

СЕКЦИЯ 3. ЗАЩИТА ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ И ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ

INFORMATION SECURITY FOR SCADA-SYSTEMS

Kamiel Iehab Abduljabbar Kamil, N. Nasonova

Supervisory Control and Data Acquisition System (SCADA) is an emerging application for industrial automation. It is being widely used in critical infrastructure for monitoring and controlling the activities. The collaborative environment and interconnectivity of SCADA system needs communications and transmission of sensed real time data like status of machines, breaks and leakages in the system across various devices in the industrial plant. Such real time data provoke security breaches to SCADA systems and results in compromise of availability, integrity, confidentiality and trust relationship between the devices of SCADA systems. As the numbers of deliberate cyber-attacks on these systems are increasing, providing a scheme to identify malicious activities and defend the attacks; thereby create secure environment for SCADA systems is an essential task. By considering constraints and efficiency requirements for such networks this article outlines the scheme that we have developed as a countermeasure to prevent information leakage through eavesdropping on emanations emitted by personal computers (PCs). It also describes the present performance of our current prototype.

The main information security threats for SCADA-systems include primarily failures of equipment and data transmission systems (up to 95% of all the cases), power supply systems and other components of the system. Mistakes of personnel are also significant, as they result in improper processing or failures in SCADA-systems. A specificity of SCADA-systems is a low level of data confidentiality in an information system. Thus, the intentional threats for information security are caused by the outside and inside malefactors, affecting the information system availability, such as DoS-attacks (overloading of the system) or hackers, practicing to compromise the systems.

Countermeasures involve physical security of SCADA-system and its separated data channels, alternative power supply. Organizational and technical measures for network security in SCADA-systems are aimed at preventing an unauthorized access and intrusions into the network and users' activity control through logs and journals auditing.

Data center of a SCADA-system is the most critical component of the information system. Its security against different types of technical attacks should be considered. Compromising emanations are mostly unexplored in the research literature. The cheap software radios-universal receivers in which all demodulation of the signal after the intermediate frequency conversion is done completely in software on high-speed DSPs will allow low-budget attackers to implement sophisticated Tempest attacks. The security of such critical systems also should include protection against the impact of intensive electromagnetic pulsed radiation, which damages the semiconductor elements of radio electronic equipment by inducing extremely strong currents in the circuits. These threats set the requirement to the data center of a SCADA-system to be protected against electromagnetic radiation traveling inside or outside the secure area, containing the data center. An optimal way to fulfill this requirement is shielded premises arrangement for the data center, as well as preferable use of fiber optics and electric filtering for the cablings of the data center.

МЕТОДИКА ОЦЕНКИ ЭФФЕКТИВНОСТИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ОПТИЧЕСКИМ КАНАЛАМ

Алавси Хайдер Али Хуссейн, М.В. Рушакович, Т.В. Борботько, В.В. Лобунов

Для обнаружения объектов используются технические средства, которые функционируют в различных диапазонах длин волн, например оптико-электронные системы видимого и ближнего инфракрасного диапазонов. Анализ изображений, получаемых с