Министерство образования и науки Российской Федерации

Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Комсомольский-на-Амуре государственный университет»

На правах рукописи

Мусихин Юрий Федорович

Разработка модели защиты данных АСУТП и исследование её устойчивости

Направление подготовки 09.04.03 - «Прикладная Информатика»
Профиль: Интеллектуальные системы

АВТОРЕФЕРАТ
МАГИСТЕРСКОЙ ДИССЕРТАЦИИ

2025

Работа выполнена в ФГБОУ ВО
«Комсомольский-на-Амуре государственный университет»

Научный руководитель: кандидат физико-математических наук, доцент, доцент кафедры «Прикладная математика» Козлова Ольга Викторовна

Рецензент: кандидат физико-математических наук, программист высшей категории отдела мобильных решений ООО «Индорсофт» Лошманов Антон Юрьевич

Защита состоится 20 июня 2025 года в 08 часов 10 мин на заседании государственной экзаменационной комиссии по направлению подготовки 09.04.03 «Прикладная Информатика», профиль: Интеллектуальные системы, в Комсомольском-на-Амуре государственном университете по адресу: 681013, г. Комсомольск-на-Амуре, пр. Ленина, 27, ауд. 204/5.

Автореферат разослан 13 июня 2025 г.

Секретарь ГЭК З.В. Широкова

ОБЩАЯ ХАРАКТЕРИСТИКА ДИСЕРТАЦИОННОЙ РАБОТЫ

Актуальность темы диссертации определяется необходимостью повышения информационной и киберустойчивости автоматизированных систем управления технологическими процессами (АСУ ТП), используемых на критически важных объектах промышленности. В условиях роста числа кибератак, развития специализированных вредоносных программ (например, Stuxnet, TRITON, BlackEnergy), и активного проникновения цифровых технологий на промышленные предприятия, вопрос обеспечения защиты АСУ ТП становится не просто актуальным, а стратегически важным. Особое значение приобретает разработка современных и интеллектуальных методов защиты, способных адаптироваться к изменяющейся инфраструктуре, выявлять аномалии в поведении операторов и оборудования, а также обеспечивать надежную аутентификацию и шифрование между всеми компонентами системы. Исследование базируется на практической реализации методов защиты на базе оборудования Siemens (S7-1500) и программной платформы TIA Portal в условиях цеха № 26 КнААЗ имени Ю. А. Гагарина. Целью данной работы является разработка автоматизированной системы, позволяющей на основе заданных признаков строить карту, содержащую n характеристик в каждой её точке, с выявлением критических областей.

Для достижения цели решаются следующие задачи:

1. Анализ угроз, уязвимостей и построение концептуальной модели защиты промышленной АСУ ТП, включая оборудование контроллерного и SCADA-уровня.
2. Проектирование и реализация программно-аппаратной архитектуры защиты, основанной на инфраструктуре открытых ключей (PKI), криптографических протоколах (TLS), сертификатной модели аутентификации и взаимодействия.
3. Разработка и внедрение интеллектуального модуля анализа поведения операторов и устройств, а также проведение оценки устойчивости и адаптивности предложенного решения к различным видам угроз.

Объектом исследования является автоматизированная система управления технологическими процессами (АСУ ТП), функционирующая в промышленной среде,

в частности — на штамповочном и прессовом оборудовании авиационного завода (КнААЗ).

Предметом исследования являются методы и средства интеллектуальной защиты компонентов АСУ ТП, включая контроллеры, SCADA, панели оператора и промышленные сети, с акцентом на реализацию криптографической защиты, самообучающихся механизмов и мониторинга аномального поведения.

Научная новизна исследования

Впервые предложена гибридная архитектура защиты АСУ ТП, сочетающая:

- криптографическую модель на базе PKI и TLS;
- систему интеллектуального поведенческого анализа операторов и устройств;
- механизм самообучения и адаптации защитной системы к изменяющейся инфраструктуре.

Разработан подход к автоматическому управлению сертификатами в среде TIA Portal и реализации защищённых каналов связи на базе контроллеров Siemens S7-1500.

Создана модель киберустойчивости, учитывающая как программные, так и физические параметры производственного процесса.

Достоверность и обоснованность результатов исследования.

Предложена гибридная архитектура защиты АСУ ТП, сочетающая:

- криптографическую модель на базе PKI и TLS;
- систему интеллектуального поведенческого анализа операторов и устройств;
- механизм самообучения и адаптации защитной системы к изменяющейся инфраструктуре.

Практическая значимость и достоверность результатов

Разработанная система может быть внедрена на действующих объектах промышленности, включая предприятия оборонного и авиационного профиля.

Методика защиты пригодна для масштабирования на другие уровни АСУ ТП (MES, ERP) и иные типы промышленных контроллеров.

Обеспечена возможность интеграции в существующую инфраструктуру, не нарушая текущих бизнес-процессов.

Результаты уже частично внедряются в цехе №26 КнААЗ, что подтверждает не только применимость, но и востребованность решений.

Подготовленные наборы Python-утилит, шаблоны сертификатов, примеры интеграции SCADA с криптографическими библиотеками — могут использоваться в учебном и промышленном процессе.

Достоверность результатов обеспечивается:

- использованием реальных промышленных данных и сетей КнААЗ;

- многократной валидацией моделей в условиях производственного стенда;

- применением проверенных математических и инженерных методов;

- экспериментальной реализацией прототипа системы в среде TIA Portal и на физическом оборудовании Siemens;

- результатами статистической обработки данных и устойчивости алгоритмов в случае различных атак (MITM, Replay, Spoofing).

Апробация результатов

Результаты работы докладывалась на:

– III-ой Всероссийской научно-практической конференции молодых учёных «Наука, инновации и технологии: от идей к внедрению», декабрь 2024 г.

– VIII Всероссийской национальной научной конференции молодых учёных «Молодёжь и наука: актуальные проблемы фундаментальных и прикладных исследований», апрель 2025 г.

Публикации

– сборник материалов III-ой Всероссийской научно-практической конференции молодых учёных «Наука, инновации и технологии: от идей к внедрению», декабрь 2024 г.

– сборник материалов VIII Всероссийской национальной научной конференции молодых учёных «Молодёжь и наука: актуальные проблемы фундаментальных и прикладных исследований», апрель 2025 г.

Структура и объем.

Магистерская диссертация состоит из введения, общей характеристики, трех глав, заключения и списка литературы. Объем работы – 99 страниц, в том числе 16 рисунка, 6 таблиц.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении сформулированы цели и задачи работы, показана необходимость интеллектуальной кибербезопасности в АСУ ТП. Сделан акцент на значении промышленной безопасности в условиях цифровой трансформации производств. Приведена структура работы: 3 главы, каждая из которых раскрывает один из этапов исследования — от анализа угроз до реальной реализации и тестирования защищённой системы.

В первой главе исследованы типовые архитектуры АСУ ТП, включая сетевые, программные и аппаратные компоненты.

Рассмотрены уязвимости промышленной сети (Profinet), контроллеров Siemens S7-1500, и SCADA (WinCC, TIA Portal).

Проведен обзор моделей угроз: STRIDE, DREAD и модель «Пирамида угроз» для АСУ ТП.

Разработана иерархическая модель Defense-in-Depth с привязкой к конкретным уровням АСУ ТП.

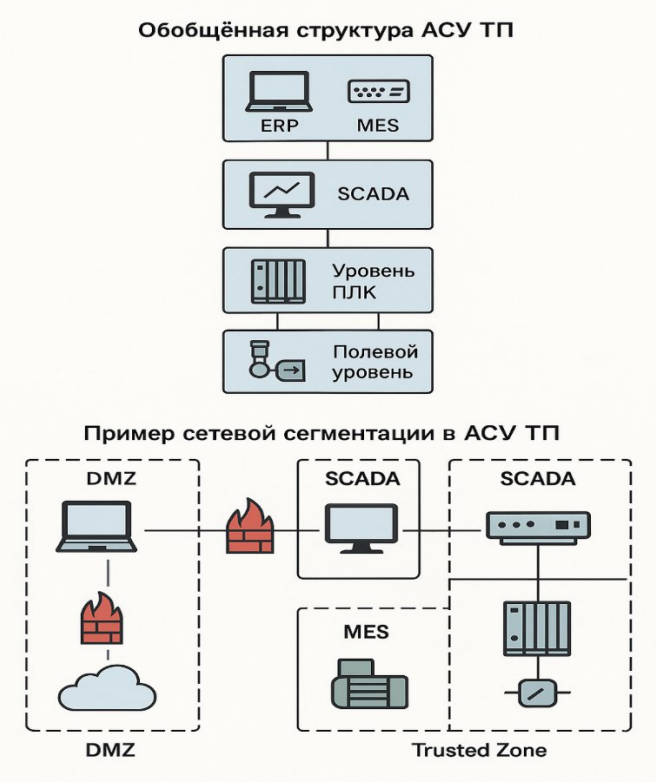

Рисунок 1 – Структура АСУ ТП и архитектура защиты от несанкционированного доступа

На рисунке 1 представлена иерархия промышленной системы управления:

Полевой уровень (Field Level): Датчики, приводы, исполнительные механизмы – взаимодействуют с оборудованием непосредственно.

Уровень ПЛК (PLC): Программируемые логические контроллеры, осуществляющие локальное управление. SCADA: Система диспетчерского управления и сбора данных – визуализирует процесс и отправляет управляющие команды. MES: Система управления производственными операциями – связывает SCADA с верхнеуровневыми системами. ERP: Корпоративная информационная система – планирование и управление ресурсами предприятия.

Между уровнями реализована сегментация и разграничение доступа:

Trusted Zone: Внутренний доверенный сегмент, ограниченный для внешнего доступа. DMZ (Demilitarized Zone): Промежуточная зона, куда выносятся серверы удалённого доступа, журналирования, обновлений. Firewalls (Межсетевые экраны): Защита между зонами – фильтрация, контроль доступа, мониторинг. VPN / IDS / Мониторинг: Применение криптографических каналов и систем обнаружения вторжений для защиты трафика и обнаружения атак.

Примечание: изначально промышленные сети проектировались без учёта киберугроз — основной акцент делался на надёжность, а не безопасность.

Общая характеристика промышленных сетей

Промышленные сети являются технологической основой функционирования АСУ ТП — систем, обеспечивающих управление сложными и часто критически важными технологическими объектами (электростанции, НПЗ, металлургия, водоканалы и др.).

Их ключевое назначение — обеспечение детерминированной, надёжной и безопасной передачи команд и данных между всеми уровнями автоматизации.

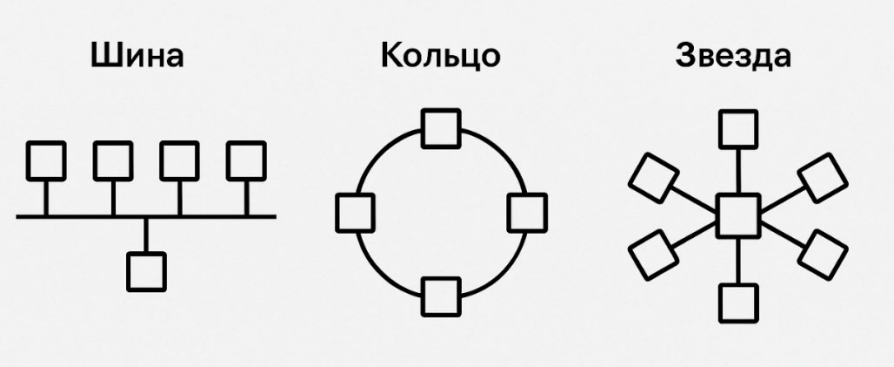

Рисунок 2 – Сравнение топологий промышленных сетей

На рисунке 2 представлены три основные топологии, используемые в промышленных сетях:

Шинная топология (Bus) — все устройства подключаются к одному общему каналу передачи данных. Преимущество — простота реализации и минимальное количество кабеля, однако при обрыве шины нарушается работа всей сети. Кольцевая топология (Ring) — устройства соединены последовательно и образуют замкнутое кольцо. Данные передаются по кругу до достижения адресата. Уязвимость — выход одного узла может повлиять на всю сеть, если не реализовано резервирование. Звездообразная топология (Star) — все устройства подключаются к центральному коммутатору или концентратору. Обеспечивает лёгкую диа-гностику и высокую надёжность при работе узлов, но центральное устройство становится точкой отказа.

Эти топологии определяют способы передачи данных, устойчивость сети к сбоям и сложность её защиты. Выбор зависит от критичности процесса, стоимости внедрения и требований к резервированию. Промышленные сети (Industrial Networks) — это специализированные системы передачи данных, предназначенные для обеспечения взаимодействия между устройствами автоматизации в составе автоматизированных систем управления технологическими процессами (АСУ ТП). В отличие от классических ИТ-сетей, промышленные сети ориентированы не на обеспечение быстрого обмена информацией между пользователями, а на жёстко детерминированную и надёжную связь между оборудованием, управляющим технологическим процессом.

Во второй главе рассмотрено проектирование и применение моделей защиты, ориентированной на действующее оборудование в гражданской авиации, в военной авиации, решения различных промышленных компаний, в том числе и Siemens.

Пример:

Завод гражданской авиации (например, Ульяновский авиазавод — ВАСО), выполняя проект по цифровизации, внедрил в SCADA-сеть:

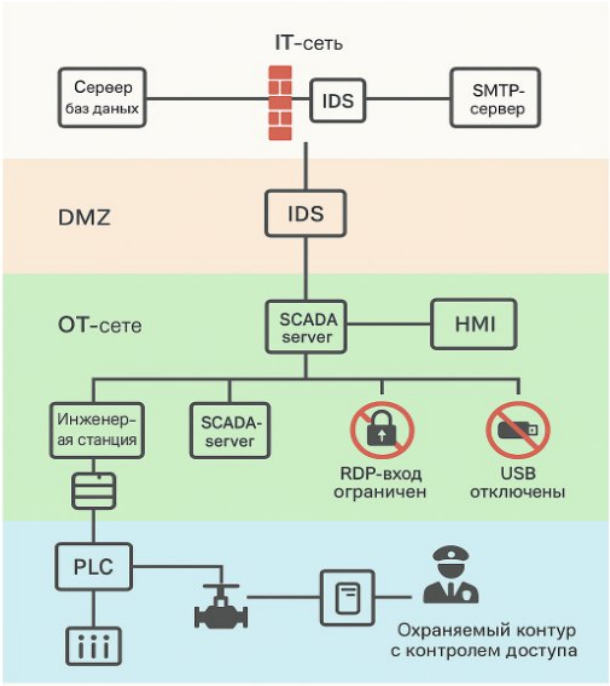

Рисунок 3 — Пример многоуровневой защиты SCADA-сети гражданского авиазавода

Практики обеспечения информационной безопасности в АСУ ТП гражданской авиационной промышленности

Общие особенности отрасли

Гражданская авиационная промышленность характеризуется высокой степенью автоматизации на всех стадиях жизненного цикла продукции — от проектирования и испытаний до производства и технического обслуживания. На предприятиях используются сложные комплексы автоматизации — SCADA-системы, ПЛК, HMI, CAD/CAM, MES, ERP — которые взаимодействуют как друг с другом, так и с внешними подрядчиками, испытательными стендами, цифровыми двойниками. Это создаёт широкую поверхность атаки: от физического доступа к оборудованию на производстве до уязвимостей в ПО и конфигурации сетевых устройств. Поэтому безопасность АСУ ТП в данной сфере опирается на принцип глубокоэшелонированной защиты.

В военной авиации:

2. Использование сертифицированного, доверенного ПО и оборудования

Применяются ОС типа Astra Linux Special Edition, защищённые BIOS и отечественные процессоры;

Аппаратные контроллеры проходят аккредитацию ФСБ и ФСТЭК, и проверяются на наличие недекларированных возможностей;

Используются моноплатформенные протоколы — не Modbus, не OPC, а внутренние стеки, не описанные в открытом доступе.

Важное правило — никакого ПО с открытым исходным кодом без верификации. Даже элементарные обновления проходят проверку в закрытом контуре тестирования.

Многоконтурный аудит и журналирование

Контроль действий ведётся на всех этапах:

Действия оператора SCADA записываются в аппаратный логер событий;

Логи передаются в военную SIEM-систему — такие как СОРМ-военный аналог;

При попытке отклонения от шаблона — автоматическое оповещение командного пункта. Siemens, благодаря своей философии Defense-in-Depth, обеспечивает именно такую архитектуру: масштабируемую, отказоустойчивую и проверенную на практике.

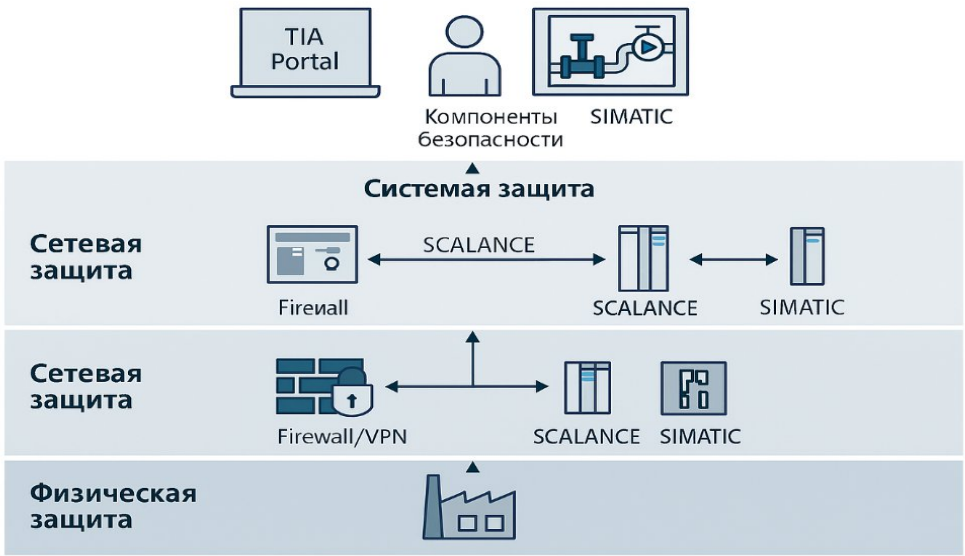

Рисунок 4 — Модель Defense-in-Depth от Siemens в авиационной промышленности

В *третей главе* описывается реализация системы защиты в производственной

среде Цеха №26 КнААЗ. Ниже приведен её фрагмент:

Установка нужных библиотек (один раз):

bash

pip install pyshark cryptography

Код Python: система защиты АСУ ТП

python

```
import pyshark
import time
from cryptography import x509
from cryptography.hazmat.backends import default_backend
# Символический список доверенных сертификатов
trusted_cert_fingerprints = {
    'AB:CD:12:34:EF:56:78:90:11:22:33:44:55:66:77:88': 'Пресс №1',
    '99:88:77:66:55:44:33:22:11:00:AA:BB:CC:DD:EE:FF': 'Пресс №2'
}
# Событие логгирования
def log_event(event_type, details):
    timestamp = time.strftime('%Y-%m-%d %H:%M:%S')
    print(f"[{timestamp}] [{event_type.upper()}] {details}")
# Проверка сертификата клиента
def verify_certificate(cert_pem):
    try:
        cert = x509.load_pem_x509_certificate(cert_pem.encode(), default_backend())
        fingerprint = cert.fingerprint(cert.signature_hash_algorithm).hex().upper()
        fingerprint_formatted = ':'.join(fingerprint[i:i+2] for i in range(0, len(fingerprint), 2))
        return trusted_cert_fingerprints.get(fingerprint_formatted, None)
    except Exception as e:
        log_event('error', f'Ошибка валидации сертификата: {e}')
        return None
# Захват сетевых пакетов (TLS/SCADA трафик)
```

```
def monitor_network(interface='Ethernet'):
    log_event('system', 'Запуск мониторинга сетевого трафика...')
    capture = pyshark.LiveCapture(interface=interface, display_filter='tls')
    for packet in capture.sniff_continuously(packet_count=100):
        try:
            ip_src = packet.ip.src
            cert_raw = packet.tls.handshake_certificate
            log_event('info', f'Получен сертификат от {ip_src}')
            device_name = verify_certificate(cert_raw)
            if device_name:
                log_event('auth', f'Аутентифицированное подключение от: {device_name} ({ip_src})')
            else:
                log_event('alert', f'Обнаружен НЕИЗВЕСТНЫЙ сертификат от {ip_src}. Блокировка.')
                block_client(ip_src)
        except AttributeError:
            continue  # Пропуск, если нет нужных TLS-данных
# Эмуляция блокировки клиента
def block_client(ip_address):
    log_event('firewall', f'Блокировка IP: {ip_address} через SCALANCE API / iptables')
    # В реальной системе тут можно выполнить:
    # subprocess.call(["iptables", "-A", "INPUT", "-s", ip_address, "-j", "DROP"])
# === Запуск ===
if __name__ == "__main__":
    try:
        monitor_network()
    except KeyboardInterrupt:
        log_event('system', 'Мониторинг остановлен пользователем.')
```

Пояснение:

pyshark используется для перехвата TLS-пакетов в сети предприятия.

В *заключении* приводятся основные результаты исследований, проводится анализ, полученных результатов системы защиты АСУ ТП.

СПИСОК ПУБЛИКАЦИЙ ПО ТЕМЕ ИССЛЕДОВАНИЯ

1 Мусихин, Ю.Ф. Математическая модель защиты данных в АСУ ТП: Подходы к разработке и анализ устойчивости / Ю.Ф. Мусихин, С.А. Гордин // сборник материалов III-ой Всероссийской научно-практической конференции молодых учёных «Наука, инновации и технологии: от идей к внедрению» - 2024. - С. 112-114.

2 Мусихин, Ю.Ф. Усовершенствование систем защиты в АСУ ТП на базе Siemens S7-1500 для авиационной промышленности / Ю.Ф. Мусихин, О.В. Козлова // сборник материалов VIII Всероссийской национальной научной конференции молодых учёных «Молодёжь и наука: актуальные проблемы фундаментальных и прикладных исследований». - 2025. - С. 165-167.

3 Мусихин, Ю.Ф. Применение технологий искусственного интеллекта в АСУ ТП на базе Siemens S7-1500 в авиационной промышленности / Ю.Ф. Мусихин, О.В. Козлова // сборник материалов VIII Всероссийской национальной научной конференции молодых учёных «Молодёжь и наука: актуальные проблемы фундаментальных и прикладных исследований». – 2025. - С. 139-142.