DOI: 10.37791/2687-0649-2025-20-6-121-142

Подход к обнаружению атак модификации цифровых 3D-моделей на умных аддитивных производствах

А.В. Мелешко[1]***, В.А. Десницкий***[1*]***, И.В. Котенко***[1]
[1]*Санкт-Петербургский федеральный исследовательский центр Российской академии наук, Санкт-Петербург, Россия*
[*]*desnitsky@comsec.spb.ru*

Аннотация. Работа посвящена исследованию вопросов обнаружения атак модификации цифровых моделей изделий (деталей), предназначенных для 3D-печати в современных комплексах интеллектуальных аддитивных производств. В общем случае такие системы представляют собой сети, включающие множество параллельно функционирующих 3D-принтеров (3D-фермы), способные по запросам пользователей печатать тиражи изделий, таких как элементы физических конструкций роботов и транспортных средств, лопасти беспилотных летательных аппаратов и другие детали из пластика, металла и иных материалов. Существующие примеры таких 3D-установок оказываются уязвимыми к действиям атакующих, пытающихся, воздействуя на цифровую модель, внести в нее скрытую несанкционированную модификацию. После такой атаки готовые изделия могут оказаться с конструктивным дефектом, но их визуальные характеристики будут почти неотличимы от оригинальных образцов таких изделий. Например, осуществив воздействие на дефективный элемент корпуса БПЛА, атакующий способен понизить его управляемость и даже привести к его разрушению. В работе проводится экспериментальное обоснование гипотезы о возможности обнаружения атак модификации цифровых моделей изделий на основе обработки и анализа программного кода таких моделей. Анализируются особенности дефектов моделей 3D-изделий, представленных на языке G-кодов и отобранных из открытых баз 3D-моделей. Сформирован набор данных, состоящий из оригинальных и модифицированных моделей изделий. Предложен подход к обнаружению модификаций с применением эмбеддинга для преобразования данных в числовые векторы и обучения на них классификаторов с использованием методов обучения с учителем. Эксперименты на тестовых выборках данных продемонстрировали работоспособность предложенного подхода к обнаружению модификаций и перспективность его дальнейшего развития и применения на практике.

Ключевые слова: кибербезопасность, 3D-модель, обнаружение, дефекты, умные аддитивные производства, атаки

Для цитирования: *Мелешко А.В., Десницкий В.А., Котенко И.В.* Подход к обнаружению атак модификации цифровых 3D-моделей на умных аддитивных производствах // Прикладная информатика. 2025. Т. 20. № 6. С. 121–142. DOI: 10.37791/2687-0649-2025-20-6-121-142

An approach to detection of modification attacks on digital 3D models in smart additive manufacturing

A. Meleshko[1], ***V. Desnitsky***[1*], ***I. Kotenko***[1]
[1]*St. Petersburg Federal Research Center of the Russian Academy of Sciences, Saint Petersburg, Russia*
[*]*desnitsky@comsec.spb.ru*

Abstract. The paper presents a study of the issues of detecting attacks on modification of digital models of products (details) intended for 3D printing in modern intelligent additive manufacturing systems. In general, such systems are networks that include multiple 3D printers (i. e. 3D farms) operating in parallel, capable of printing series of products at user requests, for instance elements of physical structures of robots and vehicles, blades of unmanned aerial vehicles and other parts made of plastic, metal and other materials. Existing examples of such 3D installations are vulnerable to the actions of attackers who try to make a hidden unauthorized modification by influencing digital models. After such an attack, end products may have a design defect with visual characteristics that are almost indistinguishable from the original sample of such a product. For instance, by influencing a defective element of the UAV body, an attacker may reduce its controllability and even lead to its crash. The paper considers an experimental substantiation of the hypothesis on the possibility of detecting modification attacks on digital models of products based on processing and analysis of the program code of such models. The features of defects in 3D product models presented in the G-code language and selected from open 3D model databases are analyzed. A data set consisting of original and modified product models is compiled. An approach to modification detection using embedding to transform data into numerical vectors and train classifiers on them using supervised learning methods is proposed. Experiments on test data samples demonstrated the feasibility of the proposed approach to modification detection and the prospects for its further development and application in practice.

Keywords: cyber-security, 3D models, detection, defects, smart additive manufacturing, attack

For citation: Meleshko A., Desnitsky V., Kotenko I. An approach to detection of modification attacks on digital 3D models in smart additive manufacturing. *Prikladnaya informatika*=Journal of Applied Informatics, 2025, vol.20, no.6, pp.121-142 (in Russian). DOI: 10.37791/2687-0649-2025-20-6-121-142

Введение

Области применения аддитивного производства и 3D-печати в частности расширяются с каждым днем. 3D-печать используется для производства деталей для водоочистки, бытовых изделий для свободной продажи, производства комплектующих и запасных частей для различных устройств, например беспилотных летательных аппаратов (БПЛА), турбин реакторов и даже для производства продуктов питания [1, 2]. Атаки со стороны злоумышленников на такие производства могут приносить финансовые убытки владельцам производств, а также приводить к катастрофическим последствиям. Исследователями отмечается слабая защита 3D-принтеров,