Департамент образования и науки Брянской области

ГБПОУ «Трубчевский профессионально - педагогический колледж»

**Капустина Анастасия Викторовна**

**Специальность:** 09.02.07 Информационные системы и программирование

**Группа:** 33И

**Профессиональный модуль:** ПМ.02 Осуществление интеграции программных модулей

**Преподаватель:** Гусакова Е.А

**ОТЧЕТ ПО УЧЕБНОЙ ПРАКТИКЕ**

2024

**Содержание**

[**Введение** 3](#_Toc165621888)

[**1.Анализ предметной области** 5](#_Toc165621889)

[**2. Проектирование модуля «ХранительПРО»** 10](#_Toc165621890)

[**3. Проектирование модуля «Стражник»** 16](#_Toc165621891)

[**4. Планирование основных этапов разработки программного продукта** 21](#_Toc165621892)

[**Список используемых источников** 24](#_Toc165621893)

[**Приложение 1. Техническое задание на разработку программного решения** 26](#_Toc165621894)

# **Введение**

Учебная практика является частью учебного процесса и направлена на формирование у студентов общих и профессиональных компетенций:

ОК 1. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам

ОК 2. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности

ОК 3 Планировать и реализовывать собственное профессиональное и личностное развитие

ОК 4 Планировать и реализовывать собственное профессиональное и личностное развитие

ОК 5 Планировать и реализовывать собственное профессиональное и личностное развитие

ОК 6 Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей

ОК 7 Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях

ОК 8 Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности

ОК 9 Использовать информационные технологии в профессиональной деятельности

ОК 10 Пользоваться профессиональной документацией на государственном и иностранном языке

ОК 11 Планировать предпринимательскую деятельность в профессиональной сфере.

ПК 2.1. Разрабатывать требования к программным модулям на основе анализа проектной и технической документации на предмет взаимодействия компонент

ПК 2.2. Выполнять интеграцию модулей в программное обеспечение

ПК 2.3 Выполнять отладку программного модуля с использованием специализированных программных средств

ПК 2.4 Осуществлять разработку тестовых наборов и тестовых сценариев для программного обеспечения

ПК 2.5. Производить инспектирование компонент программного обеспечения на предмет соответствия стандартам кодирования.

# **1.Анализ предметной области**

**ХранительПРО**

Любой объект КИИ предполагает пропускной режим на предприятие, независимо от периметра контролируемой и опасной зон. Модуль “ХранительПРО” направлен на организацию пропускного режима и включает в себя:

1. веб-сервис для заказа пропуска на предприятие для гостей и экскурсионных групп;
2. терминал сотрудника общего отдела для формальной проверки поданной заявки;
3. терминал сотрудника охраны для реализации пропускного режима;
4. терминал сотрудника подразделения для учета посещений.

Разработайте инфраструктуру, предполагающую трехзвенную модель в архитектуре “клиент-сервер”:

**Терминал сотрудника общего отдела**

Функционал сотрудника общего отдела:

1. авторизация по коду сотрудника (заранее определен в БД как тестовые данные);
2. просмотр списка заявок по всем данным, представленным в макетах (рисунок 3, рисунок 4);
3. фильтрация заявок по типу, подразделениям, статусу;
4. формальная проверка заявки в отдельном модальном окне с возможностью указания даты и времени посещения, редактирования и изменения статуса заявки.

“Черный список” - это данные по лицам, ранее посещавшим объект и допустившим нарушения по правилам посещения объекта КИИ. Порядок ручного формирования списка будет реализован в терминале сотрудника подразделения. Система автоматически добавляет пользователя в “черный список”, если дважды была отклонена заявка по причине указания заявителем заведомо недостоверных данных.

**Терминал сотрудника охраны**

Функционал сотрудника охраны:

1. авторизация по коду сотрудника (заранее определен в БД как тестовые данные);
2. просмотр списка одобренных заявок по всем данным, представленным в макетах (рисунок 3, рисунок 4);
3. фильтрация заявок по дате, типу, подразделениям;
4. поиск заявки по фамилии, имени и отчеству или номеру паспорта (при групповом посещении достаточно найти одного заявителя);
5. работа с заявкой в отдельном модальном окне с возможностью указания разрешения на доступ на территорию;
6. работа с заявкой в отдельном модальном окне с возможностью указания времени убытия посетителя/посетителей.

Для разрешения на доступ в интерфейсе сотрудника охраны предусмотрите элемент управления, по нажатию на который система дает сигнал о разрешении на проход (в рамках чемпионата - системный звук), открывает турникет (в рамках чемпионата - отправка сообщения на сервер об открытии турникета) и фиксирует время начала посещения в базе данных.

**Терминал сотрудника подразделения**

Функционал сотрудника общего отдела:

1. авторизация по коду сотрудника (заранее определен в БД как тестовые данные);
2. просмотр списка одобренных заявок на подразделение по всем данным, представленным в макетах (рисунок 3, рисунок 4) с возможной фильтрацией по датам;
3. работа с заявкой: просмотр подробной информации по заявке в модальном окне, фиксация времени входы и выхода посетителей/посетителя;
4. добавление посетителя в “черный список”.

Добавление в “черный список”: в окне просмотра информации по заявке должны быть отражены фамилия/фамилии всех посетителей, по нажатию на фамилию с помощью контекстного меню правой клавиши мыши можно добавить посетителя в “черный список”, выбрав команду “Черный список…” и указав в дополнительном окне причину добавления (текст до 5000 символов).

Правила политики безопасности по временным параметрам:

1. сотрудник подразделения не может подтвердить время прихода посетителя/посетителей, если сотрудник охраны не разрешил доступ;
2. если посетителем/посетителями превышено время перемещения от проходной до подразделения (берется из БД), то сотруднику подразделения и сотруднику охраны на терминал отправляется оповещение о нарушении;
3. сотрудник охраны не может указать время завершения посещения, если сотрудник подразделения не указал время окончания посещения.

**Стражник**

«Стражник» – система централизованного мониторинга событий на рабочих станциях сотрудников министерства обороны РФ (МО) и оборонных предприятий. Система позволяет в режиме реального времени выявлять возможные угрозы информационной безопасности (ИБ), оперативно на них реагировать, отправлять уведомления службе безопасности, соблюдать условия мандатного доступа к данным пользователей.

В состав системы «Стражник» входят инструменты мониторинга, обработки и аудита событий на персональных компьютерах (ПК) пользователей, средства визуализации данных для службы ИБ, механизмы оповещения службы ИБ о событиях, нарушающих протоколы безопасности.

Система «Стражник» состоит из набора сервисов, взаимодействующих между собой по протоколу удалённого вызова процедур – gRPC, программному интерфейсу приложений – API, протоколу обмена сообщений – WebSocket.

В состав системы входят следующие сервисы:

сервис контроля доступа;

сервис протоколов безопасности;

сервис логирования;

сервис сообщений;

клиентское приложение для ПК;

клиентское приложение для мобильных устройств.

Пользователями системы являются предприятия выполняющие государственный оборонный заказ (ГОЗ) и Министерство обороны.

Основная цель системы состоит в предотвращении утечки данных о выполнении гособоронзаказа. Предприятия выполняющие ГОЗ должны иметь возможность загрузить в систему выпускаемую ими номенклатуру продукции, указать степень выполнения ГОЗ по каждой группе номенклатуры. Служащие МО должны иметь возможность получить сводные данные о степени выполнения ГОЗ по предприятиям и видам заказанной у предприятий продукции.

Система должна обладать режимом мандатного доступа к данным, т.е. каждая из имеющихся групп пользователей системы получает возможность просматривать определенный вид данных в соответствии с протоколами безопасности. При попытки несанкционированного доступа к данным, со стороны пользователя, система должна осуществлять блокировку действий пользователя, с уведомлением службы безопасности предприятия или МО. Заблокированный пользователь должен иметь возможность связаться с представителем службы ИБ через чат клиентского приложения для ПК.

Для обеспечения наибольшего уровня безопасности, все действия пользователей системы, должны логироваться в режиме реального времени, данные о действиях всех пользователей направляются в службы безопасности предприятий и МО.

С целью обеспечения оперативной работы службы ИБ, необходимо реализовать клиентское приложение для мобильных устройств, которое позволит сотруднику службы ИБ получать информацию о несанкционированных действиях пользователей системы и сообщения от заблокированных пользователей.

# **2. Проектирование модуля «ХранительПРО»**

**Описание диаграммы деятельности добавления посетителя в «черный список»**

Основные элементы диаграммы:

* Начальный узел: Обозначает начало процесса.
* Действия: Представляют собой отдельные шаги процесса, например, "Проверить наличие посетителя в базе данных", "Ввести причину добавления в черный список".
* Решения: Указывают на точки ветвления процесса, где принимается решение о дальнейших действиях. Например, "Посетитель найден?"
* Параллельные процессы: Показывает, что несколько действий могут выполняться одновременно.
* Конечный узел: Обозначает завершение процесса.

Пример диаграммы деятельности для добавления посетителя в "черный список":

1. Начальный узел: Процесс начинается с запроса на добавление посетителя в "черный список".

2. Действие: "Проверить наличие посетителя в базе данных".

3. Решение: "Посетитель найден?"

Да: Перейти к действию "Ввести причину добавления в черный список".

Нет: Перейти к действию "Ввести данные посетителя".

4. Действие: "Ввести причину добавления в черный список" (если посетитель найден) или "Ввести данные посетителя" (если посетитель не найден).

5. Действие: "Добавить посетителя в черный список".

6. Конечный узел: Процесс завершен.

Дополнительные элементы, которые могут быть включены в диаграмму:

* Объекты данных: Указывают на данные, используемые или создаваемые в процессе.
* Участники процесса: Определяют роли, которые участвуют в выполнении действий.
* Примечания: Предоставляют дополнительную информацию о процессе.

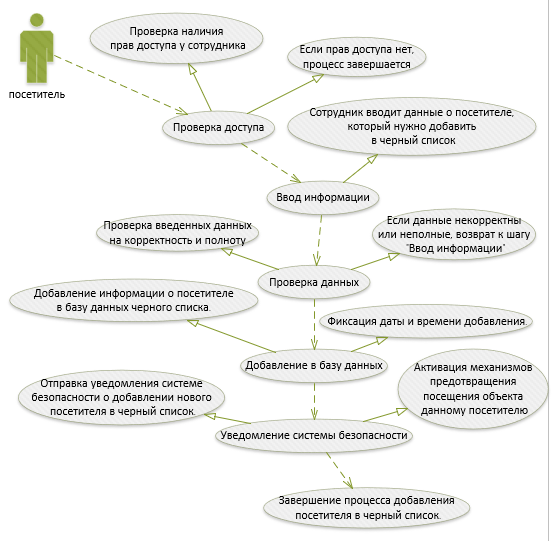


Рисунок 1- Диаграмма деятельности добавления посетителя в «черный список»

**Описание диаграммы последовательности одобрения заявки на посещение.**

1. **Заявка на посещение**:

- Посетитель предоставляет системе безопасности свои личные данные и цель посещения.

1. **Идентификация посетителя**:

- Система безопасности идентифицирует посетителя на основе предоставленных данных.

1. **Проверка доступа**:

- Система проверяет доступ посетителя к месту, которое он хочет посетить.

1. **Уведомление ответственного**:

-В случае необходимости система уведомляет ответственное лицо о заявке на посещение.

1. **Принятие решения**:

- Ответственное лицо принимает решение о разрешении или запрещении доступа посетителю.

1. **Уведомление посетителя**:

- Посетителю уведомляется о решении системы безопасности через систему уведомлений.

1. **Завершение процесса**:

-Процесс одобрения заявки на посещение завершается.

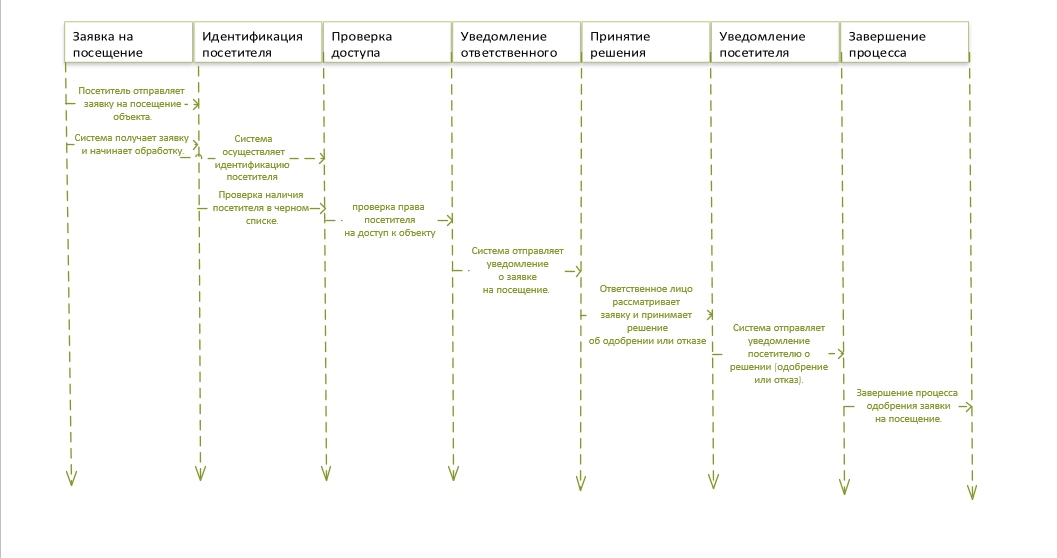


Рисунок 2- Диаграмма последовательности одобрения заявки на посещение.

**Описание диаграмма вариантов использования системы.**

Гость: подает заявку на пропуск через веб-сервис.

Сотрудник общего отдела: проверяет и подтверждает заявки на пропуск.

Сотрудник охраны: осуществляет пропускной режим на основе подтвержденных заявок.

Сотрудник подразделения: регистрирует посещения гостей/экскурсантов.

Администратор: настраивает систему, управляет пользователями и правами доступа.

**Варианты использования:**

Гость:

Подача заявки на пропуск: заполнение онлайн-формы с информацией о себе и цели посещения.

Получение подтверждения: получение уведомления о статусе заявки (одобрена/отклонена).

Проход на территорию: предъявление документа, удостоверяющего личность, для прохода на территорию.

**Сотрудник общего отдела:**

Проверка заявок на пропуск: просмотр информации о заявителях и цели их визита.

Подтверждение/отклонение заявок: одобрение или отклонение заявок на пропуск.

Управление списком гостей/экскурсантов: просмотр списка одобренных заявок и информации о посетителях.

**Сотрудник охраны:**

Проверка пропусков: сверка информации в пропуске с документом, удостоверяющим личность.

Управление доступом: предоставление или ограничение доступа на территорию на основе пропусков.

Регистрация проходов: фиксация времени входа и выхода посетителей.

**Сотрудник подразделения:**

Регистрация посещений: отметка о прибытии и убытии гостя/экскурсанта в подразделение.

Просмотр информации о посещениях: просмотр списка посещений и информации о гостях/экскурсантах.

**Администратор:**

Управление пользователями: добавление, удаление и изменение учетных записей сотрудников.

Управление правами доступа: назначение ролей и прав доступа для различных категорий пользователей.

Настройка системы: конфигурирование параметров системы, таких как правила выдачи пропусков, зоны доступа, графики работы.

Просмотр журналов событий: анализ журналов событий для выявления нарушений и расследования инцидентов.

Генерация отчетов: создание отчетов о посещениях, заявках на пропуск, активности сотрудников и т.д.

**Взаимосвязи между вариантами использования:**

Гость подает заявку на пропуск, которую проверяет сотрудник общего отдела.

Сотрудник общего отдела подтверждает заявки, на основе которых сотрудник охраны осуществляет пропускной режим.

Сотрудник подразделения регистрирует посещения гостей/экскурсантов, прошедших пропускной режим у сотрудника охраны.

Администратор настраивает систему, которой пользуются все остальные актеры, и контролирует ее работу.

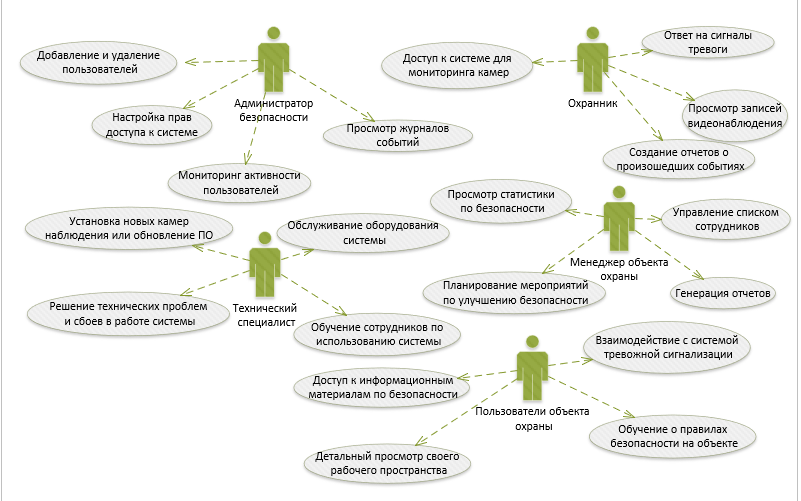
****

Рисунок 3- Диаграмма вариантов использования системы.

# **3. Проектирование модуля «Стражник»**

**Описание диаграммы вариантов использования по системе «Стражник»**

Администратор: отвечает за настройку системы, управление пользователями и правами доступа, просмотр журналов событий и отчётов.

Охранник: использует систему для мониторинга состояния объекта, получения оповещений, управления доступом и реагирования на инциденты.

Менеджер объекта охраны: просматривает отчеты, управляет доступом для пользователей объекта, взаимодействует с администратором безопасности.

Технический специалист: отвечает за установку, настройку и обслуживание оборудования системы.

Пользователи объекта охраны: используют систему для получения доступа к объекту, например, с помощью карт доступа, биометрии или мобильного приложения.

Варианты использования:

Администратор безопасности:

Управление пользователями: Добавление, удаление и изменение учетных записей пользователей системы.

Управление правами доступа: Назначение ролей и прав доступа для различных категорий пользователей.

Настройка системы: Конфигурирование параметров системы, таких как зоны безопасности, уровни доступа.

Просмотр журналов событий: Анализ журналов событий для выявления подозрительной активности и расследования инцидентов.

Генерация отчетов: Создание отчетов о состоянии системы, активности пользователей и событиях безопасности.

Охранник:

Мониторинг состояния объекта: Просмотр видеопотоков с камер наблюдения, отслеживание состояния датчиков и систем безопасности.

Получение оповещений: Получение уведомлений о событиях безопасности, таких как срабатывание датчиков, несанкционированный доступ, тревожные кнопки.

Управление доступом: Предоставление или ограничение доступа к объекту для пользователей, например, с помощью карт доступа или биометрии.

Реагирование на инциденты: Выполнение действий в ответ на события безопасности, таких как вызов подкрепления, эвакуация, задержание нарушителей.

Менеджер объекта охраны:

Просмотр отчетов: Анализ отчетов о событиях безопасности и активности пользователей.

Управление доступом для сотрудников: Запрос на добавление, изменение или удаление доступа для сотрудников объекта.

Взаимодействие с администратором безопасности: сообщать о проблемах безопасности, запрашивать изменения в системе.

Технический специалист:

Установка и настройка оборудования: Установка и настройка камер видеонаблюдения, датчиков, систем контроля доступа и другого оборудования.

Обслуживание системы: Выполнение технического обслуживания системы, устранение неполадок и обновление программного обеспечения.

Мониторинг работоспособности системы: отслеживание работоспособности оборудования и программного обеспечения системы, выявление и устранение проблем.

Пользователи объекта охраны:

Получение доступа к объекту: Использование карт доступа, биометрии или мобильного приложения для получения доступа к объекту.

Активация тревожных кнопок: В случае чрезвычайной ситуации, активация тревожной кнопки для вызова охраны.

Взаимосвязи между вариантами использования:

Администратор безопасности настраивает систему, которой пользуются охранники и технические специалисты.

Охранники используют систему для мониторинга и реагирования на события, которые могут быть проанализированы администратором безопасности и менеджером объекта охраны.

Менеджер объекта охраны взаимодействует с администратором безопасности по вопросам настройки системы и управления доступом для пользователей объекта.

Технический специалист обеспечивает работоспособность системы, которой пользуются все остальные актеры.

Пользователи объекта охраны используют систему, настроенную администратором безопасности и обслуживаемую техническим специалистом, для получения доступа к объекту, который мониторят охранники.

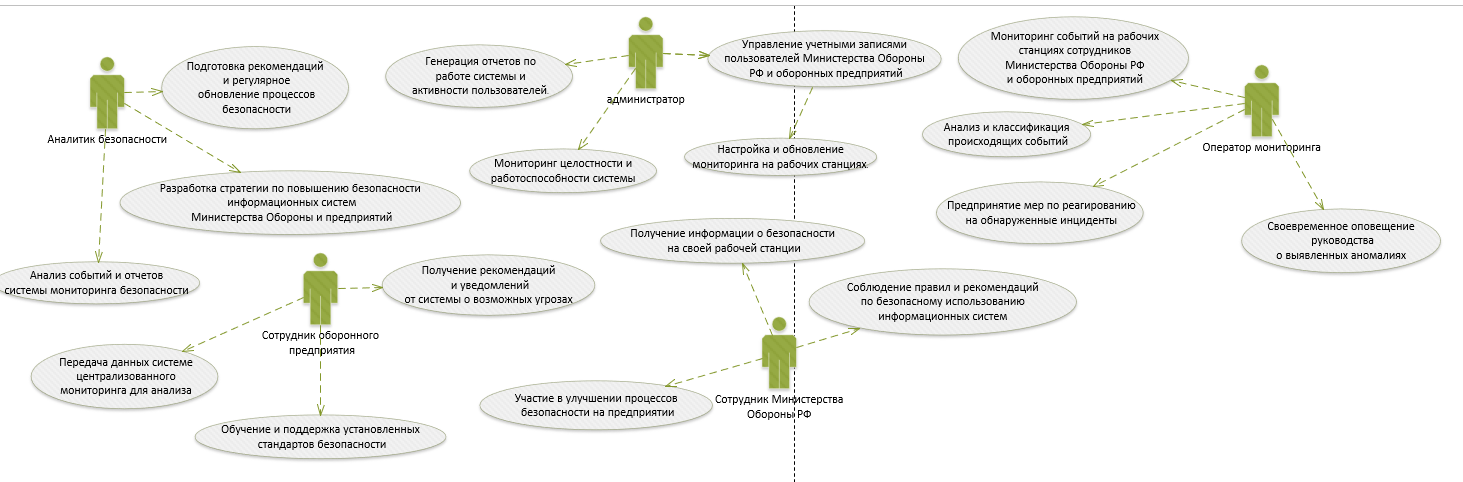


Рисунок 4- Диаграмма вариантов использования по системе «Стражник».

**Описание диаграммы компонентов.**

Управление пользователями: Отвечает за создание, изменение и удаление учетных записей пользователей, а также управление их ролями и правами доступа.

Журналирование событий: Регистрирует все действия в системе, включая вход/выход пользователей, изменения прав доступа, события безопасности и т.д.

Бизнес-логика системы: Определяет правила и процессы работы системы, такие как правила доступа, реакции на события, алгоритмы обработки данных.

База данных: Хранит информацию о пользователях, правах доступа, событиях, конфигурации системы и других данных.

Логика доступа к данным: Обеспечивает доступ к данным в базе данных, контролируя права доступа и обеспечивая целостность данных.

Интерфейс приложения: Позволяет пользователям взаимодействовать с системой, предоставляя графический интерфейс для управления пользователями, просмотра журналов событий, настройки системы и т.д.

Уведомления и оповещения: Информирует пользователей и администраторов о важных событиях, таких как нарушения безопасности, попытки несанкционированного доступа, изменения в системе.

**Взаимосвязи между компонентами:**

Управление пользователями взаимодействует с базой данных для хранения и извлечения информации о пользователях и правах доступа.

Журналирование событий записывает информацию о событиях в базу данных.

Бизнес-логика системы использует информацию из базы данных и журнала событий для принятия решений и выполнения действий.

Логика доступа к данным контролирует доступ к базе данных на основе правил, определенных в бизнес-логике системы и информации о правах доступа из управления пользователями.

Интерфейс приложения взаимодействует с управлением пользователями, журналированием событий, бизнес-логикой системы и логикой доступа к данным для предоставления функций пользователям.

Уведомления и оповещения генерируются на основе событий, зарегистрированных в журнале событий и обработанных бизнес-логикой системы.

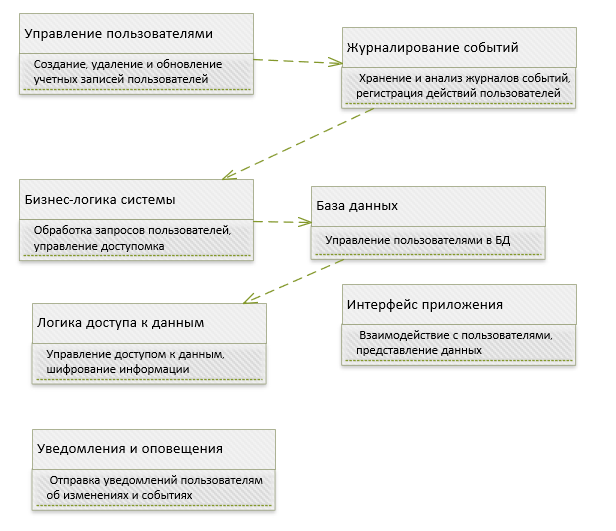
****

Рисунок 5 - Диаграмма компонентов

# **4. Планирование основных этапов разработки программного продукта**

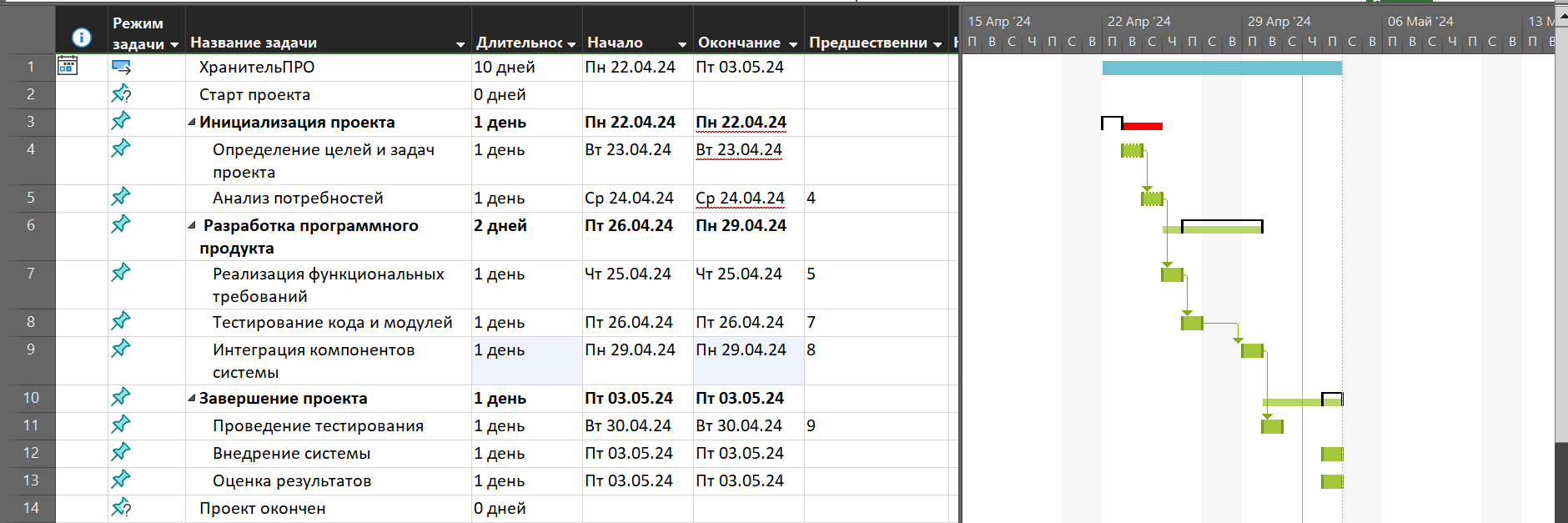
**ХранительПРО**

Рисунок 6 - Диаграмма Ганта «ХранительПРО»

**1. Инициализация проекта:**

Определение целей и задач проекта: Четкое формулирование того, что должно быть достигнуто в результате разработки "ХранительПРО".

Анализ потребностей: Изучение требований пользователей, определение функциональности системы, ограничений и рисков.

**2. Разработка программного продукта:**

Реализация функциональных требований: На этом этапе разработчики создают код и реализуют функциональные требования, которые были определены на предыдущих этапах проектирования и планирования.

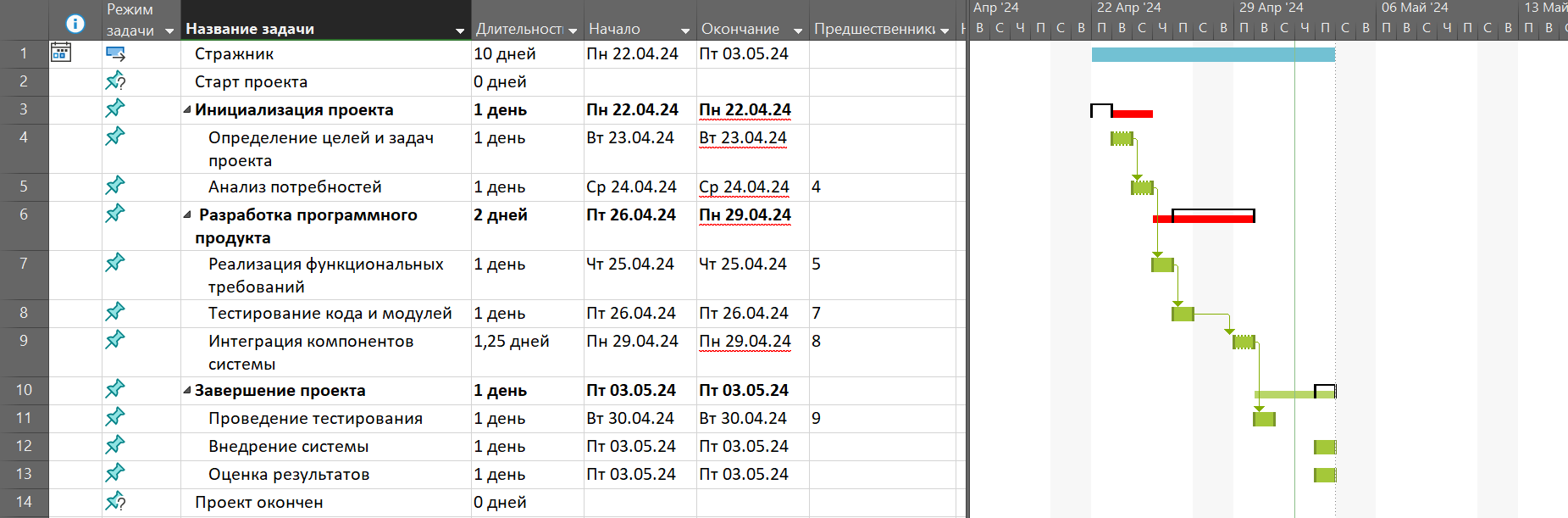
Тестирование кода и модулей: На этом этапе команда проверяет качество кода и функциональных модулей, используя различные тестовые методы и инструменты. Цель тестирования заключается в обнаружении ошибок, недостатков и потенциальных проблем, которые могут повлиять на работу и производительность программного продукта. Тестирование помогает убедиться в том, что программное обеспечение работает корректно и безопасно.

Интеграция компонентов системы: После реализации функциональных требований и тестирования кода, следующий шаг заключается в интеграции всех компонентов системы. Интеграция означает слияние различных частей программного продукта, таких как функции, модули и компоненты, в единое целое. Этот процесс может включать в себя решение конфликтов между компонентами, настройку параметров и разработку интерфейсов между компонентами.

**3. Завершение проекта:**

Тестирование и отладка: Проведите комплексное тестирование системы, исправьте выявленные ошибки.

Внедрение системы: Установите "ХранительПРО" в рабочую среду, обучите пользователей.

Оценка результатов: Проанализируйте, достигнуты ли цели проекта, и извлеките уроки для будущих проектов.

**Стражник**

Рисунок 7- Диаграмма Ганта «Стражник»

**1. Инициализация проекта:**

Определение целей и задач проекта: Четкое формулирование того, что должно быть достигнуто в результате разработки "ХранительПРО".

Анализ потребностей: Изучение требований пользователей, определение функциональности системы, ограничений и рисков.

**2. Разработка программного продукта:**

Реализация функциональных требований: На этом этапе разработчики создают код и реализуют функциональные требования, которые были определены на предыдущих этапах проектирования и планирования.

Тестирование кода и модулей: На этом этапе команда проверяет качество кода и функциональных модулей, используя различные тестовые методы и инструменты. Цель тестирования заключается в обнаружении ошибок, недостатков и потенциальных проблем, которые могут повлиять на работу и производительность программного продукта. Тестирование помогает убедиться в том, что программное обеспечение работает корректно и безопасно.

Интеграция компонентов системы: После реализации функциональных требований и тестирования кода, следующий шаг заключается в интеграции всех компонентов системы. Интеграция означает слияние различных частей программного продукта, таких как функции, модули и компоненты, в единое целое. Этот процесс может включать в себя решение конфликтов между компонентами, настройку параметров и разработку интерфейсов между компонентами.

**3. Завершение проекта:**

Тестирование и отладка: Проведите комплексное тестирование системы, исправьте выявленные ошибки.

Внедрение системы: Установите "ХранительПРО" в рабочую среду, обучите пользователей.

Оценка результатов: Проанализируйте, достигнуты ли цели проекта, и извлеките уроки для будущих проектов.

# **Список используемых источников**

1. Герберт, Ш. Полный справочник по C# [Текст]/ Ш. Герберт. – М.: Вильямс, 2004Герберт, Ш. C# Учебный Курс [Текст]/ Ш. Герберт. – М.: Вильямс, 2020. – 471 с.
2. Кабаков, Р. R в действии. Анализ и визуализация данных в программе R / Р. Кабаков. - М.: ДМК, 2020. - 588 c.
3. Ватсон, К. С#. Программист программисту [Текст]/ К. Ватсон. – СПб.: Лори, 2019. – 879с.
4. **Бьяфоре Б.** Microsoft Visio 2007. Библия пользователя. — М.: Диалектика, Вильямс, 2019. — 800 с.
5. **Кораблева Е. В.** Подготовка технической документации и бизнес-графики с использованием Microsoft Visio 2007 (Курс для пользователей). — М.: УЦ Сетевая Академия ЛАНИТ, 2018. — 82 с.
6. **Лемке Д.** Microsoft Office Visio 2007. — М.: ЭКОМ Паблишерз, 2018. — 368 с.
7. **Погосян И.** Microsoft Visio 2007: Обучающая программа. — М.: 1С: Мир компьютера, 2018. — 1 электр. опт. диск (CD-ROM).
8. **Богданов В. В.** «Управление проектами в Microsoft Project 2002». Учебный курс, 2019. – 456с.
9. Культин Н.Б. Инструменты управления проектами: Project Expert и Microsoft Project. - СПб.: БХВ-Петербург, 2020. - 160 с. Ил.
10. В.П. Романов, Н.З. Емельянова, Т.Л. Партыка Проектирование экономических информационных систем. Методологии и современные технологии. - М: Экзамен, 2021.- 256 с.;
11. Маклаков С.В. BPWin и ERWin CASE - средства разработки информационных систем / Маклаков С.В. - М: ДИАЛОГ МИФИ, 2021.-256с.;
12. Гелмерс, С.А. Microsoft Visio 2010. Русская версия / С.А. Гелмерс. - М.: ДМК Пресс, Эком**, 2020. - 727** c.
13. Скотт, А. Microsoft Visio 2013. Шаг за шагом / А. Скотт. - М.: Эком, **2019. - 481** c.
14. Солоницын, Юрий Microsoft Visio 2007. Создание деловой графики / Юрий Солоницын. - М.: Питер, **2018. - 640**c.
15. Сергеев В.И., Григорьев М.Н., Уваров С. А. Логистика. Информационные системы и технологии. - М.: Альфа-Пресс, 2020. - 608 с.
16. Дегтярев Ю.И. Системный анализ и исследования операций. - М.: Высш. ш., 2018. - 335 с.
17. Антонов А.В. Системный анализ. Методология. Построение модели: Учеб. пособие. - Обнинс: ИАТЭ, 2020. - 272 с.
18. Волова В.Н. Основы теории систем и системного анализа/В.Н. Волова, А.А. Денисов. - СПб.: СПбГТУ, 2018. - 510 с.
19. Четфилд, Карл Microsoft Project 2010. Русская версия / Карл Четфилд , Тимоти Джонсон. - М.: ЭКОМ Паблишерз, 2019. - 656 c.
20. Четфилд, Карл Microsoft Project 2013. Русская версия / Карл Четфилд , Тимоти Джонсон. - М.: ЭКОМ Паблишерз, 2019. - 672 c.

# **Приложение 1. Техническое задание на разработку программного решения**

**АТТЕСТАЦИОННЫЙ ЛИСТ**

**профессиональной деятельности студента во время учебной практики**

**Капустина Анастасия Викторовна**

*обучающаяся по специальности 09.02.07 Информационные системы и программирование*

*успешно прошла учебную практику по профессиональному модулю*

*ПМ 02. Осуществление интеграции программных модулей*

*(МДК.02.01 Технология разработки программного обеспечения; МДК.02.02 Инструментальные средства разработки программного обеспечения; МДК.02.03 Математическое моделирование)*

в объеме 72 *часов* с 20 апреля 2023 года по 3 мая 2023 года

в организации *ГБПОУ «Трубчевский профессионально-педагогический колледж»*

Формируемые компетенции: *ПК 2.1-2.5; ОК 1-11*

Преподаватель: Гусакова Екатерина Александровна

|  |  |
| --- | --- |
| Виды и объемы работ, выполненные обучающимися во время практики | Качество выполнения работ в соответствии с технологией и (или) требованиями организации, в которой проходила практика |
| Разрабатывать требования к программным модулям на основе анализа проектной и технической документации на предмет взаимодействия компонент |  |
| Выполнять интеграцию модулей в программное обеспечение |  |
| Выполнять отладку программного модуля с использованием специализированных программных средств |  |
| Осуществлять разработку тестовых наборов и тестовых сценариев для программного обеспечения |  |
| Производить инспектирование компонент программного обеспечения на предмет соответствия стандартам кодирования. |  |

«\_\_\_»\_\_\_\_\_\_\_\_2023 года

Руководитель практики Е.А. Гусакова