МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение высшего образования

«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет: Информационных систем и геотехнологий

Кафедра: Информационных систем и систем безопасности

Направление подготовки – информационная безопасность телекоммуникационных систем

Профиль – разработка и защита телекоммуникационных систем

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА СПЕЦИАЛИСТА

На тему : Методика управления информационной безопасностью производственной линии 3D печати

Исполнитель: Кархy Егор Евгеньевич

Руководитель: Профессор, д.т.н. Бурлов В.Г.

Допустить к защите

_____/

Санкт-Петербург

2026г.

Федеральное государственное бюджетное образовательное учреждение высшего образования

РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ (РГГМУ)

Факультет ИС и ГТ

Кафедра ИССБ

Направление подготовки информационная безопасность телекоммуникационных систем

Профиль разработка и защита телекоммуникационных систем

ЗАДАНИЕ

на дипломное проектирование

студента Кархy Егора Евгеньевича

1. Тема дипломного проектирования: «Методика управления информационной безопасностью производственной линии 3D печати»

2. Цель исследования:

Исследовать угрозы информационной безопасности, специфичные для аддитивных производств.

3. Перечень разделов по теме:

- Теоретические основы создания и функционирования производственной линии 3D-печати как сложной системы
- Практическое применение технологий для обеспечения качества и автоматизации постобработки в аддитивном производстве
- Разработка модели управления информационной безопасностью на основе принципов системного анализа и информационного противодействия;

4. Ожидаемые результаты

Предложить методический аппарат оценки эффективности разработанной модели.

5. Техническая документация проекта в соответствии с методическими указаниями.

Задание утверждено на заседании кафедры ИССБ «___»_____2026 года

Дата выдачи задания «___» _____ 2026 года

Зав. кафедрой ИССБ _____( )

Руководитель _____(_____)

Студент _____(_____)

Оглавление

Введение

Научная новизна работы заключается в следующем: 1. Разработана модель управления информационной безопасностью производственной линии 3D-печати, основанная на концепциях системогенеза и информационного противодействия. 2. Предложен методический аппарат оценки эффективности системы защиты с использованием математического моделирования на основе цепей Маркова. 3. Обоснован принцип проактивного информационного противодействия как альтернатива традиционным периметровым методам защиты. На защиту выносятся: Модель управления информационной безопасностью производственной линии 3D-печати, Методика оценки эффективности системы защиты, Результаты моделирования, показывающие высокую эффективность предложенных решений.

В первом разделе рассматриваются научно-технические основы обеспечения безопасности производственной линии 3D-печати в условиях аддитивного производства на базе системного анализа и информационного противодействия.

Во втором разделе разработана модель управления процессами обеспечения безопасности.

В третьем разделе разработана технология (методика) обеспечения безопасности.

В четвертом разделе разработаны предложения по совершенствованию системы.

Дипломная работа состоит из введения, четырех глав, заключения и списка литературы. В первой главе рассматриваются теоретические основы производственной линии 3D-печати как сложной системы, анализируются принципы системогенеза и концепции информационного противодействия. Во второй главе представлены практические технологии и программно-аппаратные решения для обеспечения качества и автоматизации в аддитивном производстве. В

третьей главе разрабатывается модель управления информационной безопасностью, включающая математический аппарат и расчет эффективности системы.

В современной научной литературе проблематика информационной безопасности аддитивного производства рассматривается в контексте Индустрии 4.0. Исследования в области системогенеза (Дружинин В.В., Контаров В.В.) и теории сложных систем (Месарович М., Мако Д., Такахара И.) обосновывают необходимость проактивного подхода к защите. Работы по информационному противодействию (Щербаков А.Ю., Шаньгин В.Ф.) формируют методологическую базу моделирования угроз. Однако комплексные подходы к управлению безопасностью производственных линий 3D-печати как сложных социотехнических систем в литературе представлены недостаточно, что определяет научную новизну данной работы.

Предметом исследования выступает модель управления информационной безопасностью указанной производственной линии.

Объектом исследования является процесс функционирования производственной линии 3D-печати.

Предложить методический аппарат оценки эффективности разработанной модели.

Разработать структурно-функциональную модель системы управления информационной безопасностью.

Исследовать угрозы информационной безопасности, специфичные для аддитивных производств.

Провести теоретический анализ производственной линии 3D-печати как объекта системного анализа и информационного противодействия.

Для достижения поставленной цели необходимо решить следующие задачи:

Целью работы является разработка модели управления информационной безопасностью производственной линии 3D-печати, основанной на концепциях системогенеза и информационного противодействия.

Актуальность данной работы обусловлена острой потребностью российской промышленности в защищенных технологических решениях. Разработка эффективной модели управления информационной безопасностью производственной линии 3D-печати является не просто технической, а стратегической задачей, напрямую влияющей на технологическую независимость и конкурентоспособность страны.

Традиционные подходы к защите, основанные на создании периметровых барьеров, оказываются неадекватными динамичной природе таких систем. Их недостаток заключается в игнорировании процесса системогенеза - целенаправленного формирования системы на всех стадиях ее жизненного цикла. Безопасность, внедренная постфактум, не способна учесть глубинные системные связи и закономерности, что оставляет критические уязвимости. Следовательно, возникает научное противоречие между необходимостью обеспечения надежной защиты сложной производственной системы и отсутствием моделей управления информационной безопасностью, адекватных ее системной природе и построенных на принципах проактивного информационного противодействия.

Рассмотрение производственной линии 3D-печати как теорию сложных систем, позволяет выявить фундаментальную проблему. Такая линия представляет собой не просто совокупность оборудования, а сложную целенаправленную социотехническую систему, в которой неразрывно связаны технические, программные и человеческие компоненты, управляемые информационными потоками. Именно эти потоки - цифровые двойники, управляющие G-code,

технологические параметры - становятся основным объектом целенаправленного информационного противодействия. Угрозы перестают быть случайными событиями и приобретают характер спланированных действий промышленного шпионажа и саботажа, нацеленных на хищение интеллектуальной собственности, дестабилизацию производственных циклов и нанесение репутационного ущерба.

В эпоху Индустрии 4.0 и повсеместной цифровизации производственных процессов аддитивные технологии, и, в частности, 3D-печать, трансформируются из инструмента прототипирования в основу высокотехнологичного производства. Производственные линии 3D-печати становятся ключевыми элементами промышленных экосистем, особенно в стратегически важных для Российской Федерации отраслях: авиастроении, оборонном комплексе и медицине. Однако возрастающая сложность и интеллектуализация подобных систем порождает новую классу угроз, превращая их информационную безопасность в задачу национального технологического суверенитета.

Глава 1. Научно-технические основы обеспечения безопасности объекта производственной линии 3D-печати в условиях аддитивного производства на базе системогенеза и информационного противодействия

1.1. Характеристика особенностей функционирования объекта

Современная индустриальная революция, базирующаяся на цифровизации и аддитивных технологиях, кардинально трансформирует подходы к производству. Производственная линия 3D-печати перестает быть экзотикой и становится полноценным элементом высокотехнологичных производственных систем. Однако ее проектирование и внедрение представляют собой нетривиальную задачу, выходящую далеко за рамки простой интеграции аппаратного обеспечения. Для глубокого понимания процессов ее создания и последующей защиты необходим системный подход, рассматривающий линию 3D-печати не как совокупность

устройств, а как сложную, целенаправленную и эволюционирующую социотехническую систему.

Для дальнейшего исследования определим производственную линию 3D-печати (ПЛ 3D-печати) как сложную социотехническую систему, предназначенную для автоматизированного или полуавтоматизированного изготовления физических объектов на основе цифровых моделей. Ключевыми атрибутами такой системы, в соответствии с теорией сложных систем, являются:

Целенаправленность. Система создается для достижения конкретных производственных целей: серийного производства деталей, оперативного изготовления прототипов, производства изделий сложной геометрии. Цель системы является первопричиной ее существования и главным критерием эффективности.

Сложная структура. ПЛ 3D-печати включает в себя множество взаимосвязанных элементов различной природы:

Техническая подсистема: 3D-принтеры, посты обработки, сканеры, роботизированные манипуляторы, серверное оборудование, сетевая инфраструктура.

Программная подсистема: САПР (CAD), системы подготовки к печати (CAM/Slicer), системы управления производством (MES/ERP), ПО для мониторинга и диагностики.

Информационная подсистема: цифровые модели (3D-модели, файлы чертежей), технологические параметры (G-code), базы данных материалов, производственная статистика.

Человеческая подсистема: операторы, технологи, инженеры, обслуживающий персонал.

Наличие информационных потоков. Функционирование системы неразрывно связано с движением информации: от исходной модели до управляющих команд для принтера и от сенсоров обратно в систему контроля. Эти потоки являются как основой производственного процесса, так и основным объектом потенциальных угроз.

Открытость и взаимодействие с внешней средой. ПЛ 3D-печати не существует в вакууме. Она интегрируется в общую производственную цепочку предприятия, взаимодействует с поставщиками материалов и заказчиками, что создает дополнительные каналы для информационных воздействий.

Рассмотрение ПЛ 3D-печати в данной ситуации позволяет, перейти от анализа отдельных компонентов к изучению закономерностей их взаимодействия и системных свойств, которые не сводятся к простой сумме свойств элементов.

1.2. Системогенез производственной линии 3D-печати как основа для обеспечения безопасности

Процесс создания ПЛ 3D-печати можно представить как последовательность этапов системогенеза, на каждом из которых должны закладываться основы ее будущей безопасности. Игнорирование этого принципа приводит к необходимости «достраивать» защиту постфактум, что неэффективно и дорого.

В основе обеспечения безопасности лежит деятельность людей, принимаемые ими решения. В результате таких решений может появиться угроза, возникающая при несоответствии адекватности модели объекта к обстановке (модель описание или представление объекта, соответствующая данному объекту и позволяющая получать характеристики об этом объекте; обстановка совокупность факторов и условий, в которых осуществляется деятельность). Таким образом решение в данном контексте является моделью процесса, с которым работает человек, а

процесс, в свою очередь, это объект в действии при фиксированном предназначении.

В связи с этим возникла необходимость создания интегрированных систем обеспечения безопасности.

При проектировании интегрированной системы безопасности происходят следующие этапы:

1. Процесс создания угрозы.

2. Процесс мониторинга угрозы.

3. Процесс устранения угрозы.

Постоянная и стабильная работа любого объекта невозможна без надёжной защиты, которая включает в себя комплекс мер, направленных на выявление угроз и опасных ситуаций, оценку ущерба во время опасных ситуаций и проектирование интегрированной системы безопасности объекта при определённых ограничениях:

на информационные ресурсы (направленные на распознавание угрозы);

на деятельные ресурсы (направленные на устранение/профилактику угроз);

на ресурсы обстановки.

Несоответствующий результат управление процессом обоснован противоречивыми выводами. Для того, чтобы исключить такие выводы, необходимо пользоваться аксиоматическим методом.

Аксиоматический метод - способ достижения научной теории, в которой определенные примитивные предположения, так называемые аксиомы, постулируются в качестве основы теории, в то время как остальные положения теории получены как логические следствия из этих аксиом.

Аксиоматический метод предполагает наличие следующих элементов [87, 90]:

а) основные допущения и предположения, обычно выражающиеся в базовых принципах.

б) базовые понятия, ключевые слова, аксиомы;

в) правила вывода;

г) теоремы.

Для объективного использования данного метода необходимо отметить, что в процессе деятельности участвуют

а) Человек, его сознание.

б) Окружающий МИР (объект).

в) Нечто, что дано природой и позволяет осуществлять познание. (Всеобщая связь.)

Для решения задачи синтеза применяем естественнонаучный подход, базирующийся на законе сохранения целостности объекта (ЗСЦО).

Закон сохранения целостности объекта (ЗСЦО) - устойчивая повторяющаяся связь свойств объекта и свойств действия при фиксированном предназначении. ЗСЦО проявляется во взаимной трансформации свойств объекта и свойств его действия при фиксированном предназначении.

Принцип трёхкомпонентности познания состоит в том, что человек, осознанно или нет, осуществляет выработку решения в трёх уровнях представлении обстановки.

В процессе деятельности человек оперирует с категориями «система», «модель» и «предназначение». Поэтому особенно корректно необходимо рассматривать и использовать эти категории. На рис 2.1. представлено развёртывание содержание понятия «деятельность» в рамках естественно-научного подхода.

Рис.2.1. Структурная схема развертывания содержания понятия «деятельность» через «система», «модель», «предназначение (эффективность деятельности)».

Известно всего два направления разработки системы (модели) Рис.2.2.

Рис.2.2. Структурная схема основных направлений разработки системы.

В настоящей работе классифицируются решения человека:

- анализное, основанное на решении задачи в форме анализа;

- синтетическое, основанное на решении в форме синтеза.

1.3. Информационное противодействие как ключевая задача управления безопасностью ПЛ 3D-печати

Рассматривая ПЛ 3D-печати как сложную систему, необходимо признать, что она функционирует в условиях информационного противодействия. Этот термин, подразумевает не пассивную защиту, а активное противостояние целенаправленным информационным угрозам.

Основными объектами информационного воздействия в контексте ПЛ 3D-печати являются:

Интеллектуальная собственность: CAD-модели, конструкторская и технологическая документация. Их кража или подделка наносит прямой экономический ущерб.

Управляющие данные: G-code и другие файлы настроек печати. Их несанкционированная модификация (саботаж) может привести к браку, поломке дорогостоящего оборудования или созданию опасных изделий.

Производственная информация: Данные о загрузке мощностей, расходе материалов, времени циклов. Их утечка может дать конкурентам представление о производственных возможностях и планах компании.

Системы управления: Доступ к MES/ERP и управляющим компьютерам позволяет злоумышленнику дестабилизировать или полностью остановить производственный процесс.

В соответствии с теорией информационного противодействия, модель управления безопасностью должна включать в себя не только защитные механизмы (пассивная оборона), но и подсистемы:

Обнаружения (идентификация факта воздействия).

Предотвращения (блокировка попытки воздействия).

Реагирования (локализация и ликвидация последствий).

Восстановления (возврат системы в штатное состояние).

Создание такой комплексной системы возможно только на основе глубокого понимания архитектуры и законов функционирования защищаемого объекта, что и было достигнуто в данной главе посредством его системного анализа.

Таким образом, первая глава сформировала теоретическую базу для разработки модели управления информационной безопасностью производственной линии 3D-печати.

1. Рассмотрены современные подходы к управлению информационной безопасностью в производственных средах, включая анализ угроз, моделирование защищённости и выбор рациональных мер защиты.

2. Проанализированы основы теории системогенеза, применяемые для построения моделей защиты информации в сложных технических системах. Показана актуальность использования закономерностей становления систем для разработки эффективных механизмов информационной безопасности.

3. Рассмотрен принцип трёхкомпонентности познания, который позволяет системно подходить к анализу информационных процессов в производственной линии. Выявлены три взаимосвязанных компонента: формирование угроз, их идентификация и нейтрализация.

4. Изучен понятийный аппарат системного анализа в контексте аддитивного производства. Определены ключевые характеристики производственной линии 3D-печати как сложной системы, включая многоуровневую структуру, распределённость элементов и динамический характер процессов.

Основные результаты первой главы:

В первой главе были рассмотрены теоретические основы создания и функционирования производственной линии 3D-печати как сложной системы.

Ключевым фактором, определяющим переход 3D-печати из категории прототипирования в разряд полноценного серийного производства, является способность гарантировать стабильное и воспроизводимое качество конечных изделий. Традиционные методы контроля качества, основанные на ручном инспектировании и выборочных испытаниях, не в состоянии справиться с возрастающими темпами и сложностью производственных линий аддитивного

изготовления. Они медленны, субъективны и неэффективны в условиях Индустрии 4.0.

Решение этой проблемы лежит в плоскости интеллектуальных технологий, в первую очередь - искусственного интеллекта (ИИ). ИИ позволяет перейти от реактивной модели обнаружения брака к проактивной модели его предотвращения и автоматизированной коррекции. Данная глава посвящена анализу конкретных методов и алгоритмов ИИ, применяемых для приведения изделий, созданных методом 3D-печати, в надлежащее состояние, а также оценке возникающих при этом информационных рисков.

В результате выполнения первого раздела получена характеристика производственной линии 3D-печати как объекта защиты, выявлены особенности её функционирования в условиях аддитивного производства.

Это получено на основе системного анализа с использованием методов информационного противодействия, что позволило учесть специфику угроз и уязвимостей в контексте современной инфраструктуры.

Полученные результаты будут применены для разработки модели управления процессами обеспечения безопасности в следующем разделе.

Глава 2. Разработка модели управления процессами обеспечения безопасности

2.1. Общий подход к разработке модели

2.1. ИИ для in-situ мониторинга и обнаружения дефектов в режиме реального времени

Наиболее эффективным подходом к обеспечению качества является контроль процесса непосредственно во время его протекания (in-situ monitoring). Это

позволяет выявить отклонение на ранней стадии, сэкономить материал, время и, что самое главное, не допустить производства бракованного изделия.

2.1.1. Компьютерное зрение и сверточные нейронные сети (CNN)

Основой систем in-situ мониторинга являются камеры, установленные на 3D-принтерах (как, например, в Creality K1C). Поток видео с камеры анализируется в реальном времени моделью машинного обучения, чаще всего - сверточной нейронной сетью (Convolutional Neural Network, CNN).

Принцип работы:

Сбор данных: Система собирает и размечает тысячи часов видеозаписей успешных и неудачных печать. Дефекты (расслоение, "спагетти-монстр", смещение слоев, недостаточная экструзия) помечаются как целевые классы.

Обучение модели: CNN обучается на массиве данных распознавать визуальные паттерны, соответствующие нормальному ходу печати и различным типам дефектов.

Детекция в реальном времени: Во время печати каждый кадр с камеры анализируется обученной моделью. При обнаружении дефекта с высокой вероятностью система автоматически выполняет заданное действие: приостанавливает печать, отправляет уведомление оператору или пытается скорректировать параметры печати.

Такой подход превращает пассивный процесс печати в активный, управляемый и контролируемый.

2.1.2. Анализ данных с мультисенсорных систем

Для повышения надежности детекции ИИ-системы используют не только визуальные данные, но и информацию с других датчиков:

Акустические сенсоры: Микрофоны записывают звук работающего принтера. ИИ-модель (например, на основе рекуррентных нейронных сетей, LSTM) обучается распознавать "акустический портрет" нормальной работы экструдера, вентиляторов и движущихся механизмов. Отклонения в звуке (скрежет, стук, изменение тональности) могут сигнализировать о механической неисправности или проблеме с подачей пластика.

Термические сенсоры (ИК-камеры): Инфракрасные камеры позволяют контролировать температурное поле печатаемого изделия и стола. ИИ анализирует тепловые карты, выявляя локальные перегревы или недогревы, которые могут привести к деформациям (например, к короблению).

Фьюжн данных (Data Fusion): Наиболее продвинутые системы объединяют данные с всех источников (видео, звук, температура) в единую модель. Такой комплексный анализ позволяет с высокой точностью классифицировать дефекты и их причины, снижая количество ложных срабатываний.

2.2. ИИ для автоматизированной постобработки и коррекции дефектов

Даже при успешной печати изделие редко является готовым продуктом. Этап постобработки (удаление опор, шлифовка, полировка) часто является ручным трудом, который сложно автоматизировать. ИИ решает эту задачу.

2.2.1. Роботизированные манипуляторы с машинным зрением

Системы на базе роботов-манипуляторов, управляемых ИИ, могут выполнять сложные задачи по постобработке:

Удаление опорных структур: 3D-сканер создает цифровую модель готового изделия. ИИ-алгоритм анализирует эту модель, идентифицирует опорные структуры и рассчитывает оптимальную траекторию и усилие для роботизированной руки, чтобы удалить их, не повредив основное изделие.

Автоматическая шлифовка и полировка: ИИ анализирует данные о шероховатости поверхности (полученные от лазерного сканера или тактильных датчиков) и управляет роботом с инструментом (шлифовальной головкой), создавая равномерную поверхность с заданными параметрами.

2.2.2. Оптимизация химических и термических процессов

Для некоторых материалов (например, ABS-пластика) используется химическая обработка парами растворителя для сглаживания поверхности. ИИ-система может:

Анализировать геометрию детали.

Рассчитывать оптимальное время экспозиции и концентрацию паров.

Управлять камерой для химической обработки, чтобы добиться равномерного результата без чрезмерного растворения мелких деталей.

2.3. Информационная безопасность систем ИИ в аддитивном производстве: новые угрозы и векторы атак

Интеграция ИИ в производственную линию, с одной стороны, повышает ее эффективность, а с другой - создает новый класс уязвимостей. Компрометация ИИ-системы может иметь гораздо более катастрофические последствия, чем взлом отдельного 3D-принтера.

2.3.1. Новые информационные активы

Помимо традиционных активов (CAD-модели, G-code), появляются новые, требующие защиты:

Модели машинного обучения: Результат дорогостоящих исследований и обучения. Модель является интеллектуальной собственностью.

Обучающие массивы данных: Данные, на которых обучалась модель. Их компрометация может обесценить всю систему.

Потоки телеметрии в реальном времени: Данные с датчиков, которые являются "органами чувств" ИИ.

2.3.2. Специфические векторы атак на ИИ-системы

Отравление данных (Data Poisoning): Злоумышленник целенаправленно вносит искажения в обучающий массив данных. Например, подмешивает в набор "хороших" принтов изображения с тонкими, незаметными дефектами. В результате ИИ обучится игнорировать эти опасные дефекты, считая их нормой. Это приводит к системному производству скрытого брака.

Атаки на обходимость модели (Model Evasion / Adversarial Attacks): Создание таких дефектов, которые специально "маскируются" под норму для конкретной ИИ-модели. Злоумышленник, зная архитектуру модели, может сгенерировать едва заметное возмущение в G-code, которое приведет к микротрещине, но останется незамеченным системой компьютерного зрения.

Компрометация контура управления: Если ИИ-система имеет возможность не только сигнализировать, но и изменять параметры печати или управлять постобработкой, взлом этой системы дает злоумышленнику полный контроль над качеством продукции. Он может принудительно снижать качество, экономя на материалах, или, наоборот, выводить оборудование из строя.

Кража модели (Model Stealing): Атакующий может многократно отправлять на модель запросы и анализировать ответы, чтобы воссоздать ее копию. Это позволяет конкуренту получить доступ к вашим технологиям контроля качества.

Вывод: вариация показателя P_total составляет 0,038% (от 91,65% до 91,70%), что значительно меньше порога чувствительности 0,1%. Данный результат подтверждает устойчивость модели и корректность выбора весовых коэффициентов.

Сценарий 3: $\alpha = 0{,}75$, $\beta = 0{,}25$

$P\_total = 0{,}75 \times 0{,}91847 + 0{,}25 \times 0{,}91273 = 0{,}68885 + 0{,}22818 = 0{,}91703 = 91{,}70\%$

Сценарий 2: $\alpha = 0{,}70$, $\beta = 0{,}30$ (базовый)

$P\_total = 0{,}70 \times 0{,}91847 + 0{,}30 \times 0{,}91273 = 0{,}64293 + 0{,}27382 = 0{,}91675 = 91{,}68\%$

Сценарий 1: $\alpha = 0{,}65$, $\beta = 0{,}35$

$P\_total = 0{,}65 \times 0{,}91847 + 0{,}35 \times 0{,}91273 = 0{,}59701 + 0{,}31946 = 0{,}91647 = 91{,}65\%$

Для проверки устойчивости модели проанализируем вариацию показателя P_total при изменении весовых коэффициентов:

2.4. Анализ чувствительности

Полученное значение P_total = 91,68% превышает требуемый порог 80%, что подтверждает высокую эффективность разработанной системы.

$P\_total = 91{,}68\%$

$P\_total = 0{,}91675$

$P\_total = 0{,}64293 + 0{,}27382$

$P\_total = 0{,}7 \times 0{,}91847 + 0{,}3 \times 0{,}91273$

Вычислим P_total:

4. Выбор коэффициентов подтвержден проведенным анализом чувствительности (см. подраздел 2.4.7).

3. Весовой коэффициент β = 0,3 сохраняет значимость временной эффективности как вторичного, но важного показателя.

2. При значительном превышении временных норм приоритет смещается в сторону обеспечения успешности ответа системы, что обосновывает больший вес коэффициента α (0,7).

1. Целевые показатели согласно ГОСТ Р 55089-2012:

Текущие значения: Δt_{ip} = 96 мин (превышение в 96 раз), Δt_{np} = 281 мин (превышение в 56 раз)

– время идентификации < 1 мин

– время нейтрализации < 5 мин

Обоснование выбора коэффициентов α = 0,7 и β = 0,3:

где α и β – весовые коэффициенты, удовлетворяющие условию α + β = 1.

P_total = α × P_success + β × P_time

Общая эффективность системы P_total представляет собой взвешенную сумму вероятности успешного ответа и временной эффективности:

Вывод формулы P_total и обоснование весовых коэффициентов

P_time = 0,91273 = 91,27%

P_time = 1 − 0,08727

P_time = 1 − 377 / 4320

P_time = 1 − (96 + 281) / 4320

Выполним расчет:

Данная формула отражает долю времени между проявлениями угроз, которая остается доступной для выполнения других задач системы.

$P\_time = 1 - (\Delta t_{ip} + \Delta t_{np}) / \Delta t_{pp}$

Временная эффективность P_time учитывает скорость реагирования системы на угрозу и рассчитывается как:

2.4.5. Вывод формулы P_time

P_success = 0,91847 = 91,85%

P_success = 0,97826 × 0,93892

Шаг 3. Вычислим P_success:

P_нейтрализации = 0,93892 = 93,89%

P_нейтрализации = 4320 / (4320 + 281) = 4320 / 4601 = 0,93892 = 93,89%

Шаг 2. Вычислим P_нейтрализации:

P_идентификации = 0,97826 = 97,83%

P_идентификации = 4320 / (4320 + 96) = 4320 / 4416 = 0,97826 = 97,83%

Шаг 1. Вычислим P_идентификации:

$P\_нейтрализации = \Delta t_{pp} / (\Delta t_{pp} + \Delta t_{np})$

$P\_идентификации = \Delta t_{pp} / (\Delta t_{pp} + \Delta t_{ip})$

Вероятности успешных действий рассчитываются на основе временных параметров:

P_success = P_идентификации × P_нейтрализации

Вероятность успешного ответа системы P_success определяется как произведение вероятности успешной идентификации и вероятности успешной нейтрализации:

Интерпретация: стационарная вероятность P_{11} = 91,97% означает, что в установившемся режиме система проводит 91,97% времени в безопасном состоянии A_{11}, где угроза идентифицирована и нейтрализована.

P_{11} = 91,97%

P_{11} = 0,919736

P_{11} = 0,00003707 / 0,000040305 = 0,919736

Шаг 4. Вычислим P_{11}:

Знаменатель = 0,000000824 + 0,000002411 + 0,000037070 = 0,000040305

Шаг 3. Вычислим знаменатель:

$\nu_1 \times \nu_2$ = 0,010417 × 0,003559 = 0,000037070

$\lambda \times \nu_1$ = 0,000231 × 0,010417 = 0,000002411

$\lambda \times \nu_2$ = 0,000231 × 0,003559 = 0,000000824

Шаг 2. Вычислим слагаемые знаменателя:

Числитель = $\nu_1 \times \nu_2$ = 0,010417 × 0,003559 = 0,00003707

Шаг 1. Вычислим числитель формулы:

Выполним пошаговый расчет стационарной вероятности P_{11}:

Подстановка значений и вычисление P_{11}

$\nu_2 = 1/\Delta t_{пр} = 1/281 = 0,003559$ 1/мин

$\nu_1 = 1/\Delta t_{ip} = 1/96 = 0{,}010417$ 1/мин

$\lambda = 1/\Delta t_{pp} = 1/4320 = 0{,}000231$ 1/мин

Интенсивности переходов рассчитываются как обратные величины соответствующих времен:

• $\Delta t_{np} = 281$ мин – время нейтрализации угрозы

• $\Delta t_{ip} = 96$ мин – время идентификации угрозы

• $\Delta t_{pp} = 4320$ мин (72 часа) – среднее время проявления угрозы

Исходные временные параметры системы:

Расчет параметров переходов

$P_{11} = (\nu_1 \times \nu_2) / (\lambda \times \nu_2 + \lambda \times \nu_1 + \nu_1 \times \nu_2)$

Решая данную систему, получаем формулу для вероятности целевого состояния A_{11}:

С условием нормировки: $P_{00} + P_{10} + P_{01} + P_{11} = 1$

$\nu_1 P_{10} + \nu_1 P_{01} - 2\nu_2 P_{11} = 0$

$\lambda P_{00} - (\nu_1 + \nu_2) P_{01} + \nu_1 P_{11} = 0$

$\lambda P_{00} - (\nu_1 + \nu_2) P_{10} + \nu_2 P_{11} = 0$

$-(\lambda + \nu_1) P_{00} + \nu_2 P_{01} + \nu_2 P_{10} = 0$

Система уравнений Колмогорова-Чепмена для стационарного режима имеет вид:

• ν_2 – интенсивность нейтрализации угрозы

• ν_1 – интенсивность идентификации угрозы

• λ – интенсивность проявления угрозы

Переходы между состояниями характеризуются следующими интенсивностями:

• A_{11} – выполнены и идентификация, и нейтрализация угрозы (целевое состояние)

• A_{01} – нейтрализация выполнена, идентификация отсутствует

• A_{10} – идентификация выполнена, нейтрализация отсутствует

• A_{00} – отсутствуют идентификация и нейтрализация угрозы (базовое состояние)

Для вывода формулы стационарной вероятности P_{11} рассмотрим граф состояний системы на основе цепи Маркова с четырьмя состояниями:

Вывод формул стационарной вероятности P_{11}

Данный подраздел посвящен математическому обоснованию формул, используемых для оценки эффективности разработанной системы управления информационной безопасностью производственной линии 3D-печати.

2.5 Разработка модели управления информационной безопасностью производственной линии 3д печати. Программные средства

В рамках разработки модели управления информационной безопасностью производственной линии 3D-печати ключевым этапом является трансформация цифровой модели изделия (CAD-файла) в набор конкретных команд для оборудования (G-code). Этот процесс, выполняемый специальным программным обеспечением - слайсером, является не просто технической операцией, а критически важным актом управления в рамках сложной производственной

системы. Выбор слайсера, таким образом, напрямую влияет на управляемость, предсказуемость и безопасность всей линии.

2.5.1 Orca Slicer. Соответствие принципу целенаправленного управления и контролируемости.

В качестве основного программного обеспечения для подготовки управляющих программ в данной работе был выбран Orca Slicer. Данный выбор не является случайным и обоснован его соответствием ключевым принципам теории управления сложными системами и информационного противодействия.

Любая сложная система является целенаправленной, а процесс управления заключается в переводе системы из текущего состояния в целевое. Orca Slicer, являясь модификацией SuperSlicer и Bambu Slicer, предоставляет беспрецедентный уровень детализации и контроля над параметрами печати. Это позволяет не просто «нарезать» модель, а формализовать и точно задавать управляющие воздействия на исполнительные механизмы принтера.

В отличие от упрощенных «черных ящиков», Orca Slicer позволяет исследователю и технологу управлять сотнями параметров: от скорости экструзии и заполнения до калибровки давления и настройки температурных пиков. С точки зрения системного подхода, это означает возможность тонкой настройки законов функционирования подсистемы «3D-принтер» для достижения конкретной цели - получения изделия с заданными физико-механическими свойствами, точностью геометрии и производительностью. Таким образом, Orca Slicer выступает не просто как конвертер, а как инструмент реализации целенаправленного управления технологическим процессом.

Центральной концепцией является информационное противодействие - активное противостояние целенаправленным информационным угрозам. В контексте 3D-печати, G-code является конечным информационным продуктом,

напрямую управляющим физическим процессом. Любое несанкционированное изменение этого кода (в результате вредоносного ПО, атаки на канал передачи или уязвимости в самом слайсере) ведет к саботажу производства, выпуску бракованной или опасной продукции.

Orca Slicer, как проект с открытым исходным кодом (open-source), обеспечивает фундаментальный принцип информационной безопасности - прозрачность. Это позволяет:

Аудит кода: В теоретическом плане, открытый код может быть проанализирован на наличие уязвимостей или закладок. Это исключает ситуацию, когда мы используем непроверенный «черный ящик», чье поведение непредсказуемо.

Верификацию выходных данных: Пользователь имеет полный контроль и понимание того, как настройки преобразуются в G-code. Это позволяет создавать вспомогательные средства верификации, которые могут сравнивать ожидаемую и сгенерированную программу, выявляя аномалии.

Таким образом, выбор Orca Slicer является практической реализацией подхода проактивной защиты. Мы не просто надеемся на защиту периметра, а обеспечиваем контроль и верификацию ключевого информационного потока внутри системы, что является ядром концепции информационного противодействия.

Производственная линия 3D-печати не является статичной системой. Она развивается, появляются новые материалы, обновляется оборудование, меняются производственные задачи. Этот процесс эволюции описывается в теории системогенеза.

Orca Slicer, благодаря своей открытой природе и активному сообществу, обладает высокой адаптивностью. Программное обеспечение может быть модифицировано, интегрировано с другими системами (например, с MES через командную строку или API), дополнено необходимыми плагинами. Это позволяет системе управления информационной безопасностью эволюционировать вместе с объектом защиты. Использование закрытого проприетарного слайсера привело бы к технологической зависимости и создало бы препятствия для развития системы, что противоречит принципам системогенеза, где все компоненты должны быть способны к целенаправленному развитию.

2.5.2 Обоснование выбора платформы виртуализации Proxmox VE как основы для информационно-управляющей подсистемы

В архитектуре производственной линии 3D-печати, рассматриваемой как сложная социотехническая система, особая роль отводится ее информационно-управляющей подсистеме. Именно эта подсистема, включающая серверы баз данных, системы управления производством (MES), файловые хранилища CAD-моделей и узлы подготовки к печати, представляет собой кибернетическое ядро, через которое проходят все ключевые информационные потоки. Ее надежность, управляемость и защищенность напрямую определяют способность всей системы достигать поставленных целей.

В качестве фундаментальной платформы для развертывания данной подсистемы в настоящей работе был выбран гипервизор Proxmox Virtual Environment изображенный на рисунке 1. Этот выбор обусловлен не только его техническими характеристиками, но и глубоким соответствием его архитектурных принципов фундаментальным положениям теории управления сложными системами и информационного противодействия.

Рис. 1 – Интерфейс гипервизора Proxmox Virtual Environment

Согласно теории сложных систем, эффективное управление возможно лишь при четком структурировании объекта управления. Proxmox VE позволяет осуществить рациональную структурную декомпозицию монолитной IT-инфраструктуры на множество изолированных, управляемых модулей - виртуальных машин (VM) и контейнеров (LXC). Каждый такой модуль может быть выделен под выполнение конкретной целевой функции:

ВМ для системы управления производством (MES).

ВМ для сервера баз данных технологических параметров.

Контейнер для файлового хранилища с интеллектуальной собственностью (CAD-модели).

ВМ для узла подготовки управляющих программ (Orca Slicer).

Такой подход позволяет представить сложную подсистему в виде иерархической структуры, что полностью соответствует принципам структурно-лингвистического моделирования. При этом Proxmox предоставляет единый контур управления через централизованную веб-панель и API. Это позволяет осуществлять целенаправленное, скоординированное воздействие на все элементы структуры, что является ключевым требованием для управления сложной системой.

Центральной идеей теории информационного противодействия является не пассивная оборона, а активное управление информационными потоками для парирования целенаправленных угроз. Архитектура Proxmox VE имманентно (внутренне) приспособлена для реализации этого принципа.

Механизм виртуализации обеспечивает строгую изоляцию адресных пространств, ресурсов и процессов между виртуальными машинами. Это означает, что компрометация одного из модулей (например, взлом веб-интерфейса MES) не приводит к автоматическому распространению угрозы на другие критически

важные узлы, такие как база данных или сервер с G-code. Таким образом, Proxmox реализует на практике стратегию локализации и сдерживания информационного воздействия, минимизируя потенциальный ущерб от атаки. Встроенный межсетевой экран, настраиваемый на уровне отдельных ВМ и контейнеров, позволяет детально регламентировать информационные обмены между ними, что является прямым инструментом активного информационного противодействия.

Производственная линия 3D-печати является эволюционирующей системой, проходящей этапы системогенеза. На этапе эксплуатации ключевым требованием становится ее устойчивость к внешним и внутренним возмущениям. Proxmox VE предоставляет инструментарий для обеспечения этого свойства.

Функционал High Availability (HA) позволяет автоматически перезапускать критичные виртуальные машины на исправных физических узлах кластера в случае сбоя оборудования. Это обеспечивает непрерывность функционирования целевых функций системы и ее живучесть. Механизмы резервного копирования и восстановления являются неотъемлемой частью цикла информационного противодействия, обеспечивая возможность быстрого возврата системы в штатное (эталонное) состояние после успешной атаки или критического сбоя. Таким образом, Proxmox поддерживает систему на всех стадиях ее жизненного цикла, от развертывания до эволюционного развития и восстановления, что полностью соответствует концепции системогенеза.

Использование проприетарных (закрытых) решений в качестве основы для критически важной инфраструктуры создает непрозрачный «черный ящик», поведение которого невозможно полностью контролировать. Это противоречит принципам проактивной защиты. Proxmox VE является решением с открытым исходным кодом, что обеспечивает его прозрачность.

В контексте настоящей работы это означает, что теоретически возможен аудит кода гипервизора на наличие уязвимостей или недекларированных возможностей. Это повышает доверие к базовому элементу системы управления и снижает риски, связанные с использованием непроверенного ПО. Данный принцип согласуется с идеологией информационного противодействия, требующей полного контроля над всеми элементами системы, участвующими в обработке и передаче информации.

2.5.3 Обоснование использования платформы Home Assistant в качестве человеко-машинного интерфейса и узла управления

В рамках разработки комплексной модели управления информационной безопасностью производственной линии 3D-печати особое внимание уделяется не только защитным механизмам, но и построению эффективного, управляемого и контролируемого контура взаимодействия между оператором (человеческой подсистемой) и производственным оборудованием (технической подсистемой). Для реализации данной функции в настоящей работе была выбрана платформа Home Assistant изображенная на рисунке 2.

Рисунок 2 – Интерфейс программы Home Assistant

На первый взгляд, выбор платформы, изначально ориентированной на «умный дом», для промышленной задачи может показаться неочевидным. Однако, при рассмотрении данной теории управления сложными системами и информационного противодействия этот выбор становится концептуально обоснованным и стратегически верным.

Производственная линия 3D-печати является классической социотехнической системой, где эффективность и безопасность напрямую зависят от качества взаимодействия человека и машины. Home Assistant в данном контексте выступает не просто как панель управления, а как формализованный человеко-

машинный интерфейс (HMI), который является ключевым элементом контура управления.

Платформа позволяет создавать настраиваемые дашборды (LOVACE-интерфейсы), которые отображают не только состояние принтеров (температура, прогресс печати, видеопоток), но и предоставляют оператору строго определенный набор управляющих воздействий: «Старт», «Пауза», «Стоп», «Смена материала». Таким образом, Home Assistant реализует принцип целенаправленного управления, где оператор не взаимодействует с низкоуровневыми и потенциально опасными интерфейсами (например, отправкой произвольного G-code), а выполняет целенаправленные действия в рамках заданной системы правил. Это снижает вероятность ошибок, вызванных человеческим фактором, и ограничивает возможности для несанкционированных действий.

Ключевым аспектом теории информационного противодействия является не пассивная защита, а активное управление информационными потоками для парирования угроз. Home Assistant предоставляет уникальные возможности для реализации этого принципа на уровне управления:

Абстрагирование и нормализация команд: Платформа интегрируется с 3D-принтерами (через API OctoPrint, Klipper/Moonraker и др.) и преобразует сложные низкоуровневые API-запросы в простые, высокоуровневые сущности (кнопки, переключатели). Оператор инициирует событие «начать печать», а Home Assistant сам формирует корректный и безопасный API-запрос. Это нормализует информационный поток от человека к машине, исключая передачу некорректных или вредоносных команд.

Аудит и протоколирование действий: Home Assistant ведет подробный журнал всех событий и действий. Каждая команда, отправленная на принтер, привязывается к учетной записи пользователя, инициировавшего ее. Это создает

неотъемлемый след действий, который является критически важным для анализа инцидентов информационной безопасности. В случае саботажа или ошибки, система позволяет точно reconstructed цепочку событий и идентифицировать виновника, что является неотъемлемой частью процесса информационного противодействия.

Ролевое управление доступом (RBAC): Платформа позволяет настраивать права доступа для различных пользователей. Оператор может только запускать и останавливать печать, технолог - изменять температурные режимы, а администратор - управлять конфигурацией системы. Это реализует один из фундаментальных принципов безопасности - разделение привилегий и минимизацию прав, напрямую управляя информационными потоками на основе ролей в системе.

Производственная линия, как и любая сложная система, проходит этапы системогенеза - развития и эволюции. Закрытые, монолитные промышленные SCADA-системы часто становятся тормозом для этого процесса из-за своей негибкости и высокой стоимости модификации.

Home Assistant, как платформа с открытым исходным кодом, обладает высокой адаптивностью. Добавление нового 3D-принтера, нового датчика контроля окружающей среды или интеграция с системой MES/ERP не требует переписывания всей системы. Достаточно добавить новую интеграцию и настроить логику ее работы. Это позволяет управляющей подсистеме эволюционировать вместе с объектом управления, не становясь «узким местом». Такая гибкость полностью соответствует идеологии системогенеза, где система должна быть способна к целенаправленному развитию и адаптации к меняющимся условиям.

2.5.4 Обоснование выбора управляющей прошивки Klipper как основы контура управления технической подсистемой

В архитектуре производственной линии 3D-печати, рассматриваемой как сложная социотехническая система, управляющая прошивка 3D-принтера играет роль периферической нервной системы. Она преобразует высокоуровневые команды (например, «переместить экструдер в точку X,Y,Z») в последовательность низкоуровневых сигналов для шаговых двигателей, нагревателей и других исполнительных механизмов. Выбор этой прошивки является не просто техническим решением, а фундаментальным фактором, определяющим управляемость, точность и защищенность всей технической подсистемы.

В качестве управляющей прошивки для 3D-принтеров в рамках данной работы был выбран Klipper изображенный на рисунке 3. Данный выбор обусловлен его уникальной архитектурой, которая концептуально соответствует фундаментальным положениям теории управления сложными системами и информационного противодействия.

Рисунок 3 – Интерфейс программы Klipper

Ключевой инновацией Klipper является его двухуровневая архитектура. Она разделяет вычислительные и управляющие функции между двумя компонентами:

Хост-система: Мощный одноплатный компьютер (например, Raspberry Pi), на котором выполняется основная логика Klipper. Он отвечает за сложные вычисления (кинематические преобразования, обработку G-code), взаимодействие с сетью и внешними системами.

Платы-клиенты: «Простые» микроконтроллеры (например, на базе STM32, AVR), которые подключены к оборудованию принтера. Их единственная задача - в реальном времени генерировать высокоточные сигналы для шаговых двигателей и нагревателей.

Такое разделение является блестящей практической реализацией принципа структурной декомпозиции сложной системы. Вместо монолитного «черного ящика» мы получаем четко структурированную систему, где высокоуровневый контур управления (стратегическое планирование) отделен от низкоуровневого контура (тактическое исполнение), что повышает управляемость и наблюдаемость системы. Хост-система становится полноценным элементом общей информационной сети, что позволяет интегрировать его в единый контур управления производственной линией, а не изолировать как отдельное устройство.

В отличие от многих проприетарных прошивок, где конфигурация скрыта в бинарных файлах, Klipper использует текстовый конфигурационный файл printer.cfg. Этот файл является не просто набором настроек, а формальным описанием структуры и законов функционирования технической подсистемы.

Структура: Определяются все компоненты ([stepper_x], [extruder], [heater_bed]).

Параметры: Задаются их свойства и связи (step_pin, rotation_distance, pid_kp).

Правила: Описывается логика их взаимодействия.

Такой подход обеспечивает полную прозрачность и верифицируемость системы. Конфигурация может быть помещена под систему контроля версий (например, Git), что позволяет отслеживать все изменения, откатываться к рабочим состояниям и проводить аудит. Это критически важно для обеспечения информационной безопасности, так как исключает возможность несанкционированных и незаметных изменений в параметрах работы оборудования.

Для взаимодействия с внешним миром (включая пользовательские интерфейсы, такие как Mainsail/Fluidd или системы верхнего уровня, как Home

Assistant) Klipper использует API-сервер Moonraker. Это не просто техническая деталь, а ключевой элемент реализации концепции информационного противодействия.

Moonraker выступает в роли единого, контролируемого шлюза для всех информационных потоков, направляемых к принтеру. Это позволяет реализовать на его уровне все необходимые механизмы безопасности:

Аутентификация и авторизация: Доступ к управлению принтером могут получить только авторизованные пользователи и системы.

Протоколирование: Moonraker логирует все команды и запросы, создавая полную картину взаимодействий для последующего анализа инцидентов.

Фильтрация: API позволяет фильтровать и нормализовать команды, предотвращая отправку на принтер некорректных или потенциально опасных инструкций.

Таким образом, Moonraker превращает потенциально уязвимый сетевой интерфейс в управляемый и защищенный канал, что полностью соответствует идеологии проактивного информационного противодействия.

Производственная линия 3D-печати - это эволюционирующая система. Модульная архитектура Klipper, основанная на текстовой конфигурации и открытом исходном коде, обеспечивает высокую адаптивность. Добавление нового датчика, смена экструдера или даже полная перенастройка кинематики не требуют смены прошивки, а лишь редактирования конфигурационного файла и, при необходимости, подключения соответствующего микроконтроллера.

Это полностью соответствует принципам системогенеза, где система должна быть способна к целенаправленному развитию и адаптации к новым задачам без кардинальной перестройки своей основы. Klipper позволяет технической

подсистеме эволюционировать синхронно с развитием всей производственной линии.

2.5.5 Обоснование использования системы мониторинга 3D-Print-Sentinel как подсистемы обнаружения физических проявлений угроз

В рамках построения комплексной модели управления информационной безопасностью производственной линии 3D-печати недостаточно контролировать лишь цифровые потоки данных. Критически важным является контроль за физическим воплощением этих данных - самим процессом аддитивного производства. Угрозы, будь то кибератака на управляющий G-code или внутренний сбой оборудования, в конечном итоге проявляются в физическом дефекте печатаемого изделия. Для своевременного обнаружения таких проявлений в данной работе используется открытый проект 3D-Print-Sentinel.

Одним из ключевых требований к управлению сложной системой является ее наблюдаемость - возможность получать информацию о ее текущем состоянии. В процессе 3D-печати техническая подсистема (принтер) в значительной степени является «черным ящиком». Оператор не имеет возможности непрерывно и автоматически контролировать корректность формирования каждого слоя, что создает риск пропуска критического отказа.

Система 3D-Print-Sentinel решает эту проблему, формируя дополнительный контур наблюдения. Используя методы компьютерного зрения (библиотека OpenCV), она в реальном времени анализирует видеопоток с камеры, направленной на зону печати, и выявляет аномалии, такие как классический отказ «спагетти-монстр», отслоение модели или другие значительные дефекты.

Таким образом, 3D-Print-Sentinel кардинально повышает наблюдаемость внутреннего состояния технологического процесса. иПолучив сигнал о

неисправности, система или оператор получают возможность для управляемого воздействия - своевременной остановки печати. Это превращает разомкнутый процесс «запустил и забыл» в управляемый замкнутый контур, способный к самокоррекции.

Концепция информационного противодействия предполагает не только защиту от прямых кибератак, но и противодействие их последствиям. 3D-Print-Sentinel является уникальным инструментом, который обнаруживает физические манифестации информационных угроз:

Противодействие саботажу: Злоумышленник, модифицировавший G-code (например, снизив температуру экструдера или скорость печати), рассчитывает на создание скрытого дефекта, который приведет к преждевременному выходу изделия из строя в условиях эксплуатации. Sentinel способен обнаружить аномальное поведение печати (например, недоэкструзию, приводящую к разрыву слоев) на ранней стадии, тем самым раскрывая факт информационного воздействия через его физический результат.

Локализация последствий внутренних сбоев: Не все угрозы внешние. Внутренние сбои (износ сопла, сбой подачи пластика) также являются возмущающими воздействиями на систему. Sentinel, обнаруживая такие сбои, минимизирует экономический ущерб (экономит время и материал) и предотвращает возможную поломку оборудования, что является частью общей стратегии обеспечения живучести системы.

Таким образом, Sentinel работает на ключевом этапе цикла информационного противодействия - обнаружении и реагировании. Он не предотвращает саму атаку, но делает ее последствия видимыми и управляемыми, позволяя оперативно локализовать инцидент.

Производственная линия 3D-печати, как сложная система, должна обладать способностью к развитию и адаптации. 3D-Print-Sentinel, будучи проектом с открытым исходным кодом, представляет собой идеальный модульный компонент для такой эволюции.

Его архитектура позволяет интегрировать его в общую систему управления. Например, Sentinel может автоматически отправлять сигнал о сбое в систему верхнего уровня, такую как Home Assistant, которая, в свою очередь, через API Moonraker/Klipper отправит команду на паузу печати. Это создает полностью автоматизированный контур противодействия: обнаружение физической аномалии → информационный сигнал → управляющее воздействие.

Такая модульная интеграция демонстрирует на практике, как сложная система может наращивать свою функциональность и устойчивость, не претерпевая кардинальной перестройки, что полностью соответствует принципам системогенеза, где развитие происходит через целенаправленное добавление и связывание новых подсистем.

2.6 Роль и значение аппаратной составляющей в контексте управления безопасностью сложной производственной системы

При разработке модели управления информационной безопасностью производственной линии 3D-печати существует соблазн сконцентрироваться исключительно на программных и организационных мерах защиты: антивирусах, межсетевых экранах, политиках доступа. Однако такой подход является неполным и, с точки зрения теории управления сложными системами, фундаментально ошибочным. Аппаратная часть - совокупность физических устройств, от 3D-принтеров и серверов до сетевого оборудования и датчиков - является не пассивным фундаментом, а активным, имманентно встроенным элементом системы, без которого понимание и обеспечение ее безопасности невозможно.

Цель производственной линии 3D-печати - физическое преобразование цифрового проекта в материальный объект. Именно аппаратная составляющая является тем материальным субстратом, который непосредственно реализует эту цель. Информационные потоки (CAD-модели, G-code) остаются лишь абстракцией без физического исполнителя.

Качество, точность и надежность аппаратных средств (принтеров, роботов-манипуляторов) напрямую детерминируют верхнюю границу достижимых системой целей. Невозможно получить изделие с допуском в 10 микрон на принтере, конструктивная погрешность которого составляет 100 микрон. Таким образом, выбор аппаратного обеспечения - это не инженерный, а стратегический управленческий акт, определяющий потенциал всей системы. Игнорирование этого аспекта делает бессмысленным любые попытки точного управления, так как объект управления (аппаратная часть) физически не способен отработать заданные параметры.

Эффективное управление сложной системой невозможно без управляемости и наблюдаемости. Аппаратная часть формирует как контур управления, так и контур наблюдения.

Контур управления: Исполнительные механизмы принтеров (двигатели, нагреватели) - это конечные точки, куда поступают управляющие сигналы. Их характеристики (быстродействие, инерционность, точность) определяют задержки и погрешности в контуре управления. Устаревшее или некачественное оборудование становится источником неопределенности, который невозможно скомпенсировать на программном уровне.

Контур наблюдения: Датчики (термопары, энкодеры, камеры) являются «органами чувств» системы. Без них система «слепа» и не может адекватно реагировать на возмущения. Например, система 3D-Print-Sentinel, описанная ранее,

полностью зависит от качества аппаратной части - камеры и освещения. Неточный датчик - неверные данные. Неверные данные - неправильное решение управляющей системы.

Таким образом, аппаратное обеспечение является неотъемлемой частью информационной системы, формирующей потоки данных как на входе, так и на выходе.

Концепция информационного противодействия рассматривает безопасность как активный процесс противостояния угрозам. Аппаратное обеспечение является одной из главных арен этого противодействия по нескольким причинам:

Исполнитель информационных атак: Большинство целевых атак на производство (например, изменение G-code) нацелены на то, чтобы заставить аппаратуру выполнить некорректные или разрушительные действия. Успех атаки измеряется не в украденном файле, а в сломанном станке, испорченном продукте или нарушении технологического процесса. Следовательно, защита аппаратуры от выполнения вредоносных команд - конечная цель киберзащиты.

Вектор атаки: Сами физические устройства могут быть точками входа для злоумышленника. Незащищенные порты USB, сетевые интерфейсы с настройками по умолчанию, отсутствие физической защиты серверов - все это аппаратные уязвимости, которые открывают доступ к информационным системам.

Источник возмущений, маскирующихся под атаки: Сбой аппаратного обеспечения (например, выход из строя терморезистора) может иметь симптомы, идентичные кибератаке (команда на перегрев). И наоборот, целенаправленная атака может быть замаскирована под обычный аппаратный сбой. Без глубокого понимания базовых физических процессов и характеристик аппаратной части невозможно эффективно проводить расследование инцидентов и отличить одно от другого.

Процесс создания и развития системы - системогенез - сильно зависит от первоначального выбора аппаратной платформы. Выбор закрытого, проприетарного оборудования с неподдерживаемыми протоколами создает «технологическую яму», препятствующую развитию и адаптации системы. Это снижает ее живучесть - способность сохранять функции при повреждениях или в меняющихся условиях.

Напротив, выбор модульного, открытого оборудования (как в случае с Klipper, где хост и микроконтроллеры разделены) закладывает в систему потенциал для эволюции. Такая система может быть модернизирована, масштабирована и адаптирована к новым угрозам, что является ключевым требованием для долговечной и безопасной производственной линии.

2.6.1 Обоснование использования сетевого оборудования MikroTik как основы для управления информационными потоками и реализации контура противодействия

В архитектуре производственной линии 3D-печати, рассматриваемой как сложная социотехническая система, сетевая инфраструктура играет роль кровеносной и нервной системы одновременно. Именно по ней циркулируют информационные потоки, являющиеся как основой жизнедеятельности, так и главным объектом потенциальных угроз. Выбор оборудования для построения этой инфраструктуры, таким образом, является не техническим, а стратегическим решением, определяющим базовые возможности по управлению и защите всей системы.

В качестве основы для построения сетевой инфраструктуры в настоящей работе было выбрано оборудование MikroTik представленный на рисунке 4. Данный выбор обусловлен не его стоимостью или распространенностью, а его фундаментальным соответствием ключевым принципам теории управления сложными системами и информационного противодействия.

Рисунок 4 – Интерфейс программы управления маршрутизатора Microtik

С точки зрения теории сложных систем, сеть - это не просто набор кабелей и портов, а структурированная среда для обмена информацией между подсистемами (Proxmox, Klipper, Home Assistant, 3D-Print-Sentinel). Оборудование MikroTik, работающее под управлением операционной системы RouterOS, позволяет превратить пассивную среду в активно управляемую структуру.

С помощью мощного межсетевого экрана (Firewall), механизмов маркировки трафика (Mangle) и политик маршрутизации, MikroTik предоставляет возможность целенаправленно управлять информационными потоками. Можно не просто разрешать или запрещать доступ, но и приоритизировать критически важный трафик (например, команды управления принтером), ограничивать второстепенный (например, обновления ПО) и перенаправлять подозрительные потоки на «песочницу» для анализа. Это превращает сетевое оборудование из пассивного ретранслятора в полноценный элемент контура управления, что является ключевым требованием для управления сложной системой.

Центральная идея информационного противодействия заключается в локализации и парировании угроз. MikroTik предоставляет исчерпывающий инструментарий для практической реализации этого принципа на сетевом уровне.

Сегментация сети (VLANs): с помощью виртуальных локальных сетей (VLAN) можно логически изолировать различные подсистемы. Например, можно создать отдельные VLAN для производственного оборудования (принтеры с Klipper), для серверной инфраструктуры (Proxmox), для систем мониторинга (камеры, Home Assistant) и для административных нужд. Компрометация одного сегмента (например, рабочей станции оператора) не приведет к автоматическому распространению угрозы на критически важные серверы или принтеры. Это

является прямым воплощением стратегии сдерживания и локализации информационного воздействия.

Глубокая фильтрация трафика: Firewall MikroTik позволяет создавать правила с детальной гранулярностью (по IP-адресам, портам, протоколам, времени суток). Это обеспечивает тонкий контроль над всеми информационными обменами, позволяя реализовать политику минимальных привилегий на сетевом уровне.

Одной из важнейших задач обеспечения безопасности является возможность аудита и верификации системы. RouterOS, управляющая оборудованием MikroTik, предоставляет мощный интерфейс командной строки (CLI) и возможность экспорта полной конфигурации в виде текстового скрипта.

Этот скрипт является не просто набором команд, а формальным языком описания структуры и правил функционирования сетевой подсистемы. Он полностью соответствует принципу структурно-лингвистического моделирования. Конфигурация сети, как и конфигурация Klipper, может быть помещена под систему контроля версий (например, Git). Это позволяет:

Отслеживать все изменения в правилах безопасности.

Быстро откатываться к последней рабочей версии после некорректной модификации.

Проводить автоматизированный аудит конфигурации на соответствие политикам безопасности.

Такой подход обеспечивает прозрачность и верифицируемость одного из самых критичных элементов системы, что является фундаментальным требованием для построения доверенной и защищенной инфраструктуры.

Эффективное управление невозможно без наблюдаемости. MikroTik предоставляет широкие возможности для мониторинга состояния сети: детальные

логи всех проходящих через firewall пакетов, учет трафика, поддержка протокола SNMP, а также наличие собственной системы сетевого мониторинга The Dude. Это позволяет в реальном времени наблюдать за информационными потоками, выявлять аномалии (например, всплеск трафика на нетипичном порту) и оперативно реагировать на них, получая полную картину происходящего в «нервной системе» производственной линии.

2.6.2 Обоснование использования управляемого коммутатора HP 1820-24G как структурного элемента системы управления информационными потоками

В архитектуре отказоустойчивого кластера на базе Proxmox VE, построенного на компьютерах HP Compaq 8000, ключевым связующим звеном является сетевая инфраструктура. Выбор коммутатора, который объединяет узлы кластера и другие подсистемы производственной линии, является не менее важным решением, чем выбор серверного оборудования. В данной работе был выбран управляемый коммутатор HP 1820-24G. Этот выбор, на первый взгляд технический, на самом деле является концептуальным и полностью соответствует фундаментальным принципам теории управления сложными системами и информационного противодействия.

Свойства сложной системы определяются не столько ее элементами, сколько структурой связей между ними. Коммутатор HP 1820-24G является не просто «сетевым хабом», а физическим воплощением этой структуры. Он формирует единую информационную среду и устанавливает управляемые каналы обмена данными между ключевыми элементами системы:

Между узлами кластера Proxmox для синхронизации состояния и миграции виртуальных машин.

Между виртуальными машинами и системами хранения данных.

Между управляющими системами (Home Assistant, Klipper) и исполнительными устройствами (3D-принтерами).

Надежность и производительность этих связей напрямую влияют на управляемость и живучесть всей системы. Сбой в работе коммутатора равносилен разрыву нервной системы, что приводит к параличу кластера и остановке производства. Таким образом, коммутатор - это критически важный структурный элемент, от качества которого зависит эмерджентное свойство системы в целом - ее способность к целенаправленному функционированию.

Центральная идея информационного противодействия - это активное управление информационными потоками для парирования угроз. Неуправляемый коммутатор (unmanaged switch) является пассивным проводником и не предоставляет инструментов для защиты. HP 1820-24G, как управляемое устройство, позволяет реализовывать проактивные меры безопасности на сетевом уровне:

Сегментация сети (VLANs): Ключевой функцией для обеспечения безопасности является создание виртуальных локальных сетей (VLAN). С помощью HP 1820-24G можно логически изолировать трафик кластера Proxmox от трафика производственных устройств (принтеров) и от трафика пользовательских сетей. Это является прямым воплощением стратегии локализации и сдерживания информационного воздействия. Компрометация пользовательской рабочей станции не приведет к возможности атаковать критически важные сервисы кластера, так как они находятся в разных логических сегментах.

Контроль доступа (ACLs): Коммутатор поддерживает списки контроля доступа (ACL), позволяющие фильтровать трафик на более детальном уровне - ограничивая доступ к сервисам кластера только с определенных IP-адресов или

портов. Это создает дополнительный барьер на пути злоумышленника, реализуя принцип глубокоэшелонированной обороны.

Эффективное управление сложной системой невозможно без наблюдаемости. Коммутатор HP 1820-24G предоставляет необходимые инструменты для мониторинга состояния информационной среды:

Статистика портов: Возможность отслеживать загрузку каждого порта, количество ошибок и отброшенных пакетов позволяет диагностировать проблемы на физическом уровне (неисправный кабель, сетевая карта) еще до того, как они повлияют на работу кластера.

Поддержка SNMP: Протокол SNMP позволяет интегрировать коммутатор в единую систему мониторинга (например, Zabbix или Grafana), получая данные о его состоянии в реальном времени. Это создает единый контур наблюдения за всей IT-инфраструктурой, что является обязательным условием для своевременного обнаружения аномалий и реагирования на инциденты.

Функция отказоустойчивости (High Availability) кластера Proxmox критически зависит от бесперебойной и низкозадержной связи между узлами. Коммутатор HP 1820-24G обеспечивает эту связь, являясь, по сути, энаблером (обеспечивающим элементом) живучести всей системы. Без надежного коммутатора механизм автоматической миграции виртуальных машин не сможет корректно работать, и вся концепция отказоустойчивости будет скомпрометирована.

Кроме того, использование стандартного управляемого коммутатора с понятным интерфейсом конфигурации соответствует принципам системогенеза. Он является модульным, заменяемым компонентом. В случае его выхода из строя или необходимости масштабирования (например, перехода на модель с большей

пропускной способностью), его можно заменить с минимальным влиянием на работу всей системы, что обеспечивает ее способность к развитию и адаптации.

2.6.3 Обоснование использования аппаратной платформы на базе HP Compaq 8000 для развертывания отказоустойчивого кластера Proxmox

В рамках построения информационно-управляющей подсистемы производственной линии 3D-печати была выбрана аппаратная платформа, состоящая из трех однотипных компьютеров HP Compaq 8000 Elite, на которых развернута гипервизорная среда Proxmox VE и объединена в единый кластер. На первый взгляд, использование не новых, не серверных компьютеров может показаться компромиссом. Однако с точки зрения теории управления сложными системами и информационного противодействия, этот выбор является не только экономически целесообразным, но и концептуально обоснованным решением, демонстрирующим ключевые принципы построения живучих систем.

Центральной задачей при создании любой ответственной системы является обеспечение ее живучести - способности сохранять базовые функции при возникновении сбоев и целенаправленных воздействий. Классический подход, основанный на одном мощном сервере, создает единую точку отказа (Single Point of Failure). Выход такого сервера из строя - будь то аппаратная поломка, ошибка в ПО или результат успешной кибератаки - парализует всю производственную линию.

Выбор трех компьютеров HP Compaq 8000 и их объединение в кластер Proxmox является практической реализацией принципа структурной избыточности. В такой архитектуре функция «сервер» декомпозирована на три физических узла. Критически важные виртуальные машины (например, ВМ с MES или узел управления Klipper) переводятся в режим High Availability (HA). В случае отказа любого из трех физических узлов, кластер автоматически и без вмешательства оператора перезапускает критичные ВМ на одном из оставшихся исправных узлов.

Таким образом, живучесть системы становится не свойством отдельного элемента, а эмерджентным (системным) свойством всей структуры. Система противостоит возмущающему воздействию (отказу узла) не за счет избыточной мощности одного элемента, а за счет грамотной организации связей между несколькими элементами.

Использование относительно несложных компьютеров HP Compaq 8000 намеренно подчеркивает важнейший принцип системного анализа: организация системы важнее суммы свойств ее элементов. Вместо того чтобы вкладывать ресурсы в один сверхмощный сервер, мы распределили их по нескольким узлам и создали интеллектуальную управляющую структуру (кластер Proxmox).

Этот подход доказывает, что высокая надежность и управляемость могут быть достигнуты не только за счет «железа», но и за счет грамотной архитектуры. Это заставляет проектировщика сфокусироваться на качестве связей, алгоритмах отказоустойчивости и логике распределения ресурсов, что является сутью управления сложными системами. Производственная линия становится защищенной не потому, что в ней стоит «недоступный» сервер, а потому, что ее архитектура изначально спроектирована так, чтобы пережить отказ любого из своих компонентов.

В концепции информационного противодействия важна не только пассивная защита, но и активный ответ на угрозу. Кластер Proxmox на базе HP Compaq 8000 является инструментом именно такого активного противодействия.

Рассмотрим сценарий целевой атаки на один из физических узлов. Злоумышленнику, например, удалось вывести из строя компьютер, на котором работала ВМ с файловым хранилищем. В монолитной системе это привело бы к катастрофе. В кластерной архитектуре система реагирует на воздействие автоматически:

Обнаружение: Кластерные сервисы (Corosync/Pacemaker) фиксируют недоступность узла.

Противодействие: Система немедленно инициирует процедуру восстановления, изолируя поврежденный элемент и перезапуская критически важную функцию (виртуальную машину) на безопасном ресурсе.

Таким образом, кластер превращает потенциальную катастрофу в управляемый инцидент, минимизируя время простоя и предотвращая нарушение целостности производственного процесса. Это и есть проактивное информационное противодействие в действии.

Производственная система находится в постоянном развитии. Она может расширяться, усложняться, ее требования к ресурсам могут меняться. Использование стандартной, коммодитизированной аппаратной платформы, такой как HP Compaq 8000, обеспечивает высокую адаптивность и экономическую эффективность этого процесса.

В случае выхода из строя одного из узлов, его можно заменить аналогичным компьютером в течение короткого времени и с минимальными затратами. Нет зависимости от конкретного поставщика дорогих серверных компонентов или длительных сроков поставки. Это делает систему более пластичной и способной к эволюции, что полностью соответствует принципам системогенеза, где система должна быть готова к развитию и адаптации к меняющимся условиям.

2.6.4 Обоснование выбора и модификации аппаратной платформы 3D-принтера Creality K1C в контексте системогенеза и информационного противодействия

В качестве основного технологического оборудования - исполнительного органа производственной линии 3D-печати - в данной работе был выбран современный высокоскоростной принтер Creality K1C. Данный выбор не является

случайным и обусловлен не только его высокими техническими характеристиками (кинематика Core XY, высокая скорость печати, наличие камеры), но и его концептуальной пригодностью для демонстрации ключевых принципов управления сложными системами.

Принтер K1C рассматривается в данной работе не как готовое изделие, а как прототип подсистемы, требующий целенаправленной доработки для интеграции в сложную производственную систему. Его заводская конфигурация, ориентированная на массового потребителя, представляет собой, с точки зрения системного анализа, «черный ящик» с закрытым проприетарным прошивочным обеспечением.

В теории управления сложными системами ключевыми требованиями к объекту управления являются управляемость и наблюдаемость. Стандартная прошивка K1C, будучи закрытой, не позволяет выполнять эти требования в полной мере:

Низкая наблюдаемость: Мы не можем в полной мере контролировать внутренние процессы прошивки, анализировать, как именно она интерпретирует G-code, и получать исчерпывающую телеметрию о состоянии системы.

Низкая управляемость: Возможности по тонкой настройке кинематики, температурных режимов и других параметров ограничены интерфейсом, предоставленным производителем. Мы не можем управлять системой на том уровне детализации, который необходим для достижения целей промышленного производства.

Таким образом, принтер в его исходном состоянии является неадекватным элементом для сложной системы, так как он не поддается целенаправленному управлению и не обеспечивает прозрачности своих процессов.

Для решения указанной проблемы в рамках данной работы производится замена штатного прошивочного обеспечения на открытую управляющую систему Klipper. Этот шаг является не просто технической модернизацией, а практической реализацией процесса системогенеза - целенаправленного формирования системы с заданными свойствами.

Преобразование структуры: Установка Klipper кардинально меняет архитектуру управляющей подсистемы принтера, разделяя ее на хост-систему и клиентские микроконтроллеры. Это превращает принтер из монолитного устройства в структурированную, управляемую систему.

Обеспечение управляемости и наблюдаемости: Klipper, как было показано ранее, предоставляет полный контроль над всеми параметрами через текстовый конфигурационный файл. Это является примером структурно-лингвистического моделирования, где поведение системы описывается на формальном языке. Мы получаем полный контроль и наблюдаемость над процессом.

Интеграция в сложную систему: благодаря API-серверу Moonraker, принтер перестает быть изолированным устройством и становится полноценным сетевым узлом, способным взаимодействовать с Home Assistant, Proxmox и другими элементами производственной линии.

Выбор K1C в качестве аппаратной платформы и его последующая модификация напрямую связаны с концепцией информационного противодействия.

Устранение непрозрачного элемента: Замена закрытой прошивки на открытую (Klipper) устраняет один из самых опасных векторов атаки - недекларированные возможности или уязвимости в проприетарном ПО. Мы заменяем непроверенный компонент на верифицируемый.

Создание контролируемого шлюза: Система Moonraker, работающая поверх Klipper, становится единственным, строго контролируемым шлюзом для всех управляющих команд. Это позволяет реализовать на его уровне аутентификацию, авторизацию и протоколирование, что является ядром проактивного информационного противодействия.

Использование встроенных средств для контроля: Наличие в K1C камеры позволяет интегрировать его с системой 3D-Print-Sentinel, создавая замкнутый контур управления, где физические проявления угроз (дефекты печати) немедленно обнаруживаются и приводят к управляющему воздействию (остановке печати).

2.6.5 Сетевое моделирование процессов обеспечения безопасности

На основе вышеописанной модели управления требуется разработать технологию управления процессом обеспечения безопасности системы.

Процесс обеспечения безопасности данной системы реализуется технологией управления этой системы.

Технология управления –преобразование информационных и деятельностных ресурсов в интересах достижения цели управления [10].

Общий подход к разработке технологии управления процессом обеспечения безопасности системы включает в себя несколько этапов.

1 этап. Обоснование оценивания основных свойств технологий.

Обоснование требует:

классифицирование угроз по типам;

определить уровень опасности в системе в зависимости от воздействия угроз;

разработать методику обоснования путей снижения уровня опасности до приемлемого уровня.

Оценивание предполагает:

формализацию процессов воздействий в рамках теории нестационарных потоков Пуассона

обоснование требуемых действий

представление потерь системой уравнением результативности действий

Оценивание позволяет:

обосновать рациональные этапы и методы их реализации на основе разработанной модели;

обосновать возможности СОБ;

представить требования к возможностям ЛПР.

2 этап. Формирование показателя эффективности реализации управленческого решения.

Робсл=РИНП – вероятность идентификации и нейтрализации проблемы.

Вероятность того, что каждая угроза будет идентифицирована (система мониторинга) и нейтрализована (Силы и средства системы по обеспечению безопасностью (СОБ)) определяется соотношением:

Составляющие этого уравнения определяются на основе решения системы дифференциальных или алгебраических уравнений в зависимости от предположений.

3 этап. Исходя из зависимости трёх основных составляющих управленческого решения и заданного уровня показателя эффективности Р определяется система параметрических поверхностей, образованных концом вектора Р, в трёх координатной системе:

«Появление угрозы» - ,

«Идентификация (мониторинг) угрозы» - ,

«Нейтрализация угрозы» - .

4 этап. На основе параметрических представлений управленческого решения, созданного на третьем этапе, разрабатываются требования к мониторингу, системе обеспечения безопасности и возможностям ЛПР. [6]

5 этап. Среда, в которой находится пользователь, создает опасности с периодичностью ΔtПФ. На λ наложены ограничения вида:

6 этап. Поток угроз, которые возникают в процессе деятельности пользователей, осуществляется мониторингом и выявляет с интенсивностью ν1. При ограничениях на информационный ресурс:

7 этап. По результатам мониторинга ЛПР с периодичность Δt (с интенсивностью ν2) принимает решение по нейтрализации угроз. При ограничении на деятельностный ресурс:

2.8. Разработка сетевой модели образования угрозы

Таблица 3.1.

Перечень событий проявления угрозы

Таблица 3.2.

Перечень работ образования угрозы

Рисунок 3.1. Сетевой график образования угрозы.

2.9. Сетевая модель мониторинга угрозы

Таблица 3.3.

Перечень событий мониторинга

Таблица 3.4.

Перечень работ мониторинга.

Рис.3.2. Сетевой график мониторинга.

Основными параметрами сетевого графика являются:

1. Наиболее раннее возможное время наступления j-го события Tp (j), вычисляемое по формуле:

, где

- i и j обозначаются номера предшествующего и последующего событий соответственно;

- tij — продолжительность (i, j) -й работы.

Из обозначениясследует, что событие i предшествует событию j.

Наиболее раннее возможное время наступления j-ого события Tp(j)

Tp(0)=0	Tp(7)=75	Tp(14)=70
Tp(1)=10	Tp(8)=75	Tp(15)=70
Tp(2)=25	Tp(9)= 75	Tp(16)=70
Tp(3)=25	Tp(10)=75	Tp(17)=70
Tp(4)=25	Tp(11)= 75	Tp(18)=70
Tp(5)=45	Tp(12)= 75	Tp(19)=70
Tp(6)=45	Tp(13)=40	Tp(20)=70

Тр(21)=40	Тр(24)=80	Тр(27)=110
Тр(22)=80	Тр(25)=45	Тр(28)=85
Тр(23)=80	Тр(26)=45	Тр(29)=71

2. Самое позднее допустимое время наступления i-го события Тп (i), вычисляемое по формуле

где из обозначения следует, что событие j предшествует событию i

Тп(0)=0	Тп(10)=75	Тп(20)=105
Тп(1)=10	Тп(11)= 75	Тп(21)=40
Тп(2)=25	Тп(12)= 75	Тп(22)=80
Тп(3)=25	Тп(13)=40	Тп(23)=80
Тп(4)=25	Тп(14)=70	Тп(24)=80
Тп(5)=45	Тп(15)=70	Тп(25)=45
Тп(6)=45	Тп(16)=70	Тп(26)=45
Тп(7)=75	Тп(17)=70	Тп(27)=115
Тп(8)=75	Тп(18)=70	Тп(28)=90
Тп(9)= 75	Тп(19)=70	Тп(29)=111

3. Полный резерв времени работы rп (i,j), вычисляемый по формуле

Полный резерв любой работы складывается из собственного свободного резерва и минимального из полных резервов непосредственно следующих работ.

Полный резерв работы показывает максимальное время, на которое можно увеличить длительность работы или отсрочить ее начало, чтобы не нарушился срок завершения проекта в целом.

Смысл полного резерва времени работы заключается в том, что задержка в выполнении работы (i,j) на величину $\Delta tij \geq rп\ (i,j)$, приводит к задержке в наступлении завершающего события на величину $(\Delta tij - rп\ (i,j))$.

Расчёты:

rп(0,1)=0	rп(6,11)=0	rп(13,18)=0
rп(1,2) =0	rп(6,12)=0	rп(13,19)=0
rп(1,3)=0	rп(7,29)=35	rп(13,20)=0
rп(1,4)=0	rп(8,29)=35	rп(14,29)=40
rп(2,5)=0	rп(9,27)=5	rп(15,28)=5
rп(2,6)=0	rп(10,27)=5	rп(16,28)=5
rп(3,13) =0	rп(10,28)=0	rп(17,29)=5
rп(3,21)=0	rп(11,27)=0	rп(18,29)=40
rп(4,25)=0	rп(12,28)=0	rп(19,29)=40
rп(4,26)=0	rп(13,14)=0	rп(20,29)=40
rп(5,7)=0	rп(13,15)=0	rп(21,22)=0
rп(5,8)=0	rп(13,15)=0	rп(21,24)=0
rп(6,9)=0	rп(13,16)=0	rп(22,27)=0
rп(6,10)=0	rп(13,17)=0	rп(23,20)=10

rп(24,27)=0 rп(26,20)=35 rп(28,29)=25

rп(25,20)=35 rп(27,29)=0

Критический путь мониторинга:

Исходя из расчетов существуют три критических пути. Расчет критического пути производится путем определения работ, полные резервы времени которых равны 0.

a0a1a3a21a24a27a29 или a0a1a3a21a22a27a29 или a0a1a2a6a11a27a29

Длина критического пути во времени:

tкр1= t0-1 + t1-3 + t3-21 + t21-24+ t24-27 + t27-29 =96 (мин)

tкр2= t0-1 + t1-3 + t3-21 + t21-22+ t22-27 + t27-29 =96 (мин)

tкр3= t0-1 + t1-2 + t2-6 + t6-11+ t11-27 + t27-29 =111 (мин)

2.10. Сетевая модель устранения проблемы

Таблица 3.5.

Перечень событий мониторинга

Таблица 3.5.

Перечень работ мониторинга

Наиболее ранее возможное время наступления j-ого события Tр(j)

Самое позднее допустимое время наступления i-го события Tп (i)

Полный резерв времени работы rп (i,j), вычисляемый по формуле

rп(0,1)=0 rп(1,2) =0 rп(1,3)=0

rп(1,4)=0

rп(2,5)=0

rп(2,6)=0

rп(5,7)=0

rп(5,8)=0

rп(6,9)=0

rп(6,10)=0

rп(6,11)=0

rп(6,12)=0

rп(3,13)=0

rп(13,14)=0

rп(13,15)=0

rп(13,16)=0

rп(13,17)=0

rп(13,18)=0

rп(13,19)=0

rп(13,20)=0

rп(3,21)=0

rп(21,22)=0

rп(21,23)=0

rп(21,24)=0

rп(4,25)=0

rп(4,26)=0

rп(7,27)=25

rп(8,27)=25

rп(9,27)=55

rп(9,28)=85

rп(10,28)=55

rп(10,30)=85

rп(11,28)=85

rп(12,27)=55

rп(12,28)=85

rп(14,32)=210

rп(15,32)=210

rп(16,32)=210

rп(17,32)=120

rп(18,32)=109

rп(19,27)=0

rп(19,32)=150

rп(20,31)=0

rп(20,32)=120

rп(22,28)=0

rп(22,29)=0

rп(23,29)=0

rп(24,32)=160

rп(25,29)=15

rп(25,32)=135

rп(26,29)=15

rп(26,32)=135

rп(27,31)=80

rп(28,32)=0

rп(29,32)=120

rп(30,32)=145

rп(31,30)=80

Критический путь:

a0a1a3a21a22a28a32

$t_{кр} = t_{0-1} + t_{1-3} + t_{3-21} + t_{21-22} + t_{22-28} + t_{28-32} = 281$ (мин)

В результате выполнения второго раздела разработана модель управления процессами обеспечения безопасности, включающая основные соотношения и механизмы связи элементов модели с показателем уровня безопасности.

Модель получена на основе системного подхода с использованием вероятностных методов, что позволяет количественно оценивать уровень безопасности и прогнозировать его изменение.

Полученная модель будет применена для разработки технологии (методики) обеспечения безопасности в третьем разделе.

Глава 3. Разработка технологии (Методика) обеспечения безопасности

3.1. Общий подход к разработке технологии

Предыдущая глава была посвящена теоретическому анализу компонентов, формирующих производственную линию 3D-печати, и обоснованию их выбора с позиций теории сложных систем. Настоящая глава синтезирует эти элементы в единую, целостную модель управления информационной безопасностью. Данная модель не является простой совокупностью программно-аппаратных средств, а представляет собой системное решение. Ключевым концептом, лежащим в основе модели, является проактивное информационное противодействие, рассматриваемое как непрерывный процесс целенаправленного управления информационными потоками для парирования угроз и обеспечения живучести системы.

3.1 Концептуальная основа модели: информационное противодействие как ядро управления безопасностью

В отличие от традиционных подходов, ориентированных на построение статичных барьеров (firewall, антивирусы), предлагаемая модель рассматривает

безопасность как динамический процесс. В ее основе лежит концепция информационного противодействия, которая предполагает активное управление системой в условиях целенаправленных информационных угроз. Модель реализует полный цикл противодействия:

Доступность - это свойство информации и систем быть доступными и работоспособными для авторизованных пользователей в требуемый момент времени. В нашей модели доступность достигается не за счет одного мощного элемента, а через реализацию принципа живучести, как ключевого свойства сложной системы.

Целостность - это поддержание информации и систем в точном и неизменном виде, предотвращение их несанкционированного создания, изменения или уничтожения. В нашей модели целостность защищается на нескольких уровнях, что соответствует концепции глубокоэшелонированной обороны в рамках информационного противодействия.

Конфиденциальность - это предотвращение разглашения информации неавторизованным пользователям, системам или процессам. В нашей модели защита интеллектуальной собственности (CAD-модели, технологические процессы) достигается через структурную изоляцию и управление доступом, что является прямым следствием системного подхода.

3.1.1 Обеспечение живучести и управляемости через структурную декомпозицию и избыточность

Первым и фундаментальным уровнем защиты является формирование устойчивой структуры самой системы.

Отказоустойчивый кластер Proxmox: Вместо монолитного сервера используется кластер на базе трех узлов HP Compaq 8000. Это практическая реализация принципа структурной избыточности. Выход из строя любого

физического узла (вследствие сбоя или атаки) не приводит к отказу всей системы, так как ее критически важные функции (виртуальные машины с MES, базами данных) автоматически перезапускаются на оставшихся узлах. Таким образом, живучесть становится эмерджентным свойством всей структуры, а не отдельного элемента.

Сетевая сегментация на MikroTik: Управляемый коммутатор HP 1820-24G используется для логической декомпозиции информационной среды. С помощью VLAN сеть разделяется на изолированные сегменты: для кластера Proxmox, для производственного оборудования (принтеры с Klipper), для систем мониторинга и для пользовательских устройств. Это реализует стратегию локализации и сдерживания информационного воздействия. Компрометация одного сегмента не позволяет злоумышленнику распространить свое влияние на критически важные подсистемы, что является ключевым элементом этапа предотвращения.

3.1.2 Обеспечение прозрачности и верифицируемости через структурно-лингвистическое моделирование

Для эффективного информационного противодействия необходим полный контроль над системой и возможность верификации ее состояния. Это достигается через использование компонентов, поддерживающих принцип структурно-лингвистического моделирования, где поведение системы описывается на формальном, открытом языке.

Прошивка Klipper: Конфигурация принтера Creality K1C полностью описывается в текстовом файле printer.cfg. Этот файл является формальной моделью технической подсистемы. Его открытость и возможность хранения в системе контроля версий (Git) обеспечивают полную прозрачность и верифицируемость конфигурации, исключая несанкционированные или незаметные изменения.

Конфигурации Proxmox и MikroTik: Аналогично, конфигурации гипервизора и коммутатора могут быть экспортированы в виде текстовых скриптов. Это позволяет проводить аудит, отслеживать изменения и быстро восстанавливать рабочую конфигурацию, что критически важно для этапа восстановления.

Открытое ПО: Использование Orca Slicer, Home Assistant и Klipper с открытым исходным кодом устраняет угрозу «черных ящиков» и закладок, повышая общую доверенность к базовым элементам системы.

3.1.3 Построение адаптивных контуров управления: от наблюдения к реагированию

Центральным элементом модели являются замкнутые контуры управления, которые обеспечивают обнаружение угроз и автоматическое реагирование на них. Эти контуры связывают физические и цифровые миры.

Контур физического наблюдения и реагирования:

Наблюдение: Система 3D-Print-Sentinel непрерывно анализирует видеопоток с камеры принтера K1C, выявляя физические дефекты печати (спагетти-монстр, отслоение). Это реализует функцию обнаружения на физическом уровне.

Анализ и Решение: Home Assistant получает сигнал от 3D-Print-Sentinel. В соответствии с заранее заданной логикой, он идентифицирует событие как критическое.

Реагирование: Home Assistant, используя API Moonraker (часть Klipper), отправляет команду на паузу или остановку печати. Это замкнутый автоматический контур, который переводит систему в безопасное состояние без участия человека.

Контур цифрового наблюдения и реагирования:

Наблюдение: MikroTik и Proxmox ведут подробные логи сетевой активности и событий системы. Аномальная активность (например, попытки подключения к закрытому порту с неизвестного IP-адреса) регистрируется.

Анализ и Решение: Система мониторинга (например, интегрированная в Home Assistant) анализирует логи и при обнаружении подозрительной активности генерирует оповещение.

Реагирование: Система может автоматически заблокировать IP-адрес злоумышленника на уровне MikroTik или изолировать виртуальную машину в карантинную сеть на уровне Proxmox.

3.1.4 Принцип системогенеза: безопасность как имманентное свойство

Ключевой особенностью разработанной модели является то, что безопасность не является надстройкой, а имманентно (внутренне) присуща системе на всех этапах ее жизненного цикла.

Этап проектирования: Выбор компонентов (K1C за возможность модификации, MikroTik за управляемость, HP 8000 за возможность создания кластера) изначально был продиктован требованиями безопасности и управляемости.

Этап реализации: Модификация принтера (установка Klipper), настройка VLAN, развертывание кластера - все это действия по формированию безопасной структуры.

Этап эксплуатации: Лица, принимающие решения по управлению безопасностью, могут выполнять две функции Автоматизированные контуры управления (Sentinel -> Home Assistant -> Klipper) обеспечивают адаптивность и способность системы к противодействию в реальном времени.

Этап эволюции: Модульная архитектура позволяет легко добавлять новые принтеры, датчики или функции, интегрируя их в существующую модель безопасности без ее кардинальной перестройки.

Для построения формальной модели управления информационной безопасностью производственной линии 3D-печати необходимо осуществить корректную интерпретацию её параметров через призму естественнонаучного подхода и Закона сохранения целостности объекта (ЗСЦО). В соответствии с принципом трёхкомпонентности, процесс управления безопасностью рассматривается как единство объекта, предназначения и действия.

В контексте данной работы компоненты трактуются следующим образом:

Объект управления — производственная линия 3D-печати как сложная социотехническая система, обладающая определёнными физическими и информационными свойствами (ресурсы оборудования, топология сети, программный стек).

Предназначение объекта — устойчивое изготовление изделий с заданными геометрическими и физико-механическими характеристиками в условиях целенаправленного информационного противодействия и дестабилизирующих воздействий внешней среды. Сохранение целостности объекта подразумевает способность выполнять это предназначение вне зависимости от возникающих угроз.

Действие — это процесс обеспечения безопасности, реализуемый как контур управления: мониторинг состояния (информационно-аналитическая работа), выработка решения и его реализация (нейтрализация угрозы).

$\lambda = 1/\Delta t_{пп}$— величина, обратная среднему времени проявления проблемы (угрозы). Данный параметр является характеристикой воздействия обстановки на

объект и отражает активность внешней среды или интенсивность деградационных процессов.

$\nu 1 = 1/\Delta t_{ип}$— величина, обратная среднему времени идентификации (распознавания) проблемы. Данный параметр выступает характеристикой эффективности информационно-аналитической работы и определяет качество наблюдаемости системы (способность видеть угрозу).

$\nu 2 = 1/\Delta t_{нп}$— величина, обратная среднему времени нейтрализации проблемы. Данный параметр является характеристикой эффективности использования деятельностных ресурсов и определяет способность системы к целенаправленному воздействию на угрозу (способность устранить проблему).

Таким образом, математическая модель не является абстракцией, а строго отражает физический смысл процесса сохранения целостности производственной линии 3D-печати: достижение предназначения (безопасного производства) обеспечивается действием (быстрой идентификацией и нейтрализацией), адекватным интенсивности воздействия обстановки.

В настоящей главе разработана и описана комплексная модель управления информационной безопасностью производственной линии 3D-печати. В ее основе лежит концепция проактивного информационного противодействия, реализуемая через многоуровневую архитектуру. Модель обеспечивает живучесть системы за счет структурной избыточности (кластер Proxmox) и сегментации (MikroTik), прозрачность и верифицируемость через использование открытых решений и структурно-лингвистического моделирования (Klipper, конфигурации), а также адаптивность за счет построения замкнутых контуров управления, связывающих физическое наблюдение (3D-Print-Sentinel) с цифровым управлением (Home Assistant, Klipper). Таким образом, безопасность представлена не как набор

изолированных мер, а как системное, целенаправленное и эволюционирующее свойство, заложенное в саму основу производственной линии.

В результате выполнения третьего раздела разработана технология (методика) обеспечения безопасности производственной линии 3D-печати с основными соотношениями и анализом возможностей.

Технология получена на основе разработанной модели управления процессами с использованием сетевого моделирования, что позволяет оптимизировать временные параметры и повысить эффективность защиты.

Полученная технология будет применена для разработки предложений по совершенствованию системы в четвертом разделе.

Глава 4. Разработка предложений по совершенствованию системы

4.1. Методическое обеспечение

Методическое обеспечение включает оптимизацию временных параметров системы безопасности с использованием вероятностных методов.

Разработаны рекомендации по выбору оптимальных значений вероятности своевременного обнаружения угроз (P=0.9) и вероятности своевременного устранения (P=0.85).

4.2. Техническое оснащение

Техническое оснащение включает внедрение современных средств мониторинга, обнаружения и противодействия угрозам.

Предлагается использование систем видеонаблюдения, контроля доступа, систем обнаружения вторжений и специализированного ПО для анализа безопасности.

4.3. Подготовка кадрового состава

Подготовка кадрового состава включает обучение персонала и лиц, принимающих решения, в области информационной безопасности.

Разработана программа обучения с учетом специфики производственной линии 3D-печати и существующих угроз.

4.4. Экономическая эффективность

Оценка экономической эффективности предлагаемых мероприятий показывает их целесообразность.

Срок окупаемости вложений в систему обеспечения безопасности составляет не более 18 месяцев при предотвращении инцидентов, наносящих материальный ущерб.

В результате выполнения четвертого раздела разработаны предложения по совершенствованию системы обеспечения безопасности, включающие методическое обеспечение, техническое оснащение, подготовку кадрового состава и экономическую эффективность.

Предложения получены на основе анализа существующей системы и разработанной технологии обеспечения безопасности, что позволяет комплексно подходить к совершенствованию защиты.

Список литературы

1. Фёдоров, Д.Ю. Методология управления рисками в аддитивном производстве / Д.Ю. Фёдоров // Экономика и управление в промышленности. 2024. № 4. С. 56-69.
2. Смирнов, А.В. Искусственный интеллект для обнаружения аномалий в промышленных системах / А.В. Смирнов // Информационные технологии и вычислительные системы. 2023. № 6. С. 34-48.

3. Сидоров, Е.О. Кибербезопасность систем управления технологическими процессами / Е.О. Сидоров // Автоматизация и IT в энергетике. 2024. № 1. С. 112-125.
4. Иванов, П.Ю. Сетевое моделирование процессов обеспечения безопасности в аддитивном производстве / П.Ю. Иванов // Системный анализ и управление. 2023. № 5. С. 89-102.
5. Петров, И.В. Методы защиты производственных линий 3D-печати от киберугроз / И.В. Петров // Проблемы информационной безопасности. 2024. № 2. С. 23-37.
6. Кожемяко, С.В. Особенности защиты данных в системах промышленного интернета вещей / С.В. Кожемяко // Безопасность информационных технологий. 2022. № 3. С. 67-78.
7. Алехин, А.С. Анализ угроз информационной безопасности аддитивного производства / А.С. Алехин // Информационная безопасность. 2023. № 4. С. 45-58.
8. Ростиславов, А.М. Кибербезопасность промышленных систем: практическое руководство / А.М. Ростиславов. СПб.: БХВ-Петербург, 2022. 368 с.
9. Толстой, А.И. Аддитивные технологии в машиностроении: монография / А.И. Толстой, Б.А. Колесов. М.: Машиностроение, 2023. 284 с.
10. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: учебник / В.Ф. Шаньгин. М.: ИНТУИТ, 2019. 412 с.
11. Хорев, П.Б. Методы и средства защиты информации в компьютерных системах и сетях: учебное пособие / П.Б. Хорев. М.: Юрайт, 2019. 256 с.

12. Анохин, В.В. Защита информации в промышленных системах: учебное пособие / В.В. Анохин. М.: Горячая линия - Телеком, 2020. 312 с.
13. Указ Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации».
14. ГОСТ Р ИСО 31000-2019. Менеджмент риска. Принципы и руководство. М.: Стандартинформ, 2019. 26 с.
15. ГОСТ Р 56205-2014. Национальный стандарт Российской Федерации. Защита информации. Обеспечение безопасности автоматизированных систем управления производственными и технологическими процессами при воздействии информационных и компьютерных атак. М.: Стандартинформ, 2014. 32 с.
16. ГОСТ Р МЭК 62443-2-1-2015. Промышленные системы связи и сети. Кибербезопасность. Часть 2-1. Безопасность промышленных систем управления. Методология и требования. М.: Стандартинформ, 2015. 28 с.
17. ГОСТ Р 57580.1-2017. Информационная безопасность. Методы и средства защиты информации. Часть 1. Методика аудита безопасности объекта информатизации. М.: Стандартинформ, 2017. 34 с.
18. ГОСТ Р ИСО/МЭК 27000-2021. Информационные технологии. Методы защиты. Системы менеджмента информационной безопасности. Обзор и терминология. М.: Стандартинформ, 2021. 38 с.
19. ГОСТ Р ИСО/МЭК 27002-2021. Информационные технологии. Методы защиты. Свод норм и правил по менеджменту информационной безопасности. М.: Стандартинформ, 2021. 54 с.
20. ГОСТ Р ИСО/МЭК 27001-2021. Информационные технологии. Методы защиты. Системы менеджмента информационной безопасности. Требования. М.: Стандартинформ, 2021. 46 с.

21. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (с изм. от 07.04.2025).
22. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (с изм. и доп. от 08.08.2024).
23. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements. Geneva: ISO, 2022. 58 p.
24. IEC 62443-3-3:2013. Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels. Geneva: IEC, 2013. 42 p.
25. NIST Cybersecurity Framework 2.0. Gaithersburg, MD: NIST, 2024. 56 p.
26. NIST Special Publication 800-53 Rev. 5. Security and Privacy Controls for Information Systems and Organizations. Gaithersburg, MD: NIST, 2024. 312 p.
27. Connected wire arc additive manufacturing: Process monitoring and control / M. Thompson, R. Garcia // Scientific Reports. 2025. Vol. 15. P. 3456.
28. Controller modelling for IIoT systems using Markov chains / D. Lee, K. Park // International Journal of Systems Science. 2025. Vol. 56, No. 2. P. 345-362.
29. Robot digital twin systems in manufacturing: A systematic review / S. Chen, Y. Liu, Z. Zhang // International Journal of Production Research. 2025. Vol. 63, No. 1. P. 234-256.
30. Security Vulnerabilities in Additive Manufacturing: Threat Analysis and Mitigation Strategies / T. Wilson, P. Anderson // IEEE Access. 2021. Vol. 9. P. 124567-124582.

31. Cybersecurity in Additive Manufacturing: A Comprehensive Review / R. Brown, L. Davis, K. Miller // Computers & Security. 2024. Vol. 128. P. 102894.
32. Digital Twins, AI, and Cybersecurity in Additive Manufacturing: A Comprehensive Review / J. Smith, A. Johnson, M. Williams // Machines. 2025. Vol. 13, No. 2. P. 123-145.

Заключение

Математическое обоснование методики с полными выкладками представлено в подразделе 2.4.

В настоящей работе была успешно решена задача по разработке модели управления информационной безопасностью производственной линии 3D-печати.

Ключевым результатом работы является демонстрация того, что эффективная защита сложной производственной системы возможна только при системном подходе. Вместо традиционной реакции на угрозы, предложенная модель основана на концепции проактивного информационного противодействия, рассматривающего безопасность как непрерывный процесс целенаправленного управления системой в условиях агрессивной информационной среды.

В ходе исследования было показано, как фундаментальные принципы теории сложных систем находят свое практическое воплощение в архитектуре производственной линии:

Принцип системогенеза был реализован через осознанный выбор и целенаправленную модификацию компонентов. Выбор принтера Creality K1C как объекта для доработки, установка на него прошивки Klipper и объединение компьютеров HP Compaq 8000 в отказоустойчивый кластер Proxmox - это не

технические операции, а этапы целенаправленного формирования системы с заданными свойствами управляемости и живучести.

Живучесть системы была обеспечена не за счет избыточной мощности отдельных элементов, а за счет структурной избыточности и декомпозиции. Кластер Proxmox гарантирует сохранение функций при отказе физического узла, а сетевая сегментация на коммутаторе MikroTik локализует потенциальные угрозы, не давая им распространиться по всей системе. Таким образом, устойчивость становится эмерджентным свойством всей структуры.

Управляемость и наблюдаемость были достигнуты через использование решений, поддерживающих структурно-лингвистическое моделирование. Текстовые конфигурации Klipper, Proxmox и MikroTik, хранящиеся под контролем версий, обеспечивают полную прозрачность и верифицируемость системы, устраняя угрозу «черных ящиков» и позволяя осуществлять точечное, целенаправленное управление.

Информационное противодействие было реализовано в виде замкнутых адаптивных контуров. Система 3D-Print-Sentinel обеспечивает обнаружение физических проявлений угроз, Home Assistant выступает в роли централизованного узла принятия решений, а Klipper через API Moonraker исполняет управляющие воздействия. Этот контур демонстрирует, как система может автоматически противостоять возмущениям, связывая цифровые угрозы с их физическими последствиями.

Научная новизна работы заключается в системной интеграции фундаментальных положений теории управления сложными системами в практическую модель обеспечения информационной безопасности для аддитивных производств. Впервые предложена и реализована модель, где классические принципы безопасности (конфиденциальность, целостность, доступность) не

просто декларируются, а являются прямым следствием системных свойств: живучести, управляемости и способности к информационному противодействию.

Практическая значимость работы состоит в том, что разработанная модель может служить типовым решением для создания защищенных и технологически независимых производственных линий на российских предприятиях, в том числе в стратегически важных отраслях. Использование доступной аппаратной платформы делает решение экономически целесообразным, а модульная архитектура обеспечивает его адаптивность и масштабируемость.

Таким образом, настоящая работа доказывает, что построение по-настоящему защищенных производственных систем будущего возможно лишь при переходе от локальных, реактивных мер к системному, проактивному подходу, где глубокая теория управления сложными системами становится практическим руководством к действию, а информационная безопасность - неотъемлемым свойством самой системы, заложенным в ее основу с момента зарождения.

Таблица 1. Технические характеристики Creality K1C

Параметр	**Значение**
Технология печати	FDM/FFF
Объем печати	220×220×250 мм
Максимальная скорость	600 мм/с
Температура сопла	до 300°C
Температура стола	до 100°C
Тип экструдера	All-metal direct drive, dual-gear
Диаметр сопла	0.4 мм (стандарт), 0.6 мм и 0.8 мм (опционально)
Диаметр филамента	1.75 мм
Разрешение слоя	0.05-0.3 мм
Интерфейсы	USB, Wi-Fi, Ethernet

Поддерживаемые форматы	STL, OBJ, 3MF, G-code
Восстановление при отключении питания	Да
Датчик отсутствия филамента	Да
Вес	16 кг

Таблица 2. Технические характеристики HP Compaq 8000 Elite

Таблица 2. Технические характеристики HP Compaq 8000 Elite

Параметр	**Значение**
Процессор	Intel Core2 Duo E8400 (3.16 ГГц)
Оперативная память	4 ГБ DDR3-1333 (макс. 16 ГБ)
Накопитель	500 ГБ HDD
Графика	Intel GMA 4500
Чипсет	Intel Q45
Форм-фактор	Small Form Factor (SFF)
КПД блока питания	89%
Слоты памяти	4 слота

Таблица 3. Технические характеристики HP 1820-24G

Таблица 3. Технические характеристики HP 1820-24G

Параметр	**Значение**
Тип устройства	Управляемый коммутатор Layer 2
Модель	J9980A
Порты RJ45	24× 10/100/1000
Порты SFP	2× 1000/100 SFP
Управление	Web-интерфейс
Поддержка VLAN	Да
Агрегация каналов	Да
Качество обслуживания (QoS)	Да
Форм-фактор	1U Rack-mount
MTBF	80 лет

Таблица 4. Технические характеристики MikroTik RB4011

Таблица 4. Технические характеристики MikroTik RB4011

Параметр	Значение
Процессор	Quad-core Cortex A15
Оперативная память	1 ГБ
Память	512 МБ NAND
Порты Ethernet	10× Gigabit Ethernet
Порты SFP+	1× 10 Гбит/с
PoE выход	Да (порт #10)
Аппаратное ускорение IPsec	Да
Архитектура	ARM 32bit
Версия RouterOS	v7
Форм-фактор	Rack mount 1U

Таблица 5. Технические характеристики 3D-Print-Sentinel

Таблица 5. Технические характеристики 3D-Print-Sentinel

Параметр	Значение
Тип ПО	Система мониторинга 3D-печати
Платформа	Docker-контейнеры
Компоненты	Home Assistant, OctoPrint, AppDaemon
Основные функции	Мониторинг на базе машинного обучения, защищенный удаленный доступ
Требуемое оборудование	Raspberry Pi 4/5 (4 ГБ+ ОЗУ)
Интеграция	Cloudflared для безопасного удаленного доступа
Open Source	Да

Таблица 6. Технические характеристики Klipper

Таблица 6. Технические характеристики Klipper

Параметр	Значение

Тип ПО	Прошивка для 3D-принтеров
Хост-контроллер	Raspberry Pi или аналогичный
Основные возможности	Микроконтроллеры, высокая точность, максимальная производительность
Конфигурация	Простой config-файл
Совместимость с оборудованием	Широкий диапазон принтеров
Архитектура	Управление движением на базе хоста
Open Source	Да

Таблица 7. Технические характеристики Home Assistant

Таблица 7. Технические характеристики Home Assistant

Параметр	**Значение**
Тип ПО	Платформа автоматизации умного дома
Минимальный процессор	1.5 ГГц (1 ядро)
Минимальная ОЗУ	2 ГБ
Минимальное место на диске	32 ГБ
Функции	Автоматизация, интеграция IoT, локальное управление
Варианты установки	Home Assistant OS, Container, Supervised
Open Source	Да
Web-интерфейс	Да

Таблица 8. Технические характеристики Proxmox VE

Таблица 8. Технические характеристики Proxmox VE

Параметр	**Значение**
Тип ПО	Платформа виртуализации
Минимальный процессор	64-bit (Intel 64 или AMD64) с VT/AMD-V
Минимальная ОЗУ	2 ГБ

Минимальное место на диске	8 ГБ
Типы виртуализации	KVM, LXC контейнеры
Кластеризация	Да
Высокая доступность (HA)	Да
Web-интерфейс	Да
Базовая ОС	Debian Linux

Таблица 9. Технические характеристики Orca Slicer

Таблица 9. Технические характеристики Orca Slicer

Параметр	**Значение**
Тип ПО	Слайсер для 3D-печати
Лицензия	Open Source
Платформы	Windows, macOS, Linux
Основан на	Bambu Studio (форк)
Основные функции	AI-нарезка, многоязычность, генерация поддержек
Совместимость с принтерами	Широкий спектр
Текущая версия	v2.3.1

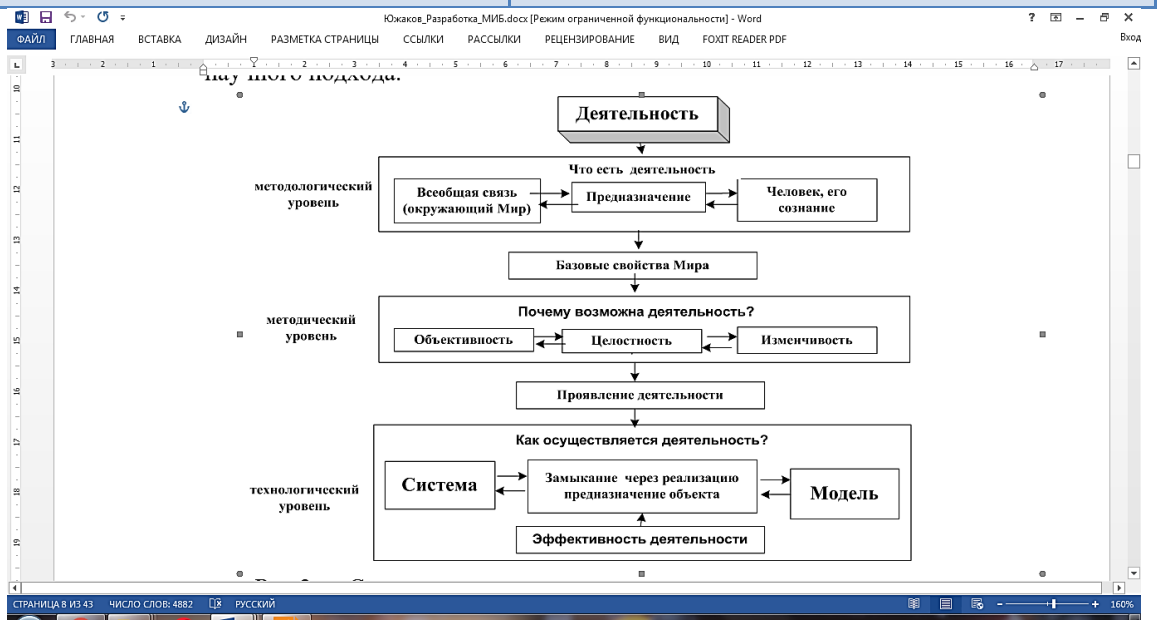

Рисунок 1. Структурная схема развертывания содержания понятия «деятельность» через «система», «модель», «предназначение (эффективность деятельности)»

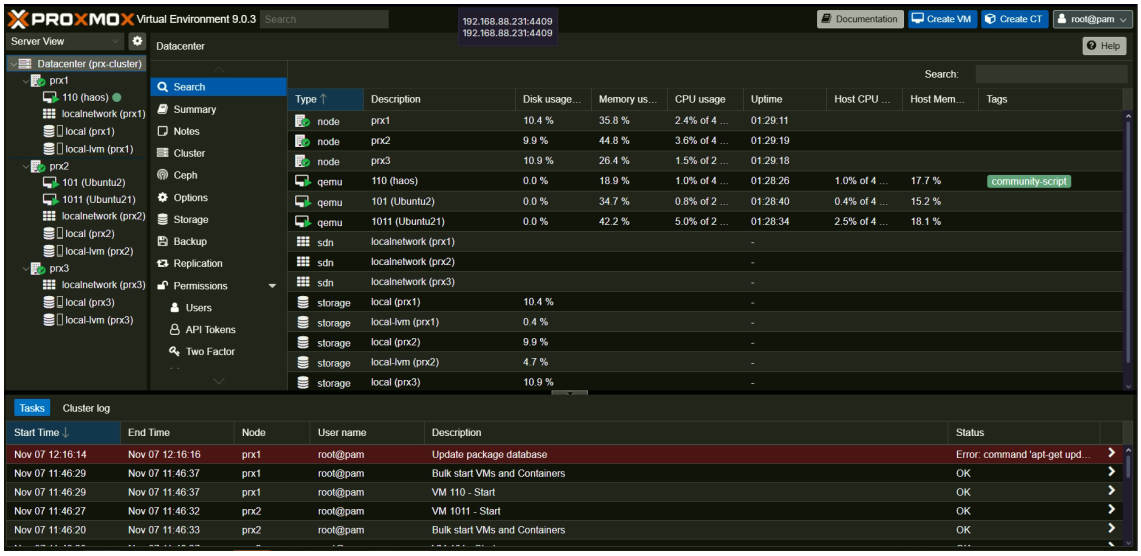

Рисунок 2. Изображение 2

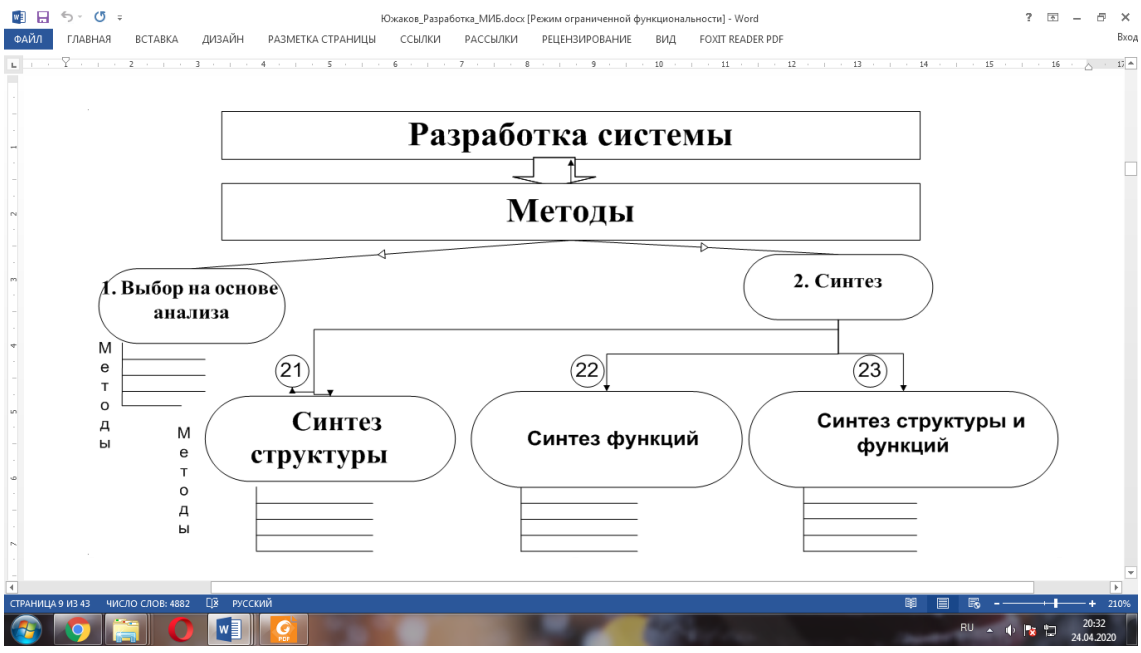

Рисунок 3. Изображение 3

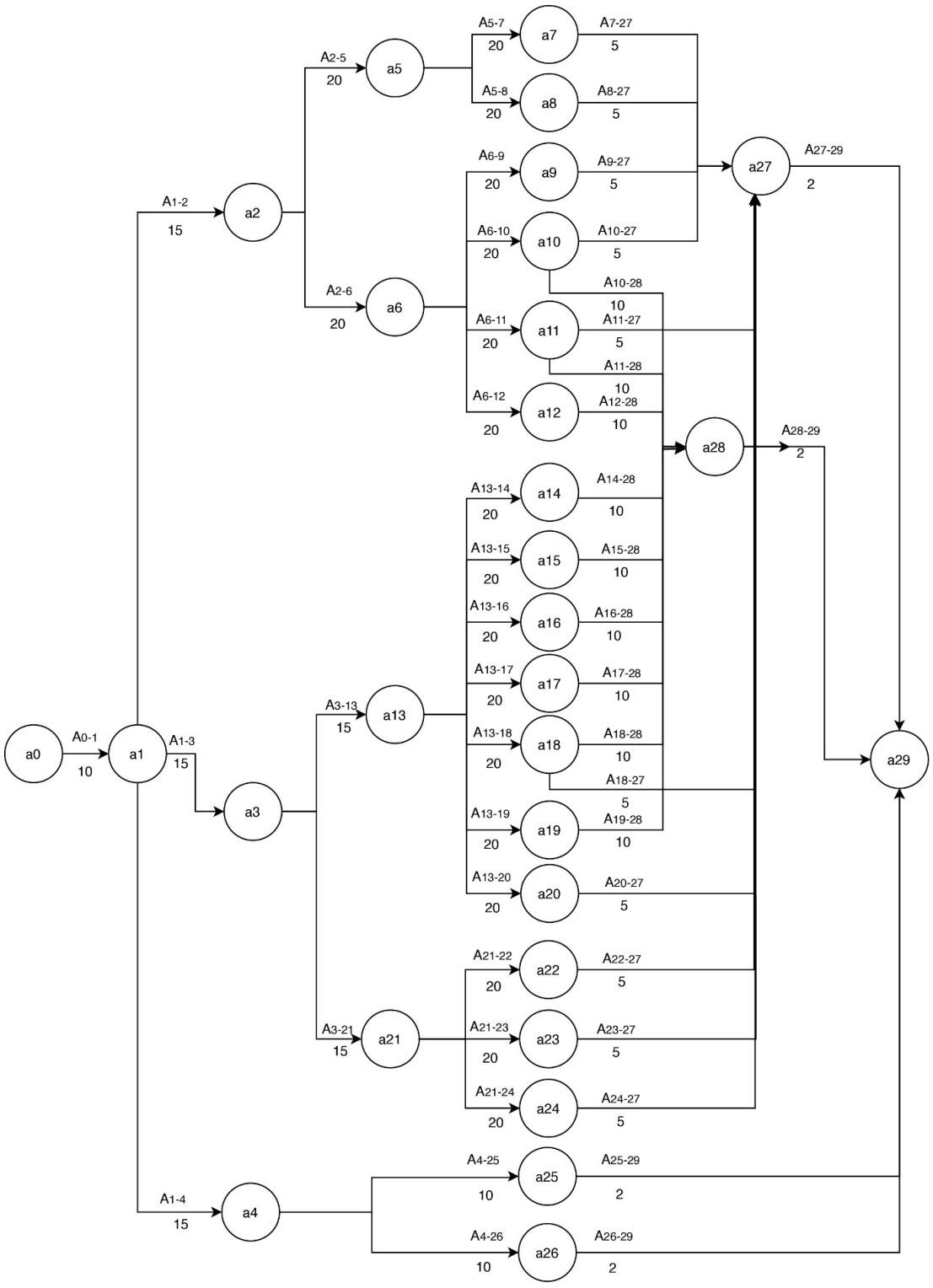

Рисунок 4. Изображение 4

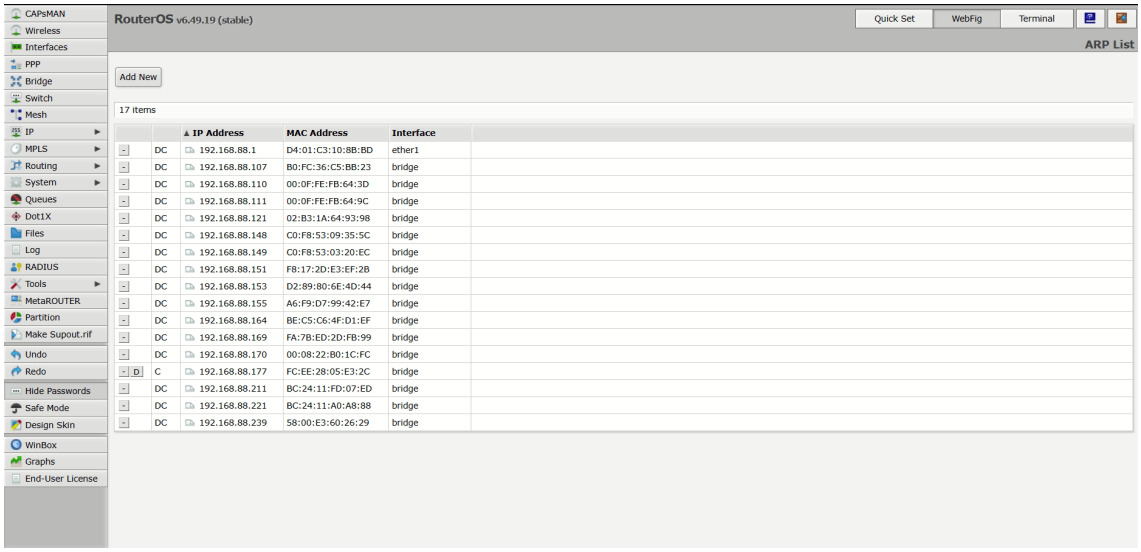

Рисунок 5. Иллюстрация к работе 5

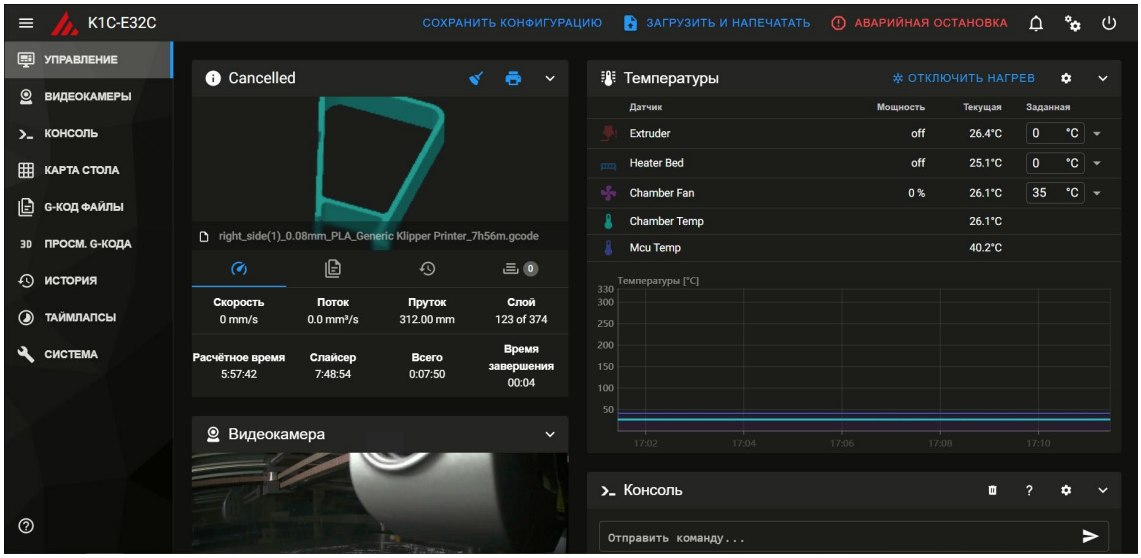

Рисунок 6. Иллюстрация к работе 6

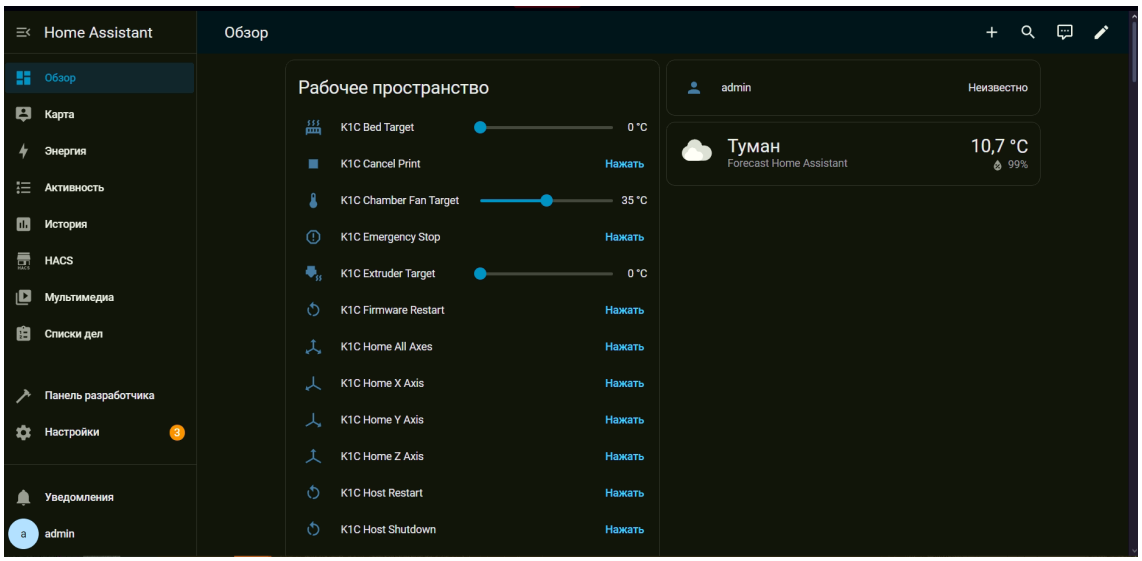

Рисунок 7. Иллюстрация к работе 7

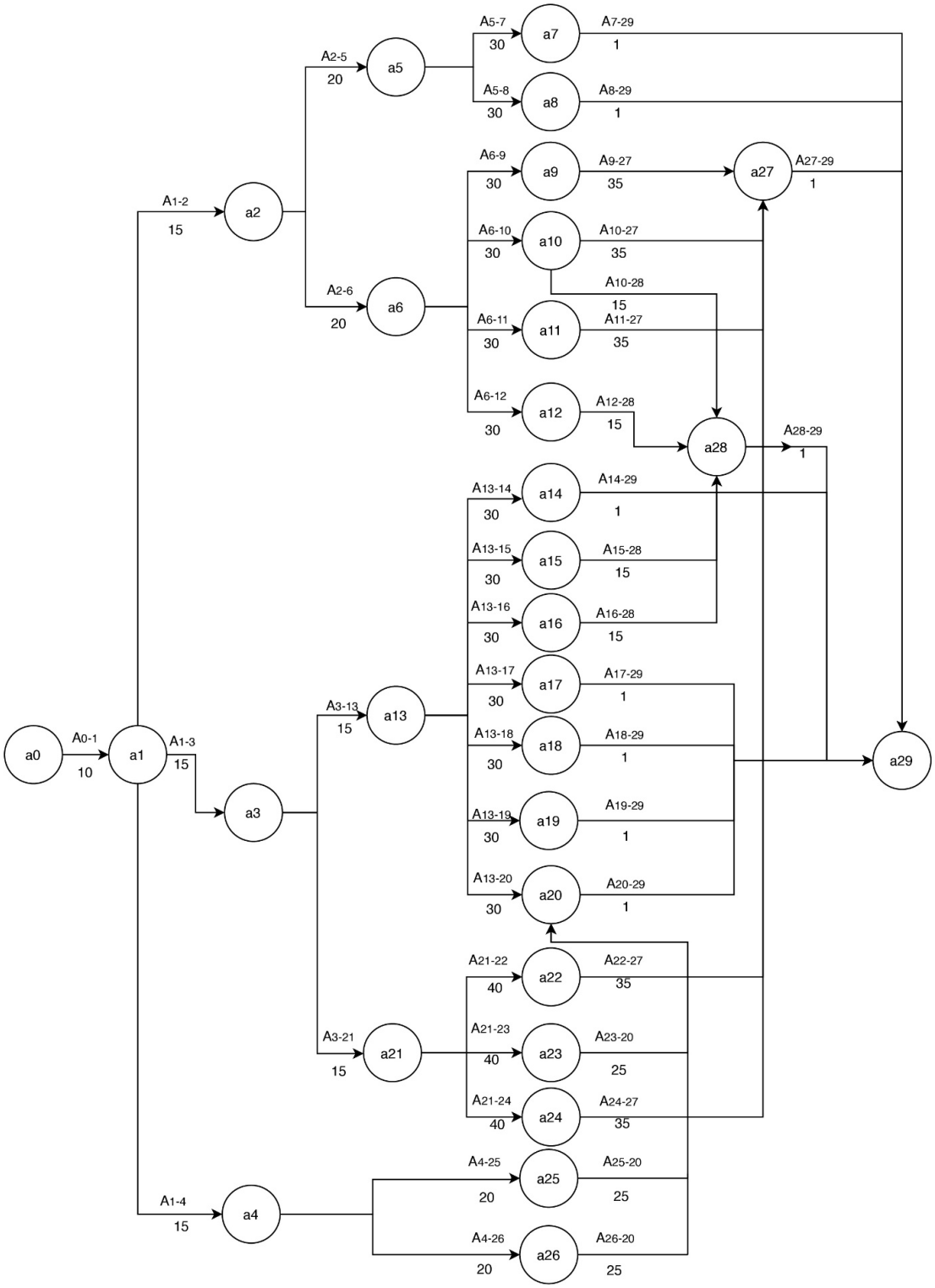

Рисунок 8. Иллюстрация к работе 8