\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

«\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2021 г.

**ТЕХНИЧЕСКОЕ ЗАДАНИЕ**

НА РАЗРАБОТКУ СИСТЕМЫ ПРОГНОЗИРОВАНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

**2023**

СОДЕРЖАНИЕ

[1. ОБЩИЕ СВЕДЕНИЯ 3](#_Toc89780156)

[1.1. Наименование и краткое описание 3](#_Toc89780157)

[1.2. Правовая основа создания ПО ППСЭБ 4](#_Toc89780158)

[1.3. Список используемых сокращений 5](#_Toc89780159)

[2. НАЗНАЧЕНИЕ, ЦЕЛЬ СОЗДАНИЯ И АКТУАЛЬНОСТЬ РАЗРАБОТКИ 6](#_Toc89780161)

[2.1. Назначение 6](#_Toc89780162)

[2.2. Цель создания 6](#_Toc89780163)

[2.3. Актуальность разработки 7](#_Toc89780163)

[3. ТРЕБОВАНИЯ К РАЗРАБОТКЕ И ПО 8](#_Toc89780161)

[3.1. Технические требования 8](#_Toc89780162)

[3.2. Функциональные требования 9](#_Toc89780162)

[3.3. Требования к безопасности 9](#_Toc89780162)

[3.4. Требования к алгоритму прогнозирования 10](#_Toc89780162)

[3.5. Требования к надежности 10](#_Toc89780162)

[3.6. Требования к численности и квалификации сотрудников 12](#_Toc89780162)

[3.7. Требования к интерфейсу 12](#_Toc89780162)

[4. ЭТАПЫ СОЗДАНИЯ И ИХ СОДЕРЖАНИЕ 12](#_Toc89780161)

[4.1. Аналитический этап](#_Toc89780162) 12

[4.2. Этап разработки 13](#_Toc89780162)

[4.3. Этап настройки 13](#_Toc89780162)

[4.4. Тестовый этап](#_Toc89780162) 14

[4.5. Этап ввода в эксплуатацию 14](#_Toc89780162)

[5. ПОРЯДОК КОНТРОЛЯ 15](#_Toc89780161)

1. ОБЩИЕ СВЕДЕНИЯ

1.1. **Наименование и краткое описание**

Настоящее техническое задание (ТЗ) разработано с целью создания программного обеспечения (ПО) для оказания помощи аналитическим подразделениям, подразделениям информационной безопасности, а также иным подразделениям МВД России при предупреждении, выявлении и раскрытии преступлений в сфере информационных технологий. Данное ТЗ определяет основные требования, к разрабатываемому на его основе, программное обеспечение, требования к последующей его работе, а также требования к построению алгоритма прогнозирования.

Внедрение системы прогнозирования (СП) позволит устанавливать показатели, характеризующих развитие (изменение) преступности в сфере информационных технологий, выявлять ее отрицательные и положительные тенденций, и на основе полученных данных отыскивать наиболее результативные способы борьбы с изучаемым видом преступности.

Полное наименование: «Программное обеспечение прогнозирования преступлений в сфере информационных технологий».

Сокращенное наименование системы: ППСИТ.

Проектирование, разработка и написание ППСИТ проводятся на основании настоящего ТЗ.

Финансирование работ осуществляется из средств Федерального Бюджета.

Порядок оформления и предъявления Заказчику результатов работ определяется на основании действующих стандартов и нормативно правовых актов.

1.2. **Правовая основа создания системы ППСИТ**

При создании данного ТЗ, а также последующей разработки системы ППСИТ необходимо руководствоваться следующими нормативно-правовыми актами:

1. Конституция Российской Федерации от 12.12.1993 // Справочно-правовая система «Гарант». – Режим доступа: <https://base.garant.ru/10103000/>
2. Закон Российской Федерации «Об основах системы профилактики правонарушений в РФ» от 23.06.2016 № 182-ФЗ // Справочно-правовая система МЧС России. – Режим доступа: <https://mchs.gov.ru/dokumenty/federalnye-zakony/472>
3. Закон Российской Федерации «Об информации, информационных технологиях и о защите информации» от 08.07.2006 № 149-ФЗ // Справочно-правовая система «Гарант». – Режим доступа: <https://base.garant.ru/12148555/>
4. Закон Российской Федерации «Кодекс Российской Федерации об административных правонарушениях» от 20.12.2001 № 195-ФЗ // Справочно-правовая система «Гарант». – Режим доступа: <https://base.garant.ru/12125267/>
5. Закон Российской Федерации «Уголовный кодекс Российской Федерации» от 24.051996 № 63-ФЗ // Справочно-правовая система «Гарант». – Режим доступа: <https://base.garant.ru/10108000/>
6. Постановление Правительства Российской Федерации «О мерах по совершенствованию использования информационно-коммуникационных технологий в деятельности государственных органов» от 25.04.2012 № 394 // Справочно-правовая система «Гарант». – Режим доступа: <https://base.garant.ru/70168870/>
7. Постановление Правительства Российской Федерации «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации» от 06.07.2015 № 676 // Справочно-правовая система «Гарант». – Режим доступа: <https://base.garant.ru/71120998/>
8. Приказ МВД России «О деятельности органов внутренних дел по предупреждению преступлений» от 17.01.2006 № 19 // Справочно-правовая система «Гарант». – Режим доступа: <https://base.garant.ru/1355153/>
9. ГОСТ Р ИСО/МЭК 90003-2014 «Разработка программных продуктов» от 01.01.2016 // Справочно-правовая система «Гарант». – Режим доступа: <https://base.garant.ru/71271084/>
10. ГОСТ 34.601-90. «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания» от 01.01.1992 // Справочно-правовая система «Гарант». – Режим доступа: <https://base.garant.ru/187735/>
11. ГОСТ 34.003-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» от 01.01.1992 // Справочно-правовая система «Гарант». – Режим доступа: <https://base.garant.ru/187632/>
12. ГОСТ 19.201-78 «Единая система программной документации. Техническое задание. Требования к содержанию и оформлению» от 04.03.2010 // Справочно-правовая система «Гарант». – Режим доступа: <https://base.garant.ru/70411260/>
13. ГОСТ 2.114-95. «Единая система конструкторской документации. Технические условия.» от 01.08.2008 // Справочно-правовая система «Гарант». – Режим доступа: <https://base.garant.ru/5145676/>
14. ГОСТ 34.602-89. «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы» от 01.07.2009 // Справочно-правовая система «Гарант». – Режим доступа: <https://base.garant.ru/193690/>
15. РД 50-34.698-90 «Автоматизированные системы. Требования к содержанию документов» от 01.01.1992 // Справочно-правовая система «Гарант». – Режим доступа: <https://base.garant.ru/193677/>

1.3. Список используемых сокращений

В настоящем ТЗ используются следующие сокращения:

БД – база данных;

ИБ – информационная безопасность;

МВД – Министерство внутренних дел;

МО – Машинное обучение;

ОВД –Органы внутренних дел;

ОЗУ – оперативное запоминающее устройство;

ОС – операционная система;

ПО – программное обеспечение;

ППО – прикладное программное обеспечение;

РФ – Российская Федерация;

СЗИ – система защиты информации;

СП – система прогнозирования;

СПД – сеть передачи данных;

ТЗ – техническое задание.

2. НАЗНАЧЕНИЕ И ЦЕЛЬ СОЗДАНИЯ

2.1. Назначение

Назначением системы ППСИТ является формирование прогноза уровня преступности в сфере информационных технологий.

Система ППСИТ должна обеспечить прогнозирование наиболее вероятной криминогенной обстановки с сфере информационных технологий на предстоящий год.

Результатом выполненных работ является сценарий развития криминогенной обстановки, на основе которых, будет строиться дальнейшая работа Министерства внутренних дел Российской Федерации, и её сотрудничество с другими государственными службами.

2.2. Цель создания

Цель создания системы прогнозирования преступлений в сфере информационных технологий:

- установление наиболее общих показателей, характеризующих развитие (изменение) преступности в будущем, выявление ее отрицательных и положительных тенденций и отыскание на этой основе способов изменения или стабилизации этих тенденций в нужном для общества и государства направлении.

В результате создания системы ППСИТ должно быть обеспечено:

- выявление возможных причин изменения отдельных показателей преступности (состояние, уровень, структура, динамика) в будущем;

- определение вероятности появления новых видов преступлений и «отмирания» существующих, а также причин и условий, способных оказать влияние на эти процессы;

- установление возможного появления новых категорий преступников или новых видов совершения преступления изучаемой направленности;

- выбор оптимального пути совершенствования деятельности органов, ведущих борьбу с преступностью;

- разработка планов по предупреждению и профилактике спрогнозированных преступлений.

2.3. Актуальность разработки

Актуальность разработки обусловлена ценностью прогнозирования преступности, так как прогнозирование позволяет приготовить научную базу для принятия перспективных решений в борьбе с преступностью, предположить сведения о будущем, которые употребляются в перспективном планировании становления и деятельности правоохранительных органов, на базе которых случается своевременное, упреждающее изменение расстановки сил и средств нареченных органов, направлений их деятельности.

3. ТРЕБОВАНИЯ К РАЗРАБОТКЕ И СИСТЕМЕ

3.1. Технические требования

Система в совокупности с механизмом поддержки функциональных подсистем не должна накладывать каких-либо существенных ограничений на информационные технологии, используемые в проекте.

Архитектура системы должна обеспечивать реализацию функций безопасности на всех этапах функционирования ПО, с целью недопущения неправомерного доступа и эксплуатации данной системы.

Эффективность системы должна достигаться комплексным применением различных средств и методов, а также аналитической работы уполномоченных сотрудников подразделений.

В системе должны использоваться только СЗИ сертифицированные в установленном порядке на соответствие функциональным требованиям ИБ в системе сертификации ФСТЭК России и ФСБ России.

При использовании СЗИ несертифицированных по требованиям ИБ, исполнитель должен провести процедуру сертификации.

Технические требования:

- ОС: Wi№dows 7 и новее

- ОЗУ: 2 Гб

- Свободное дисковое пространство: 1 Гб

- Процессор: I№tel Pe№tium 4 2,4 ГГц/AMD Athlo№ 64 2800+

3.2. Функциональные требования

При проектировании системы и выполнении пуско-наладочных работ СЗИ должны быть реализованы следующие режимы функционирования:

- режим установки и конфигурирования;

- режим отладки;

- рабочий режим;

- режим анализа и вывода данных.

Режим конфигурирования предназначен для первичной настройки системы. В этом режиме должно происходить настраивания системы, путем создания, редактировании и применения политик, шаблонов, настроек необходимых видов доступа. Режим установки и конфигурирования должен подразумевать работы по установке и начальной настройке установленной системы.

Режим отладки предназначен для оптимизации системы и должен выполняться на этапе ввода в эксплуатацию после режима конфигурирования.

Режим анализа и вывода данных предназначен для сверки правильности работы системы, актуальности полученных результатов и взаимосвязанной работы между анализом и выводом данных.

3.3. Требования к безопасности

Используемая система должна осуществлять защиту обрабатываемых им данных, функционировать в режиме круглосуточной работы и позволять осуществлять выполнение процедур сохранения и восстановления системы после сбоев, а также недопущение неправомерного доступа к системе пользователям не своего уровня доступа.

Размещение программного продукта на местах сотрудников должно обеспечивать его безопасное обслуживание и эксплуатацию.

3.4. Требования к алгоритму прогнозирования

Наиболее подходящим алгоритмом, на базе машинного обучения, для решения задачи исследования, является Пуассоновская регрессия.

Пуассоновская регрессия основывается на распределение Пуассона, которое является распределением дискретного типа случайных величин, представляющее из себя число событий, произошедших за определенный момент времени. Она идеально подходит для прогнозирования криминогенной обстановки.

Прогнозирование должно быть построено на корреляционном анализе, в основе которого лежит Пуассоновская регрессия, так как она имеет ряд преимуществ, в связи с тем, что переменные принадлежат распределению Пуассона, они целочисленные и неотрицательные, что подходит для прогнозирования количества преступлений.

3.5. Требования к надежности

Надежность работы системы достигается за счет отлаженности механизма обработки данных, полученных в результате сбора, и анализа достоверных источников.

Выбранные факторы должны в совокупности отражать информационную обстановку в стране, и их изменение должно напрямую влиять на уровень преступности. Для обеспечения надежности прогнозирования, статистические данные, вносимые в базу данных, должны формироваться из официальных источников.

К факторам, обязательными для прогнозирования, отнесем следующие:

- численность мужского и женского населения;

- количество безработного населения;

- процент раскрываемости преступлений;

- численность сотрудников правоохранительных органов;

- смертность населения;

- количество ранее совершенных преступлений в данной сфере;

- средний размер оплаты труда;

- уровень инфляции;

- уровень жизни населения;

- уровень цифровизации населения;

- количество компаний работающих в сфере информационных технологий;

- количество населения, получившего образование в сфере информационных технологий;

- количество известных «хакерских» сообществ;

- количество инцидентов кибербезопасности;

- количество инвестиций в сферу кибербезопасности.

Данный перечень несет неисчерпывающий характер, и в будущем возможно его дополнение или изменение. Отбор факторов, представленных в списке, должен проводиться в процессе корреляционного анализа с определением Критерия Фишера. Данные факторы имеют наибольшую значимость для прогнозирования криминальных событий. Для более точного прогноза, статистические данные необходимо брать поквартально за предыдущие 10-15 лет.

3.6. Требования к численности и квалификации сотрудников

Сотрудники, допущенные к разработке системы, должны обладать специализированными знаниями в этой области и иметь базовое образование и специализацию в сфере информационной безопасности.

3.7. Требования к интерфейсу

Интерфейс должен быть простым в освоении, удобным, учитывать предпочтения основных пользователей. Во время работы пользователям системы должны быть доступны только необходимые функции согласно их ролям в рабочих процессах. Обязательно наличие системы интерактивных подсказок пользователям.

4. ЭТАПЫ СОЗДАНИЯ И ИХ СОДЕРЖАНИЕ

4.1. Аналитический этап

Аналитический этап заключается в:

- постановке задачи;

- проектировании основных элементов продукта;

- анализе и сопоставлении процессов сбора, обработки и структурирования данных, анализе факторов, способствующих совершению преступлений в сфере информационных технологий;

- в постоянном дополнении и модификации функционала системы актуальными сведениями для уточненного анализа;

- в отборе факторов, влияющих на криминогенную обстановку в сфере информационных технологий;

- в постоянной доработке и оптимизации процессов системы и анализа данных;

- подготовку наборов данных, независимых от пользователя

- определение основных требований к безопасности системы.

4.2. Этап разработки

Этап разработки включает в себя:

- разработку интерфейса пользователя;

- разработку алгоритма работы системы;

- разработку базы данных;

- написание программы;

- тестирование системы и последующая его отладка, позволяющая выявить недостатки в программировании и достигнуть поставленной цели.

4.3. Этап настройки

Этап настройки включает в себя:

- первоначальную загрузку данных;

- проверку функционирования;

- оптимизацию работы, с учетом сформированных без данных;

- исключение срывов в выполнении программных процедур.

4.4. Тестовый этап

На этапе тестирования будет осуществляться проверка системы на предмет правильной работы системы ППСИТ.

После проведения тестирования осуществляется устранение обнаруженных ошибок в коде и доработка его до практически идеального состояния, так как неправильная работа механизма программы приведет к неточному прогнозированию.

После устранения выявленных недостатков, следует повторить данный этап и отследить тенденцию увеличения эффективности системы.

4.5. Этап ввода в эксплуатацию

На этапе ввода в эксплуатацию складывается окончательная картина взаимодействия пользователя с программой, а также определяется лояльность последнего к разработанному интерфейсу.

Неотъемлемой частью завершающего этапа разработки системы также является последующая техническая поддержка созданного продукта в процессе его эксплуатации.

5. ПОРЯДОК КОНТРОЛЯ

Порядок контроля за разработкой технического задания по созданию программного обеспечения должен быть четко определен и состоять из нескольких этапов.

5.1. Определение требований и задач:

5.1.1. Определение и анализ требований, предъявляемых к системе;

5.1.2. Уточнение целей и задач проекта;

5.1.3. Установление сроков и порядка разработки системы.

5.2. Разработка структуры технического задания:

* + 1. Описание функциональных возможностей и характеристик системы;
    2. Определение архитектуры и технологий, используемых в проекте;
    3. Разработка плана работы и распределение задач между участниками проекта.
  1. Контроль качества технического задания:
     1. Проверка соответствия предъявляемых требований и реализуемых функций;
     2. Анализ и устранение возможных противоречий и неточностей в документации;
     3. Оценка рисков, связанных с проектом, и разработка плана по их минимизации;
     4. Внесение корректировок в техническое задание на основе предложений.
  2. Утверждение технического задания:
     1. Предоставление технического задания;
     2. Внесение окончательных корректировок в техническое задание с учетом замечаний и предложений;
     3. Оформление и подписание утвержденного технического задания.
  3. Мониторинг и контроль хода разработки проекта:
     1. Регулярные совещания и отчеты по выполнению задач и этапов разработки;
     2. Своевременное выявление и решение проблем, возникающих в процессе разработки;
     3. Контроль соблюдения сроков и порядка разработки системы.
  4. Тестирование и контроль качества системы:
     1. Проведение различных видов тестирования (функциональное, нагрузочное, безопасности, и др.);
     2. Анализ результатов тестирования и определение необходимых доработок;
     3. Реализация исправлений и повторное тестирование до достижения установленных критериев качества.
  5. Реализация и внедрение системы:
     1. Подготовка и предоставление необходимой документации, включая руководства пользователя и техническую документацию;
     2. Поддержка в процессе внедрения системы и обучение пользователей.
  6. Завершение проекта:
     1. Оценка качества и соответствия системы требованиям технического задания;
     2. Завершение проекта и переход к его поддержке и развитию.

Важно отметить, что контроль за разработкой технического задания должен осуществляться в тесном сотрудничестве всех участников проекта.