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. Русакович, 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

помощью таких технических средств, включает в себя следующие взаимосвязанные этапы: обнаружение, идентификацию и опознавание объекта наблюдения.

На практике, при обнаружении объекта освещенность местности (фона), где он расположен, может создавать экспозицию (освещенность) фотоприемника выше пороговой, поэтому на первый план выходит задача обнаружения объекта с минимальным контрастом относительно фона. В соответствие с чем, важным показателем является контрастная чувствительность оптико-электронной системы, которая определяется минимально необходимым контрастом объекта наблюдения, который может быть обнаружен при пороговом отношении сигнал/шум фотоприемника оптико-электронной аппаратуры.

Для снижения заметности объекта наблюдения используются различные способы его скрытия, которые реализуются на практике за счет использования средств защиты. Одним из подходов в оценке эффективности средств защиты является их натурные испытания, при которых объект наблюдения скрывается с помощью средства защиты и выполняется процедура его обнаружения с использованием оптико-электронной системы обнаружения. Такой подход требует значительных финансовых и временных затрат, а полученный результат оценки эффективности соответствует тем условиям, при которых проводился такой натурный эксперимент.

Отдельные элементы оптического изображения, получаемого с помощью оптико-электронной системы, могут отличаться по яркости, цвету, размеру, геометрической форме, поэтому условием обнаружения объектов является их контраст по выше перечисленным параметрам. Наиболее важным из которых является контраст по яркости.

Возникновение контраста по яркости между объектом и фоном обусловлено отражением объектом и фоном, на котором он размещается оптического излучения, в результате чего объект может быть темнее или светлее фона. Защита информации от утечки по оптическим каналам обеспечивается с использованием средств защиты (маскировочного окрашивания, оптических искусственных масок и т.д.). Их спектральный коэффициент яркости (СКЯ) должен соответствовать аналогичному параметру окружающего фона, на котором обеспечивается скрытие объекта, что позволит существенно снизить демаскирующие признаки объекта. Для оценки их эффективности предлагается использовать следующую методику.

Исследования КСЯ средств защиты выполняется на лабораторном стенде, который содержит источник оптического излучения видимого и ближнего инфракрасного диапазона длин волн и аппаратуру позволяющую обеспечить регистрацию СКЯ при различных углах падения и отражения оптического излучения источника. В результате первого этапа записываются СКЯ исследуемого средства защиты, обработка которых позволяет рассчитать степень поляризации отраженного оптического излучения средством защиты.

На втором этапе рассчитываются дальности обнаружения, опознавания и идентификации объекта наблюдения, скрытого с помощью исследуемого средства защиты, с учетом возможных погодных условий наблюдения и основных технических характеристик телевизионной техники.

Полученные результаты дают возможность проанализировать эффективность исследуемого средства защиты для выбранного варианта применения и разработать рекомендации по его дальнейшему использованию и совершенствованию.

РАСПРЕДЕЛЕНИЕ КЛЮЧЕВОЙ ИНФОРМАЦИИ В СОВРЕМЕННЫХ КРИПТОСИСТЕМАХ

Алхалбус Муаяд Абдулкадес Аббас, В.Ф. Голиков

Современные криптосистемы строятся таким образом, что их надежность обеспечивается стойкими криптографическими алгоритмами взлом, которых без знания секретных параметров, называемых ключевой информацией, даже с использованием самых