резервным копированием
% АРМ с шифрованием
% покрытия DLP
04 Конфигурирование устройств и ПО
% соответствия безопасной конфигурации
% внедренных политик
05 Управление учетными записями
% активных УЗ
% УЗ соответствующих политикам
% хостов без локальных УЗ
06 Управление доступом
% УЗ с MFA
% систем с SSO
% актуальных прав доступа
% покрытия сканированием
Кол-во уязвимостей
% критических уязвимостей

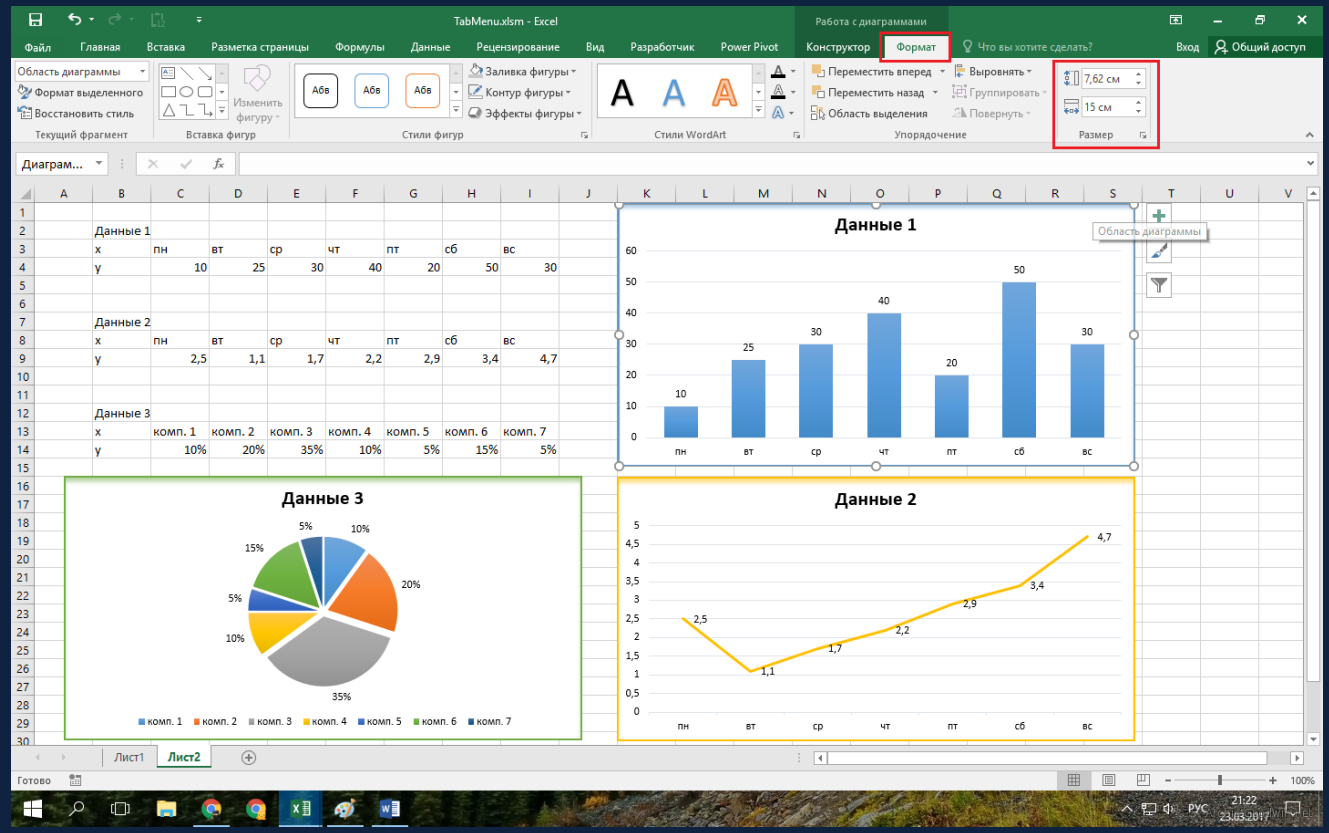

The 18 CIS CSC
07 Управление уязвимостями
% покрытия сканированием
Кол-во уязвимостей
% критических уязвимостей
Уровень интегральной уязвимости
Время устранения уязвимостей
08 Управление журналами регистрации событий
% покрытия централизованным журналирова
09 Защита электронной почты и браузера
% инспектированного траффика
10 Защита от вредоносного кода
% покрытия АВЗ
11 Восстановление данных
% покрытия резервным копированием
% свежих резервных копий
12 Управление сетевой инфраструктурой
% документирования сети
% актуальных правил доступа
13 Контроль и защита сети
% покрытия HIDS/HIPS
% трафика через NIDS|NIPS
% инспектируемого трафика


% инспектируемого трафика
14 Повышение осведомленности и обучение в области ИБ
% обученных/ознакомленных
% прохождения фишинговых атак
Кол-во обращений пользователей об инцидентах
% актуальных обучений
15 Управление поставщиками услуг
% контрагентов с NDA
16 Защита прикладного программного обеспечения
Количество уязвимостей в проектах
% покрытия проектов требованиями ИБ / сканированиями
% прохождения проверок (тестов) ИБ
17 Управление реагированием на инциденты
Время реагирования / % исполненных SLA
% решенных инцидентов
18 Тестирование на проникновение
Соблюдение периодичности тестирований
% устраненных нарушений, выявленных на тестировании

Сбор и расчет метрик

Быстрый старт

Ручной сбор



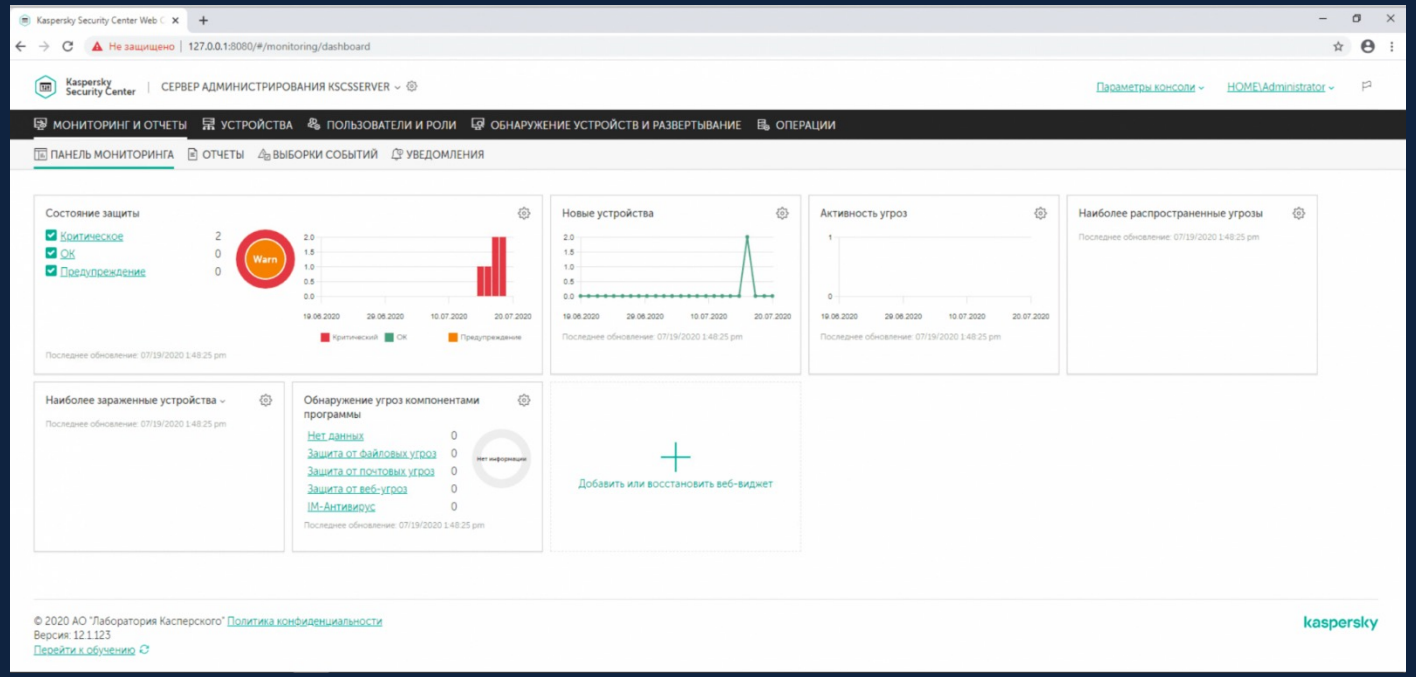
Сбор и расчет метрик

Консоли СЗИ

Автоматический сбор

Ограниченный набор метрик

Множество несвязанных консолей

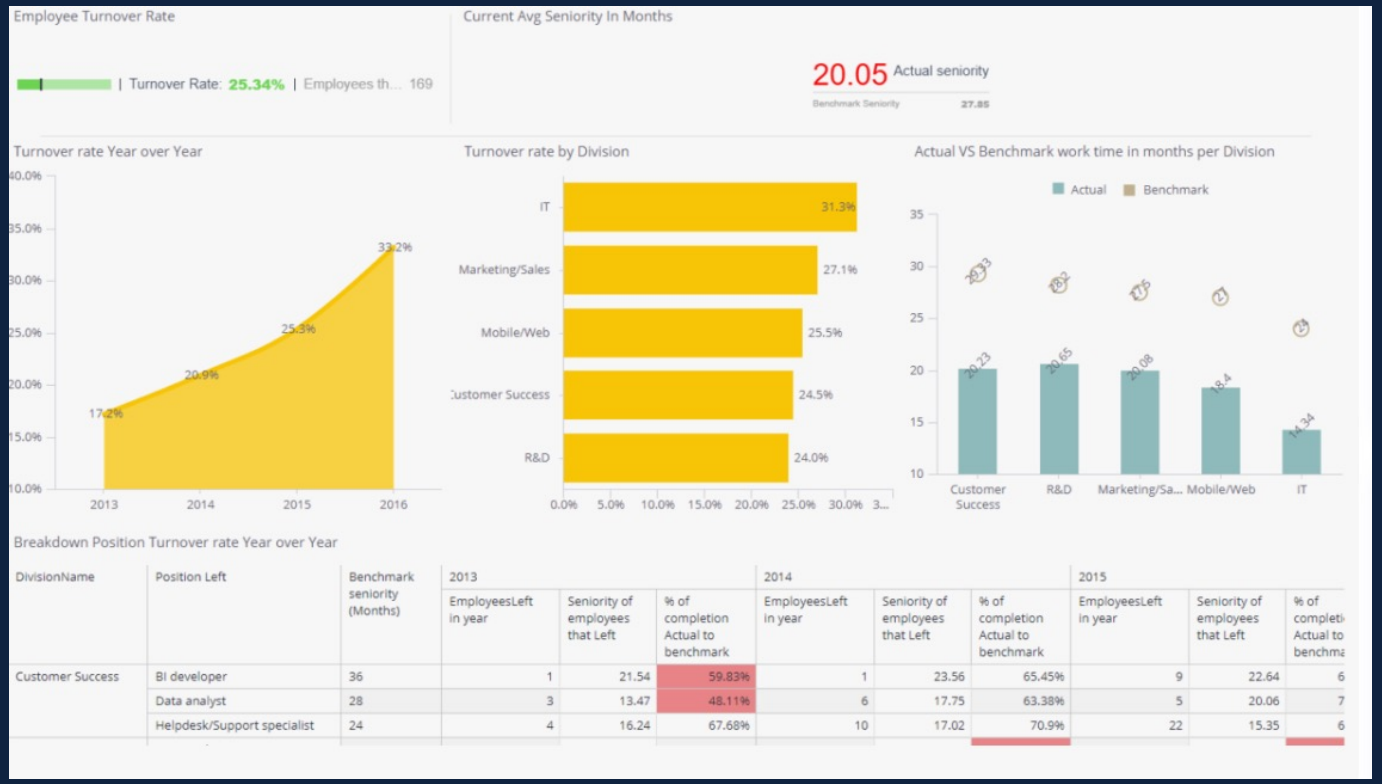


Сбор и расчет метрик

BI

Объединение разных источников

Нет реакции на изменение метрик

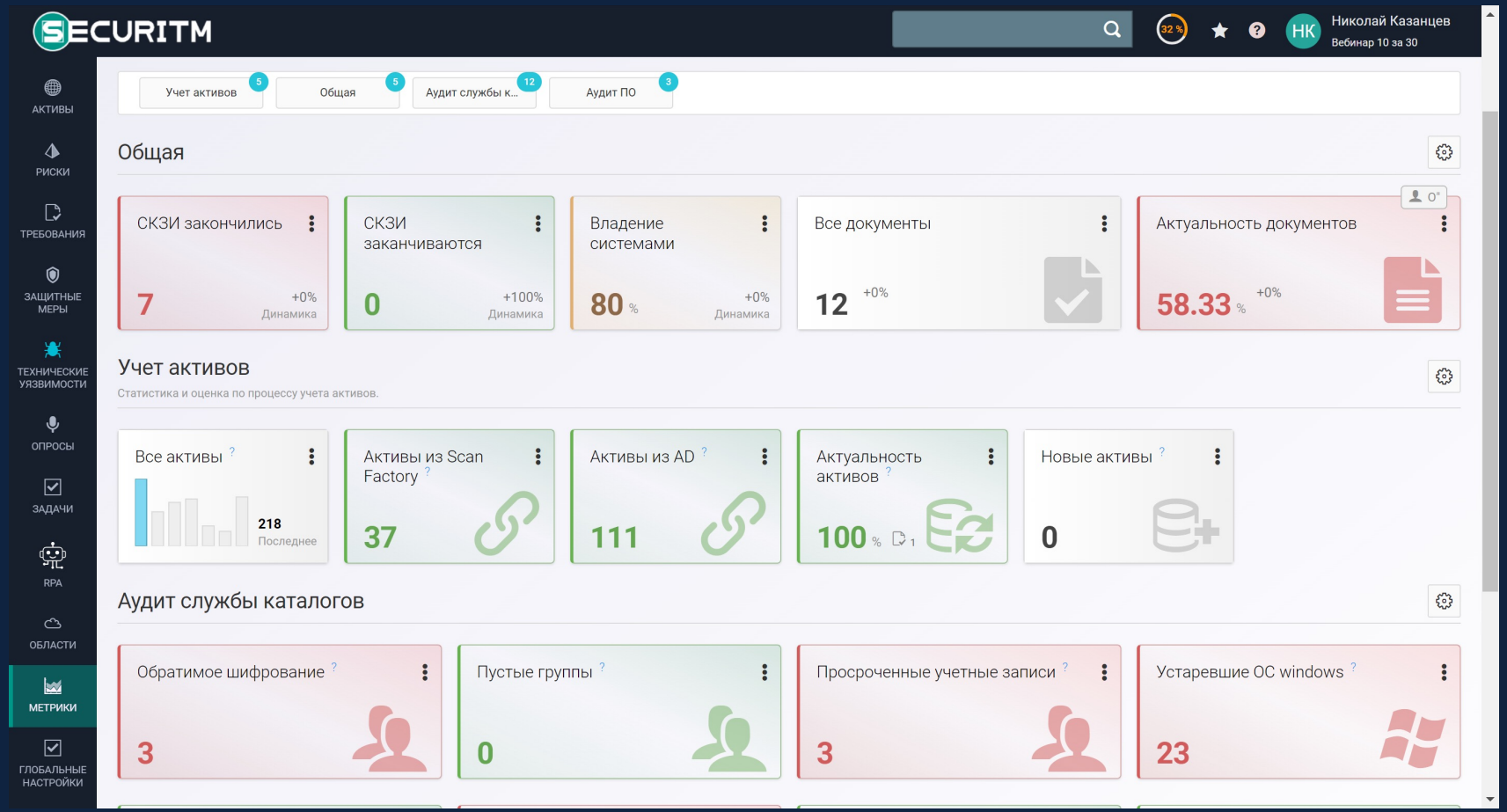


DivisionName	Position Left	Benchmark seniority (Months)	2013			2014			2015		
			EmployeesLeft in year	Seniority of employees that Left	% of completion Actual to benchmark	EmployeesLeft in year	Seniority of employees that Left	% of completion Actual to benchmark	EmployeesLeft in year	Seniority of employees that Left	% of completi Actual to benchma
Customer Success	BI developer	36	1	21.54	59.83%	1	23.56	65.45%	9	22.64	6
	Data analyst	28	3	13.47	48.11%	6	17.75	63.38%	5	20.06	7
	Helpdesk/Support specialist	24	4	16.24	67.68%	10	17.02	70.9%	22	15.35	6

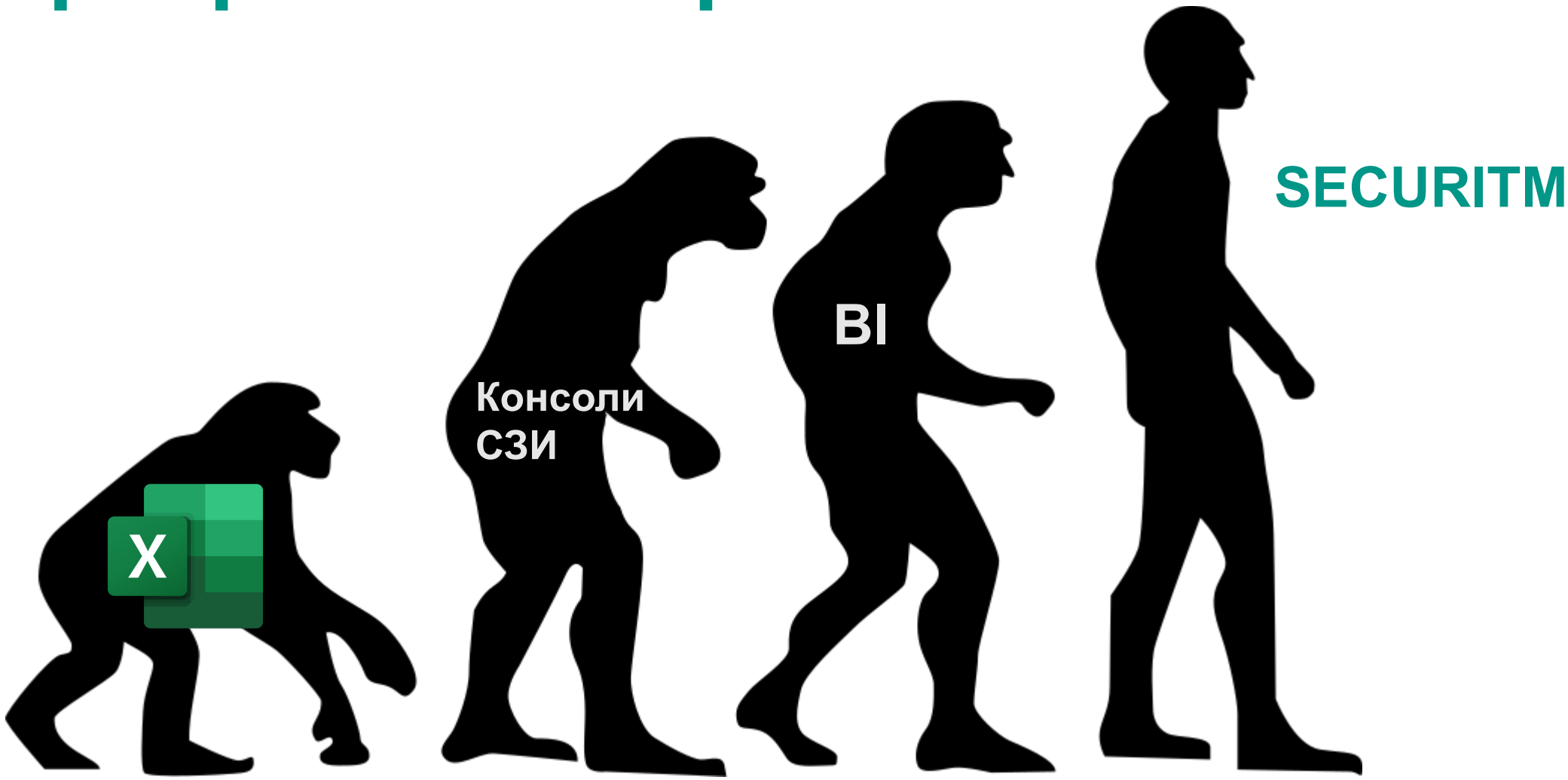
Сбор и расчет метрик

SECURITM

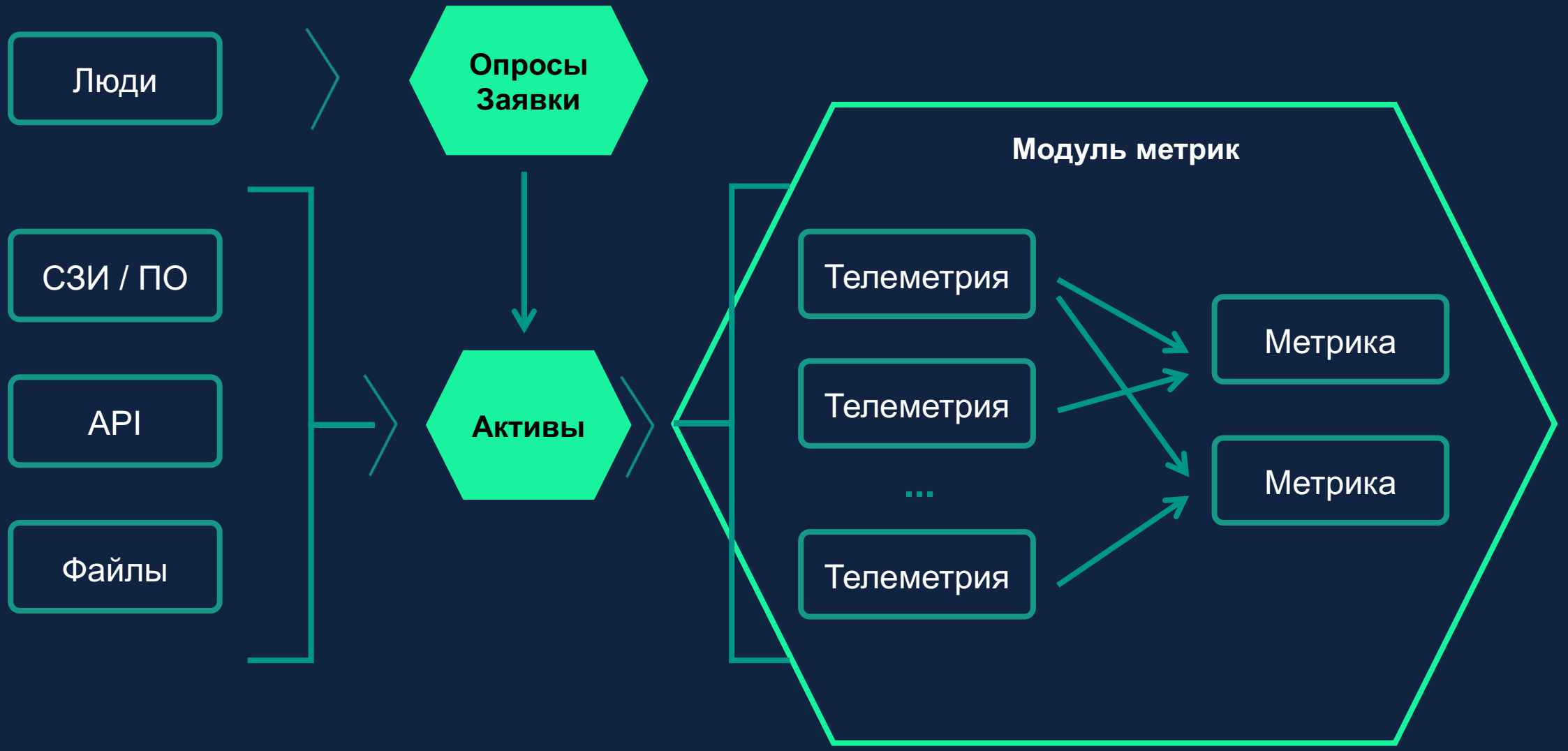
- Автоматический или ручной сбор
- Орг. и тех. метрики в 1 месте
- Влияние метрик на процессы



Сбор и расчет метрик



Сбор метрик


Люди
СЗИ / ПО
API
Файлы
Опросы
Заявки
Активы
Модуль метрик
Телеметрия
Телеметрия
...
Телеметрия
Метрика
Метрика

Метрики из Compliance

Russian Unified Cyber Security Framework (на основе The 18 CIS CSC)

Framework

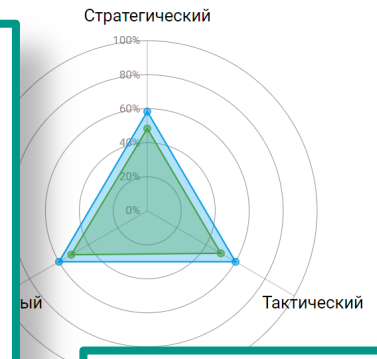
Уровень соответствия: 52 %

52% (79) | 48% (74)

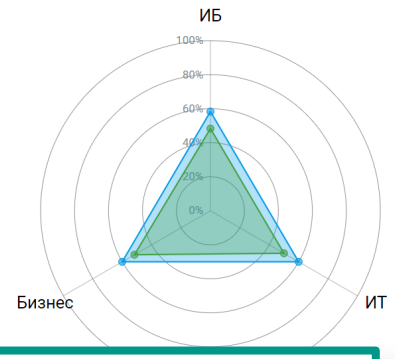
Классификация

Планируемый уровень | Текущий уровень

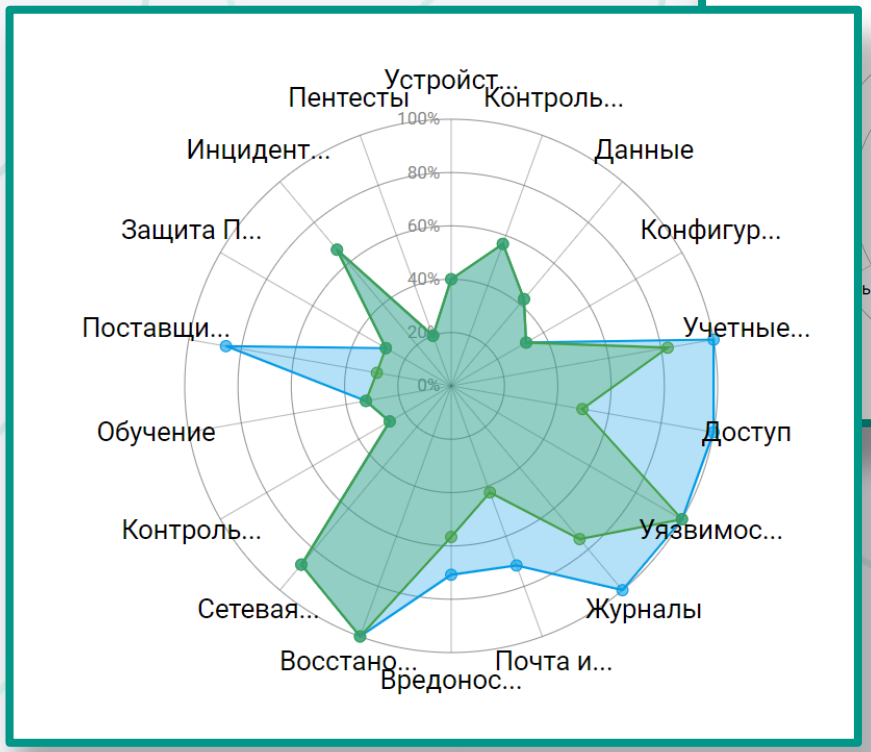
Управляемость КБ

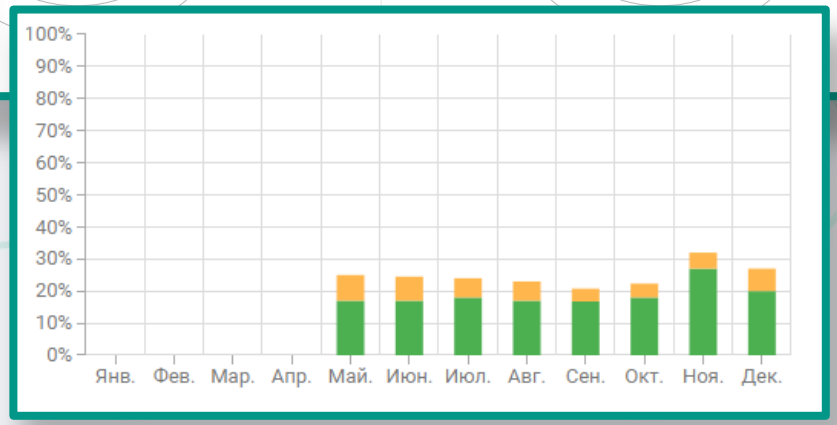


Партнерство КБ с функциями

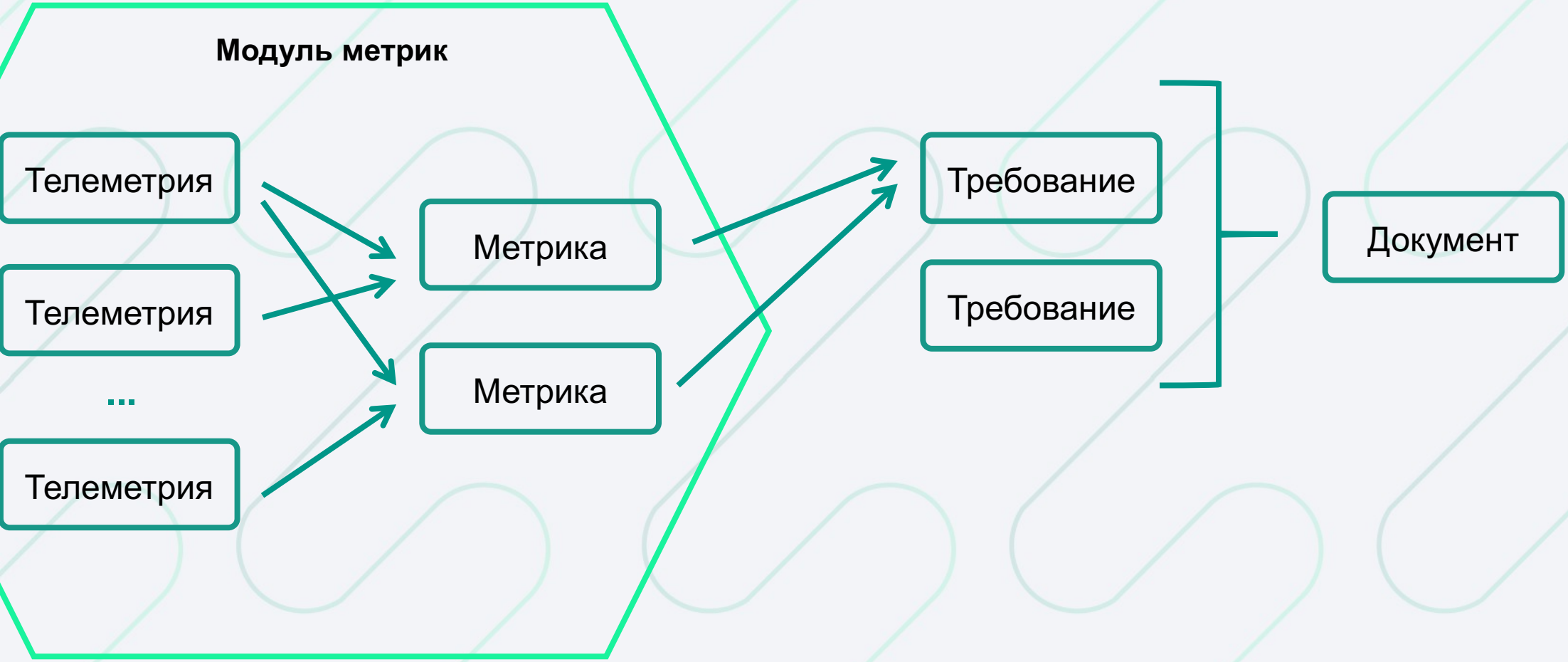


Киберустойчивость компании





Compliance через Метрики



Приказ ФСТЭК России № 21 от 18.02.2013

Состав и содержание мер по обеспечению безопасности персональных данных, необходимых для обеспечения каждого из уровней защищенности персональных данных

АВЗ.1

Уровень соответствия: 0 %

100% (1)

1
АКТУАЛЬНЫХ ТРЕБОВАНИЙ

0
ЗАЩИТНЫХ МЕР

Актуальные требования

Требований всего	1
Выполнено полностью	0
Выполнено частично	1
Не выполнено	0

Подробная статистика

Покрытие антивирусом АРМ

40 % 1 12

Установленные АВЗ обновлены

84 % 1 8

Список требований

VI. Антивирусная защита (АВЗ) 0% (0 из 1)

АВЗ.1 Реализация антивирусной защиты 50% (1 / 2)

Обоснование статуса отсутствует

Обязательно для уровня защищенности УЗ1 УЗ2 УЗ3 УЗ4

Benchmark

Бенчмаркинг нужен для определения эффективности использования средств защиты для бизнес-потребностей компании, а также помогает развивать взаимодействие ИБ-структуры с другими отделами.

Бенчмаркинг фокусируется на **эффективности**

Сравнение своих активов:

- **Дочерних структур**
- **Информационных систем**
- **Подрядчиков**

Сравнение себя с внешним миром:

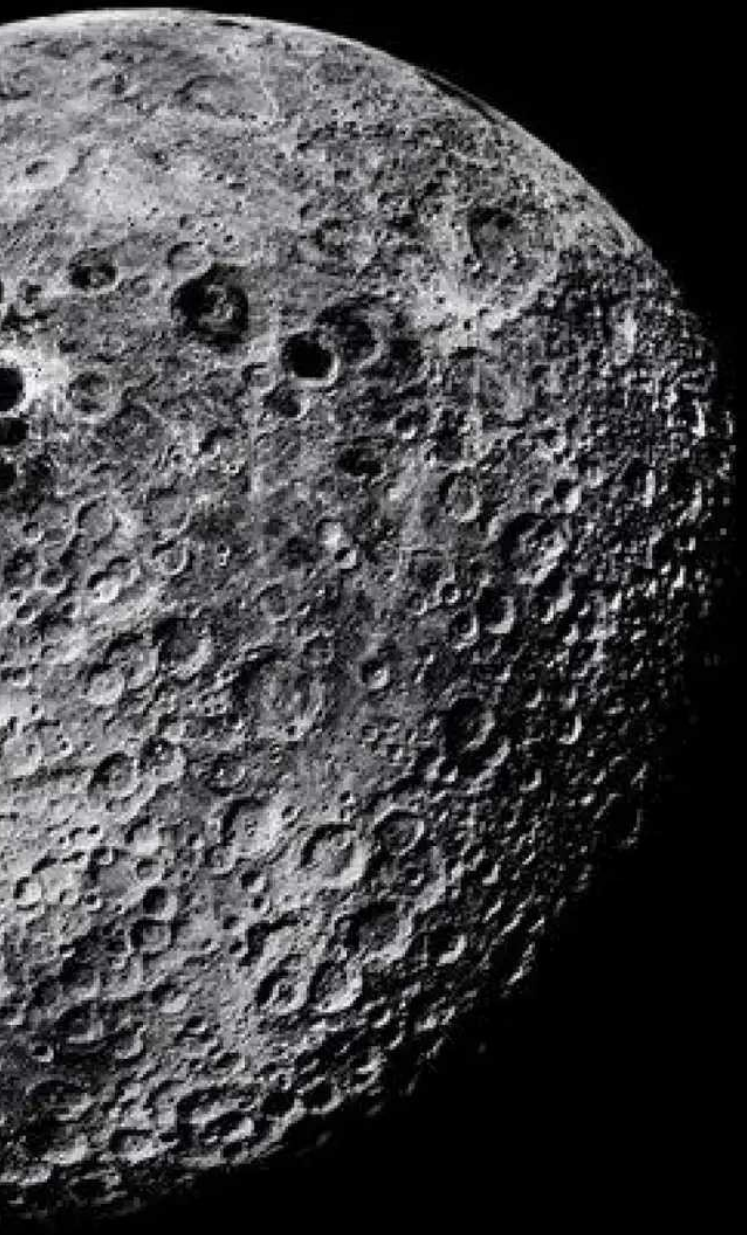
- **с средним уровнем по рынку**
- **с конкретными компаниями**

Реагирование

Что дальше?

Считать метрики вручную
от случая к случаю когда заставят

Строить метрико-центричную ИБ
и использовать их во всех процессах



- Не все можно собрать автоматически
- У каждой инфраструктуры свои метрики
- Высокие трудозатраты

t.me/SECURITM

Николай Казанцев
nk@securitm.ru
securitm.ru