УДК 004.056

Обзорная статья

https://doi.org/10.32603/2071-8985-2026-19-2-25-39

Информационная безопасность 3D-производств: актуальные атаки и подход к их обнаружению

А. В. Мелешко

Санкт-Петербургский Федеральный исследовательский центр Российской академии наук, Санкт-Петербург, Россия

meleshko.a@iias.spb.su

Аннотация. Вопросы безопасности 3D-производств актуальны на сегодняшний день ввиду широкого применения таких производств, а также вариативности различных атак на них. Цель настоящей статьи – анализ атакующих воздействий, значимых для области 3D-печати, и разработка подхода к их обнаружению. Проанализированы и описаны различные атаки на аддитивные производства, которые упоминаются в релевантных работах начиная с 2016 г., а также предложен подход к обнаружению данных атак. Подход состоит из четырех этапов, каждый из которых направлен организацию процесса обнаружения атак на 3D-производства. Отличительная особенность подхода – его универсальность, т. е. возможность применения на любых аддитивных производствах. В рамках данной статьи была проведена реализация одного из этапов подхода, а именно был проведен анализ и систематизация атак, актуальных для области 3D-печати, определены механизмы реализации выделенных атак, а также проанализированы данные для их обнаружения.

Ключевые слова: аддитивные производства, 3D-печать, безопасность, атаки на 3D-принтеры

Для цитирования: Мелешко А. В. Информационная безопасность 3D-производств: актуальные атаки и подход к их обнаружению // Изв. СПбГЭТУ «ЛЭТИ». 2026. Т. 19, № 2. С. 25–39. doi: 10.32603/2071-8985-2026-19-2-25-39.

Финансирование: Работа выполнена при частичной финансовой поддержке бюджетной темы FFZF-2025-0016.

Review article

Information Security for 3D Manufacturing: Current Attacks and Approaches to Their Detection

A. V. Meleshko

St. Petersburg Federal Research Center of the Russian Academy of Sciences, Saint Petersburg, Russia

meleshko.a@iias.spb.su

Abstract. Security issues in 3D production are relevant today, due to the widespread use of such production, as well as the variability of various attacks on them. The purpose of this paper is to analyze attack vectors relevant to 3D printing and develop an approach for their detection. This paper analyzes and describes various attacks on additive manufacturing, cited in relevant studies since 2016, and proposes an approach for detecting these attacks. The approach consists of four stages, each aimed at organizing the process of detecting attacks on 3D manufacturing systems. A distinctive feature of the approach is its versatility, meaning it can be applied to any

additive manufacturing process. This article completed one stage of the approach. Specifically, we analyzed and systematized attacks relevant to 3D printing, identified the mechanisms for implementing the identified attacks, and analyzed the data for their detection.

Keywords: additive manufacturing, 3D printing, security, attacks on 3D printers

For citation: Meleshko A. V. Information Security for 3D Manufacturing: Current Attacks and Approaches to Their Detection // LETI Transactions on Electrical Engineering & Computer Science. 2026. Vol. 19, no. 2. P. 25–39. doi: 10.32603/2071-8985-2026-19-2-25-39.

Funding: The work was carried out with partial financial support from the FFZF-2025-0016 budget theme.

Введение. Область аддитивных производств и 3D-печати развивается с каждым днем. С помощью 3D-печати производят различные изделия для промышленности – турбины, винты летательных аппаратов, лопасти [1] и др. Также она применяется для производства пищевых продуктов [2] или же в биоинженерии [3]. 3D-печать представляет собой послойное создание объемного изделия методом экструзии. В качестве материалов для печати могут использоваться различные материалы, например пластик для легких деталей или же бетон для печати конструкций модульного строительства зданий [4].

Обобщенная схема процесса создания изделий на 3D-производствах показана на рис. 1. Алгоритм печати изделий состоит из нескольких шагов (рис. 1). Первым шагом служит создание 3D-модели изделия. Модель создается в системах автоматизированного проектирования (САПР), например Компас-3D или AutoCAD. На втором шаге 3D-модель нарезается на слои (слайсинг) с использованием программ слайсинга (например, PrusaSlicer) и преобразуются G-код печати. G-код представляет собой набор команд для принтера, которыми описываются все важные параметры печати – температура, скорость печати, траектория печати и др. На третьем шаге полученный G-код загружается на компьютер, с которого осуществляется управление 3D-принтером и процессом печати. Последний, четвертый шаг – это последовательная отправка команд печати из файла с G-кодом (G-команд) от управляющего компьютера на 3D-принтер. Передача команд осуществляется либо по USB-каналу связи, либо по локальной сети производства с использованием TCP (если 3D-принтер поддерживает сетевые подключения).

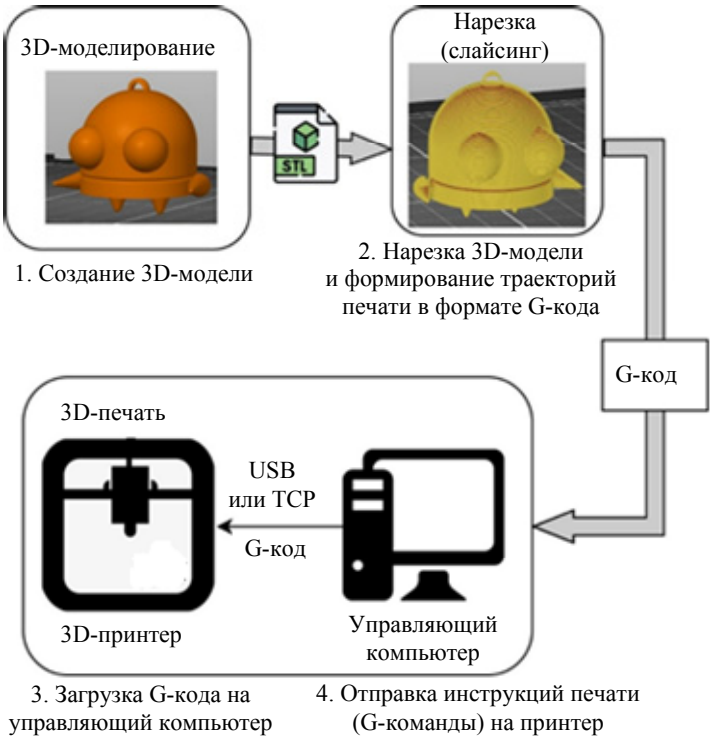

Рис. 1. Обобщенная схема создания изделий на 3D-производствах
Fig. 1. Generalized scheme for creating products in 3D manufacturing

На каждом из описанных шагов создания изделия возможна реализация различных атак, которые будут нарушать данный процесс. Например, при передаче G-кодов печати от управляющего компьютера 3D-принтеру возможна их модификация [5], которая приведет к появлению дефектов в готовом изделии. Последствия таких дефектов могут быть катастрофическими, особенно если на производстве печатаются, например, элементы силовых конструкций зданий. Подобные атаки модификации в литературе часто называют атаками саботажа. Кроме того, модифицировать G-код можно и на шаге нарезки или загрузки на управляющий компьютер. Отсутствие механизмов аутентификации пользователей, которые подключаются к 3D-принтерам, а также передача G-кода печати в открытом виде только увеличивает вероятность реализации атак саботажа и атак, направленных на нарушение конфиденциальности 3D-моделей как объекта интеллектуальной собственности. Поэтому важно правильно разработать и настроить механизмы защиты и безопасности аддитивных производств от возможных воздействий злоумышленников.

Вследствие сказанного цель настоящей статьи состоит в анализе атак, которым могут быть подвержены аддитивные производства, а также в разработке подхода к обнаружению атак на 3D-производствах. Вкладом данного исследования можно считать систематизацию атак на аддитивные производства, которые упоминаются различными исследователями за последние 10 лет, а также предложенный подход к их обнаружению. К элементам новизны предложенного подхода можно отнести модель атак, которая включает в себя наиболее актуальные для 3D-производств атаки, описывает возможные действия злоумышленника и пути реализации атак, а также систематизацию данных, необходимых для обнаружения выделенных атак с указанием мест сбора этих данных. Отличительная особенность подхода – его универсальность, а именно, возможность применения на любых аддитивных производствах вне зависимости от производителя используемых 3D-принтеров.

Обзор релевантных работ. Для всестороннего изучения вопросов безопасности 3D-производств, а именно изучения специфических для данной области атак, анализа данных, которые необходимы для их обнаружения и самих механизмов обнаружения, был проведен поиск и анализ релевантных работ. Для обзора отбирались зарубежные и отечественные статьи, посвященные описанию процессов реализации атак на аддитивные производства и отдельные 3D-принтеры, в частности.

[6] посвящена исследованию атак на 3D-принтеры по сторонним каналам с использованием смартфонов. В частности, атакам кражи интеллектуальной собственности, т. е. краже кода печати (G-кода) изделия. Под сторонними каналами связи авторы понимают акустический и магнитный каналы. В процессе печати электромоторы принтера издают звуки, а также излучают магнитное поле. Суть атаки, описанной авторами, заключается в расположении смартфона в непосредственной близости от работающего 3D-принтера, который записывает звук работы принтера и магнитное поле моторов осей. Данные записи позволяют восстанавливать траектории движения печатающего сопла (экструдера), – по сути, восстановить весь код печати (G-код) изделия. Авторами отмечается, что запись звуков работы принтера лучше проводить с помощью профессионального оборудования, но для записи магнитного поля достаточно обычного смартфона. В статье показан эксперимент, показывающий выполнимость описанных атак. Для эксперимента использовался смартфон Nexus 5 с операционной системой (ОС) Android OS 6.01 и 3D-принтер Ultimaker 2 Go. Экспериментальные результаты показали, что, используя сигналы побочных каналов, собираемые смартфоном, а именно магнитное поле моторов осей принтера, можно реконструировать G-код печатаемого изделия со средней погрешностью 5.87 % для простых и 9.67 % для сложных конструкций. Кроме того, в публикации описываются возможные механизмы защиты от атак по сторонним каналам связи – добавление случайных траекторий без расхода материала, манипуляции со скоростью печати, экранирование источников излучений и внедрение шума в излучения от 3D-принтера. Проведенное авторами исследование демонстрирует новую и практичную атаку на основе побочных каналов с использованием смартфона для компрометации интеллектуальной собственности во время 3D-печати.

В [7] авторы уделяют внимание вопросам онлайн-мониторинга процессов 3D-печати для предотвращения киберфизических атак, целью которых служит нарушение процесса печати. Авторы отмечают, что прочность, термостойкость, разме-

ры объектов, напечатанных на 3D-принтере, могут ухудшаться в результате злонамеренного изменения настроек печати. Предлагается подход к мониторингу процессов печати в режиме реального времени, который позволяет обнаружить киберфизические атаки на программное обеспечение (ПО) 3D-принтеров, а также реализовать защиту от таких атак. В качестве входных данных для предлагаемого подхода используются четыре основных параметра 3D-печати – траектория заполнения, скорость печати, толщина слоя и скорость вращения вентилятора. Контроль данных параметров осуществляется в реальном времени с помощью сторонних устройств (акселерометр, магнитометр и камера). Подход был экспериментально протестирован при печати сложной 3D-конструкции и результаты показали высокую эффективность подхода и его применимость для задач эффективной защиты принтеров от атак.

Авторы статьи [8] уделяют внимание стеганографическим атакам, которым могут подвергаться файлы для 3D-печати. Такие атаки подразумевают незаметное сокрытие какой-либо информации в файлах, в данном случае в файлах 3D-моделей (stl-файлы). Авторы провели исследования формата описания файлов 3D-моделей stl (STereoLithography) и выявили места, в которые возможно добавление зашифрованной информации (текст, сообщение), при этом сама модель не изменяется. Т. е. при открытии и печати модели в нее не вносится никаких дополнительных дефектов или элементов. Схематично алгоритм описываемой атаки можно представить следующим образом: отправитель шифрует сообщение; далее, с помощью предложенного авторами подхода, зашифрованное сообщение добавляется в stl-файл модели и данный файл отправляется получателю под видом обыкновенного файла модели; затем получатель имеет возможность восстановить зашифрованное сообщение и провести его расшифровку. В результате отправитель и получатель проводят обмен сообщениями по открытым каналам связи, но при этом сам факт обмена скрыт. Авторы провели эксперимент по скрытому внедрению сообщения в stl-файл модели с последующей печатью на 3D-принтере. Результаты показали, что печатаемая модель, в которую добавили зашифрованное сообщение, полностью соответствует исходной, что доказывает применимость предложенного подхода по реализации стеганографической атаки и подтверждает возможность реализации подобных атак применительно к файлам 3D-печати.

В [9] авторы рассматривают уязвимости и атаки на системы аддитивного производства, которые управляются с использованием шины CAN (Controller Area Network, локальная сеть контроллеров). Использование CAN имеет ряд преимуществ, например возможность легкого подключения к ней новых устройств, и выгодно отличается от других традиционных протоколов взаимодействия. Однако CAN имеет уязвимости, которые могут привести к нарушениям и сбоям, и обнаружить данные сбои непросто. Например, манипуляции с пакетами данных, несанкционированный сбор или перехват пакетом дают возможность злоумышленникам манипулировать всей информацией с датчиков, командами и создавать небезопасные условия работы, используя всего один скомпрометированный узел в сети CAN. Все это возможно из-за того, что протокол лишен различных механизмов аутентификации и для работы с шиной CAN злоумышленнику достаточно просто подключиться к ней. Авторы статьи рассматривают возможные атаки на аддитивные производства на базе CAN и их последствия. В основном атаки реализуют манипулирование передаваемыми данными, отключение различных систем и внедрение злонамеренных команд в шину. В качестве примера авторы смоделировали одну атаку, суть которой состояла в нарушении работы критически важных механизмов 3D-принтера (система подачи материала, охлаждение экструдера и прочие).

В [10] авторы рассматривают динамико-термические и локальные кинетические атаки на процесс 3D-печати. Суть данных атак заключается в манипулировании параметрами подачи и температуры материала для печати (например, пластикового прутка) с целью модификации механических свойств готового изделия. Авторы показывают примеры подобных модификаций – создание полостей в изделии с помощью манипуляций с процессом плавления пластикового прутка, изменение плотности изделия с помощью манипуляций скоростью печати, а также динамико-термические манипуляции, которые связаны с изменением температуры экструдера. Все описанные модификации вносят незаметные изменения в итоговое изделие, но негативно сказываются на его механических характеристиках. В статье приводится практическая реализация описанных модификаций изделий, представляющих собой

прямоугольные стержни, напечатанные на 3D-принтере. Для оценки влияния модификаций на свойства изделий авторы проводят механические испытания, которые показали, что подвергшиеся модификации стержни имеют заметные отклонения в физических свойствах пиковой нагрузке, напряжении при изгибе и деформации и др. Отдельно отмечается, что рассматриваемые атаки актуальны для множества современных принтеров.

В [11] авторы публикуют обсуждение развития области 3D-печати, а также рассматривают аспекты информационной безопасности в данной области. Подробно рассматриваются виды принтеров для 3D-печати и описаны разновидности процесса печати различных изделий. В плане безопасности авторы выделяют необходимость надежной зашиты канала передачи модели на принтер, а также защиты от таких внешних воздействий, как механические, вибрационные и электромагнитные воздействия. Отдельно отмечается необходимость обучения персонала для правильного и безопасного функционирования 3D-производств.

Авторы [12] рассматривают аспекты защиты 3D-принтеров от возможного возгорания. Разрабатывается трехфакторная система защиты, которая опирается на контроль температуры экструдера, а также постоянный мониторинг дыма в помещении с принтером. Анализ данных от этих датчиков реализован с помощью контроллера. Использование такой системы защиты от возгораний, которые могут быть вызваны действиями злоумышленников (например, намеренная модификация параметров работы принтера), позволяет повысить безопасность при работе с 3D-принтерами.

В [13] авторы уделяют внимание атакам кражи данных с 3D-принтеров и удаленному их использованию. В частности, рассматриваются уязвимости сетевого 3D-принтера производителя MakerBot Industries. Используя одноплатный компьютер Raspberry Pi 2, авторы подключились к сети, в которой работает принтер, и выявили три основные уязвимости: реализация https (HyperText Transfer Protocol Secure) между 3D-принтером и оператором не безопасна, так как проверка подлинности используемого сертификата SSL/TLS отсутствует; задания для печати (G-коды печатаемых моделей) передаются на принтер в незашифрованном виде и находятся в открытом доступе для любого устройства в локальной сети. Это означает, что злоумышленник, подключившись к локальной сети с 3D-принтерами, имеет возможность просматривать все печатаемые модели изделий, а также отправлять на принтеры собственные команды, тем самым реализуя атаку кражи данных интеллектуальной собственности и несанкционированное управление процессом печати. Данный факт был экспериментально подтвержден авторами статьи. Однако стоит отметить, что предложенная реализация атак справедлива только для сетевых 3D-принтеров. Кроме подтверждений о выполнимости указанных атак, авторы предлагают ряд контрмер по защите от них. А именно, организация защиты сети, к которой подключены 3D-принтеры, и подключение принтера к управляющему компьютеру оператора напрямую, минуя сеть, например через USB. Прямое подключение принтера может предотвратить прямые сетевые атаки на него, но не исключает возможности реализации иных атак.

Авторы [14] исследуют и классифицируют атаки на киберфизические цепочки поставок аддитивного производства. Под цепочками поставок понимается обширный процесс от закупки материалов и комплектующих для аддитивного производства до отправки готовой продукции конечному потребителю. Всего авторами выделено шесть этапов цепочки поставок и для каждого этапа выявлены возможные угрозы и атакующие воздействия. Выявленные угрозы авторы структурируют в виде таксономии атак, которая классифицирует их по трем ключевым параметрам: цели, объекты и методы. Под целями понимаются предполагаемые результаты, которых достигнет злоумышленник (по сути, сами атаки), под объектами понимается все, чем злоумышленник может воспользоваться для достижения целей, а под методами – тактика, которой будет пользоваться злоумышленник. Среди целей авторы выделяют кражу интеллектуальной собственности, несанкционированное производство изделий, модификацию данных, отказ в обслуживании и саботаж (манипуляции с качество изделия). В качестве объектов выделяются следующие: спецификация и дизайн 3D-изделия, готовые изделия, траектории движения при создании изделия, оборудование производства, цифровые 3D-модели, а в качестве методов реализации атак выделяют нарушение производственных процессов аддитивного производства, использование слабых мест производства и цепочки поставок в целом, обход систем защиты. Кроме таксономии атак авторы также предлагают несколько механизмов их смягчения – использование систем обнаружения

вторжений (для кибератак, предполагающих незаконное проникновение в сеть производства), использование подходов на основе искусственного интеллекта, а также применение технологии блокчейн для обеспечения целостности данных, что позволяет уменьшить количество случаев подмены изделий во время производства. Применимость предложенной таксономии атак была показана на примере реального аддитивного производства Strata Aerospace.

В [15] описывается метод обнаружения атак на аддитивные производства, основанный на применении средств видеозаписи процесса печати изделий на 3D-принтерах. Целью данного метода служит реализация механизма обнаружения атаки модификации G-кода печатаемого изделия. Такая модификация обычно направлена на искажение эксплуатационных характеристик готового изделия. Предложенный метод основывается на записи всего процесса печати изделия, т. е. записи траекторий движения печатающего сопла на каждом слое в процессе создания изделия. Затем полученная видеозапись разделяется на кадры и из кадров выделяются необходимые признаки, а именно проводится расчет отклонений траектории печати модифицированного изделия от нормального. Для дальнейшей классификации полученных признаков в качестве метода машинного обучения используется метод опорных векторов (SVM). Апробацию предложенного метода авторы проводили на стенде, состоящем из 3D-принтера и камеры, расположенной на его экструдере. Проведенные эксперименты показали, что метод, предложенный авторами, более эффективен по сравнению с такими подходами, как независимый компонентный анализ и сверточные нейронные сети. Кроме того, предложенный метод может работать в реальном времени.

В [16] описаны атаки саботажа (нарушения эксплуатационных свойств изделий, изготовленных на 3D-принтере) малой мощности. Под малой мощностью понимается то, что в процессе модификации изделия изменения в его конструкции незначительны и незаметны (в пределах допусков конкретного 3D-принтера), но изделие уже не будет иметь требуемых изначально механических и прочностных характеристик. В качестве основы для подобных атак авторы рассматривают атаку «человек посередине», суть которой заключается в подмене кода печати изделий (G-кода) в процессе его передачи от управляющего компьютера на сам принтер. Подмененный код содержит в себе модификации, которые искажают характеристики изделия. Такие модификации реализованы за счет нарушения процесса склейки слоев изделия между собой (как межслойной, так и в рамках одного слоя), а также нарушения склейки периметра изделия с его внутренним заполнением. Авторы провели натурное моделирование четырех разновидностей таких модификаций, которые незначительно меняют параметры склейки слоев изделия, и провели механические испытания напечатанных модифицированных и оригинальных образцов. Результаты показали, что несмотря на малые изменения изделия, данные атаки эффективны и снижают прочность на растяжение и изгиб до 25 %. Кроме реализации атак, авторы провели эксперименты по их обнаружению с помощью метода Sophos. Данный метод анализирует пространственно-временные и тепловые аномалии сразу после печати каждого слоя с помощью датчиков, которые отслеживают важные параметры печати, такие как положение печатающей головки и платформы, длина нити, а также температура сопла и платформы. Однако результаты обнаружения показали, что атаки обнаруживаются с большим количеством ложноотрицательных и ложноположительных срабатываний. В результате авторами был сделан вывод об актуальности и сложности точного обнаружения подобных атак саботажа.

Авторы [17] проводят разработку фреймворка FRoMEPP, который призван помочь в проведении цифровой криминалистической экспертизы для процесса 3D-печати. Авторы определяют данные, которые необходимо собирать в процессе печати изделия. В случае выходе изделия из строя собранные данные смогут помочь в локализации конкретного этапа производства, в котором был допущен дефект или была реализована атака. Выделяют следующие данные: журналы операционной системы управляющего компьютера, сетевой трафик, журналы приложений для создания и подготовки (нарезки) 3D-модели, журналы работы принтера, содержащие информацию о процессе печати (скорость подачи материала, температура и др.). Также в статье описываются методы сбора всех перечисленных данных.

В [18] описаны атаки, эксплуатирующие известную уязвимость программ по подготовке (нарезке) 3D-моделей к печати, с помощью которой злоумышленники имеют возможность манипулировать температурой при печати и внутренним заполнением изделия. Уязвимость связана с

тем, что программное обеспечение для нарезки моделей хранит G-код печати каждого слоя в динамической памяти, поэтому злоумышленник имеет возможности точечно его модифицировать, подключившись к локальной сети предприятия. В качестве мер по защите от подобных атак авторы выделяют строгую аутентификацию пользователей в сети и контроль доступа, а также обфускацию G-кода печати изделия.

В [19] описывается процесс реконструкции кода печатаемого на 3D-принтере изделия с помощью акустического канала. Суть подхода к реконструкции заключается в записи звуковой дорожки в процессе работы 3D-принтера и в использовании методов машинного обучения для самой реконструкции G-кода. Данный подход реализует атаку кражи интеллектуальной собственности и, по сути, выполняет прогнозирование последовательности команд G-кода из записей работы принтера. Авторы провели эксперименты по реконструированию кода печати, и результаты показали возможность восстановления G-кода с точностью до 78.35 % и средней погрешностью в 17 %.

Авторы статьи [20] описывают результаты своего исследования влияния скорости вращения вентилятора экструдера 3D-принтера на качество готового изделия. Кроме того, ими разработан плагин Fan Speed Attack Detection (FSAD), который позволяет в процессе печати обнаружить манипуляции со скоростью вентилятора, а также предсказать, приведут ли данные манипуляции к искажению печатаемого изделия. Плагин работает на основе машинного обучения и кроме текущей скорости вентилятора использует еще такие данные, как толщина каждого слоя изделия, плотность заполнения. Для обучения моделей машинного обучения авторы напечатали 135 различных комбинаций 3D-изделий и собрали набор данных требуемых параметров. Для предсказания критичности изменения скорости вращения использовались методы кластеризации K-means, а также логистическая регрессия и нейронная сеть.

В [21] авторы представляют решение по классификации производства на 3D-принтерах запрещенного оружия. Предложенное решение работает на основе сверточной нейронной сети. В качестве входных данных используются 3D-модели в формате stl, которые в дальнейшем преобразуются с распределением формы D2 в распределение вероятностей. Полученное распределение в дальнейшем используется нейронной сетью для классификации оружия. Для апробации предложенного решения авторы собрали набор данных, состоящий из файлов 3D-моделей. Результаты экспериментов показали достижимость показателя точности классификации в 98 %.

В [5] авторы проводят анализ атак, связанных с модификацией G-кода печати 3D-изделий. Уделяется особое внимание конкретным командам G-кода, которые могут свидетельствовать о наличии модификации. Кроме того, была разработана модель атакующего, которая разделяется на четыре уровня в зависимости от возможностей атакующего. Авторы выявили 278 потенциально вредоносных кодов, которые были разделены по категориям атак – модификация модели, отказ в обслуживании, кража информации и др.

По результатам проведенного отбора релевантных работ можно сделать следующий вывод: тематика обеспечения безопасности 3D-производств и защиты их от различных атак актуальна, авторы каждой из рассмотренных статей подчеркивают ее важность и критичность последствий от реализации атакующих воздействий. Однако далеко не все статьи описывают эффективные механизмы обнаружения атак и разработки мер противодействия им. В ряде публикаций ([5], [8]–[10], [16]–[17]) описывается и подтверждается на практике возможность реализации различных атак (например, кража интеллектуальной собственности или модификация изделия), но не приводятся механизмы их обнаружения либо делается вывод о том, что существующие подходы к обнаружению не способны обнаружить показанные атаки. В [13], [18], [21] авторы выделяют ряд мер обнаружения атак и защиты от них, но они либо очень специфичны и направлены на одну группу изделий (например, обнаружение печати запрещенного оружия), либо направлены на конкретную марку 3D-принтера (например, MakerBot Industries). И только в [15], [20] представлены методы обнаружения атак модификации процесса печати, которые выдают хорошие показатели качества их работы. Однако в случае с [20] предложенное решение охватывает только манипуляции со скоростью вращения вентилятора экструдера, а в случае с [15] для обнаружения используется видеопоток с последующим применением нейронной сети. Подобный подход может потреблять избыточное количество вычислительных ресурсов, а также требует пере-

обучения нейронной сети в случае появления новых атак. Поэтому тематика исследования и разработки эффективных механизмов по обнаружению и предотвращению кибератак на 3D-производства остается актуальной. В рамках данной статьи решается первоначальная задача исследования наиболее актуальных классов атак на такие производства, а также задача разработки подхода к их обнаружению, которая включает в себя подзадачу анализа и выявления данных, с помощью которых можно реализовать данный процесс.

Модель атак. Опираясь на анализ релевантных работ в области безопасности аддитивных производств и 3D-печати, были выделены наиболее актуальные атаки для данной области. Многие исследователи выделяют атаки, целью которых служат саботаж, кража интеллектуальной собственности, печать несанкционированных изделий, физическое разрушение элементов аддитивного производства и скрытая передача данных (атаки стеганографии).

Саботаж представляет собой несанкционированную модификацию печатаемого на 3D-принтере изделия, которая приводит к ухудшению его эксплуатационных свойств. Причем зачастую такие модификации незаметны при визуальном контроле и их последствия могут проявиться только в процессе эксплуатации. Негативными последствиями атаки саботажа могут быть: преждевременная поломка изделия, нарушение его механических свойств и пр., а владельцы производства могут понести значительные финансовые и репутационные потери.

Кража интеллектуальной собственности подразумевает незаконное получение третьими лицами какой-либо информации об изделии. Это может быть информация об используемом для производства материале, конструкции изделия,

Табл. 1. Модель атак на 3D-производства
Tab. 1. Attack model on 3D manufacturing

Цель атаки	Источники	Вид атаки	Пути реализации
Саботаж (модификация изделия). Данный класс атак влияет на механические и эксплуатационные характеристики изделий	[7], [9], [10], [14]–[18]	Манипулирование характеристиками материала при печати (температура, количество материала, скорость подачи материала)	Модификация команд G-кода, отвечающих за температуру экструдера, скорость подачи, количество материала, скорость вентилятора охлаждения. Необходим доступ к локальной сети 3D-принтера или физический доступ
		Модификация траекторий движения экструдера и стола 3D-принтера	Модификация команд G-кода, отвечающих за траектории движения экструдера. Необходим доступ к локальной сети 3D-принтера или физический доступ
		Модификация процента внутреннего наполнения изделия	Модификация команд G-кода, отвечающих за траектории движения экструдера. Необходим доступ к локальной сети 3D-принтера или физический доступ
		Нарушение физического процесса склеивания слоев изделия	Модификация команд G-кода, отвечающих за температуру и траектории движения. Необходим доступ к локальной сети 3D-принтера или физический доступ
		Внедрение вредоносного кода в прошивку 3D-принтера или программ для моделирования или нарезки	Подмена ПО на этапе поставки, обновления прошивки принтера из ненадежных источников, распространение через зараженные файлы, подмена с физическим доступом к принтеру
		Подмена изделия в процессе транспортировки потребителю	Доступ к службе логистики
		Подмена материалов для производства изделия (например, пластиковая нить)	Доступ к поставщикам материалов, либо к каналам его поставки

Окончание табл. 1
End of tab. 1

Цель атаки	Источники	Вид атаки	Пути реализации
Кража интеллектуальной собственности. Направлены на незаконное получение информации об изделии (его конструкция, материалы и прочее)	[3], [6], [13], [14], [17]–[19]	Несанкционированная реконструкция G-кода печати изделия	Запись звука работы 3D-принтера. Фиксация магнитного поля от моторов осей принтера во время печати Необходим физический доступ к 3D-принтеру
		Внедрение вредоносного кода в прошивку 3D-принтера или программ для моделирования или нарезки	Подмена ПО на этапе поставки, обновления прошивки принтера из не надежных источников, распространение через зараженные файлы, подмена с физическим доступом к принтеру
		Манипулирование протоколом передачи данных на 3D-принтер	Подключение у локальной сети с 3D-принтером, либо физический доступ к шине передачи данных (USB, CAN)
Физические атаки на оборудование 3D-печати. Направлена на физическое разрушение оборудования, например 3D-принтера	[12], [14]	Несанкционированное нарушение режима работы 3D-принтера	Удаленное подключение к принтеру по локальной сети. Необходим удаленный доступ к локальной сети предприятия
		Подмена комплектующих на этапе поставки	Доступ к поставщикам комплектующих, либо к каналам их поставки
Изготовление несанкционированных изделий. Печать изделий, которые запрещены на конкретном производстве или запрещенных к обороту	[21]	Внедрение вредоносного кода в прошивку 3D-принтера	Удаленное подключение к принтеру по локальной сети. Необходим удаленный доступ к локальной сети предприятия, либо физический доступ к 3D-принтеру
		Несанкционированное управление 3D-принтером	Удаленное подключение к принтеру по локальной сети. Необходим удаленный доступ к локальной сети предприятия, либо физический доступ к 3D-принтеру
		Манипулирование протоколом передачи данных на 3D-принтер	Подключение у локальной сети с 3D-принтером, либо физический доступ к шине передачи данных (USB, CAN)
Атаки сокрытия информации в файлах 3D-печати (стеганография). Скрытая передача данных с использованием файлов 3D-производства	[8]	Добавление зашифрованного сообщения в файл с 3D-моделью	Доступ к локальному хранилищу файлов моделей на производстве

авторских методах постобработки изделия. Печать несанкционированных изделий подразумевает несанкционированный перехват управления 3D-принтером с целью печати изделий, которые не производятся на рассматриваемом производстве. Или же вовсе печать запрещенных изделий.

Под физическим разрушением элементов производства понимается намеренное создание условий, при которых 3D-принтеры быстро выйдут из строя, т. е. данная атака направлена на физическое уничтожение самого принтера, создав условия его преждевременного износа.

Атаки стеганографии подразумевают использование файлов 3D-производства (моделей, файлов G-кодов печатей) для скрытой передачи данных. Прямой угрозы для аддитивного производства данные атаки не несут, однако добавленная в файлы информация может косвенно отражаться на качестве изготавливаемых изделий.

В табл. 1 представлена модель атак для 3D-производств. В процессе выбора конкретных видов атак для модели были использованы такие критерии отбора, как специфичность атаки для области 3D-печати, и незаметность негативных

последствий от реализации атаки. Данная модель представляет виды атак, классифицированные по целям. Также для создания модели были проанализированы и определены конкретные пути реализации каждой выделенной атаки. Таким образом, модель атак отражает конкретные действия злоумышленника, а также определяет конкретные уровни доступа реализации атак (физический доступ, удаленный доступ по сети и прочее).

Как видно из табл. 1, атаки одного вида могут преследовать разные цели. Например, при реализации атак саботажа злоумышленник может также преследовать цель кражи интеллектуальной собственности или же физического разрушения 3D-принтеров. Атаки же одного вида могут иметь различные пути реализации.

Также из таблицы видно, что для реализации большинства атак злоумышленнику необходим доступ к локальной сети производства. Это означает, что для предотвращения таких атак необходимо реализовать систему контроля доступа к устройствам и их аутентификации в сети предприятия. Однако даже в случае реализации такой системы риски проникновения нарушителя не сводятся к нулю, так как у него имеется возможность скомпрометировать уже авторизованные в сети устройства. Поэтому создание механизмов обнаружения выделенных ранее атак – актуальная задача. Для разработки и настройки механизмов обнаружения атак необходимо проанализировать данные, которые потребуются для обнаружения.

Данные для обнаружения атак. Опираясь на проведенный анализ релевантных работ и на пути реализации выделенных ранее актуальных атак на 3D-производства, был проведен анализ данных, с помощью которых можно будет обнаружить данные атаки. Результаты анализа сведены в табл. 2.

В ней представлены конкретные данные, которые необходимо собирать в процессе работы аддитивного производства и которые позволят реализовать процесс обнаружения атак на данном производстве. Для каждой из выявленных ранее атак были подобраны данные, которые так или иначе способны сигнализировать о реализации атаки. Кроме того, были определены конкретные места, в которых необходимо эти данные собирать.

Например, для обнаружения атаки манипулирования характеристиками материала при печати необходимо собирать данные о скорости подачи материала, движения экструдера и температуре экструдера. Все перечисленные данные можно получить из G-кода печати изделия.

Отдельно хотелось бы отметить, что часть данных можно получить от самих устройств (например, штатные логи 3D-принтеров или логи ПО для нарезки моделей), а часть – установкой дополнительных датчиков. Т. е. для реализации эффективных механизмов обнаружения атак на аддитивных производствах необходимо получать информацию не только от 3D-принтеров, но и от других элементов производства – таких, как операционная система управляющего компьютера, данные о сетевой активности, дополнительные датчики, установленные не производстве.

Подход к обнаружению атак на 3D-производствах. Данный подраздел посвящен описанию подхода к обнаружению атак на 3D-производствах. Обзор релевантных работ показал, что вопросы именно обнаружения атак на таких производствах раскрыты не в полном объеме, поэтому разработка подхода, который позволит формализовать процессы обнаружения атак на 3D-производствах, учитывая их специфику, актуальна и целесообразна. Основные требования к разрабатываемому подходу – это его универсальность, т. е. возможность применения к любым 3D-производствам независимо от конкретных марок используемых принтеров, а также учет специфики атак на такие производства. Обобщенная схема предлагаемого подхода показана на рис. 2. Подход определяет конкретные этапы, которые необходимо пройти в процессе реализации механизмов обнаружения атак на аддитивных производствах и описывает результаты реализации выделенных этапов.

Предлагаемый подход состоит из четырех этапов: изучения; анализа и подготовки данных; создания моделей обнаружения; внедрения. На первом этапе проводится подробное изучение предметной области безопасности 3D-производств. Изучаются атаки, которые специфичны для таких производств, их отличия от других атак (рис. 2, подп. 1.1, 1.2), проводится систематизация атак, а именно выявление наиболее актуальных и критичных для 3D-производств атак с анализом механизмов их реализации (рис. 2, подп. 1.3). Кроме того, на первом этапе проводится анализ данных, которые необходимо собирать на производстве с целью возможности реализации механизмов обнаружения. Этап изучения обеспечивает универсальность предлагаемого подхода за счет того, что проводится изучение и анализ всех возможных атак, специфичных области 3D-печати, без

Табл. 2. Данные для обнаружения атак
Tab. 2. Data for attack detection

Вид атаки	Данные для обнаружения	Предполагаемое место сбора данных
Манипулирование характеристиками материала при печати (температура, количество) Модификация траекторий движения экструдера и столе 3D-принтера Модификация процента внутреннего наполнения изделия Нарушение физического процесса склеивания слоев изделия	Скорость подачи материала	Файл с G-кодом, параметр E у команд перемещения по координатам
	Скорость движения стола\экструдера	Файл с G-кодом, параметр F у команд перемещения
	Температура экструдера и стола	Файл с G-кодом, коды M104, M140, M190, M109
	Координаты перемещения экструдера\стола во время печати (траектории)	Файл с G-кодом, команды перемещения по координатам, например G1 X0 Y0
	Видеозапись процесса печати	Видеокамера, установленная непосредственно на экструдере 3D-принтера
	Записи трафика, поступающего на принтер от управляющего компьютера в процессе печати изделия (TCP, USB)	Сниффер трафика, установленный на стороне 3D-принтера
	Записи звука, издаваемого 3D-принтером во время работы (для реконструкции кода печати и дальнейшего сравнения с оригинальным G-кодом)	Звукозаписывающее оборудование, например смартфон
	Магнитное поле от моторов осей принтера во время печати (для реконструкции кода печати и дальнейшего сравнения с оригинальным G-кодом)	Оборудование, способное зафиксировать магнитное поле
	Скорость вращения вентилятора для охлаждения экструдера и изделия	Сторонний датчик потока воздуха
Внедрение вредоносного кода в прошивку 3D-принтера или программ для моделирования или нарезки	Версия ПО	3D-принтер, характеристики прошивки принтера
	Дата последнего обновления ПО	
	Данные о загруженных файлах	Журнал операционной системы на управляющем компьютере
Подмена изделия в процессе транспортировки потребителю	Подтверждения надежности логистической компании	Лицензия, положительные отзывы
Подмена материалов для производства изделия (например, пластиковая нить)	Подтверждение подлинности материалов для производства изделия	Сертификаты соответствия
Несанкционированная реконструкция G-кода печати изделия	Временная задержка трафика, поступающего на принтер от управляющего компьютера в процессе печати изделия (TCP, USB)	Сниффер трафика, установленный на стороне 3D-принтера
	Данные о подключениях к управляющему компьютеру	Журнал операционной системы на управляющем компьютере
Манипулирование протоколом передачи данных на 3D-принтер	Записи трафика, передаваемого на принтер	Сниффер трафика, установленный на стороне 3D-принтера
	Данные о подключениях к управляющему компьютеру	Журнал операционной системы на управляющем компьютере
Несанкционированное нарушение режима работы 3D-принтера	Данные о температуре 3D-принтера	Сторонний датчик температуры, установленный на 3D-принтере
	Данные о наличии задымления	Сторонний датчик дыма
	Температура экструдера и стола, полученная от встроенных датчиков 3D-принтера	Файл с G-кодом, коды M104, M140, M190, M109
	Скорость вращения вентилятора для охлаждения экструдера и изделия	Сторонний датчик потока воздуха
Подмена комплектующих на этапе поставки	Данные о подлинности комплектующих	Сертификаты соответствия
Внедрение вредоносного кода в прошивку 3D-принтера	Версия ПО	3D-принтер, характеристики прошивки принтера
	Дата последнего обновления ПО	
	Данные о загруженных файлах	Журнал операционной системы на управляющем компьютере
Несанкционированное управление 3D-принтером	Записи трафика, передаваемого на принтер	Сниффер трафика, установленный на стороне 3D-принтера
	Логи 3D-принтера, содержащие список последних подключений к принтеру	3D-принтер
	Данные о подключениях к управляющему компьютеру	Журнал операционной системы на управляющем компьютере
Добавление зашифрованного сообщения в файл с 3D-моделью	Контрольная сумма файла с 3D-моделью	Локальная база данных всех 3D-моделей печати
	Файлы с 3D-моделями	

привязки к конкретному производству или производителю оборудования. А последующие этапы уже адаптируют подход к конкретному 3D-производству. Результат выполнения первого этапа – обобщенная модель атак, которая включает в себя список всех релевантных атак и способов их реализации злоумышленником, а также описание данных, которые требуются для обнаружения атак, с указанием мест сбора этих данных.

На втором этапе проводится адаптация под конкретное 3D-производство – анализ архитектуры производства с выделением атак и данных, которые релевантны именно этому производству (рис. 2, подп. 2.1). Например, если на производстве отсутствует локальная сеть и выход в Интернет, часть атак можно не рассматривать ввиду невозможности их реализации злоумышленником. Также в таком случае отсутствует необходимость в сборе сетевых данных. После выявления релевантных атак разрабатываются механизмы сбора требуемых для обнаружения данных, проводится установка устройств для сбора данных и осуществляется их сбор (рис. 2, подп. 2.2–2.4). Результатом работы второго этапа служит набор данных, который в дальнейшем может быть использован для обучения и настройки моделей обнаружения атак.

Третий этап посвящен разработке самих моделей обнаружения атак. На данном этапе проводится их выбор, настройка их параметров, обучение (в случае применения методов искусственного интеллекта), а также оценка качества обнаружения (рис. 2, подп. 3.1–3.3). Результатом выполнения третьего этапа служит получение обученных моделей обнаружения атак. Заключительный, четвертый, этап – внедрение всех разработанных ранее решений на производство (рис. 2, подп. 4.1), результатом которого служит работающая система обнаружения атак.

Как отмечалось ранее, именно первый этап обеспечивает универсальность предложенного подхода, а остальные позволяют провести его адаптацию к конкретному 3D-производству. В рамках данного исследования был реализован первый этап подхода – были проведены анализ и систематизация атак, которые релевантны для области 3D-печати; были определены механизмы реализации данных атак, а также проанализированы данные для их обнаружения с выделением мест сбора этих данных. В рамках дальнейших исследований планируется реализация остальных этапов подхода, т. е. адаптация под конкретное производство и реализация моделей обнаружения.

Рис. 2. Обобщенная схема подхода к обнаружению атак на 3D-производствах
Fig. 2. Generalized scheme of approach to detecting attacks in 3D manufacturing

Заключение. В настоящей статье представлен всесторонний обзор предметной области безопасности аддитивных производств. Подобные 3D-производства на данный момент набирают популярность – 3D-печать применяется в биоинженерии, производстве различных изделий и продуктов питания, поэтому настолько актуальна тематика обеспечения их безопасности и предотвращения атак.

Представлен обобщенный подход к обнаружению атак на 3D-производствах. Он отличается универсальностью, а именно возможностью применения на любых аддитивных производствах вне зависимости от производителя используемых 3D-принтеров. Кроме того, подход включает в себя механизмы адаптации предложенных решений под конкретное производство.

В рамках предложенного подхода была проведена частичная его реализация, т. е. обзор релевантных работ в данной области. Результатом обзора стало понимание того, что существующие на сегодняшний день публикации имеют недостатки: часть их описывают только реализацию различных атак, но не приводят механизмы их обнаружения; другие охватывают узкий спектр методов обнаружения, рассчитанных либо на одну группу изделий, либо на конкретную марку принтера, т. е. отсутствует универсальность предлагаемых решений.

Также была разработана модель атак. Были выделены конкретные виды атак на аддитивные производства. Основными их целями служат саботаж, кража интеллектуальной собственности, печать несанкционированных изделия, физическое разрушение элементов аддитивного производства и скрытая передача данных. Для выделенных видов атак были проанализированы пути их реализации. В завершение были проанализированы конкретные данные для обнаружения выделенных видов атак с выявлением места сбора этих данных.

В качестве дальнейшей разработки данной тематики можно выделить следующие направления: адаптация предложенного подхода к конкретному 3D-производству, т. е. анализ архитектуры конкретного производства и разработка механизмов обнаружения атак, который будет основан на выделенных в данной статье данных; практическая реализация моделей обнаружения атак; разработка рекомендаций для внедрения разработанных решений.

Список литературы

1. 3D printing for membrane separation, desalination and water treatment / L. D. Tijing, J. C. Dizon, I. Ibrahim, A. N. Nisay, H. K. Shon, R. C. Advincula // App. Materials Today. 2020. Vol. 18, no. 100486. P. 1–22.

2. Sundarsingh A., Zhang M., Mujumdar A. S. Research progress in printing formulation for 3D printing of healthy future foods // Food Bioproc. Technol. 2024. Vol. 17. P. 3408–3439.

3. 3D Bioprinter firmware attacks: Categorization, implementation, and impacts / M. Ahsan, B. Najarro-Blancas, J. T. Ebode, N. Lewinski, I. Ahmed // 2025 IEEE Int. Symp. on Hardware Oriented Security and Trust (HOST). CA, USA: San Jose, 2025. P. 99–110. doi: 10.1109/HOST64725.2025.11050047.

4. Иванов Ф. Я. Внедрение практики 3D-печати модулей в рамках модульного строительства // Вестн. науки. 2025. Т. 1, № 5 (86). С. 809–813.

5. Security implications of malicious G-Codes in 3D printing / J. Rossel, V. Mladenov, N. Wordenweber, J. Somorovsky // USENIX Security'25, 2025, P. 1–19. URL: https://www.researchgate.net/publication/393050501_Security_Implications_of_Malicious_G-Codes_in_3D_Printing (дата обращения: 10.11.2025).

6. My smartphone knows what you print: Exploring smartphone-based side-channel attacks against 3D printers / C. Song, F. Lin, Z. Ba, K. Ren, C. Zhou, W. Xu // Proc. of the 2016 ACM SIGSAC Conf. on Comp. and Communications Security (CCS '16). Vienna, Austria: Association for Comp. Machinery, 2016. P. 895–907. doi: 10.1145/2976749.2978300. URL: https://cse.buffalo.edu/~wenyaoxu/papers/conference/xu-ccs2016.pdf (дата обращения: 11.11.2025).

7. Watching and safeguarding your 3D printer: Online process monitoring against cyber-physical attacks / Y. Gao, B. Li, W. Wang, W. Xu, C. Zhou, Z. Jin // Proc. of the ACM on Interact., Mobile, Wearable and Ubiquitous Technol. 2018. Vol. 2, is. 3, no. 108. P. 1–27. doi: 10.1145/3264918.

8. What did you add to my additive manufacturing data? Steganographic attacks on 3D printing files / M. Yampolskiy, L. Graves, J. Gatlin, A. Skjellum, M. Yung // Proc. of the 24th Int. Symp. on Research in Attacks, Intrusions and Defenses (RAID '21). P. 266–281. doi: 10.1145/3471621.3471843. URL: https://www.researchgate.net/publication/355135376_What_Did_You_Add_to_My_Additive_Manufacturing_Data_Steganographic_Attacks_on_3D_Printing_Files (дата обращения: 10.11.2025).

9. Cultice T., Thapliyal H. Vulnerabilities and attacks on CAN-based 3D printing/additive manufacturing // IEEE Consumer Electron. Magazine. 2024. Vol. 13, no. 1. P. 54–61. doi: 10.1109/MCE.2023.3240849.

10. Rais M. H., Li Y., Ahmed I. Dynamic-thermal and localized filament-kinetic attacks on fused filament fabrication based 3D printing process // Additive Manufacturing. 2021. Vol. 46. P. 102200. doi: 10.1016/j.addma.2021.102200.

11. Филяк П. Ю., Пажинцев Д. А., Тырин И. А. 3D-принтеры – реальность и будующие. Аспекты информационной безопасности // Информационная безопасность. 2020. Т. 23. Вып. 4. С. 525–534. doi: 10.36622/VSTU.2020.23.4.005.

12. Танаева М. С., Семиглазов В. А. Трехфакторная защита 3D-принтеров от возгорания // Инноватика-2019. Сб. материал. XV Междунар. школы-конф. студентов, аспирантов и молодых ученых. Томск: ООО «СТТ», 2019. С. 529–532.

13. Do Q., Martini B. Choo K.-K. R. A Data exfiltration and remote exploitation attack on consumer 3D printers // IEEE Trans. on Inform. Forensics and Security, 2016. Vol. 11, no. 10. P. 2174-2186. doi: 10.1109/TIFS.2016.2578285.

14. Kumar M., Epiphaniou G., Maple C. Security of cyber-physical Additive Manufacturing supply chain: Survey, attack taxonomy and solutions // Comp. & Security. 2015. Vol. 157, no. 104557. doi: 10.1016/j.cose.2025.104557.

15. Smart manufacturing towards cyber-physical resilience in 3D printing process monitoring and anomaly detection / A. A. Mamun, M. Kuzlu, V. Jovanovic, W. Sealy // The Int. J. of Advanced Manufacturing Technol. 2025. Vol. 141. P. 2007–2026. doi: 10.1007/s00170-025-16795-y.

16. Rais M. H., Ahsan M., Ahmed I. Sabotaging material extrusion-based 3D printed parts through low-magnitude kinetic manipulation attacks // ACM Trans. on Cyber-Phys. Syst. 2025. Vol. 9, iss. 1, no. 5. P. 1–26. doi: 10.1145/3704735.

17. Rais M. H., Ahsan M., Ahmed I. FRoMEPP: Digital forensic readiness framework for material extrusion based 3D printing process // Forensic Sci. Intern.: Digital Investigation. 2023. Vol. 44. P. 301510. doi: 10.1016/j.fsidi.2023.301510.

18. Manipulation of G-code toolpath files in 3^{d} printers: attacks and mitigations / E. Kurkowski, A. Van Stockum, J. Dawson, C. Taylor, T. Schulz, S. Shenoi // Critical Infrastructure Protection XVI. ICCIP 2022. IFIP Advances in Inform. and Communication Technol. 2022. Vol. 666. P. 155–174. doi: 10.1007/978-3-031-20137-0_6.

19. Acoustic side-channel attacks on additive manufacturing systems / M. A. Al Faruque, S. R. Chhetri, Canedo A., J. Wan // 2016 ACM/IEEE 7^{th} Int. Conf. on Cyber-Phys. Syst. (ICCPS). Vienna, Austria: IEEE, 2016. P. 1–10. doi: 10.1109/ICCPS.2016.7479068.

20. Machine learning-based investigation of the 3D printer cooling effect on print quality in fused filament fabrication: A cybersecurity perspective / H. Si, Z. Zhang, O. Huseynov, I. Fidan, S. R. Hasan, M. Mahmoud // Inventions. 2023. Vol. 8(1), no. 24. doi: 10.3390/inventions8010024.

21. Anti-3D weapon model detection for safe 3D printing based on convolutional neural networks and D2 shape distribution / G. N. Pham, S. H. Lee, O. H. Kwon, K. R. Kwon // Symmetry. 2018. Vol. 10(4), no. 90. P. 1–15. doi: 10.3390/sym10040090.

Информация об авторе

Мелешко Алексей Викторович – младший научный сотрудник. Международный центр цифровой криминалистики. Санкт-Петербургский Федеральный исследовательский центр Российской академии наук, 14-я линия В. О., д. 39, Санкт-Петербург, 199178, Россия.
E-mail: meleshko.a@iias.spb.su
http://orcid.org/0000-0002-1209-4230

References

1. 3D printing for membrane separation, desalination and water treatment / L. D. Tijing, J. C. Dizon, I. Ibrahim, A. N. Nisay, H. K. Shon, R. C. Advincula // App. Materials Today. 2020. Vol. 18, no. 100486. P. 1–22.

2. Sundarsingh A., Zhang M., Mujumdar A. S. Research Progress in printing formulation for 3D printing of healthy future foods // Food Bioproc. Technol. 2024. Vol. 17. P. 3408–3439.

3. 3D Bioprinter firmware attacks: Categorization, implementation, and impacts / M. Ahsan, B. Najarro-Blancas, J. T. Ebode, N. Lewinski, I. Ahmed // 2025 IEEE Int. Symp. on Hardware Oriented Security and Trust (HOST). CA, USA: San Jose, 2025. P. 99–110. doi: 10.1109/HOST64725.2025.11050047.

4. Ivanov F. Ja. Vnedrenie praktiki 3D-pechati modulej v ramkah modul'nogo stroitel'stva // Vestn. nauki. 2025. T. 1, № 5 (86). S. 809-813. (In Russ.).

5. Security implications of malicious G-Codes in 3D printing / J. Rossel, V. Mladenov, N. Wordenweber, J. Somorovsky // USENIX Security '25, 2025, P. 1-19. URL: https://www.researchgate.net/publication/393050501_Security_Implications_of_Malicious_G-Codes_in_3D_Printing (data obrashhenija: 10.11.2025).

6. My smartphone knows what you print: Exploring smartphone-based sidechannel attacks against 3D Printers / C. Song, F. Lin, Z. Ba, K. Ren, C. Zhou, W. Xu // Proc. of the 2016 ACM SIGSAC Conf. on Comp. and Communications Security (CCS'16). Vienna, Austria: Association for Computing Machinery, 2016. P. 895–907. doi: 10.1145/2976749.2978300. URL: https://cse.buffalo.edu/~wenyaoxu/papers/conference/xu-ccs2016.pdf (data obrashhenija: 11.11.2025).

7. Watching and Safeguarding your 3D printer: Online process monitoring against cyber-physical attacks / Y. Gao, B. Li, W. Wang, W. Xu, C. Zhou, Z. Jin // Proc. of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technol. 2018. Vol. 2, is. 3, no. 108. P. 1–27. doi: 10.1145/3264918.

8. What did you add to my additive manufacturing data? Steganographic attacks on 3D printing files / M. Yampolskiy, L. Graves, J. Gatlin, A. Skjellum, M. Yung // Proc. of the 24th Int. Symp. on Research in Attacks, Intrusions and Defenses (RAID '21). P. 266–281. doi: 10.1145/3471621.3471843. URL: https://www.researchgate.net/publication/355135376_What_Did_You_Add_to_My_Additive_Manufacturing_Data_Steganographic_Attacks_on_3D_Printing_Files (data obrashhenija: 10.11.2025).

9. Cultice T., Thapliyal H. Vulnerabilities and attacks on CAN-based 3D printing/additive manufacturing // IEEE Consumer Electron. Magazine. 2024. Vol. 13, no. 1. P. 54–61. doi: 10.1109/MCE.2023.3240849.

10. Rais M. H., Li Y., Ahmed I. Dynamic-thermal and localized filament-kinetic attacks on fused filament fabrication based 3D printing process // Additive Manufacturing. 2021. Vol. 46. P. 102200. doi: 10.1016/j.addma.2021.102200.

11. Filjak P. Ju., Pazhincev D. A., Tyrin I. A. 3D-printery – real'nost' i budujushhie. Aspekty informacionnoj bezopasnosti // Informacionnaja bezopasnost'. 2020. T. 23. Vyp. 4. S. 525-534. doi: 10.36622/VSTU.2020.23.4.005. (In Russ.).

12. Tanaeva M. S., Semiglazov V. A. Trehfaktornaja zashhita 3D-printerov ot vozgoranija // Innovatika-2019. Sb. material. XV Mezhdunar. shkoly-konf. studentov, aspirantov i molodyh uchenyh. Tomsk: OOO «STT», 2019. S. 529-532. (In Russ.).

13. Do Q., Martini B. Choo K.-K. R. A data exfiltration and remote exploitation attack on consumer 3D printers // IEEE Trans. on Inform. Forensics and Security, 2016. Vol. 11, no. 10. P. 2174-2186. doi: 10.1109/TIFS.2016.2578285.

14. Kumar M., Epiphaniou G., Maple C. Security of cyberphysical Additive Manufacturing supply chain: Survey, attack taxonomy and solutions // Comp. & Security. 2015. Vol. 157, no. 104557. doi: 10.1016/j.cose.2025.104557.

15. Smart manufacturing towards cyber-physical resilience in 3D printing process monitoring and anomaly detection / A. A. Mamun, M. Kuzlu, V. Jovanovic, W. Sealy // The Intern. J. of Advanced Manufacturing Technol. 2025. Vol. 141. P. 2007–2026. doi: 10.1007/s00170-025-16795-y.

16. Rais M. H., Ahsan M., Ahmed I. Sabotaging material extrusion-based 3D printed parts through low-magnitude kinetic manipulation attacks // ACM Trans. on Cyber-Phys. Syst. 2025. Vol. 9, iss. 1, no. 5. P. 1–26. doi: 10.1145/3704735.

17. Rais M. H., Ahsan M., Ahmed I. FRoMEPP: Digital forensic readiness framework for material extrusion based 3D printing process // Forensic Sci. Intern.: Digital Investigation. 2023. Vol. 44. P. 301510. doi: 10.1016/j.fsidi.2023.301510.

18. Manipulation of G-code toolpath files in 3d printers: attacks and mitigations / E. Kurkowski, A. Van Stockum, J. Dawson, C. Taylor, T. Schulz, S. Shenoi // Critical Infrastructure Protection XVI. ICCIP 2022. IFIP Advances in Inform. and Commun. Technol. 2022. Vol. 666. P. 155–174. doi: 10.1007/978-3-031-20137-0_6.

19. Acoustic side-channel attacks on additive manufacturing systems / M. A. Al Faruque, S. R. Chhetri, Canedo A., J. Wan // 2016 ACM/IEEE 7th Int. Conf. on Cyber-Phys. Syst. (ICCPS). Vienna, Austria: IEEE, 2016. P. 1–10. doi: 10.1109/ICCPS.2016.7479068.

20. Machine learning-based investigation of the 3D printer cooling effect on print quality in fused filament fabrication: A cybersecurity perspective / H. Si, Z. Zhang, O. Huseynov, I. Fidan, S. R. Hasan, M. Mahmoud // Inventions. 2023. Vol. 8(1), no. 24. doi: 10.3390/inventions8010024.

21. Anti-3D weapon model detection for safe 3D printing based on convolutional neural networks and D2 shape distribution / G. N. Pham, S. H. Lee, O. H. Kwon, K. R. Kwon // Symmetry. 2018. Vol. 10(4), no. 90. P. 1–15. doi: 10.3390/sym10040090.

Information about the author

Aleksei V. Meleshko – junior researcher, International Digital Forensics Center, St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS), 14th line V. O., 39, St. Petersburg, 199178, Russia.
E-mail: meleshko.a@iias.spb.su
http://orcid.org/0000-0002-1209-4230

Статья поступила в редакцию 18.11.2025; принята к публикации после рецензирования 24.12.2025; опубликована онлайн 26.02.2026.

Submitted 18.11.2025; accepted 24.12.2025; published online 26.02.2026.