kaspersky

Kaspersky Industrial Cybersecurity Conference 2021

Алексей Новиков

Сотрудник, Национальный координационный центр по компьютерным инцидентам (НКЦКИ), Россия

#KasperskyICS

Чат конференции: https://kas.pr/kicscon

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Об опыте реагирования на компьютерные инциденты в 2020-2021

Алексей Новиков

Скорость реализации угроз

Тенденции 2020/21

Скорость реализации угроз

Доступность средств нападения

Тенденции 2020/21

Скорость реализации угроз

Доступность средств нападения

Растущая квалификация злоумышленников

Объекты устремлений злоумышленников

Объекты КИИ, объекты промышленности

Объекты устремлений злоумышленников

Объекты КИИ, объекты промышленности

Информационные ресурсы государственных организаций

Объекты устремлений злоумышленников

Объекты КИИ, объекты промышленности

Информационные ресурсы государственных организаций

«Подрядчики» : интеграторы, поставщики, разработчики ПО

Защитим периметр

Защитим периметр

Достаточно ?

Вектора проникновения

Взлом веб-приложений

Вектора проникновения

Взлом веб-приложений

Фишинговые рассылки

Вектора проникновения

- Взлом веб-приложений
- Фишинговые рассылки
- Атаки через подрядчиков

Вектора проникновения

- Взлом веб-приложений
- Фишинговые рассылки
- Атаки через подрядчиков
- «Обычное» ВПО

К инцидентам нужно готовиться

Логи сетевых взаимодействий

DNS – обязательный минимум

Есть обращение к вредоносному домену с внешнего адреса, надо найти скомпрометированный объект внутри

Логи сетевых взаимодействий

DNS – обязательный минимум

Есть обращение к вредоносному домену с внешнего адреса, надо найти скомпрометированный объект внутри

Готовы 50%

Логи сетевых взаимодействий

DNS – обязательный минимум

Есть обращение к вредоносному домену с внешнего адреса, надо найти скомпрометированный объект внутри

Готовы 50%

Сохранение сетевых сессий

Есть обращение к вредоносному IP с внешнего адреса, надо найти скомпрометированный объект внутри

Логи сетевых взаимодействий

DNS – обязательный минимум

Есть обращение к вредоносному домену с внешнего адреса, надо найти скомпрометированный объект внутри

Готовы 50%

Сохранение сетевых сессий

Есть обращение к вредоносному IP с внешнего адреса, надо найти скомпрометированный объект внутри

Готовы 10%

Подготовка к инциденту

Запись и анализ трафика

- сегментирование сети
- заранее выбранные оптимальные точки записи
- заранее определено чем записывать и чем анализировать

Подготовка к инциденту

Запись и анализ трафика Реализуют 60%

- сегментирование сети
- заранее выбранные оптимальные точки записи
- заранее определено чем записывать и чем анализировать

Подготовка к инциденту

Запись и анализ трафика

Реализуют 60%

- сегментирование сети
- заранее выбранные оптимальные точки записи
- заранее определено чем записывать и чем анализировать

Инвентаризация

- знаем состав инфраструктуры
- отслеживаем изменения активов

Подготовка к инциденту

Запись и анализ трафика Реализуют 60%

- сегментирование сети
- заранее выбранные оптимальные точки записи
- заранее определено чем записывать и чем анализировать

Инвентаризация Реализуют 50%

- знаем состав инфраструктуры
- отслеживаем изменения активов

Подготовка к инциденту

Управление аутентификацией

- регулярная смена паролей
- логирование действий
- возможность централизованной блокировки

Подготовка к инциденту

Управление аутентификацией

Реализуют 70%

- регулярная смена паролей
- логирование действий
- возможность централизованной блокировки

Подготовка к инциденту

Управление аутентификацией Реализуют 70%

- регулярная смена паролей
- логирование действий
- возможность централизованной блокировки

Фиксация состояния

- определена процедура снятия образов
- готовы средства и носители
- определена процедура остановки элементов инфраструктуры

Подготовка к инциденту

Управление аутентификацией Реализуют 70%

- регулярная смена паролей
- логирование действий
- возможность централизованной блокировки

Фиксация состояния Реализуют 30%

- определена процедура снятия образов
- готовы средства и носители
- определена процедура остановки элементов инфраструктуры

Подготовка к инциденту

Мониторинг ключевых объектов инфраструктуры

устранение последствий инцидента класса APT без мониторинга практически невозможно

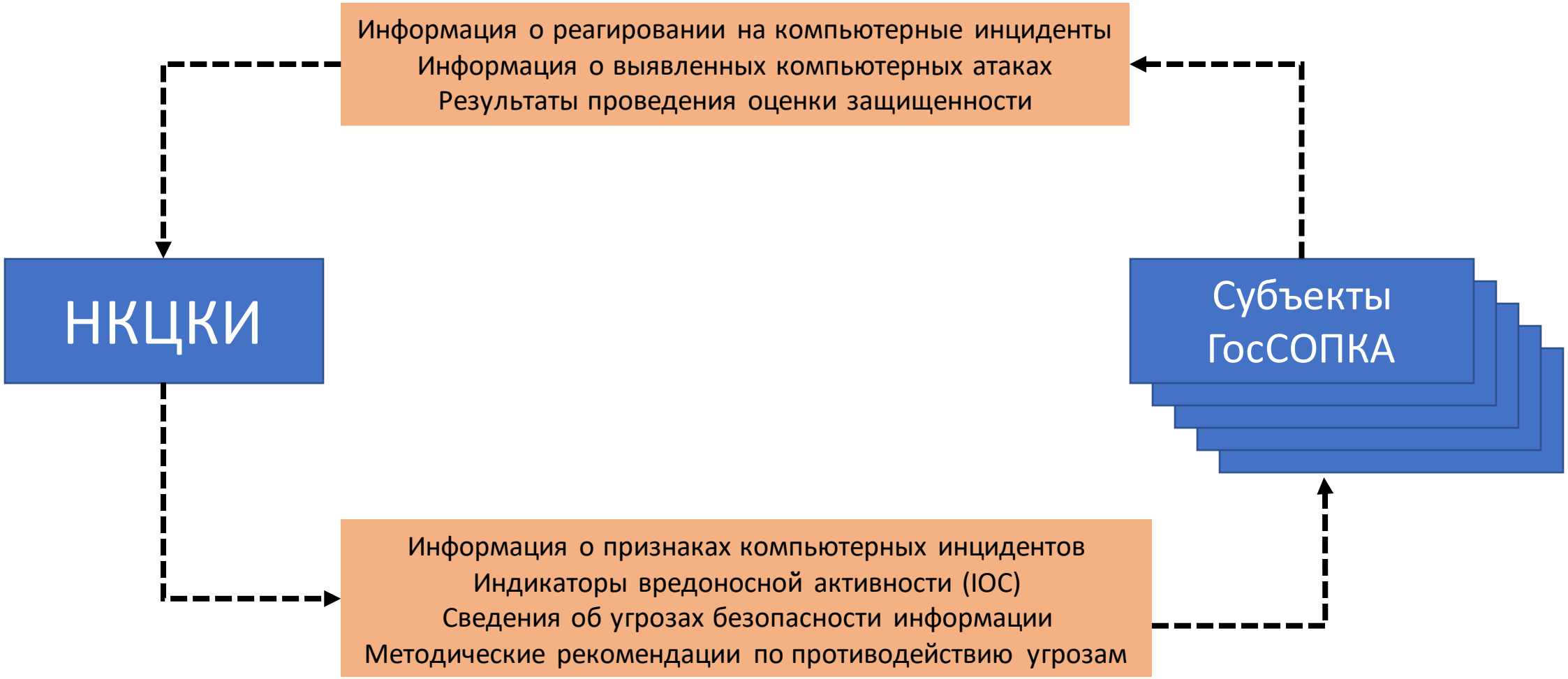
Подготовка к инциденту

Мониторинг ключевых объектов инфраструктуры

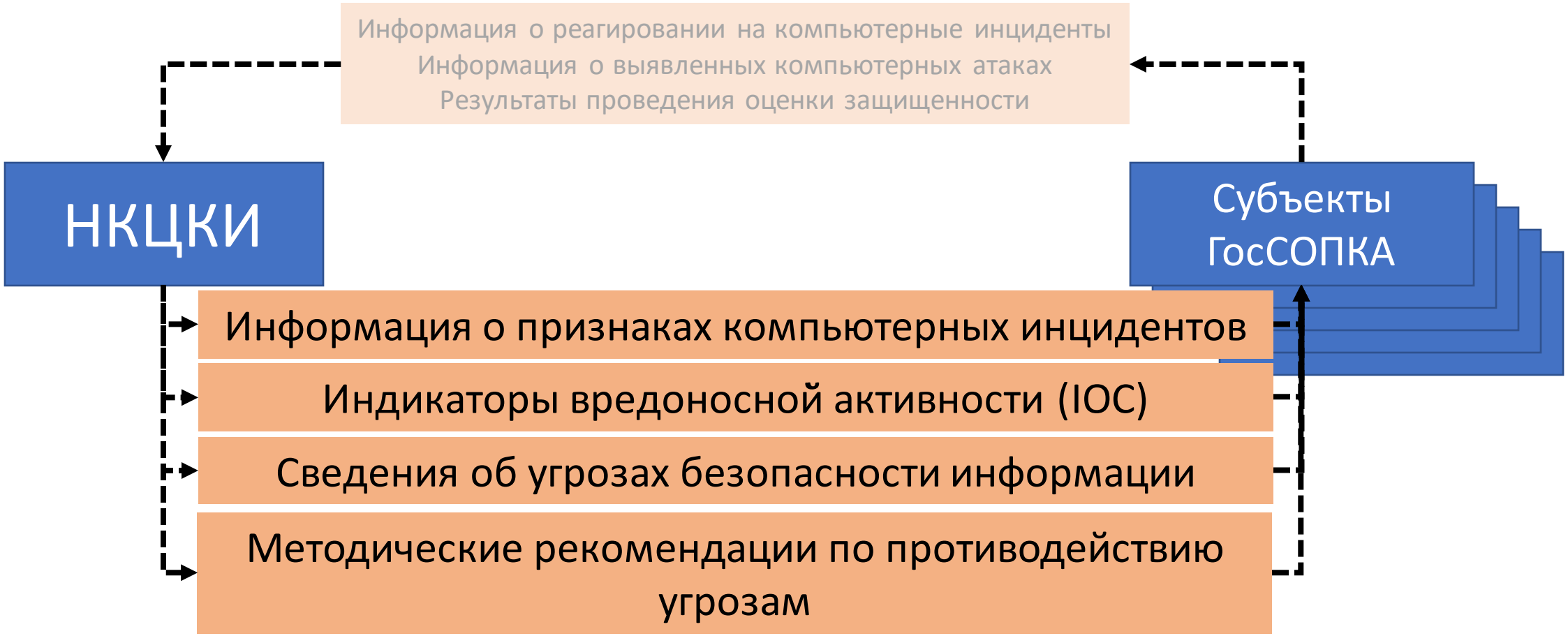
устранение последствий инцидента класса APT без мониторинга практически невозможно

Реализуют 20%

Чем раньше выявил - тем меньше потерял



Опыт одних помогает всем



Проверьте себя

Есть обращение к вредоносному домену с внешнего адреса вашей организации, например, лог трафика запроса к вышестоящему DNS-серверу.
Необходимо найти источник запроса внутри инфраструктуры

Реализуемо? Сколько времени займет?
На какой промежуток времени можно отследить?

Проверьте себя

Есть обращение к вредоносному IP-адресу с внешнего адреса вашей организации, например, трафик сессии взаимодействия с C&C. Есть время, адреса, порты… Необходимо найти скомпрометированный объект внутри инфраструктуры

Реализуемо? Сколько времени займет?

На какой промежуток времени можно отследить?

Спасибо за внимание

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ