KasperskyOS

Микроядерная операционная система для отраслей с повышенными требованиями к информационной безопасности

KasperskyOS привносит на рынок операционных систем общего назначения экспертизу «Лаборатории Касперского» в области информационной безопасности и лучшие практики разработки исходно безопасных специализированных ОС.

KasperskyOS позволяет создавать IT-системы с высочайшим уровнем гарантий защищенности. Подавляющее большинство видов кибератак на такие системы не может повлиять на выполнение ими основных функций.

«Лаборатория Касперского» долгое время работает над решением задачи по созданию доверенной IT-системы из недоверенных компонентов. Результаты реализованы в операционной системе KasperskyOS, предназначенной для разработки продуктов для отраслей с повышенными требованиями к безопасности, надежности и предсказуемости работы.

Цель KasperskyOS — обеспечить защиту IT-систем от вредоносного кода и эксплуатации уязвимостей. Эти угрозы могут привести к потере или утечке конфиденциальных данных, снижению производительности. Кроме того, KasperskyOS снижает риски, связанные с ошибками в коде, а также со случайными или преднамеренными повреждающими действиями.

Особенности архитектуры

В основе KasperskyOS лежит комбинация различных подходов к безопасности.

Благодаря особенностям архитектуры, KasperskyOS создает окружение, в котором можно безопасно запускать недоверенные и потенциально уязвимые программы.

В большинстве операционных систем безопасность достигается за счет разделения прав и контроля доступа к ресурсам системы. В KasperskyOS к этому добавляется возможность настраивать и гарантировать выполнение свойств безопасности, необходимых для каждой конкретной задачи.

Микроядро. Минимальный объем кода, достаточный для работы механизмов ядра, позволяет обеспечить строгий контроль качества кода ОС.

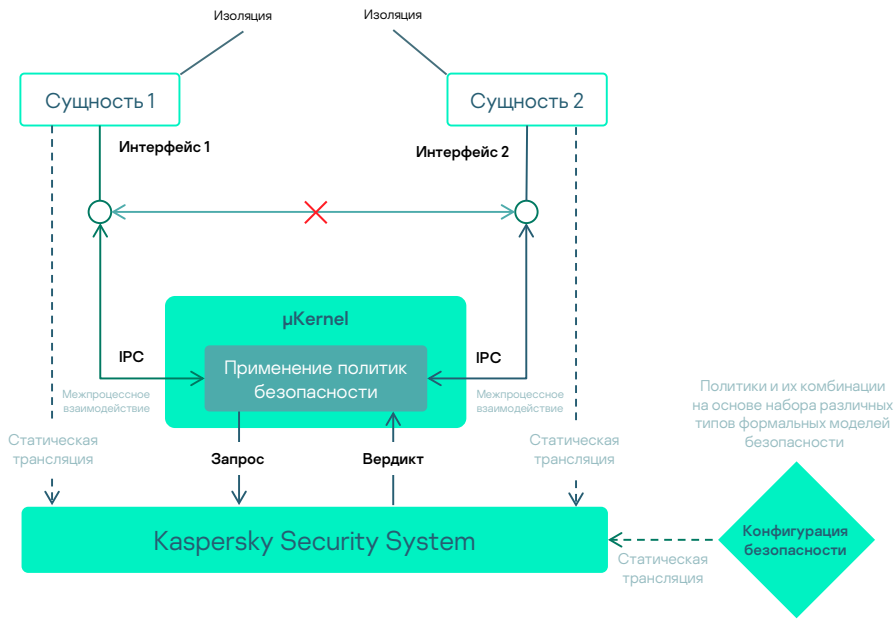
Строгая изоляция. Система гарантирует изоляцию доменов безопасности и отделение свойств безопасности от функциональных компонентов.

Унифицированный механизм межпроцессного взаимодействия (IPC). Микроядро обеспечивает наличие единого механизма IPC.

Строго определенные типизированные интерфейсы. Для каждого приложения или драйвера должны быть статически определены интерфейсы взаимодействия.

Kaspersky Security System. Подсистема KSS проверяет корректность всех IPC-сообщений в соответствии с определениями интерфейсов и контролирует взаимодействие между частями системы, делая эксплуатацию уязвимостей бесполезной для злоумышленников.

Статическая настройка безопасности. Все процессы и доступные для них типы взаимодействий заранее настроены и выверены до начала работы системы.



Основные принципы безопасности KasperskyOS

kaspersky

Системные требования

Требования к CPU:
Memory Management Unit (MMU);
IOMMU (SDMA для ARM) настоятельно рекомендуется для надежной изоляции аппаратных ресурсов.

Поддерживаемые архитектуры:
x86, x86_64, ARMv5, ARMv7, ARMv8 и MIPS32.

Протестированные аппаратные платформы:
- Intel Generic и Atom CPUs,
- NXP i.MX6 (Solo, Duo и Quad),
- NXP i.MX27, TI Sitara AM335x,
- TI Sitara AM43xx, HiSilicon Kirin620,
- MIPS24k.

Минимальный объем RAM зависит от решения. Рекомендуемый объем RAM 128 МБ.

Патенты:
US 7386885 B1, US 7730535 B1, US 8370918 B1, EP 2575318 A1, US 8522008 B2, US 20130333018 A1, US 8381282 B1, EP 2575317 A1, US 8370922 B1, EP 2575319 A1, US 9015797 B1, DE 202014104595 U1.

Преимущества

Проприетарное микроядро
KasperskyOS не является модификацией какой-либо из существующих ОС; в ее основе — микроядро собственной разработки, допускающее только определенный способ взаимодействий.

Многоуровневая совместимость
Для KasperskyOS разработан ряд библиотек, обеспечивающих частичную совместимость с POSIX, что упрощает создание и портирование приложений.

Обязательная идентификация и маркировка
Все приложения KasperskyOS имеют свою безопасную конфигурацию, без которой установить их невозможно. Аппаратное обеспечение и ресурсы уровня приложений (файлы, базы данных, сетевые порты и пр.) маркируются соответствующими атрибутами безопасности. Получить доступ к ресурсу, не имеющему метки безопасности, также невозможно.

Модульная архитектура
Модульный подход к архитектуре системы минимизирует размер доверенной кодовой базы и позволяет построить каждое отдельное решение на индивидуальной основе.

Компонентная модель
Архитектура приложений основана на компонентной модели, благодаря чему разработка решения становится проще и удобнее.

Легко настраиваемые политики
Простой язык настройки позволяет легко задавать правила межпроцессного взаимодействия и контроля доступа.

Сокращение поверхности атаки
Разделение приложений на домены безопасности и полный контроль межпроцессных взаимодействий позволяет безопасно использовать потенциально уязвимые и/или недоверенные приложения.

Возможность проверки
Строгое соблюдение принципов безопасности при проектировании и внедрении системы позволяет верифицировать безопасность всех решений на базе KasperskyOS.

Secure by design система
KasperskyOS была спроектирована и разработана как исходно безопасная.

Области применения

KasperskyOS применяется в отраслях, где существуют повышенные требования к кибербезопасности, надежности и предсказуемости работы IT-систем.

KasperskyOS

Подробнее на os.kaspersky.ru

www.kaspersky.ru