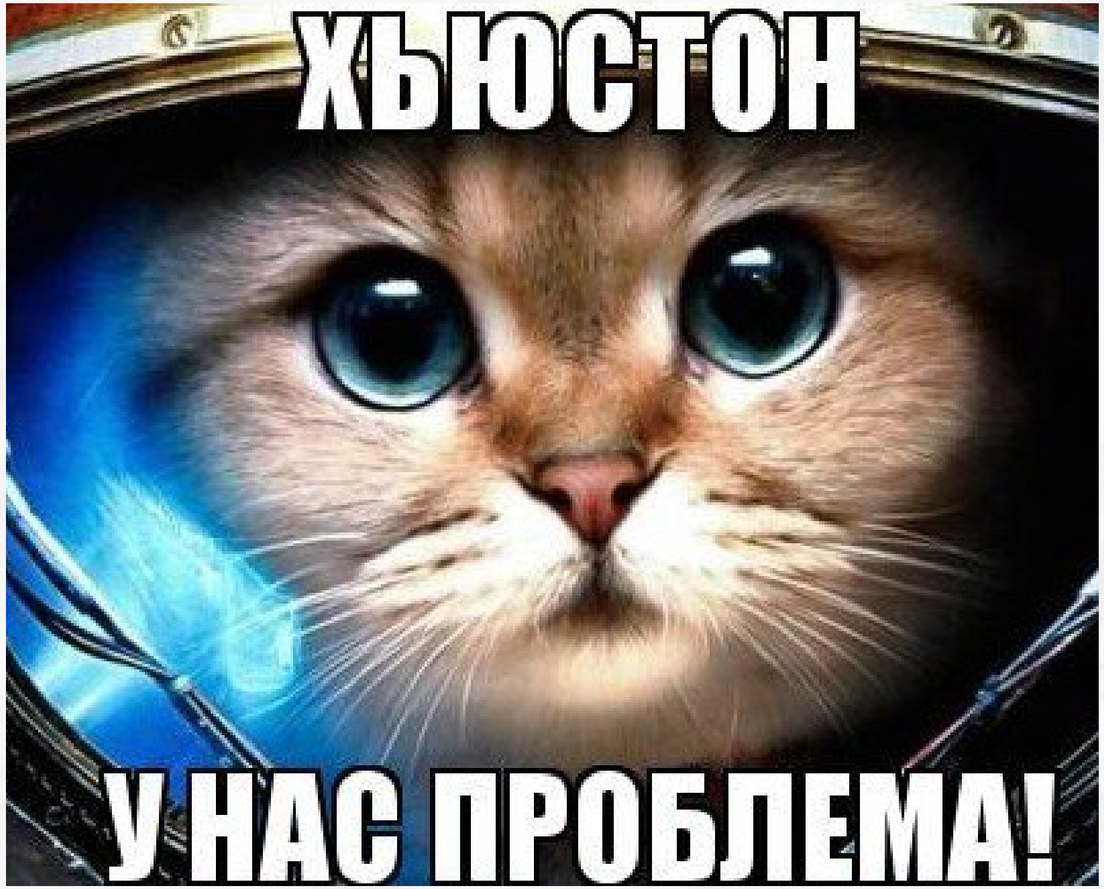
Антон Тростянко

Начальник департамента информационной безопасности и центра кибербезопасности hoster.by

Кибербезопасность. Опыт практиков.

Проблематика.
Центры кибербезопасности как решение.
Требования и проблемы в их реализации.
Пример реализации.
Как обеспечивать защиту объектов.

Проблематика



В рамках законодательства в сфере информационной безопасности и защиты персональных данных предъявляются требования к защите информации ограниченного распространения, что приводит к тому, что, как правило, не уделяется должное внимание объектам информационной инфраструктуры, на которых обрабатывается общедоступная информация.

Такие объекты для злоумышленников становятся «лакомым кусочком» и являются точкой входа в инфраструктуру, или определенным плацдармом для совершения неправомерных действий.

Решение

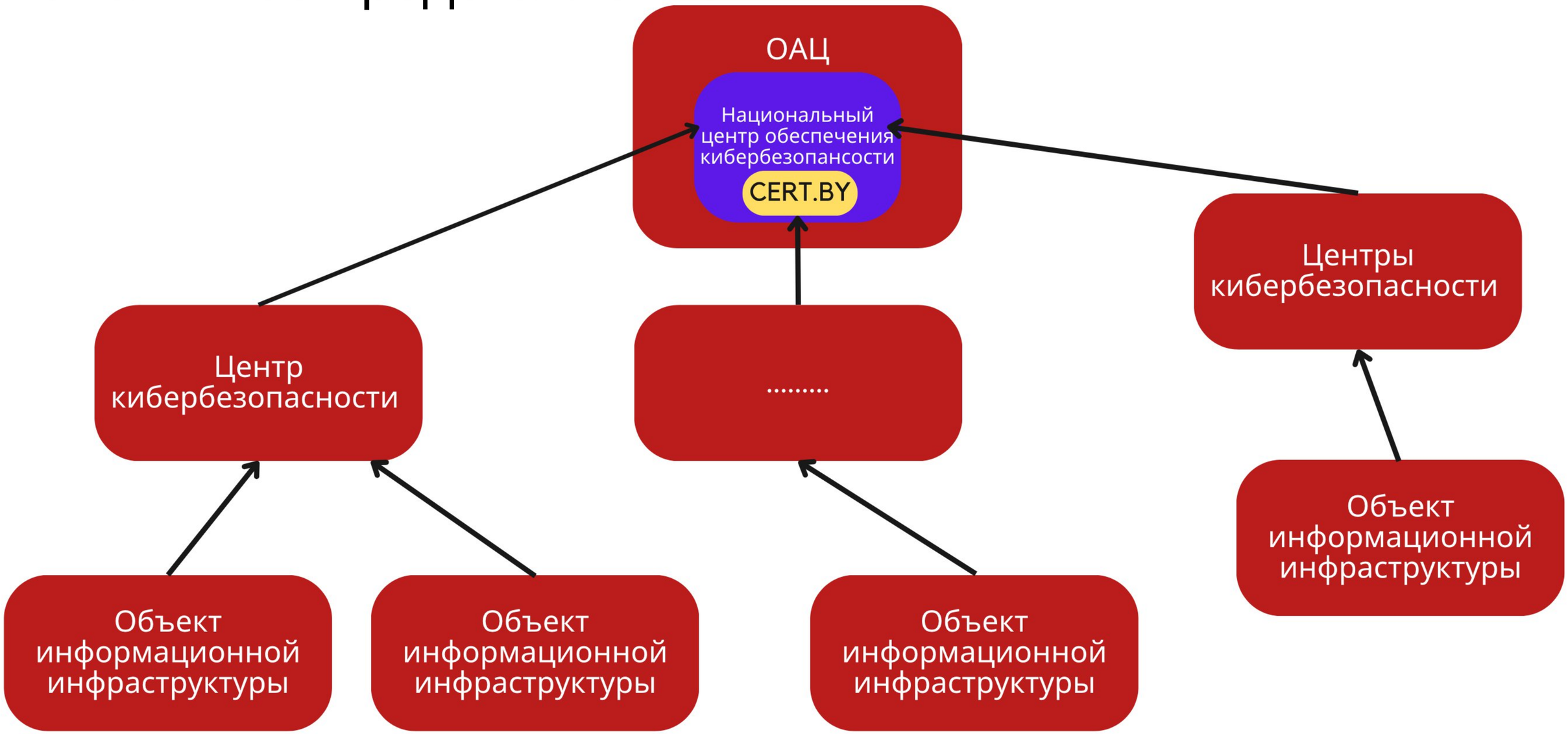
Решением стало принятие законодательства о кибербезопасности, в рамках которого стало понятно, что это такое, чем будет достигаться и кому придется его выполнять вне зависимости от желания.

Так появилась Национальная систему обеспечения кибербезопасности, а вместе с ней Национальный центр обеспечения кибербезопасности и реагирования на киберинциденты, и сами центры обеспечения кибербезопасности и реагирования на киберинциденты.

Кроме понятий появились и требования, предъявляемые к объектам, которые необходимо защищать, и тем, кто такую защиту будет обеспечивать.

Решение

Схематичное представление

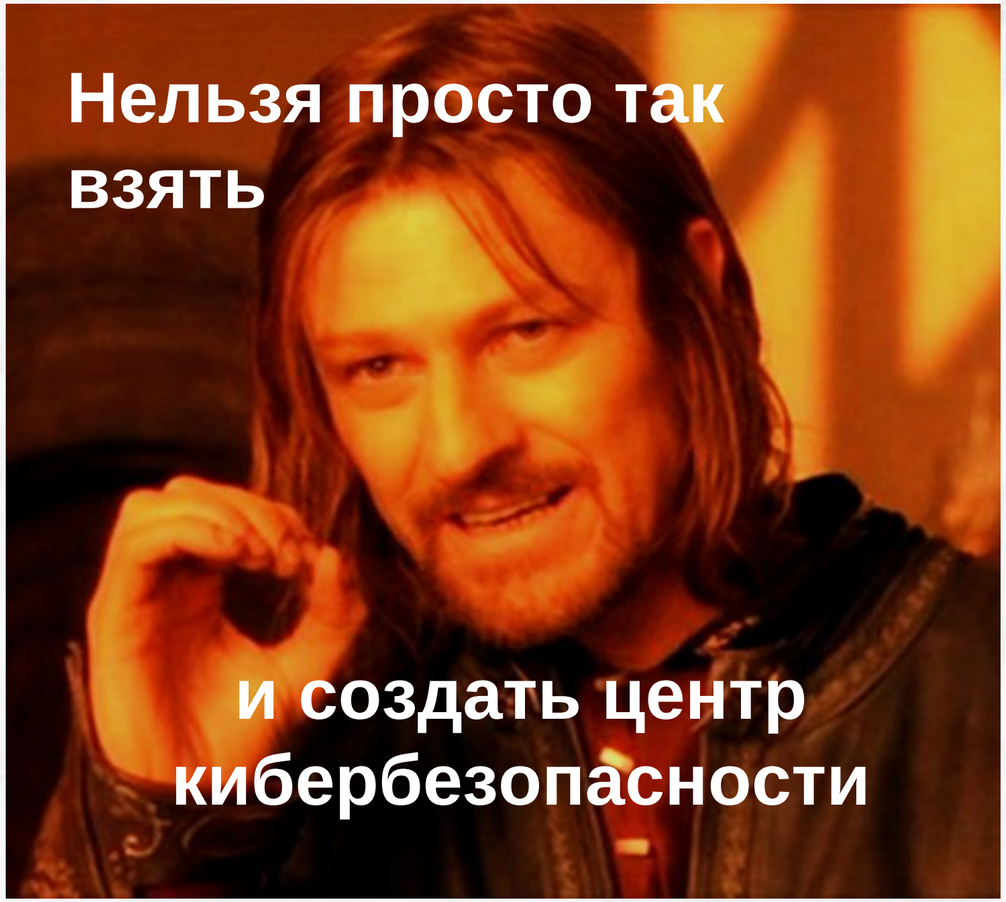


Решение
Центры кибербезопасности

Центры кибербезопасности призваны обеспечить кибербезопасность объектов информационной инфраструктуры, в том числе реализовать мероприятия по выявлению, предупреждению и исследованию кибератак и вызванных ими киберинцидентов, реагировать на такие киберинциденты.

Для ряда организаций требования по построению Центра кибербезопасности стали обязательными. Таким компаниям предоставлен 1 год для проектирования, создания и аттестации Центра кибербезопасности.

Требования



В рамках создания Центра кибербезопасности необходимо реализовать следующие требования:

- соответствовать типовой структуре Центра кибербезопасности;
- иметь на праве собственности необходимые для обеспечения кибербезопасности программные и аппаратные средства;
- иметь аттестованную систему защиты информации Центра кибербезопасности;
- иметь выстроенные бизнес-процессы.

Требования

Типовая структура

Для подтверждения объективной возможности центра кибербезопасности оказывать соответствующие услуги при прохождении аттестации в нем должны быть созданы подразделения следующей численностью:

Структурное подразделение, выполняющие функции по обработке информации, - **не менее шести штатных единиц**, включая руководителя (полная занятость);

Структурное подразделение, выполняющее функции по администрированию, - **не менее двух штатных единиц**, включая руководителя (полная занятость);

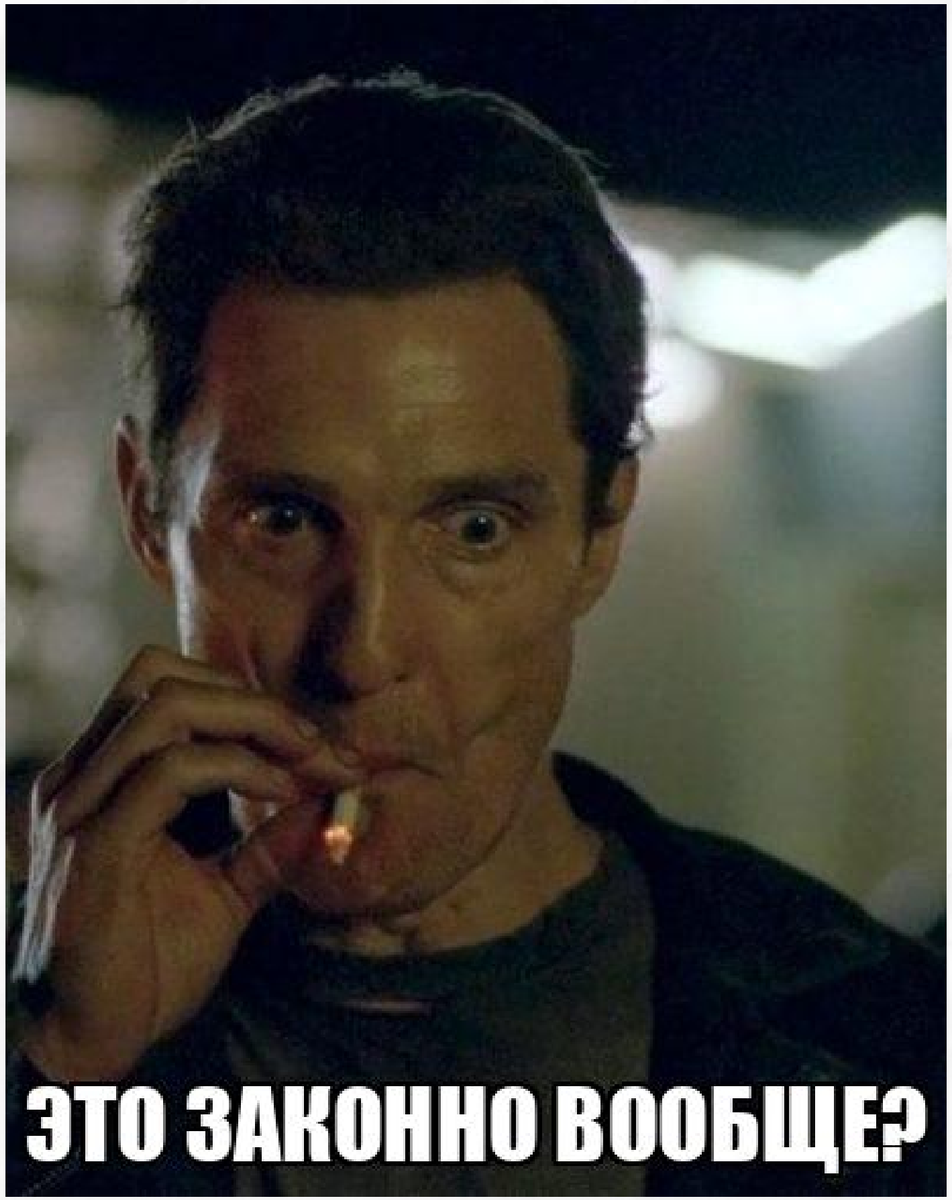
Структурное подразделение, выполняющие функции команды реагирования на киберинциденты, а также функции по администрированию технических, программно-аппаратных и программных средств, в том числе средств защиты информации, - **не менее двух штатных единиц**, включая руководителя (полная занятость);

Структурное подразделение или лицо, ответственное за обеспечение кибербезопасности, - не менее одной штатной единицы (полная занятость).

Требования

Типовая структура. Проблемы

- Формирование отдельных структурных подразделений
- Поиск подходящих кандидатов
- Конкурентная заработная плата
- Проведение обучения



Требования

Средства.

- TIP (обязательно)
- IRP
- SIEM
- Средство анализа защищенности
- Sandbox
- Иные средства защиты

Требования

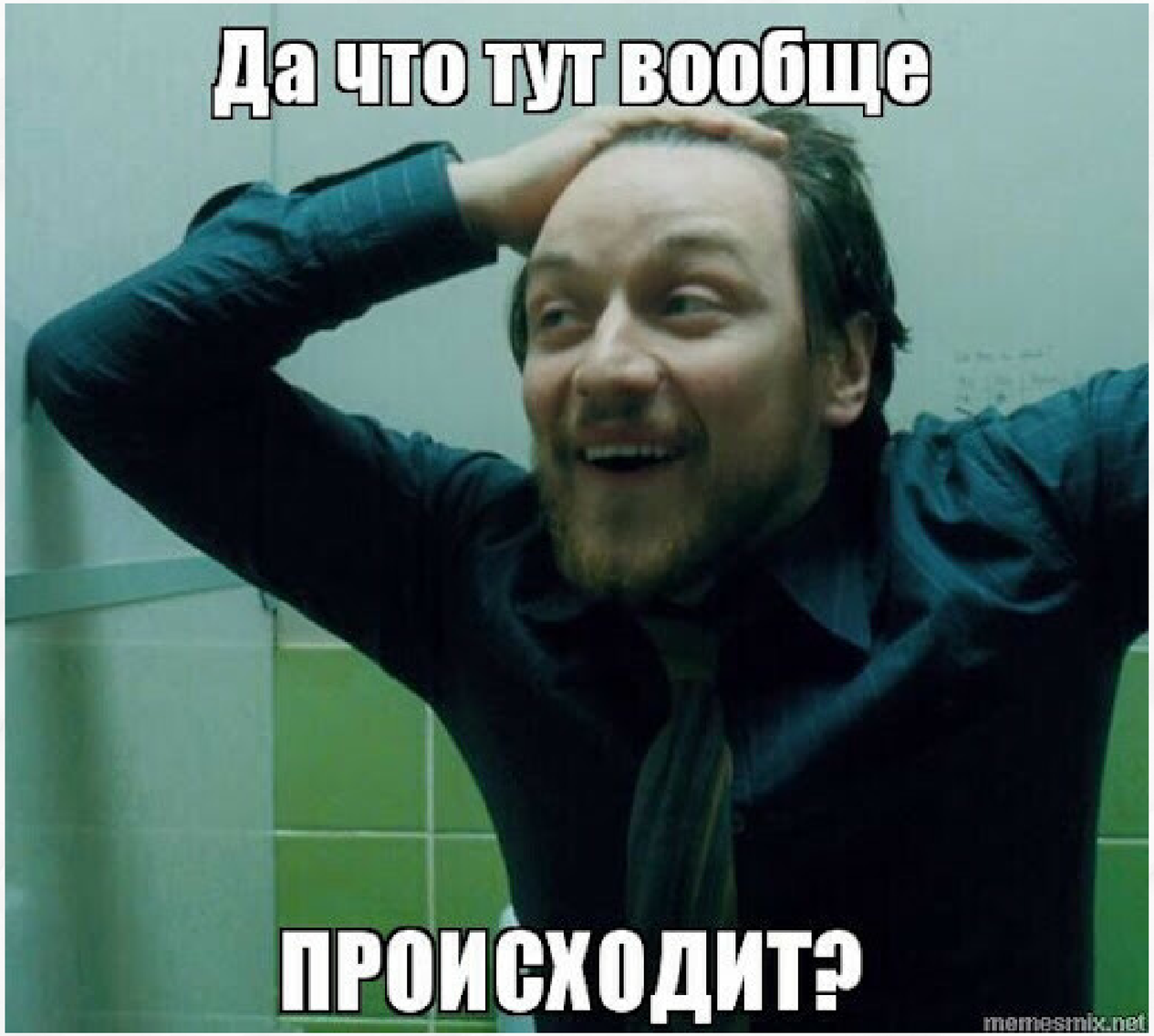
Средства. Проблемы

- Стоимость
- Интеграция
- Обучения персонала
- Вычислительные мощности
- Разработка документации

Требования

Выстроенные процессы.

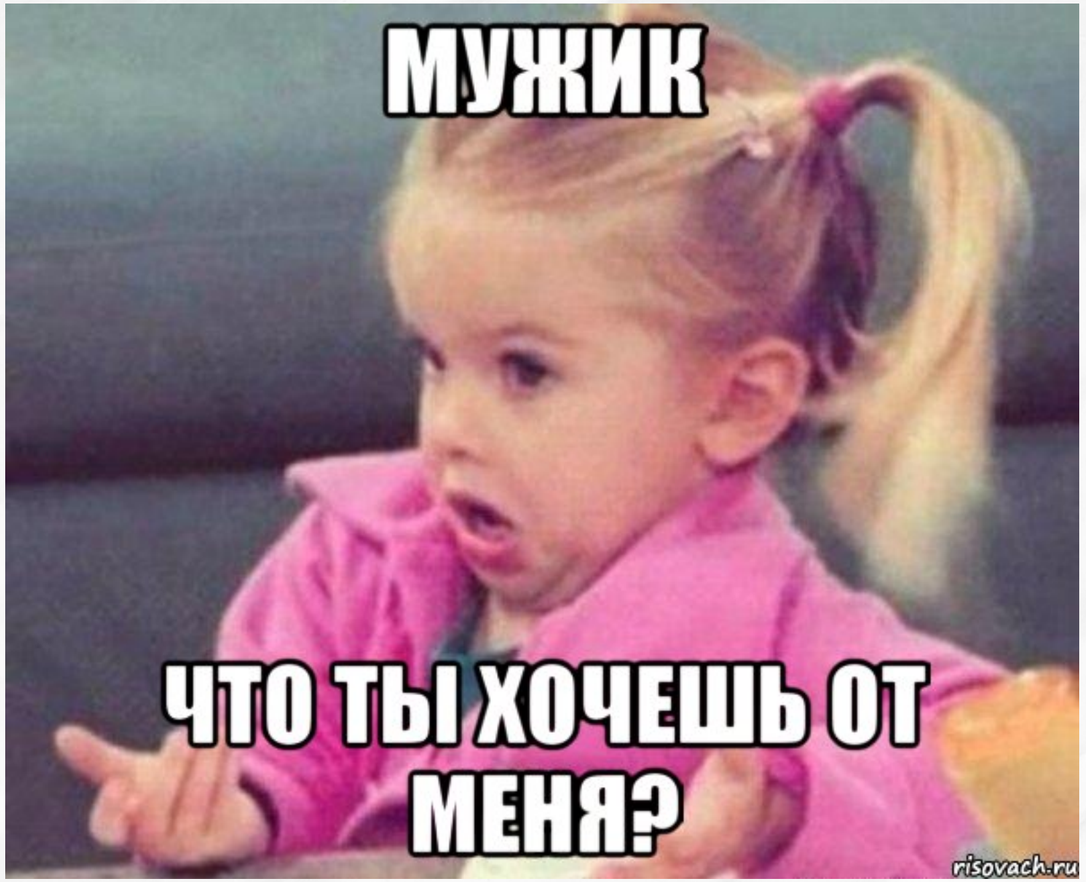
- Детектирование
  - ошибки первого и второго рода
  - менеджмент
- Оповещение
  - Каналы связи
  - Способы оповещения
- Реагирование
  - Наличие playbooks
  - Формирование группы
  - План мероприятий
  - Очередность реагирования
- Анализ



Требования

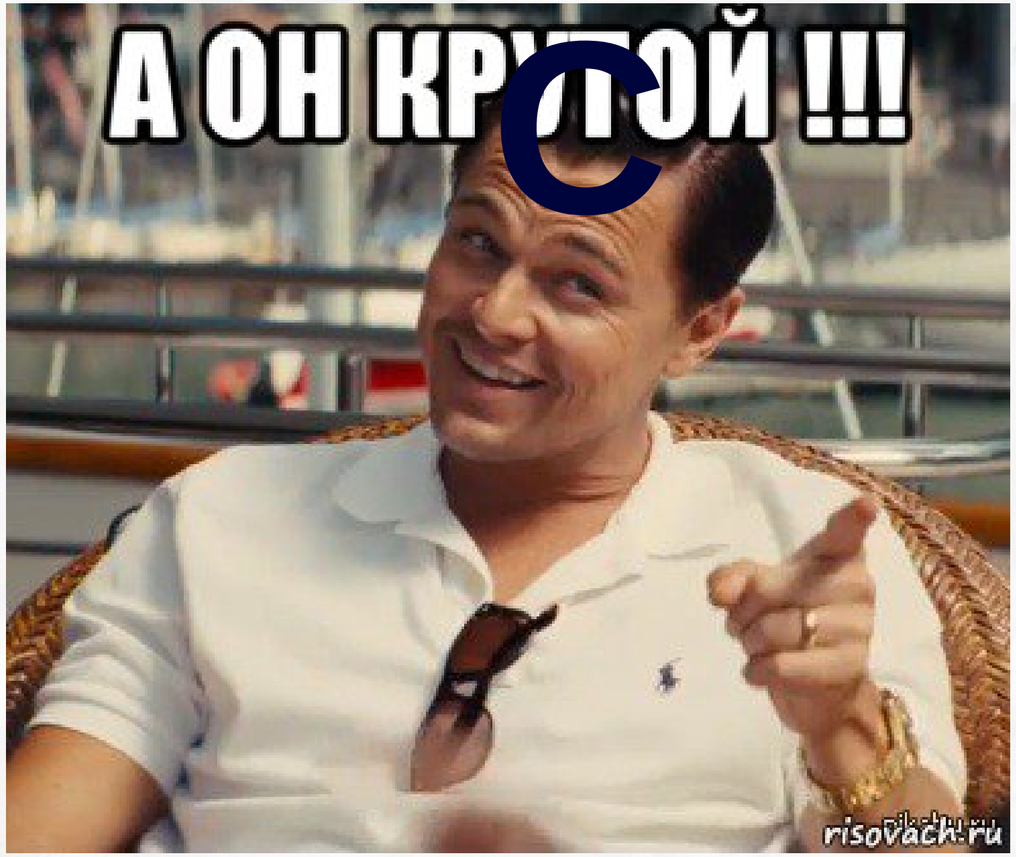
Выстроенные процессы.
Проблемы.

- Отсутствие компетенций
- Отсутствие опыта
- Средства автоматизации
- Непонимание со стороны коллег



Центр кибербезопасности hoster.by

- 19 человек
- Стек решений с открытым исходным кодом
- Ежедневно порядка 700 инцидентов
- Ежедневно порядка 5-7 инцидентов, требующих вмешательства группы реагирования
- 35+ playbooks



Центр кибербезопасности hoster.by

Структура.

- Руководитель ЦК (1)
- Специалист по кибербезопасности (1)
- Отдел обработки информации (24x7) (6)
- Отдел реагирования (5)
- Группа администрирования (2)
- Группа анализа защищенности (2)
- Группа анализа ВПО и форензики (2)

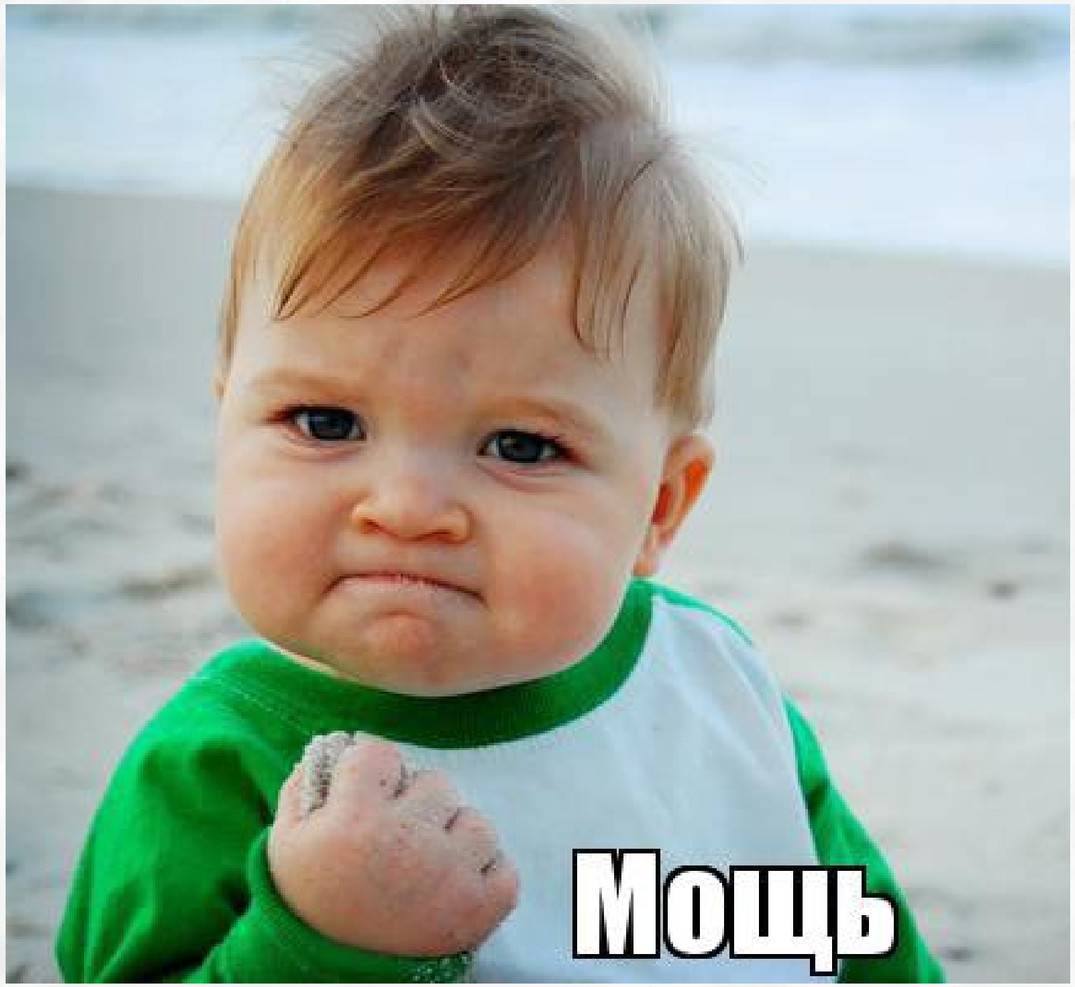
Центр кибербезопасности hoster.by

Стек решений.

Центр кибербезопасности hoster.by

Объем работ.

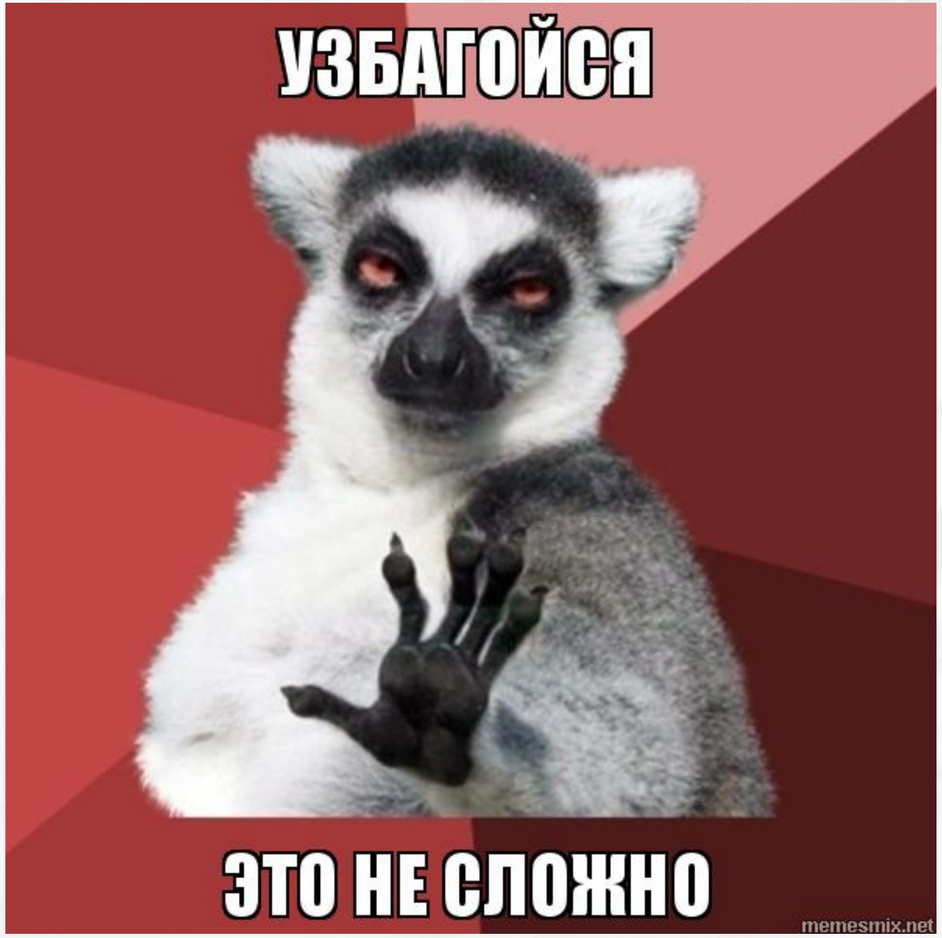
- Ежедневно порядка 700 инцидентов
- Ежедневно порядка 5-7 инцидентов, требующих вмешательства группы реагирования
- 35+ playbooks
- Среднее время реагирования на низкоуровневые инциденты 6 минут



ВЫВОДЫ

SOC hoster.by самый вкусный и полезный

Выводы



- Персонал
- Средства
- Процессы

Спасибо за внимание!

Берегите себя и свои данные!

Подписывайтесь на каналы по защите данных

E-mail: anton.trostyanko@hoster.by
tel: +375-29-175-25-15