OS Day 2024

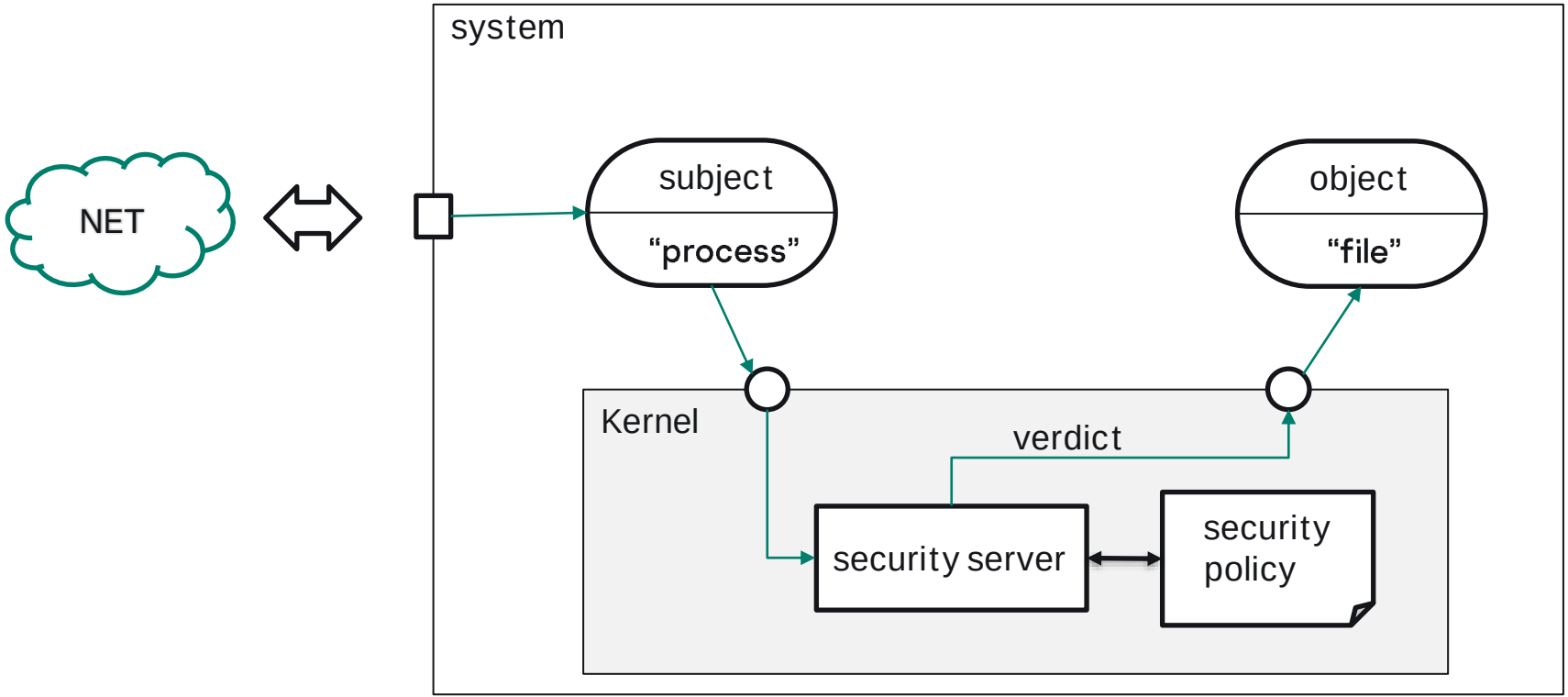
Повышение безопасности решений KasperskyOS на основе анализа графа потока управления

Игорь Сорокин
Руководитель группы системных исследований, «Лаборатория Касперского»

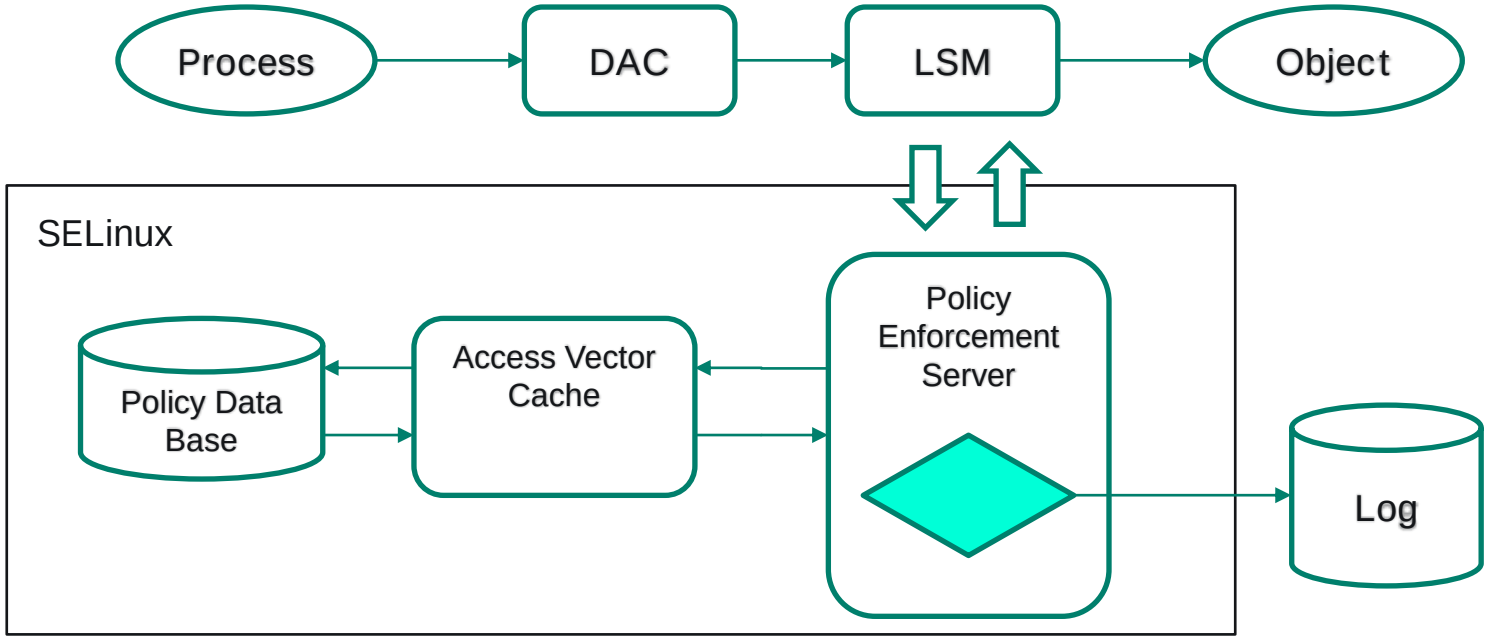
KasperskyOS

Работоспособность – это состояние системы в котором оно способно выполнять заложенные функции

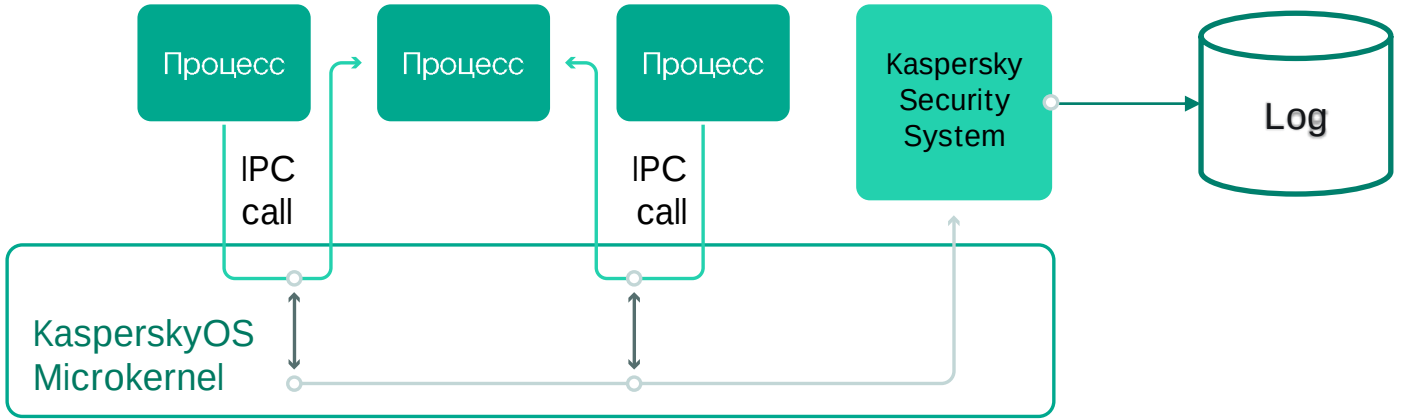
Поддержание работоспособности с помощью политик безопасности



SE Linux: принцип работы



Базовые принципы KasperskyOS



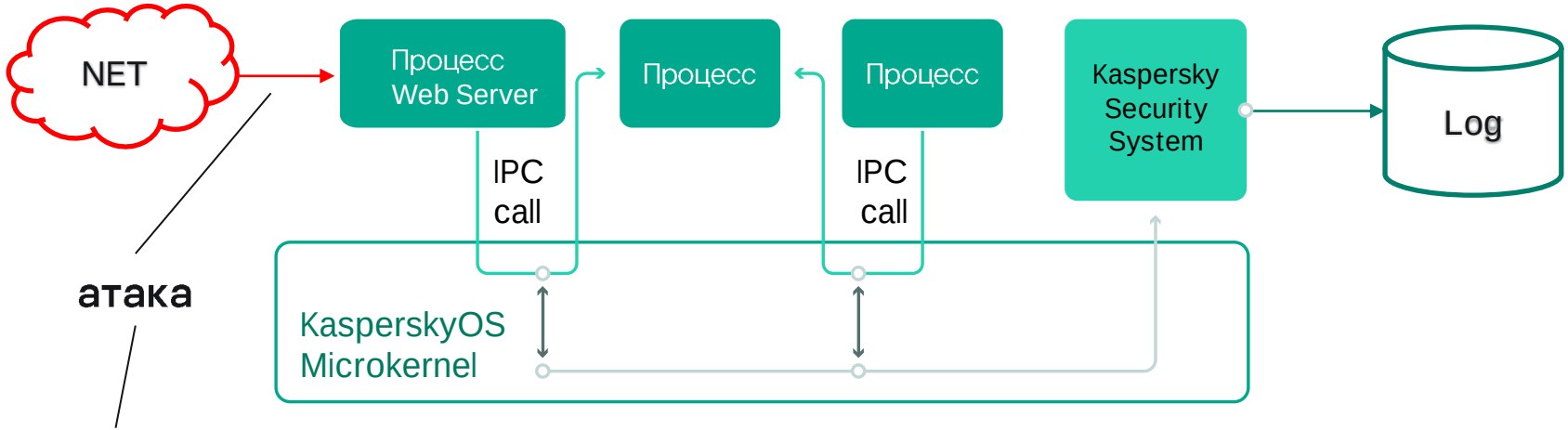
Микроядерная операционная система

Взаимодействие между процессами только по IPC-каналам

Контроль IPC-взаимодействий с помощью политик безопасности (Kaspersky Security System)

Взаимодействие процесса с ядром осуществляется по IPC-каналам

Постановка задачи



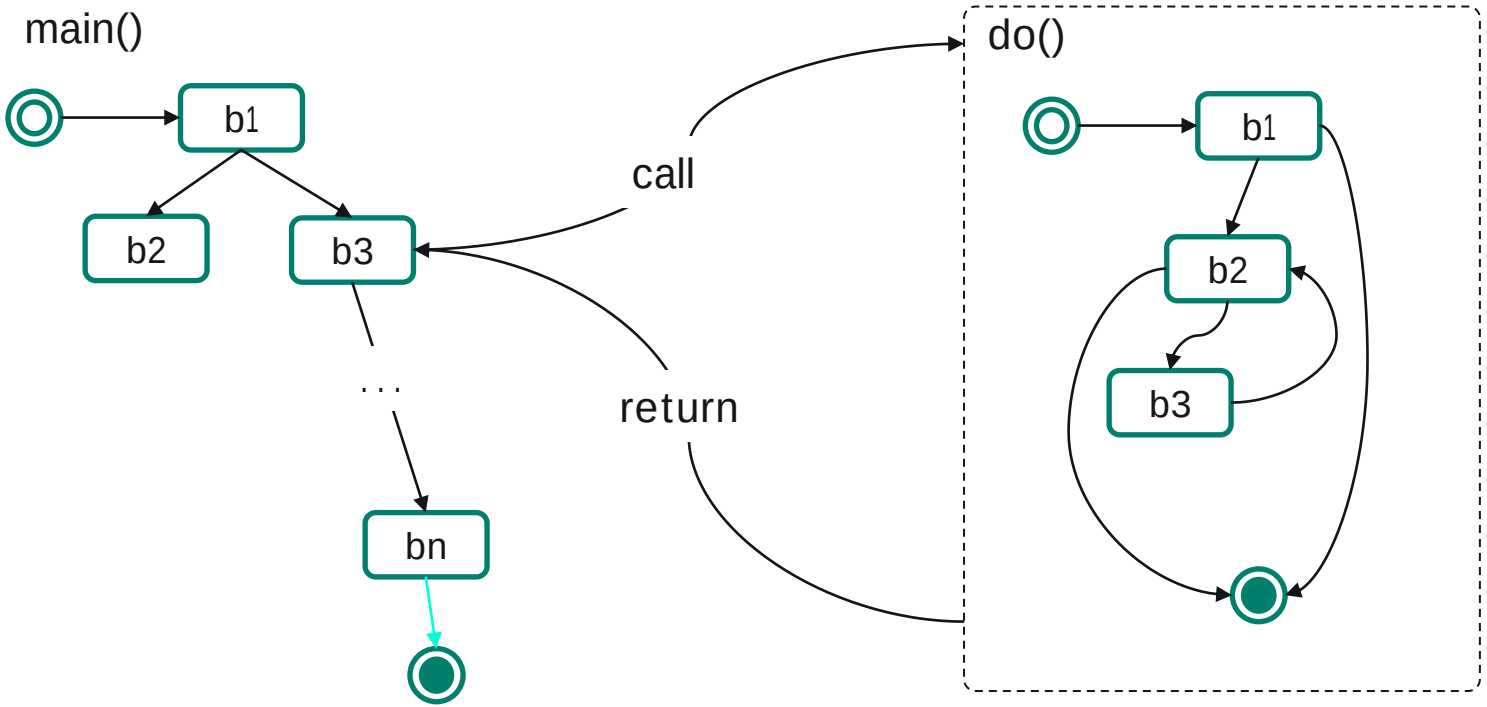
KSS блокирует распространение атаки

Вредоносный код продолжает функционировать:
- расходуются вычислительные ресурсы;
- нарушается «доступность»
- ...

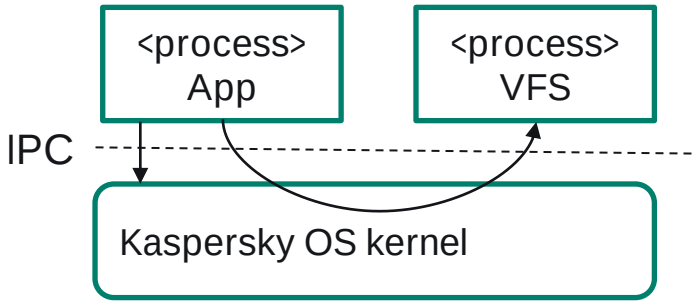
Задача: определить нарушение работоспособности контролируемого процесса

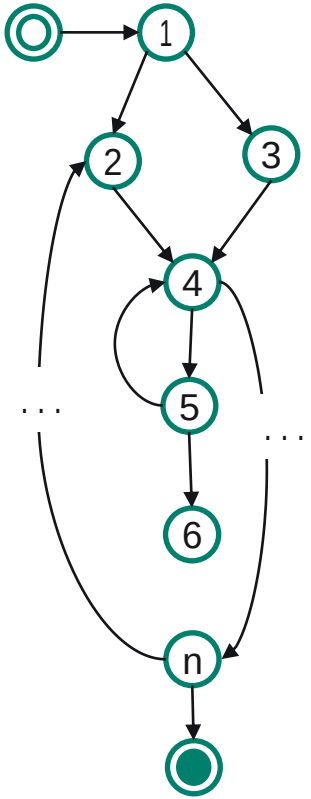
Граф потока управления (CFG)

CFG - **множество всех возможных путей исполнения программы, представленное в виде графа.**



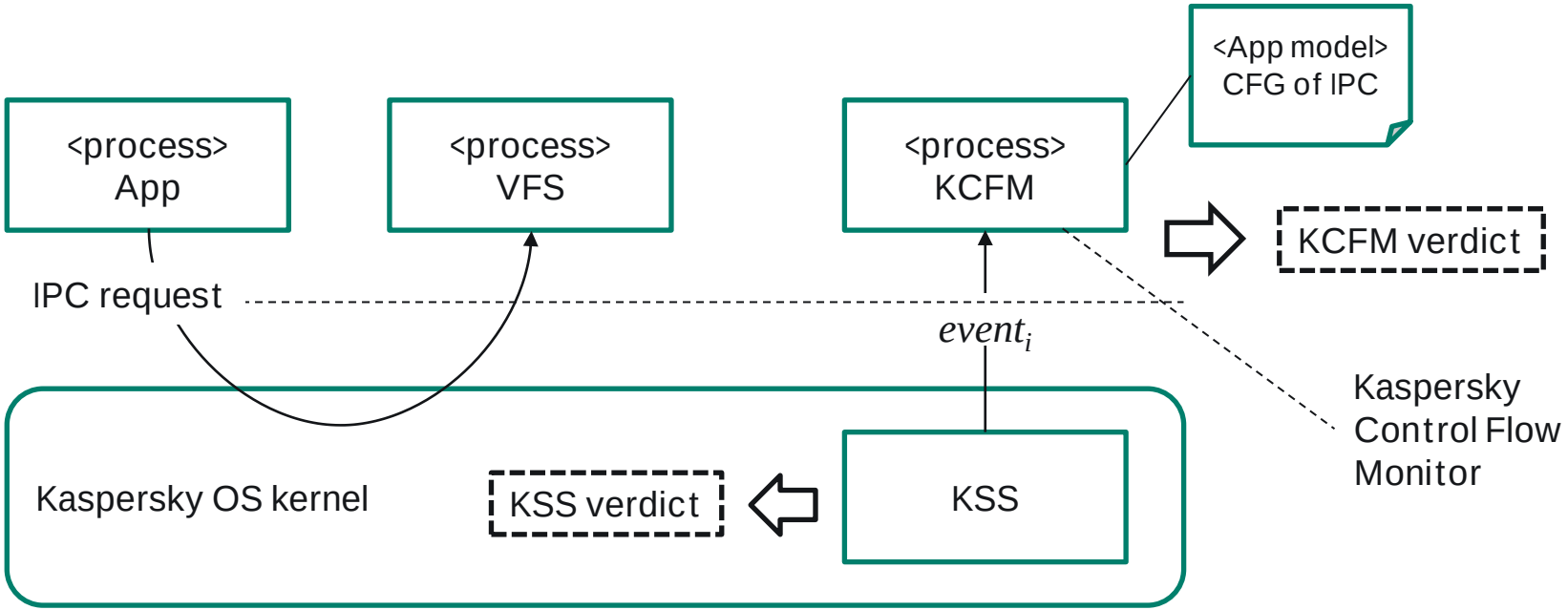
Построение модели процесса на основе графа потока управления





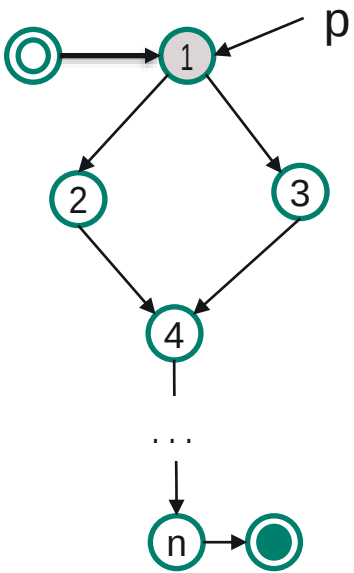
CFG of IPC calls
={1, 2, ..., n}

Использование модели процесса на основе графа потока управления

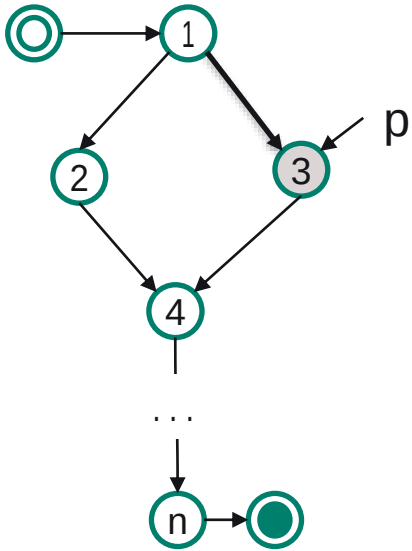


Вычисление вердикта контроля работоспособности (KCFM verdict)

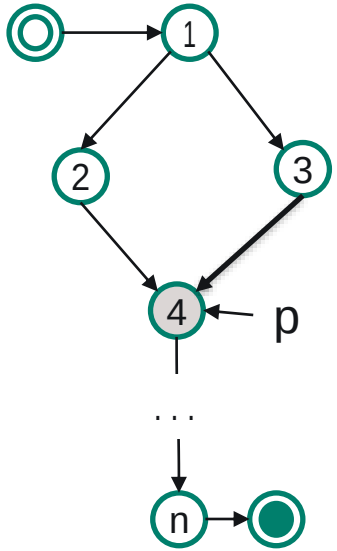
Seq={ev1}
ev1 = (IPC1)



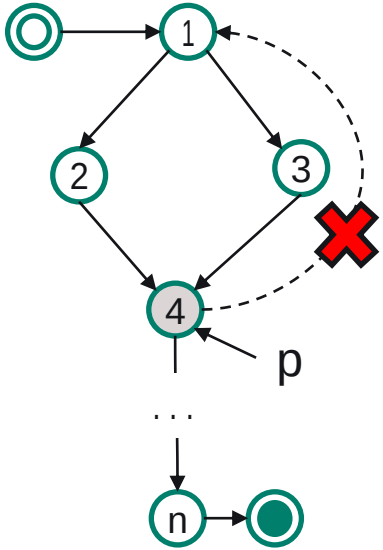
Seq={ev1, ev2}
ev2 = (IPC3)



Seq={ev1, ev2, ev3}
ev3 = (IPC4)

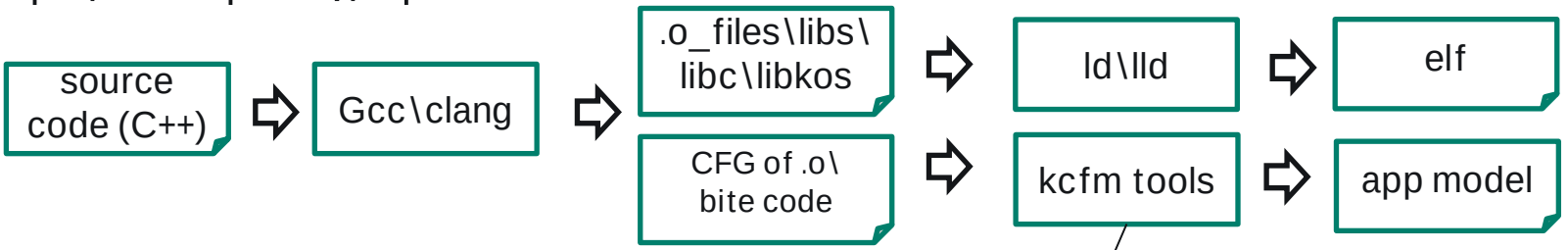


Seq={ev1, ev2, ev3, ev4}
ev4 = (IPC1)

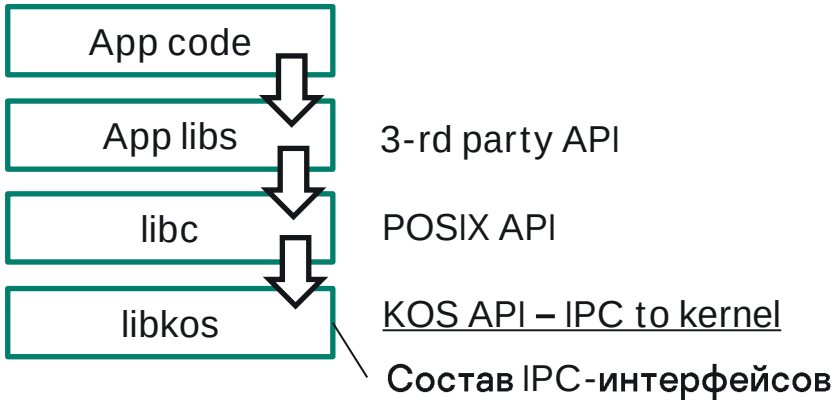


Формирование модели приложения

Процесс сборки кода приложения



Структура приложения



Результат

Возможность определения нарушения работоспособности приложения при выполнении в run-time со следующими особенностями:

- Наложенные средств защиты (антивирус, IPS, IDS) – не нужны
- Инструментирование исходного кода приложения – нет
- Замедление выполнения кода приложения - нет
- Формирование модели приложения производится автоматически в процессе сборки

Спасибо за внимание!

Игорь Сорокин

Руководитель группы системных исследований

Igor.Sorokin@kaspersky.com

KasperskyOS