



KasperskyOS

Микроядерная операционная система для отраслей с повышенными требованиями к информационной безопасности

Операционная система KasperskyOS реализует новый, кибериммунный подход к защите IT-систем и позволяет сделать неэффективными как известные, так и новые типы кибератак.

Необходимость защиты:

По данным Kaspersky ICS CERT, 31,84% компьютеров АСУ в первом полугодии 2022 г. было атаковано вредоносным ПО

Преимущества:

- Минимизация киберрисков
- Сокращение затрат на приобретение и эксплуатацию дополнительных продуктов IT-безопасности
- Оптимизация трудозатрат IT и ИБ департаментов
- Гибкая настройка с учетом индивидуальных требований к функциональности и безопасности

Почему это важно

С каждым годом ландшафт киберугроз усложняется, а квалификация злоумышленников растет. Атакам подвергаются промышленные предприятия, энергетический сектор, транспортная инфраструктура и IT-системы умного города.

В этих условиях классические подходы к безопасности IT-систем малоэффективны, и поэтому возрастает спрос на операционные системы с высоким уровнем гарантий защищенности.

Решение

В качестве ответа на современные реалии «Лаборатория Касперского» разработала кибериммунный подход к созданию IT-решений, а также собственную операционную систему KasperskyOS — платформу для разработки кибериммунных продуктов.

Благодаря особенностям архитектуры, на базе KasperskyOS можно создавать IT-продукты, обладающие кибериммунитетом — встроенной защищенностью от подавляющего большинства типов кибератак. Для этого разработчикам необходимо следовать специальной методологии.

Кибериммунные продукты практически невозможно скомпрометировать в плановых режимах работы и повлиять на выполнение ими критичных функций, в них принципиально минимизировано число возможных уязвимостей. Таким системам не нужны дополнительные (наложенные) средства безопасности — все необходимое уже есть внутри.

Области применения

Кибериммунные продукты на базе KasperskyOS применяются в отраслях, где существуют повышенные требования к кибербезопасности, надежности и предсказуемости работы IT-систем, например, в промышленности, энергетике, транспортной инфраструктуре, в системах умного города.



Интернет вещей, включая индустриальный



Транспорт



Инфраструктура виртуальных рабочих столов (VDI)



Корпоративные мобильные устройства



Kaspersky IoT Infrastructure Security



Kaspersky Automotive Adaptive Platform



Kaspersky Secure Remote Workspace



Kaspersky Professional Mobile Platform

kaspersky

Ключевые технологии:

Кибериммунитет

Собственная методология разработки исходно безопасных (secure by design) систем, не требующих дополнительных средств защиты

Микроядро

Обеспечивает надежность и прозрачность операционной системы. Минимальный объем ядра позволяет гарантировать строгий контроль качества кода.

Подсистема Kaspersky Security System

Контролирует все взаимодействия компонентов KasperskyOS, проверяет их соответствие политикам безопасности и запрещает любое нежелательное поведение.

Ядро операционной системы разработано в «Лаборатории Касперского» с нуля, без использования сторонних библиотек и кода

Что делает KasperskyOS безопасной?

«Врожденная» безопасность KasperskyOS заложена в ее архитектуре и философии. В основе операционной системы — собственный подход «Лаборатории Касперского» к разработке кибериммунных IT-продуктов.

Кибериммунитет обеспечивается разделением IT-системы на изолированные части и контролем взаимодействий между ними. На этапе проектирования продукта задаются политики безопасности, которые описывают каждое разрешенное действие. Запускаться и работать может только то, что разрешено администраторами системы и разработчиками приложений.

Операционная система KasperskyOS в совокупности с методологией разработки IT-продуктов служит эффективной и надежной основой для создания доверенных информационных систем, обладающих иммунитетом в отношении киберугроз.

Особенности архитектуры

KasperskyOS разработана в соответствии с известными и хорошо задокументированными архитектурными концепциями, подходами и принципами, а также собственными технологиями безопасности «Лаборатории Касперского».

Операционная система позволяет гибко задавать политики безопасности — правила, которым будет следовать IT-система на протяжении жизненного цикла и которые не дадут ей выполнять потенциально опасные операции.

Компоненты KasperskyOS разделены на изолированные домены безопасности, которые не могут взаимодействовать напрямую. Все их взаимодействия проходят через микроядро, а подсистема Kaspersky Security System проверяет их и выносит вердикты безопасности каждому. Любое действие, не разрешенное политикой безопасности напрямую, будет заблокировано еще до выполнения.

Благодаря этому при разработке на нашей ОС можно использовать и недоверенные компоненты, не обладающие кибериммунитетом. Даже в случае взлома недоверенного компонента, злоумышленник не сможет развить атаку и повлиять на работу системы.



KasperskyOS

Подробнее на os.kaspersky.ru

www.kaspersky.ru

© 2022 АО «Лаборатория Касперского»
Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.