Горун Олег Максимович
студент
Научный руководитель
Сомова Марина Валериевна
доцент

Институт космических и информационных технологий
ФГАОУ ВО «Сибирский федеральный университет»
г. Красноярск, Красноярский край

КИБЕРБЕЗОПАСНОСТЬ В РОБОТОТЕХНИКЕ: УСТОЙЧИВОСТЬ И ЗАЩИТА В НОВОМ ЦИФРОВОМ МИРЕ

Аннотация*: в работе представлен систематизированный обзор основных уязвимостей, которые характерны для роботов и роботизированных систем, а также проведён анализ современных методов их защиты от угроз кибербезопасности. Рассмотренные уязвимости роботов включают вредоносное программное обеспечение, атаки типа «отказ в обслуживании», манипуляции данными, недостаточную аутентификацию, слабое шифрование и уязвимости сетевой инфраструктуры. Особое внимание уделено решениям, применимым в контексте промышленных, медицинских и бытовых роботизированных систем, с акцентом на рекомендации по эффективному противодействию кибератакам. Рассмотрены основные тенденции развития киберугроз и новые подходы, а также стратегии для совершенствования защиты роботизированных систем.*

Ключевые слова*: кибербезопасность, киберугрозы, роботы, ROS, робототехника.*

Современное общество стремительно движется к интеграции робототехники в повседневную жизнь и промышленность, при этом кибербезопасность становится важнейшим аспектом, определяющим успешность этого процесса. Беспилотные транспортные средства, промышленные роботы и системы

автономной навигации подвержены многим киберугрозам, реализация которых нарушает функционирование систем.

Кибербезопасность в робототехнике – многослойная задача, включающая защиту оборудования, сетей, программного обеспечения (ПО) и данных. Угрозы включают атаки через незащищённые сети, манипуляции с данными, вредоносные программы, а также DoS- и DDoS-атаки. Особое внимание уделяется операционной системе роботов – Robot Operating System (ROS).

В критически важных сферах, таких как здравоохранение и защита данных, обеспечение безопасности особенно важно, поскольку сбои могут угрожать жизни людей и инфраструктуре. К основным угрозам относятся вредоносные программы, уязвимости сетевого и аппаратного обеспечения [1].

ROS подвержена уязвимостям как в ПО, так и в аппаратных компонентах. Центральный узел может стать точкой отказа, а недостаток контроля за поведением узлов открывает возможности для атак, включая спуфинг, DoS и повышение привилегий, ведь любой узел может подписываться на данные и передавать их без ограничений, что делает систему уязвимой [2]. Интегрированная система защиты, способная выявлять уязвимости, контролировать узлы и реагировать на атаки в реальном времени и децентрализованный подход и гибкие методы защиты значительно повышают безопасность этого ПО.

ROS 2.0 и ROS-M предлагают улучшенную защиту, включая продвинутое шифрование и адаптацию для военных задач [3]. Современные методы, основанные на биологических моделях, позволяют лучше адаптироваться к угрозам. Искусственные нейронные сети помогают обнаруживать аномалии, распознавать угрозы и анализировать большие объемы данных.

Следует уточнить, что роботы функционируют не только в сетевом пространстве, но и в физическом, что позволяет им взаимодействовать с окружающей средой. Это взаимодействие порождает проблемы, касающиеся потенциального ущерба как окружающей среде, так и производственным процессам. К тому же следует выделить в отдельную категорию медицинских роботов, которые могут непосредственно угрожать здоровью человека.

Современные роботизированные хирургические системы становятся всё более распространёнными благодаря их высокой точности, улучшенной визуализации и возможностям удалённого управления. Однако такие системы также подвержены кибератакам, которые могут привести к физическому ущербу пациентам, нарушению операций из-за потери связи или задержек, а также к утечкам персональных данных [4]. Медицинские роботы, уязвимы перед кибератаками, которые могут привести к физическому ущербу, сбоям в работе и утечкам данных. Основные угрозы включают DDoS-атаки, перехват данных, атаки «человек посередине» и уязвимости облачных платформ. Дополнительные риски связаны с человеческим фактором, ошибками эксплуатации и устаревшим ПО.

Для минимизации рисков необходимы регулярные обновления, шифрование, защита сетей, обучение персонала и сотрудничество с производителями.

Дополнительно следует развивать исследования в области киберпреступлений, связанных с медицинской робототехникой, особенно в анализе данных и доказательств на базе ROS.

Список литературы

1. Bhardwaj A. Cyber security attacks on robotic platforms / A. Bhardwaj, V. Avasthi, S. Goundar // Network Security. – 2019. – №10. – DOI 10.1016/S1353-4858(19)30122-9. – EDN FEVLVX

2. Rivera S. Securing Robots: An Integrated Approach for Security Challenges and Monitoring for the Robotic Operating System (ROS) / S. Rivera, R. State // Proceedings of the IFIP/IEEE International Symposium on Integrated Network Management. – 2021. – P. 754–759.

3. Santoso F. An In-Depth Examination of Artificial Intelligence-Enhanced Cybersecurity in Robotics, Autonomous Systems, and Critical Infrastructures / F. Santoso, A. Finn // IEEE Transactions on Services Computing. – 2024. – №17 (3). – P. 1293–1310.

4. Gordon W. J. Protecting procedural care-cybersecurity considerations for robotic surgery / W.J. Gordon, N. Jkoma, H. Lyu, G.P. Jackson, A. Landman // npj Digital Medicine. – 2022. – №5. – 148 p. – DOI 10.1038/s41746-022-00693-8. – EDN JGTSKJ