О целях и задачах субъектов ГосСОПКА

Алексей Новиков

ГОССОПКА

ГОССОПКА

Что значит быть субъектом ГосСОПКА?

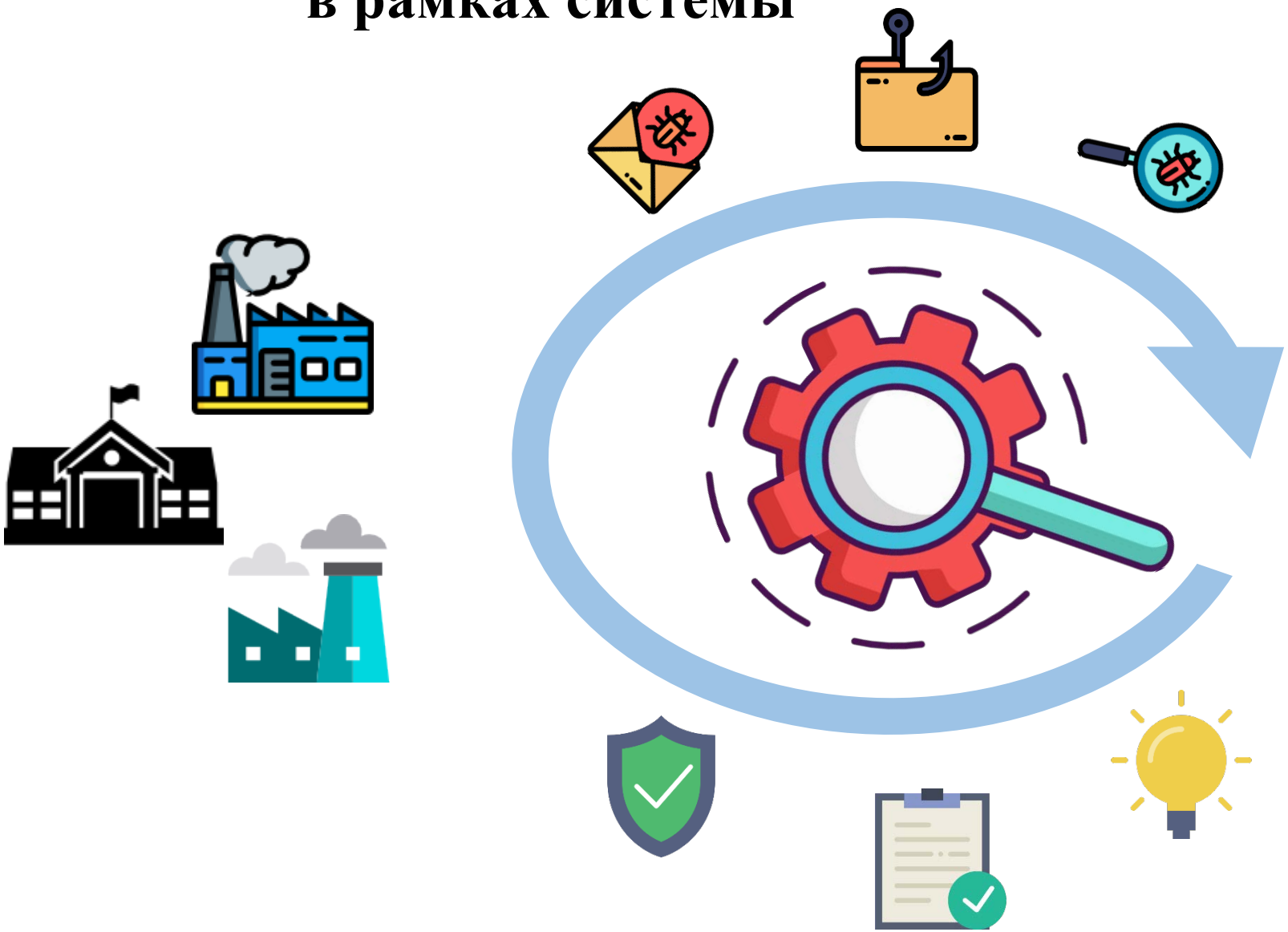
Я обнаруживаю атаки! Я в ГосСОПКА?

Я заключил соглашение! Я в ГосСОПКА?

Мы создали отдел реагирования на инциденты!
Мы в ГосСОПКА?

Информационное взаимодействие в рамках системы

ГОССОПКА



НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

ГОССОПКА

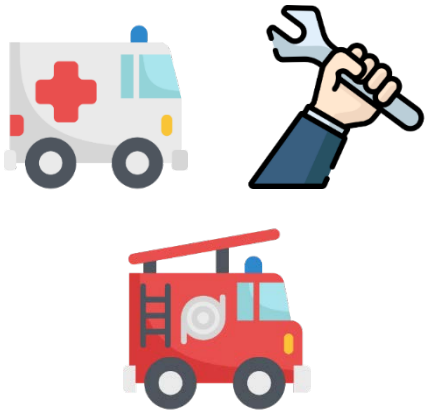
Современные тенденции

Быстрое усложнение механизмов, используемых злоумышленниками

Растущая скорость реализации угроз

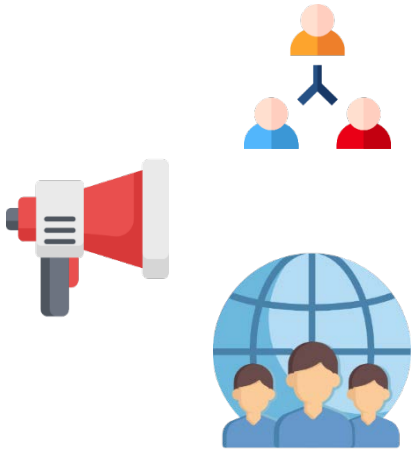
Направления работы НКЦКИ

ГОССОПКА



Практическая помощь в реагировании

Организация информационного взаимодействия



ГОССОПКА

Сведения, распространяемые НКЦКИ

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

IOC, уведомления об угрозах

Сигнатуры, YARA - правила

Признаки инцидентов

Функции центров ГосСОПКА

ГОССОПКА

инвентаризация
выявление уязвимостей
анализ угроз информационной безопасности
повышение квалификации персонала

прием сообщений о возможных инцидентах от персонала и пользователей
обнаружение компьютерных атак
анализ данных о событиях безопасности

регистрация инцидентов
реагирование на инциденты и ликвидация их последствий
установление причин инцидентов
анализ результатов устранения последствий инцидентов

Обработка данных в НКЦКИ

ГОССОПКА

Данные о вредоносной активности от участников системы

Сведения об объектах

Признаки инцидентов

Уведомления об угрозах

Данные об уязвимостях ПО

IOCs:
MD5 FBAS63…
MD5 0A32RS…

Индикаторы вредоносной активности

Результаты анализа инцидентов

Данные из специальных источников

Данные от сообщества

НКЦКИ в 2018 году

ГОССОПКА

15,5 тыс.

объектов КИИ различных отраслей подключено к ГосСОПКА

300 раз

НКЦКИ оказывал практическое содействие в выявлении и реагировании на КИ

700

уведомлений об угрозах направлено субъектам ГосСОПКА

ГОССОПКА

Спасибо за внимание

gov-cert@gov-cert.ru
+7 (916) 901-07-42