

**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 : Разработка модели управления информационной безопасностью**  
**производственной линии 3D печати**

Исполнитель: Деркач Денис Иванович

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 Деркача Дениса Ивановича**

1. Тема дипломного проектирования: «Разработка модели 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.....	6
Глава 1. Теоретические основы создания и функционирования производственной линии 3D-печати как сложной системы.....	9
1.1. Концептуализация производственной линии 3D-печати как объекта системного анализа .....	9
1.2. Системогенез производственной линии 3D-печати как основа для обеспечения безопасности.....	11
1.3. Информационное противодействие как ключевая задача управления безопасностью ПЛ 3D-печати.....	14
Глава 2. Практическое применение технологий для обеспечения качества и автоматизации постобработки в аддитивном производстве .....	17
2.1. ИИ для in-situ мониторинга и обнаружения дефектов в режиме реального времени.....	17
2.1.1. Компьютерное зрение и сверхточные нейронные сети (CNN) .....	17
2.1.2. Анализ данных с мультисенсорных систем .....	18
2.2. ИИ для автоматизированной постобработки и коррекции дефектов .....	18
2.2.1. Роботизированные манипуляторы с машинным зрением.....	18
2.2.2. Оптимизация химических и термических процессов.....	19
2.3. Информационная безопасность систем ИИ в аддитивном производстве: новые угрозы и векторы атак .....	19
2.3.1. Новые информационные активы .....	19
2.3.2. Специфические векторы атак на ИИ-системы.....	20
2.4. Разработка модели управления информационной безопасностью производственной линии 3д печати. Программные средства .....	20
2.4.1. Orca Slicer. Соответствие принципу целенаправленного управления и контролируемости.....	21
2.4.2. Обоснование выбора платформы виртуализации Proxmox VE как основы для информационно-управляющей подсистемы.....	23
2.4.3. Обоснование использования платформы Home Assistant в качестве человеко-машинного интерфейса и узла управления .....	26
2.4.4. Обоснование выбора управляющей прошивки Klipper как основы контура управления технической подсистемой.....	28
2.4.5. Обоснование использования системы мониторинга 3D-Print-Sentinel как подсистемы обнаружения физических проявлений угроз.....	32
2.5. Роль и значение аппаратной составляющей в контексте управления безопасностью сложной производственной системы .....	34
2.5.1. Обоснование использования сетевого оборудования MikroTik как основы для управления информационными потоками и реализации контура противодействия.....	37
2.5.2. Обоснование использования управляемого коммутатора HP 1820-24G как структурного элемента системы управления информационными потоками .....	40
2.5.3. Обоснование использования аппаратной платформы на базе HP Compaq 8000 для развертывания отказоустойчивого кластера Proxmox.....	42

2.5.4 Обоснование выбора и модификации аппаратной платформы 3D-принтера Creality K1C в контексте системогенеза и информационного противодействия.....	45
2.6 Сетевое моделирование процессов обеспечения безопасности.....	47
2.7. Разработка сетевой модели образования угрозы.....	49
2.8. Сетевая модель мониторинга угрозы.....	54
2.9. Сетевая модель устранения проблемы.....	63
Глава 3. Разработка модели управления информационной безопасностью на основе принципов системного анализа и информационного противодействия	72
3.1 Концептуальная основа модели: информационное противодействие как ядро управления безопасностью.....	72
3.1.1 Обеспечение живучести и управляемости через структурную декомпозицию и избыточность.....	73
3.1.2 Обеспечение прозрачности и верифицируемости через структурно-лингвистическое моделирование.....	74
3.1.3 Построение адаптивных контуров управления: от наблюдения к реагированию.....	74
3.1.4 Принцип системогенеза: безопасность как имманентное свойство .....	75
Заключение .....	79
Список источников .....	81

## **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.

Дипломная работа состоит из введения, трех 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. Теоретические основы создания и функционирования производственной линии 3D-печати как сложной системы**

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.

### **1.1. Концептуализация производственной линии 3D-печати как объекта системного анализа**

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:

1. на информационные ресурсы (направленные на распознавание угрозы);

2. на деятельные ресурсы (направленные на устранение/профилактику угроз);
3. 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:

- а) основные допущения и предположения, обычно выражающиеся в базовых принципах.
- б) базовые понятия, ключевые слова, аксиомы;
- в) правила вывода;
- г) теоремы.

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 представления 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. [3]

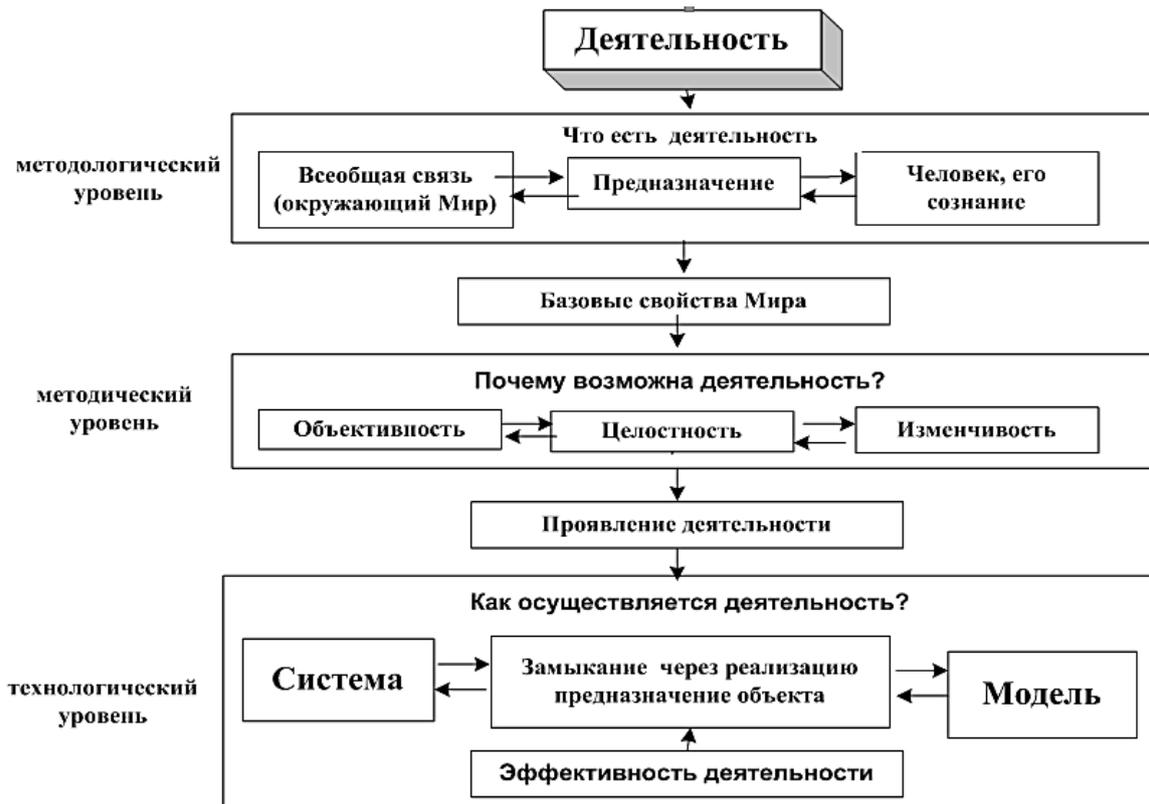


Рис.2.1. Структурная схема развертывания содержания понятия «деятельность» через «система», «модель», «предназначение (эффективность деятельности)».

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

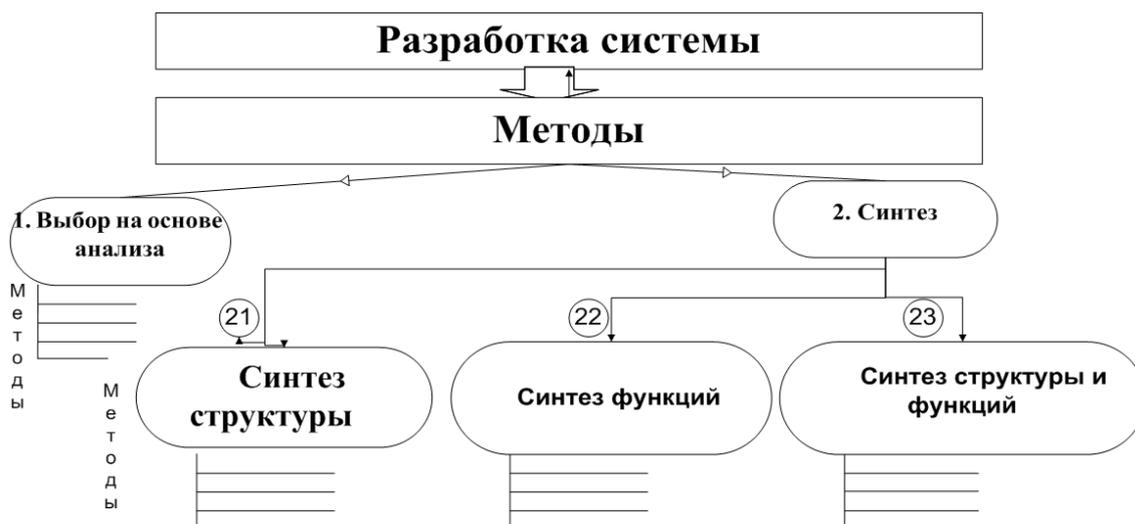


Рис.2.2. Структурная схема основных направлений разработки системы.

В настоящей работе классифицируются решения человека:

- основанное на решении задачи в форме анализа;

- 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.

## **Глава 2. Практическое применение технологий для обеспечения качества и автоматизации постобработки в аддитивном производстве**

### **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.

## **2.4 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.

#### **2.4.1 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.

## 2.4.2 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.

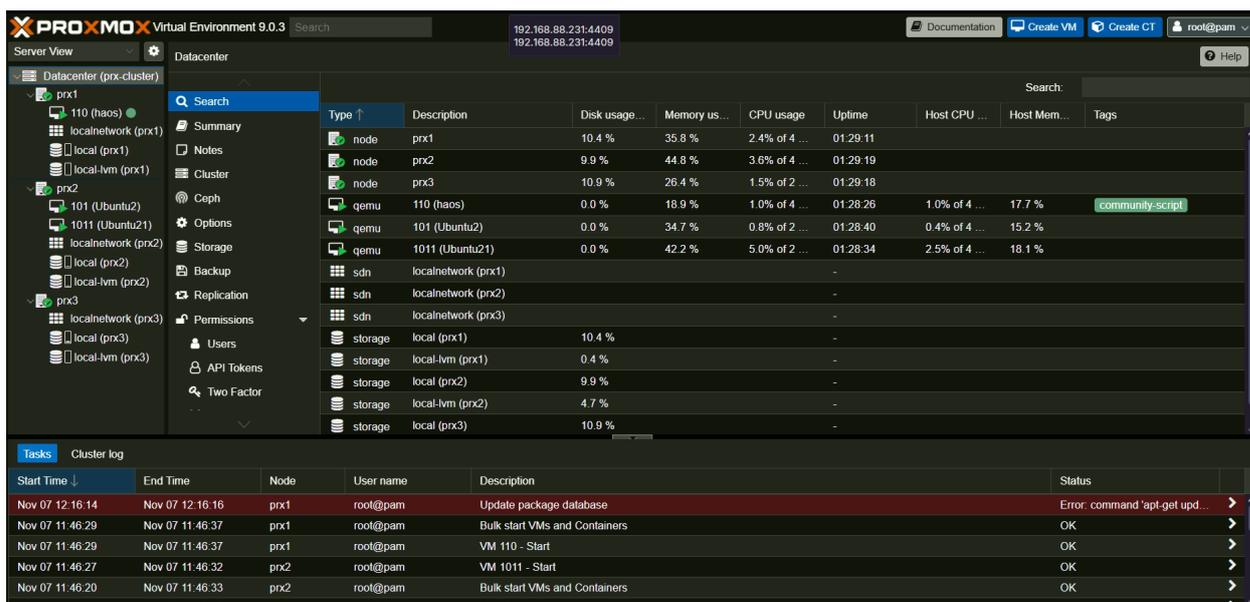


Рис. 1 – Интерфейс гипервизора Proxmox Virtual Environment

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

VM для системы управления производством (MES).

VM для сервера баз данных технологических параметров.

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

VM 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 недеklarированных 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.

### 2.4.3 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.

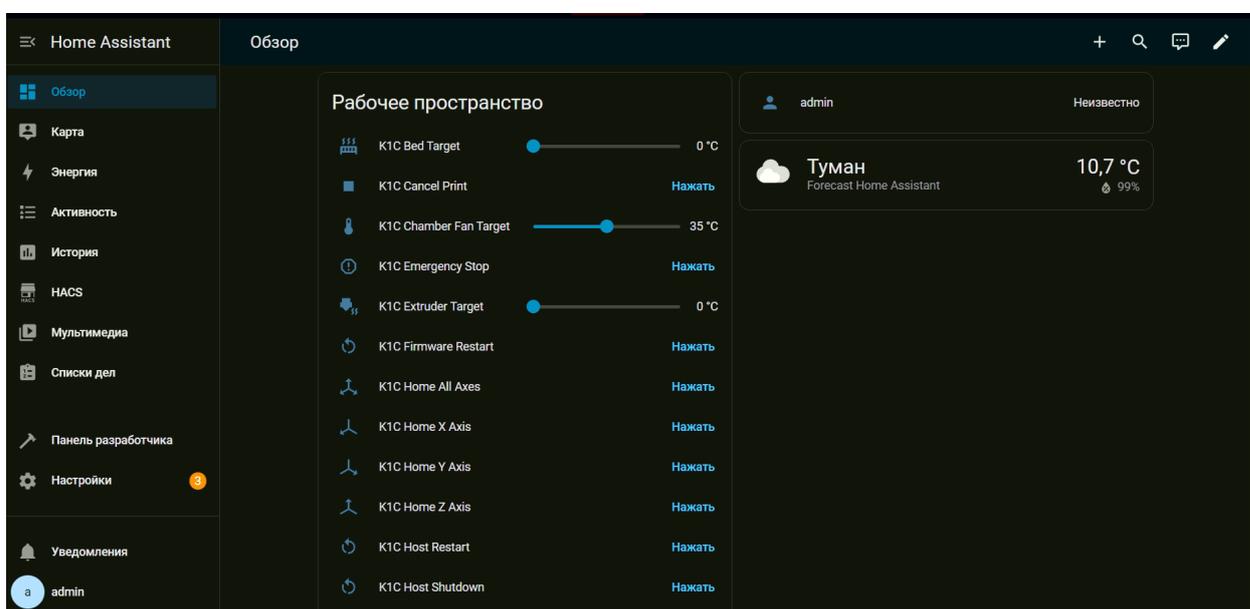


Рисунок 2 – Интерфейс программы Home Assistant

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 восстановить 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.

#### **2.4.4 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.

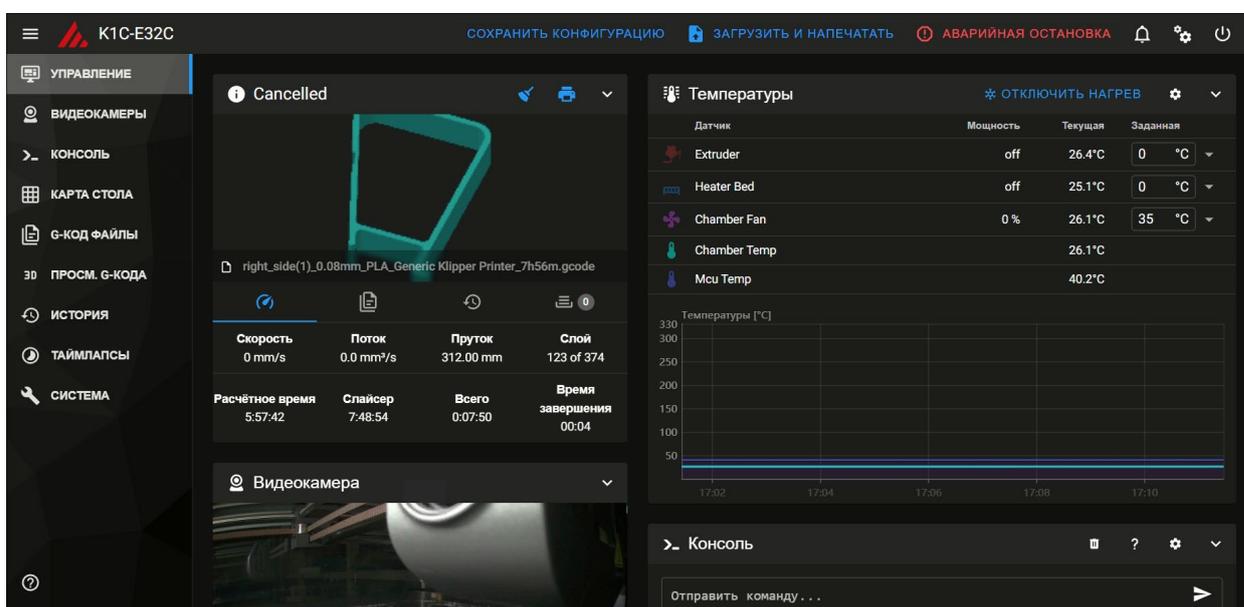


Рисунок 3 – Интерфейс программы Klipper

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.

#### **2.4.5 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, недозэкструзию, 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.

## **2.5 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 обработать 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.

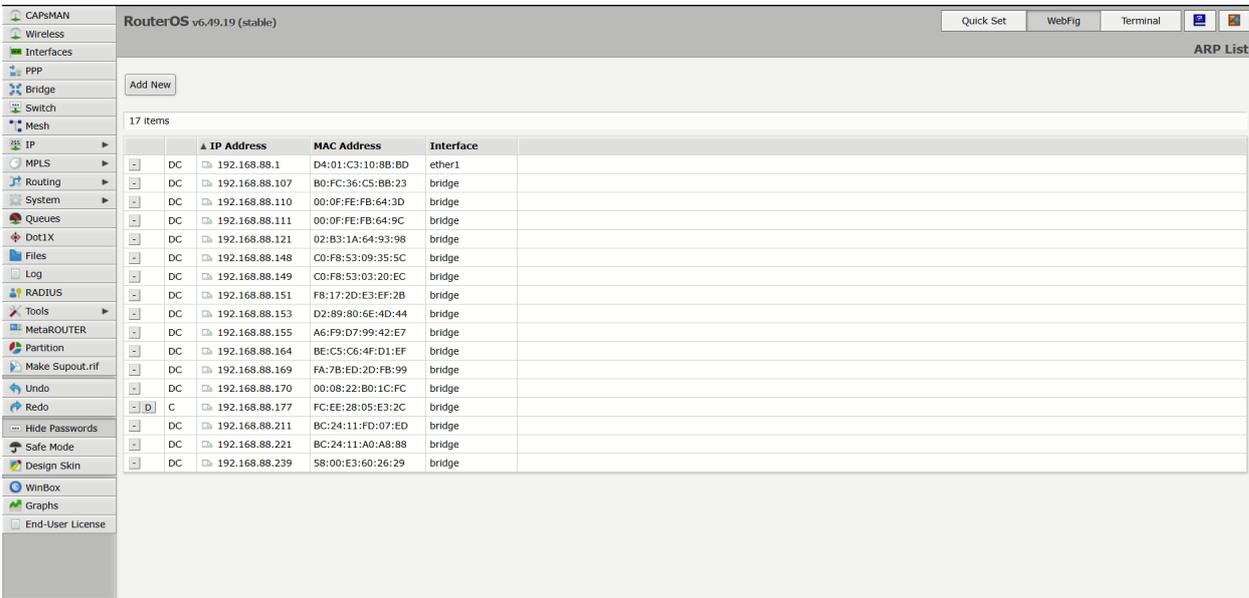
Процесс создания и развития системы - системогенез - сильно зависит от первоначального выбора аппаратной платформы. Выбор закрытого, проприетарного оборудования с неподдерживаемыми протоколами создает «технологическую яму», препятствующую развитию и адаптации системы. Это снижает ее живучесть - способность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

## 2.5.1 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.



The screenshot shows the MikroTik RouterOS v6.49.19 (stable) web interface. The left sidebar contains various configuration menus such as CAPsMAN, Wireless, Interfaces, PPP, Bridge, Switch, Mesh, IP, MPLS, Routing, System, Queues, Dot1X, Files, Log, RADIUS, Tools, MetaROUTER, Partition, Make Supout.rif, Undo, Redo, Hide Passwords, Safe Mode, Design Skin, WinBox, Graphs, and End-User License. The main content area displays the 'ARP List' table with 17 items. The table has columns for IP Address, MAC Address, and Interface.

	IP Address	MAC Address	Interface
DC	192.168.88.1	D4:01:C3:10:8B:BD	ether1
DC	192.168.88.107	B0:FC:36:C5:BB:23	bridge
DC	192.168.88.110	00:0F:FE:FB:64:3D	bridge
DC	192.168.88.111	00:0F:FE:FB:64:9C	bridge
DC	192.168.88.121	02:B3:1A:64:93:98	bridge
DC	192.168.88.148	C0:F8:53:09:35:5C	bridge
DC	192.168.88.149	C0:F8:53:03:20:EC	bridge
DC	192.168.88.151	F8:17:2D:E3:EF:2B	bridge
DC	192.168.88.153	D2:89:80:6E:4D:44	bridge
DC	192.168.88.155	A6:F9:D7:99:42:E7	bridge
DC	192.168.88.164	BE:C5:C6:4F:D1:EF	bridge
DC	192.168.88.169	FA:7B:ED:2D:FB:99	bridge
DC	192.168.88.170	00:08:22:80:1C:FC	bridge
C	192.168.88.177	FC:EE:28:05:E3:2C	bridge
DC	192.168.88.211	BC:24:11:FD:07:ED	bridge
DC	192.168.88.221	BC:24:11:A0:A8:88	bridge
DC	192.168.88.239	58:00:E3:60:26:29	bridge

Рисунок 4 – Интерфейс программы управления маршрутизатора MikroTik

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.

## **2.5.2 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 равносителен 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 Proxmoх 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 ИТ-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.

### **2.5.3 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, VM 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 VM 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 Proxmoх 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.

#### **2.5.4 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 - недеklarированные 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 К1С 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 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.

$$P_{\text{инп}} = F(\Delta t_{\text{пп}}, \Delta t_{\text{ип}}, \Delta t_{\text{нп}})$$

$P_{\text{обсл}} = P_{\text{инп}}$  – 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:

$$P_{\text{обсл}} = P_{00} = \frac{\nu_1 \nu_2}{\lambda(\lambda + \nu_1 + \nu_2) + \nu_1 \nu_2},$$

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  $P$  определяется система параметрических поверхностей, образованных концом вектора  $P$ , в трёх координатной системе:

«Появление угрозы» -  $\Delta t_{\lambda} = f_{\lambda}(x_1, x_2, \dots, x_n)$ ,

«Идентификация (мониторинг) угрозы» -  $\Delta t_{\nu_1} = f_{\nu_1}(y_1, y_2, \dots, y_m)$ ,

«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  $\Delta t_{\text{ПФ}}$ . На  $\lambda$  наложены ограничения вида:

$$\int_T \lambda(t) dt = W$$

6 этап. Поток угроз, которые возникают в процессе деятельности пользователей, осуществляется мониторингом и выявляет с интенсивностью  $v_1$ . При ограничениях на информационный ресурс:

$$\int_T v_1(t) dt = V_1$$

7 этап. По результатам мониторинга ЛПП с периодичность  $\Delta t$  (с интенсивностью  $v_2$ ) принимает решение по нейтрализации угроз. При ограничении на деятельностный ресурс:

$$\int_T v_2(t) dt = V_2$$

## 2.7. Разработка сетевой модели образования угрозы

Таблица 3.1.

Перечень событий проявления угрозы

Обозначение	Наименование событий
$a_0$	Проявление угрозы в работе системы линия 3д печати
$a_1$	Следствие проявления угрозы в системе
$a_2$	Проблемы в работе системы линия 3д печати, связанные с устройством
$a_3$	Проблемы в работе системы линия 3д печати, связанные с планом функционирования
$a_4$	Проблемы в работе системы «линия 3д печати», связанные с ресурсами
$a_5$	Неполадки с ПО
$a_6$	Неполадки аппаратной части
$a_7$	Отказ системного программного обеспечения
$a_8$	Отказ прикладного программного обеспечения

$a_9$	Отказы и сбои сетевого оборудования
$a_{10}$	Отказы и сбои датчиков
$a_{11}$	Помехи на линиях связи от внешних воздействий
$a_{12}$	Непреднамеренная ошибка маршрутизации
$a_{13}$	Преднамеренные угрозы безопасности
$a_{14}$	Модификация информации
$a_{15}$	Манипулирование информацией
$a_{16}$	Подмена имени авторизованными пользователями
$a_{17}$	Перехват информации
$a_{18}$	Хищение оборудования
$a_{19}$	Хакерская атака
$a_{20}$	Вредоносное программное обеспечение (ПО)
$a_{21}$	Случайные угрозы безопасности
$a_{22}$	Схемные и системотехнические ошибки разработчиков
$a_{23}$	Структурные, алгоритмические и программные ошибки
$a_{24}$	Ошибки человека как звена информационной системы
$a_{25}$	Проблема с электропитанием в системе
$a_{26}$	Проблема с водоснабжением в системе
$a_{27}$	Нарушение работы системы или отказ в обслуживании
$a_{28}$	Кража конфиденциальных данных
$a_{29}$	Факт воздействия угроз

Таблица 3.2.

Перечень работ образования угрозы

<b>Обозначение работ</b>	<b>Наименование работ</b>	<b>Время выполнения</b>	<b>Предшествующие работы</b>	<b>Последующие работы</b>

		<b>работ ы, мин</b>		
A <sub>0-1</sub>	Началась проверка угроз в системе	10	-	A <sub>1-2</sub> A <sub>1-3</sub> A <sub>1-4</sub>
A <sub>1-2</sub>	Переход к проблеме возникновения угрозы, связанной с устройством	15	A <sub>0-1</sub>	A <sub>2-5</sub> , A <sub>2-6</sub>
A <sub>1-3</sub>	Переход к проблеме возникновения угрозы, связанные с планом функционирования	15	A <sub>0-1</sub>	A <sub>3-13</sub> , A <sub>3-21</sub>
A <sub>1-4</sub>	Переход к проблеме возникновения угрозы, связанные с ресурсами	15	A <sub>0-1</sub>	A <sub>4-25</sub> , A <sub>4-26</sub>
A <sub>2-5</sub>	Неполадки с ПО	20	A <sub>1-2</sub>	A <sub>5-7</sub>
A <sub>2-6</sub>	Неполадки аппаратной части	20	A <sub>1-2</sub>	A <sub>5-8</sub>
A <sub>5-7</sub>	Отказ системного программного обеспечения	20	A <sub>2-5</sub>	A <sub>7-27</sub>
A <sub>5-8</sub>	Отказ прикладного программного обеспечения	20	A <sub>2-5</sub>	A <sub>8-27</sub>
A <sub>6-9</sub>	Отказы и сбои сетевого оборудования	20	A <sub>2-6</sub>	A <sub>9-27</sub>
A <sub>6-10</sub>	Отказы и сбои датчиков	20	A <sub>2-6</sub>	A <sub>10-27</sub> , A <sub>10-28</sub>
A <sub>6-11</sub>	Помехи на линиях связи от внешних воздействий	20	A <sub>2-6</sub>	A <sub>11-27</sub> , A <sub>11-28</sub>
A <sub>6-12</sub>	Непреднамеренная ошибка маршрутизации	20	A <sub>2-6</sub>	A <sub>12-28</sub>

A <sub>3-13</sub>	Преднамеренные угрозы безопасности	15	A <sub>1-3</sub>	A <sub>13-18</sub>
A <sub>13-14</sub>	Модификация информации	20	A <sub>3-13</sub>	A <sub>14-27</sub>
A <sub>13-15</sub>	Манипулирование информацией	20	A <sub>3-13</sub>	A <sub>15-27</sub>
A <sub>13-16</sub>	Подмена имени авторизованными пользователями	20	A <sub>3-13</sub>	A <sub>16-27</sub>
A <sub>13-17</sub>	Перехват информации	20	A <sub>3-13</sub>	A <sub>17-27</sub>
A <sub>13-18</sub>	Хищение оборудования	20	A <sub>3-13</sub>	A <sub>18-27</sub>
A <sub>13-19</sub>	Хакерская атака	20	A <sub>3-13</sub>	A <sub>19-27</sub>
A <sub>13-20</sub>	Вредоносное программное обеспечение (ПО)	20	A <sub>3-13</sub>	A <sub>20-27</sub>
A <sub>3-21</sub>	Случайные угрозы безопасности	15	A <sub>1-3</sub>	A <sub>21-22</sub> , A <sub>21-23</sub> , A <sub>21-24</sub>
A <sub>21-22</sub>	Схемные и системотехнические ошибки разработчиков	20	A <sub>3-21</sub>	A <sub>22-27</sub>
A <sub>21-23</sub>	Структурные, алгоритмические и программные ошибки	20	A <sub>3-21</sub>	A <sub>23-27</sub>
A <sub>21-24</sub>	Ошибки человека как звена информационной системы	20	A <sub>3-21</sub>	A <sub>24-27</sub>
A <sub>4-25</sub>	Проблема с электропитанием в системе	10	A <sub>1-4</sub>	A <sub>25-27</sub>
A <sub>4-26</sub>	Проблема с водоснабжением в системе	10	A <sub>1-4</sub>	A <sub>26-27</sub>
A <sub>7-27</sub>	Обнаружение нарушения работы системы	5	A <sub>5-7</sub>	A <sub>27-29</sub>

A <sub>8-27</sub>	Обнаружение нарушения работы системы	5	A <sub>5-8</sub>	A <sub>27-29</sub>
A <sub>9-27</sub>	Обнаружение нарушения работы системы	5	A <sub>6-9</sub>	A <sub>27-29</sub>
A <sub>10-27</sub>	Обнаружение нарушения работы системы	5	A <sub>6-10</sub>	A <sub>27-29</sub>
A <sub>10-28</sub>	Обнаружение кражи конфиденциальных данных	10	A <sub>6-10</sub>	A <sub>28-29</sub>
A <sub>11-27</sub>	Обнаружение нарушения работы системы	5	A <sub>6-11</sub>	A <sub>27-29</sub>
A <sub>11-28</sub>	Обнаружение кражи конфиденциальных данных	10	A <sub>6-11</sub>	A <sub>28-29</sub>
A <sub>12-28</sub>	Обнаружение кражи конфиденциальных данных	10	A <sub>6-12</sub>	A <sub>28-29</sub>
A <sub>14-28</sub>	Обнаружение кражи конфиденциальных данных	10	A <sub>13-14</sub>	A <sub>28-29</sub>
A <sub>15-28</sub>	Обнаружение кражи конфиденциальных данных	10	A <sub>13-15</sub>	A <sub>28-29</sub>
A <sub>16-28</sub>	Обнаружение кражи конфиденциальных данных	10	A <sub>13-16</sub>	A <sub>28-29</sub>
A <sub>17-28</sub>	Обнаружение кражи конфиденциальных данных	10	A <sub>13-17</sub>	A <sub>28-29</sub>
A <sub>18-27</sub>	Обнаружение нарушения работы системы	5	A <sub>13-18</sub>	A <sub>27-29</sub>
A <sub>18-28</sub>	Обнаружение кражи конфиденциальных данных	5	A <sub>13-18</sub>	A <sub>28-29</sub>
A <sub>19-28</sub>	Обнаружение кражи конфиденциальных данных	10	A <sub>13-19</sub>	A <sub>28-29</sub>
A <sub>20-27</sub>	Обнаружение нарушения работы системы	5	A <sub>13-20</sub>	A <sub>27-29</sub>

	работы системы			
A <sub>22-27</sub>	Обнаружение нарушения работы системы	5	A <sub>21-22</sub>	A <sub>27-29</sub>
A <sub>23-27</sub>	Обнаружение нарушения работы системы	5	A <sub>21-23</sub>	A <sub>27-29</sub>
A <sub>24-27</sub>	Обнаружение нарушения работы системы	5	A <sub>21-24</sub>	A <sub>27-29</sub>
A <sub>25-29</sub>	Определение фактора воздействия угрозы	5	A <sub>4-25</sub>	-
A <sub>26-29</sub>	Определение фактора воздействия угрозы	5	A <sub>4-26</sub>	-
A <sub>27-29</sub>	Определение фактора воздействия угрозы	2	A <sub>7-27</sub> , A <sub>8-27</sub> , A <sub>9-27</sub> , A <sub>10-27</sub> , A <sub>11-27</sub> , A <sub>18-27</sub> , A <sub>20-27</sub> , A <sub>22-27</sub> , A <sub>24-27</sub>	-
A <sub>28-29</sub>	Определение фактора воздействия угрозы	2	A <sub>10-28</sub> , A <sub>11-28</sub> , A <sub>12-28</sub> , A <sub>14-28</sub> , A <sub>15-28</sub> , A <sub>16-28</sub> , A <sub>17-28</sub> , A <sub>18-28</sub> , A <sub>19-28</sub>	-

Рисунок 3.1. Сетевой график образования угрозы.

## 2.8. Сетевая модель мониторинга угрозы

Таблица 3.3.

### Перечень событий мониторинга

Обозначение	Наименование событий
-------------	----------------------

$a_0$	Начало мониторинга системы «линия 3д печати»
$a_1$	Мониторинг проявления угрозы в системе
$a_2$	Мониторинг системы «линия 3д печати», связанные с устройством
$a_3$	Мониторинг системы «линия 3д печати», связанные с планом функционирования
$a_4$	Мониторинг системы «линия 3д печати», связанные с ресурсами
$a_5$	Начало мониторинга ПО
$a_6$	Начало мониторинга аппаратной части
$a_7$	Проверка системного программного обеспечения
$a_8$	Проверка прикладного программного обеспечения
$a_9$	Мониторинг сетевого оборудования
$a_{10}$	Проверка датчиков
$a_{11}$	Проверка линий связи
$a_{12}$	Проверка включения службы маршрутизации
$a_{13}$	Начало мониторинга преднамеренных угроз безопасности
$a_{14}$	Мониторинг доступа в дом ограниченному кругу лиц
$a_{15}$	Проверка данных с датчиков
$a_{16}$	Мониторинг доступа в систему «линия 3д печати» с помощью индивидуального логина/пароля
$a_{17}$	Проверка перехвата информации
$a_{18}$	Проверка наличия оборудования
$a_{19}$	Мониторинг хакерских атак
$a_{20}$	Поиск вредоносных программных обеспечений
$a_{21}$	Начало мониторинга случайных угроз безопасности
$a_{22}$	Проверка на схемные и системотехнические ошибки разработчиков

$a_{23}$	Проверка на структурные, алгоритмические и программные ошибки
$a_{24}$	Проверка действий пользователя
$a_{25}$	Мониторинг электропитания в системе
$a_{26}$	Мониторинг водоснабжения в системе
$a_{27}$	Проверка полной работоспособности с помощью ПО
$a_{28}$	Проверка включения удаленного доступа
$a_{29}$	Анализ информации и запись ее в журнал тестирования

Таблица 3.4.

Перечень работ мониторинга.

<b>Обозначение работ</b>	<b>Наименование работ</b>	<b>Время выполнения работ, мин</b>	<b>Предшествующие работы</b>	<b>Последующие работы</b>
A <sub>0-1</sub>	Начало мониторинга системы «линия 3д печати»	10	-	A <sub>1-2</sub> A <sub>1-3</sub> A <sub>1-4</sub>
A <sub>1-2</sub>	Мониторинг системы «линия 3д печати», связанные с устройством	15	A <sub>0-1</sub>	A <sub>2-5</sub> , A <sub>2-6</sub>
A <sub>1-3</sub>	Мониторинг системы «линия 3д печати», связанные с планом функционирования	15	A <sub>0-1</sub>	A <sub>3-13</sub> , A <sub>3-21</sub>
A <sub>1-4</sub>	Мониторинг системы «линия 3д печати», связанные с ресурсами	15	A <sub>0-1</sub>	A <sub>4-25</sub> , A <sub>4-26</sub>
A <sub>2-5</sub>	Начало мониторинга ПО	20	A <sub>1-2</sub>	A <sub>5-7</sub>

A <sub>2-6</sub>	Начало мониторинга аппаратной части	20	A <sub>1-2</sub>	A <sub>5-8</sub>
A <sub>5-7</sub>	Проверка системного программного обеспечения	30	A <sub>2-5</sub>	A <sub>7-27</sub>
A <sub>5-8</sub>	Проверка прикладного программного обеспечения	30	A <sub>2-5</sub>	A <sub>8-27</sub>
A <sub>6-9</sub>	Мониторинг сетевого оборудования	30	A <sub>2-6</sub>	A <sub>9-27</sub>
A <sub>6-10</sub>	Проверка датчиков	30	A <sub>2-6</sub>	A <sub>10-27</sub>
A <sub>6-11</sub>	Проверка линий связи	30	A <sub>2-6</sub>	A <sub>11-27</sub>
A <sub>6-12</sub>	Проверка включения службы маршрутизации	30	A <sub>2-6</sub>	A <sub>12-27</sub>
A <sub>3-13</sub>	Начало мониторинга преднамеренных угроз безопасности	15	A <sub>1-3</sub>	A <sub>13-18</sub>
A <sub>13-14</sub>	Мониторинг доступа в дом ограниченному кругу лиц	30	A <sub>3-13</sub>	A <sub>14-27</sub>
A <sub>13-15</sub>	Проверка данных с датчиков	30	A <sub>3-13</sub>	A <sub>15-27</sub>
A <sub>13-16</sub>	Мониторинг доступа в систему «линия 3д печати» с помощью индивидуального логина/пароля	30	A <sub>3-13</sub>	A <sub>16-27</sub>
A <sub>13-17</sub>	Проверка перехвата информации	30	A <sub>3-13</sub>	A <sub>17-27</sub>
A <sub>13-18</sub>	Проверка наличия оборудования	30	A <sub>3-13</sub>	A <sub>18-27</sub>
A <sub>13-19</sub>	Мониторинг хакерских атак	30	A <sub>3-13</sub>	A <sub>19-27</sub>
A <sub>13-20</sub>	Поиск вредоносных программных обеспечений	30	A <sub>3-13</sub>	A <sub>20-27</sub>

A <sub>3-21</sub>	Начало мониторинга случайных угроз безопасности	15	A <sub>1-3</sub>	A <sub>21-22</sub> , A <sub>21-23</sub> , A <sub>21-24</sub>
A <sub>21-22</sub>	Проверка на схемные и системотехнические ошибки разработчиков	40	A <sub>3-21</sub>	A <sub>22-27</sub>
A <sub>21-23</sub>	Проверка на структурные, алгоритмические и программные ошибки	40	A <sub>3-21</sub>	A <sub>23-27</sub>
A <sub>21-24</sub>	Проверка действий пользователя	30	A <sub>3-21</sub>	A <sub>24-27</sub>
A <sub>4-25</sub>	Мониторинг электропитания в системе	20	A <sub>1-4</sub>	A <sub>25-27</sub>
A <sub>4-26</sub>	Мониторинг водоснабжения в системе	20	A <sub>1-4</sub>	A <sub>26-27</sub>
A <sub>7-29</sub>	Анализ информации и запись ее в журнал тестирования	1	A <sub>5-7</sub>	-
A <sub>8-29</sub>	Анализ информации и запись ее в журнал тестирования	1	A <sub>5-8</sub>	-
A <sub>9-27</sub>	Проверка полной работоспособности с помощью ПО	35	A <sub>6-9</sub>	A <sub>27-29</sub>
A <sub>10-27</sub>	Проверка полной работоспособности с помощью ПО	35	A <sub>6-10</sub>	A <sub>27-29</sub>
A <sub>10-28</sub>	Проверка включения удаленного доступа	15	A <sub>6-10</sub>	A <sub>28-29</sub>
A <sub>11-27</sub>	Проверка полной работоспособности с помощью ПО	35	A <sub>6-11</sub>	A <sub>27-29</sub>
A <sub>12-28</sub>	Проверка включения удаленного доступа	15	A <sub>6-12</sub>	A <sub>28-29</sub>

A <sub>14-29</sub>	Анализ информации и запись ее в журнал тестирования	1	A <sub>13-14</sub>	-
A <sub>15-28</sub>	Проверка включения удаленного доступа	15	A <sub>13-15</sub>	A <sub>28-29</sub>
A <sub>16-28</sub>	Проверка включения удаленного доступа	15	A <sub>13-16</sub>	A <sub>28-29</sub>
A <sub>17-29</sub>	Анализ информации и запись ее в журнал тестирования	1	A <sub>13-17</sub>	-
A <sub>18-29</sub>	Анализ информации и запись ее в журнал тестирования	1	A <sub>13-18</sub>	-
A <sub>19-29</sub>	Анализ информации и запись ее в журнал тестирования	1	A <sub>13-19</sub>	-
A <sub>22-27</sub>	Проверка полной работоспособности с помощью ПО	35	A <sub>21-22</sub>	A <sub>27-29</sub>
A <sub>23-20</sub>	Проверка действий пользователя	25	A <sub>21-23</sub>	A <sub>20-29</sub>
A <sub>24-27</sub>	Проверка полной работоспособности с помощью ПО	35	A <sub>21-24</sub>	A <sub>27-29</sub>
A <sub>25-20</sub>	Проверка действий пользователя	25	A <sub>4-25</sub>	A <sub>20-29</sub>
A <sub>26-20</sub>	Проверка действий пользователя	25	A <sub>4-26</sub>	A <sub>20-29</sub>
A <sub>27-29</sub>	Анализ информации и запись ее в журнал тестирования	1	A <sub>13-17</sub>	--
A <sub>28-29</sub>	Анализ информации и запись ее в журнал тестирования	1	A <sub>13-17</sub>	--

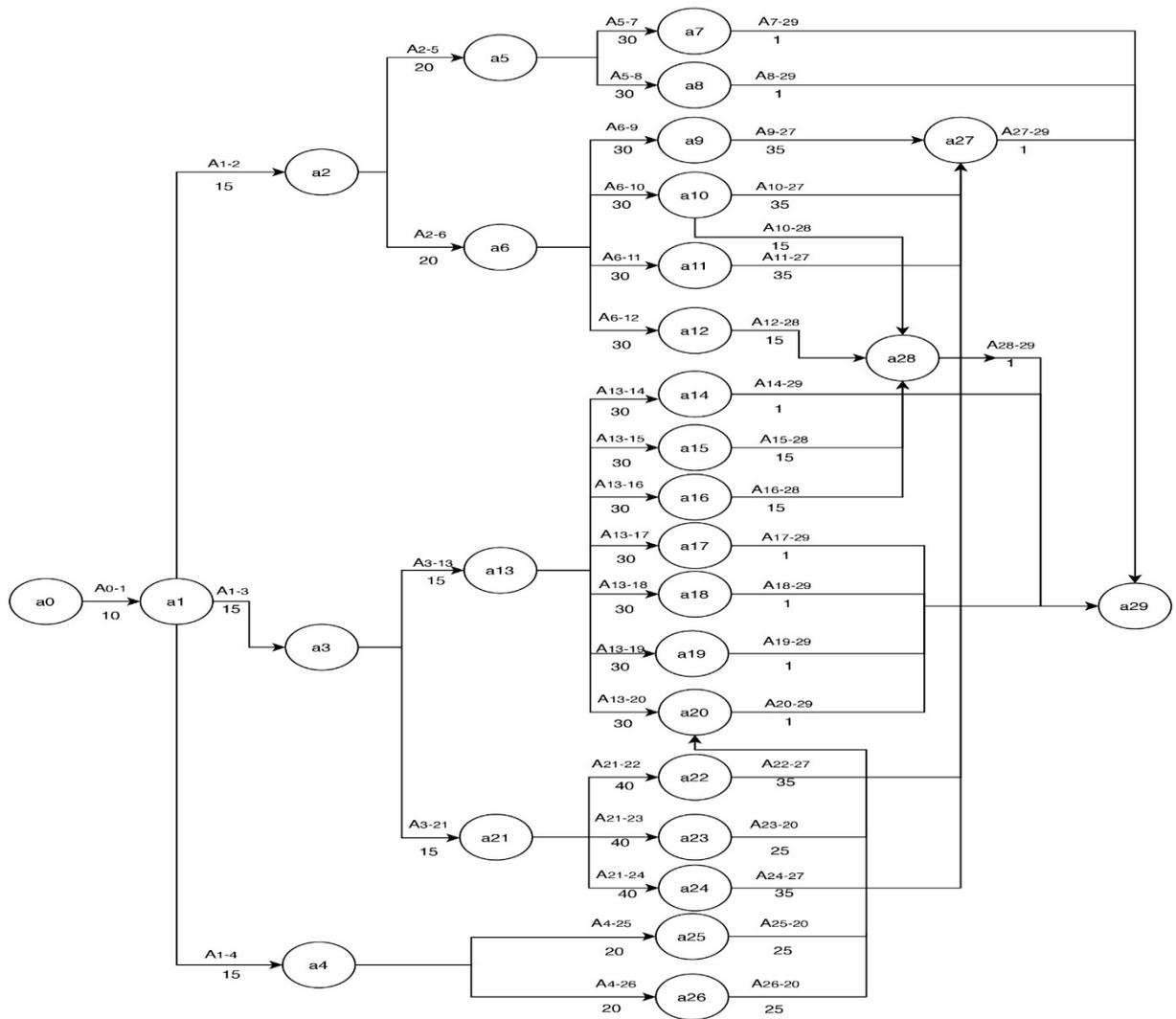


Рис.3.2. Сетевой график мониторинга.

Основными параметрами сетевого графика являются:

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

$$T_p(j) = \max_{i \subset j} (T_p(i) - t_{ij}), \text{ где}$$

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

-  $t_{ij}$  - продолжительность  $(i, j)$  -й работы.

Из обозначения  $i \subset j$  следует, что событие  $i$  предшествует событию  $j$ .

Наиболее раннее возможное время наступления  $j$ -го события  $T_p(j)$

$$T_p(0)=0$$

$$T_p(1)=10$$

$$T_p(2)=25$$

$T_p(3)=25$	$T_p(12)=75$	$T_p(21)=40$
$T_p(4)=25$	$T_p(13)=40$	$T_p(22)=80$
$T_p(5)=45$	$T_p(14)=70$	$T_p(23)=80$
$T_p(6)=45$	$T_p(15)=70$	$T_p(24)=80$
$T_p(7)=75$	$T_p(16)=70$	$T_p(25)=45$
$T_p(8)=75$	$T_p(17)=70$	$T_p(26)=45$
$T_p(9)=75$	$T_p(18)=70$	$T_p(27)=110$
$T_p(10)=75$	$T_p(19)=70$	$T_p(28)=85$
$T_p(11)=75$	$T_p(20)=70$	$T_p(29)=71$

2. Самое позднее допустимое время наступления  $i$ -го события  $T_{п}(i)$ , вычисляемое по формуле

где из обозначения следует, что событие  $j$  предшествует событию  $i$

$T_{п}(0)=0$	$T_{п}(18)=70$
$T_{п}(1)=10$	$T_{п}(19)=70$
$T_{п}(2)=25$	$T_{п}(20)=105$
$T_{п}(3)=25$	$T_{п}(21)=40$
$T_{п}(4)=25$	$T_{п}(22)=80$
$T_{п}(5)=45$	$T_{п}(23)=80$
$T_{п}(6)=45$	
$T_{п}(7)=75$	
$T_{п}(8)=75$	
$T_{п}(9)=75$	
$T_{п}(10)=75$	
$T_{п}(11)=75$	
$T_{п}(12)=75$	
$T_{п}(13)=40$	
$T_{п}(14)=70$	
$T_{п}(15)=70$	
$T_{п}(16)=70$	
$T_{п}(17)=70$	

3. Полный резерв времени работы  $r_{п}(i,j)$ , 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.

$$r_{п}(i,j) = (T_{п}(j) - T_{р}(i) - t_{ij})$$

Смысл полного резерва времени работы заключается в том, что задержка в выполнении работы  $(i,j)$  на величину  $\Delta t_{ij} \geq r_{п}(i,j)$ , приводит к задержке в наступлении завершающего события на величину  $(\Delta t_{ij} - r_{п}(i,j))$ .

Расчёты:

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

Критический путь мониторинга:

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

$a_0a_1a_3a_21a_24a_27a_29$  или  $a_0a_1a_3a_21a_22a_27a_29$  или  $a_0a_1a_2a_6a_11a_27a_29$

Длина критического пути во времени:

$$t_{кр1} = t_{0-1} + t_{1-3} + t_{3-21} + t_{21-24} + t_{24-27} + t_{27-29} = 96 \text{ (мин)}$$

$$t_{кр2} = t_{0-1} + t_{1-3} + t_{3-21} + t_{21-22} + t_{22-27} + t_{27-29} = 96 \text{ (мин)}$$

$$t_{кр3} = t_{0-1} + t_{1-2} + t_{2-6} + t_{6-11} + t_{11-27} + t_{27-29} = 111 \text{ (мин)}$$

## 2.9. Сетевая модель устранения проблемы

Таблица 3.5.

Перечень событий мониторинга

Обозначение	Наименование событий
$a_0$	Начало устранения выявленных угроз в системе «линия 3д печати»
$a_1$	Обращение к журналу тестирования
$a_2$	Устранение проблем в работе «умного дома», связанные с устройством
$a_3$	Устранение проблем в работе «умного дома», связанные с планом функционирования
$a_4$	Устранение проблем в работе «умного дома», связанные с ресурсами
$a_5$	Начало устранения проблем в ПО
$a_6$	Начало устранения проблем аппаратной части
$a_7$	Устранения проблем системного программного обеспечения
$a_8$	Устранения проблем прикладного программного обеспечения

a <sub>9</sub>	Устранения проблем сетевого оборудования
a <sub>10</sub>	Устранения проблем у датчиков
a <sub>11</sub>	Устранены проблемы в линии связи
a <sub>12</sub>	Устранена проблема в службе маршрутизации
a <sub>13</sub>	Начало устранения преднамеренных угроз безопасности
a <sub>14</sub>	Устранения проблем с доступом в дом ограниченному кругу лиц
a <sub>15</sub>	Устранения проблем, связанных с данными датчиков
a <sub>16</sub>	Устранения проблем с доступом в систему «линия 3д печати» с помощью индивидуального логина/пароля
a <sub>17</sub>	Устранения проблем с перехватом информации
a <sub>18</sub>	Оборудование самостоятельно починено
a <sub>19</sub>	Система проверена антивирусом
a <sub>20</sub>	Удалены вредоносные программные обеспечения
a <sub>21</sub>	Начало устранения случайных угроз безопасности
a <sub>22</sub>	Начало устранения схемных и системотехнические ошибки разработчиков
a <sub>23</sub>	Устранены структурные, алгоритмические и программные ошибки
a <sub>24</sub>	Устранены последствия действий пользователя
a <sub>25</sub>	Устранены проблемы с электропитанием в системе
a <sub>26</sub>	Устранены проблемы с водоснабжением в системе
a <sub>27</sub>	Оборудование перезагружено
a <sub>28</sub>	Оборудование самостоятельно починено
a <sub>29</sub>	Оборудование заменено на новое
a <sub>30</sub>	Перестановлены компоненты ПО
a <sub>31</sub>	Отключены ненужные приложения
a <sub>32</sub>	Анализ информации и запись ее в журнал тестирования

## Перечень работ мониторинга

Обозначение работ	Наименование работ	Время выполнения работ, мин	Предшествующие работы	Последующие работы
А0-1	Начало устранения выявленных угроз в системе «линия 3д печати»	10	-	А <sub>1-2</sub> А <sub>1-3</sub> А <sub>1-4</sub>
А1-2	Устранение проблем в работе «умного дома», связанные с устройством	15	А <sub>0-1</sub>	А <sub>2-5</sub> , А <sub>2-6</sub>
А1-3	Устранение проблем в работе «умного дома», связанные с планом функционирования	15	А <sub>0-1</sub>	А <sub>3-13</sub> , А <sub>3-21</sub>
А1-4	Устранение проблем в работе «умного дома», связанные с ресурсами	15	А <sub>0-1</sub>	А <sub>4-25</sub> , А <sub>4-26</sub>
А2-5	Начало устранения проблем в ПО	20	А <sub>1-2</sub>	А <sub>5-7</sub>
А2-6	Начало устранения проблем аппаратной части	20	А <sub>1-2</sub>	А <sub>5-8</sub>
А5-7	Устранения проблем системного программного обеспечения	60	А <sub>2-5</sub>	А <sub>7-27</sub>

A5-8	Устранения проблем прикладного программного обеспечения	60	A <sub>2-5</sub>	A <sub>8-27</sub>
A6-9	Устранения проблем сетевого оборудования	30	A <sub>2-6</sub>	A <sub>9-27</sub>
A6-10	Устранения проблем у датчиков	60	A <sub>2-6</sub>	A <sub>10-27</sub>
A6-11	Устранены проблемы в линии связи	30	A <sub>2-6</sub>	A <sub>11-27</sub>
A6-12	Устранена проблема в службе маршрутизации	30	A <sub>2-6</sub>	A <sub>12-27</sub>
A3-13	Начало устранения преднамеренных угроз безопасности	15	A <sub>1-3</sub>	A <sub>13-18</sub>
A13-14	Устранения проблем с доступом в дом ограниченному кругу лиц	30	A <sub>3-13</sub>	A <sub>14-27</sub>
A13-15	Устранения проблем, связанных с данными датчиков	90	A <sub>3-13</sub>	A <sub>15-27</sub>
A13-16	Устранения проблем с доступом в систему «линия 3д печати» с помощью индивидуального логина/пароля	30	A <sub>3-13</sub>	A <sub>16-27</sub>
A13-17	Устранения проблем с перехватом информации	120	A <sub>3-13</sub>	A <sub>17-27</sub>
A13-18	Оборудование самостоятельно починено	60	A <sub>3-13</sub>	A <sub>18-27</sub>
A13-19	Система проверена антивирусом	90	A <sub>3-13</sub>	A <sub>19-27</sub>

A13-20	Удалены вредоносные программные обеспечения	120	A <sub>3-13</sub>	A <sub>20-27</sub>
A3-21	Начало устранения случайных угроз безопасности	15	A <sub>1-3</sub>	A <sub>21-22</sub> , A <sub>21-23</sub> , A <sub>21-24</sub>
A21-22	Начало устранения схемных и системотехнические ошибки разработчиков	120	A <sub>3-21</sub>	A <sub>22-27</sub>
A21-23	Устранены структурные, алгоритмические и программные ошибки	120	A <sub>3-21</sub>	A <sub>23-27</sub>
A21-24	Устранены последствия действий пользователя	90	A <sub>3-21</sub>	A <sub>24-27</sub>
A4-25	Устранены проблемы с электропитанием в системе	120	A <sub>1-4</sub>	A <sub>25-27</sub>
A4-26	Устранены проблемы с водоснабжением в системе	120	A <sub>1-4</sub>	A <sub>26-27</sub>
A7-27	Оборудование перезагружено	5	A <sub>5-7</sub>	A <sub>27-31</sub>
A8-27	Оборудование перезагружено	5	A <sub>5-8</sub>	A <sub>27-31</sub>
A9-27	Оборудование перезагружено	5	A <sub>6-9</sub>	A <sub>27-31</sub>
A9-28	Оборудование самостоятельно починено	120	A <sub>6-9</sub>	A <sub>28-32</sub>
A10-28	Оборудование самостоятельно починено	120	A <sub>6-10</sub>	A <sub>28-31</sub>
A10-30	Удалены все компоненты, затем переустановлены	30	A <sub>6-10</sub>	A <sub>30-32</sub>
A11-	Оборудование	120	A <sub>6-11</sub>	A <sub>28-32</sub>

28	самостоятельно починено			
A12-27	Оборудование перезагружено	5	A <sub>6-12</sub>	A <sub>27-31</sub>
A12-28	Оборудование самостоятельно починено	120	A <sub>6-12</sub>	A <sub>28-32</sub>
A14-32	Анализ информации и запись ее в журнал тестирования	1	A <sub>13-14</sub>	-
A15-32	Анализ информации и запись ее в журнал тестирования	1	A <sub>13-15</sub>	-
A16-32	Анализ информации и запись ее в журнал тестирования	1	A <sub>13-16</sub>	-
A17-32	Анализ информации и запись ее в журнал тестирования	1	A <sub>13-17</sub>	-
A18-32	Анализ информации и запись ее в журнал тестирования	1	A <sub>13-18</sub>	-
A19-27	Оборудование перезагружено	5	A <sub>13-19</sub>	A <sub>27-31</sub>
A19-32	Анализ информации и запись ее в журнал тестирования	1	A <sub>13-19</sub>	-
A20-31	Отключение всех приложений, которые не используются и не требуются для работы	30	A <sub>13-20</sub>	A <sub>31-30</sub>
A20-32	Анализ информации и запись ее в журнал тестирования	1	A <sub>13-20</sub>	-
A22-28	Оборудование самостоятельно починено	120	A <sub>21-22</sub>	A <sub>28-32</sub>
A22-29	Замена сломанного оборудование на новое, которое	15	A <sub>21-22</sub>	A <sub>29-32</sub>

	имеется			
A23-29	Замена сломанного оборудование на новое, которое имеется	15	A <sub>21-23</sub>	A <sub>29-32</sub>
A24-32	Анализ информации и запись ее в журнал тестирования	1	A <sub>21-24</sub>	-
A25-29	Замена сломанного оборудование на новое, которое имеется	15	A <sub>4-25</sub>	A <sub>29-32</sub>
A25-32	Анализ информации и запись ее в журнал тестирования	1	A <sub>4-25</sub>	-
A26-29	Замена сломанного оборудование на новое, которое имеется	15	A <sub>4-26</sub>	A <sub>29-32</sub>
A26-32	Анализ информации и запись ее в журнал тестирования	1	A <sub>4-26</sub>	-
A26-20	Проверка действий пользователя	25	A <sub>4-26</sub>	A <sub>20-29</sub>
A27-31	Отключение всех приложений, которые не используются и не требуются для работы	30	A <sub>7-27</sub> , A <sub>8-27</sub> , A <sub>9-27</sub> , A <sub>12-27</sub> , A <sub>19-27</sub>	A <sub>31-30</sub>
A28-32	Анализ информации и запись ее в журнал тестирования	1	A <sub>9-28</sub> , A <sub>10-28</sub> , A <sub>11-28</sub> , A <sub>12-28</sub> , A <sub>22-28</sub>	--
A29-32	Анализ информации и запись ее в журнал тестирования	1	A <sub>22-29</sub> , A <sub>23-29</sub> , A <sub>25-29</sub> , A <sub>26-</sub>	-

			29	
A30-32	Анализ информации и запись ее в журнал тестирования	1	A <sub>10-30</sub> , A <sub>31-30</sub>	-
A31-30	Удалены все компоненты, затем переустановлены	30	A <sub>27-31</sub> , A <sub>20-31</sub>	

Наиболее раннее возможное время наступления j-ого события  $T_p(j)$

$T_p(0)=0$	$T_p(11)=75$	$T_p(22)=160$
$T_p(1)=10$	$T_p(12)=75$	$T_p(23)=160$
$T_p(2)=25$	$T_p(13)=40$	$T_p(24)=120$
$T_p(3)=25$	$T_p(14)=70$	$T_p(25)=145$
$T_p(4)=25$	$T_p(15)=70$	$T_p(26)=145$
$T_p(5)=45$	$T_p(16)=70$	$T_p(27)=80$
$T_p(6)=45$	$T_p(17)=160$	$T_p(28)=195$
$T_p(7)=105$	$T_p(18)=100$	$T_p(29)=160$
$T_p(8)=105$	$T_p(19)=130$	$T_p(30)=135$
$T_p(9)=75$	$T_p(20)=160$	$T_p(31)=110$
$T_p(10)=105$	$T_p(21)=40$	

Самое позднее допустимое время наступления i-ого события  $T_{\Pi}(i)$

$T_{\Pi}(0)=0$	$T_{\Pi}(11)=75$	$T_{\Pi}(22)=160$
$T_{\Pi}(1)=10$	$T_{\Pi}(12)=75$	$T_{\Pi}(23)=160$
$T_{\Pi}(2)=25$	$T_{\Pi}(13)=40$	$T_{\Pi}(24)=120$
$T_{\Pi}(3)=25$	$T_{\Pi}(14)=70$	$T_{\Pi}(25)=145$
$T_{\Pi}(4)=25$	$T_{\Pi}(15)=70$	$T_{\Pi}(26)=145$
$T_{\Pi}(5)=45$	$T_{\Pi}(16)=70$	$T_{\Pi}(27)=135$
$T_{\Pi}(6)=45$	$T_{\Pi}(17)=160$	$T_{\Pi}(28)=280$

$T_{\Pi}(7)=105$	$T_{\Pi}(18)=100$	$T_{\Pi}(29)=175$
$T_{\Pi}(8)=105$	$T_{\Pi}(19)=130$	$T_{\Pi}(30)=220$
$T_{\Pi}(9)=75$	$T_{\Pi}(20)=160$	$T_{\Pi}(31)=190$
$T_{\Pi}(10)=105$	$T_{\Pi}(21)=40$	

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

$$r_{\Pi}(i, j) = (T_{\Pi}(j) - T_P(i) - t_{ij})$$

$r_{\Pi}(0,1)=0$	$r_{\Pi}(13,20)=0$	$r_{\Pi}(17,32)=120$
$r_{\Pi}(1,2)=0$	$r_{\Pi}(3,21)=0$	$r_{\Pi}(18,32)=109$
$r_{\Pi}(1,3)=0$	$r_{\Pi}(21,22)=0$	$r_{\Pi}(19,27)=0$
$r_{\Pi}(1,4)=0$	$r_{\Pi}(21,23)=0$	$r_{\Pi}(19,32)=150$
$r_{\Pi}(2,5)=0$	$r_{\Pi}(21,24)=0$	$r_{\Pi}(20,31)=0$
$r_{\Pi}(2,6)=0$	$r_{\Pi}(4,25)=0$	$r_{\Pi}(20,32)=120$
$r_{\Pi}(5,7)=0$	$r_{\Pi}(4,26)=0$	$r_{\Pi}(22,28)=0$
$r_{\Pi}(5,8)=0$	$r_{\Pi}(7,27)=25$	$r_{\Pi}(22,29)=0$
$r_{\Pi}(6,9)=0$	$r_{\Pi}(8,27)=25$	$r_{\Pi}(23,29)=0$
$r_{\Pi}(6,10)=0$	$r_{\Pi}(9,27)=55$	$r_{\Pi}(24,32)=160$
$r_{\Pi}(6,11)=0$	$r_{\Pi}(9,28)=85$	$r_{\Pi}(25,29)=15$
$r_{\Pi}(6,12)=0$	$r_{\Pi}(10,28)=55$	$r_{\Pi}(25,32)=135$
$r_{\Pi}(3,13)=0$	$r_{\Pi}(10,30)=85$	$r_{\Pi}(26,29)=15$
$r_{\Pi}(13,14)=0$	$r_{\Pi}(11,28)=85$	$r_{\Pi}(26,32)=135$
$r_{\Pi}(13,15)=0$	$r_{\Pi}(12,27)=55$	$r_{\Pi}(27,31)=80$
$r_{\Pi}(13,16)=0$	$r_{\Pi}(12,28)=85$	$r_{\Pi}(28,32)=0$
$r_{\Pi}(13,17)=0$	$r_{\Pi}(14,32)=210$	$r_{\Pi}(29,32)=120$
$r_{\Pi}(13,18)=0$	$r_{\Pi}(15,32)=210$	$r_{\Pi}(30,32)=145$
$r_{\Pi}(13,19)=0$	$r_{\Pi}(16,32)=210$	$r_{\Pi}(31,30)=80$

### Критический путь:

$$a_0 \rightarrow a_1 \rightarrow a_3 \rightarrow a_{21} \rightarrow a_{22} \rightarrow a_{28} \rightarrow a_{32}$$

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

### **Глава 3. Разработка модели управления информационной безопасностью на основе принципов системного анализа и информационного противодействия**

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).

На основе данной декомпозиции осуществляется переход от содержательного описания к математической модели процесса. Временные характеристики, полученные в ходе сетевого планирования (Глава 2), трансформируются в интенсивности потоков событий, определяющих динамику системы:

$\lambda=1/\Delta t_{пп}$  - величина, обратная среднему времени проявления проблемы (угрозы). Данный параметр является характеристикой воздействия обстановки на объект и отражает активность внешней среды или интенсивность деградиционных процессов.

$v_1=1/\Delta t_{ип}$  - величина, обратная среднему времени идентификации (распознавания) проблемы. Данный параметр выступает характеристикой эффективности информационно-аналитической работы и определяет качество наблюдаемости системы (способность видеть угрозу).

$v_2=1/\Delta t_{нп}$  - 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 Proxmoх) 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 самую основу производственной линии.

## Заключение

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.

## Список источников

1. Общий подход к моделированию систем обеспечения безопасности. Авторы: Бурлов В.Г., Магулян Г.Г., Матвеев А.В. Издатель: Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Информатика. Телекоммуникации. Управление.
2. Основы теории синтеза облика системы обеспечения безопасности и способов ее функционирования на потенциально опасных объектах. Авторы: Бурлов В.Г., Матвеев А.В. Издатель: Проблемы управления рисками в техносфере.
3. Security trends and advances in manufacturing systems in the era of industry 4.0. Авторы: Sujit Rokka Chhetri. Издатель: IEEE.
4. Defining and Addressing the Cybersecurity Challenges of Additive Manufacturing. Авторы: Chris Adkins, Stephan Thomas, Daniel Moore Издатель: ACM.
5. zkSTAR: A zero knowledge system for time series attack detection enforcing regulatory compliance in critical infrastructure networks. Авторы: Paritosh Ramanan, H.M. Mohaimanul Islam, Abhiram Reddy Alugula Издатель: IEEE.
6. An LSTM-autoencoder based online side channel monitoring approach for cyber-physical attack detection in additive manufacturing. Авторы: Zhangyue Shi, Abdullah Al Mamun, Chen Kan, Wenmeng Tian & Chenang Liu. Издатель: Springer Nature.
7. QualSec: An Automated Quality-Driven Approach for Security Risk Identification in Cyber-Physical Production Systems. Авторы: Matthias Eckhart, Andreas Ekelhart, Stefan Biffel, Arndt Lüder, Edgar Weippl. Издатель: IEEE.
8. A Methodology to Enhance Industrial Control System Security. Авторы: Dominic Timpson a, Esmiralda Moradian. Издатель: ScienceDirect.