KasperskyOS

Кибериммунная операционная система для отраслей с повышенными требованиями к информационной безопасности

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, 39,61% компьютеров АСУ в 2021 г. было атаковано вредоносным ПО

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.

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

Решение

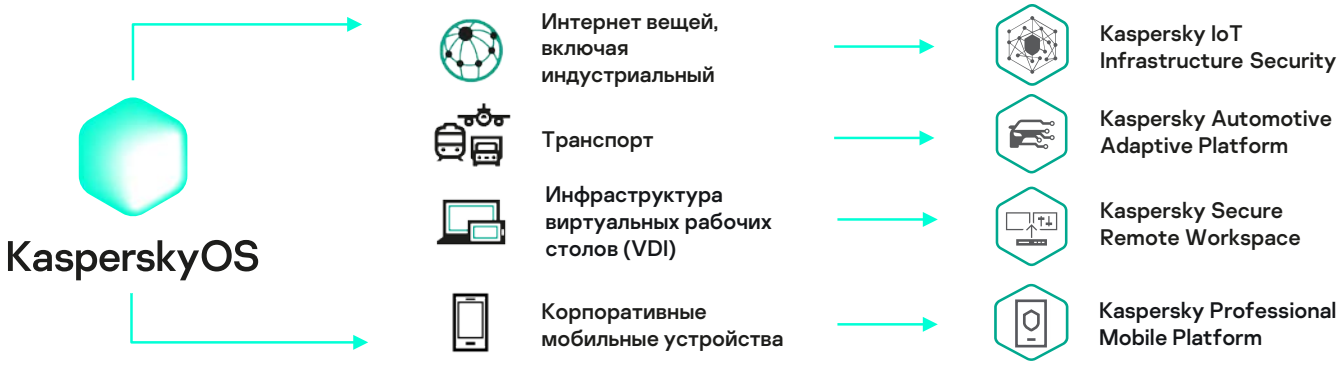
В качестве ответа на современные реалии «Лаборатория Касперского» разработала собственную операционную систему KasperskyOS.

Благодаря особенностям архитектуры, на базе KasperskyOS можно создавать IT-продукты, обладающие кибериммунитетом – встроенной защищенностью от подавляющего большинства типов кибератак. Такие продукты практически невозможно взломать и повлиять на выполнение ими критичных функций, они продолжают надежно функционировать даже в условиях агрессивной среды.

Решениям, построенным на KasperskyOS, не нужны дополнительные (наложенные) средства безопасности – все необходимое уже есть внутри системы.

Области применения

KasperskyOS применяется в отраслях, где существуют повышенные требования к кибербезопасности, надежности и предсказуемости работы IT-систем, например, в промышленности, энергетике, транспортной инфраструктуре, в системах умного города. Она позволяет обеспечить конфиденциальность и целостность данных и обезопасить их от подмены.



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.

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 концепциями, подходами и принципами, включая MILS и FLASK, а также собственными технологиями безопасности «Лаборатории Касперского».

Операционная система позволяет гибко задавать политики безопасности – правила, которым будет следовать 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.

Методология разработки

Для разработки кибериммунного продукта на базе KasperskyOS необходимо следовать специальной методологии:

- четко определить цели безопасности (например, конфиденциальность данных), а также условия, в которых будет эксплуатироваться система;
- разделить решения на изолированные домены безопасности, учитывая функциональность и степень доверия к каждому из них;
- обеспечить контроль информационных потоков между этими доменами, разрешая только заданные виды взаимодействий.

KasperskyOS предоставляет необходимые интерфейсы, механизмы и инструменты для разработки кибериммунных решений, включая изоляцию доменов безопасности и контроль взаимодействий между ними.

KasperskyOS

Подробнее на os.kaspersky.ru

www.kaspersky.ru