ФИЛИАЛ ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО
ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ
«СИБИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ПУТЕЙ СООБЩЕНИЯ»
ТОМСКИЙ ТЕХНИКУМ ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

РАЗРАБОТКА ИНТЕРАКТИВНОЙ ТЕТРАДИ ПО ТЕМЕ “ИНТЕГРАЛ”

Пояснительная записка

ДП 09.02.07 000 000 021

Разработал: И. А. Тесляк

Руководитель: В. Г. Галяминских

2025

ФИЛИАЛ ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ «СИБИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ПУТЕЙ И СООБЩЕНИЯ» ТОМСКИЙ ТЕХНИКУМ ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

УТВЕРЖДАЮ:
заместитель директора по
учебно-методической работе
_____Н.Н.Куделькина
«___»_____2025 г.

ЗАДАНИЕ НА РАЗРАБОТКУ ДИПЛОМНОГО ПРОЕКТА

студенту очной формы обучения специальности
09.02.07 Информационные системы и программирование
Тесляк Игорю Алексеевичу

1. Тема проекта: Разработка интерактивной тетради по теме “Интеграл” утверждена приказом № 64-ст/о от 03.03.2025 г.
2. Задание выдано «21» апреля 2025 г.
3. Срок сдачи законченного проекта «…..» ……. 2025 г.
4. Исходные данные: техническое задание, исходные данные по предметной области. На основании исходных данных: разработка интерактивной тетради по теме “Интеграл» цикловой комиссии специальности с использованием языка гипертекстовой разметки HTML, каскадных таблиц стилей CSS, клиентского языка программирования JavaScript.

СОСТАВ ПОЯСНИТЕЛЬНОЙ ЗАПИСКИ

Руководитель_____/Галяминских В. Г./

Председатель цикловой комиссии_____ /Савина И.А./

Протокол № _____

Задание к исполнению принял _____/Тесляк И.А/

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Дипломный проект выполнен в соответствии с заданием на дипломное проектирование. Тема дипломного проекта — «Разработка интерактивной тетради по теме “Интеграл”».

В данном проекте рассматривается создание веб-приложения — интерактивной тетради, предназначенной для изучения темы «Интеграл». Основной задачей разработки является обеспечение доступного, наглядного и эффективного инструмента обучения, включающего структурированные разделы: Теория, Задания, Тесты, Видео и Глоссарий. Такой формат позволяет пользователям не только получать теоретические знания, но и сразу применять их на практике, проходить тесты и обращаться к справочным материалам.

Цели и задачи проекта

Цели: разработать интерактивную тетрадь по теме “Интеграл”

Задачи:

1. Собрать и структурировать материал по теме интегралов
2. Разработать дизайн и интерфейс сайта
3. Реализовать функциональные разделы: Теория, Задания, Тесты, Видео, Глоссарий
4. Обеспечить возможность интерактивного взаимодействия с контентом
5. Обеспечить простоту навигации и доступность использования

1 ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

1.1 Основные понятия

Интерактивная тетрадь (ИРТ) — это современное электронное учебное пособие, которое сочетает в себе элементы тетради (Теоретический материал, задания и тесты) с интерактивными возможностями цифровой среды.

Тест — это стандартизированный метод оценки знаний, умений и навыков учащихся. Он помогает выявить и сформировать индивидуальный темп обучения, пробелы в текущей и итоговой подготовке.

Лекция — систематическое, последовательное изложение учебного материала, какого-либо вопроса, темы, раздела, предмета, методов науки. Практическая работа — это вид учебной деятельности, направленный на формирование практических умений и навыков в конкретной профессиональной области.

Презентация — это способ передачи информации, идей или предложений аудитории с использованием визуальных и аудиовизуальных средств.

Видео — электронная технология формирования, записи, обработки, передачи, хранения и воспроизведения подвижного изображения, основанная на принципах телевидения.

Глоссарий — это алфавитный список терминов, используемых в некоторой области знаний, и их определений.

Анализ объекта автоматизации — это исследование, которое направлено на изучение процесса, процесса управления или действующей системы с целью определения возможностей автоматизации.

Функциональное моделирование — это подход к описанию и анализу систем, при котором процессы рассматриваются как последовательность операций или функций, выполняемых для достижения определённых целей.

Техническое задание (ТЗ) — документ или несколько документов, определяющих цель, структуру, свойства и методы какого-либо проекта. Это инструмент коммуникации между заказчиком и исполнителем.

Программное обеспечение (ПО, софт) — это набор программ, которые позволяют устройству (компьютеру, смартфону, планшету) выполнять определённые задачи.

Браузер — это программа для просмотра веб-страниц, которая преобразует получаемый из сети код в понятные для человеческого восприятия элементы и позволяет управлять ими. Название происходит от английского слова browse — просматривать.

Сайт (веб-сайт) — это совокупность связанных веб-страниц, доступных в интернете и объединённых под одним доменным именем

1.2 Выбор стратегии автоматизации

Для разработки сайтов есть достаточно много решений, среди популярных решений можно выделить:

С помощью языков программирования

Этот метод требует знаний в области веб-разработки, но позволяет получить максимальный контроль над дизайном и функциональностью сайта. Для создания используют, например, HTML, CSS и JavaScript. Такой вариант подходит для сложных и нестандартных проектов.

HTML (HyperText Markup Language) — это язык гипертекстовой разметки. Он объясняет браузеру, как должна выглядеть веб-страница, указывает, где разместить заголовки, картинки, параграфы, кнопки и другие элементы.

CSS (Cascading Style Sheets, «каскадные таблицы стилей») — это язык описания внешнего вида веб-страниц. Он определяет, как элементы HTML будут отображаться в браузере, включая макет, цвета, шрифты и другие визуальные аспекты.

JavaScript (JS) — это интерпретируемый язык программирования, который используется для создания интерактивных и динамических веб-страниц.

Преимущества

1. Гибкость и контроль. Вы можете создать любой дизайн и функциональность, которые ограничены лишь вашей фантазией или опытом в проектировании.
2. Производительность. Оптимизированный код может обеспечить высокую скорость работы сайта.
3. Безопасность. Вы можете внедрить собственные меры безопасности и защитить сайт от уязвимостей.
4. Недостатки
5. Сложность. Требуются знания по веб-разработке и опыт в программировании.

6. Время. Создание сайта с нуля может занять много времени.
7. Поддержка. Вам придется самостоятельно поддерживать и обновлять сайт.

С помощью конструкторов сайтов. Это платформы с готовыми шаблонами проектов. Нужно выбрать подходящий дизайн, отредактировать отдельные блоки и загрузить контент. Такой метод лучше всего подходит для создания простых сайтов-одностраничников (лендингов), личных блогов, портфолио и небольших интернет-магазинов. Некоторые конструкторы: Tilda, Wix, Flexbe.

Tilda Publishing (сокр. Tilda) — блочный конструктор сайтов, не требующий навыков программирования. Позволяет создавать сайты, интернет-магазины, посадочные страницы, блоги и email-рассылки.

Wix — международный сервис-конструктор сайтов, облачная платформа. Позволяет создавать веб-сайты и их мобильные версии с помощью инструментов перетаскивания (drag-and-drop).

Преимущества

1. Простота использования. Не требуется знание веб-разработки, особенно по части бэкенда.
2. Быстрое создание. Вы можете создать сайт с базовым функционалом за несколько часов.
3. Готовые шаблоны. Большой выбор шаблонов и блоков для различных типов сайтов.
4. Недостатки
5. Малая гибкость в проектировании. Вы ограничены функциональностью конструктора.
6. Платные функции. Некоторые функции могут быть доступны только в платных подписках на сервис.
7. Слабый SEO-потенциал. Ограниченные возможности для оптимизации сайта под поисковые системы.

С помощью систем управления контентом (CMS). Это программное обеспечение, которое помогает создавать и поддерживать веб-сайты без сложных навыков программирования. С помощью CMS можно гибко настраивать сайт, добавляя нужные

функции через плагины и выбирая подходящие темы оформления. Некоторые CMS: WordPress, Joomla, OpenCart.

WordPress — это система управления контентом (CMS) для создания и управления сайтами. С её помощью можно добавлять текст, изображения, видео и другие элементы на сайт через простой редактор.

Joomla — это бесплатная система управления контентом (CMS) с открытым исходным кодом для публикации веб-контента на веб-сайтах

Преимущества

1. Гибкость. Большое количество плагинов и тем для настройки сайта.
2. Сообщество. Поддержка со стороны большого сообщества пользователей и разработчиков.
3. Масштабируемость. Возможность расширения функционала сайта по мере его развития.
4. Недостатки
5. Сложность. Может потребоваться время для освоения всех возможностей системы.
6. Безопасность. Требуется регулярное обновление и защита от уязвимостей. Однако для этого обычно есть готовые решения от поставщика CMS-решения.
7. Производительность. Некоторые готовые плагины могут замедлять работу сайта. И, возможно, придется пользоваться сторонними либо разработать собственные.

Из всех вышеперечисленных вариантов для разработки проекта был выбран способ создания сайта при помощи языков программирования.

2 ОПЫТНО – ЭКСПЕРЕМЕНТАЛЬНАЯ ЧАСТЬ

2.1 Анализ объекта автоматизации

Интерактивная тетрадь по теме «Интеграл» для студентов 1 курса всех специальностей.

Интерактивная тетрадь включает в себя несколько разделов, которые помогают пользователю поэтапно изучать теорию, решать задачи и проверять свои знания.

Основные разделы интерактивной тетради:

1. Теория - содержит краткую и понятную информацию по теме интегралов. В этом разделе даются основные определения, отличия определённых и неопределённых интегралов, а также основные правила и методы интегрирования. Материал изложен простым языком, дополнен формулами и примерами для лучшего понимания.
2. Задания - интерактивный раздел с практическими упражнениями. Задания можно выполнять прямо на сайте, а система автоматически проверяет ответы и даёт обратную связь. Это помогает лучше понять и закрепить материал.
3. Тесты - раздел для проверки знаний. Пользователь может пройти тесты по разным темам и сразу узнать результат. Это удобно для самопроверки и подготовки к контролю.
4. Видео - включает обучающие видеоролики, которые наглядно объясняют, как применять интегралы на практике. Видео помогают лучше усвоить материал тем, кто воспринимает информацию визуально.
5. Глоссарий - сборник основных терминов, встречающихся при изучении интегралов. Удобная навигация по буквам позволяет быстро находить нужные определения.

2.2 Техническое задание

Основание для разработки является задание цикловой комиссии специальности 09.02.07 на дипломный проект. Тема дипломного проекта «Разработка интерактивная тетрадь по теме “Интеграл”».

Целевая аудитория:

Для студентов 1 курса всех специальностей.

Интерактивная тетрадь может использоваться в образовательных целях в техникумах и университетах

Назначение интерактивной тетради:

Интерактивная тетрадь по теме «Интеграл» предназначена для самостоятельного и наглядного изучения основ интегрального исчисления. Она помогает пользователю последовательно изучить теоретический материал, закрепить знания с помощью заданий, проверить уровень усвоения через тесты и использовать дополнительные ресурсы, такие как видео и глоссарий.

1. Основные функции тетради:
2. Просмотр краткой и доступной теории
3. Воспроизведение обучающих видео по ключевым темам
4. Решение тестов с автоматической проверкой
5. Выполнение интерактивных практических заданий
6. Использование глоссария для быстрого поиска и уточнения терминов

Требования к разработке

В рамках проекта необходимо создать интерактивную тетрадь по теме «Интеграл», которая будет включать:

1. Главную страницу
2. Раздел «Теория» 5 лекционных материалов с краткими объяснениями, формулами и примерами
3. Раздел «Задания» не менее 5 интерактивных заданий для практики
4. Раздел «Тесты» 5 тестов, каждый минимум на 5 вопросов
5. Раздел «Видео» обучающие видеоролики
6. Раздел «Глоссарий» справочник терминов с удобной навигацией

Дополнительные требования:

1. Перед началом каждого интерактивного задания должна отображаться инструкция.
2. В лекциях ключевые термины должны быть отмечены и при нажатии автоматически вести в глоссарий сразу к нужному определению.
3. Глоссарий должен поддерживать:

1. Поиск по первой букве

Требования к внешнему виду

1. Интерфейс должен быть простым, интуитивно понятным и доступным для пользователей разного уровня подготовки
2. Дизайн сайта должен быть спокойным, неярким, чтобы не отвлекать от учебного материала
3. Все разделы должны быть связаны между собой через удобную навигацию, доступную на каждой странице

Требования к программным средствам:

Язык разметки: HTML

Язык программирования: CSS, JavaScript (JS)

Браузеры: Firefox, chrome, yandex, safari

Минимальные требования для запуска:

1. Операционная система: Windows 7, 8, 10
2. Для Linux: Ubuntu 04, Debian 6+, OpenSuSE 11.3+, Fedora Linux 14. Для компьютеров Mac нужно установить Mac OS X 10.6 или позднее.
3. Тактовая частота процессора: 800 МГц Intel Pentium 4 или аналог.
4. Объём оперативной памяти: 512 Мб.
5. Количество свободного места на диске: 16гб.
6. Версия DirectX: 1 или выше.

2.3. Моделирование информационной системы

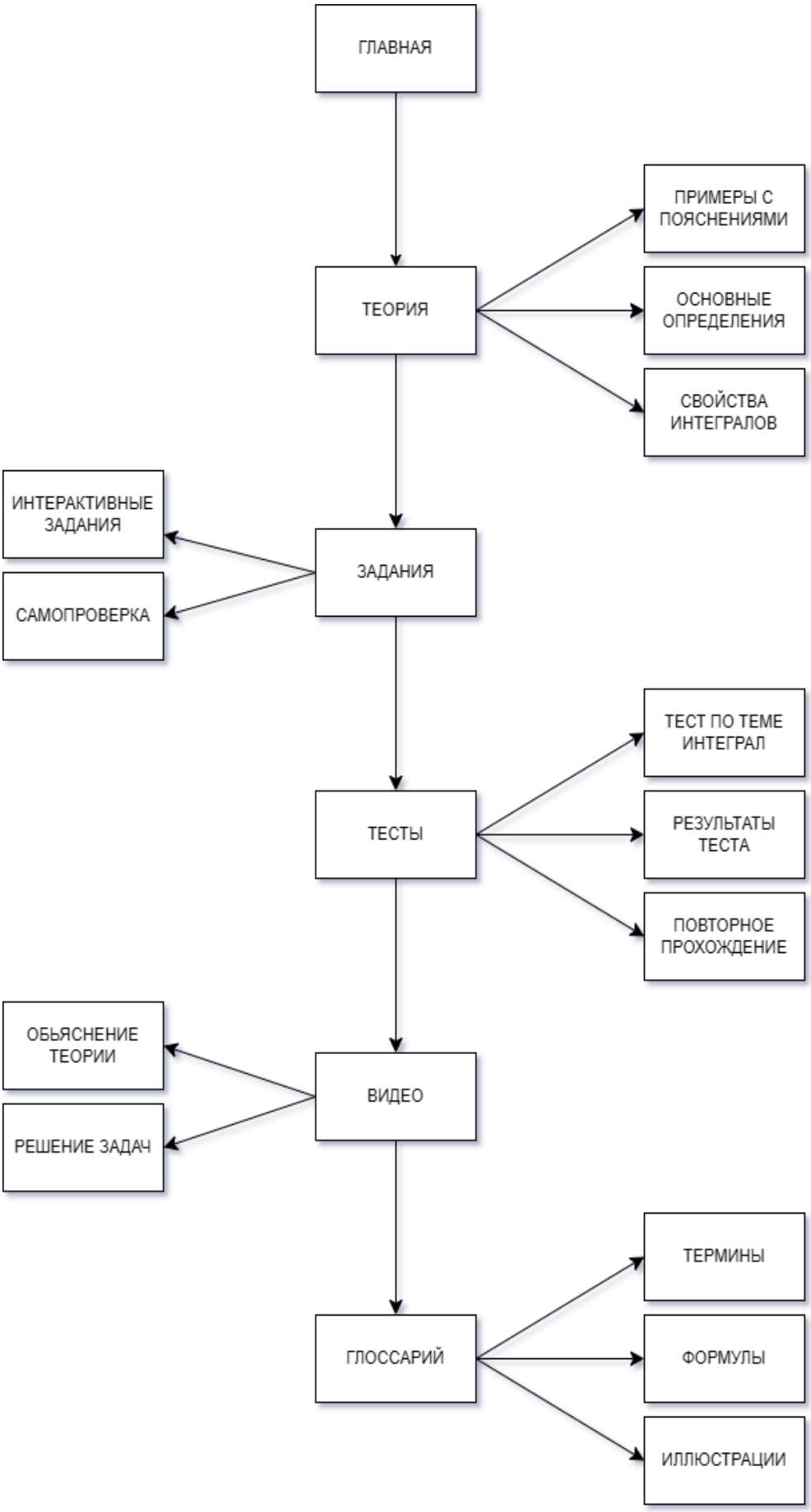

Рисунок 1 - Структурная схема

Функциональное моделирование

IDEF0 — методология функционального моделирования (англ. *function modeling*) и графическая нотация, предназначенная для формализации и описания бизнес-процессов. Отличительной особенностью IDEF0 является её акцент на соподчинённость объектов. В IDEF0 рассматриваются логические отношения между работами, а не их временная последовательность.

Диаграмма IDEF0, показаны на рисунках 2, 3, 4

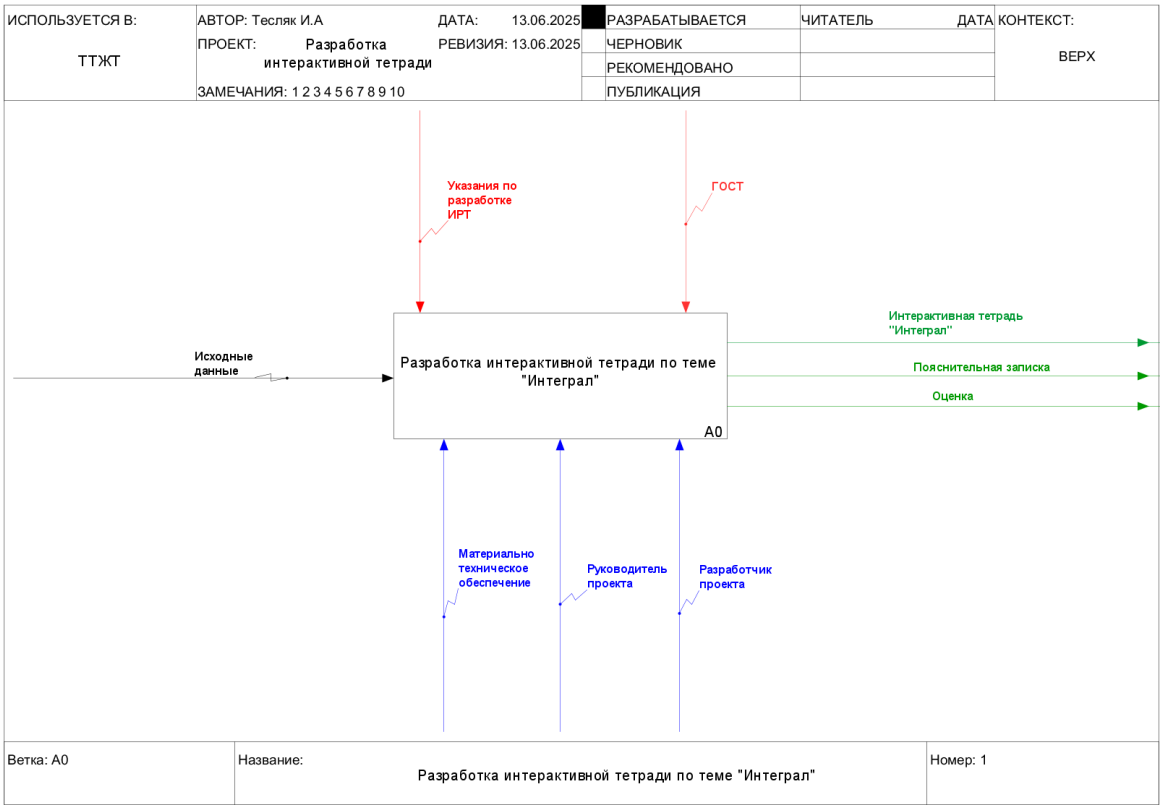

Рисунок 2 - Функциональная модель IDEF0

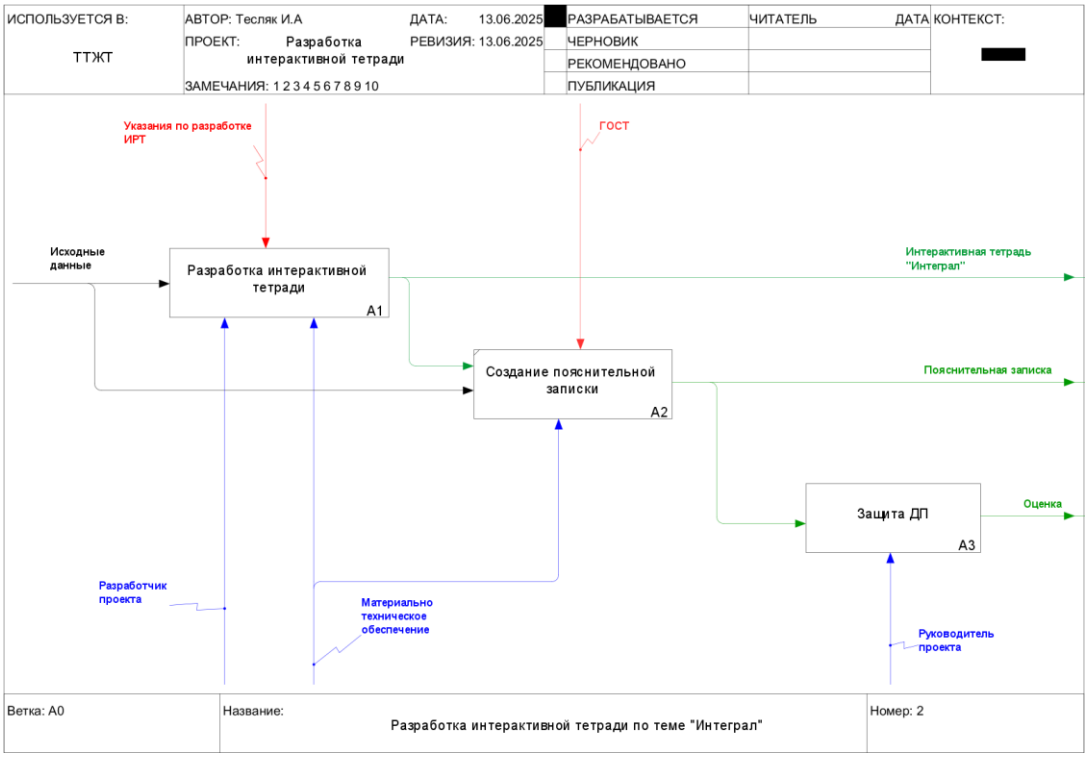

Рисунок 3 - Декомпозиция IDEF 1

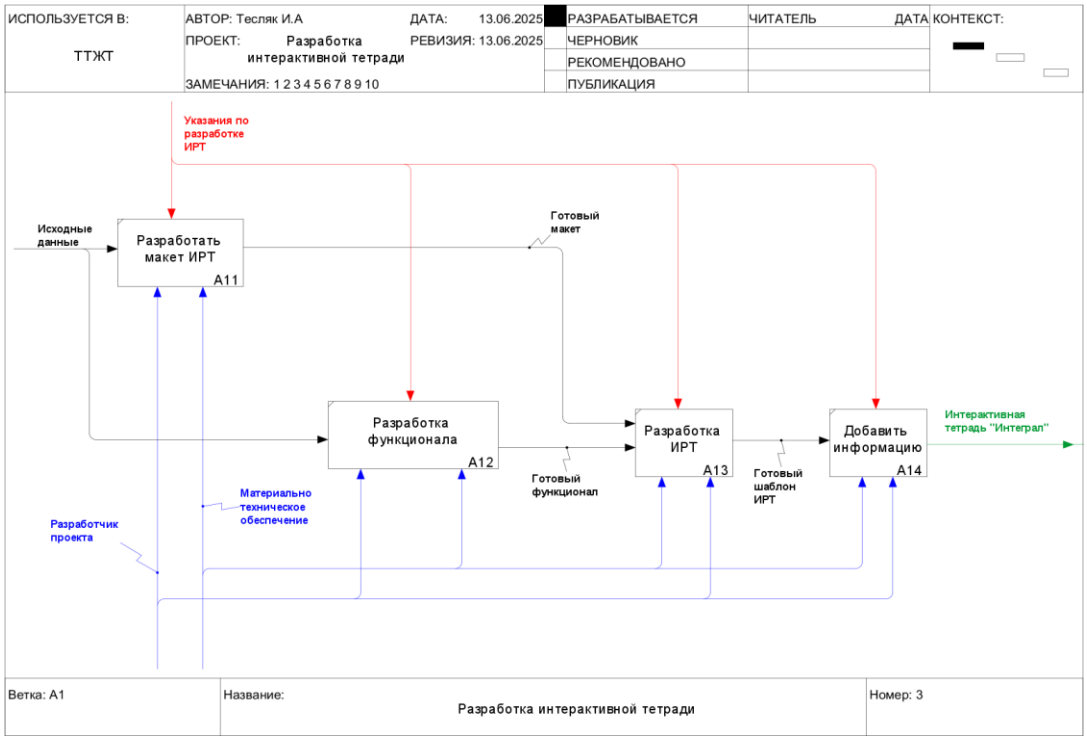

Рисунок 4 - Декомпозиция IDEF 2

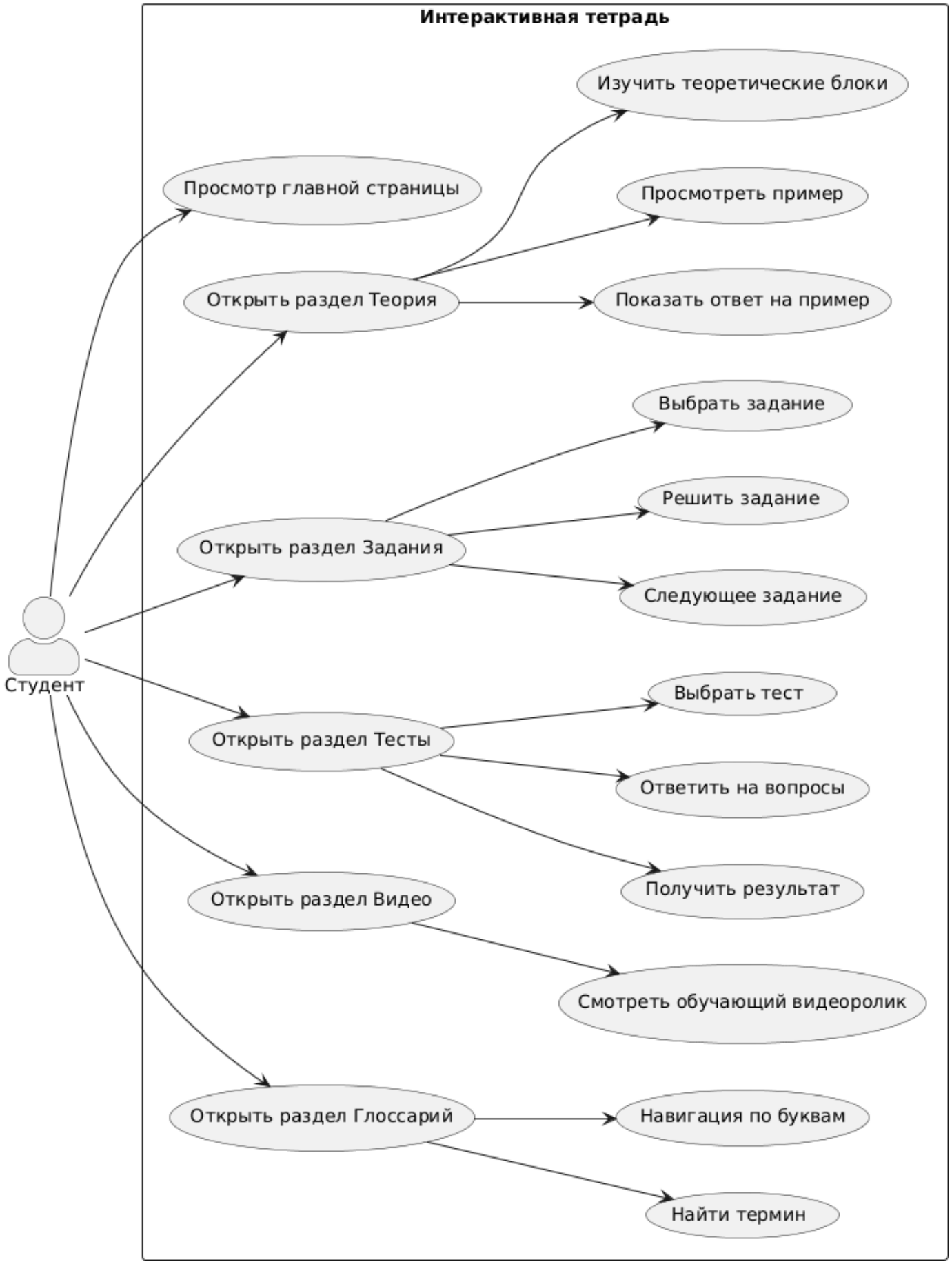

Рисунок 5 – UML диаграмма прецедентов

2.4 Выбор и обоснование выбора программного обеспечения

Visual Studio Code (VS Code) — текстовый редактор для разработчиков от компании Microsoft. Работает на Windows, macOS и Linux.

Ramus — это программа для построения визуальных диаграмм, используемых для наглядного отображения функциональных схем информационной системы и различных бизнес-процессов.

Mozilla Firefox (Firefox) — свободный браузер с открытым исходным кодом от разработчика Mozilla Corporation.

Google Chrome — веб-браузер от компании Google, обеспечивающий более удобную, быструю и безопасную работу в Интернете.

Яндекс Браузер — бесплатный веб-браузер, разработанный российской компанией «Яндекс». Используется движок Blink, основанный на проекте Chromium с открытым исходным кодом.

2.5 Реализация интерактивной тетради по теме “Интеграл”

На рисунке 5 представлена главная страница интерактивной тетради.

Интерфейс сайта состоит из: Sidebar (боковое меню) это основная навигационная панель, расположенная слева. Она содержит иконки и названия разделов: Главная, Теория, Задания, Тесты, Видео, Глоссарий и о тетради. Меню отображается на всех страницах и позволяет быстро переходить между разделами. Благодаря иконкам и подписанным названиям, пользователь легко ориентируется в структуре сайта.

Content (основная область) центральная часть страницы, где отображается соответствующий содержимому раздел. На главной странице размещён приветственный блок с изображением, кратким описанием возможностей сайта и кнопкой перехода к заданиям.

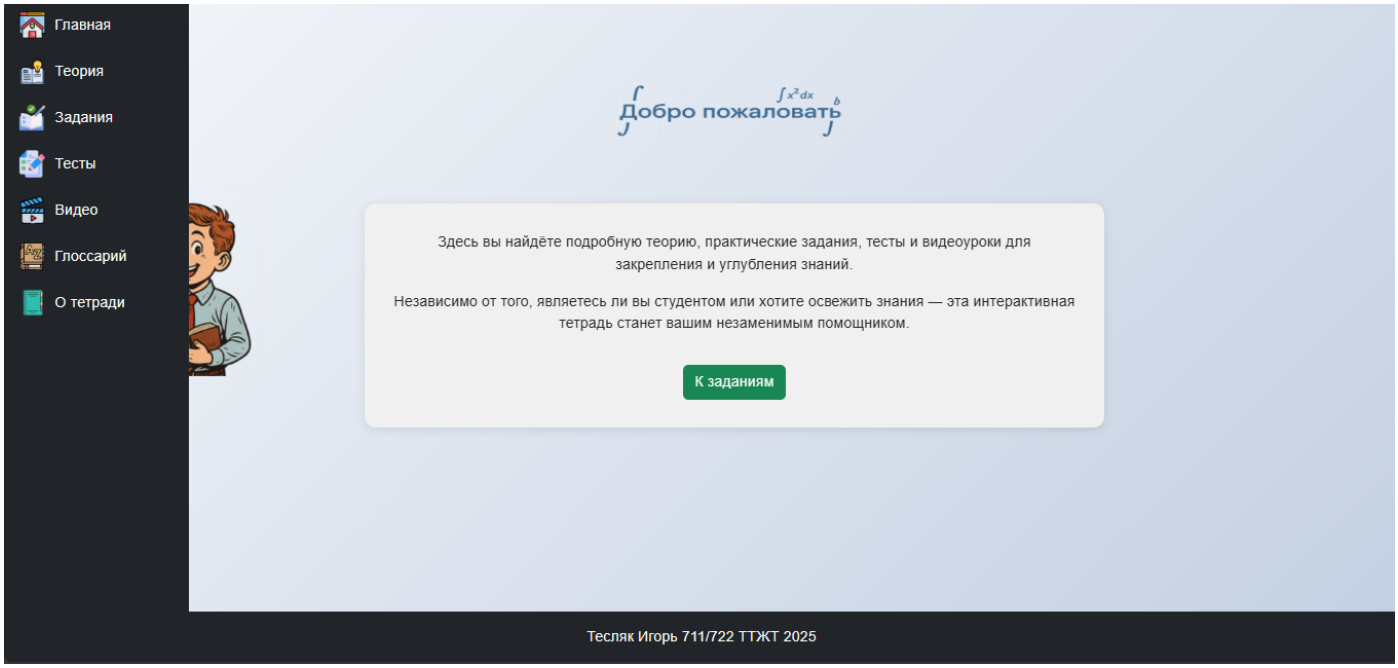

Рисунок 6 - Главная страница

Страница "Теория" предназначена для изучения учебного материала по теме «Интегралы». Визуально она состоит из основного заголовка и раскрывающихся тематических блоков (аккордеонов), каждый из которых содержит краткое описание, теоретические определения, формулы, а также примеры с возможностью просмотра решений.

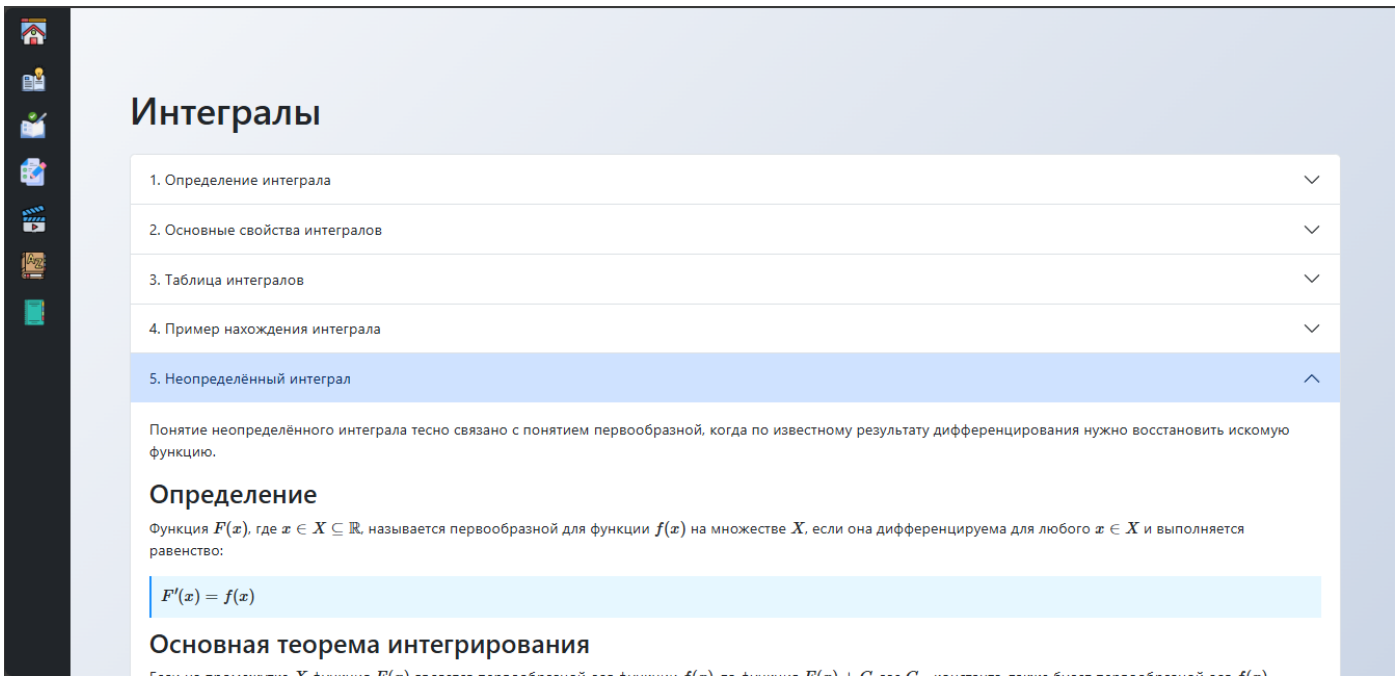

Рисунок 7 - Теория

Пользователь может раскрыть интересующую тему, чтобы ознакомиться с теоретическим материалом.

Интерактивная часть реализована через примеры с кнопкой "Ответ": при нажатии на неё отображается решение соответствующего примера. Это позволяет учащимся сначала самостоятельно попытаться решить задание, а затем свериться с правильным ответом.

Такая реализация способствует постепенному освоению материала и формирует навыки анализа, позволяя применять теоретические знания на практике.

Страница "Задания" предоставляет пользователю выбор различных вариантов заданий, которые можно выполнить для закрепления теоретических знаний.

После выбора конкретного варианта задания, открывается интерактивная форма, в которой пользователь может выполнить задание.

Кроме того, на странице имеется кнопка «Следующее задание», которая позволяет перейти к следующему заданию без необходимости возвращаться в список. Этот функционал удобен для пользователя, так как облегчает процесс перехода между заданиями, делая обучение более динамичным и непрерывным.

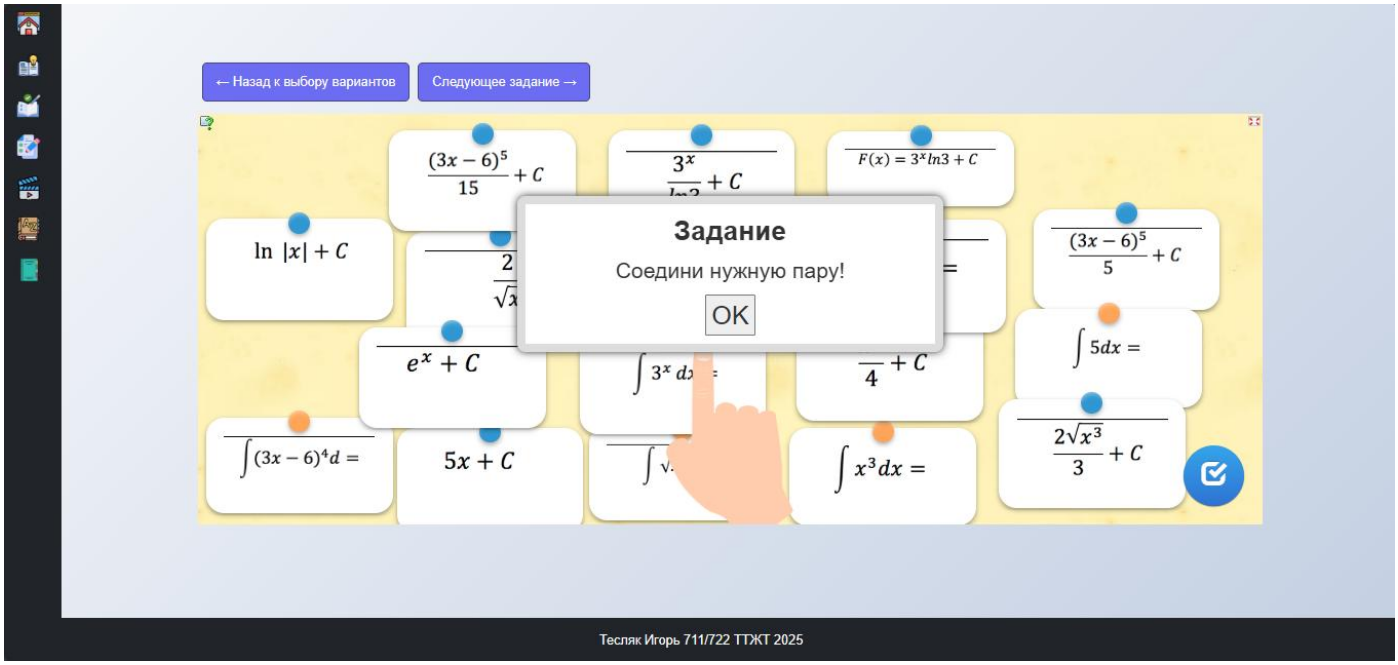

Рисунок 8 - Задания

Страница "Тесты" предназначена для проверки усвоения теоретического материала по теме «Интеграл». В начале страницы пользователю предлагается выбрать один из доступных тестов. Каждый тест представляет собой отдельный набор вопросов, направленных на оценку знаний по определённой теме.

После выбора теста открывается форма с тестовыми заданиями, которые, как правило, включают от 5 до 10 вопросов.

Пользователь последовательно отвечает на вопросы, а по завершении может получить результат прохождения теста, что позволяет оценить уровень своей подготовки и выявить темы, требующие повторения.

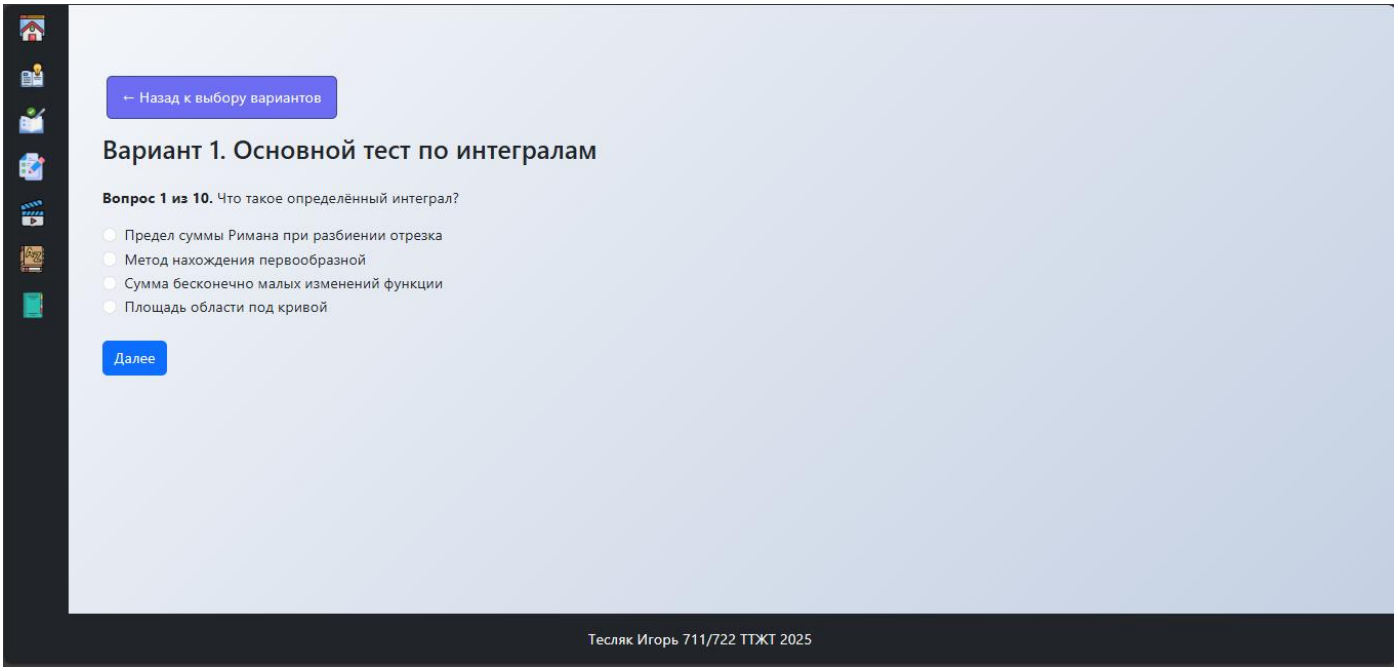

Рисунок 9 Тесты

Страница «Видео» содержит подборку обучающих видеороликов, направленных на визуальное объяснение темы интегралов.

Каждый ролик демонстрирует различные аспекты интегрирования: от базовых понятий до решений определённых и неопределённых интегралов.

Видео позволяют пользователю закрепить теоретический материал, представленный в других разделах, и лучше понять применение интегралов на практике.

Контент на данной странице помогает разнообразить формы восприятия информации, ориентируясь на учащихся, предпочитающих аудиовизуальный формат обучения.

Все видеоматериалы упорядочены по темам и доступны для просмотра прямо на сайте без перехода на сторонние ресурсы.

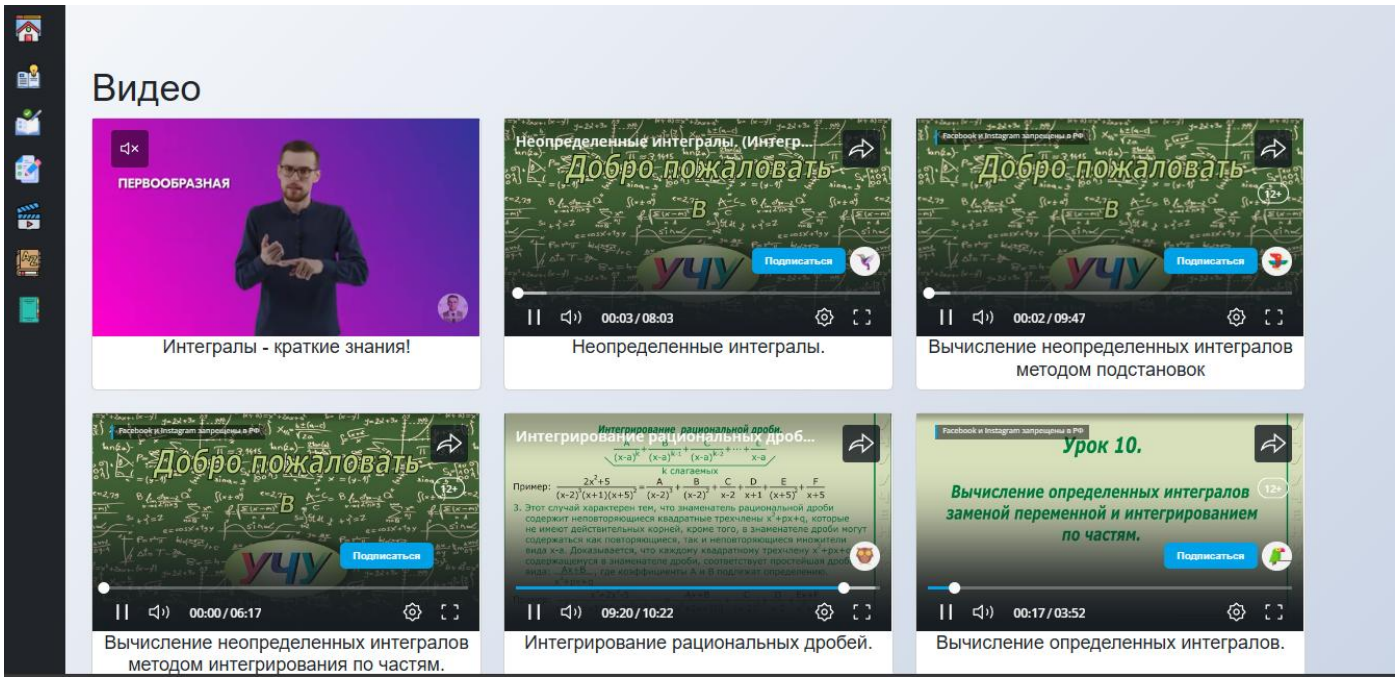

Рисунок 10 - Видео

Страница «Глоссарий» содержит полный перечень ключевых терминов и определений, необходимых для понимания темы интегралов.

Здесь пользователь может быстро найти объяснение любых специальных понятий и математических терминов, встречающихся в других разделах сайта.

Для удобства поиска все термины упорядочены по алфавиту и снабжены навигацией по буквам, что позволяет моментально перейти к нужному разделу.

Такой подход упрощает изучение материала и помогает закрепить знания, расширяя словарный запас пользователя.

Данная страница предназначена для тех, кто хочет быстро освежить значение терминов или разобраться в непонятных понятиях без необходимости искать информацию вне сайта.

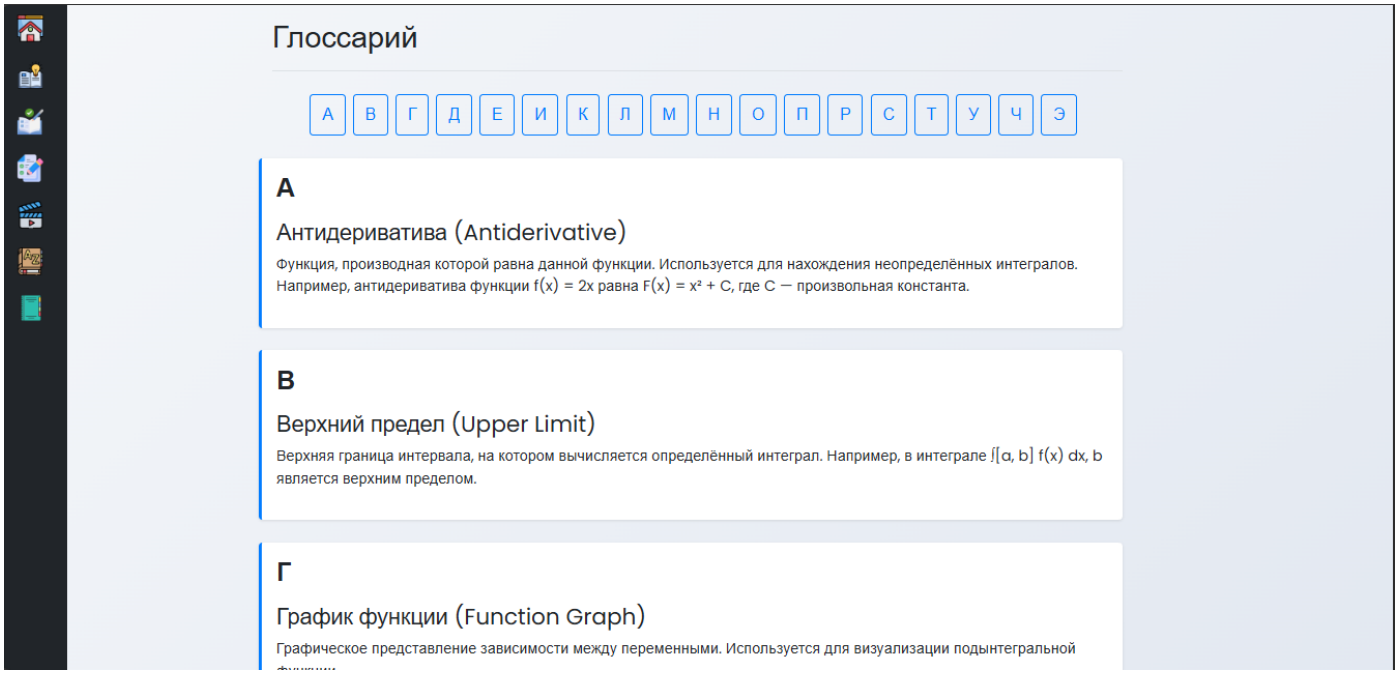

Рисунок 11 - Глоссарий

2.6 Информационная безопасность

Информационная безопасность направлена на обеспечение соблюдения законодательства и требований регуляторов, защиту репутации компании и обеспечение непрерывности бизнес-процессов.

Кибербезопасность охватывает только цифровые данные и интернет-угрозы. Также кибербезопасность включает защиту необработанных, несекретных данных, а информационная безопасность.

Основная цель ИБ — обеспечить защиту от любого несанкционированного доступа, утечек и изменения данных. Это достигается применением различных технических, программных, аппаратных и организационных мер, призванных предупреждать, а также своевременно обнаруживать и реагировать на кибератаки.

Принципы информационная безопасность - информационная безопасность строиться из трех основных принципов. Они являются основой для созданий защитных систем:

Конфиденциальность - этот принцип направлен на обеспечение защиты тайны информации от несанкционированного доступа. Конфиденциальная информация должна быть доступна только лицам, которым она необходима для выполнения своих обязанностей, и не должна быть открыта для посторонних.

Целостность - принцип целостности информации направлен на обеспечение защиты от изменений или утраты. Это означает, что данные должны быть защищены от любых видов несанкционированных изменений: внесения ошибочных данных, умышленного искажения и т. д.

Доступность - принцип доступности информации предполагает обеспечение доступа для авторизованных пользователей. Информация должна быть доступна для использования и обработки в нужном объеме и в то время, когда это необходимо.

Источники угроз информационной безопасности:

Несовершенное ПО или аппаратное обеспечение. Устаревшие версии ПО или не обновляемая «прошивка» аппаратной части нередко содержат уязвимости, которые злоумышленники могут использовать для атак.

Неправильное функционирование систем. Ошибочная конфигурация или неполное обновление системы также приводят к возникновению уязвимостей.

Уязвимости в протоколах. Создать возможности для атак может некорректная реализация протоколов связи или интерфейсов, связывающих компоненты системы.

Сложные или несовершенные условия эксплуатации. Сюда отнесем в том числе нестандартные сценарии использования ПО и оборудования, а также недостаточное тестирование.

Человеческий фактор. Это ошибки персонала и недостаточное знание правил безопасности, а также фишинг и другие приемы социальной инженерии.

Инструменты для защиты информации

Физические. Это инструменты, которые существуют в физическом мире. К ним обычно относится различное оборудование.

Технические и программные**.** Это то, что относится скорее к софту, а не к железу, от защищенных протоколов до антивируса.

Административные. Сюда относится построение внутренней инфраструктуры, регламенты и контроль доступа.

Программные средства — это, прежде всего, ПО, которое обеспечивает защиту информации. Сюда относятся антивирусы, антишпионский софт, системы управления доступом, мониторинга безопасности и шифрования данных.

Организационные средства - меры, которые принимает руководство компании. Например, разработка политики корпоративной безопасности и контроль за её соблюдением, обучение сотрудников и подписание NDA при приёме на работу.

Антивирусное ПО - программное обеспечение помогающие обнаруживать и удалять вредоносное ПО с компьютеров и сетей. Регулярное обновление антивирусных баз данных и проведение сканирований — важные меры для поддержания безопасности. Важно понимать, что антивирусное ПО не является панацеей и должно использоваться в сочетании с другими методами защиты.

Технические средства — брандмауэры, системы обнаружения вторжений, защиты от DDoS-атак, аутентификации пользователей, системы шифрования данных и другие инструменты.

Аппаратные средства — это физическое оборудование. Сюда входят серверы, маршрутизаторы, коммутаторы, устройства хранения и т. д. Из конкретных средств обеспечения безопасности информационных систем все знают про антивирусы, межсетевые экраны, VPN и прокси-серверы, сканеры уязвимостей. Менее известны, но более эффективны комплексные решения обеспечения безопасности информационной среды.

Вот некоторые из них:

1. IPS/IDS — программно-аппаратные комплексы обнаружения вторжений;
2. DLP — ряд технологий для предотвращения утечек данных;
3. SIEM — решение для превентивных «ударов» по уязвимостям, когда они обнаруживаются раньше, чем могут быть использованы;
4. DevSecOps — практики комплексной защиты программных продуктов в течение всего периода разработки;
5. EDR — комплексные решения для обнаружения подозрительной активности на конечных точках корпоративных сетей (компьютерах или мобильных устройствах сотрудников).
6. CASB — промежуточная защита между пользователями и облачными хранилищами и сервисами.

Фишинг — это метод социальной инженерии, при котором злоумышленники пытаются обманом заставить пользователей раскрыть конфиденциальную

информацию, такую как пароли или номера кредитных карт. Обычно это происходит через поддельные электронные письма или веб-сайты. Фишинг-атаки могут быть очень убедительными и трудно различимыми от легитимных сообщений.

Криптография — технология преобразования данных, с помощью которой они становятся зашифрованными с помощью специальных ключей или методов. Криптографические методы используют, например, государственные учреждения для создания цифровых подписей, банки — для денежных переводов, пользователи — когда заходят в интернет с подключенным VPN.

Блокчейн — технология децентрализованного хранения данных. Данные разделяются на блоки (на англ. block), каждый из блоков связан с предыдущим, тем самым выстраивая цепочку (на англ. chain). Изменения данных в предыдущих блоках является ресурсоёмким процессом и в большинстве случаев невозможным. Поэтому всё, что попадает в сеть блокчейна, остается в неизменном состоянии навсегда. Этот способ используют, например, в здравоохранении — организации хранят в блокчейне медицинские карты пациентов.

Брандмауэр — это система безопасности, которая контролирует и фильтрует входящий и исходящий трафик в сети. Брандмауэры помогают предотвратить несанкционированный доступ к сетям и защищают от различных видов атак. Важно понимать, что брандмауэры могут быть как аппаратными, так и программными, и их настройка требует определенных знаний и навыков.

Аутентификация — это процесс проверки подлинности пользователя или устройства. Наиболее распространенные методы аутентификации включают в себя пароли, биометрические данные (например, отпечатки пальцев) и двухфакторную аутентификацию (2FA). Аутентификация является ключевым элементом кибербезопасности, так как она помогает предотвратить несанкционированный доступ к системам и данным.

Двухфакторная аутентификация (2FA) - добавляет дополнительный уровень защиты, требуя не только пароль, но и второй фактор, такой как код, отправленный на мобильный телефон. Это значительно усложняет несанкционированный доступ к учетным записям. Важно понимать, что двухфакторная аутентификация является

ключевым элементом кибербезопасности и должна использоваться для защиты важных учетных записей.

Идентификация — это процесс установления уникального имени (идентификатора), связанного с конкретным пользователем, устройством или ресурсом.

Идентификация бывает:

1. Первичная — проводится при регистрации нового пользователя в системе. Успешная первичная идентификация завершается регистрацией, то есть присвоением уникального идентификатора.
2. Вторичная — осуществляется при каждом запросе пользователя на доступ. Система проверяет предъявленный идентификатор по списку зарегистрированных.

DDoS (Distributed Denial of Service) атаки направлены на перегрузку серверов или сетей, делая их недоступными для пользователей. Это достигается за счет отправки большого количества запросов с множества зараженных устройств. Важно понимать, что DDoS-атаки могут нанести значительный ущерб, включая потерю доходов, нарушение работы систем и утрату доверия клиентов.

Трояны — это вредоносные программы, которые маскируются под легитимное ПО. Они могут предоставлять злоумышленникам удаленный доступ к зараженному компьютеру или использоваться для кражи данных. Важно понимать, что трояны могут быть скрытыми и незаметными, что делает их обнаружение и удаление сложной задачей.

Ransomware — это тип вредоносного ПО, который шифрует данные на компьютере жертвы и требует выкуп за их расшифровку. Ransomware-атаки могут нанести серьезный ущерб как частным лицам, так и организациям. Важно понимать, что ransomware может быть скрытым и незаметным, что делает его обнаружение и удаление сложной задачей.

IDS-системы (сокр. от Intrusion Detection System) — технология для обнаружения вторжений. IDS отслеживает сетевой трафик или трафик внутри корпоративной системы и выявляет необычную активность, которая указывает на возможное нарушение безопасности. Например, попытки взлома сети или атаки на серверы. IDS-

систему можно установить на уровне сети или на уровне отдельного устройства. В первом случае система будет анализировать весь трафик, во втором — только тот, что проходит через устройство.

IPS-системы (сокр. от Intrusion Prevention System) — технология для предотвращения вторжений. В отличие от IDS, не только фиксирует потенциальные угрозы безопасности, но и принимает активные меры для защиты информации. Например, автоматически блокирует IP-адреса, с которых пытаются взломать систему. При этом IPS обнаруживает не только внешние атаки, но и внутренние — когда атака идёт с рабочего компьютера кого-то из сотрудников. Ещё IPS-система может сканировать скачиваемые файлы и не допускать установки вирусов на компьютеры пользователей.

DLP-системы (сокр. от Data Loss Prevention) — технология, которая предотвращает утечку информации. Например, блокирует отправку конфиденциальных данных по электронной почте или через мессенджеры. С помощью системы можно также запретить распечатку документов с определённого устройства. Эту функцию можно активировать в случае увольнения сотрудника, чтобы он не смог забрать с собой корпоративную информацию ни в цифровом, ни в печатном виде.

EDR-системы (сокр. от Endpoint Detection and Response) — технология для обнаружения вредоносной активности на конечных узлах сети, например компьютерах или смартфонах. EDR отслеживает подозрительные действия пользователей или попытки взлома устройств и отправляет уведомления о них ИБ-специалисту. По сути, системы типа EDR — это более современные виды антивирусных программ. Они в режиме реального времени выявляют сложные угрозы, например вредоносное ПО для корпоративного шпионажа. EDR-система анализирует активность устройства и выявляет отклонения от обычного паттерна.

UBA-аналитика (сокр. от User Behavior Analytics) — технология, которая анализирует поведение пользователей в информационных системах и сетях, чтобы отслеживать подозрительную активность. Например, UBA может выявить несанкционированный доступ к учётной записи пользователя, проанализировав отклонения в его поведении. Это может быть вход в систему из другой страны или просмотр файлов, которые обычно не нужны пользователю для работы. Обнаружив

отклонения, система UBA может заблокировать скомпрометированную учётную запись.

Риски информационной безопасности

В современных условиях количество угроз информационной безопасности неуклонно растёт. Развитие технологий, в том числе облачных решений, Интернета вещей (IoT), искусственного интеллекта и удалённых рабочих мест, приводит к расширению «поверхности атаки». Это означает, что злоумышленники получают всё больше потенциальных точек входа в системы, что требует комплексного подхода к управлению рисками. Оценка рисков становится обязательной практикой: выявляются наиболее ценные ресурсы, возможные уязвимости, потенциальные последствия утечек и составляются планы реагирования.

Политика информационной безопасности

Одним из важнейших организационных инструментов является разработка политики информационной безопасности. Она представляет собой свод правил и норм, регламентирующих поведение сотрудников, использование технических ресурсов и порядок реагирования на инциденты. Политика должна быть понятной, доступной для изучения и регулярно актуализироваться в связи с изменением законодательства и появлением новых угроз.

Аудит и мониторинг

Контроль за состоянием информационной безопасности осуществляется с помощью регулярного аудита и постоянного мониторинга систем. Аудит может быть как внутренним, так и внешним, и включает проверку соответствия требованиям безопасности, наличие уязвимостей, анализ журналов событий и эффективность мер защиты. Мониторинг позволяет своевременно выявлять аномалии в работе систем, попытки несанкционированного доступа или утечки данных.

Социальная инженерия

Одной из самых опасных форм атак остаются методы социальной инженерии. Злоумышленники не только используют технические средства, но и активно воздействуют на человеческий фактор. Это может быть звонок от «службы поддержки», письмо с просьбой срочно подтвердить логин и пароль или сообщение от «коллеги» с вложением. Такие методы часто оказываются более эффективными, чем

сложные вирусные атаки, поэтому особое внимание должно уделяться повышению осведомлённости персонала.

Облачные технологии и безопасность

Использование облачных решений позволяет компаниям масштабировать бизнес и сокращать издержки, однако требует пересмотра подходов к безопасности. Ответственность за защиту данных часто делится между поставщиком облака и клиентом. Это требует точного понимания зон ответственности, настройки уровней доступа, шифрования данных в облаке и резервного копирования.

Резервное копирование (бэкап)

Надёжная система резервного копирования — неотъемлемый элемент обеспечения доступности и целостности информации. Бэкапы позволяют восстановить данные в случае сбоев, атак вымогателей (ransomware), человеческих ошибок или стихийных бедствий. Современные стратегии бэкапа включают использование облачных хранилищ, создание резервных копий в режиме реального времени и регулярное тестирование восстановления данных.

Законодательство в области ИБ

Вопросы информационной безопасности регулируются как национальными, так и международными нормативными актами. В России, например, важнейшими являются ФЗ «О персональных данных», ФЗ «О защите информации», а также требования ФСТЭК и ФСБ. Международные стандарты, такие как ISO/IEC 27001, GDPR и NIST, также играют ключевую роль в формировании политики защиты информации в глобальных компаниях.

3 ВОПРОСЫ ОХРАНЫ ТРУДА И ТЕХНИКИ БЕЗОПАСНОСТИ

Вот основные документы по охране труда, которые могут понадобиться IT-компании:

1. Политика в области охраны труда – документ, в котором изложены основные принципы и цели охраны труда в компании.
2. Система управления ОТ.
3. Решение о создании службы ОТ.
4. Приказы о назначении ответственных за обеспечение безопасных условий труда и охраны труда в организации.
5. Программа производственного контроля за соблюдением санитарных правил и выполнением санитарно-эпидемиологических мероприятий.
6. План мероприятий по обеспечению охраны труда — меры, которые будут предприняты для обеспечения безопасных условий труда
7. Отчет о проведении специальной оценки условий труда.
8. Оценка профессиональных рисков с целью анализа потенциальных рисков, связанных с трудовой деятельностью сотрудников.
9. Производственный контроль — проведение систематических комиссионных проверок состояния ОТ.
10. Документы по обучению (заключение договора на обучение работников или проведение обучения своими силами): программы обучения, приказы о создании комиссии, тесты по программам, протоколы, а также регистрация работников в реестре обученных лиц.
11. Инструктажи и стажировка работников. Инструкции по охране труда для работников, журналы регистрации проведения инструктажей, программы стажировок.
12. Инструкции по использованию оборудования – правила безопасной работы с техникой, которая используется в компании.
13. В случае если в IT компании штатным расписанием предусмотрены штатные единицы для выполнения работ:

14. требующих проведение медицинских осмотров (при наличии вредных факторов или видов работ согласно Приказу Минздрава России от 28.01.2021 № 29 н);
15. требующих выдачу СИЗ и СиОС (уборщики и пр.): обеспечение работников средствами индивидуальной защиты (СИЗ) и смывающие и (или) обезвреживающие средства (СиОС).
16. Документы по учету несчастных случаев и микротравм

Инструкции по охране труда необходимо разрабатывать исходя из должности работника или профессии, направления трудовой деятельности или вида выполняемой работы (приказ Минтруда России от 29.10.2021 № 772н «Об утверждении основных требований к порядку разработки и содержанию правил и инструкций по охране труда, разрабатываемых работодателем»).

Инструкция по охране труда должна содержать:

1. общие требования;
2. требования ОТ перед началом работы;
3. требования ОТ во время работы;
4. требования в аварийных ситуациях;
5. требования охраны труда по окончании работы.

Со всеми вновь принятыми сотрудниками специалистом по охране труда в компании или ответственным лицом, прошедшим обучение по соответствующим программам в лицензированном центре, проводится по общей программе вводные инструктажи по охране труда.

Далее сотрудников инструктируют непосредственно на рабочем месте. Инструктажи по охране труда в компании позволяют подготовить программистов к правилам безопасности:

1. подготовки рабочего места до начала работы;
2. во время работы;
3. после окончания работы;
4. в аварийной ситуации.

Для обеспечения безопасности и снижения рисков травматизма, ухудшения здоровья и развития профзаболеваний, в период выполнения своих трудовых

обязательств удаленно, дистанционных работников также необходимо ознакомить с требованиями охраны труда при использовании оборудования

С целью выявления факторов, оказывающих вредное воздействие и представляющих опасность, принимаются меры по созданию безопасных условий труда для IT-специалистов на основании специальной оценки рабочих мест.

Основные аспекты специальной оценки:

1. Кабинет, где работает программист, должен соответствовать санитарно-гигиеническим нормам, иметь естественное и искусственное освещение, и возможность нормализации микроклимата (подразумевается подача свежего воздуха).
2. Перед началом работы необходимо проверить правильность подключения оборудования в электросеть, расположение и угол наклона монитора.
3. Чтобы исключить длительное напряжение тела в неудобных позах, снижение уровня вредного для зрения воздействия электромагнитного поля – проводят регулировку элементов компьютера, стула, стола, правильно проектируют освещение.
4. Так как в процессе деятельности IT специалист анализирует и перерабатывает огромное количество информации, разрабатывает программные продукты, чтобы снизить риски умственного перенапряжения, важно соблюдать режим работы. Через каждые 1,5 ч помещение проветривается, делается перерыв 10-15 мин, что позволит снять напряжения мышц, глаз.

Требования к работающим с компьютерами

К выполнению работ с компьютерами допускаются работающие, прошедшие:

– медосмотр;

– инструктаж по охране труда.

Направлять работающих при наблюдении ими за экранами ВДТ на медицинский осмотр необходимо согласно подп. 5.6.3 п. 5 приложения 1 «Факторы производственной среды, показателей, тяжести и напряженности трудового процесса, при работе с которыми обязательны предварительные, периодические и внеочередные медосмотры» к Инструкции № 47:

Во время работы на айти-специалиста могут подвергаться воздействию таких опасностей и рисков, как например:

1. перенапряжение зрительного анализатора при работе за экраном дисплея;
2. недостаточная освещенность рабочего места;
3. длительное статическое напряжение мышц спины, шеи, рук и ног, что может привести к статическим перегрузкам программиста;
4. повышенный уровень шума;
5. повышенный уровень ионизирующего излучения;
6. статическое электричество;
7. электрический ток, путь которого в случае замыкания на корпус может пройти через тело человека;
8. нарушение эргономических норм при работе с компьютером;
9. запыленность и загазованность воздуха;
10. риск возникновения пожара;

Требования к компьютерам

Конструкция компьютера, дизайн и совокупность эргономических параметров должны обеспечивать надежное и комфортное считывание отображаемой информации в условиях эксплуатации:

1. конструкция компьютера должна обеспечивать возможность поворота корпуса в горизонтальной и вертикальной плоскостях с фиксацией в заданном положении для обеспечения фронтального наблюдения экрана;
2. дизайн компьютера должен предусматривать окраску корпуса в спокойные мягкие тона с диффузным рассеиванием света, т.е. рассеиванием света во всевозможных направлениях;
3. корпус компьютера должен иметь матовую поверхность с коэффициентом отражения (0,4–0,6) и не иметь блестящих деталей, способных создавать блики;
4. конструкция компьютера должна предусматривать регулирование яркости и контрастности.

Организация и оборудование рабочих мест пользователей компьютеров

При размещении рабочих мест с компьютерами расстояние между рабочими столами с видеомониторами (в направлении тыла поверхности одного видеомонитора

и экрана другого видеомонитора) должно быть не менее 2,0 м, а расстояние между боковыми поверхностями видеомониторов – не менее 1,2 м.

Рабочие места с компьютерами в помещениях с источниками вредных производственных факторов должны размещаться в изолированных кабинах с организованным воздухообменом.

Рабочие места с компьютерами при выполнении творческой работы, требующей значительного умственного напряжения или высокой концентрации внимания, рекомендуется изолировать друг от друга перегородками высотой 1,5–2,0 м.

Экран видеомонитора должен находиться на расстоянии 600–700 мм от глаз пользователя, но не ближе 500 мм с учетом размеров алфавитно-цифровых знаков и символов.

Конструкция рабочего стола должна обеспечивать оптимальное размещение на рабочей поверхности используемого оборудования с учетом его количества и конструктивных особенностей, характера выполняемой работы. При этом допускается использование рабочих столов различных конструкций, отвечающих современным требованиям эргономики.

Высота рабочей поверхности стола должна регулироваться в пределах 680–800 мм. При отсутствии такой возможности высота рабочей поверхности стола должна составлять 725 мм.

Рабочий стол должен иметь пространство для ног высотой не менее 600 мм, шириной – не менее 500 мм, глубиной на уровне колен – не менее 450 мм и на уровне вытянутых ног – не менее 650 мм.

Конструкция рабочего стула (кресла) должна обеспечивать поддержание рациональной рабочей позы при работе на компьютере, позволять изменять позу с целью снижения статического напряжения мышц шейно-плечевой области и спины для предупреждения развития утомления. Тип рабочего стула (кресла) следует выбирать с учетом роста пользователя, характера и продолжительности работы с компьютером.

Рабочий стул (кресло) должен быть подъемно-поворотным, регулируемым по высоте и углам наклона сиденья и спинки, а также расстоянию спинки от переднего края сиденья, при этом регулировка каждого параметра должна быть независимой, легко осуществляемой и иметь надежную фиксацию.

Поверхность сиденья, спинки и других элементов рабочего стула (кресла) должна быть полумягкой, с нескользящим, слабо электризующимся и воздухопроницаемым покрытием, обеспечивающим легкую очистку от загрязнений.

Конструкция рабочего стула (кресла) должна обеспечивать:

– ширину и глубину поверхности сиденья не менее 400 мм;

– поверхность сиденья с закругленным передним краем;

– регулировку высоты поверхности сиденья в пределах 400–550 мм и угла наклона вперед до 15° и назад до 5°;

– высоту опорной поверхности спинки 300±20 мм, ширину не менее 380 мм и радиус кривизны горизонтальной плоскости – 400 мм;

– угол наклона спинки в вертикальной плоскости в пределах 0±30°;

– регулировку расстояния спинки от переднего края сиденья в пределах 260–400 мм;

– стационарные или съемные подлокотники длиной не менее 250 мм и шириной – 50–70 мм;

– регулировку подлокотников по высоте над сиденьем в пределах 230±30 мм и внутреннего расстояния между подлокотниками в пределах 350–500 мм.

Рабочее место пользователя компьютера следует оборудовать подставкой для ног, имеющей ширину не менее 300 мм, глубину не менее 400 мм, регулировку по высоте в пределах до 150 мм и по углу наклона опорной поверхности подставки до 20°. Поверхность подставки должна быть рифленой и иметь по переднему краю бортик высотой 10 мм.

Клавиатуру следует располагать на поверхности стола на расстоянии 100–300 мм от края, обращенного к пользователю, или на специальной, регулируемой по высоте рабочей поверхности, отделенной от основной столешницы.

Поверхности периферийных устройств (клавиатура, манипулятор «мышь», принтер, сканер и др.) необходимо протирать мягкой ветошью с применением специальных или бытовых чистящих средств, не содержащих кислот и отбеливателей, не реже 1 раза в неделю, а при необходимости и чаще

ЗАКЛЮЧЕНИЕ

В ходе выполнения дипломной работы была разработана интерактивная тетрадь по теме «Интеграл», включающая основные разделы: теория, задания, тесты, видео и глоссарий.

Работа над дипломом проводилась поэтапно:

1. сначала был собран и проанализирован теоретический материал по теме интегралов из учебников, сборников и электронных источников;
2. затем выполнен анализ объекта автоматизации и целевой аудитории;
3. составлено техническое задание, определяющее функциональные требования к интерактивной тетради;
4. проведено моделирование информационной системы, в том числе построены структурные и функциональные схемы, а также диаграммы прецедентов;
5. выполнен обоснованный выбор программных средств, таких как HTML, CSS, JavaScript, редактор Visual Studio Code и браузеры для тестирования;
6. осуществлена реализация интерактивной тетради, в том числе создание всех разделов и интерфейса с учётом требований к дизайну и навигации;
7. проведено тестирование функциональности и взаимодействия с пользователем;
8. рассмотрены вопросы информационной безопасности и охраны труда при работе с ИТ-средствами.

Разработанная интерактивная тетрадь может использоваться как дополнительный образовательный инструмент в учебном процессе техникумов и вузов, способствуя эффективному изучению темы «Интеграл».

СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ

Основные источники по интегралам

Задорожный В. Н., Зальмеж В. Ф., Трифонов А. Ю., Шаповалов А. В. *Высшая математика для технических университетов. Ч. III. Интегральное исчисление* / Задорожный В. Н. и др. [Электронный ресурс] // Сайт Научной библиотеки ТПУ: [tpu.ru]. — URL: https://www.lib.tpu.ru (дата обращения: 18.05.2025).

Баландюк А. В., Преображенский С. П. *Учебное пособие по интегралам* / Баландюк А. В., Преображенский С. П. [Электронный ресурс] // Электронная библиотека СПбПУ: [elib.spbstu.ru]. — URL: https://elib.spbstu.ru (дата обращения: 20.05.2025).

Градштейн И. С., Рыжик И. М. *Таблицы интегралов, сумм, рядов и произведений* / Градштейн И. С., Рыжик И. М. — М.: Физматлит, 2003. — 1120 с. — ISBN 5-9221-0331-8.

Дополнительные источники по интегралам

Комиссарова Н. В., Мартынов Г. П. *Сборник задач «Интеграл» для студентов 1–2 курсов* / Комиссарова Н. В., Мартынов Г. П. [Электронный ресурс] // Informio: [informio.ru]. — URL: https://www.informio.ru/Sbornik_zadach_Integral_Informio.pdf (дата обращения: 22.05.2025).

Туганбаев А. А. *Математический анализ: интегралы: учебное пособие* / Туганбаев А. А. [Электронный ресурс] // ЭБС «БиблиоКлаб»: [biblioclub.ru]. — URL: https://biblioclub.ru/index.php?id=103835 (дата обращения: 15.05.2025).

Первообразная и интеграл: рабочая тетрадь [Электронный ресурс] // Инфоурок: [infourok.ru]. — URL: https://infourok.ru/material.html?mid=119635 (дата обращения: 18.05.2025).

Источники по веб-дизайну и программированию web-приложений

Фролов А. Б., Нагаева И. А., Кузнецов И. А. *Основы web-дизайна. Разработка, создание и сопровождение web-сайтов: учебное пособие для СПО* / Фролов А. Б. и др. [Электронный ресурс] // Профобразование: [profspo.ru]. — URL: https://profspo.ru/books/96765 (дата обращения: 22.05.2025).

Полуэктова Н. Р. *Разработка веб-приложений: учебное пособие для СПО* / Полуэктова Н. Р. [Электронный ресурс] // Издательство Юрайт: [urait.ru]. — URL: https://urait.ru/book/razrabotka-veb-prilozheniy-545237 (дата обращения: 25.05.2025).

Тузовский А. Ф. *Проектирование и разработка web-приложений: учебное пособие для СПО* / Тузовский А. Ф. [Электронный ресурс] // ЛитРес: [litres.ru]. — URL: https://www.litres.ru/book/anatoliy-tuzovskiy/proektirovanie-i-razrabotka-web-prilozheniy-uchebnoe-po-39149186/ (дата обращения: 20.05.2025).

Диков А. *Web-программирование на JavaScript: учебное пособие для СПО* / Диков А. [Электронный ресурс] // Лабиринт: [labirint.ru]. — URL: https://www.labirint.ru/books/786072/ (дата обращения: 22.05.2025).

Заяц А. М., Васильев Н. *Проектирование и разработка web-приложений на JavaScript и Node.js: учебное пособие для СПО* / Заяц А. М., Васильев Н. [Электронный ресурс] // ЭБС Лань: [lanbook.com]. — URL: https://e.lanbook.com/book/269867 (дата обращения: 21.05.2025).