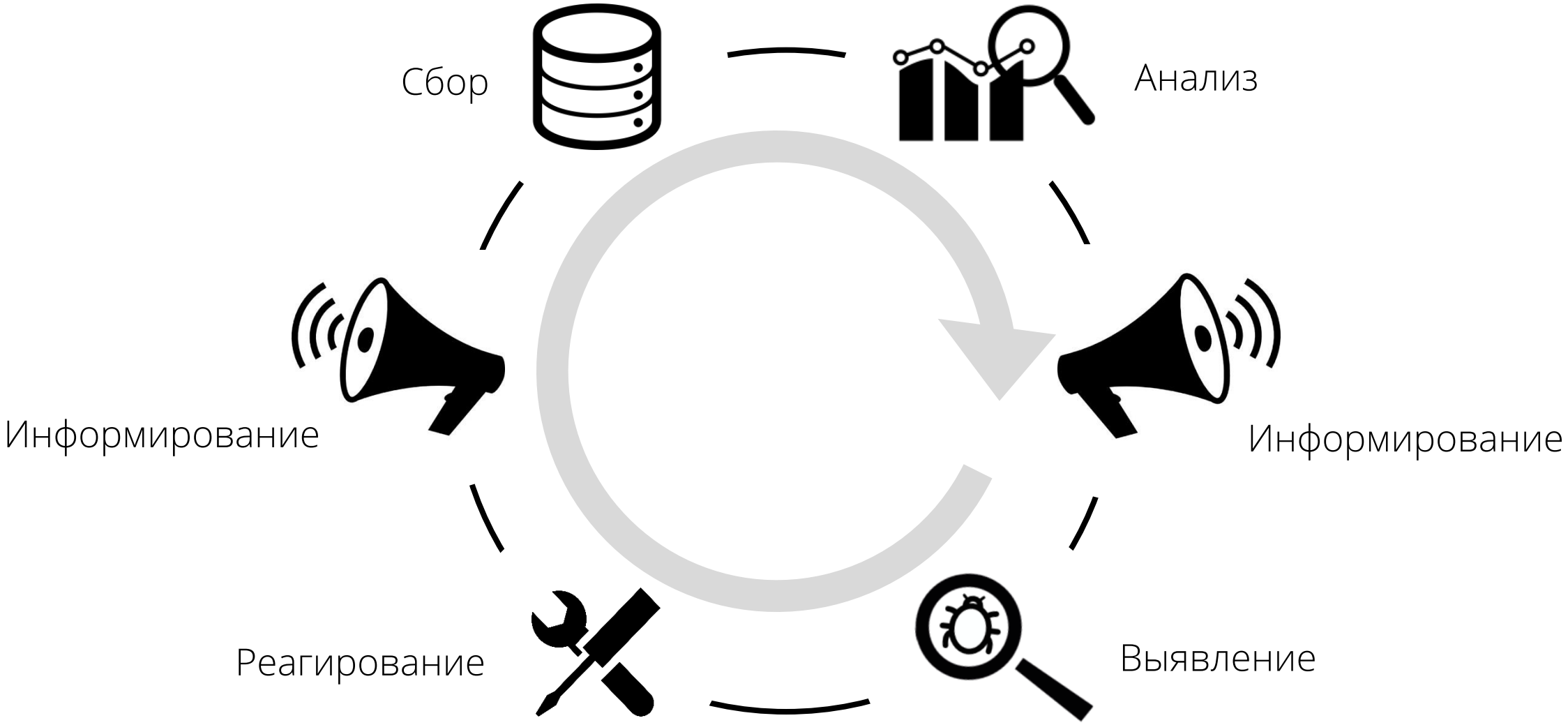
ГОССОПКА

Взаимодействие с НКЦКИ

Сергей Корелов, ФСБ России

ИНФОРМАЦИОННОЕ ВЗАИМОДЕЙСТВИЕ В ГОССОПКА

ГОССОПКА



По телекоммуникационным каналам сети Интернет:

•через портал НКЦКИ
(личный кабинет субъекта ГосСОПКА)

•через техническую инфраструктуру НКЦКИ
(файлы в формате JSON)

Посредством электронной, почтовой, факсимильной и телефонной связи

НКЦКИ СОБИРАЕТ СВЕДЕНИЯ:

ГОССОПКА

об атаках и инцидентах

об объектах

о программном обеспечении

об угрозах

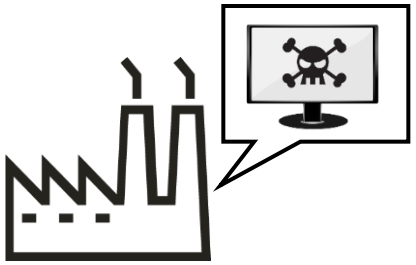
НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ
ЦЕНТР ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

ИНФОРМАЦИОННЫЕ СООБЩЕНИЯ (ПО КАТЕГОРИИ ЗНАЧИМОСТИ ИНФОРМАЦИИ)

ГОССОПКА

Оперативная информация:



об инцидентах на объектах КИИ

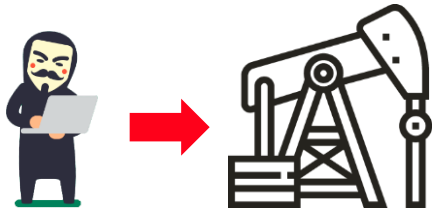
об инцидентах, требующих содействия специалистов НКЦКИ

об угрозах в отношении объектов КИИ

другая срочная информация

Текущая информация :

о выявленных компьютерных инцидентах, предпринятых мерах и результатах реагирования



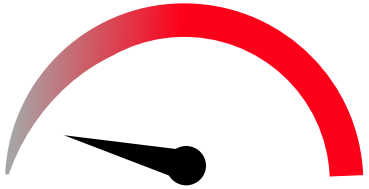
о выявленных попытках проведения атак в отношении объектов КИИ

уточняющие сведения о ресурсах и объектах КИИ

справочная, прогнозная и другая информация

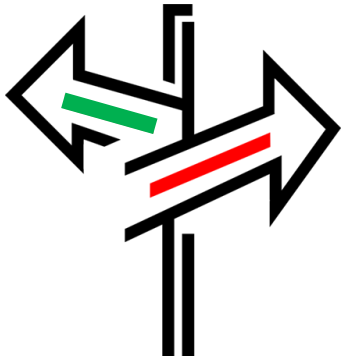
ТИПЫ КОМПЬЮТЕРНЫХ ИНЦИДЕНТОВ

ГОССОПКА



Нарушение или замедление работы информационного ресурса

Внедрение ВПО



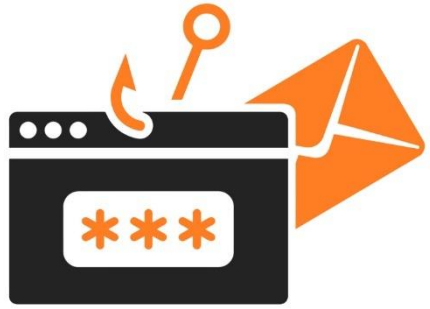
Нелегитимное изменение маршрутно-адресной информации в сети Интернет

Нелегитимное использование данных для авторизации в информационном ресурсе

ТИПЫ КОМПЬЮТЕРНЫХ ИНЦИДЕНТОВ

ГОССОПКА

Эксплуатации уязвимости информационного ресурса



Использование информационного ресурса для публикации мошеннического ресурса

Использование информационного ресурса в целях распространения ВПО или управления бот-сетью

Использования информационного ресурса в целях проведения компьютерных атак

ТИПЫ КОМПЬЮТЕРНЫХ ИНЦИДЕНТОВ

ГОССОПКА

Использование информационного ресурса
для публикации запрещенной информации

Нелегитимное изменение
содержимого информационного ресурса

Использование информационного ресурса
в целях распространения спама

ТИПЫ КОМПЬЮТЕРНЫХ АТАК

ГОССОПКА

«Отказ в обслуживании»

Загрузка модулей ВПО

Изменение маршрутно-адресной информации

Подбор аутентификационных данных

ТИПЫ КОМПЬЮТЕРНЫХ АТАК

ГОССОПКА

Эксплуатация уязвимости ПО

Эксплуатация программных
или программно-аппаратных закладок

Вредоносные сетевые воздействия
с использованием недостатков конфигурации
в информационном ресурсе

СБОР ИНФОРМАЦИИ О КОНТЕКСТЕ КОМПЬЮТЕРНОЙ АТАКИ

ГОССОПКА

1. Когда была предпринята попытка атаки?
2. В какой точке системы произошла атака?
3. Для чего была предпринята попытка атаки?
4. Какие еще цели мог преследовать злоумышленник?
5. Какие индикаторы вредоносной активности оставил злоумышленник?

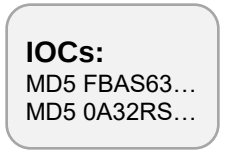
НКЦКИ ПРЕДОСТАВЛЯЕТ СВЕДЕНИЯ:

ГОССОПКА

о признаках компьютерных инцидентов

об уязвимостях ПО

об угрозах



индикаторы вредоносной активности

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

КОНТАКТЫ ДЛЯ ОРГАНИЗАЦИИ ВЗАИМОДЕЙСТВИЯ

ГОССОПКА

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

gov-cert@gov-cert.ru

+7 (916) 901-07-42

ГОССОПКА

Спасибо за внимание!