kaspersky BRING ON THE FUTURE

A Cyber Immunity-based approach to information system security

KasperskyOS®

When it comes to securing information technologies used by individuals, wider society and the state, the most important thing is the credibility of existing and emerging information systems.

KasperskyOS is a basis for a Cyber Immunity approach that allows any IT system to perform its functions in an aggressive environment without additional (superimposed) security features.

Kaspersky has long been working on the problem of how to create a trusted information system out of untrusted components. The results of this work have been implemented in the Kaspersky operating system, which is designed to serve as the basis for IT systems with high information security requirements.

As a rule, IT system design does not take into account the impact of adverse factors such as undeclared software or hardware capabilities, malware, bad guy attacks, etc. To ensure successful operation in a real-life environment, these systems need to be equipped with antivirus programs, firewalls and other superimposed protection. This leads to complicated systems and leaves them vulnerable to external attacks, because, once an attacker has overcome the protective barrier, he finds himself in an unprotected space where all sorts of destructive activity can be performed.

Key technologies

The following key technologies can be highlighted in KasperskyOS:

KasperskyOS – a microkernel operating system based on a unique microkernel with advanced security features developed from scratch by Kaspersky specialists.

Kaspersky Security System – a security policy verdict computation engine capable of working simultaneously with different types of security policies (role-based and mandatory access control, temporal logic, control flow, type enforcement, etc.).

Kaspersky Secure Hypervisor – a Type 2 hypervisor that runs on the KasperskyOS microkernel. The main benefit of a virtualization solution is the separation of potentially untrusted guest operating systems from each other and from critical services collocated on the same physical machine, reducing the attack surface and minimizing the possible impact of exploited vulnerabilities.

KasperskyOS, together with methodology for developing and porting applications, serves as an effective and reliable foundation for developing trusted information systems for various purposes and complexities that are Cyber Immune to cyberthreats.

Recommendations for the development of IT systems

To implement the Cyber Immunity-based approach, an IT system needs to be developed that takes the following recommendations into account:

- First, it's necessary to develop a threat model, and on the basis of that to form a security policy.
- The system needs to be designed in accordance with the threat model and security policy, with separate trust domains – areas with the same attributes relative to the security policy.
- All interactions between trust domains should be transparent and monitored for compliance with the security policy.
- The controlling component should be as compact as possible so that it itself can be verified.

If you follow these recommendations, you can embed untrusted components in an information system by placing the necessary restrictions on them. This will significantly reduce the risk of any negative impact an untrusted component may have on the security of the system as a whole. It should be noted that the above recommendations need to be taken into consideration not only when designing new systems but also when modernizing existing systems.

These and other secure development principles are implemented in KasperskyOS. Moreover, a methodology has been created that allows the effective use of KasperskyOS, and core technologies based on it, in the industrial development and adaptation of hardware drivers, in operating system-level services and in various user-level applications.

Main applications of KasperskyOS

- Logic controllers for:
  - Transport systems
  - ICS
  - Energy systems
- Internet of things
- Automobiles
- Network equipment
- Embedded electronics
- Trusted workstations for working with confidential information

KasperskyOS®

Read more on os.kaspersky.com

www.kaspersky.com