## **Информационная безопасность.**

Система должна обеспечивать выполнение нормативно-правовых актов РФ:  
1. Федеральный закон от 26.07.2017 № 187-ФЗ

2. Приказ ФСТЭК России от 14.03.2014 № 31

3. Приказ ФСТЭК России от 25.12.2017

4. № 239 РД ФСТЭК России Федеральный закон от 29.07.2004

5. № 98-ФЗ ГОСТ Р 56542-2015

6. Приказ ФСТЭК России от 18.02.23 № 21

7. Федеральный закон от 27.07.2006 № 152-ФЗ

**П**одсистема **О**беспечения **И**нформационной **Б**езопасности реализована с учетом существующих НПА, а также международных стандартов по обеспечению безопасности и включает в себя подсистемы:

1. Подсистема идентификации и аутентификации

2. Подсистема авторизации и управления доступом

3. Подсистема регистрации и учета событий

4. Подсистема сетевой безопасности

5. Конфиденциальность

6. Подсистема антивирусной защиты

7. Подсистема контроля защищенности

8. Подсистема криптографической защиты

9. Подсистема резервного копирования

10. Подсистема целостности данных

11. Реализация требований к компонентам: API, безопасная разработка

12. Реализация требований к AI/ML

1. Подсистема идентификации и аутентификации

Идентификация и аутентификация в Системе (включая АСУ ТП) производится исключительно с использованием технологии единого входа (Single Sign-On, SSO) на основе доменных учетных записей пользователей. Система не предоставляет интерфейсов для идентификации и аутентификации, обходящих SSO, чтобы предотвратить несанкционированный доступ и обеспечить централизованный контроль. Идентификацию и аутентификацию устройств и процессов соответствует ИАФ.1–ИАФ.2 по Приказу № 239.

В Системе предусмотрены сервисные учетные записи для идентификации и аутентификации субъектов доступа при интеграционных связях со смежными системами и взаимодействии между компонентами. Установлен строгий контроль над сервисными записями (УПД.1 по Приказу № 239), включая автоматическое создание/отзыв и ротацию ключей/паролей. В АСУ ТП запрещено использование общих сервисных аккаунтов; каждая интеграция (например, с PLC) должна иметь уникальный идентификатор. Добавлен аудит использования (логирование всех вызовов). При размещении системы вне АСУ ТП должны быть предусмотрены подобные меры, не противоречащие текущим мерам.

В Системе обеспечивается выполнение условий к применению паролей (минимальная длина, сложность, срок действия и т.д.). Управление средствами аутентификации (ИАФ.4) включает запрет хранения паролей в открытом виде и обязательную ротацию каждые 90 дней. Для АСУ ТП обеспечена защита аутентификационной информации при передаче (ИАФ.7), используя шифрование (TLS 1.3 или СКЗИ). Рекомендуется переход на беспарольные методы (токены, биометрия) для администраторов, если не противоречит реальному времени.

Добавлено ограничение параллельных сеансов (УПД.9) и блокировку при неактивности (УПД.10, например, после 15 минут) с помощью настройки в AD или IdM; интеграция с SIEM для мониторинга сеансов.

1. Подсистема авторизации и управления доступом

Разделение ролей (УПД.4) с назначением минимальных прав (УПД.5) описана в проектной документации. При внедрении в АСУ ТП добавлена ролевая модель для операторов (чтение/мониторинг) и инженеров (конфигурация), с аудитом изменений. Внедрены предупреждения при доступе (УПД.7) и оповещения о входе (УПД.8).

Административный доступ (уровень ОС и ПО) к тестовым, предпродуктивным и продуктивным серверам рекомендовано осуществлять только с применением СКДСА УЗ через СКДСА. Рекомендовано добавить защищенный удаленный доступ (УПД.13) с использованием СКЗИ (средств криптографической защиты). В АСУ ТП должна быть обеспечена сегментация (физическую/логическую) для административных интерфейсов, с контролем доступа из внешних систем (УПД.14) при внедрении системы, предусмотрен мониторинг и реагирование на инциденты (логирование всех доступов).

Разработана политика ИАФ.0 и УПД.0 в рамках предприятия АСУ ТП. Возможна интеграция с промышленными СЗИ для поддержки специфических протоколов.

Должна быть обеспечена реализация соблюдения срока отзыва и перевыпуска ключей.

1. Подсистема регистрации и учета событий

Регистрация событий безопасности (вход/выход, запуск процессов, изменения полномочий и т.д.) соответствуют мерам АУД.1–АУД.4 Приказа № 239, требующим определения событий для регистрации, их сбора и хранения не менее 6 месяцев (или дольше для категорий значимости 1–2). Параметры регистрации (объект/субъект доступа, результат, дата/время, IP-адрес) отражают АУД.2 (сбор сведений о событиях) и АУД.3 (анализ событий), включая фиксацию причин отказов для расследования инцидентов. Уровни регистрации (ОС, ППО) и ограничение доступа к журналам соответствуют АУД.5 (защита информации о событиях) и требованиям к сегментации в АСУ ТП (Приказ № 31). Запрет раскрытия конфиденциальной информации в ошибках и журналах отражает меры по конфиденциальности (ЗКИ.1–ЗКИ.3) и предотвращение утечек (УПД.11).

Применимость текущих мер должна определяться предприятием АСУ ТП и зависит от категории значимости ЗОКИИ (1–3 по Приказу № 239) и уровня защиты информации (по Приказу № 31). Для высококритических АСУ ТП требования: добавлены меры по защите журналов от модификации (криптографическая целостность), интеграция с SIEM-системами для автоматизированного анализа и уведомлений о инцидентах. Данные мероприятия должны быть реализованы и проработаны в рамках АСУ ТП. Срок локального хранения журналов не менее 6 месяцев (возможно расширить до 1–5 лет для категорий значимости 1–2 по Приказу № 239). Доступ к событиям безопасности ограничен (RBAC с минимальными привилегиями). Обеспечено удаленное хранение в защищенном архиве (ЗКИ.3) с сегментацией и аудитом доступа. В АСУ ТП система интегрируется с СОИБ (системой обеспечения информационной безопасности) для автоматизированного анализа).

Конфиденциальная информация, а также сведения о системе, идентификаторы сессии или информация об учетной записи, пароли, не раскрываются в ответах об ошибках в интерфейсе ИС. Конфиденциальная информация и пароли не хранятся в журналах.

1. Подсистема сетевой безопасности

Разработана сетевая архитектура с сегментацией (DMZ, VLAN для промышленных и административных сетей). Используются СКЗИ для шифрования трафика (TLS 1.3 или ГОСТ-алгоритмы).

При размещении в сервисе контейнеризации используются NetworkPolicy для подов, ограничивая трафик по портам и IP. Производится ежеквартальный аудит открытых портов.

Рекомендовано обеспечить проведение ежемесячного аудита сетевой безопасности (СЗД.5), моделирование угроз и обучение персонала, разработать план реагирования на сетевые инциденты, данная информация описывается в документации на АСУ ТП.

В рамках АСУ ТП и инфраструктуры предприятий должен быть расширен контроль портов на уровне ОС, СУБД и сетевых устройств (СЗД.3, фильтрация трафика).

1. Конфиденциальность

В системе не предполагается обработка персональных данных (ПДн) в смысле Федерального закона № 152-ФЗ "О персональных данных". При обработке персональных данных заказчиком должны быть реализованы меры по защите ПДн в соответствии с законодательством РФ.

Система может обрабатывать другие категории конфиденциальной информации (ЗКИ.1 по Приказу № 239), такие как технологические данные, коммерческая тайна или информация ограниченного доступа. В АСУ ТП должна быть классификацию всех данных (например, "конфиденциально" для схем процессов) и запрет на интеграцию с системами, обрабатывающими ПДн без дополнительных мер в связи с предотвращением случайных утечек при интеграциях (например, с ERP-системами).

Необходимо в рамках АСУ ТП проработать вопрос наличия конфиденциальной информации (ЗКИ.3, защита при передаче), включая технологические данные в АСУ ТП (например, уведомления о сбоях). При наличии должно быть добавлено шифрование email (PGP или S/MIME) и фильтрацию контента. В АСУ ТП должно быть реализована интеграция с защищенными каналами (например, внутренние мессенджеры или SCADA-интерфейсы) вместо email (допустимо при интеграции в системы не АСУ ТП).

1. Подсистема антивирусной защиты

Антивирусная защита с централизованным управлением соответствует мерам АЗ.1 (применение средств антивирусной защиты) и АЗ.2 (централизованное управление обновлениями и сканированием) по Приказу № 239.   
Контроль целостности (отключение неиспользуемых служб, удаление средств разработки, контроль ПО и СЗИ, ограничение административного доступа) отражает КЦ.1 (контроль целостности ПО), КЦ.2 (отключение ненужных компонентов) и УПД.5 (минимальные привилегии) по Приказу № 239, а также требования к hardening в АСУ ТП по Приказу № 31 (п. 4.3, минимизация конфигурации). Данные мероприятия должны быть проработаны в рамках развертывания инфраструктуры на АСУ ТП или на иных мощностях.

Необходимо обязательное использование сертифицированных средств антивирусной защиты (АЗ.1), с учетом специфики АСУ ТП (например, низкоуровневые сканеры для контроллеров PLC) для предотвращения угроз внедрения вредоносного ПО в реальном времени.

1. Подсистема контроля защищенности

Включено планирование ежегодных аудитов защищённости (КЗИ.1), с моделированием угроз и оценкой рисков. В АСУ ТП добавлена проверка на влияние на технологические процессы (например, симуляция в тестовой среде) в связи с обеспечением проактивного подхода к выявлению уязвимостей. В рамках предпрития рекомендовано предусмотрено проверку цепочки поставок (НДВ.2). В АСУ ТП должны быть ограничены библиотеки совместимыми с промышленными стандартами в связи с предотвращением supply chain attacks.

При размещении системы в облаке рекомендуется добавить интеграцию с PaaS-security (например, Kubernetes RBAC). В АСУ ТП адаптировать к гибридным облакам, с сегментацией.

Рекомендовано обеспечить ежемесячные сканирования (КЗИ.3). В АСУ ТП интегрировать с промышленными сканерами.

1. Подсистема криптографической защиты

Запрет хранения и передачи паролей в незащищенном виде соответствует мерам ИАФ.4 (управление средствами аутентификации) и ЗКИ.2 (шифрование конфиденциальной информации) по Приказу № 239.

Криптозащита при передаче по незащищенным каналам за пределы контролируемой территории отражает КЗИ.3 (защита каналов связи) и требования к сегментации сетей в АСУ ТП по Приказу № 31 (п. 4.2), где внешние каналы (например, для удаленного мониторинга) должны использовать VPN или СКЗИ.

По рекомендациям NIST и ФСТЭК (в проектах обновлений к Приказу № 239) используется TLS версии 1.3

1. Подсистема резервного копирования

Срок хранения резервных копий – в соответствии с регламентными нормами, а также мерами НДВ.3 Приказа ФСТЭК № 239 (минимум 6 месяцев для категории 3 ЗОКИИ, до 5 лет для категории 1).

Дифференциацию: ежедневные бэкапы — 1 месяц, еженедельные — 3 месяца, ежемесячные — 1 год, архивные — до 5 лет в зависимости от данных (критические технологические логи — дольше). В АСУ ТП добавлено хранение конфигураций контроллеров и баз данных реального времени.

В рамках АСУ ТП рекомендовано предусмотреть процедуры в едином регламенте; проводить симуляции восстановления ежеквартально. Интегрировать с SIEM для триггеров бэкапов при инцидентах.

1. Подсистема целостности данных

В системе необходимо реализовать контроль целостности информации, в соответствии с мерами КЦ.1–КЦ.4 Приказа ФСТЭК № 239 - реализовано интеграцией с СУБД. Рекомендуется проводить ежеквартальный аудит целостности.

Рекомендуется, чтобы на размещаемой инфраструктуре обеспечивалось сохранение информации при потере электропитания, программных и технических отказах путем выполнения процедур регулярного полного или выборочного резервного копирования данных, а также процедур восстановления данных из их резервных копий, в соответствии с НДВ.2 по Приказу № 239.

1. Реализация требований к компонентам API, безопасная разработка

Язык/стек: Python 3 + FastAPI

Используемые библиотеки:

**uvicorn  
catboost**

**numpy**

**pandas**

**scipy**

Логи: уровень INFO, WARNING, DEBUG

Аутентификация: предусмотрена в соответствии с “Идентификация и аутентификация”

Статические файлы: раздаются с каталога ../public

Базовые каталоги данных:

../data/data — загруженные файлы current\_{N}.csv

../data/data\_summary — сводки \*.csv

../data/data\_processed — обработанные данные processed\_{N}.csv

../data/data\_feature — фичи feature\_data\_{N}.csv

1. Загрузка файлов

POST /upload

Параметры запроса:

Ответы: 200 ОК, 500 Internal Server Error

1. Получение очтётов

GET /get\_summary

Ответы: 200 OK, 404 NOT FOUND, 500 Internal Server Error

1. Скачивание отчётов

Ответы: 200 OK, 404 NOT FOUND

1. Список загруженных файлов

Ответы: 200 OK, 500 Internal Server Error

1. Удаление отчетов

Ответы: 200 OK, 404 NOT FOUND, 500 Internal Server Error

1. Реализация требований к AI/ML

В рамках проекта сформирована частная модель угроз на основе источников: OWASP Top-10 LLM 2025, MITRE ATLAS. Модель угроз приведена ниже:

## **Частная модель угроз для систем AI/ML**

## **Объекты защиты**

Объекты защиты определяют ключевые компоненты AI-системы, подверженные угрозам. Они включают:

1. **Этап сбора и подготовки данных**:
   * Инфраструктура подготовки и хранения данных: Программно-аппаратные средства для сбора, обработки и хранения данных.
   * Источники данных: Внешние (публичные датасеты, API) и внутренние (корпоративные БД, логи).
   * Подготовка данных: Очистка, нормализация, фильтрация.
   * Датасеты для обучения: Наборы данных после подготовки.
2. **Этап разработки модели и обучения**:
   * Инфраструктура обучения модели: Средства для обучения и оптимизации.
   * Оценка и валидация модели: Тестирование качества и безопасности.
   * Обучение и дообучение: Применение алгоритмов ML.
   * Модель (MR03): Итоговая обученная модель.
   * Фреймворки и код: Библиотеки и исходный код.
   * Open-source модели: Предобученные модели из репозиториев.
   * Модели в открытых источниках: Проприетарные модели, размещенные публично.
3. **Этап эксплуатации и интеграции**:
   * Инфраструктура размещения и инференса: Средства для развертывания в production.
   * Обработка входных/выходных данных: Механизмы пред- и постобработки.
   * Инфраструктура приложения: Средства для выполнения AI-приложений.
   * Приложение: Конечная система с AI.
   * AI-агенты: Автономные системы на базе AI.
   * Функции: Внутренние или внешние функции бизнес-логики.
   * Источники данных: Внешние и внутренние.
   * Обработка пользовательского ввода/вывода: Механизмы валидации и фильтрации.

Требования направлены на защиту этих объектов от несанкционированного доступа, модификации и утечек.

## **Требования, связанные с данными**

### **Проверка данных из внешних источников на отравление**

Система должна обеспечивать автоматизированную проверку и верификацию всех данных и датасетов, загружаемых из внешних источников, на наличие вредоносных элементов (отравленных примеров), перед использованием в обучении или дообучении модели. Это включает сканирование на аномалии, сравнение с эталонными хэшами и применение ML-методов обнаружения отравлений.

Отравленных данных приводит к искажению модели, снижению точности и созданию бэкдоров. Нарушает конфиденциальность, целостность и доступность.

**Меры реализации**:

* Внедрить инструменты типа Data Poisoning Detection (на базе библиотек scikit-learn или custom ML-моделей).
* Организовать процессы: обязательная изоляция загруженных данных в карантинной зоне, ручная/автоматизированная валидация экспертами.
* Интегрировать с CI/CD: автоматизированные тесты на отравление в пайплайне подготовки данных.
* Мониторить источники: вести реестр доверенных внешних источников с периодической проверкой.

### **Контроль модификации данных из внешних источников**

Система должна отслеживать и предотвращать модификацию данных или датасетов из внешних источников после их добавления в реестр, включая мониторинг изменений в источниках и применение цифровых подписей для обеспечения целостности.

Модифицированные данные вызывают искажение модели и создание бэкдоров. Нарушает конфиденциальность, целостность и доступность. Последствия: снижение точности, финансовые потери.

**Меры реализации**:

* Использовать хэширование (SHA-256) и блокчейн-подобные технологии для фиксации состояния данных.
* Реализовать уведомления о изменениях в источниках via API мониторинга.
* Процессуальные меры: политика обновления реестра источников с утверждением изменений.
* Интеграция с SIEM-системами для логирования и алертинга.

### **Предотвращение использования ПДн из внешних источников**

Перед обучением модели, с использованием анонимизации и маскировки для соблюдения ФЗ-152.

ПДн приводят к их воспроизведению в ответах модели. Нарушает конфиденциальность. Последствия: юридические риски, нарушения приватности.

**Меры реализации**:

* Внедрить инструменты типа Presidio или custom NLP для детекции ПДн (имена, адреса, номера).
* Процессы: обязательный скрининг данных с отчетами, интеграция с DLP-системами.
* Обучение персонала: семинары по обработке ПДн.
* Мониторинг: аудит логов на наличие ПДн в датасетах.

### **Проверка внутренних данных на отравление**

Система должна обеспечивать проверку данных из внутренних источников на наличие вредоносных элементов перед использованием в обучении, включая сканирование на аномалии и контроль доступа.

Отравленные внутренние данные искажают модель. Нарушает конфиденциальность, целостность, доступность. Последствия: бэкдоры, снижение точности.

**Меры реализации**:

* Интеграция с антивирусами и ML-детекторами.
* Разграничение доступа: RBAC с минимальными привилегиями.
* Автоматизация: скрипты на Python с библиотеками pandas для анализа датасетов.

### **Контроль конфиденциальной информации во внутренних данных**

Система должна предотвращать загрузку конфиденциальной информации в датасеты для обучения, с классификацией данных и автоматизированной фильтрацией.

**Н**еконтролируемая загрузка приводит к утечкам. Нарушает конфиденциальность. Последствия: воспроизведение конфиденциальных данных.

**Меры реализации**:

* Классификация данных: метки конфиденциальности в БД.
* Фильтры: DLP-инструменты для блокировки загрузки.
* Процессы: утверждение датасетов перед использованием.

### **Управление жизненным циклом данных**

Система должна реализовывать полный контроль над данными для обучения, включая классификацию, метаданные, хранение, удаление и архивирование, с аудитом операций.

**О**тсутствие контроля увеличивает поверхность атаки. Нарушает конфиденциальность, целостность. Последствия: утечки, нарушения ФЗ-152.

**Меры реализации**:

* MDM-системы для управления данными.
* Логирование: все операции с данными в SIEM.
* Политики: срок хранения, автоматическое удаление.

## **Требования, связанные с инфраструктурой**

### **Защита реестра источников данных**

Система должна обеспечивать защиту реестра источников данных от несанкционированной модификации, включая шифрование, контроль доступа и мониторинг изменений.

Модификация реестра приводит к использованию скомпрометированных данных. Нарушает целостность. Последствия: искажение модели.

**Меры реализации**:

* RBAC и MFA для доступа к реестру.
* Версионирование реестра с Git-like инструментами.
* Алертинг на изменения.

### **Защита обучающих данных от модификации**

Система должна предотвращать несанкционированную модификацию обучающих

Модификация данных искажает модель. Нарушает целостность.

**Меры реализации**:

* Immutable storage (WORM).
* Регулярные бэкапы с верификацией.
* Мониторинг файловой системы.

**Ответственные лица**: Владелец ИТ-инфраструктуры хранения данных; владелец

## **Требования, связанные с моделью**

### **Документация данных обучения**

Система должна поддерживать полную документацию данных, использованных для обучения, включая источники, метаданные и историю, для обеспечения traceability и расследования инцидентов.

Отсутствие информации затрудняет реагирование. Нарушает целостность.

**Меры реализации**:

* SBOM-подобные документы для данных.
* Интеграция с MLflow или аналогами.

## **Требования, связанные с приложениями**

### **Безопасное проектирование интеграций**

При проектировании приложений должны использоваться безопасные интеграции компонентов, включая проверку входных/выходных данных, шифрование и контроль доступа.

Ошибки проектирования приводят к утечкам. Нарушает конфиденциальность, целостность, доступность.

**Меры реализации**:

* Secure by Design принципы.
* Code review и penetration testing.

## **Материалы и источники**

Требования разработаны на основе указанных в модели угроз источников: OWASP Top-10 LLM 2025, MITRE ATLAS и др.