

Информационно-телекоммуникационная система
**«Автоматизированная информационная система «FRONTIERA» (далее
АИС «FRONTIERA»)**

Технические требования для разработки

1. ОБЩИЕ СВЕДЕНИЯ.....	4
1.1. ОСНОВНЫЕ ПОНЯТИЯ И ОПРЕДЕЛЕНИЯ	4
1.2. ОБЩИЕ ПОЛОЖЕНИЯ	6
1.3. НОРМАТИВНО-ПРАВОВЫЕ ДОКУМЕНТЫ, ИСПОЛЬЗОВАННЫЕ ПРИ СОЗДАНИИ СИСТЕМЫ	8
2. НАЗНАЧЕНИЕ И ЦЕЛИ СОЗДАНИЯ СИСТЕМЫ	10
2.1 Цель создания системы	10
2.2 Ожидаемые результаты	11
2.3 Задачи АИС «FRONTIERA».....	11
2.4 Порядок развития системы.....	12
2.4.1 КОМПОНЕНТЫ РЕАЛИЗАЦИИ МОДЕРНИЗАЦИИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ЦЕНТРАЛЬНОГО УРОВНЯ / FRONTIERA	12
2.5 Порядок выполнения работ.....	14
3 ОБЩИЕ ТРЕБОВАНИЯ К СИСТЕМЕ	14
3.1 ОПИСАНИЕ ОСНОВНОГО ФУНКЦИОНАЛА СИСТЕМЫ.....	14
3.2 СТРУКТУРА И ФУНКЦИОНАЛЬНАЯ СХЕМА	14
3.3 ОПИСАНИЕ РОЛЕЙ ПОЛЬЗОВАТЕЛЕЙ СИСТЕМЫ И ДОСТУПОВ.....	15
3.4 ТЕХНОЛОГИЧЕСКИЙ СТЕК.....	16
4 ФУНКЦИОНАЛЬНЫЕ ТРЕБОВАНИЯ	19
4.1 БАЗОВЫЕ ФУНКЦИИ	19
4.2 Документы АИС «FRONTIERA».....	19
4.2.1 Удостоверяющие личность документы	19
4.2.2 Документ правовой единицы	20
4.2.3 Документы водителя	20
4.2.4 Документы на транспортное средство	20
4.2.5 Сопроводительные документы на груз.....	21
4.2.6 Документы Государственной санитарно-эпидемиологической службы.....	22
4.2.7 Документы Государственной ветеринарной службы	22
4.2.8 Документы Государственной фитосанитарной карантинной службы	22
4.2.9 Документы Государственной экологической инспекции	22
4.2.10 Технологические документы	22
4.3 ИНФОРМАЦИОННОЕ ПРОСТРАНСТВО АИС «FRONTIERA»	22
4.3.1 ОБЪЕКТАМИ УЧЕТА И КОНТРОЛЯ АИС «FRONTIERA» ЯВЛЯЮТСЯ:.....	22
4.3.2 Идентификация объектов АИС «FRONTIERA»	24
4.3.3 БАЗОВЫЕ СЦЕНАРИИ.....	27
4.3.4 В АИС «FRONTIERA» СОДЕРЖАТСЯ СЛЕДУЮЩИЕ ДАННЫЕ	28
4.3.5 КЛАССИФИКАТОРЫ.....	30
4.4 ИНФОРМАЦИОННАЯ ПЛОЩАДКА АИС «FRONTIERA»	31
4.5 ТЕХНОЛОГИЧЕСКОЕ ПРОСТРАНСТВО СИСТЕМЫ АИС «FRONTIERA».....	32
4.5.1 НАЗНАЧЕНИЕ И СТРУКТУРА ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОГО КОМПЛЕКСА ЦЕНТРАЛЬНОГО УРОВНЯ 33	
4.5.2 ЦЕНТРАЛЬНЫЙ БАНК ДАННЫХ.....	34

4.5.3	СТРУКТУРА ХРАНИЛИЩА ДАННЫХ	35
5	НЕФУНКЦИОНАЛЬНЫЕ ТРЕБОВАНИЯ	36
5.1	ТРЕБОВАНИЯ К НАДЕЖНОСТИ И ОТКАЗОУСТОЙЧИВОСТИ	36
5.1.1	ТРЕБОВАНИЯ К МОЩНОСТИ ПОДСИСТЕМЫ	37
5.2	ТРЕБОВАНИЯ К ИНТЕРФЕЙСУ ПОЛЬЗОВАТЕЛЯ.....	37
5.3	ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ В АИС «FRONTIERA»	37
5.3.1	ОПРЕДЕЛЕНИЕ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.....	37
5.3.2	УГРОЗЫ БЕЗОПАСНОСТИ АИС «FRONTIERA»	38
5.3.3	ОБЩИЕ ТРЕБОВАНИЯ К БЕЗОПАСНОСТИ.....	38
5.3.4	ЗАЩИТА ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА.....	39
5.3.5	ОБЕСПЕЧЕНИЕ СОХРАННОСТИ ИНФОРМАЦИИ В СЛУЧАЕ АВАРИИ.....	40
5.3.6	ЗАЩИТА ОТ ВОЗДЕЙСТВИЯ ВНЕШНИХ ФАКТОРОВ	40
5.3.7	ТРЕБОВАНИЯ К ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	40
5.4	ТРЕБОВАНИЯ К РАЗВИТИЮ И МОДЕРНИЗАЦИИ ЭЛЕМЕНТОВ СИСТЕМЫ	41
5.4.1	ТРЕБОВАНИЯ К СТАНДАРТИЗАЦИИ И УНИФИКАЦИИ	41
5.4.2	ТРЕБОВАНИЯ К ИНФОРМАЦИОННОМУ ОБЕСПЕЧЕНИЮ	42
5.4.3	ТРЕБОВАНИЯ К ВИДАМ ОБЕСПЕЧЕНИЯ.....	42
6	ПРОГРАММНО-ТЕХНИЧЕСКИЙ КОМПЛЕКС	43
6.1	ПРОГРАММНО-ТЕХНИЧЕСКИЙ КОМПЛЕКС ЦЕНТРАЛЬНОГО УРОВНЯ	43
6.2	НАЗНАЧЕНИЕ И СТРУКТУРА ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОГО КОМПЛЕКСА ЛОКАЛЬНОГО УРОВНЯ.....	43
6.2.1	ПРОГРАММНО-ТЕХНИЧЕСКИЙ КОМПЛЕКС ЛОКАЛЬНОГО УРОВНЯ	44
6.3	АДМИНИСТРАТИВНАЯ ИНФРАСТРУКТУРА	45
6.3.1	РАЗМЕЩЕНИЕ СИСТЕМЫ.....	45
6.3.2	СИСТЕМА РЕЗЕРВНОГО КОПИРОВАНИЯ И ВОССТАНОВЛЕНИЯ ПОСЛЕ АВАРИЙ.....	45
6.3.3	СИСТЕМА ЛОГИРОВАНИЯ.....	45
6.3.4	СИСТЕМА АВТОМАТИЧЕСКОГО ТЕСТИРОВАНИЯ	46
6.3.5	ПОРЯДОК КОНТРОЛЯ И ПРИЕМКИ СИСТЕМЫ	46
6.3.6	ПОДГОТОВКА И НАСТРОЙКА ТЕХНИЧЕСКОГО ОБЕСПЕЧЕНИЯ	47
6.3.7	ПОДГОТОВКА ПЕРСОНАЛА	47
	ПРИЛОЖЕНИЕ А: ОСОБЫЕ ФУНКЦИОНАЛЬНЫЕ ТРЕБОВАНИЯ	48
	ПРИЛОЖЕНИЕ В: ИНСТИТУЦИОНАЛЬНЫЕ АСПЕКТЫ	59
	ПРИЛОЖЕНИЕ С: МИНИМАЛЬНЫЕ КРИТЕРИИ ОТБОРА И КВАЛИФИКАЦИИ	60
	ПРИЛОЖЕНИЕ D: ТРЕБОВАНИЯ К ПРОЕКТНОЙ ГРУППЕ	61
	ПРИЛОЖЕНИЕ Е: ЭТАПЫ МОДЕРНИЗАЦИИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ОРИЕНТИРОВОЧНЫЕ СРОКИ	63

1. Общие сведения

1.1. Основные понятия и определения

Автоматизированная информационная система «FRONTIERA» (далее АИС «FRONTIERA») – единая интегрированная автоматизированная информационная система учета и контроля лиц, транспортных средств и товаров (грузов), пересекающих государственную и/или таможенную границу Республики Молдова. АИС «FRONTIERA» является составной частью Национальной информационной системы Республики Молдова, расположенной в сегменте «Государственное управление и безопасность» (рис. 1).



Рис. 1. Место АИС «FRONTIERA» в Национальной информационной системе.

Государственная граница – линия, отделяющая сухопутную и водную территории Республики Молдова от территории соседних государств, а вертикальная поверхность, проходящая по этой линии, разделяет ее воздушное пространство и недра от воздушного пространства и недр соседних государств.

Режим государственной границы – совокупность правовых норм, регламентируемых Законом о государственной границе Республики Молдова и другими нормативными актами, договорами (соглашениями), заключенными Республикой Молдова с соседними государствами.

Пограничный режим – комплекс мер, призванных создать необходимые условия для охраны государственной границы в пограничной полосе, а также в пограничных водах и на расположенных на этой территории островах в порядке, установленном Правительством.

Пункт пропуска через государственную границу – территория в пределах железнодорожного, автодорожного вокзала (станции), речного порта (пристани),

аэропорта (аэродрома), открытых для международного сообщения, а также иные специально оборудованные места, где осуществляется контроль и разрешается пропуск через государственную границу лиц, транспортных средств, товаров (грузов) и иного имущества.

Органы центрального публичного управления создаются в пунктах пропуска через государственную границу и содержат в нормальном порядке **контрольно-пропускные пункты** пограничных войск, таможенные и иные структуры, осуществляющие контроль за пропуском через государственную границу лиц, транспортных средств, товаров (грузов) и иного имущества.

Различают следующие **типы контрольно-пропускных пунктов**:

- международные (аэропорт Кишинэу);
- межгосударственные (Молдова - Румыния);
- локальные (для жителей приграничной зоны).

Таможенная граница – государственная граница Республики Молдова, периметры свободных зон и свободных таможенных складов.

Территория Республики Молдова составляет **единую таможенную территорию**, включающую сухопутную территорию, внутренние и территориальные воды, а также воздушное пространство над ними.

Таможенный режим – совокупность таможенных правил, определяющих статус товаров и транспортных средств в зависимости от цели коммерческой операции и назначения товаров; любой таможенный режим начинается с представления товаров и транспортных средств таможенным органам и заканчивается предоставлением таможенной свободы.

Таможенный контроль – выполнение таможенным органом операций по проверке товаров, наличия и подлинности документов; рассмотрение бухгалтерской и финансовой отчетности; досмотр транспортных средств; багажа и других перемещаемых товаров; осуществление следственных и других подобных действий в целях обеспечения соблюдения таможенных правил и других норм, касающихся товаров, находящихся под таможенным надзором.

Таможенная декларация – односторонний документ, в котором лицо выражает свое волеизъявление в форме и способами, предусмотренными таможенным законодательством относительно помещения товаров под определенный таможенный режим.

Таможенные платежи – платежи, взимаемые таможенными органами в соответствии с действующим законодательством при ввозе и вывозе товаров: таможенная пошлина, налоги (налог на добавленную стоимость, акцизы), сбор за осуществление таможенных процедур, сбор за выдачу лицензий и другие платежи.

Единый платежный ордер – сводный документ по взиманию наличными платежами по перечислению, начисленных при пересечении государственной (таможенной) границы

гражданами и правовыми единицами независимо от участия их во внешнеэкономических сделках.

Фитосанитарный контроль – совокупность мер, направленных на защиту растений и продуктов их переработки, сырья, различных грузов и т. п. от карантинных объектов.

Ветеринарный контроль – это процедура проверки животных и продуктов животного происхождения при их ввозе. Импортируемые живые животные и продукты животного происхождения представляют самый высокий уровень риска, поскольку они могут передавать серьезные заболевания людей и животных.

Санитарно-эпидемиологический контроль – совокупность мер, обеспечивающих соблюдение санитарно-гигиенических правил и норм, а также выполнение обязательных требований государственных стандартов по показателям безопасности для здоровья и жизни людей и окружающей среды.

Экологический контроль – государственный инструментальный контроль на токсичность и дымность выхлопных газов автотранспортных средств независимо от их ведомственной принадлежности и форм собственности в соответствии с экологическим законодательством и действующими стандартами.

Транспортными средствами считаются легковые автомобили, автобусы, грузовые автомобили (в том числе с прицепом), мотоциклы, мопеды, сельскохозяйственная техника, дорожно-строительная техника, железнодорожные вагоны (пассажирские или товарные), специализированные вагоны, тяговые составы (электровозы, локомотивы), суда маломерного флота.

Далее в тексте под словом «**граница**» понимается государственная и/или таможенная граница Республики Молдова.

1.2. Общие положения

Создание **Информационной Системы «Frontiera»** основано на Постановлении Правительства № 1126 от 28.08.2002 г. Об утверждении Концепции и Положения об автоматизированной информационной системе учета и контроля лиц, транспортных средств и товаров (грузов), которые пересекать государственную и / или таможенную границу.

Согласно Концепции в зоне контроля, для проведения расчетов платежей и налогов, которые необходимо уплатить при пересечении государственной границы, были расположены следующие службы:

Пограничная служба - в обязанности которой входило открытие маршрута путем ввода данных о транспортном средстве и его водителе, контроль документов, впоследствии основанный на подтверждении всеми службами, расположенными в зоне контроля, выдает разрешение на выезд из транспортной единицы;

Национальное агентство автомобильного транспорта (АНТА) - в обязанности которого входило введение в информационную систему, касательно исчисленных сумм налогов, дорог;

Санитарно-ветеринарное агентство - обязано вводить в систему данные о выданных документах, результатах проверок и рассчитанных суммах;

Фитосанитарная инспекция - в обязанности которой входило занесение в систему данных выданных документах, результатах проверок и о рассчитанных суммах;

Таможенная служба - в обязанности которой входит введение в информационную систему данных о транспортных средствах, введение информации о перевозимых товарах, формирование единой платежной квитанции и передачу через АПИ в платёжную систему М-Пэй;

Банк - подтверждение оплаты квитанции и возврат подтверждения оплаты платежа в информационную систему при помощи АПИ.

Постановлением Правительства № 1073 от 19.09.2008 г. «Об оптимизации способа пересечения государственной границы автомобильным транспортом с грузами и пассажирами» и Совместным Приказом № 202/68/372 от 17 октября 2008 г., Министерство сельского хозяйства и пищевой промышленности, Главная государственная инспекция по фитосанитарному карантину, Национальное агентство автомобильного транспорта, экологического контроля и Таможенная служба Республики Молдова регламентировали процедуры оптимизации проезда государственной границы автомобильным транспортом с товарами, подлежащими санитарному контролю - ветеринарными и фитосанитарными, экологическими платежами, проверкой транспортных документов АНТА - по принципу **единого окна**.

Поэтому Таможенная служба поручила Гос.предприятию Вамтехинформ как можно скорее разработать инструмент для автоматического расчета экологических платежей и дорожных сборов, который впоследствии будет доступен таможенным инспекторам на пограничных постах. Основываясь на четко определенных требованиях к функциональности новой системы, отсутствие каких-либо дополнительных требований на будущее при разработке системы в дальнейшем, привело к созданию системы, основанной на структурированном программировании с использованием языка программирования Java и WEB-технологий.

Со временем ИС «Frontiera» претерпела большое количество расширений функциональных возможностей системы. ИС «Frontiera» не проектировалась как модульная система и, как следствие, любое функциональное дополнение требует большего объема человеческих ресурсов и времени. В то же время добавленные функциональные возможности подчиняются тому же принципу одного шага.

Принципы, основанные на ИС «Frontiera», не предлагали управление, настройку, безопасность, администрирование, аудит системы, не предусматривалось расширение системы за счет добавления новых модулей.

В результате мы вынуждены констатировать, что новые требования к существующей ИС «Frontiera» не могут быть выполнены без пересмотра технологии и принципов, на которых она была создана. Структура текущего положения ИС «Frontiera» представлена ниже.

В этом документе приведены технические и качественные характеристики системы, перечень и сроки предоставления услуг по разработке и внедрению системы управления автомобильными пунктами пропуска. Требования указаны в данном документе не являются исчерпывающими и в них могут вноситься уточнения или не существенны изменения в процессе разработки продукта.

Реализована система должна отвечать следующим основным требованиям:

- веб-ориентированная;
- универсальная;
- функционально достаточна (полная)
- надежная (автоматически сохранения всех данных и корректное завершение работы программ без потери данных);
- пригодна к модернизации и масштабирования;
- модульная;
- иметь интуитивно понятный пользовательский интерфейс;
- защищена от внешних воздействий;
- осуществлять документирование всех действий пользователей системы.

1.3. Нормативно-правовые документы, использованные при создании системы

Целью формирования нормативно-правовой базы АИС «FRONTIERA» является создание необходимых организационно-правовых условий обеспечивающих разработку и использование комплексной интегрированной автоматизированной информационной системы учета и контроля лиц, транспортных средств и товаров (грузов), пересекающих границу Республики Молдова. Правовое обеспечение АИС «FRONTIERA» базируется на нормативно-правовых актах, регламентирующих существующую систему учета и контроля объектов регистрации, а также процессы информатизации и формирования единого информационного пространства Республики Молдова.

Основными нормативно-правовыми актами, регламентирующими создание и функционирование АИС «FRONTIERA», являются:

- Конституция Республики Молдова;
- Закон о санитарно-эпидемиологическом обеспечении населения № 1513-XII от 16 июня 1993 года;

- Закон о государственной границе Республики Молдова № 108-XIII от 17 мая 1994 г.;
- Закон о бюджете (принимается ежегодно);
- Закон об удостоверяющих личность документах национальной паспортной системы № 273-XIII от 9 ноября 1994 г.;
- Закон о правовом положении иностранных граждан и лиц без гражданства в Республике Молдова № 275-XIII от 10 ноября 1994 г.»;
- Закон о фитосанитарном карантине № 506-XIII от 22 июня 1995 г.;
- Закон о государственной безопасности № 618-XIII от 31 октября 1995 г.;
- Закон о выезде из Республики Молдова и въезде в Республику Молдова № 269-XIII от 9 ноября 1995 г.;
- Таможенный кодекс, принятый законом № 1149-XIV от 20 июля 2000 г.;
- Закон Республики Молдова о зонах свободного предпринимательства № 440-XV от 27 июля 2001 г.;

Постановления Правительства Республики Молдова:

- № 496 от 6 сентября 1991 г. «О создании контрольно-пропускных и таможенных пунктов»;
- № 1052 от 8 ноября 1999 г. «О регулировании деятельности служб в пограничных контрольно-пропускных пунктах»;
- № 808 от 9 августа 2000 г. «О взаимодействии служб, упорядочении взимания платежей и автоматизации системы учета при осуществлении контроля в пунктах пропуска на государственной границе Республики Молдова»;
- № 903 от 30 августа 2001 г. «О разработке и внедрении информационной системы учета и контроля транзита перевозок»;
- № 1009 от 27 сентября 2001 г. «О предотгрузочной инспекции импортируемых товаров»;
- Положение о постах экологического контроля и диагностики автотранспортных средств на территории Республики Молдова от 18 июля 1996 г. (Министерство транспорта и связи);
- другие ведомственные нормативные акты.

В то же время создание и эффективное функционирование АИС «FRONTIERA» требуют принятия новых законов и совершенствования действующего законодательства, которые регулировали бы отношения, возникающие при сборе, обработке, хранении, выдаче и защите данных, а также устанавливали бы правовой режим функционирования АИС «FRONTIERA».

2. Назначение и цели создания системы

АИС «FRONTIERA» создается преимущественно в целях обеспечения безопасности Республики Молдова в частности путем борьбы с незаконным импортом - экспортом товаров, предупреждения фальсификации товаров и подделки документов, осуществления контроля за незаконной миграцией, выявления лиц и транспортных средств, которым запрещен въезд в страну и выезд из нее.

Основными целями создания АИС «FRONTIERA» являются:

- обеспечение экономического суверенитета Республики Молдова путем установления оптимально прозрачной границы;
- увеличение поступлений в национальный бюджет в результате строгого контроля за импортом-экспортом и транзитом товаров;
- повышение уровня стабильности внутри государства посредством регистрации и проверки физических лиц, пересекающих границу, а также контроля притока иностранных граждан и лиц без гражданства;
- усиление борьбы с преступностью путем эффективного противодействия организованной преступности, нелегальной миграции, наркобизнесу, незаконному провозу оружия и иным противоправным деяниям в пунктах перехода границы;
- повышение пропускной способности контрольно-пропускных пунктов;
- обеспечение эффективного сотрудничества и взаимодействия между заинтересованными министерствами и департаментами по вопросам регистрации и контроля.

2.1 Цель создания системы

АИС «FRONTIERA» создается на следующих основных принципах:

- принцип **легитимности** системы, предполагающий создание и использование АИС «FRONTIERA» в соответствии с положениями внутреннего действующего законодательства;
- принцип **соблюдения прав человека**, предусматривающий эксплуатацию указанной системы в строгом соответствии с национальными нормативными документами, в пределах положений договоров и соглашений по правам человека, стороной которых Республика Молдова является;
- принцип **первого лица/одного центра**, требующий наличия руководителя высокого ранга, обладающего достаточными полномочиями для принятия решений и координации работ по созданию и эксплуатации системы;
- принцип **обоснованности данных** системы, предписывающий введение данных в систему только на основании записей в документах, принятых в качестве источника информации;
- принцип **целостности, полноты и достоверности данных**, где:
 - под целостностью данных понимается такое их состояние, когда они сохраняют содержание и однозначность интерпретации в условиях влияния случайных

факторов. Целостность данных считается сохраненной, если они не искажены и не разрушены (не стерты);

- под **полнотой данных** понимается объем информации, собираемой об объектах учета и контроля системы в соответствии с нормативными актами;

- под **достоверностью данных** понимается степень соответствия информации, хранимой в памяти ЭВМ или в документах, реальному состоянию отображаемых ими объектов конкретной области системы;

- принцип **государственной идентификации объектов регистрации**, согласно которому объектами идентификации являются физические лица, транспортные средства пересекающие границу, у каждого из которых проверяется государственный идентификационный номер (например у физического лица - государственный идентификационный номер физического лица, а у правовой единицы – государственный идентификационный номер правовой единицы);

- принцип **контроля за формированием и использованием системы**, осуществляемый посредством целого ряда технико-организационных мер и программ применения, призванных обеспечить высокое качество государственных информационных ресурсов, высокую надежность их хранения и управления ими, в том числе правильность использования их в соответствии со стандартами, предусмотренными действующим законодательством;

2.2 Ожидаемые результаты

Ввод в эксплуатацию системы позволит:

- существенно ускорить процесс пересечения транспортными средствами пунктов пропуска.
- повысить безопасность вследствие недопущения въезда или выезда транспортных средств и лиц, к которым есть вопросы у правоохранительных органов;
- получить инструмент для контроля нахождения транспортных средств на пунктах пропуска;
- получить инструмент для онлайн-мониторинга и работы с архивами во всех пунктах пропуска;
- минимизировать человеческий фактор;
- обеспечить прозрачность деятельности таможенных органов на пунктах пропуска;
- ввести единые, понятные и прозрачные правила и процедуры на пунктах пропуска;
- унифицировать перечень данных, которые будут фиксироваться пользователями системы по каждому транспортному средству при пересечении границы.

2.3 Задачи АИС «FRONTIERA»

На АИС «FRONTIERA» возлагаются следующие задачи:

- обеспечение руководства республики достоверной и оперативной информацией о въезде/выезде лиц и транспортных средств и импорте/экспорте

товаров, необходимой для принятия продуманных решений на государственном уровне;

- обеспечение автоматизированного учета и контроля лиц, транспортных средств и товаров, пересекающих границу;
- обеспечение автоматизированного учета и контроля представляемых документов;
- выявление лиц, не имеющих права на въезд в Республику Молдова и выезда из нее, а также транспортных средств и товаров, запрещенных к ввозу в страну или вывозу из нее;
- повышение пропускной способности пунктов пропуска путем внедрения машиночитаемых документов и компьютерных справочников;
- повышение уровня обслуживания посредством ускорения процедур регистрации, контроля и взимания установленных таможенных пошлин и налогов;
- создание единого интегрированного банка данных о пересечении границы лицами, транспортными средствами и товарами;
- обеспечение ведомственных информационных систем достоверной и оперативной информацией о пересечении границы лицами, транспортными средствами и товарами;
- обеспечение нормального функционирования системы в непрерывном режиме.

2.4 Порядок развития системы

2.4.1 Компоненты реализации модернизации программного обеспечения центрального уровня / Frontiera

Базовая конфигурация модернизации АИС состоит в внедрении микросервисной архитектуры вместо монолитной модели и замене сервера приложений для обеспечения масштабируемости и повышения безопасности. Достижение масштабируемости достигается внедрением микросервисной модели. На практике это обозначает что для того, чтобы добавить или изменить функционал какого-то из модулей не будет необходимости каждый раз пересобирать ядро системы. Что в свою очередь снизит затраты на развитие и сопровождение системы так как для ее развития можно будет привлекать разные команды разработчиков на небольшие задачи. Так же существующее решение JBOSS уже находится вне поддержки производителя, то есть уязвимости НЕ отслеживаются и НЕ исправляются. Что на практике обозначает повышенную уязвимость ПО, которую приходится компенсировать дополнительными затратами (покупать более дорогое сетевое оборудование и программное обеспечение для защиты от угроз пропорционально степени уязвимости корневой системы).

Этапы разработки
Модернизация архитектуры приложения с заменой сервера приложений
Модернизация конструктор отчетов
Модернизация модуля обмена с внешними системами
Вынесение модуля обмена информацией с другими участниками в Mconnect (министерства, ведомства)
Модуль «Авто» - будет брать данные из Пограничной полиции или ручной регистрации, или из других внешних систем (считыватели номеров, системы электронных билетов и др .) И добавлять дополнительные данные для дальнейшей обработки;
Модуль «АНТА» - обеспечит функции проверки документов выданных «АНТА» для выполнения международных перевозок, и расчета дорожного налога в согласовании с Действующим законодательством;
Модуль «Банк» - ведение счетов по налогам и Таможенным платежам. Обмен информацией с Web Service «Единое окно таможенное службы для оплаты»;
Модуль ANSA (Национальное Агентство по Безопасности продуктов питания)
Модуль Ветеринарная служба

По состоянию на 2021 год в законодательстве республики Молдова произошли изменения, касающиеся правил взаимодействия между государственными информационными системами. Была внедрена система MConnect.
<https://www.egov.md/ru/projects/mconnect>

Правительственная платформа взаимодействия MConnect - облегчает обмен данными между органами власти и повышает качество и эффективность обмена данными между государственными структурами. С помощью платформы взаимодействия, государственные органы обмениваться данными в режиме реального времени, что уменьшает число затребованных документов от физических и юридических лиц в виде справок, отчетов и т.д.

ПРЕИМУЩЕСТВА:

- повышение эффективности информационных систем, которые обеспечивают электронные государственные услуги;
- повышение эффективности использования государственных средств;
- повышение комфорта людей;
- повышение безопасности информационных систем центрального и местного публичного управления;
- повторное использование ресурсов, вовлеченных в рамках информационных систем;
- улучшение сотрудничества между государственными учреждениями;
- продвижение веб-доступности;

В связи с этой законодательной инициативой обмен с внешними системами не может производиться в действующей системе так как первоначально не существовала данная платформа обмена.

На сегодняшний день обмен должен производиться только через платформу **MConnect**, что требует модернизацию решения в части модулей обменов с другими участниками внутри страны так и с внешними партнёрами.

2.5 Порядок выполнения работ

Помимо комплексной модернизации ядра системы, сценарий включает обновление ключевых модулей, необходимых для таможенной службы Республики Молдова.

Ожидаемый результат:

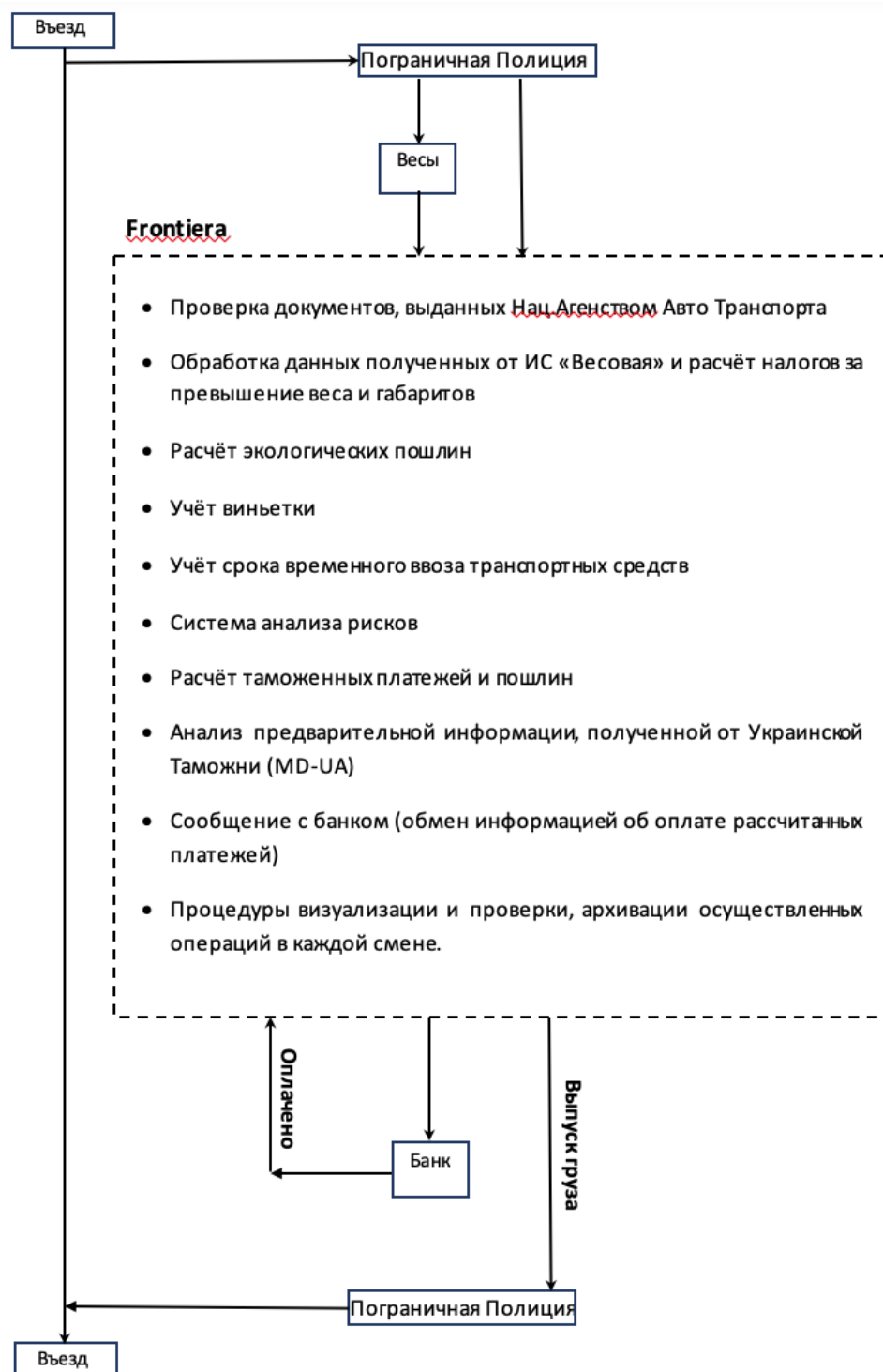
- для достижения исключительной гибкости, легкости управления, надежности и безопасности будет разработано комплексно модернизированное ядро системы
- разработан алгоритм и создан механизм управления системой комплексного видеонаблюдения включающий в себя ANPR и CC TV
- АИП отвечает современным требованиям по безопасности Топ-10 OWASP
- создан новый модуль, согласно требованиям законодательства механизм электронного взаимодействия с другими государственными институтами в том числе с внедрением MConnect
- модернизирован модуль информационного обмена с Украиной

3 Общие требования к системе

3.1 Описание основного функционала системы

Система должна обеспечивать создание, обновление, наполнение записей о движении транспортных средств по территории пункта пропуска и реализация смежного функционала п. 3.5.

3.2 Структура и функциональная схема



3.3 Описание ролей пользователей системы и доступов

В рамках системы должно быть настроена ролевая модель пользователей с возможностью разграничения прав доступа и возможностью создавать неограниченное количество пользователей каждой роли.

3.4 Технологический стек

Для достижения Исключительной гибкости, легкости управления, надежности и безопасности были выбраны из существующих технологии наиболее проверенные, современные и доступные. Также нужно заметить, что внедрение новых компонентов в интегрированную инфосистему Таможенной Службы Молдовы может заменить часть существующих, но при условии сохранения функционала и без падения производительности. Так, к примеру, была выбран технология виртуализации на основе Docker + Kubernetes, также предлагается заменить монолитную JBOSS архитектуру на сервисную архитектуру и разработать пользовательские интерфейсы с внедрением современных решений, к примеру, Заменяя JSP на React. Все эти меры Должны привести к созданию так называемое future proof системы, которая будет употребляться длительное время, предоставит переиспользуемые компоненты и улучшит общее качество инфосистемы Таможенной Службы Молдовы.

Технологии:

Proxy Server - обратный прокси-сервер необходим для безопасного и отказоустойчивого подключения пользователей из внешней сети.

Kubernetes cluster - необходим для автоматизации развертывания, масштабирования контейнеров Docker.

Docker container - приложение со всем его окружением и зависимостями, Которым можно легко и просто управлять: переносит на другой сервер, масштабировать, обновлять.

Frontend / Backend - модульный подход, основанный на использовании распределённых, слабо связанных компонентов, оснащённых стандартизированными интерфейсами для взаимодействия по стандартизированным протоколам.

Apache Kafka - распределённая, горизонтально масштабируемая система, обеспечивающая пропускную способность при росте нагрузки. Также поддерживается возможность временного хранения данных для последующей пакетной обработки. Одной из особенностей является применение техники, сходной с журналами транзакций, используемыми в системах управления базами данных, позволяя дополнительно защитить и гарантировать доставку данных.

React - библиотека с открытым исходным кодом для разработки пользовательских интерфейсов. Его цель - ПРЕДОСТАВИТЬ Высокую скорость, простоту и масштабируемость.

Spring Boot - набор инструментов, Которые автоматизируют процедуру настройки и ускоряют процесс создания и развертывания Spring -приложений.

Функциональные компоненты:

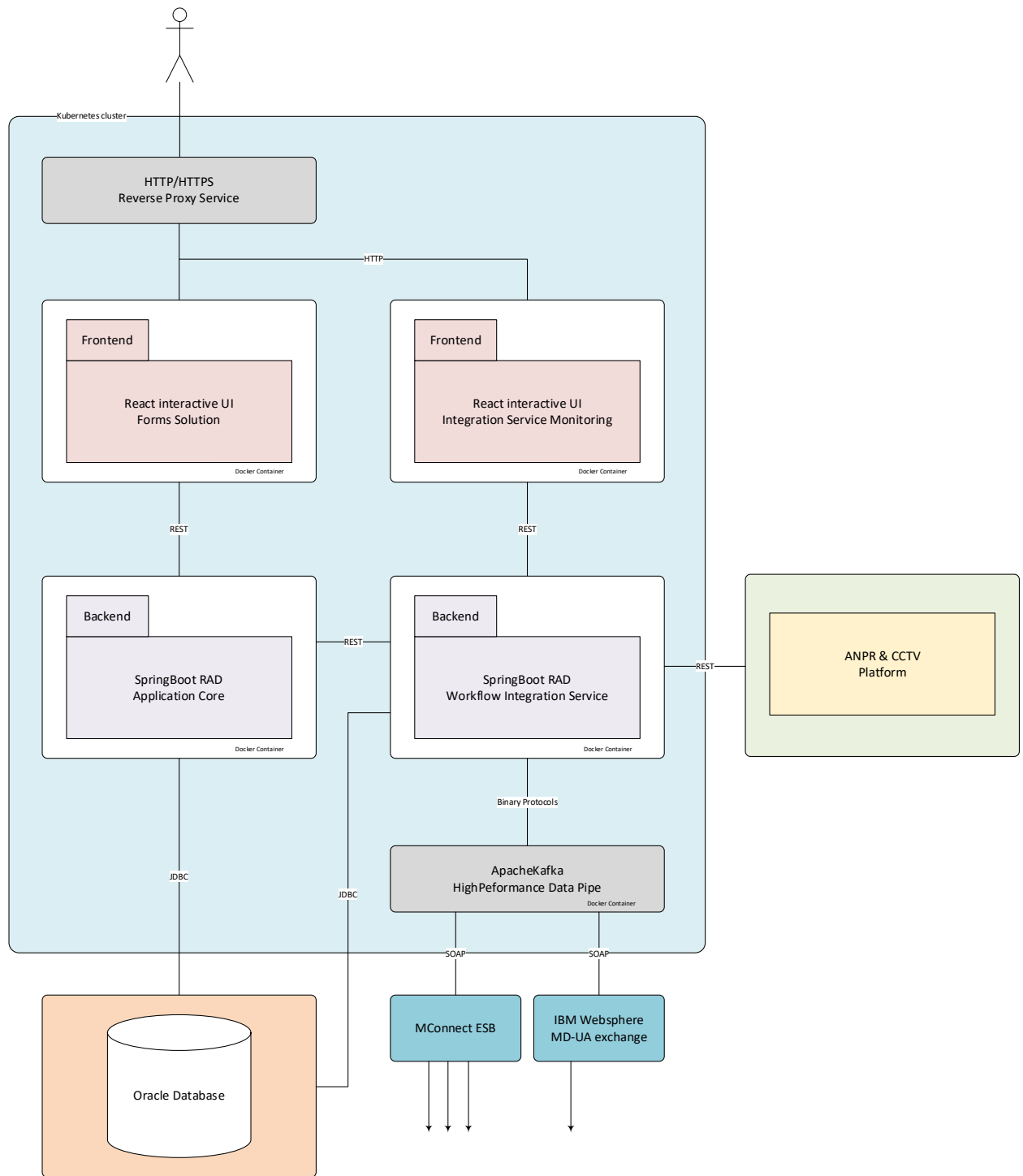
Forms Solution - современное web-приложение, которое включает в себя пользовательские возможности доступа к ANPR & CCTV и т. Д.

Integration Service Monitoring - приложение для мониторинга процессов обмена данными, общих системных параметров.

Application Core - приложение, которое обеспечивает абстракцию бизнес-логики, предоставляет интерфейсы для пользовательских приложений.

Workflow Integration Service - приложение, которое обеспечивает агрегации и обработку данных для связи с внешними системами, в том числе ANPR & CCTV.

ANPR & CCTV - внешняя система, которая интегрируется при помощи стандартных интерфейсов. Для этой интеграции специальные возможности предоставляются через Workflow Integration Service.



4 Функциональные требования

4.1 Базовые функции

Базовыми функциями АИС «FRONTIERA» являются:

а) формирование банка данных, включающее функции первоначального взятия объекта на учет, актуализации данных и снятия с учета. Данные функции осуществляются в ходе сбора данных об объектах учета, выдаче таможенных документов, при регистрации, а также при информационном обмене с руководящими органами государства и органами местного публичного управления.

В банк данных АИС «FRONTIERA» информация вносится только на основании документов, подтверждающих достоверность сведений об объекте учета, с четкой ссылкой на документ, на базе которого произошла актуализация данных;

б) организация информационного обеспечения из банка данных;

с) обеспечение качества информации за счет создания и поддержания компонентов системы качества;

д) всестороннее обеспечение функционирования АИС «FRONTIERA».

Конкретные функциональные требования для расширения и обновления АИС «Frontiera» включены в Приложение А: Функциональные требования.

4.2 Документы АИС «FRONTIERA»

Документы, учитываемые в АИС «FRONTIERA», подразделяются на следующие категории:

- документы, удостоверяющие личность;
- документы правовой единицы;
- документы водителя;
- документы на транспортное средство;
- сопроводительные документы на товары (грузы);
- единый платежный ордер;
- документы Государственной санитарно-эпидемиологической службы;
- документы Государственной ветеринарной службы;
- документы Государственной фитосанитарной карантинной службы;
- документы Государственной экологической инспекции;
- технологические документы.

4.2.1 Удостоверяющие личность документы

К удостоверяющим личность документам относятся:

- документы Национальной паспортной системы Республики Молдова:
 - паспорт гражданина Республики Молдова;
 - дипломатический паспорт;
 - служебный паспорт;
 - паспорт лица без гражданства;
 - удостоверение личности гражданина Республики Молдова;
 - удостоверение личности лица без гражданства;
 - вид на жительство иностранного гражданина, постоянно проживающего в Республике Молдова;
 - временный вид на жительство лица без гражданства;
 - временный вид на жительство иностранного гражданина;
 - паспорт моряка;
- национальные паспорта иностранных граждан;
- справка посольства иностранного государства в Молдове, выданная взамен утерянного документа;
- свидетельство о возвращении в Республику Молдова.

4.2.2 Документ правовой единицы

При пересечении границы представитель правовой единицы представляет следующие документы:

- машиночитаемую регистрационную карточку правовой единицы;
- договор или копию договора;
- регистрационные документы иностранной правовой единицы.

4.2.3 Документы водителя

При пересечении границы водитель транспортного средства обязан представить удостоверение на право управления транспортным средством.

При выполнении международных автомобильных перевозок, в том числе транзита, водитель дополнительно должен предъявить следующие документы:

- книжку регистрации валюты транспортных служащих или справка на ввоз иностранной валюты;
- медицинский страховой полис водителя транспортного средства;
- личную контрольную книжку водителя (при отсутствии или неисправности тахографа на автомобиле);
- удостоверение водителя-международника (центра CIPIT);
- свидетельство о соответствующей квалификации водителя (только при перевозке опасных грузов).

4.2.4 Документы на транспортное средство

При пересечении границы на транспортном средстве представляются следующие документы:

- свидетельство о регистрации транспортного средства;
- талон о прохождении технического тестирования;
- свидетельство о страховании гражданской ответственности;
- удостоверение таможни (выдается при первичном ввозе автотранспортного средства в Республику Молдова).

При выполнении международных автомобильных перевозок (в том числе транзите) дополнительно предъявляются следующие необходимые документы на транспортное средство:

- свидетельство о пригодности транспортного средства к международной перевозке товаров (грузов), выданное на условиях конвенции МДП (с фотографиями);
- разрешение на выполнение перевозки по иностранной территории;
- свидетельство о допуске транспортного средства к перевозкам опасных грузов (только при перевозке таких грузов);
- лицензионная машиночитаемая карточка;
- путевой лист (копия договора на перевозку или тетрадь учета доходов);
- бортовой журнал (для государств, где это требуется).

При пересечении границы железнодорожным транспортом представляется передаточная ведомость (на каждый железнодорожный состав).

4.2.5 Сопроводительные документы на груз

При выполнении перевозок (в том числе транзитом) дополнительно предъявляются следующие сопроводительные документы на груз:

- заявка на предотгрузочное инспектирование импортируемой продукции;
- отчет о положительных результатах инспекции или отчет о расхождениях (используется таможенными органами Республики Молдова для упрощения оформления таможенных документов при ввозе материальных ценностей в страну), защитный ярлык (для оплаты);
- таможенная декларация для юридического лица;
- таможенная декларация для физического лица;
- свидетельство о происхождении, качестве и соответствии товаров;
- счет фактура (инвойс), где указаны количество и стоимость товаров;
- товарно-транспортная накладная на перевозимые товары, где указывается транспорт (дорожный, воздушный, железнодорожный и др.);
- доверенность, выданная физическому лицу, которое занимается импортом/экспортом товаров;
- товарно-транспортные накладные CMR со спецификациями и другими необходимыми сопроводительными документами;
- оформленные книжки TIR;
- страховка ответственности перевозчиков (копия страхового полиса);
- справка Торгово-промышленной палаты.

4.2.6 Документы Государственной санитарно-эпидемиологической службы

- различные справки.

4.2.7 Документы Государственной ветеринарной службы

- ветеринарный сертификат;
- санитарное разрешение.

4.2.8 Документы Государственной фитосанитарной карантинной службы

- фитосанитарный пропуск;
- санитарное разрешение.

4.2.9 Документы Государственной экологической инспекции

- экологический сертификат.

4.2.10 Технологические документы

- различные справки;
- различного рода аналитические и статистические отчеты;
- доверенность на право сопровождения физического лица.

4.3 Информационное пространство АИС «FRONTIERA»

АИС «FRONTIERA», как и любая другая информационная система, формируется из неделимого ядра, которое включает данные всех объектов учета и контроля и сценарии, по которым они взаимодействуют (рис. 4). Формирование поля данных осуществляется путем приведения в действие атрибутов данных объектов в результате их взаимодействия по штатным сценариям цикличного характера.

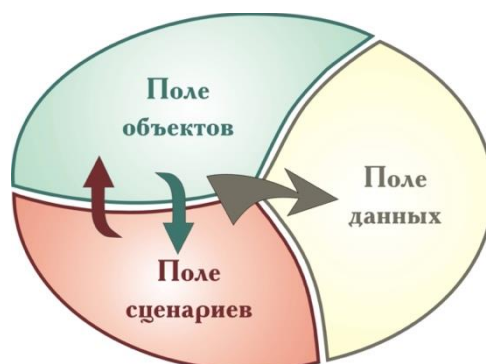


Рис. 4. Структура информационного ядра АИС «FRONTIERA».

4.3.1 Объектами учета и контроля АИС «FRONTIERA» являются:

1) рейс – понятие, объединяющее в себе:

- факт пересечения границы;

- транспортное средство, пересекшее границу;
- физическое лицо, управляющее этим транспортным средством;
- физических лиц - пассажиров данного транспортного средства;
- товары (грузы), перевозимые на данном транспортном средстве;
- правовую единицу, ответственную за соответствующие товары (грузы) (получатель/отправитель, владелец груза).

Пересечение границы пешеходом или велосипедистом также считается отдельным рейсом;

2) физические лица следующих категорий:

- иностранные граждане и лица без гражданства, постоянно проживающие на территории Республики Молдова;
- граждане Республики Молдова, постоянно проживающие за рубежом;
- граждане Республики Молдова, въезжающие в Республику Молдова или выезжающие из нее;
- лица без гражданства и иностранные граждане, временно находящиеся на территории Республики Молдова;

3) Правовые единицы следующих категорий:

- органы публичной власти;
- предприятия;
- общественные объединения;
- партии и общественно-политические организации;
- профессиональные союзы;
- кооперативы (ассоциации кооперативов);
- части религиозных культов;
- ассоциации совладельцев в кондоминиуме;

4) транспортные средства:

- автомобили (в том числе с прицепом);
- автобусы
- грузовые автомобили (включительно с прицепом);
- мотоциклы;
- сельскохозяйственная техника, техника для дорожного строительства и содержания дорог;
- железнодорожные вагоны (пассажирские или товарные);
- специальные вагоны;
- тяговые составы (электровозы, локомотивы), пересекающие границу на собственном ходу или с помощью буксировки;

5) товары (грузы).

6) документы:

- документы, удостоверяющие личность;
- документы визового режима;
- документы правовой единицы;
- документы водителя;
- документы на транспортное средство;
- документы на груз;
- единый платежный ордер;
- документы, выданные санитарно-эпидемиологической, ветеринарной, фитосанитарной карантинной и экологической службами.

7) бланки документов строгой отчетности.

4.3.2 Идентификация объектов АИС «Frontiera»

Основными идентификационными признаками каждого объекта учета и контроля АИС «Frontiera» являются идентификатор рейса, государственный идентификационный номер физического лица (IDNP), государственный идентификационный номер правовой единицы (IDNO, используемый по международной практике аббревиатурой слов на английском языке «Identification Number of Organization»), идентификационный номер транспортного средства (VIN-cod, используемый по международной практике аббревиатурой слов на английском языке «Vehicle Identification Number»), код товара по товарной номенклатуре.

Идентификация рейса

Идентификатор рейса представляет собой строго определенную последовательность 13 цифр (рис. 5):



Рис.5. Содержание символов идентификатора рейса.

Идентификация физического лица

Государственный идентификационный номер физического лица (IDNP) является основным признаком идентификации физического лица и представляет собой строго определенный порядок 13 буквенно-цифровых символов (рис. 6).



Рис.6. Содержание символов Государственного идентификационного номера физического лица.

Идентификация правовой единицы

Основным идентифицирующим признаком правовой единицы является Государственный идентификационный номер правовой единицы (IDNO), представляющий собой строго определенный порядок 13 буквенно-цифровых символов (рис. 7).

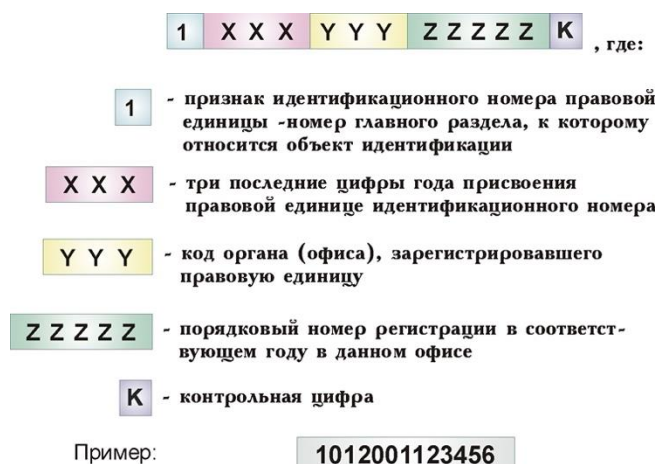


Рис. 7. Содержание символов Государственного идентификационного номера правовой единицы

Идентификация транспортного средства

Основным идентификационным признаком транспортного средства является идентификационный номер транспортного средства (VIN-cod), представляющий собой уникальный номер транспортного средства, нанесенный производителем в соответствии с требованиями стандартов ИСО 3779-76 «Автомобили. Международный идентификационный номер» и ИСО 3780-76 «Автомобили. Международный идентификационный код производителей» (рис. 8).

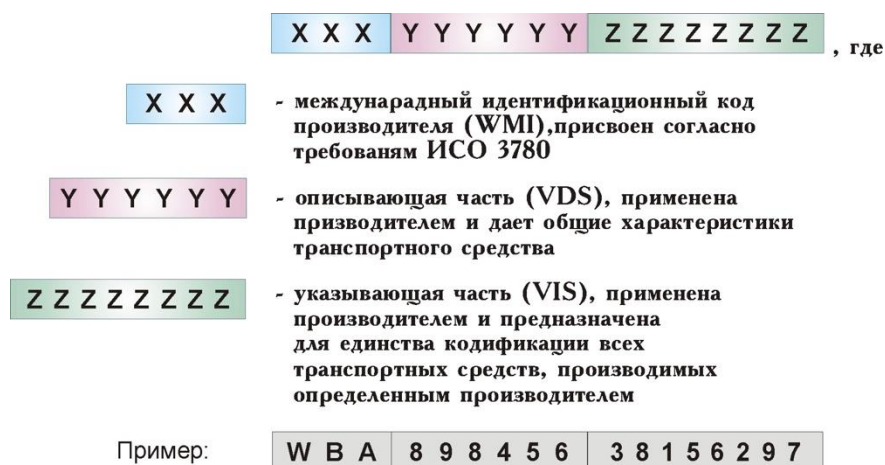


Рис. 8. Содержание символов VIN-cod.

Если VIN-cod не нанесен производителем транспортного средства, фальсифицирован или уничтожен, он присваивается и наносится при оформлении допуска к эксплуатации. Номерные агрегаты идентифицируются следующим образом:

тип + номер

Идентификация товаров

Идентификация товаров осуществляется путем их кодирования в соответствии с национальной номенклатурой товаров. Код представляет собой строгую последовательность 9 цифр (рис. 9):

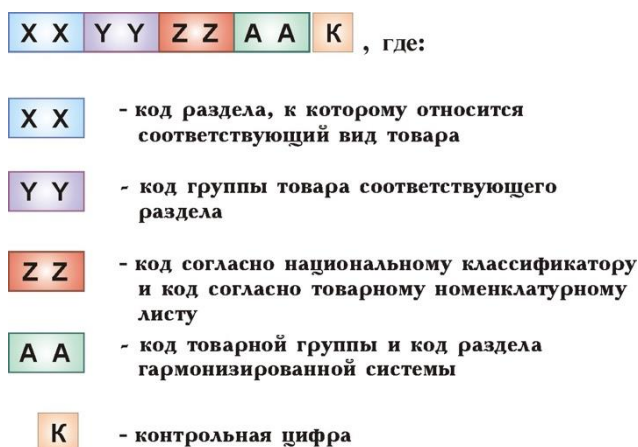


Рис.9. Содержание разрядов кода товаров

Способ идентификации единицы товара будет определен после разработки автоматизированной информационной системы «Товарооборот».

Идентификация документов и бланков строгой отчетности

Идентификация документов и бланков строгой отчетности осуществляется по комбинированному ключу, включающему следующие элементы:
код документа + серия + номер.

4.3.3 Базовые сценарии

Реализация функций АИС «FRONTIERA» в ходе учета и контроля объектов при пересечении границы осуществляется по следующим базовым сценариям:

1) рейс:

- идентификация (присвоение идентификационного номера);
- определение состава рейса;
- осуществление сценариев для участников рейса;
- внесение всех платежей по единому платежному ордеру;
- принятие решений по рейсу на основании решений, принятых по его участникам;
- занесение информации в базу данных;

2) физическое лицо:

- идентификация (если не фигурирует в Государственном регистре населения – регистрация в этом регистре с присвоением IDNP);
- оформление визы (в случае необходимости при ее отсутствии);
- определение статуса лица в данном рейсе;
- определение мотива пересечения границы;
- контроль представленных документов;
- проверка документов по фильтрационным массивам;
- заполнение таможенной декларации для физического лица (в случае необходимости);
- принятие решения по лицу;
- занесение информации в базу данных;

3) правовая единица:

- идентификация (если нет в Государственном регистре правовых единиц – регистрация в этом регистре с присвоением IDNO);
- определение роли правовой единицы в данном рейсе и ее полномочий;
- контроль представленных документов;
- проверка документов по фильтрационным массивам;
- принятие решения по правовой единице;
- занесение информации в базу данных;

4) транспортное средство:

- идентификация (если нет в Государственном регистре транспорта – регистрация в этом регистре);
- определение мотива пересечения границы;
- контроль представленных документов;
- проверка документов по фильтрационным массивам;
- применение различных видов контроля и оформление соответствующих документов;
- исчисление необходимых таможенных платежей;
- принятие решения по транспортному средству;

- занесение информации в базу данных;

5) товары (грузы):

- идентификация (идентификационный код товаров);
- определение основания для перемещения через границу;
- проверка представленных документов;
- заполнение таможенной декларации для правовой единицы;
- осуществление необходимых видов контроля и оформление соответствующих документов;

- опломбирование (при въезде в пункт пропуска) и контроль сохранности пломб (при выезде);

- исчисление необходимых таможенных платежей;
- принятие решения по товару;
- занесение информации в базу данных;

7) документы:

- идентификация;
- контроль;
- изъятие в случае необходимости;
- отметки о недействительности;
- занесение информации в базу данных.

Практическое применение сценариев осуществляется сотрудниками соответствующих служб, в соответствии с действующим законодательством и ведомственными приказами и инструкциями.

4.3.4 В АИС «FRONTIERA» содержатся следующие данные

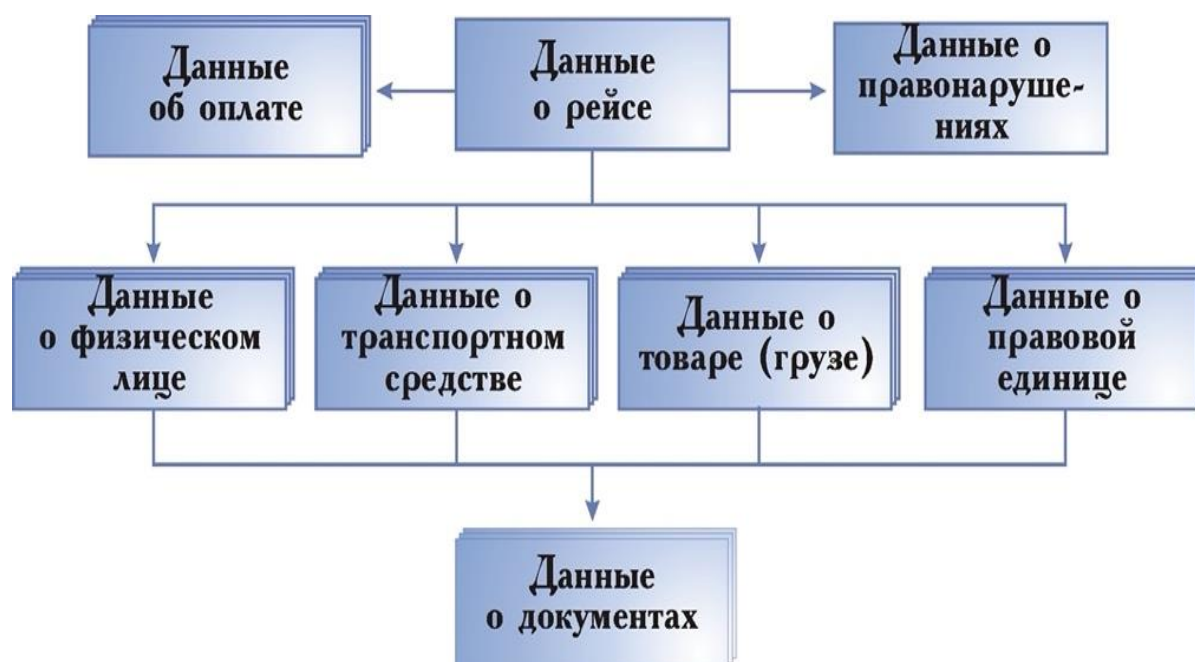


Рис. 10. Данные, содержащиеся в АИС «FRONTIERA».

(1) данные о рейсе:

- идентификатор рейса;
- дата и время пересечения границы;
- пункт пересечения;
- въезд в страну и выезд из нее;

(2) данные о физическом лице:

- государственный идентификационный номер физического лица (IDNP);
- идентификационные персональные данные лица:
 - фамилия;
 - имя;
 - имя отца (отчество);
 - пол;
 - дата рождения;
 - место рождения;
- данные о гражданстве;
- мотив пересечения границы;
- ссылка на физическое лицо, вместе с которым пересек границу гражданин, не имеющий своего документа;
- категория лица (водитель, пассажир, сопровождающий другое лицо, сопровождающий груз);
- страна отправления/назначения;

(3) данные о правовой единице:

- государственный идентификационный номер правовой единицы (IDNO);
- идентификационные данные:
 - название правовой единицы;
 - категория правовой единицы;
- организационно-правовые данные:
 - вид собственности;
 - организационно-правовая форма;
- в качестве кого выступает правовая единица при осуществлении операций с товарами (грузами);

(4) данные о транспортном средстве:

- VIN-код;
- тип транспортного средства;
- марка-модель транспортного средства;
- номер кузова;
- номер шасси;
- номер двигателя;
- регистрационный знак;
- тип регистрационного знака;
- технические характеристики;
- страна регистрации транспортного средства;
- мотив пересечения границы;
- данные о владельце:
 - физическое лицо;

- правовая единица;

(5) данные о товарах (грузах):

- идентификационный код товара;
- наименование товара;
- количество товара;
- стоимость товара;
- единица измерения:
 - основная;
 - дополнительная;
- код внутренней таможи;

(6) данные об оплате:

- вид платежа;
- сумма;
- плательщик;
- порядок оплаты;

(7) данные о документах:

- тип документа;
- серия документа;
- номер;
- дата выдачи;
- кем выдан;
- срок действия;

(8) данные о правонарушениях:

- вид нарушения;
- дата совершения;
- мера воздействия;

(9) слой электронно-цифровой карты, включающий:

- линию государственной границы;
- линию таможенной границы;
- пункты перехода границы;
- внутренние таможни;
- таможенные склады;
- зоны свободного предпринимательства.

4.3.5 Классификаторы

В целях обеспечения достоверности информации и сокращения объема хранимых в АИС «FRONTIERA» данных используется система классификаторов, которые могут быть разделены на три категории:

- международные классификаторы;
- национальные классификаторы;

- внутрисистемные классификаторы.

В рамках АИС «FRONTIERA» внутрисистемные классификаторы разрабатываются и используются только при отсутствии утвержденных международных и национальных классификаторов.

4.4 Информационная площадка АИС «FRONTIERA»

АИС «FRONTIERA» является единственным источником информации о фактах пересечения границы физическими лицами, транспортными средствами и товарами (грузами) для ведомственных автоматизированных информационных систем. АИС «FRONTIERA» использует данные следующих регистров, составляющих его информационную платформу (рис. 12):

Государственный регистр населения, содержащий данные о физических лицах и выданных им документах;

Государственный регистр правовых единиц, включающий информацию обо всех типах правовых единиц, в том числе о их деятельности, документах и печатях;

Государственный регистр транспорта, охватывающий данные о транспортных средствах (включая номерные агрегаты) и регистрационных документах;

Государственный регистр водителей, содержащий данные о праве физического лица на управление соответствующим транспортным средством;

Автоматизированная информационная система «CONTROL RM», осуществляющая мониторинг движения товаров по территории страны, их транзита, а также перевода товаров из одного таможенного режима в другой (находится в стадии разработки).

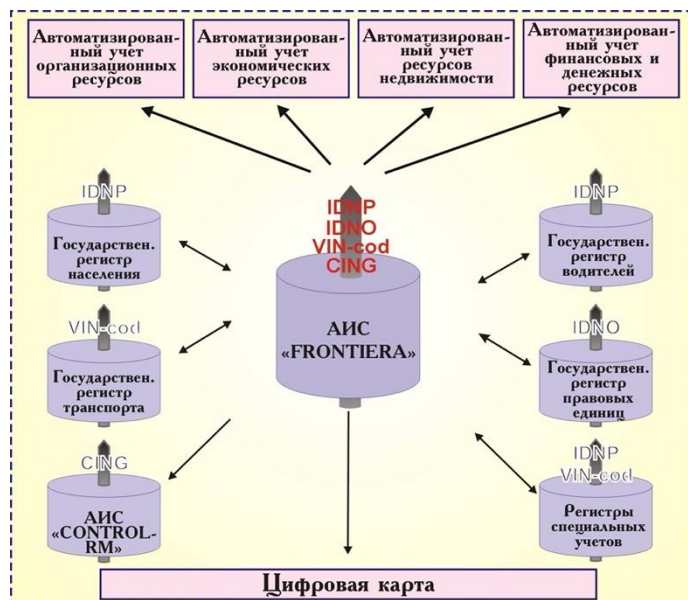


Рис.12. Информационная платформа АИС «FRONTIERA»

Отдельно следует отметить **регистры специальных учетов**, входящие в состав системы государственного контроля за соблюдением законодательства и финансовой

дисциплины Национальной информационной системы. Ими являются налоговый регистр и криминогенный контур.

Использование во всех вышеуказанных регистрах идентификаторов объектов учета (IDNP, IDNO, VIN-cod, и др.) и единообразное представление данных обеспечивает возможность получения в случае необходимости интегрированных данных по любому объекту учета или сводных статистических данных. В то же время раздельное существование баз данных обеспечивает защиту информации от несанкционированного доступа.

В свою очередь, АИС «FRONTIERA» служит источником информации о фактах пересечения границы для всех составных частей Национальной информационной системы, прежде всего для Государственного регистра населения (учет миграции населения) и Государственного регистра транспорта (учет местонахождения транспорта).

4.5 Технологическое пространство системы АИС «FRONTIERA»

Уровни АИС «FRONTIERA»

В соответствии с административно-территориальным делением Республики Молдова и организационной структурой подразделений, участвующих в формировании АИС «FRONTIERA», система построена в двух уровнях (рис. 13):

- центральный уровень;
- локальный уровень.

Каждый из уровней содержит один или несколько информационно-телекоммуникационных комплексов.

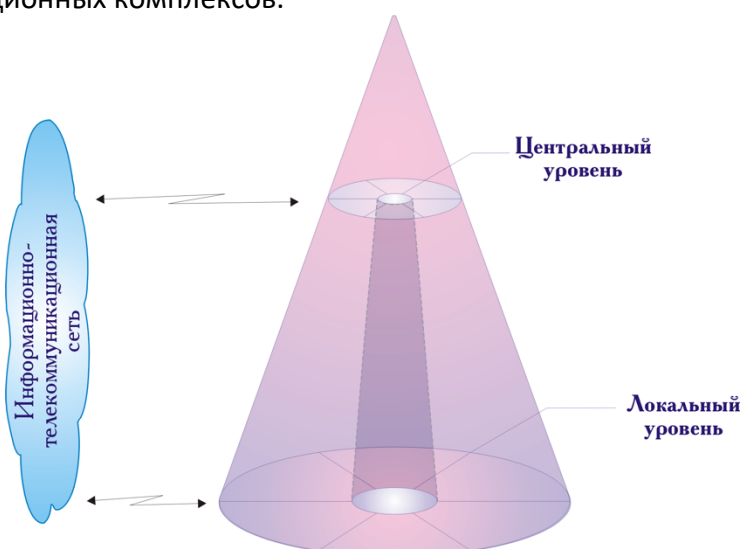


Рис. 13. Уровни АИС «FRONTIERA».

Территориальное расположение информационно-телекоммуникационных комплексов центрального и локального уровней показано на рис. 14.



Рис. 14. Расположение информационно-телекоммуникационных комплексов АИС «FRONTIERA».

4.5.1 Назначение и структура информационно-телекоммуникационного комплекса центрального уровня

Информационно-телекоммуникационный комплекс центрального уровня размещаются в муниципии Кишинева и призван обеспечивать функционирование организаций, привлеченных к созданию и эксплуатации АИС «FRONTIERA», включая управление системой и изготовление нужных документов.

В состав информационно-телекоммуникационного комплекса центрального уровня входят (рис. 15):

- центральный банк данных;
- автоматизированные рабочие места (АРМ) администраторов системы;
- автоматизированные рабочие места системных аналитиков;
- локальные вычислительные сети (ЛВС) организаций, участвующих в управлении АИС «FRONTIERA». Каждая из указанных сетей включает автоматизированные рабочие места

администраторов соответствующих подсистем и сотрудников соответствующих организаций, а также локальные банки данных (ЛБНД), содержащих специфическую информацию данной службы;

- телекоммуникационное оборудование для обеспечения связи автоматизированных рабочих мест и локальных вычислительных сетей с центральным банком данных, а также всего комплекса с локальными информационно-телекоммуникационными комплексами.

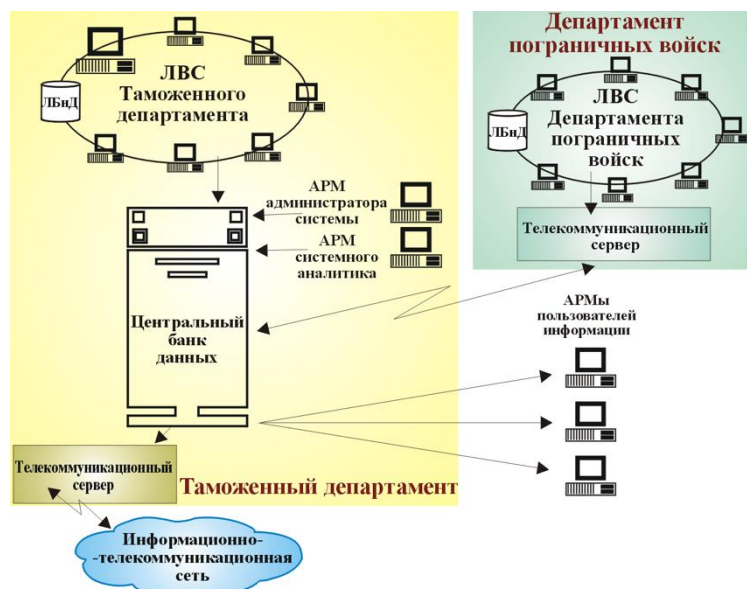


Рис. 15. Информационно-телекоммуникационный комплекс центрального уровня.

Несколько функциональных модулей, выполняющих конкретные функции, могут быть сгруппированы на одном автоматизированном рабочем месте, или наоборот, один и тот же функциональный модуль может быть установлен на нескольких однотипных автоматизированных рабочих местах по указанию администратора системы и администраторов соответствующих подсистем.

4.5.2 Центральный банк данных

Центральный банк данных предназначен для хранения и обработки информации, содержащейся в АИС «FRONTIERA» (рис.16) и состоит из следующих частей:

- **хранилище данных**, используемое для постоянного хранения в полном объеме информации об объектах учета и контроля и документах, включая данные о документах, на основании которых была актуализирована информация (формуляры) об этапах принятия решений и о датах принятия решений и именах сотрудников, принявших эти решения;
- **база форматов**, предназначенная для обеспечения безопасности при работе с удаленными пользователями, а также для хранения классификаторов и определения права доступа к информации того или иного пользователя. Связь автоматизированных рабочих мест пользователей с центральным банком данных осуществляется исключительно через базу форматов;
- **технологические базы данных**, предназначенные для временного хранения информации, поступившей с нижних уровней и требующей принятия решения

полномочными сотрудниками, а также для осуществления всех необходимых проверок при принятии решения. Информация из технологической базы данных закладывается в хранилище данных только после принятия окончательного решения по формуляру;

- **витрины данных**, представляющие собой базы данных с выдержками из центрального хранилища данных и предназначены обеспечивать пользователей быстрым и удобным доступом к необходимой информации без доступа к хранилищу данных. Витрины данных могут предоставлять отдельным категориям пользователей данные в наиболее удобном для использования виде (например, для Главной государственной налоговой инспекции предоставляется информация об экспортно-импортных операциях и их участниках). При этом они являются одним из элементов защиты от несанкционированного доступа к информации, так как содержат только объем данных, доступный пользователю. Обновление данных в витринах осуществляется автоматически при актуализации информации в хранилище данных.

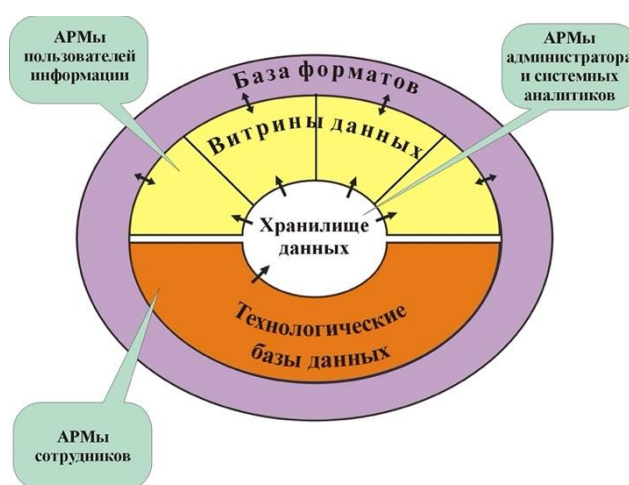


Рис. 16. Структура Центрального банка данных.

В свою очередь, АИС «FRONTIERA» пользуется витринами данных других информационных систем, в частности витринами данных Государственного регистра населения, Государственного регистра правовых единиц и Государственного регистра транспорта.

Обмен информацией между составными частями центрального банка данных осуществляется посредством процедур, недоступных для внешних пользователей и являющихся элементом системы защиты банка данных.

4.5.3 Структура хранилища данных

Хранилище данных включает в себя следующие базы данных:

«Рейс», где содержатся данные о последствиях пересечения границы, а также о физических лицах, правовых единицах, транспортных средствах и товарах (грузах), вовлеченных каким-либо образом в пересечение границы.

«Фильтр», предназначенная для хранения фильтрационных массивов; примером такого массива может служить список лиц, которым запрещен въезд в Республику.

5 Нефункциональные требования

5.1 Требования к надежности и отказоустойчивости

Надежность элементов подсистемы должна быть обеспечена по следующим направлениям:

- обеспечение работоспособности компонентов каждой подсистемы;
- хранения данных.

При этом должна требоваться минимальное внимание со стороны системного администратора по реакции на устранение последствий отказов компонентов, а также программно-аппаратными средствами должно быть обеспечено сохранение данных.

Подсистема должна обеспечивать:

- отказоустойчивую работу в режиме 24/7/365;
- гарантировать доступность для работы конечных пользователей на уровне минимум 99.5%;
- максимальное время восстановления работоспособности подсистемы (RTO) не более 30 минут;
- максимальное время восстановления данных (RPO) не более чем 2:00;
- максимальное время перехода, в автоматическом режиме, на резервное электроснабжение 5 минут;
- резервное электроснабжение не менее 2-х суток.

Подсистема должна быть защищена от физических отказов оборудования средствами логического резервирования данных и компонентов подсистем с использованием соответствующих протоколов и средств контейнеризации и виртуализации. Для защиты от ошибок в системном и прикладном программном обеспечении должна быть создана система резервного копирования с целью оперативного восстановления рабочих конфигураций из резервных копий.

Сохранность информации в случае аварий должна быть обеспечена в полном объеме. Резервное копирование должно обеспечиваться функциональностью, реализованной в рамках системы и одновременно штатными средствами СУБД, используемых.

Для обеспечения резервного копирования информации на случай аварий создается отдельные территориально разнесены с ЦОД хранилища (хранилище). Резервное копирование должно происходить с периодичностью, обеспечивающей полную сохранность и восстановление данных. Затраты времени на восстановление подсистемы с учетом технических задержек, подключение к резервному ЦОД и

операцией контроля работоспособности, должны быть минимальными для обеспечения непрерывной работы и превышать одного часа.

Сохранение данных должно обеспечиваться в случаях:

- отключение питания;
- отказа технических средств обработки информации;
- ошибки, сбоев или разрушения программного обеспечения.

5.1.1 Требования к мощности подсистемы

Мощность элементов системы должна быть рассчитана на обработку соответствующего количества обращений с двойным запасом.

Предварительные данные для расчета нагрузки на систему:

- запросов в сутки: ~ 50000;
- запросов в час (среднее) ~ 2000;
- запросов в час (пиковое $\times 4$) ~ 8000;
- нагрузки запросов / час ~ 16 000 (включая дополнительный двойной запас)
- нагрузки запросов / сек ~ 4,5 (учитывая дополнительный двойной запас).

5.2 Требования к интерфейсу пользователя

Необходимо предусмотреть универсальность интерфейсов для различных функционалов и приборов, возможность доступа к платформе с планшетов через веб-интерфейс.

Одним из представлений интерфейса на уровне Мониторингового центра Гостаможслужбы электронная карта Молдовы с отображением локации всех Пунктов Пропуска.

5.3 Обеспечение защиты информации в АИС «Frontiera»

5.3.1 Определение системы информационной безопасности

Под системой информационной безопасности понимается единая совокупность правовых и морально-этических норм, организационных (административных) мер и программно-технических средств, направленных на противодействие опасности, угрожающей системе АИС «FRONTIERA» для сведения до минимума ущерба, который может быть причинен пользователям и владельцам информации.

Основной целью, преследуемой при защите информации в системе АИС «FRONTIERA», является предотвращение любого несанкционированного вмешательства в процесс ее функционирования, а также попыток хищения, модификации, выведения из строя или

разрушения ее структурных компонентов, то есть защита всех компонентов системы: оборудования, программного обеспечения, данных и персонала.

5.3.2 Угрозы безопасности АИС «Frontiera»

Важнейшими аспектами обеспечения безопасности системы АИС «Frontiera» являются определение, анализ и классификация возможных угроз целостности и работоспособности системы.

Под угрозой понимается появление возможных событий, действий (воздействий), процессов или явлений, которые могут стать причиной нанесения ущерба элементам системы.

Наиболее серьезными видами угроз, которые учитывались при создании системы безопасности Департамента информационных технологий, являются:

- аварии систем электро-, водо- и теплоснабжения;
- сбои и отказы технических средств системы;
- последствия ошибок в проектировании и разработке компонентов системы (технических средств, технологии обработки информации, программ, структур данных и т.д.);
- ошибки эксплуатации (пользователей, операторов и другого персонала);
- преднамеренные разрушительные действия возможных правонарушителей.

5.3.3 Общие требования к безопасности

Основной принцип регистрового учета - персонификация, что предполагает строгое соблюдение конфиденциальности информации. Когда в базу данных АИС «FRONTIERA» вводятся персональные данные, работа осуществляется в следующих формах:

- сертификации и аттестации информационных подсистем персональных данных;
- лицензирования работы с персональными данными;
- межгосударственных соглашений о трансграничной передаче персональных данных.

Требования к информационной безопасности, отраженные в эксплуатационных документах, обеспечивают безопасность при монтаже, наладке, эксплуатации и ремонте технических средств и соответствуют действующим стандартам и Правилам техники безопасности при эксплуатации электроустановок.

Концептуальная модель информационной безопасности АИС «FRONTIERA» представлена на рис. 18.



Рис. 18. Концептуальная модель безопасности системы.

5.3.4 Защита информации от несанкционированного доступа

В систему защиты информации от несанкционированного доступа входят организационные меры и программно-аппаратные методы и технические средства, обеспечивающие блокирование:

- оттока информации по техническим каналам;
- несанкционированного доступа к ресурсам сети.

Организационные меры обеспечиваются соответствующими службами и исключают неконтролируемый доступ посторонних лиц к техническим средствам информационно-телекоммуникационной сети, магнитным носителям, средствам выдачи твердых копий и к кабельным системам.

Программно-аппаратные средства защиты информации от несанкционированного доступа обеспечивают:

- идентификацию защищаемых ресурсов;
- аутентификацию защищаемых ресурсов и пользователей;
- конфиденциальность информации, циркулирующей в системе;
- аутентифицированный обмен данными;
- целостность данных при возникновении, передаче, использовании и хранении информации;
- разрешенный доступ ко всем ресурсам системы в условиях нормальной эксплуатации;
- разграничение доступа пользователей к системе;
- разграничение доступа пользователей к защищаемым ресурсам;
- управление (обозначение права доступа к защищаемым ресурсам, обработка информации из регистрационных журналов, установка и снятие системы защиты);

- регистрацию действий по входу в систему и выходу из нее пользователей, а также нарушений правил доступа к защищаемым ресурсам;
- проверку целостности и работоспособности системы защиты;
- безопасность в аварийных ситуациях.

5.3.5 Обеспечение сохранности информации в случае аварии

В случае аварий в информационно-телекоммуникационной сети сохранность информации обеспечивается путем:

- остановки работы отдельных технических средств;
- прекращения электроснабжения.

5.3.6 Защита от воздействия внешних факторов

На работоспособность технических и программных средств информационно-телекоммуникационной сети не влияют существующие в зоне эксплуатации электрические и магнитные поля, возможные повреждения источников электропитания и природные катаклизмы.

5.3.7 Требования к информационной безопасности

Подсистема должна быть защищена от наиболее распространенных типов атак, например SQL injection, XSS, доступа методом переборки паролей и тому подобное.

Информация, ослабляет информационной безопасности (такая, как id сессии, id пользователя и т.д.), не должна отражаться публично.

На физическом уровне должны быть выполнены следующие правила:

- физический доступ к оборудованию должен быть ограниченным и все действия должны быть зафиксированы; + СКУД
- обеспечение однозначной идентификации пользователей;
- физический доступ к резервным копиям подсистемы должен быть ограниченным в соответствии с регламентом администрирования подсистемы и все действия должны быть зафиксированы;
- обеспечение на сетевом уровне прохождения только разрешенных информационных потоков со стороны телекоммуникационных сетей к системе, а также в обратном направлении;
- обеспечение регистрации событий, связанных с получением пользователями доступа к ресурсам системы (прохождение / непрохождение аутентификации), действий администраторов по модификации журналов регистрации событий, изменения настроек программного обеспечения, серверов и коммутационного оборудования;
- обеспечение возможности отследить историю запросов, направленных на внесение изменений в информации, хранящейся в базах данных системы, и однозначной идентификации пользователей, выполняющих такие изменения (внесение, изменение, удаление);

- система должна иметь функционал по ограничению количества запросов к БД с целью ее защиты от перегрузки.

Дополнительные требования к информационной безопасности:

- подключения модулей к локальной шине, обмен и обработка данными с ней должна быть возможной только при условии подтверждения соответствия в установленном порядке созданной в ней комплексной системы защиты информации;
- подключаемый модуль должен выполнять минимальные требования по киберзащите своей ИТС, а именно:
- необходимость регулярного установки обновлений общего программного обеспечения (операционных систем, систем управления базами данных, программных библиотек и т.д.);
- необходимость контроля целостности и подлинности обновлений программного обеспечения (как системного программного обеспечения, так и прикладного программного с учетом особенностей построения и функционирования соответствующего программного обеспечения;
- обеспечение антивирусной защиты (обеспечение защиты от внесения в модуль вредоносного программного кода (вирусов, троянских программ и др.), Проверку на наличие вредоносного кода всех вложений загружаемых пользователями в модуль и в случае поражения вложений вредоносным программным кодом, блокировать загрузку для предотвращения использованию модулей в противоправных и преступных целях, блокировка загрузки исполняемых файлов и скриптов к модулям и т.п.);
- должно обеспечивать предоставление соответствующих рекомендаций конечным пользователям по обеспечению безопасности данных, обрабатываются и хранятся в их информационных системах (в том числе, развернутых с использованием организационно-технических решений на развертывание типовых составляющих компонент комплексной системы защиты информации).

5.4 Требования к развитию и модернизации элементов системы

Каждый элемент системы должен быть разработанным с учетом возможности масштабирования. Все API подсистемы должны иметь возможность горизонтального масштабирования. Серверы БД должны иметь возможность вертикального или, если возможно, горизонтального масштабирования.

5.4.1 Требования к стандартизации и унификации

Стандартизация и унификация функций системы должна быть обеспечена путем использования современных инструментальных программных средств, поддерживающих единую технологию проектирования и разработки функционального, информационного и программного обеспечения.

Программное обеспечение в целом, и другие программные компоненты подсистемы должны соответствовать основным международным и национальным соглашениям и стандартам в области информационных технологий.

Для разработки документации этапа разработки системы должны быть применены стандарты, не старше по:

- IEEE 830 Software requirements specification and Software Engineering Institute templates;
- IEEE 1016 Software architecture design and Software Engineering Institute templates.

5.4.2 Требования к информационному обеспечению

Информационное обеспечение должно отвечать следующим требованиям и возможностям:

- обеспечение физической и логической целостности данных;
- минимизация избыточности хранимых данных;
- стандартизация представления данных;
- достоверность и актуальность данных.

Система должна обладать свойствами интегрированной информационной среды:

- обеспечивать распределение и предоставление прав доступа основанных на ролевом или другом подобном принципе;
- предусматривать с помощью документированного API возможность интеграции с другими информационными системами.

5.4.3 Требования к видам обеспечения

5.4.3.1 Требования к математическому обеспечению

Математическое обеспечение подсистемы должно включать необходимые алгоритмы для выполнения операций поиска данных, обработки статистической информации, анализа данных.

Средства анализа информации должны обеспечить быстрый доступ к информации и ее представления в интуитивно понятной форме.

5.4.3.2 Требования к информационному обеспечению

Информационное обеспечение, создаваемое в рамках подсистемы, должно обеспечивать:

- хранение данных в виде, что позволяет организовать работу с системой для многих пользователей, а также автоматическое восстановление системы в аварийной ситуации;
- распределение и предоставление прав доступа на основе системных ролей;
- работу пользователей системы с информационными ресурсами в режиме реального времени;

- хранение данных об истории изменений данных пользователями (ведение персонализированного протокола изменений);
- обеспечение целостности географически распределенных данных.

Информационное обеспечение системы должно отвечать следующим требованиям:

- соответствие базы данных требованиям нормативно-правовых документов;
- использование государственных классификаторов и справочников;
- обеспечение контроля обработки входных данных на корректность типов, правильность написания в соответствии с действующими классификаторами и справочниками, соответствие установленным диапазонам значений, непротиворечивость данных о перечне правил;
- обеспечение возможности работы как со структурированной, так и не структурированной информацией.

6 Программно-технический комплекс

6.1 Программно-технический комплекс центрального уровня

Программно-технический комплекс центрального уровня включает в себя следующие компоненты:

- серверы баз данных: два сервера 10 поколения (128 Gb -RAM, 4 Processor -10 core, storage – 100 GB for operating system and 4 TB for database)
- операционные системы – ReadHat Oracle 7.5.
- система управления базой данных Oracle 11.2.0.4.

Автоматизированные рабочие места базируются на персональных компьютерах с операционной системой Windows 10.

6.2 Назначение и структура информационно-телекоммуникационного комплекса локального уровня

Информационно-телекоммуникационные комплексы локального уровня обеспечивают функционирование всех организаций, задействованных в управлении системой и находятся в следующих пунктах:

- районные центры (на внутренних таможах);
- пункты пропуска через границу (с пешеходными, автомобильными, железнодорожными путями). (Пункты пропуска в речных портах и аэропортах приравниваются к пешеходным, автомобильным и железнодорожным);
- пункты пропуска через таможенную границу (таможенные склады, зоны свободного предпринимательства);

В состав информационно-телекоммуникационного комплекса локального уровня входят:

- витрина данных;

- технологическая база данных;
- автоматизированное рабочее место администратора системы;
- локальные вычислительные сети всех задействованных организаций;
- телекоммуникационное оборудование для обеспечения связи автоматизированных рабочих мест и локальных вычислительных сетей с витринами данных, а также всего комплекса - с центральным информационно-телекоммуникационным комплексом (Рис. 17).

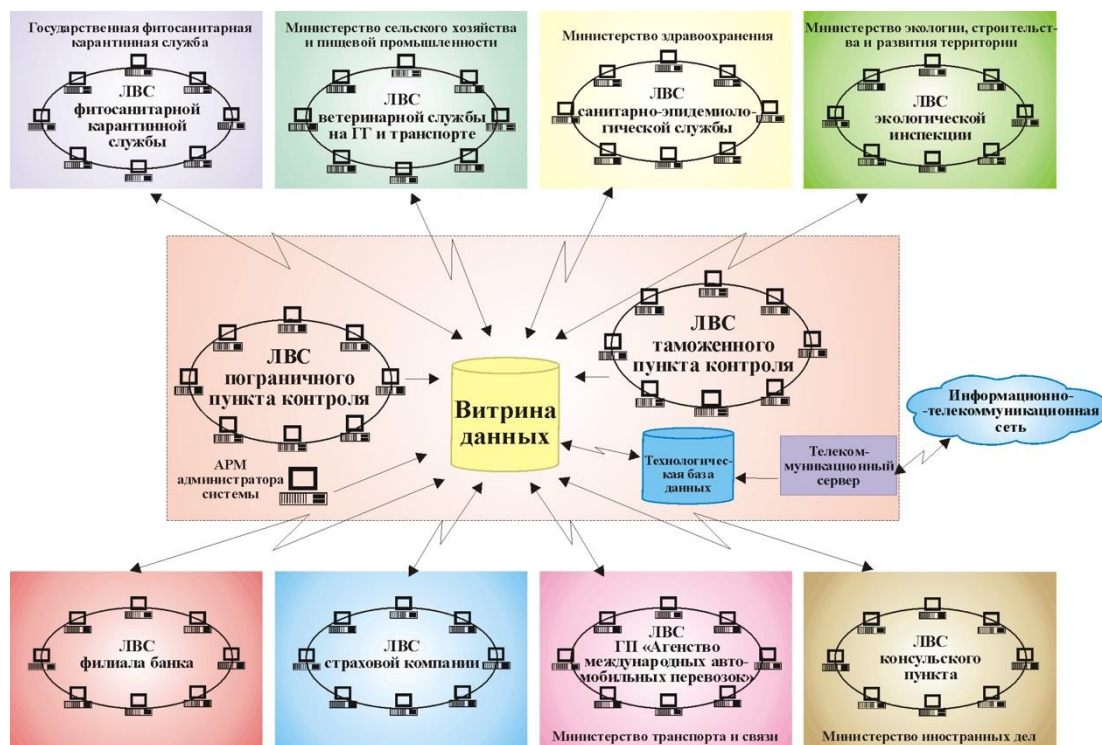


Рис. 17. Информационно-телекоммуникационный комплекс локального уровня.

Несколько функциональных модулей, реализующих конкретные функции, могут быть сгруппированы на одном автоматизированном рабочем месте или, наоборот, один и тот же функциональный модуль может быть установлен на нескольких однотипных автоматизированных рабочих местах по указанию администратора системы и администраторов соответствующих подсистем.

Технологическая база данных предназначена для накопления информации, передаваемой на центральный уровень, с целью уменьшения нагрузки на каналы связи или в случае отсутствия связи по техническим причинам.

6.2.1 Программно-технический комплекс локального уровня

Автоматизированные рабочие места локального уровня базируются на персональных компьютерах с операционной системой Windows 10. Автоматизированные рабочие места включают в себя специализированное оборудование для контроля документов и ридеры для считывания машиночитаемых документов. Автоматизированные рабочие места локального уровня включают также в себя специализированное оборудование для считывания и записи информации с электронных чипов и соответствующее программное обеспечение.

В состав программного обеспечения автоматизированных рабочих мест входят различные справочники, в том числе справочник удостоверяющих личность документов стран мира.

6.3 Административная инфраструктура

6.3.1 Размещение системы

На период разработки и внедрения - система должна быть размещена в облачном сервисе. С целью эксплуатации системы в соответствии с регламентом работы система должна иметь отдельные среды приведены в таблице ниже.

Таблица - Список сред

Среда	Описание
PROD	продуктивную среду
UAT	Стабильную среду с наиболее современной функциональностью. Используется для тестирования новой функциональности

Было решено, что достаточно двух сред: PROD, UAT.

6.3.2 Система резервного копирования и восстановления после аварий

В рамках разработки системы должны быть предусмотрены механизмы резервного копирования системы, регламент резервного копирования и инструкции по восстановлению системы после аварий. Наличие средств для бронирования конфигурационных файлов и критически важных для функционирования оборудования системных файлов (создание образов дисков, резервирование операционных систем серверов и коммутационного оборудования) с целью их последующего быстрого восстановления в случае сбоев. Восстановление системы включает в себя:

- восстановление конфигураций системного и прикладного программного обеспечения;
- восстановление информации о пользователях;
- восстановления данных.

6.3.3 Система логирования

Система должна предусматривать интеграцию с центральными модулями логирования Гостаможслужбы, которая предусматривает логирования следующих событий:

- запуск / остановка отдельных сервисов подсистемы;
- события безопасности типа login / logout;
- ошибок в работе подсистемы, таких как коммуникационные, целостности данных в подсистеме, непредсказуемые задержки в обработке информации;

- критические события от подсистемы мониторинга (критический объем памяти, дискового пространства и т.д.);
- работы веб-сервисов, включая сохранение аудиторского следа для каждого запроса / ответа веб-сервисов;
- иные события безопасности.

6.3.4 Система автоматического тестирования

Все модули системы необходимо полностью или частично покрыть автотестами и модульными тестами.

Система автоматического тестирования создана с целью тестирования нового функционала, эмуляции искусственной нагрузки и воспроизведения возможных ошибок в режиме, максимально приближенном к реальному.

6.3.5 Порядок контроля и приемки системы

Для принятия системы в эксплуатацию должна быть создана приемная комиссия в составе представителей Заказчика и приобретателем.

Исполнитель передает приобретателю исключительные права на разработанное программное обеспечение. В случае невозможности передачи исключительных прав, Исполнитель передает права на программное обеспечение, предусматривающих возможность осуществления Приобретателем, или избранными Приобретателем третьими сторонами, любых модификации в программном обеспечении.

При сдаче в эксплуатацию система должна пройти приемное тестирование для определения ее соответствия техническому заданию.

По результатам приемочных испытаний составляется акт, в котором содержится вывод о степени соответствия системы требованиям технического задания и решение о принятии ее в промышленную эксплуатацию.

Программное обеспечение, поставляемое, должно быть установлено и настроено на серверах, определенных Приобретателем. Исполнитель проводит принятие системы в целом.

Система должна иметь следующую документацию:

- 1) функциональное описание системы;
- 2) Схема потоков данных + структура базы данных + ER диаграмма;
- 3) подробная L2 / L3 топология системы в виде диаграмм;
- 4) инструкция администратора системы;
- 5) инструкция пользователя и их функций
- 6) инструкция по развертыванию, обновления и восстановления;

- 7) акт передачи-приемки экземпляра Произведения (Программное обеспечение, поставляемое)
- 8) программа и методика предварительных испытаний;
- 9) протокол предварительных испытаний и других тестирований.

6.3.6 Подготовка и настройка технического обеспечения

Приобретатель предоставляет Исполнителю доступ к техническим средствам для установления и налаживания комплекта программного обеспечения, необходимого для функционирования системы.

Приобретатель обеспечивает доступ специалистов Исполнителя к вышеупомянутым средствам для выполнения окончательной настройки и оперативного внесения изменений в программное обеспечение.

6.3.7 Подготовка персонала

Подготовка персонала к началу эксплуатации осуществляется на рабочем экземпляре системы.

Инструктаж операторов и администраторов системы осуществляется Исполнителем путем предоставления соответствующих руководств пользователей и проведение тренинга по месту, согласованным с Приобретателем.

Количество должностных лиц (операторов), которые проходят тренинг не должна быть менее 3-х человек от каждого территориального органа, но не менее 3-х человек от каждого структурного подразделения ЦА.

Продолжительность тренинга - в 5:00.

Требования к проведению обучения пользователей системы:

В рамках внедрения системы должны быть разработаны материалы для обучения. На основе разработанных материалов проводить обучение ключевых пользователей. В процессе обучения должны освещаться темы, необходимые и достаточные для выполнения пользователями и администраторами своих функций.

Перед началом обучения должны быть подготовлены учебные Сценарии.

Приобретатель должен обеспечить присутствие на занятиях ключевых пользователей платформы по направлениям внедрения.

По завершению обучения разработчик должен оформить протокол о проведении обучения. Все сотрудники, прошедшие обучение, должны подписать протокол о проведенном обучении.

Приложение А: Особые функциональные требования

№	Задача	Описание
Система интеграций		
1.	Интеграция AIS Frontiera с ANPR&CCTV	Таможенная служба внедряет системы видеонаблюдения VICOS на пограничных таможенных постах. Внедрение этих систем предполагает установку интеллектуальных камер для считывания и оцифровки номерных знаков транспортных единиц, установку умных флагбаумов и светофоров. Внедрение видеомониторинга подразумевает необходимость интеграции с СИ таможенной службы для обеспечения автоматизации и флюидизации движения в пределах зон контроля, исключения человеческого фактора из процесса регистрации транспортных единиц в зонах контроля. Формирование автоматизированных электронных средств контроля светофоров и заграждений (на основе решений в информационных системах) о разрешении въезда / выезда и перемещения транспортных единиц между контрольно-пропускными пунктами.
2.	Интеграция AIS Frontiera с ASP	В настоящее время данные о лицах (водителях), пересекающих государственную границу, автоматически проходят через пограничную полицию. Однако бывают случаи, когда таможенный инспектор обязан ввести в AIS Frontiera информацию о лицах, которые не участвуют в обмене данными с пограничной полицией (владелец транспортного подразделения в случае таможенного оформления по действию, владелец товаров в пределах маршрута и т. д.). В этом контексте для физических лиц-резидентов RM AND Frontier необходимо обеспечить обмен данными с Национальным регистром населения, управляемым PMI. AIS Frontiera будет запрашивать данные у ASP на основе IDNP человека. ASP вернет как минимум следующие данные (имя, имя, адрес, дату рождения, статус).
3.	Интеграция AIS Frontiera с реестром юридических лиц ASP	В настоящее время в AIS Frontiera нет реестра юридических лиц. Сведения о юридических лицах вводятся таможенными инспекторами вручную по каждой отдельной сделке. Реестр экономических агентов SI Asycuda World не может быть использован из-за отсутствия информации, запрашиваемой AIS Frontiera (отсутствие транспортных компаний). В этом контексте для юридических лиц-резидентов PM «AIS Frontier» должен обеспечить обмен данными с Национальным регистром предприятий, управляемым ASP. AIS Frontiera будет запрашивать данные у ASP на основе IDNO компании. ASP вернет как минимум следующие данные (имя, адрес, статус).
4.	Интеграция AIS Frontiera с транспортными	В настоящее время данные о транспортных средствах, пересекающих государственную границу, поступают автоматически через пограничную полицию. Однако бывают случаи, когда данные получены неверно (ручной ввод). В этом контексте необходимо

	подразделениями ASP	проверить данные о транспортных единицах, зарегистрированных в Национальном регистре транспортных единиц в ASP. AIS Frontiera будет запрашивать данные у ASP на основании регистрационного номера транспортной единицы. ASP вернет как минимум следующие данные (VIN-код, технические характеристики, включая массу UT, статус).
5.	Изменение обмена данными с ANSA	В настоящее время обмен данными с ANTA является односторонним, при котором сотрудник таможни запрашивает подтверждение действительности разрешений на перевозку. ANTA отправляет в AIS Frontiera электронную версию разрешения. На основании электронной формы инспектор таможни получает решение о разрешении транспортной единице покинуть Зону таможенного контроля. Это риск превышения количества транзакций, разрешенных авторизацией, или несоблюдения условий использования авторизации. Поэтому для каждой транзакции, зарегистрированной в AIS Frontiera на разрешениях на транспортировку, требуется передавать информацию о транзакции на адрес ANTA (номер разрешения, страна отправления, страна назначения, страна регистрации и т. Д.). Таким образом, ANTA будет проверять данные и записывать использованные разрешения на транспортировку. ANTA доставит в «AIS Frontier» результат контроля (принятие / отказ, причина отказа). Как следствие, ответственность за разрешение транзакции в рамках авторизации остается за ANSA.
6.	Интеграция с Anti-fraud	Обеспечение синхронизации черных списков AIS Frontiera со списками лиц, экономических агентов и транспортных единиц, которые совершили преступления или были обнаружены с повышенным риском совершения преступлений в SI Anti-Fraud. Выдача информации из AIC Frontiera в IS Antifraud о результатах проверок назначенных лиц и транспортных единиц.
7.	Интеграция с пограничной службой	В настоящее время пассажиры транспортного средства, пересекающие государственную границу, не подлежат обмену данными между «AIS Frontier» и СИ Пограничной службы. Поэтому запрашивается следующий механизм обмена данными с пограничной полицией. SI Anti-Fraud формирует профиль риска и передает его на адрес SI Пограничной службы. Пограничная служба подтверждает его прием. Если ИБ пограничной полиции обнаруживает присутствие в зоне контроля заинтересованного лица, ИБ пограничной службы передает эту информацию на адрес AIS Frontiera (информация о человеке, информация о профиле риска).
Изменения в пользовательском интерфейсе		
8.	Дополнительный пользовательский интерфейс ANSA	Первоначальный интерфейс ANSA был разработан как часть интерфейса на таможенном контрольно-пропускном пункте. В настоящее время инспекторы ANSA присутствуют в зонах

		таможенного контроля и де-факто не включены в информационные потоки в зонах таможенного контроля. Таким образом, рассчитанные платежи не включаются в единый платежный ваучер, а контроль ANSA даже не отражается в информационных системах (контрольное время, результат контроля и т.д.). Поэтому контроль ANSA делает использование VICOS на таможенных постах практически бесполезным. Интерфейс ANSA должен гарантировать, что пользователи ANSA могут указывать результаты контроля и включение рассчитанных платежей в единый платежный ваучер. Интерфейс ANSA не автоматизирует внутренние процессы ANSA.
9.	Пользовательский интерфейс Addice Warehouse	В настоящее время представители таможенных складов (должностные лица CTIF) не имеют доступа к SI Frontiera. Плата за услуги на складах не включается в разовый платежный чек. Рабочий интерфейс для пользователей таможенных складов должен содержать следующую информацию: • Описание предоставляемой услуги (классификатор) • Дата начала обслуживания • Дата окончания обслуживания • Объем предоставленной услуги • Как оплатить предоставленную услугу Услуги, требующие оплаты наличными, будут включены в ваучер разовой оплаты, проводные платежи за услуги.
10.	Переход на интерфейс сканирования	В дополнение к существующим данным в AIS Frontiera интерфейс должен обеспечивать возможность добавления графических изображений (результат сканирования). В подозрительных случаях прикрепление изображения должно быть обязательным. Формат графических файлов и режим прикрепления будут определены разработчиком совместно с ответственными лицами Таможенной службы на этапе бизнес-анализа процесса.
11.	Добавление интерфейса въезда / выезда	В настоящее время транзакция инициируется пограничной полицией или на таможенном посту. С внедрением системы VICOS возникла необходимость в автоматизации контрольно-пропускных пунктов на въездных / выездных барьерах в / из зон таможенного контроля. Поскольку контрольный пункт въезда / выезда в / из контрольной зоны в направлении выезда из Республики Молдова и контрольный пункт въезда / выезда в / из контрольной зоны в направлении въезда в Республику Молдова управляются лицом в каждом направлении, интерфейс должен объединять контрольные точки въезда / выезда в / из зоны таможенного контроля. Следовательно, интерфейс ввода / вывода должен содержать две отдельные зоны. • Вход в зону контроля • Выйдите из контрольной зоны.

		Область ввода должна обеспечивать возможность регистрации новой транзакции, т.е. пользователь должен ввести в систему следующие данные: • Автоматическая работа системы («Вход в зону контроля») • Автоматическая система направления (RM / RM Output) в зависимости от конфигурации КПП. • Регистрационный номер (тягач / прицеп) • Дата и время автоматической регистрации транзакции в системе. Подтверждение регистрации транзакции в разделе AIS «Frontiera» автоматически активирует входной барьер (если применимо). Если контрольно-пропускной пункт подключен к системе ANPR и CCTV, регистрационный номер будет автоматически заполнен системой. В этом случае пользователь должен подтвердить правильность считывания регистрационного номера. Если система ANPR и CCTV не смогла прочесть регистрационный номер или неправильно его интерпретировать, пользователь должен исправить регистрационный номер. А при регистрации транзакции AIS Frontiera отправит на адрес системы ANPR & CCTV информацию о скорректированном номере. Зона выезда должна обеспечивать подтверждение выхода из зоны таможенного контроля, т.е. «AIS Frontiera» предоставляет пользователю список транспортных единиц, для которых разрешен выход из зоны контроля в направлении пункта контроля. Пользователь должен подтвердить выход транспортной единицы к шлагбауму. После подтверждения выхода (закрытия сделки) «AIS Frontiera» автоматически активирует выходной барьер (если есть). Если контрольно-пропускной пункт подключен к системе ANPR и видеонаблюдения, решение о закрытии транзакции будет принято системой автоматически. Если система ANPR и CCTV не смогла прочесть регистрационный номер или неправильно его интерпретировать, пользователь должен исправить регистрационный номер. А при регистрации транзакции AIS Frontiera отправит на адрес системы ANPR & CCTV информацию о скорректированном номере.
12.	Добавление вкладки VICOS для доступа к ANPR и CCTV	В зависимости от конфигурации контрольно-пропускных пунктов, в случаях, когда контрольно-пропускной пункт подключен к системе ANPR и видеонаблюдения, AIS Frontiera представит пользователям вкладку VICOS TAB. Вкладка будет содержать графическую информацию (изображения, видео), присвоенную транспортной единице при ее проверке. В случаях, когда система ANPR и CCTV не может связать транзакцию с графической информацией, AIS Frontiera заставит пользователя вручную назначить графические изображения транзакции. В этом случае «AIS Frontiera» предоставит пользователю список изображений и видео, которые не были привязаны к какой-

		либо транзакции. Пользователь выберет одно или несколько изображений / видео и прикрепит их к транзакции. Если КПП подключен через систему VICOS к шлагбауму и (или) светофору, AIS Frontiera предоставит пользователю (через TAB) ручное управление шлагбаумом и/или светофором.
Другие функции		
13.	Возврат	Функция возврата будет доступна пользователю на таможенном посту для начальника смены и местного администратора. Опция может использоваться для всех активных транзакций, независимо от того, были ли проверки завершены или нет. Транзакция будет направлена на контрольную точку выхода с того направления, через которое транзакция была записана. При выборе операции возврата пользователь системы должен исправить как минимум следующие данные: • Дата и время операции (автоматическая система) • Данные о пользователе, выполнившем операцию возврата (система автоматическая) • Причина возврата (классификатор) • Комментарии к операции возврата (свободный текст)
14.	Разгрузка в зоне таможенного контроля	В настоящее время AIS Frontiera не ведет учет товаров, хранящихся на территории зоны таможенного контроля (без процедуры таможенного оформления). На практике часто случается, что по разным причинам перевозчики не могут ввозить или вывозить в / из страны определенные категории товаров (отсутствие документов, отсутствие финансовых средств для таможенного оформления и т. Д.). В этом случае AIS Frontiera предоставит пользователю на таможенном посту возможность зафиксировать факт выгрузки (хранения) товаров в зоне таможенного контроля. По крайней мере, следующие данные будут записаны для регистрации операции загрузки в «AIS Frontiera»: • Идентификатор транзакции • Загрузить идентификатор операции • Дата и время операции (автоматическая система) • Данные о пользователе, выполнившем операцию загрузки (система автоматическая) • Причина разгрузки (консервации) (классификатор) • Комментарии к операции загрузки (свободный текст) • Место хранения • Код товара (4-10 знаков) • Описание товара • Количество • Масса • Стоимость

		AIS Frontiera позволит регистрировать несколько товаров по мере необходимости.
15.	Погрузка в зоне таможенного контроля	AIS Frontiera позволит забирать товары, хранящиеся в зоне таможенного контроля, двумя способами: • Самостоятельное движение • Погрузка товара в другую транспортную единицу В случае самоперемещения - пользователь на таможенном посту инициирует новую транзакцию и определяет направление выхода. После инициирования транзакции поток продолжится как стандартный поток обработки транзакции. В случае погрузки товаров в другую транспортную единицу пользователь из пункта таможенного контроля прикрепит данные о товарах к сделке, открытой для данной транспортной единицы, и определит направление выхода. Поток обработки будет продолжен как стандартный поток обработки транзакции. В этом контексте AIS Frontiera предоставит пользователю на таможенном посту возможность выбрать из списка товаров, хранящихся в зоне таможенного контроля, товары, которые будут удалены, путем записи следующих данных в систему: • Идентификатор предыдущей транзакции (автоматически из реестра хранимых товаров) • Идентификатор текущей транзакции (автоматическая система) • Идентификатор операции разгрузки (автоматически из реестра консервных товаров) • Дата и время операции (автоматическая система) • Данные о пользователе, выполнившем операцию загрузки (система автоматическая) • Причина загрузки (сохранения) (классификатор) • Комментарии к операции загрузки (свободный текст) • Код товара (4-10 знаков) (автоматически из реестра хранимых товаров) • Описание товара (автоматически из реестра хранимых товаров) • Количество (руководство пользователя в случае частичной и автоматической загрузки системы в случае полной загрузки) • Вес (руководство пользователя в случае частичной и автоматической загрузки системы в случае полной загрузки) • Значение (руководство пользователя в случае частичной и автоматической загрузки системы в случае полной загрузки) AIS Frontiera позволит регистрировать частичную загрузку товаров, если это необходимо. В случае частичной загрузки AIS Frontiera будет управлять запасами товаров, находящихся в зоне таможенного контроля.
16.	Обновление транзакции	Доступ к изменению транзакции будет предоставлен локальному администратору и центральному администратору. Функциональность

		позволит пользователю изменять любые данные для всех контрольно-пропускных пунктов в пределах таможенного поста. AIS Frontiera гарантирует, что транзакция будет поддерживаться до тех пор, пока транзакция не будет изменена как история транзакций. Чтобы зарегистрировать изменение AIS Frontiera, пользователь попросит пользователя ввести как минимум следующие данные: • Дата и время изменения (автоматически) • Пользовательские данные (автоматически) • Причина изменения (классификатор) • Комментарии (свободный текст)
17.	Отмена транзакции	Доступ к отмене транзакций будет предоставлен локальному администратору и центральному администратору. Функционал позволит пользователю полностью отменить транзакцию. AIS Frontiera обеспечит сохранность транзакции и пометит ее индикатором «Отменена». Для регистрации отмены AIS Frontiera потребует от пользователя ввести как минимум следующие данные: • Дата и время отмены (автоматически) • Пользовательские данные (автоматически) • Причина отмены (классификатор) • Комментарии (свободный текст)
Администрирование		
18.	Управление пользователями	В настоящее время управление пользователями осуществляется разработчиками системы. Нет распределения ролей по контрольным путям и другим элементам управления пользователями (активная или свободная смена и т. Д.). Эти несоответствия связаны с первоначальным бременем системы, в которой все контрольные пункты были заменены одним таможенным контрольно-пропускным пунктом. Таким образом, правильное управление пользователями AIS Frontiera обеспечит следующие функциональные возможности: • Регистрация администраторов местного уровня будет разрешена исключительно центральным администраторам. • Регистрация пользователей на уровне контрольной точки будет разрешена локальным администраторам и администраторам на центральном уровне. • Назначение пользователей на контрольных путях и назначение на контрольно-пропускных пунктах будет разрешено сменным менеджерам, местным администраторам и администраторам на центральном уровне. Для регистрации пользователей в системе администратор должен ввести как минимум следующие данные. • Дата и время регистрации (автоматически) • Данные о человеке, который сделал запись (автоматически) • IDNP человека (инструкция) • Имя, имя (веб-сервис ASP)

		• Функция (вручную) • Орган, на имя которого зарегистрировано лицо (классификатор) • Таможенный пост, на котором происходит регистрация (классификатор) • Роль пользователя (классификатор) • Показатель администрирования (указывается для управления таможенными постами, начальниками смен и администраторами) • Статус человека • Дата контакта • электронное письмо После того, как пользователь регистрируется администратором, система присвоит созданному пользователю статус «Ожидает подтверждения». После регистрации пользователь получит ссылку по электронной почте, по которой он сможет продолжить регистрацию (установит имя пользователя и пароль). После завершения записи система присвоит ему статус «Активный». AIS Frontiera будет содержать как минимум следующие роли: • Администратор на центральном уровне • Таможенная служба • Администратор на центральном уровне • Управление таможенным постом • Начальник смены • CP Entry RM • Таможня CP • CP ANSA • Шкала CP • Сканер CP • Склад CP • CP Exit RM В список органов власти должны входить как минимум следующие органы: • Пограничник • Таможенная служба • ANSA • CTIF Пользователи без индикатора «Администрирование» не будут иметь доступа к операциям на станции до тех пор, пока менеджер смены не назначит пользователю путь и контрольную точку во время смены. Для распределения пользователей во время смены AIS Frontiera предоставит начальнику смены интерфейс, в котором будет просматриваться список пунктов пропуска в соответствии с конфигурацией таможенного поста. При выборе контрольной точки система будет просматривать список лиц, имеющих доступ к
--	--	--

		соответствующей контрольной точке. Назначенный руководитель смены для каждого пользователя отмечает следующие индикаторы: • Он в смену (да / нет) • Направление (вход RM или / и выход RM), если контрольная точка обеспечивает • Отслеживание (товаров или / и пассажиров, или / и компакт-диска, или / и тренера), если контрольно-пропускной пункт предоставляет После установки смены менеджером смены все пользователи с «Работает в смене» будут иметь доступ к спискам транзакций в назначенных контрольных точках. Система управления пользователями должна обеспечивать надлежащую практику защиты информации пользователей (шифрование пароля, проверка соответствия пароля, запрос на изменение пароля). AIS Frontiera должна разрешить авторизацию в системе с помощью цифровых подписей.
19.	Конфигурация контрольных точек	Текущая функциональность отсутствует в SI Frontiera. Настройка контрольных точек выполняется разработчиками на уровне исходного кода. Конфигурация пунктов пропуска - чрезвычайно важная функциональность из-за большого разнообразия пунктов пропуска, начиная с типов таможенных пунктов пропуска (железнодорожные, автомобильные, воздушные, пункты пропуска на административном периметре с Приднестровьем) и размеров пунктов пропуска (включая общий въезд / ВПП) Оборудование пунктов пропуска (без весов, со шкалой с несколькими весами и т. д.), с присутствием других ведомств или без присутствия Таможенной службы. В этом контексте AIS Frontiera должна заверить администраторов на центральном уровне в возможности создания каждого отдельного таможенного поста. Интерфейс конфигурации контрольной точки должен требовать от пользователя ввода следующих данных: • Код таможенного пункта пропуска (классификатор Asycuda) • Название таможенного поста (Asycuda Classifier) • Код страны, в которой расположена почта (Asycuda Classifier) • Тип таможенного поста (автомобильный / воздушный / железнодорожный / речной) • Количество входящих путей (вручную) • Количество выходных дорожек (вручную) • Список контрольных точек и их названия (классификационные контрольные точки) • Настроить КПП (набор параметров) Список контрольных точек должен содержать как минимум следующие значения: • CP Entry RM • Таможня CP • CP ANSA

		• Шкала CP • Сканер CP • Склад CP • CP Exit RM При выборе контрольной точки администратор может установить описание контрольной точки. Система позволит дублировать контрольно-пропускные пункты. Параметры конфигурации контрольной точки будут содержать как минимум следующие значения: • Подключен к ANPR (да / нет) • Подключен к светофору (да / нет) • Подключен к шлагбауму (да / нет) • Направление (вход и / или выход) • Режим (пассажиры или / и груз, или / и компакт-диск, или / и тренер) • Назначение взлетно-посадочной полосы (номер трека) • Последовательность расположения (без указания направления трека) • Обязательные проверки (да / нет) • % Проверяет прогресс (0-100) • Случайное распределение (да / нет) Результат настройки таможенного пункта будет служить AIS Frontiera для реконфигурации бизнес-процессов внутри таможенного пункта и окажет прямое влияние на систему управления пользователями.
20.	Система журналов	Все действия пользователей AIS Frontiera должны фиксироваться в журналах, чтобы: • аутентификация (вход и выход) пользователей, успешные и неудачные попытки аутентификации; • Создание, копирование, перемещение, удаление, изменение локальных учетных записей и файлов конфигурации. • неудачные или отклоненные действия пользователя. • пользователь, имеющий доступ к объектам доступа. Журнал должен содержать следующие поля: • Дата и время • название источника события (услуга / услуга) • имя учетной записи / идентификатор пользователя; • IP-адрес клиента; • время начала операции; • время окончания операции; • уровень события (определяется оператором); • категория события (определяется Оператором); • описание события. AIS Frontiera должна предоставить администраторам инструменты для просмотра и фильтрации данных из журнала. «AIS Frontiera»

		предоставляет администраторам инструменты для получения статистических данных из журналов LOG. Для записи в журналы LOG должен быть предусмотрен специальный режим доступа - для системного администратора (для просмотра), а также для сотрудников службы информационной безопасности. Все действия системных администраторов также фиксируются в журналах журнала SI Frontiera.
--	--	--

Приложение В: Институциональные аспекты

Поставщик услуг будет работать под руководством Координатора проекта MOM что касается существенных аспектах задания и под прямым контролем Координатора по закупкам MOM по административным аспектам.

Ожидается, что Поставщик услуг будет тесно сотрудничать с представителями Таможенной службы Республики Молдова, Главного Инспектората Пограничной Полиции, Агентством Электронного Управления, другими государственными органами, задействованными в AIS «FRONTIERA», а также с техническими экспертами MOM.

Все результаты должны быть представлены на английском и румынском языках в бумажном и/или электронном формате. Вся остальная документация, относящаяся к заданию, должна быть на румынском языке. Все представленные документы на английском и румынском языках подлежат вычитке и редактированию для обеспечения соответствия языку и терминологии национального законодательства, регулирующего предмет задания.

Перед подачей окончательных результатов поставщик услуг обсудит проекты документов с вовлеченными сторонами, чтобы конечные продукты отражали их комментарии. Все результаты Поставщика услуг должны быть согласованы с командой проекта MOM.

Поставщик предоставит поддержку своей группе экспертов (back-stopping) во время выполнения контракта.

Поставщики соглашаются, что эксперты предоставят высококачественные результаты и знания и будут участвовать в проекте на указанном уровне и продолжительности. Если в этом отношении потребуются какие-либо изменения, должен быть подан официальный запрос о согласии координатора проекта MOM разрешить замены.

Во время задания группа экспертов Поставщика услуг должна доказать приверженность основным ценностям Организации Объединенных Наций, в частности, уважать различия в культуре, поле, религии, этнической принадлежности, национальности, языке, возрасте, ВИЧ-статусе, инвалидности или другом статусе.

Приложение С: Минимальные критерии отбора и квалификации

Претенденты должны предоставить документальное подтверждение того, что они соответствуют следующим финансовым требованиям:

Средний годовой оборот Участника торгов должен составлять не менее 350 000,00 долларов США (триста пятьдесят тысяч) или эквивалента за последние три (3) года (2018, 2019, 2020), и этот оборот должен быть получен исключительно за счет предоставления систем и услуг информационных технологий (ИТ).

Претендент должен предоставить аудированные финансовые отчеты и балансы за последние три полных финансовых года, демонстрирующие надежность финансового положения Претендента и демонстрирующие наличие у него финансовых ресурсов, необходимых для выполнения требований предлагаемого Контракта.

Опыт и технические возможности:

Участник торгов должен предоставить документальные свидетельства (включая информацию о завершенных контрактах и контактную информацию клиентов, от которых можно получить рекомендации или которых Покупатель может, при необходимости, посетить для ознакомления с системами, введенными в действие Участником торгов), чтобы продемонстрировать что он соответствует следующим требованиям к опыту:

Он должен был проработать не менее 5 лет, и важной частью его бизнеса было предоставление систем информационных технологий (ИТ), включая программное обеспечение и услуги.

Успешно завершенные аналогичные контракты должны быть документально подтверждены копией акта приемки к эксплуатации (или эквивалентной документации, удовлетворяющей покупателя), выданной покупателем (покупателями).

Приложение D: Требования к проектной группе

В техническом предложении, Участник торгов представит данные о персонале, задействованном в проекте, и их квалификации. Приветствуется привлечение квалифицированного персонала с опытом разработки и внедрения информационных систем аналогичной сложности для пограничных и таможенных органов Молдовы.

Для всех членов команды требуется знание английского языка, а знание румынского и / или русского является преимуществом. В связи со сложностью задачи и увеличенной рабочей нагрузкой участнику торгов предлагается предоставить 4 (четыре) разработчика программного обеспечения (Full Stack Software Developers).

Участнику торгов предлагается предоставить следующую основную группу экспертов:

1	Project Manager:
	University degree in Management, Engineering, ITC or another relevant field
	At least 10 (ten) years of professional experience in the field of design, development and implementation of complex software solutions
	At least 3 (three) similar successfully completed ICT projects with similar complexity, in a leading role throughout the entire duration, proven by brief descriptions of project scope and outcome, and proofs of completion
	Experience in the development of software for border/customs authorities would be an advantage
	Proved certification in Project Management
	Proficiency in Romanian, Russian and English language
2	Software Architect:
	University degree in the field of Computer Science and/or Information Technologies
	At least 10 (ten) years of proven track record of designing enterprise systems
	Docker and Kubernetes Certifications is a strong advantage
	Proven track record of designing and successfully implementing projects for the Government of Moldova. Experience with MCloud integration is a strong advantage.
	Proficiency in English language. Knowledge of Romanian or Russian is an asset
3	Senior Technical Lead
	University degree in the field of Computer Science and/or Information Technologies
	At least 5 (five) years of experience developing projects of similar complexity
	Proven track record of designing and successfully implemented projects for the Government of Moldova
	Strong experience and knowledge in MCloud, Java, Docker, Kubernetes, Microservices, Apache Kafka, JavaScript, React
	Fluency in English. Knowledge of Romanian or Russian is an asset
4	Senior Full Stack Software Developer
	University degree in the field of Computer Science and/or Information Technologies
	At least 3 (three) years of experience developing projects of similar complexity
	Experience with MCloud, Java, Docker, Kubernetes, Microservices, Apache Kafka, JavaScript, React
	Fluency in English. Knowledge of Romanian or Russian is an asset
5	Database Developer

	Master's degree in the field of Computer Science and/or Information Technologies
	At least 3 (three) years of experience of developing/maintaining databases of similar complexity
	Oracle professional certification
	Fluency in English. Knowledge of Romanian or Russian is an asset

Приложение Е: Этапы модернизации программного обеспечения и ориентировочные сроки

План действий, предназначенный для выполнения задания, представлен ниже.
Согласно Плану мероприятий, сроки проведения мероприятий по Проекту следующие:

No.	Действие	Предлагаемые сроки
1.	Начальная фаза	<i>1 Месяц</i>
	1) Подготовка подробного рабочего плана, презентации системы управления проектом, коммуникационного плана для предоставления промежуточных и основных результатов работы. Утверждение плана MOM и бенефициаром. 2) Обновление «Технического задания» и его представление в электронном и бумажном формате. Обновленное ТЗ будет соответствовать государственным стандартам для программного обеспечения и документации ИТС, согласованным с MOM и бенефициаром, и должно содержать согласованный список технической документации, которая будет предоставлена после обновления системы. Подробное техническое задание также будет включать требования к оборудованию (серверам и аппаратной инфраструктуре), на котором будет установлено программное обеспечение.	
2.	Фаза II	<i>3 Месяца</i>
	1) Демонстрация функциональности, отвечающей за реализацию ключевых бизнес-процессов и подсистемы администрирования, за исключением функциональности, отвечающей за интеграцию с другими системами. 2) Предоставление документации в бумажной и электронной форме, содержащей план тестирования, тестовые примеры, протокол тестирования системы, предварительные инструкции для пользователя. 3) Утверждение протокола тестирования системы MOM бенефициаром.	
3.	Фаза III	<i>2 Месяца</i>
	1) Демонстрация функциональности, отвечающей за интеграцию с другими системами. Предоставление документации в бумажном и электронном виде, содержащей описание правил разграничения доступа пользователей, параметров интеграции с другими системами.	

	2) Утверждение протокола тестирования системы MOM бенефициаром.	
4.	Фаза IV	<i>1 Месяц</i>
	1) Установка модернизированной информационной системы в производственной среде бенефициара 2) Тестирование обновленной системы. Функциональное тестирование. Тестирование производительности и безопасности. 3) Обучение отобранных пользователей. Требования к обучению описаны в параграфе 6.3.7 настоящего ТЗ. 4) Окончательная приемка и ввод системы в эксплуатацию. Ввод системы в эксплуатацию начинается с подписания акта ввода в эксплуатацию ИТ-системы и начала ее эксплуатации.	
5	Фаза Технической поддержки	<i>12 Месяца</i>
	В течение этого периода поставщик предоставит техническую поддержку для исправления любых недостатков, связанных с функционированием Системы, и поможет бенефициару системы в поддержании способности ИТ-системы предоставлять услуги, а также в модификации продукта (устранение ошибок, оптимизация рабочих параметров, установка и внесение поправок), сохраняя ее целостность. Поставщик услуг также обеспечит передачу дополнительных знаний, если персонал-получатель сочтет это необходимым в период технической поддержки. Кроме того, подрядчик предоставит все доступные обновления и обновления для установленного ИТ-решения, включая СУБД и другие программные компоненты.	
6	Гарантийная поддержка	<i>36 Месяца</i>
	В течение этого периода поставщик принимает на себя обязательство перед бенефициаром по оказанию помощи в устранении проблем, связанных с разработкой / настройкой функциональных возможностей АИС, не выявленных на этапах тестирования и приемки в гарантийный период.	

В целом, для обеспечения разработок потребуется примерно 7 календарных месяцев, 36 календарных месяцев для гарантийной поддержки и 12 месяцев для услуг по техническому обслуживанию.