Министерство науки и высшего образования Российской Федерации
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО

Факультет безопасности информационных технологий

Дисциплина:

«Основы теории надежности»

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №4

«Перечень угроз и опасностей»

Выполнили:

Чу Ван Доан, студент группы N3347

(подпись)

Проверил:

Мухамеджанов Санжар

(отметка о выполнении)

(подпись)

Санкт-Петербург

2025 г.

Содержание

Введение

Цель работы – Идентификация и анализ угроз и опасностей системы, их причин, последствий и методов контроля. Определение мер для перевода системы в безопасное состояние при отказах. Учет программных ошибок и внешних взаимосвязей. Применение методов нормирования рисков (GAMAB, ALARP, MEM) для дальнейшего анализа.

Задание

Перечень угроз и опасностей должен описывать характеристику каждой опасности системы (подсистемы), причины, которые могут вызвать опасность, опасные события и последствия их возникновения, а также методы и мероприятия, контролирующие правильность выполнения ответственных функций и переводящие систему в безопасное состояние.

Дополнительно для каждого опасного события можно описать метод нормирования (GAMAB, ALARP, MEM). который будет применяться на следующем этапе жизненного цикла функциональной безопасности – анализ (оценка) рисков.

Анализируя деревья опасностей (FTA), которые проектировались в лабораторной работе №2, должны выделить опасности системы.

При не обнаружении опасностей наступает опасное событие, которое считается отказом защитных мер системы.

Необходимо учитывать связь с внешними системами (соседними подсистемами).

Программные ошибки также влияют на работу функций. Для проверки правильной работы программных компонентов необходимо использовать контролирующие функции, которые переводят систему в безопасное состояние в случае наступления отказа. Здесь необходимо определить, что будет являться для рассматриваемой системы безопасным состоянием.

Ход работы

1. Дерево неисправностей построено в лабораторной работе №2

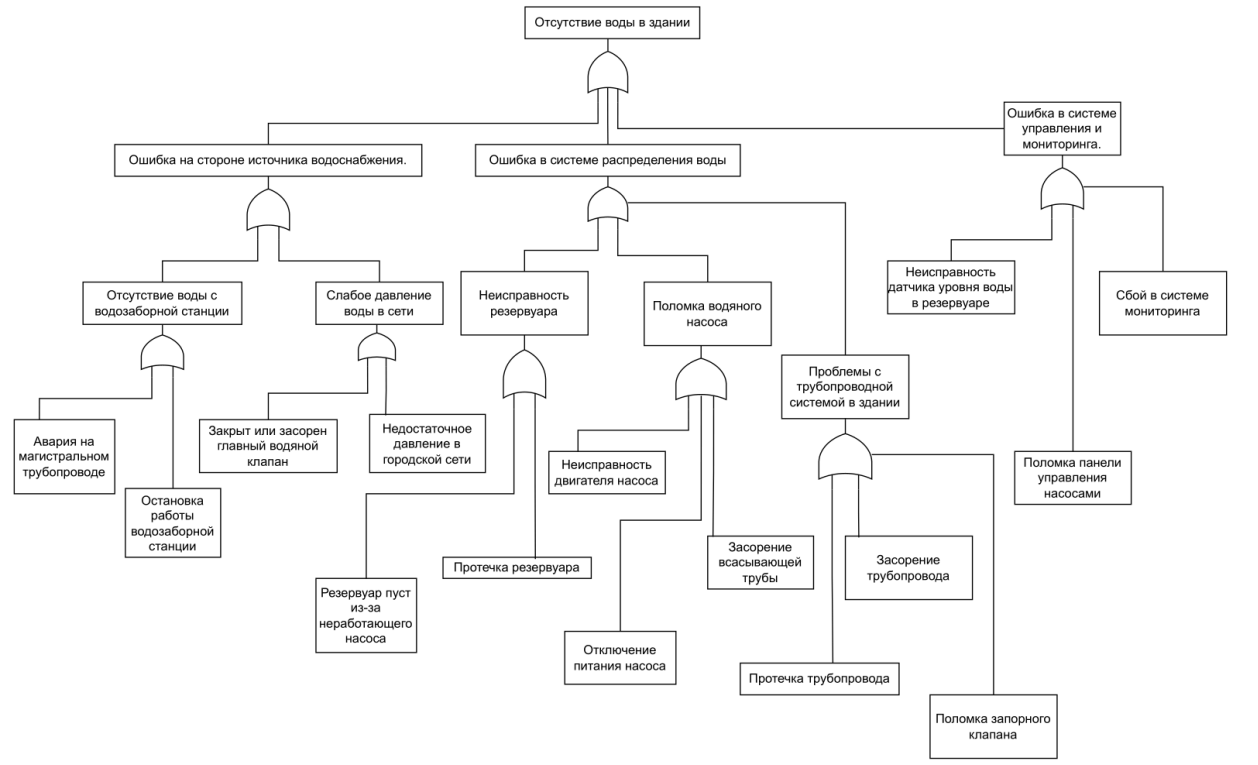

Рисунок 1 - Схема FTA

2. Анализ опасностей на основе дерева отказов (FTA)

Таблица 1 – Анализ опасностей на основе дерева отказов

Опасность	Причина	Опасное событие	Последствия	Методы и меры контроля
Отказ источника водоснабжения	Авария на магистральном трубопроводе	Прекращение подачи воды	Полное отсутствие воды в здании	Получение уведомлений от городских служб, резервный источник воды

Отказ источника водоснабжения	Остановка водозаборной станции (авария/профилактика)	Нет подачи воды	Нарушение всех видов деятельности в здании	Мониторинг, резервная насосная установка
Недостаточное давление в сети	Закрыт или засорён главный водяной клапан	Снижение давления или полное прекращение	Вода не поступает в здание	Плановая проверка клапанов, установка датчиков давления
Недостаточное давление в сети	Недостаточное давление в городской системе	Вода не поднимается на верхние этажи	Частичное отсутствие воды (верхние этажи)	Использование повысительных насосов, накопительные баки
Отказ распределительной системы	Пустой резервуар из-за неработающего насоса	Нет воды для распределения	Отсутствие подачи воды по этажам	Контроль состояния насоса, резервный насос
Отказ распределительной системы	Протечка резервуара	Быстрая потеря воды	Опустошение резервуара, остановка системы	Плановый осмотр, устранение протечек
Отказ водяного насоса	Неисправность двигателя	Насос не работает	Нет циркуляции воды, даже при наличии в резервуаре	Диагностика, резервный насос
Отказ водяного насоса	Отключение питания насоса	Насос не запускается	Потеря подачи воды	Источник бесперебойного питания (UPS), переключение на аварийное питание
Отказ водяного насоса	Засорение всасывающей трубы	Снижение эффективности насоса	Снижение объёма подачи воды	Фильтрация, регулярная прочистка труб
Повреждение трубопровода	Протечка труб	Потеря давления, утечка	Потеря воды, риск затопления	Датчики утечки,

				аварийные клапаны
Повреждение трубопровода	Засорение труб	Блокировка потока воды	Нет воды в отдельных зонах здания	Промывка трубопроводов, фильтрация
Неисправность запорного клапана	Заклинивание или износ	Нарушение распределения воды	Одни зоны получают воду, другие — нет	Замена клапанов, использование автоматических систем управления
Отказ датчиков уровня воды	Поломка датчика	Насос не включается или работает без остановки	Переполнение или нехватка воды	Резервные датчики, аварийные сигналы
Неисправность панели управления насосами	Сбой оборудования или ПО	Насосы не запускаются	Нарушение всей системы даже при наличии воды	Резервное управление, диагностика
Отказ системы мониторинга	Программный или аппаратный сбой	Не выявляется авария	Задержка устранения проблемы, длительное отсутствие воды	Дублирование каналов мониторинга, ручной контроль

3. Безопасное состояние системы

Безопасное состояние — это такое состояние системы, при котором она не представляет опасности для людей, имущества или окружающей среды, даже в случае отказа.

Таблица 2 - Безопасное состояние в зависимости от опасности

Модуль / Подсистема	Тип отказа / Опасность	Безопасное состояние системы
Источник водоснабжения	Отсутствие воды от городской сети или остановка станции	Переход на резервный источник (резервуар, автоцистерна); аварийное оповещение технического персонала

Насосная система	Отказ основного насоса, отключение питания, засорение труб	Отключение неисправного насоса; включение резервного насоса; отправка сигнала об ошибке
Резервуары и накопительные баки	Переполнение или опустошение резервуара	Автоматическое отключение насоса при переполнении; перекрытие входа воды при утечке
Трубопроводная система	Протечка или засорение труб	Изоляция повреждённого участка при помощи автоматических или ручных клапанов; сигнал тревоги
Система управления и мониторинга	Отказ датчиков, программная ошибка	Переход в ручной режим управления, блокировка опасных автоматических операций, оповещение оператора
Панель управления насосами	Отказ в управлении насосами	Переход в аварийный режим, остановка насосов для предотвращения цепной неисправности
Вся система в целом	Неопределённое состояние системы	Полное отключение подачи воды, блокировка насосов, сигнал тревоги и активация независимого мониторинга

Принципы перевода системы в безопасное состояние

1. Fail-Safe Shutdown — остановка потенциально опасных компонентов (насосов, клапанов).
2. Явное оповещение об ошибке — передача сигнала на диспетчерский пульт или ответственному персоналу.
3. Переключение на резерв — использование резервного источника при наличии.
4. Ручной контроль — при недостоверности данных от автоматической системы.
5. Ограничение распространения отказа — локализация проблемы (отключение сегментов, активация реле, защит).

Безопасное состояние системы водоснабжения — это такое состояние, при котором система либо полностью прекращает работу, либо переходит на резервные режимы, не допуская угрозы для людей и оборудования, с обязательным оповещением и возможностью восстановления.

4. Безопасное состояние системы

Таблица 3 - Модель нормирования риска: обзор

Метод	Расшифровка	Суть
GAMAB	Globalement Au Moins Aussi Bon	Риск допустим, только если система как минимум столь же безопасна, как существующие аналоги.
ALARP	As Low As Reasonably Practicable	Риск допустим, если он снижен до разумно возможного минимума с учётом затрат и технологий.
MEM	Minimum Endogenous Mortality	Риск допустим, если вероятность гибели ниже уровня естественной смертности в обществе.

Таблица 4 - Подход к нормированию риска для каждого опасного события

Опасное событие	Краткое описание	Предлагаемый метод нормирования риска	Обоснование выбора метода
Полное отсутствие воды в здании	Городская сеть или станция отключена	GAMAB	Сравнивается с аналогичными зданиями – требуется минимум такой же надёжный уровень
Невозможность подачи воды на верхние этажи	Низкое давление в сети	ALARP	Возможны технические решения (повысительный насос), но с разумными затратами
Остановка насоса из-за поломки	Механический отказ	ALARP	Подлежит контролю через ТО и резерв – риск можно снизить разумными мерами
Утечка воды из трубопровода	Повреждение труб, потеря воды	ALARP	Можно минимизировать с помощью датчиков утечки и изоляции
Переполнение резервуара	Отказ датчика уровня воды	ALARP	Простое техническое решение – дублирование датчиков

Отказ системы управления насосом	Программная или аппаратная ошибка	GAMAB	Требуется надёжность на уровне промышленных систем
Задержка реагирования из-за сбоя мониторинга	Нет своевременного уведомления	ALARP	Допускается при наличии периодической ручной проверки
Неравномерное распределение воды	Клапан не работает	ALARP	Технически легко устранимо – проверка и замена
Насос не включается при наличии воды	Отказ электропитания или ПО	GAMAB	Требуется высокая надёжность – система должна иметь бесперебойное питание
Засорение труб или входа	Грязь, ржавчина, мусор	ALARP	Регулярная прочистка позволяет контролировать уровень риска

Таблица 5 - Итог

Подход	Применение в системе водоснабжения
GAMAB	Для критически важных элементов, где допустим только минимум, проверенный по аналогии.
ALARP	Для элементов, где риск можно разумно снизить, применяя ТО, резерв, автоматизацию.
MEM	Не применяется в данной системе напрямую, так как уровень угроз не связан с летальным исходом.

Заключение

В ходе выполнения лабораторной работы №4 был проведён всесторонний анализ надёжности и функциональной безопасности системы водоснабжения здания. Исходным материалом послужило дерево отказов (FTA), разработанное ранее, которое позволило выделить основные причины и следствия критического события — отсутствия воды в здании.

На основании дерева отказов были систематизированы:

- возможные угрозы и опасности;
- соответствующие опасные события;
- их причины и последствия;
- допустимые методы контроля и восстановления;
- формулировка безопасного состояния системы для каждого случая отказа.

Дополнительно для каждого опасного события был предложен подход к нормированию риска с использованием методик GAMAB, ALARP и частично MEM, в зависимости от характера риска и возможности его управления. Основной упор был сделан на достижение максимально допустимого уровня остаточного риска с разумными затратами и техническими мерами.

Полученные результаты демонстрируют важность системного подхода к обеспечению безопасности на ранних этапах проектирования и эксплуатации инженерных систем. Предложенные методы и меры могут быть масштабированы и адаптированы к другим техническим объектам, требующим высокой надёжности и устойчивости к отказам.

Таким образом, цели лабораторной работы достигнуты. Выполненный анализ является важной частью общего цикла обеспечения функциональной безопасности и даёт основу для проведения оценки рисков, а также дальнейшего проектирования защитных мер.