Ханты-Мансийского Автономного округа – Югры

«СУРГУТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Политехнический институт

Кафедра информатики и вычислительной техники

Курсовая работа

По дисциплине «Методы и средства проектирования информационных

систем»

Выполнил:

студент группы 607-01

Шнайдер В.А.

Проверяет:

Преподаватель кафедры ИВТ

Столбов Д.А.

Сургут, 2024

**Содержание**

[Видение 3](#_Toc1)

[Дополнительная спецификация 9](#_Toc2)

[Use case-диаграмма 13](#_Toc3)

[Описание прецедента 14](#_Toc4)

[Диаграмма компонентов 15](#_Toc5)

[Концептуальная модель 16](#_Toc6)

[Диаграмма классов 17](#_Toc7)

[Прототип UI 18](#_Toc8)

[BPMN 19](#_Toc9)

# Видение

**Краткое наименование:** Health-Guard

**Полное наименование:** Система контроля версий приложений.

**Введение**

В наше время пользователи сталкиваются с огромным количеством установленных приложений на своих устройствах — от мобильных телефонов до персональных компьютеров. Столь разнообразные программы представляют собой важные инструменты для работы, обучения, развлечений и многого другого. Однако, с ростом числа установленных приложений возникает необходимость в эффективном управлении версиями этого программного обеспечения.

Именно в этом контексте разрабатывается программа, которая облегчит пользовательскую жизнь, предоставляя возможность управлять просмотром и установкой новых версий приложений. Основная цель — сделать этот процесс простым, удобным и безопасным для всех пользователей. Данное решение поможет пользователям всегда оставаться в курсе актуальных версий и обновлений для своих программ, а также легко устанавливать их.

**Возможности**

Health-Guard предлагает следующие возможности:

1. Просмотр текущих версий приложений: Пользователь сможет легко просматривать список установленных приложений на своем устройстве и их текущие версии.
2. Оповещения о доступных обновлениях: Программа будет автоматически сканировать установленные приложения и уведомлять пользователя о доступных обновлениях.
3. Получение информации о новых версиях: Пользователь будет получать подробную информацию о новых версиях приложений, включая список изменений и улучшений.
4. Легкость установки обновлений: Программа предоставит возможность однократной установки всех доступных обновлений или выборочной установки конкретных приложений.
5. Уровень опасности: Программа по мимо проверки текущего обновления, также будет проверять его уровень критичности, что даст пользователю понять, что нужно обновить свою версию приложения до актуальной.

**Проблема**

В современном цифровом мире пользователи сталкиваются с рядом проблем, связанных с управлением версиями приложений:

1. Неактуальные версии приложений: Многие пользователи не следят за обновлениями своих приложений из-за занятости или недостатка информации. Это может привести к использованию устаревших версий приложений, что может повлечь за собой уязвимости безопасности и отсутствие новых функций.
2. Сложности в обновлении: Для неопытных пользователей обновление приложений может быть сложным и неудобным процессом. Они могут столкнуться с техническими проблемами или опасениями по поводу установки новых версий.
3. Отсутствие автоматических уведомлений: Многие приложения не предоставляют автоматических уведомлений о доступных обновлениях, что требует от пользователей активного поиска и установки новых версий.
4. Безопасность: Неактуальные версии приложений могут представлять угрозу для безопасности данных пользователя из-за уязвимостей, которые могут быть исправлены в последних обновлениях.

**Заинтересованные лица**

|  |  |  |
| --- | --- | --- |
| **Роль** | **Цель** | **Текущее решение** |
| Администраторы информационной системы | Управление версиями лицензионных продуктов | Функция обновления встроенные в ПО |
| Пользователи | Получение актуальных версий | Функция обновления встроенные в ПО |

**Конкуренты (Анализ рынка)**

|  |  |  |  |
| --- | --- | --- | --- |
| **Критерии** | **SUMo** | **UpdateStar Premium 4** | **Health-Guard** |
| Простота использования | + | - | + |
| Ссылка на официальный сайт продукта или авто обновление | - | + | + |
| Проверка уровня угрозы | - | - | + |
| Кроссплатформенность | - | - | + |

**Расчет рынка**

**Заработок**

Продажа лицензионных ключей активации является основным источником дохода для "Health-Guard". Организации, заинтересованные в обеспечении информационной безопасности, могут приобрести ключи, что позволит вашей компании генерировать стабильный поток дохода. Ключи могут предоставляться в различных форматах, включая одноразовые, временные или многопользовательские лицензии, в зависимости от потребностей и бюджетов клиентов.

**Перспективы решения**

1. Программа будет кроссплатформенной, это значит, что её можно использовать как на операционных системах Windows 10/11, так и на системах Linux (Alt, Astra, РедОС).
2. Программа будет отслеживать уровень угрозы версии программного обеспечения и уведомлять пользователя о их наличии, что позволить повысить уровень безопасности компьютерной системы.

Словарь терминов

|  |  |  |
| --- | --- | --- |
| **Термин** | **Определение** | **Синонимы** |
| Система мониторинга | Система, предназначенная для наблюдения и контроля за определенными явлениями или процессами. | Система наблюдения, система контроля |
| Версия приложения | Конкретная идентифицирующая метка или номер, присвоенный определенной версии программного приложения. | Релиз, обновление |
| Информационная безопасность | Защита информации от несанкционированного доступа, использования, раскрытия, изменения или уничтожения. | Безопасность информации |
| Разработка информационной системы | Процесс создания информационной системы, включающий анализ требований, проектирование, программирование, тестирование и внедрение. | Разработка ИС, разработка ПО |
| Мониторинг версий | Процесс отслеживания изменений и обновлений версий программного приложения. | Контроль версий, отслеживание обновлений |
| Функциональные возможности | Характеристики и возможности системы или приложения, определяющие его функциональность и способность выполнять определенные задачи. | Функциональные характеристики, возможности |
| Безопасность | Состояние защищенности от угроз и рисков, связанных с несанкционированным доступом, вмешательством или повреждением. | Защита, безопасность данных |
| ПО (программное обеспечение) | Комплекс программ, выполняющих определенные функции на компьютере или другом устройстве. | Софт, приложение |
| Информационная система | Система, предназначенная для сбора, хранения, обработки, передачи и использования информации. | Система обработки данных, информационный комплекс |
| Доверенная зона | Область системы, считающаяся безопасной | Безопасная зона, защищенная зона |
| Уровень угрозы | Оценка степени опасности для системы или данных | Степень опасности, риск |

# Дополнительная спецификация

**Введение**

Проект "Health-Guard" направлен на создание инструмента для мониторинга версий программного обеспечения. Данная дополнительная спецификация описывает различные аспекты функциональности, безопасности, удобства использования и другие важные аспекты проекта.

**Функциональность**

1. Отслеживание версий ПО:

• Описание: Разработка и реализация механизма для отслеживания и регистрации версий программного обеспечения. • Отношение к прецедентам: Каждая версия ПО связана с прецедентами, определяющими ее особенности, изменения и связанные задачи.

2. Уведомления о новых версиях:

• Описание: Разработка системы уведомлений, которая будет информировать пользователей о доступных обновлениях и новых версиях ПО. • Отношение к прецедентам: Уведомления о новых версиях связаны с прецедентами, определяющими условия и критерии для отправки уведомлений.

3. Хранение истории версий:

• Описание: Разработка механизма для хранения истории всех предыдущих версий ПО, включая информацию о выпущенных обновлениях и изменениях. • Отношение к прецедентам: Хранение истории версий связано с прецедентами, определяющими процесс регистрации и архивирования каждой версии.

4. Оценка уровня угрозы:

Описание: Разработка системы оценки уровня угрозы, связанной с каждой обнаруженной уязвимостью. Отношение к прецедентам: Уровень угрозы связан с прецедентами, определяющими критерии оценки и категоризации (критичная, высокая, средняя, низкая).

**Подключаемые бизнес-правила:**

1. Автоматический сбор информации о версиях:

• Описание: Разработка механизма, которая будет автоматически собирать информацию о версиях ПО из выбранной системы мониторинга, включая номера версий, даты выпуска, описания изменений и другую сопутствующую информацию. • Изменение: Возможность автоматически собирать информацию о версиях ПО.

2. Уведомления о новых версиях и изменениях:

• Описание: Разработка механизма уведомления, позволяющие системе мониторинга версий ПО отправлять уведомления о новых версиях ПО и связанных с ними изменениях разработчикам, администраторам и другим заинтересованным сторонам. • Изменение: Возможность получать уведомления о новых версиях ПО.

3. Отображение и анализ информации о версиях:

• Описание: Разработка интерфейса, позволяющий пользователям просматривать и анализировать информацию о версиях ПО, включая номера версий, даты выпуска, описания изменений и другие связанные данные. • Изменение: Просмотр и анализ информации о версиях ПО.

**Интеграция:**

Интеграция с базами данных уязвимостей (CVE, NVD, OWASP).

Интеграция с системами управления ИТ-инфраструктурой (ITSM).

**Безопасность:**

Обеспечение конфиденциальности информации об уязвимостях.

Защита от несанкционированного доступа к данным.

**Удобство использования:**

Интуитивный пользовательский интерфейс: Описание: Создание удобного и интуитивно понятного пользовательского интерфейса (UI), обеспечивающего простоту навигации и взаимодействия с инструментом Health-Guard. Включает в себя понятные иконки, легкость освоения основных функций и минимизацию необходимости в дополнительных объяснениях. Краткие и понятные инструкции: Описание: Предоставление четких и кратких инструкций для пользователя на протяжении всего процесса мониторинга версий ПО с использованием Health-Guard. Включение подсказок и объяснений новых функций и возможностей инструмента. Быстрый доступ и загрузка: Описание: Оптимизация процесса запуска инструмента и скорости загрузки данных о версиях ПО с помощью Health-Guard. Обеспечение минимального времени ожидания, чтобы пользователи могли быстро получить доступ к актуальной информации о версиях. Фильтрация и сортировка информации по различным критериям (уровень угрозы, тип ПО, дата обнаружения).

**Производительность:**

Обеспечение быстрой и эффективной работы системы сканирования и оценки уязвимостей.

**Ограничения:**

Технические ограничения, связанные с доступностью информации об уязвимостях.

Финансовые и временные ограничения, связанные с разработкой и поддержкой системы.

**Программные интерфейсы:**

Интерфейс пользователя (User Interface, UI): позволяет пользователю взаимодействовать с системой мониторинга версий ПО, отображает информацию о доступных обновлениях и предлагает их установку. Интерфейс программирования приложений (Application Programming Interface, API): может использоваться для получения информации о доступных версиях ПО из внешних источников.

**Средства разработки:**

Для разработки пользовательского интерфейса будет использоваться платформа – VisualStudio с использованием инструмента WinForms.

**Бизнес-правила:**

Правило 1: Автоматическое сканирование ПО на наличие уязвимостей.

Правило 2: Определение уровня угрозы для каждой обнаруженной уязвимости.

Правило 3: Уведомление пользователей об обнаруженных уязвимостях.

Правило 4: Предоставление рекомендаций по исправлению уязвимостей.

|  |  |  |  |
| --- | --- | --- | --- |
| **Имя бизнес-правила** | **Описание бизнес-правила** | **Возможность изменения** | **Источник** |
| Правило 1 | Автоматическое сканирование ПО на наличие уязвимостей. | Да | Внутренний |
| Правило 2 | Определение уровня угрозы для каждой обнаруженной уязвимости. | Да | Внутренний |
| Правило 3 | Уведомление пользователей об обнаруженных уязвимостях. | Да | Внутренний |
| Правило 4 | Предоставление рекомендаций по исправлению уязвимостей. | Да | Внутренний |

**Вопросы законодательства:**

Соблюдение требований к защите данных.

Соблюдение авторских прав и лицензионных условий использования ПО.

**Информация из предметной области:**

Текущие тенденции в области ИТ-безопасности.

Популярные практики и стандарты управления уязвимостями.

Требования и ожидания пользователей по поводу защиты от уязвимостей.

**Влияние на другие компоненты:**

Расширение функциональности системы мониторинга версий ПО.

Интеграция с системами ИТ-безопасности.

# Use case-диаграмма

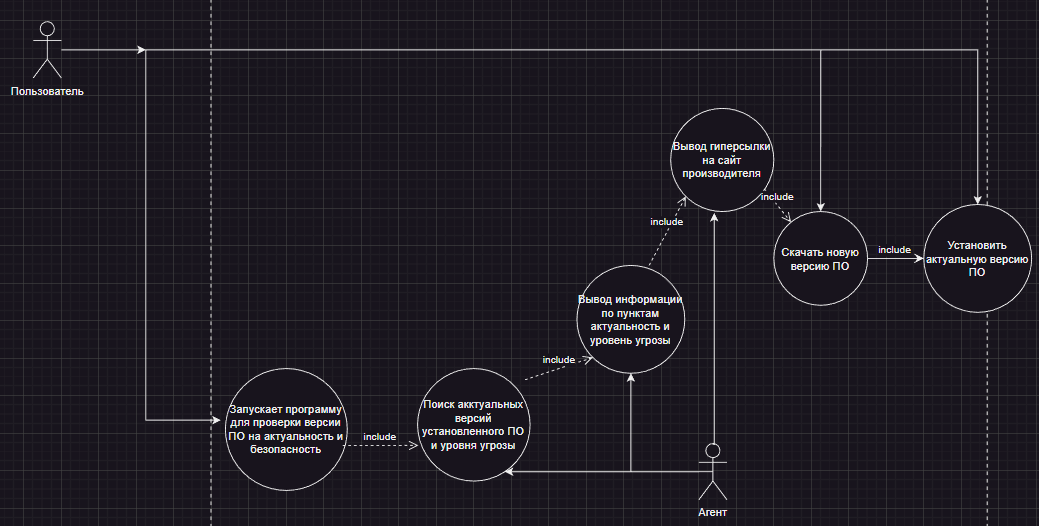


Рис. 1. Usecase – прецедент

# Описание прецедента

**Название прецедента:**

Текущая версия ПО является уязвимой

**Участники:**

1. Пользователь
2. Программа проверки обновления ПО (часть программного обеспечения)

**Описание:**

Данный прецедент описывает ситуацию, в которой программа проверяет установленное ПО на устройстве и обнаруживает, что версия одного или нескольких приложений являются уязвимыми. Прецедент позволяет пользователю быть уверенным, что установленное ПО является актуальным и безопасным.

**Предусловия:**

1. Пользователь запустил программу проверки версии ПО.

**Основной сценарий:**

1. Пользователь запускает программу проверки версии ПО.
2. Система выводит список ПО(название, производитель, текущая версия, актуальная версия, ссылка на сайт продукта, уровень угрозы) установленное в его системе.
3. Система обнаруживает одну или несколько версий ПО, которые являются уязвимыми и уведомляет об этом пользователя, если ничего не обнаруживается, то перейти к шагу 7.
4. Пользователь принимает во внимание данное уведомление и заходит на официальный сайт разработчика ПО.
5. Пользователь скачивает либо актуальную версию ПО, либо предыдущую версию, чтобы ПО было безопасным.
6. После установки новой версии ПО, система выдаст что версия ПО актуальна и безопасна.
7. Завершение работы программы.

**Постусловия:**

1. Пользователь получает обновленную версию ПО для дальнейшего безопасного использования.

**Альтернативные потоки:**

Нет.

Этот прецедент описывает основной сценарий использования системы по мониторингу версий ПО, где пользователь взаимодействует с программным обеспечением для проверки версии ПО на актуальность и безопасность.

# Диаграмма компонентов

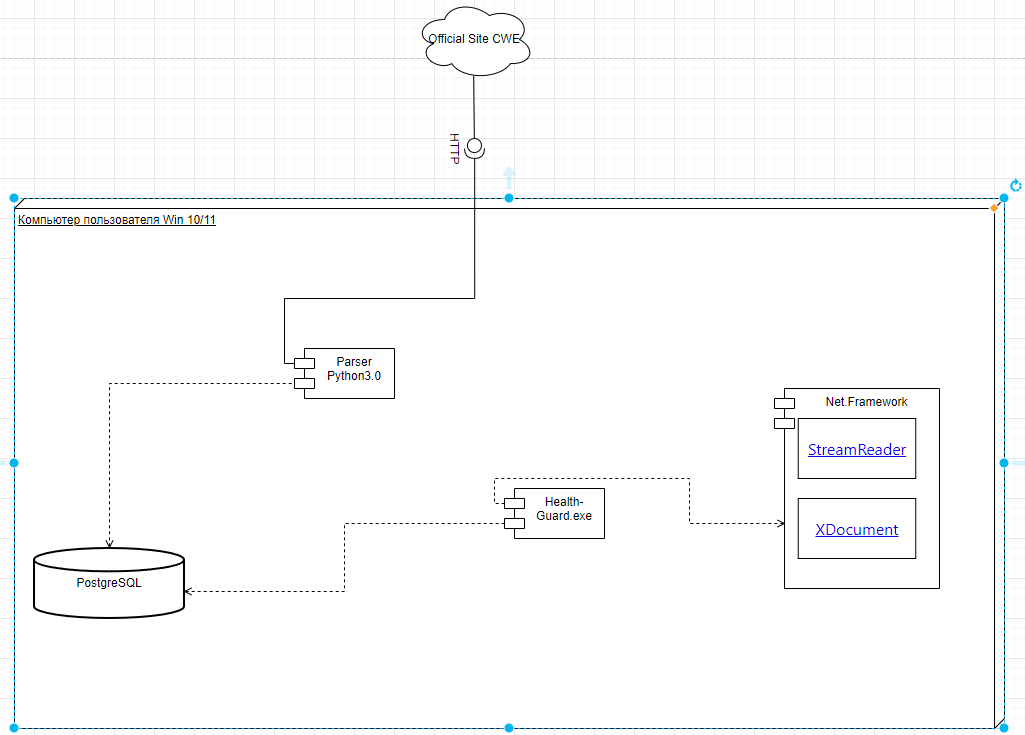


Рис.2. Диаграмма компонентов

# Концептуальная модель

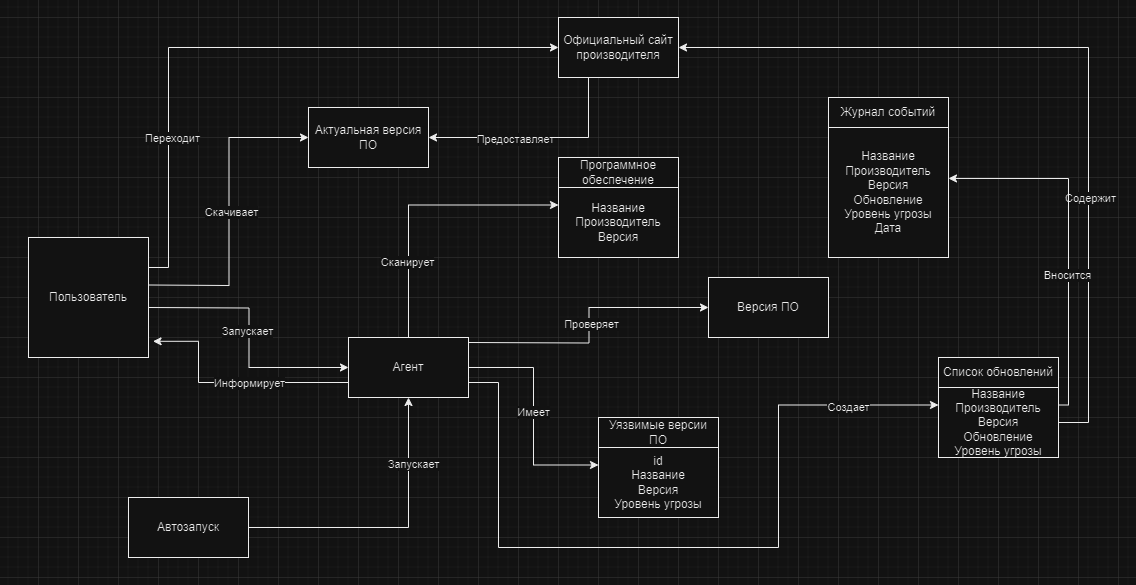
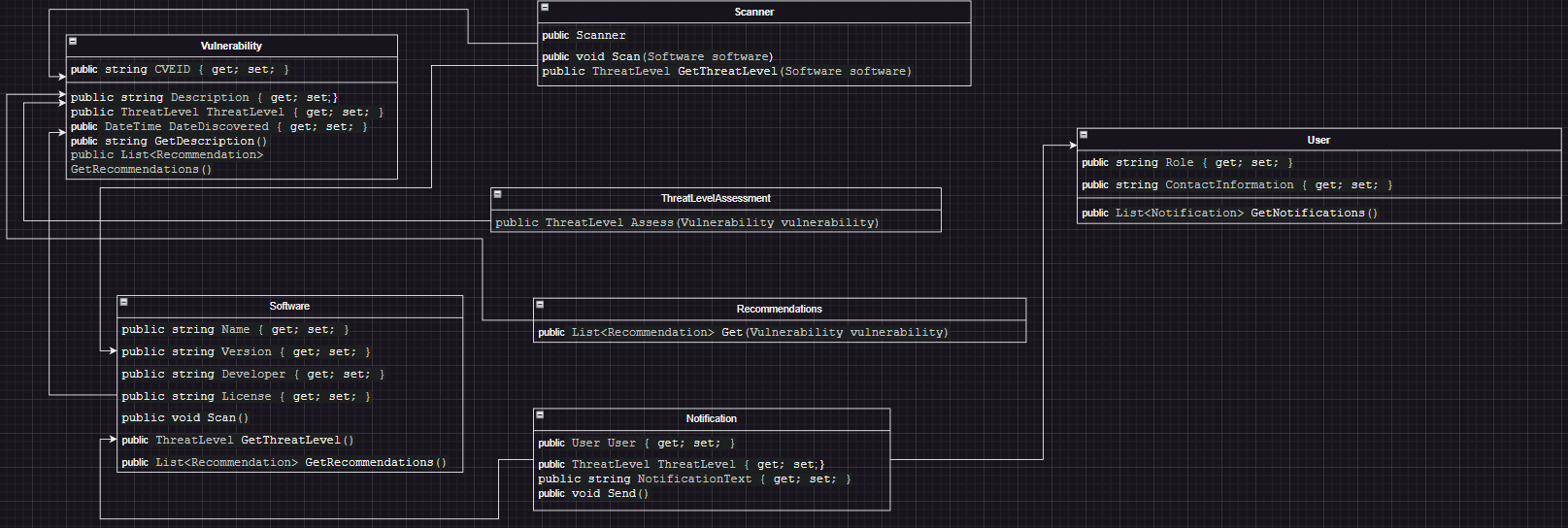


Рис. 3. Концептуальная модель

# Диаграмма классов

Рисунок 4. Диаграмма классов



# Прототип UI

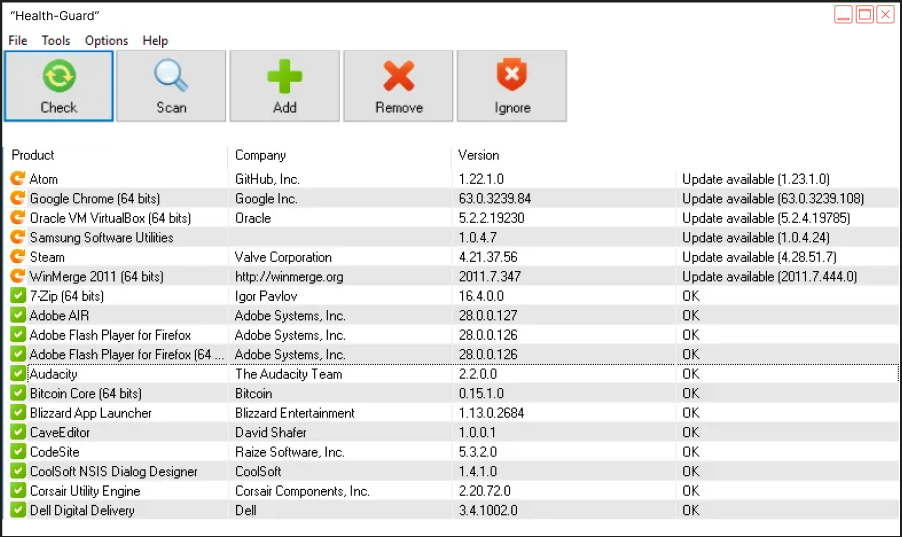


Рис. 5. Прототип UI

# BPMN

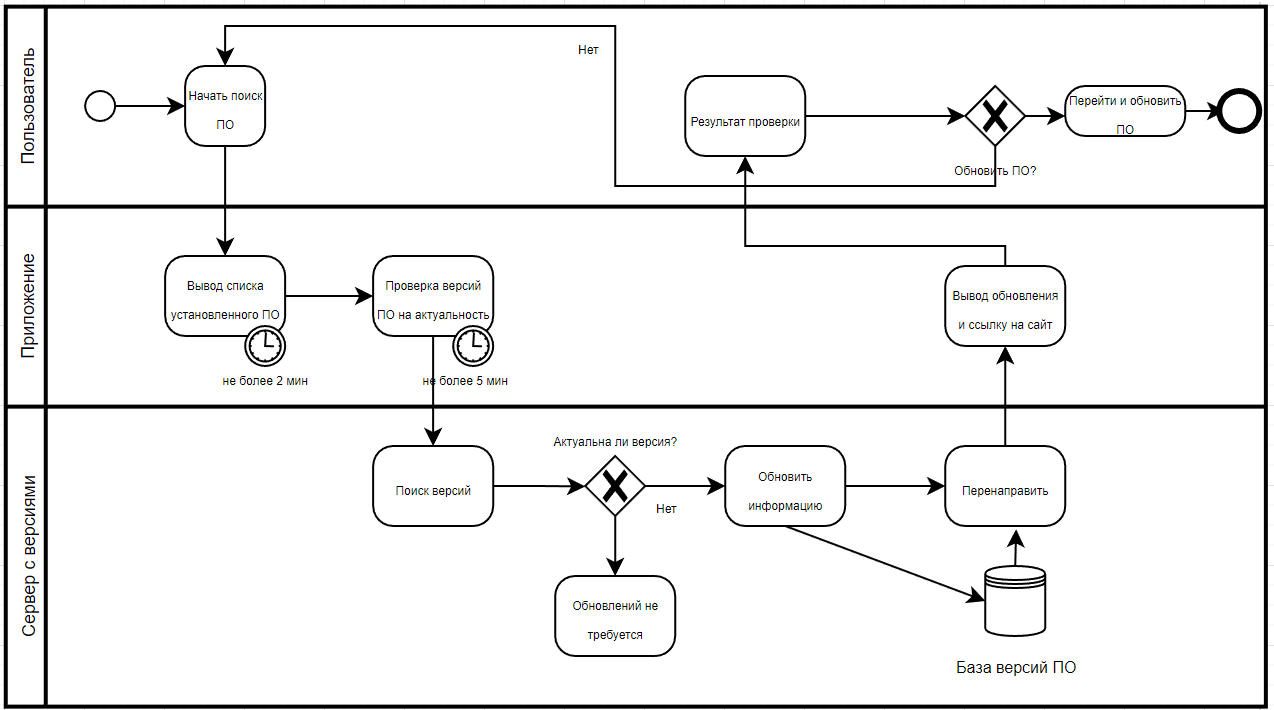


Рис. 6. BPMN - диаграмма