ГОССОПКА

Взаимодействие с НКЦКИ

СИЛЫ ГОССОПКА:

ГОССОПКА

Подразделения и должностные лица ФСБ России

Подразделения и должностные лица субъектов КИИ

НКЦКИ
НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Национальный координационный центр по компьютерным инцидентам

ФУНКЦИИ НКЦКИ

ГОССОПКА

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Задача:

- координация деятельности субъектов ГосСОПКА

Функции:

- выявление, предупреждение и ликвидация последствий компьютерных атак
- обмен информацией о компьютерных инцидентах между субъектами КИИ, а также уполномоченными органами иностранных государств
- информационное и методическое обеспечение деятельности в области обнаружения и предупреждения компьютерных атак
- анализ информации о компьютерных инцидентах и компьютерных атаках

НКЦКИ СОБИРАЕТ СВЕДЕНИЯ:

ГОССОПКА

об атаках и инцидентах

об объектах

о программном обеспечении

об угрозах

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

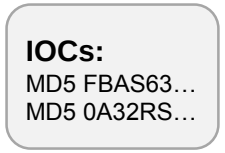
НКЦКИ ПРЕДОСТАВЛЯЕТ СВЕДЕНИЯ:

ГОССОПКА

о признаках компьютерных инцидентов

об уязвимостях ПО

об угрозах

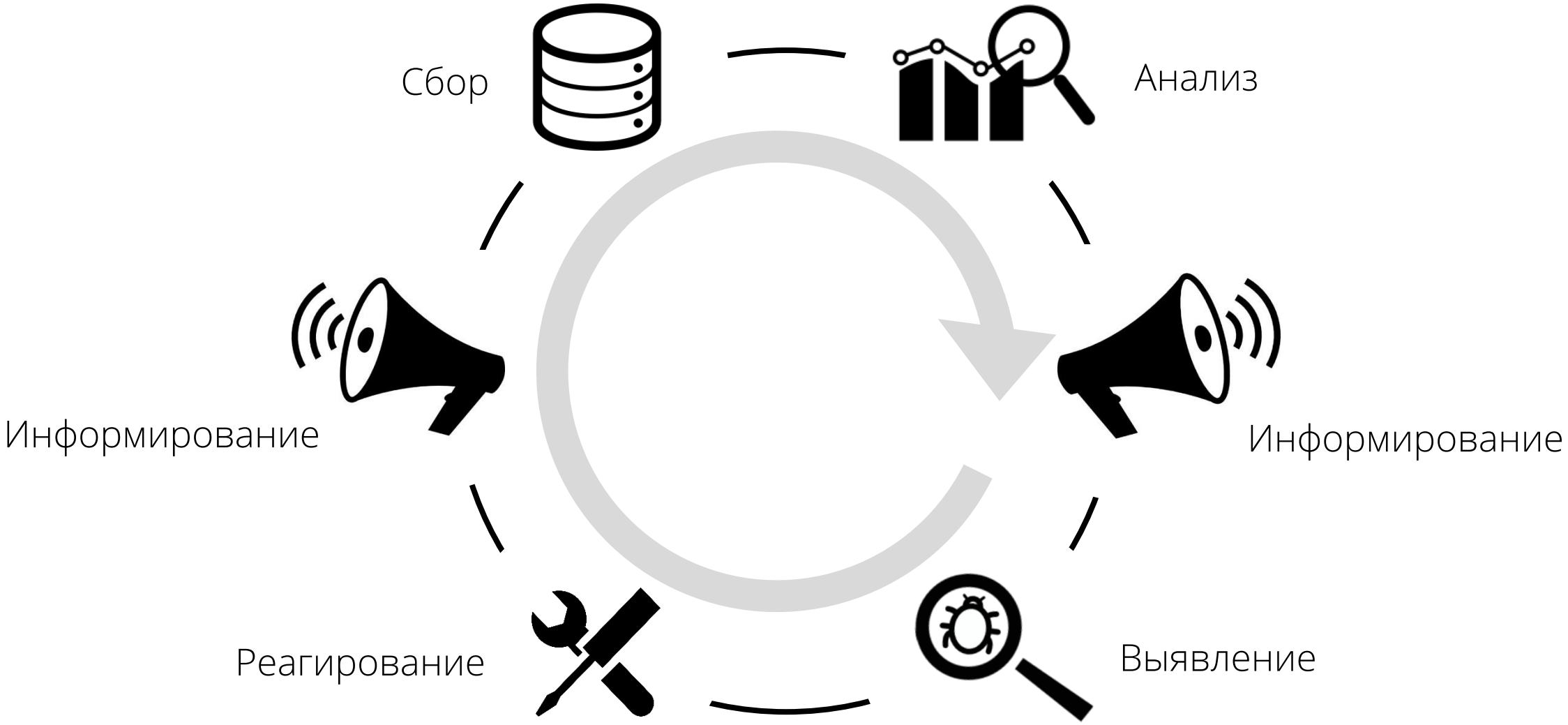


индикаторы вредоносной активности

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

ИНФОРМАЦИОННОЕ ВЗАИМОДЕЙСТВИЕ В ГОССОПКА



НОРМАТИВНО-ПРАВОВЫЕ АКТЫ ФСБ РОССИИ

ГОССОПКА

Приказ ФСБ России от 24.07.2018 №366 «О Национальном координационном центре по компьютерным инцидентам»

Приказ ФСБ России от 24.07.2018 №367 «Об утверждении перечня информации, предоставляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ и порядка предоставления информации в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ»

Приказ ФСБ России от 24.07.2018 №368 «Об утверждении порядка обмена информацией о компьютерных инцидентах между субъектах критической информационной инфраструктуры РФ и уполномоченными органами иностранных государств, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты и порядка получения субъектами критической информационной инфраструктуры РФ информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения»

ПЕРЕЧЕНЬ ИНФОРМАЦИИ, ПРЕДОСТАВЛЯЕМОЙ В ГОССОПКА

ГОССОПКА

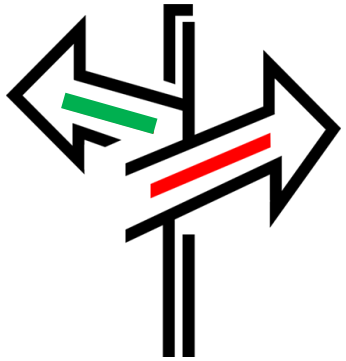
1. Информация из реестра значимых объектов КИИ
2. Информация об отсутствии необходимости присвоения объекту КИИ одной из категорий значимости
3. Информация об исключении объекта КИИ из реестра значимых объектов КИИ или изменении его категории
4. Информация по результатам государственного контроля
5. Информация о компьютерных инцидентах, связанных с функционированием объектов КИИ
6. Иная информация в области обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты

ТИПЫ КОМПЬЮТЕРНЫХ ИНЦИДЕНТОВ

ГОССОПКА

Нарушение или замедление работы информационного ресурса

Внедрение ВПО



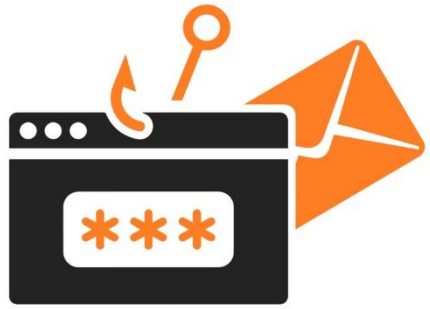
Нелегитимное изменение маршрутно-адресной информации в сети Интернет

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

Использование информационного ресурса
для публикации запрещенной информации

Нелегитимное изменение
содержимого информационного ресурса

Использование информационного ресурса
в целях распространения спама

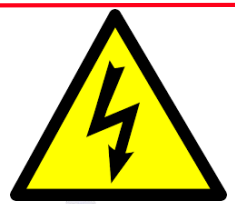
СОСТАВ ИНФОРМАЦИИ О КОМПЬЮТЕРНОМ ИНЦИДЕНТЕ

ГОССОПКА

1. Дата, время, место нахождения или географическое положение объекта КИИ, вовлеченного в компьютерный инцидент
2. Наличие причинно-следственной связи между компьютерным инцидентом и компьютерной атакой
3. Связь с другими компьютерными инцидентами
4. Состав технических параметров компьютерного инцидента
5. Последствия компьютерного инцидента

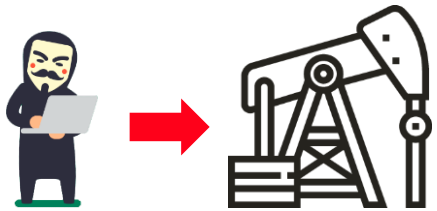
ИНАЯ ИНФОРМАЦИЯ В ОБЛАСТИ ОБНАРУЖЕНИЯ И ПРЕДУПРЕЖДЕНИЯ АТАК

ГОССОПКА



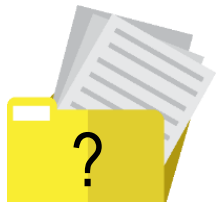
об угрозах в отношении объектов КИИ

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

По телекоммуникационным каналам сети Интернет:

- через техническую инфраструктуру НКЦКИ

Посредством электронной, почтовой, факсимильной и телефонной связи

ПОЛУЧЕНИЕ ИНФОРМАЦИИ СУБЪЕКТАМИ КИИ

1. Обращение к веб-сайту НКЦКИ http://cert.gov.ru
2. Направление запросов в НКЦКИ
3. Направление обращений в ФСБ России
4. Направление запросов другим субъектам КИИ
5. Посредством технической инфраструктуры НКЦКИ

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

http://cert.gov.ru

gov-cert@gov-cert.ru

+7 (916) 901-07-42

+7 (4812) 20-37-37

ГОССОПКА

Спасибо за внимание!