Аутентификация в информационно-управляющей системе робототехнического комплекса

УДК 004.056

В.Е. ЕРМОЛАЕВ, адъюнкт кафедры безопасности инфокоммуникационных систем специального назначения ФГКВОУ ВО "Военная орденов Жукова и Ленина Краснознаменная академия связи имени Маршала Советского Союза С.М. Буденного" Минобороны РФ, О.М. ЛЕПЕШКИН профессор кафедры безопасности инфокоммуникационных систем специального назначения доктор технических наук, Ю.К. ХУДАЙНАЗАРОВ, докторант кафедры безопасности инфокоммуникационных систем специального назначения кандидат технических наук

Аутентификация в информационно-управляющей системе робототехнического комплекса
Authentication in the information and control system of a robotic complex

В статье рассмотрены технологии аутентификации, применимые в информационно-управляющей системе робототехнического комплекса специального назначения.

Показано, что для робототехнического комплекса аутентификация должна рассматриваться не только как процедура допуска оператора к автоматизированному рабочему месту, но и как сквозной процесс подтверждения подлинности субъектов доступа, программно-аппаратных компонентов, каналов связи, команд управления, телеметрических сообщений и обновлений программного обеспечения. Обоснована необходимость многоуровневой архитектуры аутентификации, включающей многофакторную аутентификацию оператора, криптографическую аутентификацию устройств, контроль подлинности сообщений, доверенную загрузку и непрерывную переоценку доверия в процессе функционирования комплекса.

Предложена обобщенная модель аутентификации для информационно-управляющей системы робототехнического комплекса специального назначения, учитывающая требования достоверности, оперативности, устойчивости к отказам и защищенности от несанкционированного доступа.

The article considers authentication technologies applicable to the information and control system of a robotic complex.

It is shown that authentication in such systems should be considered not only as a procedure for granting an operator access to an automated workstation, but also as an end-to-end process of verifying the authenticity of access subjects, hardware and software components, communication channels, control commands, telemetry messages and software updates. The necessity of a multi-level authentication architecture is substantiated, including multi-factor operator authentication, cryptographic authentication of devices, message authentication, trusted boot and continuous trust reassessment during system operation.

A generalized authentication model for the information and control system of a robotic complex is proposed, taking into account the requirements of reliability, timeliness, fault tolerance and protection against unauthorized control.

Ключевые слова: роботизированный и робототехнический комплекс, информационно-управляющая система, аутентификация, идентификация, многофакторная аутентификация, криптографическая защита, доверенная загрузка, контроль доступа, военная робототехника.

Keywords: *robotic complex, information and control system, authentication, identification, multi-factor authentication, cryptographic protection, trusted boot, access control, military robotics.*

Введение

Современные робототехнические комплексы специального назначения (РТК СН) являются сложными киберфизическими системами, в которых программные, аппаратные, коммуникационные, сенсорные и исполнительные компоненты объединяются в единую информационно-управляющую систему. Такая система обеспечивает сбор и обработку данных, передачу команд управления, получение телеметрии, контроль состояния исполнительных механизмов и взаимодействие оператора с роботизированной платформой.

В условиях применения РТК СН особую значимость приобретает обеспечение достоверности субъектов и объектов информационного взаимодействия.

Статью целиком читайте в бумажной версии журнала