kaspersky АКТИВИРУЙ БУДУЩЕЕ

Иммунный подход к защите информационных систем

KasperskyOS®

В основе KasperskyOS лежит иммунный подход, позволяющий любой ИТ-системе исполнять свое функциональное назначение в условиях агрессивной среды без дополнительных (наложенных) средств безопасности.

Важнейшим вопросом обеспечения безопасности информационных технологий (далее ИТ), используемых в Российской Федерации в интересах личности, общества и государства, является доверие к уже существующим и создаваемым информационным системам (далее ИС).

«Лаборатория Касперского» уже долгое время работает над решением задачи по созданию доверенной информационной системы из недоверенных компонентов. Результаты этой работы были реализованы в операционной системе KasperskyOS, которая призвана служить основой ИТ-систем с высокими требованиями к информационной безопасности.

В настоящее время ИТ-системы проектируются, как правило, без учета воздействия на них неблагоприятных факторов – недекларированных возможностей программно-аппаратных средств, вирусов, хакерских атак и др. Для успешного функционирования в реальной среде такие системы приходится дооснащать антивирусными программами, сетевыми экранами и другими наложенными средствами защиты. Это приводит к усложнению систем и их уязвимости в отношении внешних атак, поскольку, преодолев защитный барьер, злоумышленник попадает в незащищенное пространство, где может выполнить любое негативное действие.

Ключевые технологии

В составе KasperskyOS можно выделить следующие ключевые технологии:

KasperskyOS – микроядерная операционная система, основой которой служит уникальное микроядро с расширенными функциями безопасности, разработанное «с нуля» специалистами «Лаборатории Касперского».

Kaspersky Security System – движок, выполняющий вычисление вердиктов безопасности, который может одновременно работать с различными типами политик (ролевой и мандатный контроль доступа, контроль потоков управления, политики доменов и типов, политики на основе темпоральных логик и пр.).

Kaspersky Secure Hypervisor – гипервизор второго типа, работающий на микроядре KasperskyOS. Основным преимуществом виртуализированного решения является отделение потенциально недоверенных виртуальных гостевых операционных систем друг от друга и от критически важных сервисов, физически работающих на одной аппаратной платформе. Это позволяет сократить поверхность атаки и минимизировать возможный ущерб от эксплуатации уязвимостей.

KasperskyOS в совокупности с методологией разработки и портирования приложений служит эффективной и надежной основой для разработки доверенных ИС различного назначения и сложности, обладающих иммунитетом в отношении киберугроз.

Рекомендации по разработке ИТ-систем

Для реализации иммунного подхода ИТ-системы необходимо разрабатывать с учетом следующих рекомендаций:

- В начале необходимо разработать модель угроз, и на ее основе сформировать политику безопасности.
- В соответствии с моделью угроз и политикой безопасности систему необходимо проектировать с разделением на домены доверия – области с одинаковыми атрибутами относительно политики безопасности.
- Все взаимодействия между доменами доверия должны быть прозрачными и контролироваться на предмет соответствия политике безопасности.
- Контролирующий компонент должен быть как можно более компактным, чтобы его самого можно было верифицировать.

Придерживаясь данных рекомендаций, можно встраивать в информационную систему недоверенные компоненты, задавая для них необходимые ограничения. Это позволит значительно снизить риски негативного воздействия со стороны недоверенных компонентов на безопасность системы в целом.

Необходимо отметить, что указанные выше рекомендации следует учитывать не только при проектировании новых систем, но и при модернизации уже существующих.

Эти и другие принципы безопасной разработки реализованы в KasperskyOS. Кроме того, создана методология, позволяющая успешно применять KasperskyOS и базовые технологии на ее основе для промышленной разработки и адаптации драйверов аппаратуры, сервисов уровня операционной системы и различных приложений пользовательского уровня.

Основные области применения KasperskyOS

- Логические контроллеры для:
  - Транспортных систем
  - АСУ ТП
  - Энергетических систем
- Интернет вещей
- Автомобили
- Сетевое оборудование
- Встраиваемая электроника
- Доверенные рабочие станции для работы с конфиденциальной информацией

KasperskyOS®

Подробнее на os.kaspersky.ru

www.kaspersky.ru