KasperskyOS®

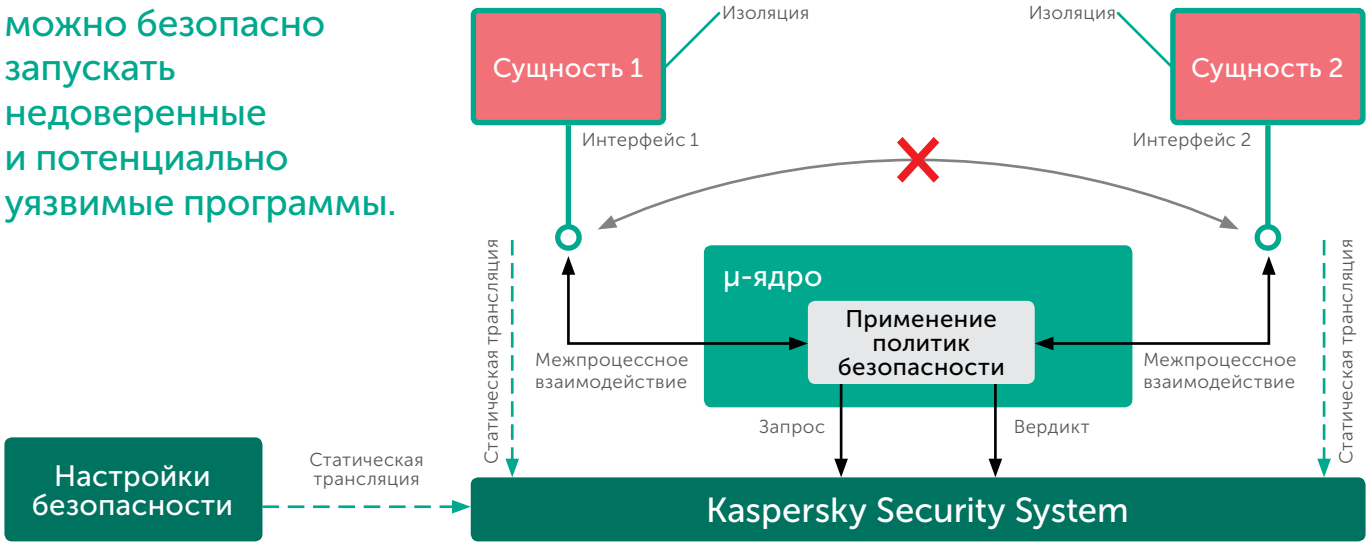
KasperskyOS. Техническая информация

KasperskyOS – это безопасная операционная система для встраиваемых устройств, подключенных к интернету и имеющих специальные требования к кибербезопасности.

Основные особенности KasperskyOS:

- **Безопасная микроядерная ОС**. Создана на базе специально разработанного с нуля микроядра; не является модификацией какой-либо из существующих ОС.
- **Безопасно спроектирована**. Разработана на базе принципов MILS; имеет в своем составе гибкую систему контроля доступа (KSS).
- **API для драйверов пользовательского пространства**. SDK может использоваться с драйверами и приложениями заказчика.
- **Поддержка POSIX**. Поддержка около 98% POSIX API.
- **Портирование**. KasperskyOS работает на платформах Intel x86/x86_64 и ARM. Поддержка других аппаратных платформ с MMU может быть организована по запросу.
- **Поддержка аппаратной виртуализации**. KasperskyOS может использоваться как основа для безопасного гипервизора с поддержкой технологий Intel VT-x и VT-d.
- **Защита межпроцессного взаимодействия**. Тщательно продуманный подход к контролю межпроцессного взаимодействия в соответствии с преднастроенными политиками безопасности.
- **Сокращение поверхности атаки**. Разделение приложений на домены безопасности и полный контроль междоменных взаимодействий позволяет безопасно использовать потенциально уязвимые и/или недоверенные приложения.

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



В основе KasperskyOS лежит комбинация различных подходов к безопасности.

Принципы безопасности:

Для большинства 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.

- **µ-ядро**. Минимальный объем кода, достаточный для работы механизмов ядра, позволяет обеспечить более строгий контроль качества кода ОС.
- **Гарантированная 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. KSS проверяет корректность всех IPC сообщений в соответствии с этими определениями интерфейсов.
- **Статическая настройка безопасности**. Все процессы и доступные для них типы взаимодействий заранее настроены и выверены до начала работы системы.
- **Полное посредничество**. Все межпроцессные взаимодействия проходят через микроядро, которое проверяет их с помощью Kaspersky Security System (KSS). KSS вычисляет вердикт о возможности доступа, руководствуясь настройками безопасности.
- **Отказ по умолчанию**. Любое действие, не предусмотренное политиками безопасности, запрещено по умолчанию.
- **Драйверы пользовательского пространства**. Драйверы, ядра и приложения изолированы друг от друга; драйверы запускаются как непривилегированный код, и ошибка в одном драйвере не оказывает негативного влияния на систему в целом. Также есть возможность ограничить доступ драйвера к физическому устройству.

Доверенные компоненты в недоверенном окружении

Хотя полностью исключить возможность ошибок кода нельзя, мы хотим, чтобы программное обеспечение было безопасным. Задача KasperskyOS – обеспечить безопасность всей системы, используя минимум доверенных компонентов.

Одной из основных целей KasperskyOS является обеспечение безопасности сложных систем с использованием минимума доверенных компонентов. С помощью KasperskyOS сложная система может быть разделена на ряд изолированных сущностей или компонентов (доменов безопасности). Критически важные функции безопасности могут быть определены в разные компоненты с небольшой поверхностью атаки, которые легко контролировать. Доверенным считается небольшой набор функций, в то время как другие компоненты, которые могут нести в себе проблемы и уязвимости различных видов, доверенными не считаются. Применение свойств безопасности, определенных средствами KasperskyOS и KSS, обеспечивается в рамках всей системы. Даже если эксплуатация уязвимости в одном из недоверенных компонентов будет успешной, это не окажет влияния на решение в целом и не затронет критически важные функции.

KasperskyOS позволяет создать гибкое и безопасное решение, но это не означает, что любое решение на базе KasperskyOS является безопасным.

Методология

В рамках комплексного подхода мы предлагаем тщательно разработанную методологию, которая описывает, как создавать и внедрять безопасно спроектированное решение. В соответствии с этой методологией, прежде всего необходимо понять, какой функционал планируется реализовать в решении. Далее нужно провести анализ угроз для построения модели угроз, которая позволит выявить слабые места решения и сформулировать требования к его безопасности. Затем следует разработать функциональный проект, выделить домены безопасности (сущности с общими свойствами безопасности), определить доверенную вычислительную базу, выполнить проектирование интерфейсов взаимодействия и дизайн конфигурации безопасности (спецификация свойств безопасности). После того, как дизайн проверен и утвержден, безопасное решение может быть внедрено при соблюдении требований к его безопасности. И наконец, после внедрения решение должно быть еще раз тщательно проверено с помощью различных техник (модульное, системное, функциональное, случайное тестирование, а также тесты на проникновение и др.) и окончательно утверждено. Следование предписаниям методологии критически важно для создания безопасного решения.

Технологии на базе KasperskyOS

Вместе с KasperskyOS могут использоваться следующие безопасные решения:

- **Безопасная Загрузка** – процедура, требующая поддержки со стороны аппаратной платформы и гарантирующая целостность и подлинность образа загрузки KasperskyOS.
- **Безопасное Обновление** – помогает удаленно осуществлять доверенное и безопасное обновление программного обеспечения.
- **Безопасный Аудит** – решение, осуществляющее идентификацию, запись и хранение журнала событий и позволяющее гарантировать, что записи журнала не будут подменены. Соответствует требованиям ISO/IEC 15408-2.
- **Безопасное Хранилище** – хранилище типа ключ\значение, глубоко интегрированное с KSS для контроля доступа к конфиденциальной информации.
- **Доверенный канал** – платформа на базе протокола защиты транспортного уровня, обеспечивающая канал передачи шифрованных данных удаленным участникам, успешно прошедшим аутентификацию и авторизацию. Платформа доверенного канала может быть сконфигурирована для поддержки различных бэкэндов и схем взаимодействия.
- **Безопасный Гипервизор (KSH)** – решение для виртуализации различных операционных систем на базе KasperskyOS. KSH поддерживает большое количество недоверенных гостевых операционных окружений на единой аппаратной платформе, делая невозможными любые незапланированные взаимодействия гостевых систем между собой и с хостовой ОС.

Поддерживаемые языки для нативной разработки приложений KasperskyOS – C и C++. Также предусмотрен ряд скриптовых языков: Java, Lua, Qt Script, QML, JavaScript.

Разработка KasperskyOS

KasperskyOS, Kaspersky Security Hypervisor, Kaspersky Security System, все базовые драйверы, сервисы и библиотеки пользовательского пространства написаны на языке C. Пакет инструментальных средств основан на наборе компиляторов GNU.

Для описания свойств всех доменов безопасности и политик безопасности для развертываемой системы используется набор стандартных декларативных языков (язык описания интерфейса, язык описания политик безопасности и т.п.). Компилятор позволяет осуществить трансляцию с этих языков на C.

Драйверы KasperskyOS – это сущности пользовательского режима, которые должны соответствовать описанной модели драйверов KasperskyOS.

Системные требования

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

Поддерживаемая архитектура:
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 объём RAM зависит от решения. Рекомендуемый объём RAM 128 Мб.

Поставка KasperskyOS

KasperskyOS поставляется в виде SDK, специально разработанного и сконфигурированного с учетом индивидуальных потребностей каждого заказчика.

KasperskyOS SDK – это основа, которая содержит все необходимые компоненты, необходимые заказчику для реализации собственного решения.

Как правило, для каждого заказчика «Лаборатория Касперского» готовит отдельный SDK, который соответствует конкретным требованиям к аппаратной платформе и набору компонентов.

В KasperskyOS SDK входит:

- µ-ядро KasperskyOS в бинарном виде;
- среда выполнения KSS в бинарном виде;
- драйверы, системные библиотеки и другие компоненты, разработанные «Лабораторией Касперского», в бинарном виде;
- сторонние компоненты кода с открытыми исходниками;
- примеры для разработчиков, включающие исходный код;
- наборы компиляторов и прочих инструментов, включая компиляторный набор на базе GCC и набор компиляторов для KasperskyOS.

Лицензии стороннего кода:
В µ-ядре, KSS и базовом наборе компонентов SDK используются компоненты с открытым исходным кодом и разрешающими их использование лицензиями.

Совместимость KasperskyOS

Приложения KasperskyOS могут использовать слой совместимости ISO/IEC 9899:1999 и/или POSIX.

Профили PSE51 и PSE52 POSIX 1003.13 полностью поддерживаются. Стандарт POSIX 1003.1 также поддерживается, за исключением примитивов управления процессами (таких как fork() и exec()).

Kaspersky Secure Hypervisor поддерживает в качестве гостевых операционных систем немодифицированные Linux и Windows для платформ с поддержкой аппаратной виртуализации.

Приложения, работающие внутри гостевых ОС, могут иметь доступ к нативным примитивам KasperskyOS для передачи сообщений. Это позволяет отвязать бизнес-логику безопасных нативных приложений KasperskyOS от логики многофункциональных приложений гостевых ОС.

www.kaspersky.ru

АО «Лаборатория Касперского», Россия, Москва **www.kaspersky.ru**
Аналитика и отчеты о киберугрозах от экспертов «Лаборатории Касперского»:
www.securelist.ru
KasperskyOS®: **os.kaspersky.ru**

#kasperskyos
#truecybersecurity