ПРОБЛЕМЫ КИБЕРБЕЗОПАСНОСТИ В РОБОТОТЕХНИКЕ

И.Ю. Изгачёв, М.А. Климович, А.И. Гридасов, А.А. Григорьев

Роботы используются уже более 50 лет в разных сферах деятельности человека: экономике, производстве, логистике, военном деле. Как и в случае других встроенных систем, производители робототехники уделяют первостепенное внимание безопасности, стоимости разработки, скорости выхода на рынок и предоставлению функций клиентам. Кибербезопасность имеет более низкий приоритет потому, что безопасность не является основным фактором для клиентов [1].

Роботы представляют собой встроенные системы и могут быть подвержены тем же типам кибератак, что и другие встроенные системы, а именно аппаратным атакам при изготовлении подобных систем, а также во время их использования.

Так, в штате Калифорния разрешили тестирование автомобилей, для которых водитель-человек не будет нужен даже в качестве запасного варианта. Этим транспортным средствам не обязательно иметь рулевое колесо, педаль тормоза или газа [2]. Подобные машины, смогут получать обновления программного обеспечения удаленно через Интернет. Гипотетическая атака будет состоять из двух частей: получение доступа к беспроводной системе обновления ПО автомобиля, дальнейшей загрузке в сеть измененной версии прошивки автомобиля, возможно, такой, которая позволит дистанционно управлять транспортным средством. Теперь злоумышленник контролирует легион автоматизированных автомобилей.

Военные дроны - это беспилотные летательные аппараты (БПЛА), дистанционно управляемые пилотом, их можно использовать для наблюдения и нападения на вражеские цели. Эти дроны могут быть модифицированы противником при изготовлении или транспортировке их частей. Модификации могут включать в себя удаленный выключатель, который позволит в определенный момент времени отключить дроны.

Согласно исследованию World Robotics 2019, к концу 2017 года насчитывалось около 2,44 млн. промышленных роботов [3]. Атака на предприятие может начаться с зараженного письма, которое устанавливает вредоносное ПО в корпоративной сети, позволяющее нарушителю напрямую управлять промышленными роботами, что может привести к их повреждению или уничтожению.

Литература

1. Mirjalili S.H., Lenstra A.K. Security observance throughout the life-cycle of embedded systems // Proceedings of the 2008 International Conference on Embedded Systems and Applications, ESA 2008. – 2008. – P. 186–192.

2. Baron E. Fully autonomous cars get lift from gov. jerry brown [Electronic resource]. – Access mode: http://www.mercurynews.com/2016/09/29/fullyautonomous-self-driving-cars-get-lift-from-governor. – Date of access: 10.05.2020.

3. Hagerty J. Meet the new generation of robots for manufacturing // Wall Street Journal. – 2015. – P. 3–4.