# Метрики
# как ключевой инструмент управления ИБ

Николай Казанцев

SECURITM

# Николай Казанцев

## Образование

Специалитет и аспирантура на кафедре комплексного обеспечения информационной безопасности
ГУМ РФ им. Адм. Макарова

## Опыт работы

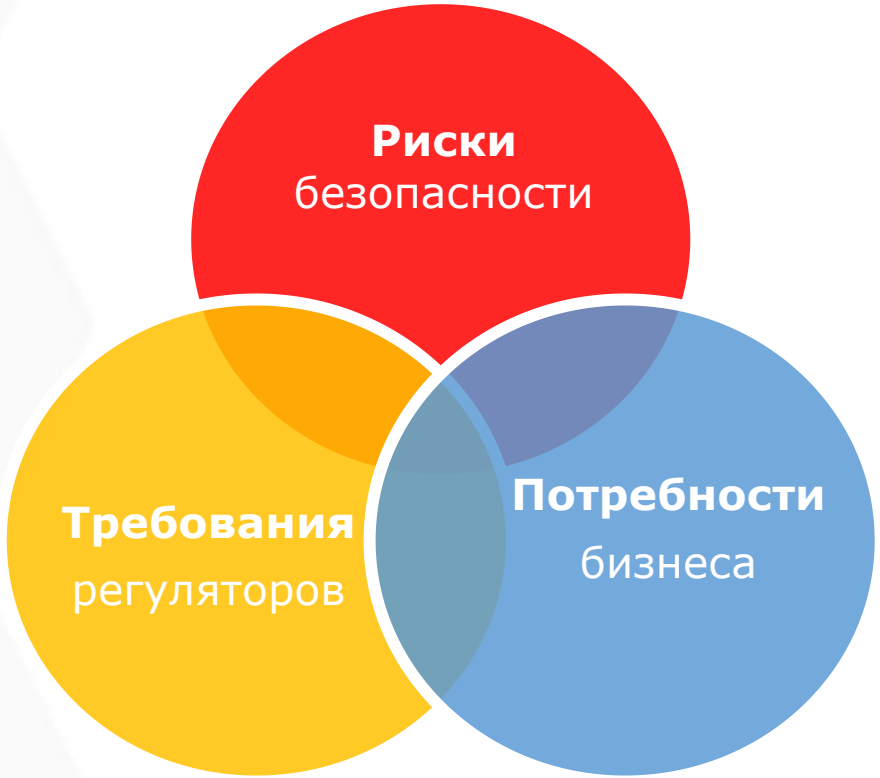
В ИБ с 2010, работал в Лаборатории противодействия промышленному шпионажу, Администрации Санкт-Петербурга,  начальником отдела ИБ в фарм-компании ПОЛИСАН, сейчас - CEO SECURITM SGRC

## Сертификаты

EC Council CEH, Comptia Security+,
Медаль ФСТЭК за укрепление государственной системы защиты информации

SECURITM

# Цели ИБ




**СНИЖАТЬ РИСКИ**
информационной безопасности

**ИСПОЛНЯТЬ ТРЕБОВАНИЯ**
регуляторов и стандартов

**ЗАКРЫВАТЬ ПОТРЕБНОСТИ**
заинтересованных сторон

**Метрики ИБ**

SECURITM

# О чем?

Метрика - численный показатель качества, эффективности процесса

Чаще всего метрика выражается в **%** / **Цифре** / **Да-Нет**

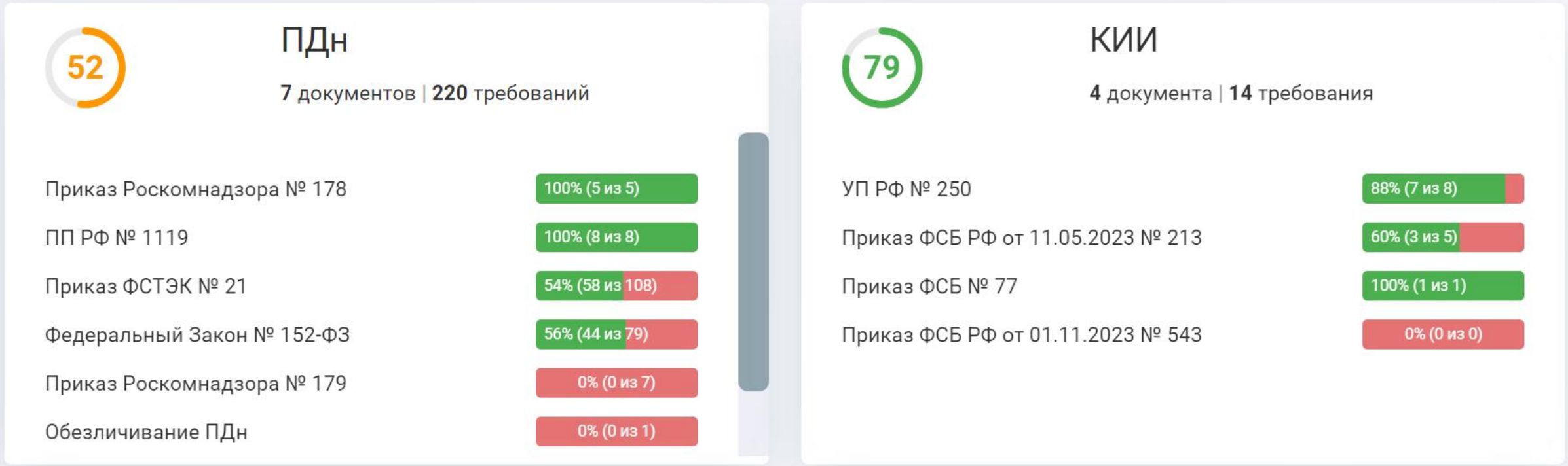
У метрики всегда должна быть **цель**

- Сейчас хорошо ?
- Стало ли лучше ?
- Работает ли процесс ?

SECURITM

# Метрики Комплаенса

## % соответствия требованиям ОРД




SECURITM

# Метрики Комплаенса

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

Framework

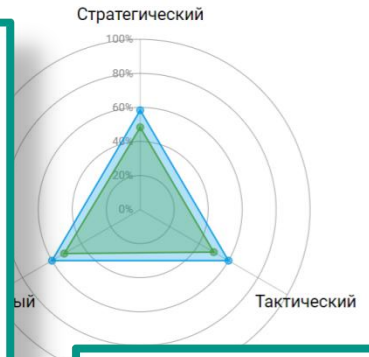
**Уровень соответствия: 52 %**

52% (79) | 48% (74)

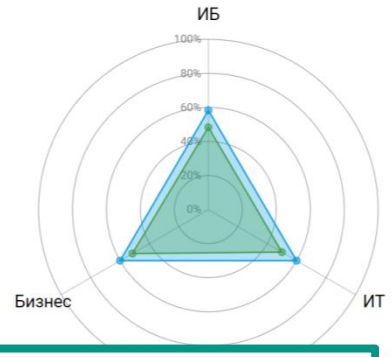
Классификация

Планируемый уровень  Текущий уровень

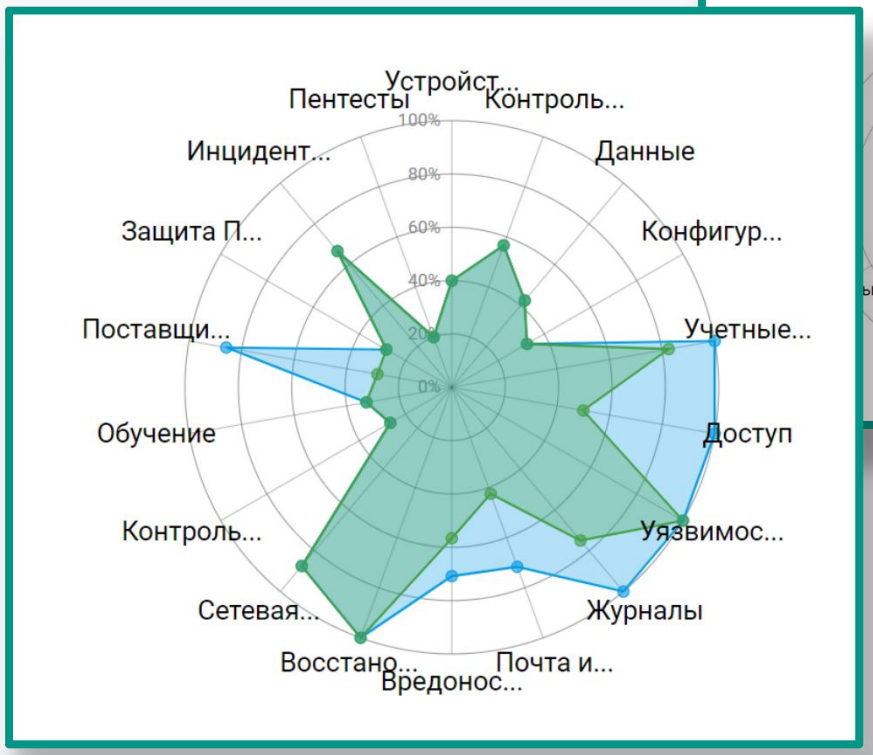
Управляемость КБ

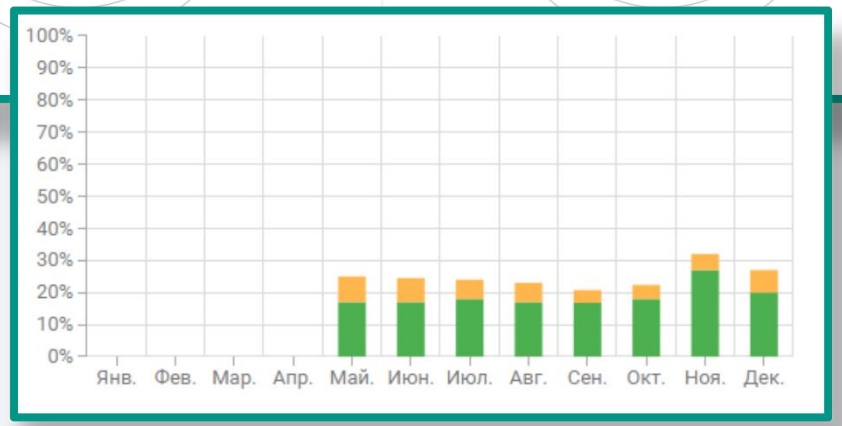



Партнерство КБ с функциями




Киберустойчивость компании


SECURITM

# Метрики Комплаенса

Оценка реализации ГОСТ 57580

Область: Выберите область | Нарушения (Б) | Формы В.1-8 и В.9: Оценка соответствия (В.1-8) Жизненный цикл (В.9) | Формы В.10-13: Обоснование полноты реализации Оценка полноты реализации | Итоговая оценка

/ Соответствие требованиям / Оценка реализации ГОСТ 57580 — Экспорт данных | Группы документов | Все документы

| Наименование процесса системы ЗИ, направления ЗИ | Оценка технических мер ЗИ | Оценки за направления | | | | Качественная оценка уровня соответствия (ЗИ) | Уровень соответствия (ЗИ) | Итоговая оценка |
|---|---|---|---|---|---|---|---|---|
| | | 8.2 Планирование | 8.3 Реализация | 8.4 Контроль | 8.5 Совершенствование | | | |
| 7.2 Процесс 1 "Обеспечение защиты информации при управлении доступом" | 0.84 | 0.5 | 0.9 | 0.91 | 0.88 | 0.83 | Третий | |
| 7.3 Процесс 2 "Обеспечение защиты вычислительных сетей" | 0.61 | 0.5 | 0.71 | 0.86 | 0.88 | 0.67 | Второй | |
| 7.4 Процесс 3 "Контроль целостности и защищенности информационной инфраструктуры" | 0.83 | 0.5 | 0.71 | 0.92 | 0.88 | 0.79 | Третий | |
| 7.5 Процесс 4 "Защита от вредоносного кода" | 0.92 | 0.5 | 0.75 | 1 | 0.88 | 0.85 | Третий | |
| 7.6 Процесс 5 "Предотвращение утечек информации" | 0.39 | 0.5 | 0.71 | 0.86 | 0.88 | 0.56 | Второй | |
| 7.7 Процесс 6 "Управление инцидентами защиты информации" | 0.95 | 0.5 | 0.75 | 0.95 | 0.88 | 0.86 | Четвертый | |
| 7.8 Процесс 7 "Защита среды виртуализации" | 0.76 | 0.5 | 0.75 | 1 | 0.88 | 0.77 | Третий | |
| 7.9 Процесс 8 "Защита информации при осуществлении удаленного логического доступа с использованием мобильных (переносных) устройств" | 0.67 | 0.5 | 0.63 | 0.92 | 0.88 | 0.69 | Второй | |
| Применение организационных и технических мер ЗИ на этапах жизненного цикла АС | | | | | | | | 0.84 |
| Итоговая оценка соответствия ЗИ с учетом выявленных нарушений ЗИ | | | | | | | | |
| Количество нарушений ЗИ, выявленных в результате оценки соответствий ЗИ | | | | | | | | 0 |
| | | | | | | | Итоговая оценка соответствия ЗИ (R) | 0.76 |

12-МР для 802-П

Расчет оценки выполнения технологических мер защиты информации, предусмотренных требованиями Положения Банка России № 802-П

Технологические меры

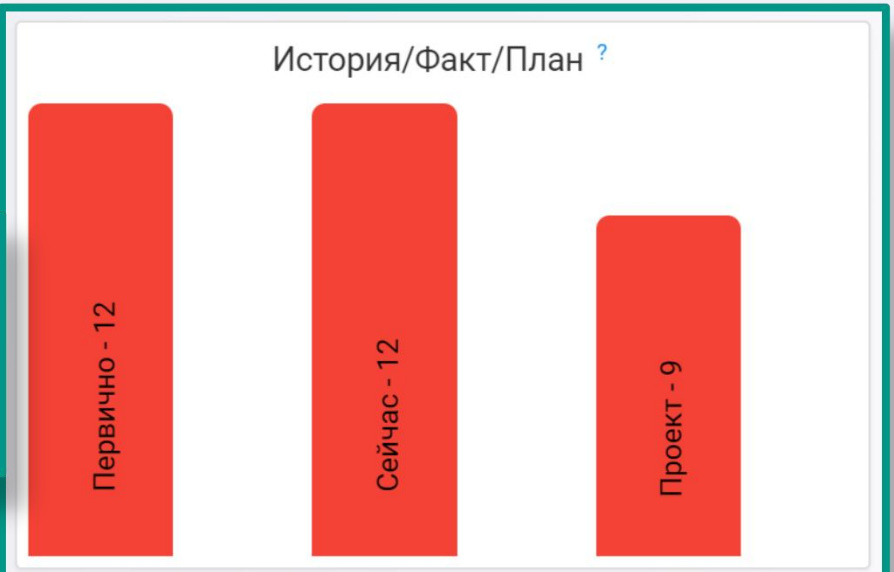
ETM 0.45

| Планирование | Реализация | Контроль | Совершенствование |
|---|---|---|---|
| ETMП 1 | ETMP 0.625 | ETMK 0 | ETMC 0 |

SECURITM

# Метрики Рисков

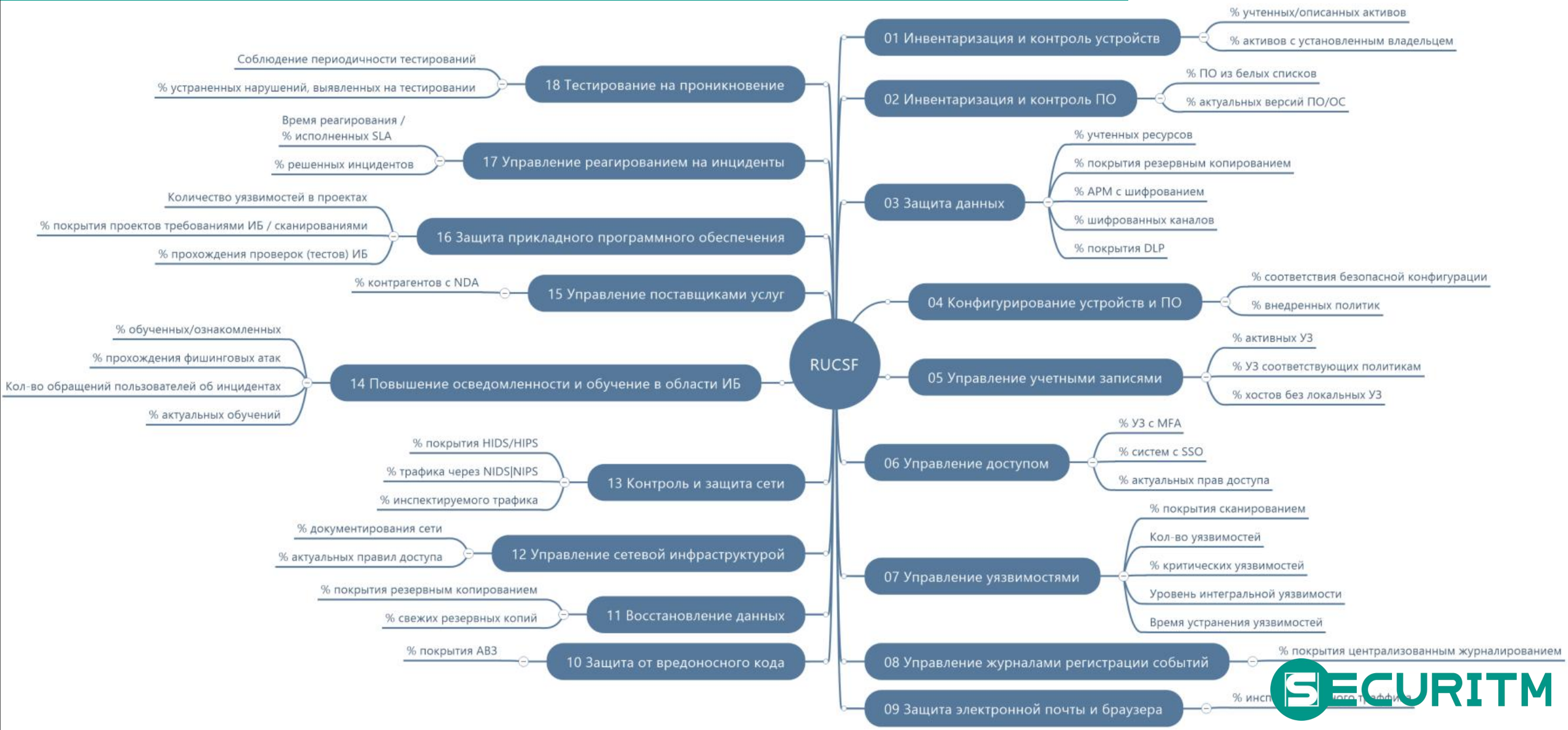

- Совокупная величина риска
- Количество рисков выше риск-аппетита
- Регулярность идентификации рисков



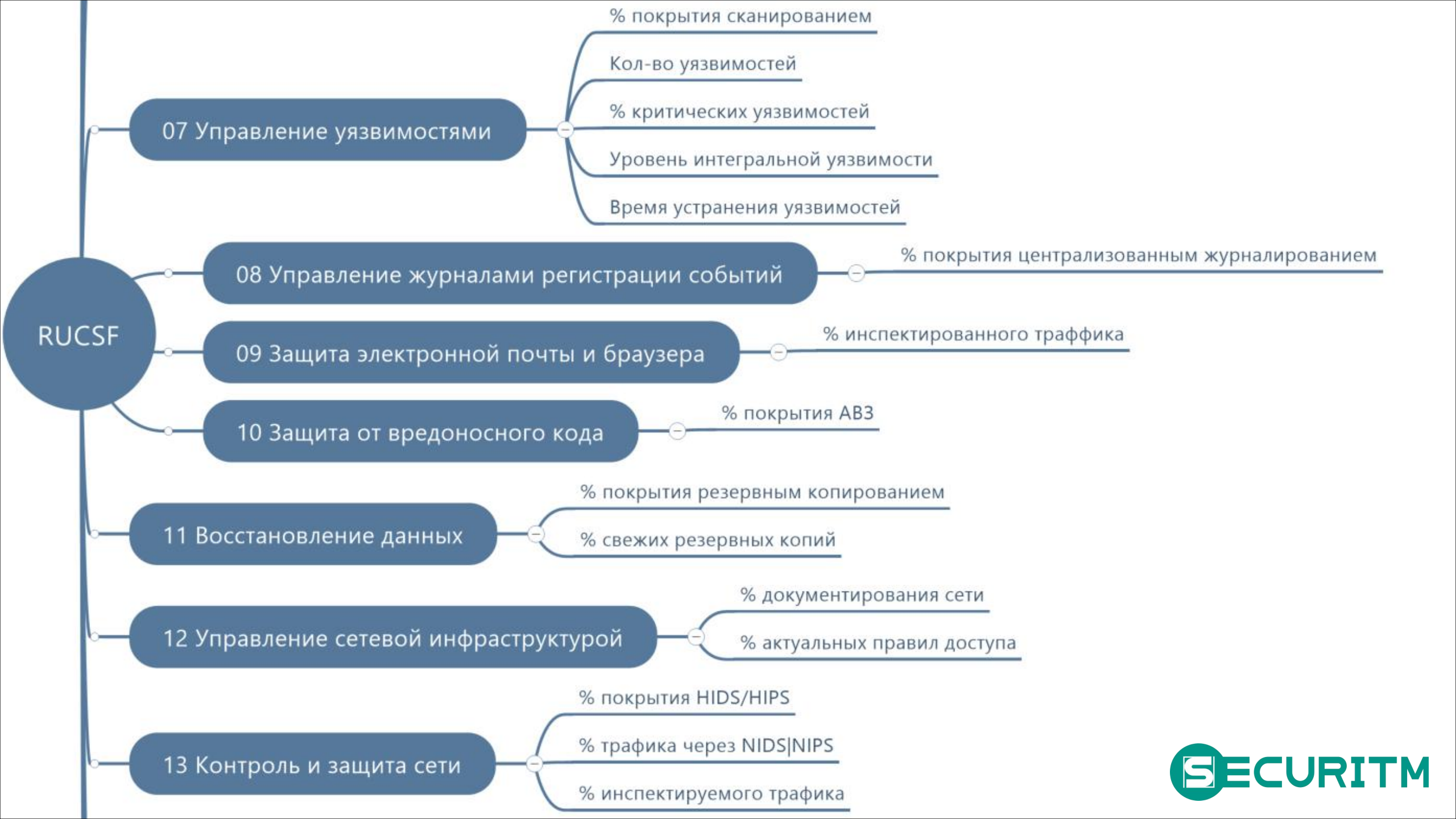
SECURITM

# Метрики по всем доменам ИБ




SECURITM


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

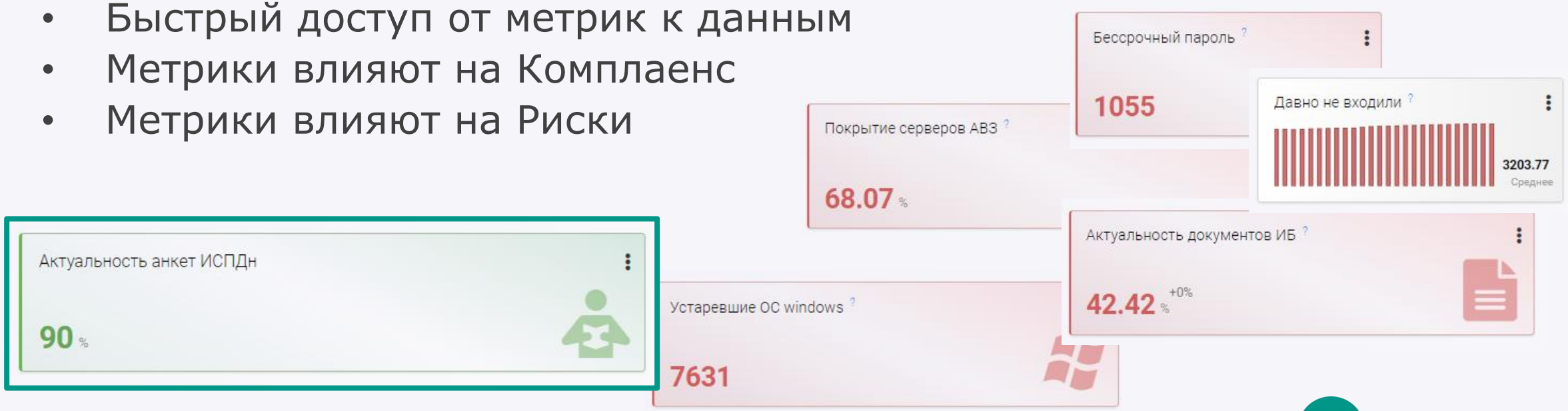

RUCSF
07 Управление уязвимостями
% покрытия сканированием
Кол-во уязвимостей
% критических уязвимостей
Уровень интегральной уязвимости
Время устранения уязвимостей
08 Управление журналами регистрации событий
% покрытия централизованным журналированием
09 Защита электронной почты и браузера
% инспектированного 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


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

SECURITM

# Рекомендации

- Быстрый и повторяемый доступ к данным
- Минимум 1 метрика для каждого направления
- За цифрой должен стоять смысл
- Используйте метрики максимально:
  - Быстрый доступ от метрик к данным
  - Метрики влияют на Комплаенс
  - Метрики влияют на Риски




SECURITM

Спасибо за внимание

SECURITM

Николай Казанцев