

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Нижегородский государственный университет им. Н.И. Лобачевского

**А.В. Усков
О.В. Яснев**

ИНФОРМАЦИОННЫЕ ТАМОЖЕННЫЕ ТЕХНОЛОГИИ

Учебное пособие
Часть 2

Рекомендовано ученым советом финансового факультета для студентов ННГУ,
обучающихся по специальности 036401 «Таможенное дело»

Нижний Новгород
2014

УДК 339.543
ББК 32.973
У75

У75 Усков А.В., Ясенов О.В. ИНФОРМАЦИОННЫЕ ТАМОЖЕННЫЕ ТЕХНОЛОГИИ: Учебное пособие. Часть 2. / Под редакцией профессора, к.э.н. Ясенева В.Н. Нижний Новгород: Нижегородский госуниверситет им. Н.И. Лобачевского, 2014 – 60 с.

Рецензенты: д.э.н., профессор **В.С. Чеботарев**
д.э.н., доцент **М.Л. Горбунова**

Учебное пособие «Информационные таможенные технологии» предназначено для проведения лекционных и практических занятий по дисциплине «Информационные таможенные технологии». Содержит сведения об информационно-технической политике Таможенного союза, о функциональных и обеспечивающих компонентах информационной системы таможенных органов, включая новые информационные технологии, а также методы и средства информационной безопасности.

Для студентов, обучающихся по специальности 036401 «Таможенное дело».

УДК 339.543
ББК 32.973

© Нижегородский государственный
университет им. Н.И. Лобачевского

Оглавление

Введение	4
Глава 1. Основы информационных таможенных технологий	6
1.1. Технологии и методы работы с современными справочными системами	6
1.2. Электронное декларирование	12
1.3. Комплексные автоматизированные системы таможенных органов	23
Глава 2. Информационная безопасность информационных систем в таможенных органах	33
2.1. Нормативно правовая база обеспечения информационной безопасности таможенных органов	33
2.2. Информационные угрозы и их виды в таможенных органах	38
2.3. Политика информационной безопасности	45
Список сокращений	54
Библиографический указатель	56

ВВЕДЕНИЕ

Развитие информационных технологий является приоритетным направлением для таможенных органов. Если в начале двадцать первого века наблюдался достаточно сильный разброс как в программном обеспечении для участников внешнеэкономической деятельности, так и для таможенных органов, было слабо развито электронное декларирование, то в настоящее время уже свершившимся фактом стал переход на стопроцентное декларирование товаров и единые комплексные автоматизированные системы, функционирующие в рамках единой автоматизированной системы таможенных органов (ЕАИС). Отметим, что в ЕАИС объединены все технические и программные средства, используемые для автоматизации деятельности ФТС.

На современном этапе в таможенных органах огромное внимание уделено электронному документообороту (ЭДО) непосредственно в самой структуре ФТС. Ставится задача в максимальной степени сократить традиционный (бумажный) документооборот, используя, в том числе опыт зарубежных стран, где ЭДО появился значительно раньше.

В значительной степени упростили взаимодействие между участниками внешнеэкономической деятельности (ВЭД) и таможенными органами разработчики программного обеспечения для участников ВЭД. К наиболее известным относятся ООО «СТМ» и «Софтлэнд» (г. Санкт-Петербург), «Альта-Софт» (Москва) и т.д. Спектр программного обеспечения очень широк. К нему относятся справочные информационные системы, программы для специалистов по таможенному оформлению, непосредственно занимающихся заполнением деклараций на товары, программы для проверки таможенных деклараций, деклараций таможенной стоимости, корректировки таможенной стоимости и описи документов до представления в таможенные органы и для внесения изменений в электронный вид документов, программы для автоматизации работ на таможенном складе, программы, предназначенные для создания документов, необходимых при помещении товаров под таможенную процедуру таможенного транзита, программное обеспечение для электронного декларирования товаров через интернет.

При подготовке материалов первой главы учебного пособия была поставлена задача не только раскрыть теоретические аспекты информационных таможенных технологий, но и привести примеры современного программного обеспечения, которое используют участники ВЭД и таможенные органы в области электронного декларирования товаров.

Непосредственное отношение к информационным технологиям таможенных органов имеют вопросы информационной безопасности. Особое внимание уделяется нормативно-правой базе обеспечения информационной безопасности таможенных органов. В первую очередь это «Концепция обеспечения информационной безопасности таможенных органов Российской

Федерации на период до 2020 г.», разработанная на основе Стратегии национальной безопасности Российской Федерации до 2020 года и Доктрина информационной безопасности Российской Федерации 2000 г.

Учебное пособие по дисциплине «Информационные таможенные технологии» разработано в соответствии с государственным образовательным стандартом высшего профессионального образования.

Пособие предназначено для студентов высших учебных заведений, обучающихся по специальности «Таможенное дело», а также преподавателей, аспирантов и научных сотрудников, интересующихся данной тематикой.

ГЛАВА 1. ОСНОВЫ ИНФОРМАЦИОННЫХ ТАМОЖЕННЫХ ТЕХНОЛОГИЙ

- 1.1. Технологии и методы работы с современными справочными системами.
- 1.2. Электронное декларирование.
- 1.3. Комплексные автоматизированные системы таможенных органов.

1.1. Технологии и методы работы с современными справочными системами

СПС «Консультант Плюс»

Справочно-правовая система «Консультант Плюс» была разработана в 1992 году и на данный момент является самой распространенной СПС (по исследованию ВЦИОМ 2012 г). Система «Консультант Плюс» содержит свыше 20 200 000 документов [40].

Общероссийская Сеть распространения правовой информации «Консультант Плюс» состоит из 300 региональных информационных центров, расположенных в крупных городах, и более 400 сервисных подразделений в небольших населенных пунктах.

Система «Консультант Плюс» содержит следующие разделы:

1. Законодательство. Включает документы Федерального законодательства и 83 субъектов РФ.
2. Судебная практика. Содержит документы высших судебных органов, практику Федеральных арбитражных судов всех 10 округов, арбитражную практику округов по налоговым спорам, судебные акты всех 20 арбитражных апелляционных судов, подборку судебных решений.
3. Финансовые и кадровые консультации. Раздел включает путеводители по налогам, сделкам, кадровым вопросам, консультации в форме «вопрос-ответ», статьи из бухгалтерской прессы.
4. Комментарии законодательства. Содержит постатейные комментарии к законам и кодексам, книги, монографии, учебные пособия, статьи из юридической прессы, консультации для юристов в форме вопрос-ответ.
5. Формы типовых документов-договоров, заявлений, деклараций и т.д.
6. Международные договоры РФ со странами дальнего и ближнего зарубежья (СНГ).
7. Правовые акты по здравоохранению.

Нормативно-правовые базы органов государственной власти

Сайтом Российской газеты www.rg.ru представлена группировка нормативных документов на сайтах органов государственной власти, являющихся справочными интернет-системами:

1. [Банк документов, подписанных Президентом России](http://document.kremlin.ru) – <http://document.kremlin.ru>
2. Нормативные документы Правительства Российской Федерации – <http://government.consultant.ru/>.

3. База данных «Федеральные законы» Федерального Собрания Российской Федерации – <http://graph.garant.ru:8080/SESSION/PILOT/main.htm>.

4. Банк данных «Правовое регулирование деятельности органов внутренних дел Российской Федерации» Министерства внутренних дел – <http://mvd.consultant.ru/>.

5. Банк документов Министерства обороны – http://doc.mil.ru/documents/quick_search.htm

Более полный список представлен на сайте <http://www.rg.ru/zakon.html>.

Справочные информационные системы таможенных органов

В настоящее время для таможенных органов и участников внешнеэкономической деятельности (ВЭД) справочные информационные системы (СИС) представлены широким спектром. Данные программы позволяют найти код, товар и его описание, получить информацию о размерах пошлины, НДС, узнать цены на товары, перевозимые через границу.

В соответствии с письмом «Об обеспечении таможенных органов справочными правовыми системами» от 9 августа 2001 г. N 01-25/31868 были заключены договора о сотрудничестве в области правовой информатизации с ЗАО «Консультант Плюс» (19.02.2001), некоммерческим партнерством «Информационно-правовой консорциум «Кодекс» (22.06.2001), ООО Научно-производственное предприятие «Гарант – Сервис» (09.07.2001) и ООО «Равновесие – Медиа» (09.07.2001).

В соответствии с упомянутыми договорами организации на безвозмездной основе обеспечивают установку, переустановку в таможенных органах (региональных таможенных управлениях, таможнях, акцизных таможенных постах) справочных правовых систем и их текущее обновление.

В настоящее время работники таможенных органов в основном используют системы «Консультант +» и «ВЭД-Инфо».

Участники ВЭД используют СИС следующих разработчиков: ООО «СТМ», ООО «СОФТЛЭНД», «Альта – Софт».

Справочные информационные системы ООО «СТМ»

ВЭД-Контракт – справочно-информационная программа по среднестатистическим таможенным ценам на ввозимые и вывозимые из Российской Федерации товары с учетом страны их происхождения. Она предназначена для участников внешнеэкономической деятельности и сотрудников таможенных органов [44].

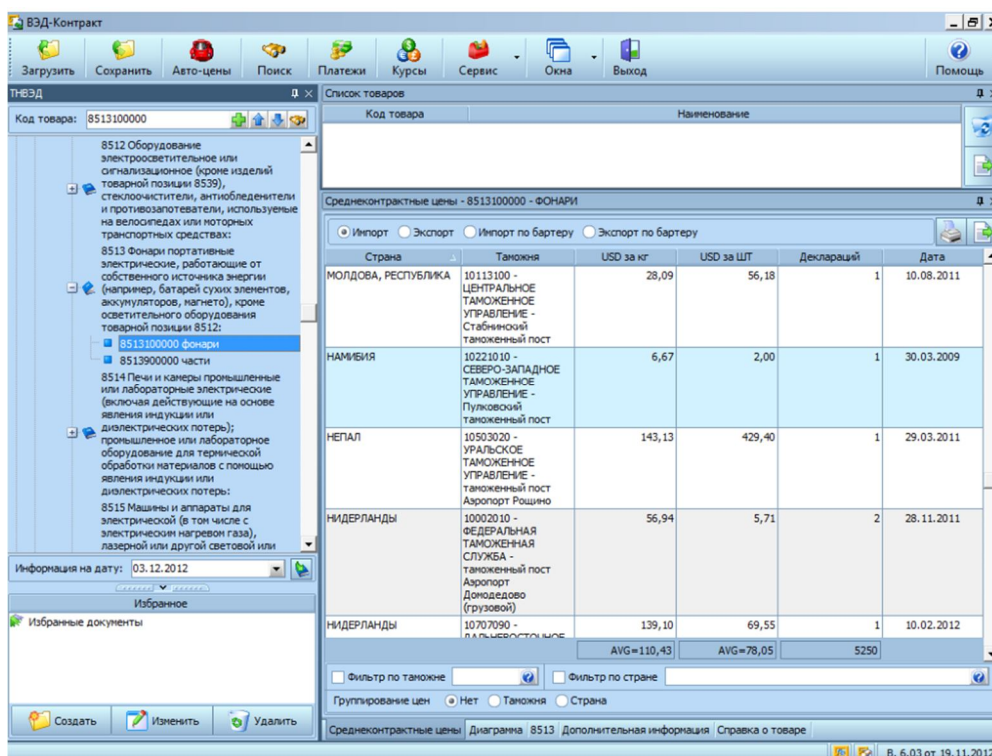


Рис. 1.1. Справочно-информационная программа ВЭД-Контракт

ВЭД-Инфо позволяет найти код и описание конкретного товара и получить справочную информацию о размерах пошлины, акциза, НДС, мерах нетарифного регулирования (лицензируемость товара, необходимость на товар различных сертификатов и др.). ВЭД-Инфо систематизирует нормативные акты по различным направлениям внешнеэкономической деятельности и осуществляет отслеживание изменений законодательства.

ВЭД-Алфавит – дополнение к программе ВЭД-Инфо, алфавитный указатель к ТН ВЭД. Программа позволяет произвести поиск по:

- ЕТН ВЭД (включает не только все слова, входящие в ЕТН ВЭД, но и присутствующие в пояснениях);
- классификационным решениям;
- базе уже декларированных товаров (содержит примерно 300000 наименований).

Рассмотрим справочную систему «ВЭД-Инфо» более подробно.

ВЭД-Инфо

Электронный справочник «ВЭД-Инфо» является полноценным справочником по действующему таможенному законодательству, аналогично правовым базам «Консультант+», «Гарант» или «Кодекс», но ориентированным не на профессиональных юристов, а на специалистов по внешнеэкономической деятельности и таможенных брокеров [44].

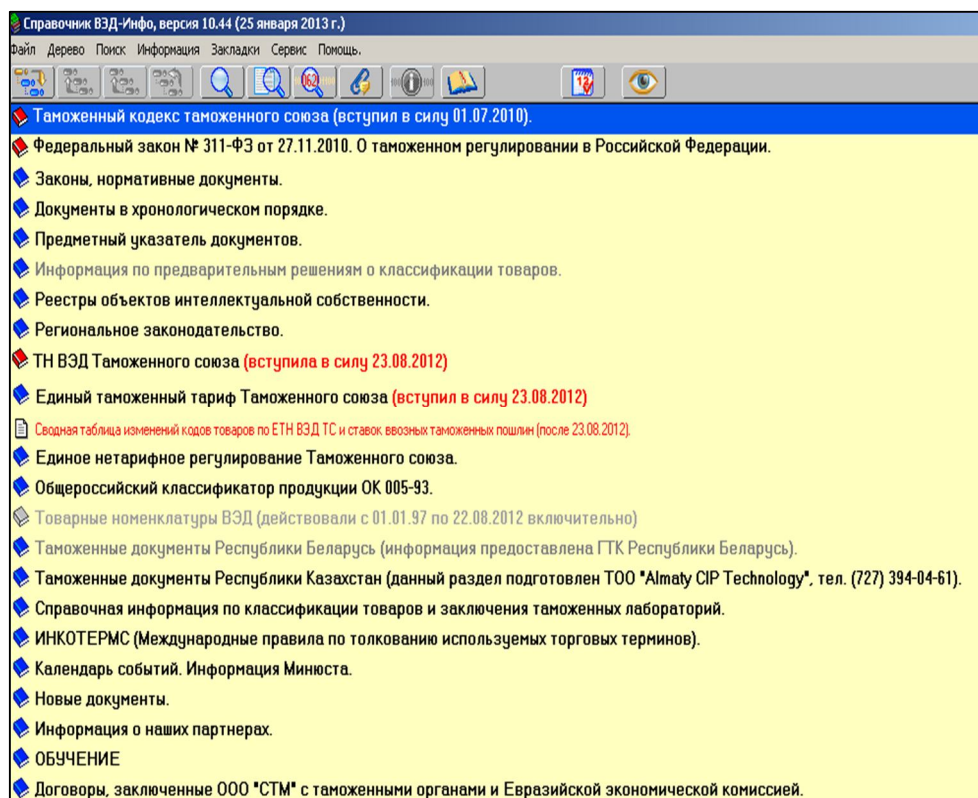


Рис. 1.2. Справочник «ВЭД-Инфо»

Справочник включает в себя:

- базу нормативных документов ГТК РФ (более 10000 документов, начиная с 1950 г.) с гипертекстовыми ссылками между ними и возможностями просмотра, как в хронологическом, так и тематическом порядке;
- подборку правовых документов, связанных с внешнеэкономической деятельностью (Таможенный и Налоговый кодексы, законы РФ, указы Президента, постановления и распоряжения Правительства РФ, международные договоры, ИНКОТЕРМС 1990 и 2000 и проч.);
- товарную номенклатуру внешнеэкономической деятельности (ТН ВЭД СНГ, издание 2-е, и ТН ВЭД России в действующей редакции);
- справочную информацию по классификации товаров (на основании документов ГТК), заключения Центральной таможенной лаборатории;
- функцию получения справки по товару: размер ставок экспортных и импортных пошлин, размер ставок акцизных сборов и НДС, требования к наличию лицензий, сертификатов, разрешений и иные особенности таможенного оформления в зависимости от страны происхождения или страны назначения товара. Все позиции справки имеют гипертекстовую ссылку на тексты соответствующих приказов ГТК РФ или региональных ТУ;
- вызов справочника из других программ фирмы «СТМ» (модульный принцип);
- получение информации о дополнительных единицах измерения для любого товара;

– удобная и быстрая система поиска, настроенная на потребности практиков;

– еженедельное обновление справочника по удобным и современным автоматизированным технологиям;

– горячую линию поддержки для всех пользователей.

«ВЭД-Инфо» распространяется в двух вариантах: базовая и расширенная версии. Расширенная версия программы, помимо функций, включенных в базовую версию, имеет следующие дополнительные возможности:

1. Включены Пояснения к Товарной номенклатуре внешнеэкономической деятельности Российской Федерации, подготовленные ГТК России (издание 2002 года) (в дополнение к Пояснениям, подготовленным Минэкономразвития России – издание 6-е).
2. Реализована возможность загрузки документа или фрагмента документа и работа с ним в формате MS Word (включая таблицы).
3. Реализована возможность загрузки документа или фрагмента документа в формате HTML.
4. Включены и поддерживаются разделы «Международные договора и конвенции», «Документы союзного государства», «Таможенные документы Республики Беларусь».
5. Включен и поддерживается раздел «Региональное законодательство».
6. Включен и поддерживается раздел «Товарные номенклатуры ВЭД» (действовали с 01.01.97 по 31.12.2001 включительно) (вместе со «Справкой о товаре»).
7. Включен Гражданский Кодекс.
8. В раздел «Справочная информация» включен подраздел «Информация по предварительным решениям о классификации товаров», который создан на базе решений, выданных в 2003 году ГУТНР ГТК России.
9. Включен «Сравнительный анализ правил заполнения ГТД (на основе приказов ГТК РФ № 848 от 16.12. 1998 г. и № 915 от 21.08.2003 г.)».
10. Добавлена настройка «Отображать «-» в кодах «ТН ВЭД», позволяющая отображать позиции ТН ВЭД в том виде, в котором они приведены в печатном издании ТН ВЭД.

Справочные информационные системы ООО «СОФТЛЭНД»

ПравоВЭД

Справочно-правовая система (СПС) «ПравоВЭД» ООО «СОФТЛЭНД» содержит полную базу нормативных документов Федерального и Регионального таможенного законодательства и предназначена для изучения таможенного законодательства Российской Федерации и оперативного ознакомления с изменениями вносимыми в него [4].

Программа создана на основе СУБД таким образом, что позволяет осуществлять практически мгновенный поиск необходимого нормативного акта по различным параметрам (номеру, названию, времени и т.д.). При разработке системы использовалась современная технология клиент-сервер.

ТН ВЭД Про

«ТН ВЭД Про» (аналог «ВЭД-Инфо») предназначена для получения справочной информации по товарной номенклатуре внешнеэкономической деятельности. Программа позволяет осуществлять поиск товара по слову или по коду, получить отдельные справки по разным видам налогообложения со ссылками на таможенный документ, формирование полной справки по товару.

Помимо вышеперечисленных функций в «ТН ВЭД Про» входят:

- модуль предварительного расчёта таможенных платежей по коду товара;
- справочник среднеконтрактных цен;
- реквизиты таможен – коды, адреса, телефоны;
- информация по данным банков (названия, адреса, коды ОКПО);
- справочник курсов валют.

Справочные информационные системы ООО «АЛЬТА-СОФТ»

Данный разработчик предлагает следующие программы:

- «Такса» ВЭД-разрешения и платежи.
- «Tax» Russian Custom Duties.
- «ТамДок» Таможенные документы.
- «Пояснения к ТНВЭД».
- «Товары и коды».

«Такса» ВЭД-разрешения и платежи позволяет определить особенности перемещения товара через границу – таможенные сборы, меры нетарифного регулирования, набор необходимых документов, возможные проблемы при оформлении и доставке, а также рассчитать таможенные платежи для товара (или группы товаров) [45].

Пример использования программы представлен на рис.1.3.

[[TAXWIN]] Отчет о товаре

Фирма: Изменить

Код ТНВЭД: 2208609100 [Импорт]

Наименование товара: Водка, с концентрацией спирта более 45, 4 об. %, в сосудах емкостью 2 л или менее

Страна:

Код	Наименование	Тип
012	АЛЖИР	Развив

Ставки сборов:

Тип сбора	Базовые	Минимальные
Пошлина для Прочих	4евро/л	
Акциз	162р/л.сп	
НДС	18%	

Залоговый депозит: 340 руб/л

Особенности товара:

Запреты и ограничения	
Лицензия	Приказ 46 от 06.02.97 (алкогольная продукция)
Сертификат соответствия	Письмо 06-73/44906 от 19.12.06 (сертификация 2007)
Сан/эпид экспертиза	Письмо 06-73/44168 от 14.12.06 (санэпидзаключение - 2007г.)
Акцизная маркировка	Распоряжение 130-р от 10.04.06 (алкогольная продукция)
Усиленный контроль	
Согласование при выпуске	Письмо 01-06/18051 от 19.05.04 (гр."риска" и "прикрытия")

Рис. 1.3. Отчет о товаре в системе «Такса»

Программа «ТамДок», также как «ВЭД-Инфо» и «ПравоВЭД», предназначена для работы с нормативно-справочной базой.

СИС «Пояснения к ТНВЭД» и «Товары и коды» во многом схожи с одноименными программами «СТМ» и «Софтлэнд».

1.2. Электронное декларирование

История внедрения электронного декларирования

Таможенная служба достаточно давно активно внедряет технические новшества информационного характера.

Идея предварительного декларирования возникла в 1996 г. в сфере авиационных перевозок. Тогда термин «предварительное таможенное декларирование» не соответствовал ни таможенному законодательству, ни практике. Было предложено разделить весь процесс внедрения технологии на два блока: электронное предварительное информирование и электронное таможенное декларирование.

С 25 ноября 2002 г. применяется декларирование товаров в электронном виде (ЭД-1). На начальном этапе это был эксперимент, регламентированный Приказом ГТК России от 29 июля 2002 г. №801. Позже приказами ГТК России от 30 марта 2004 г. №395 и от 27 мая 2004 г. №619 был определен порядок совершения таможенных операций при декларировании товаров в электронном виде.

На смену электронному декларированию пришло интернет-декларирование (ЭД-2) (приказом ФТС России от 24 января 2008 г. №52) [18].

Внедрение ЭД-2 значительно расширило возможности участников внешнеэкономической деятельности и позволило уменьшить время совершения таможенных операций и таможенного контроля, сократить расходы, увеличить товарооборот.

Правовые основы применения технологии электронного декларирования

Стандартными правилами 3.11, 3.18 и 3.21 Генерального приложения к Международной конвенции об упрощении и гармонизации таможенных процедур (далее – Киотская конвенция) закреплена возможность представлять таможенным органам декларацию на товары, а также подтверждающие документы в электронном виде посредством электронных средств связи. Глава 7 Киотской конвенции посвящена применению информационных технологий. Так, указывается, что в целях поддержки проведения таможенных операций таможенная служба применяет информационные технологии в тех случаях, когда это экономически выгодно и эффективно для таможенной службы и участников торговой деятельности.

Действующий в настоящее время Таможенный кодекс Таможенного союза выделяет две формы таможенного декларирования товаров: письменную и электронную (ст. 179 ТК ТС). Декларант вправе самостоятельно выбрать

наиболее приемлемую для него форму декларирования. Однако Федеральный закон «О таможенном регулировании» (ст. 204) закрепил электронную форму декларирования товаров как основную и приоритетную. Правительству Российской Федерации предоставлено право устанавливать перечни товаров, таможенных процедур, а также случаи, при которых декларирование может осуществляться в письменной форме.

Федеральным законом «О таможенном регулировании», закреплено положение позволяющее применять исключительно электронную форму декларирования с 01.01.2014 года [3].

С целью реализации указанной нормы необходимо проведение определенных мероприятий по ускоренному внедрению информационных технологий включающих в себя надлежащее оснащение таможенных органов соответствующей техникой, позволяющей организовать бесперебойную работу при представлении таможенным органам сведений в электронной форме с использованием международной ассоциации сетей Интернет.

Технология электронного декларирования

Порядок реализации декларирования товаров в электронной форме регламентирован в действующих в настоящее время: приказ ГТК России от 30.03.2004 №395 «Об утверждении Инструкции о совершении таможенных операций при декларировании товаров в электронной форме» (далее – Инструкция), приказ ФТС РФ от 22.04.2011 №845 «Об утверждении Порядка совершения таможенных операций при таможенном декларировании в электронной форме товаров, находящихся в регионе деятельности таможенного органа, отличного от места их декларирования», приказ ФТС РФ от 01.04.2011 №695 «Об утверждении Временного порядка совершения должностными лицами таможенных органов таможенных операций при таможенном декларировании в электронной форме товаров, классифицируемых в группе 27 ТН ВЭД ТС, в соответствии с Приказом ФТС России от 03.12.2010 № 2330 «О местах декларирования отдельных видов товаров» в случае, если местонахождение данных товаров или место их погрузки и (или) перегрузки (перевалки) не совпадает с местом их декларирования» и рядом других нормативных актов.

Как установлено п. 4 Инструкции о совершении таможенных операций при декларировании товаров в электронной форме, таможенной декларацией, подаваемой в электронной форме, является электронный документ, представляющий собой совокупность сведений, подлежащих указанию в письменной таможенной декларации, поданной в таможенный орган в электронной форме в формате, определенном ФТС России, и подписанной электронной подписью.

По общему правилу при применении электронной формы декларирования не требуется представление документов, подтверждающих заявленные в таможенной декларации сведения.

Уполномоченное должностное лицо таможенного органа по результатам проверки электронной декларации принимает решение о формах таможенного

контроля товаров, а также о необходимости представления электронных документов, указанных в описи документов, прилагаемых к электронной декларации. Принятое решение о необходимости представления электронных документов, указанных в описи, доводится до декларанта посредством авторизованного сообщения.

Лицо, декларирующее товары в электронной форме, может представить электронные документы, необходимые для таможенного оформления, которые будут использоваться в дальнейшем (без внесения в них изменений и дополнений), однократно, в том числе до подачи первой электронной декларации, для их включения в электронный архив. Электронному архиву присваивается индивидуальный номер, который сообщается лицу, декларирующему товары, посредством направления авторизованного сообщения. При декларировании электронных долгосрочные документы, помещенные в электронный архив, повторно таможенному органу не представляются. Лицо, декларирующее товары, указывает номер электронного архива, в котором хранятся электронные долгосрочные документы, относящиеся к поданной декларации, в описи документов.

При этом бумажные экземпляры документов, подтверждающих заявленные в электронной декларации сведения, могут быть потребованы таможенным органом только:

- в случае выявления рисков, по которым в качестве прямых мер по минимизации рисков предусмотрена проверка бумажных носителей информации;
- если в результате таможенного досмотра или таможенного осмотра выявлено несоответствие сведений, заявленных в электронной декларации, и сведений, полученных в результате применения данных форм таможенного контроля.

Следует отметить, что если в результате таможенного досмотра или таможенного осмотра выявлено несоответствие сведений, заявленных в электронной декларации, и сведений, полученных в результате применения форм таможенного контроля, данная декларация распечатывается таможенным органом на бумажном носителе, а лицу, декларирующему товары, направляется авторизованное сообщение, содержащее данную информацию и требование о представлении документов на бумажных носителях. Дальнейшее таможенное оформление товаров должно производиться в общеустановленном порядке с использованием таможенной декларации и документов на бумажных носителях.

Таким образом, применение электронной формы таможенного декларирования товаров имеет большое будущее и хорошие перспективы развития. Существенная часть рабочего времени должностного лица таможенного органа, производящего таможенное оформление, уходит на уведомления и согласования с профильными структурными подразделениями. Приведение всего механизма к электронному знаменателю и автоматизация технических процессов позволит больше времени уделять тщательной проверке документов и сведений, представленных при таможенном оформлении.

Программное обеспечение ЭД-2

В состав программных средств, реализующих информационную технологию по представлению сведений в электронной форме для целей таможенного оформления с использованием сети Интернет, входят:

- автоматизированная подсистема «Представление сведений в электронной форме таможенным органам для целей таможенного оформления в процессе декларирования товаров» (АПС «Электронное представление сведений»);
- программные компоненты комплексной системы таможенного оформления «АИСТ-РТ21» (КАСТО «АИСТ-РТ21»);
- программные компоненты автоматизированной информационной системы таможенного оформления «АИСТ-М» (АИС «АИСТ-М»);
- программные компоненты комплекса программных средств «Экспертная унифицированная проверка электронных копий таможенных документов» (КПС «Контроль»)[44].

АПС «Электронное представление сведений» обеспечивают прием из единой точки входа, расположенной на уровне ЦИТТУ ФТС России, информации, предоставляемой декларантом (брокером), с последующей маршрутизацией принятых сведений до таможенного органа, которому осуществляется декларирование. Вся информация, участвующая в обмене, подписывается электронной цифровой подписью (ЭЦП), проверка корректности которой осуществляется на основе взаимодействия с системой ведомственных удостоверяющих центров таможенных органов (СВУЦ ТО).

Обработка представленных декларантом сведений осуществляется на основе полной интеграции подсистемы электронного представления сведений с автоматизированными системами таможенного оформления и контроля (КАСТО «АИСТ-РТ21» и АИС «АИСТ-М»), позволяя проводить все этапы таможенного оформления в рамках штатных программных средств.

Для целей предварительного контроля достоверности электронных таможенных документов (ГТД, ДТС, КТС и Описи) используется программная компонента, входящая в состав комплекса программных средств «Экспертная унифицированная проверка электронных копий таможенных документов» (КПС «Контроль»).

АПС «Электронное представление сведений» предназначена для реализации процесса автоматизированного информационного взаимодействия между автоматизированными системами (программными средствами) предприятий и организаций (лиц), декларирующих товары и транспортные средства в электронной форме, и используемыми в таможенных органах комплексными автоматизированными системами таможенного оформления и контроля (КАСТО).

АПС «Электронное представление сведений» состоит из двух подсистем:

1) подсистемы «Обработка сообщений», включающей в себя:

- комплекс программных средств (КПС) «Интеллектуальная маршрутизация»;
- КПС «Сервисы функциональной обработки»;

- КПС «Электронный архив декларанта»;
- 2) подсистемы «Управление и контроль», включающей в себя:
 - программную задачу (ПЗ) «Мониторинг-ДКЛ»;
 - КПС «Эксперт-ДКЛ»;
 - ПЗ «Администрирование-ДКЛ».

КПС «Контроль» предназначен для обеспечения форматно-логического контроля таможенных документов, поступающих в АПС «Электронное представление сведений».

КПС «Контроль» состоит из следующих компонент:

- программная задача «Форматно-логический контроль электронных копий таможенных документов» (ПЗ «ФЛК»);
- программная задача «Экспертиза соответствия Правил по стандартизации и алгоритмов контроля электронных копий таможенных документов» (ПЗ «Эксперт»).

АПС «Электронное представление сведений» и ПЗ «ФЛК» функционируют на уровне региональных таможенных управлений.

АПС «Электронное представление сведений» осуществляет информационное взаимодействие с АИС «АИСТ-М» и КАСТО «АИСТ-РТ21», информационными системами участников ВЭД (опосредованно с использованием АСВД).

Информационное взаимодействие АПС «Электронное представление сведений» с АИС «АИСТ-М», КАСТО «АИСТ-РТ21» и АСВД осуществляется средствами, предоставляемыми транспортной технологической подсистемой ЕАИС таможенных органов.

Уровень регионального таможенного управления

На уровне региональных таможенных управлений (далее – РТУ) функционируют следующие программные продукты:

1. АПС «Электронное представление сведений» и ПЗ «ФЛК».
2. Программное обеспечение транспортной технологической подсистемы (ТТП).

На уровне РТУ должно быть установлено серверное оборудование ТТП в кластерной конфигурации.

На уровне РТУ должно быть настроено следующее программное обеспечение ТТП:

- программное обеспечение подсистемы гарантированной асинхронной доставки сообщений;
- программное обеспечение подсистемы информационной безопасности.

Уровень таможни, таможенного поста (ОТОиТК), пункта пропуска

На уровне таможни должно быть установлено серверное оборудование ТТП в кластерной конфигурации.

На уровне таможенного поста (ОТОиТК), пункта пропуска должно быть установлено серверное оборудование ТТП (транспортный сервер).

На транспортную станцию уровня таможни, таможенного поста (ОТОиТК), пункта пропуска должно быть установлено следующее программное

обеспечение:

1. Общесистемное программное обеспечение: операционная система Microsoft Windows Server.

2. Прикладное программное обеспечение ТТП:

- служба Microsoft Cluster (только для уровня таможни);
- программное обеспечение подсистемы гарантированной асинхронной доставки сообщений;
- программное обеспечение подсистемы информационной безопасности.

В таможенных органах, которые будут осуществлять таможенное оформление товаров и транспортных средств, декларируемых в электронной форме участниками внешнеэкономической деятельности, использующими информационную технологию представления таможенным органам сведений в электронной форме для целей таможенного оформления товаров с использованием международной ассоциации сетей «Интернет», должны быть установлены и настроены программные компоненты КАСТО «АИСТ-РТ21» или АИС «АИСТ-М», используемые в рамках данной технологии.

После установки программного обеспечения ЕАИС таможенных органов, необходимого для применения электронной формы декларирования с использованием международной ассоциации сетей «Интернет», совместно с ЦИТТУ ФТС России проводятся комплексные испытания согласно Порядку проведения таможенными органами и ЦИТТУ ФТС России комплексных испытаний программных средств ЕАИС таможенных органов, необходимых для применения электронной формы декларирования с использованием международной ассоциации сетей «Интернет». В случае успешного завершения комплексных испытаний оформляется акт ввода в опытную эксплуатацию программных средств, необходимых для применения электронной формы декларирования с использованием международной ассоциации сетей «Интернет» в соответствующем таможенном органе, утверждаемый начальником РТУ (таможни, непосредственно подчиненной ФТС России).

Электронное декларирование на уровне участника ВЭД

Электронное декларирование (ЭД) – это комплекс программных и аппаратных средств, который позволяет осуществлять таможенное оформление товаров и транспортных средств в электронном виде. Данная система направлена на упрощение взаимодействия между участниками ВЭД и таможенными органами и ускорение процесса таможенного оформления с использованием качественно нового подхода к вопросам таможенного оформления на основе безбумажных технологий [44].

Благодаря использованию системы электронного декларирования участники ВЭД имеют возможность подачи грузовой таможенной декларации из любой точки России.

Функционирование системы основано на принципах обмена информацией между декларантами и уполномоченными должностными лицами таможенного органа («таможенными инспекторами»), исключительно в электронном виде с

использованием электронной цифровой подписи (ЭЦП). Наличие ЭЦП удостоверяет, что передаваемые сведения имеют юридическую силу.

Электронное декларирование – это процесс, который предусматривает предоставление таможенному брокеру, а затем, от него таможенному инспектору, совокупности всех сведений о товарах и транспортных средствах, подлежащих таможенному оформлению, в формализованном виде. В идеале, эта информация должна поступать из-за рубежа, от поставщика товара. На основании этих данных, содержащихся более чем в одиннадцати документах, таможенный брокер может заранее, до прихода транспортного средства на таможенный терминал, подготовить электронную ДТ (ЭДТ). По приходу груза, если загрузка соответствует предварительно высланным документам, и отправитель не производил каких-либо изменений в номенклатуре товаров или их количестве, следовательно, мы имеем уже практически заполненную таможенную декларацию. Далее брокеру только остается внести туда сведения о транспортном средстве и в электронном же виде переслать таможенному инспектору.

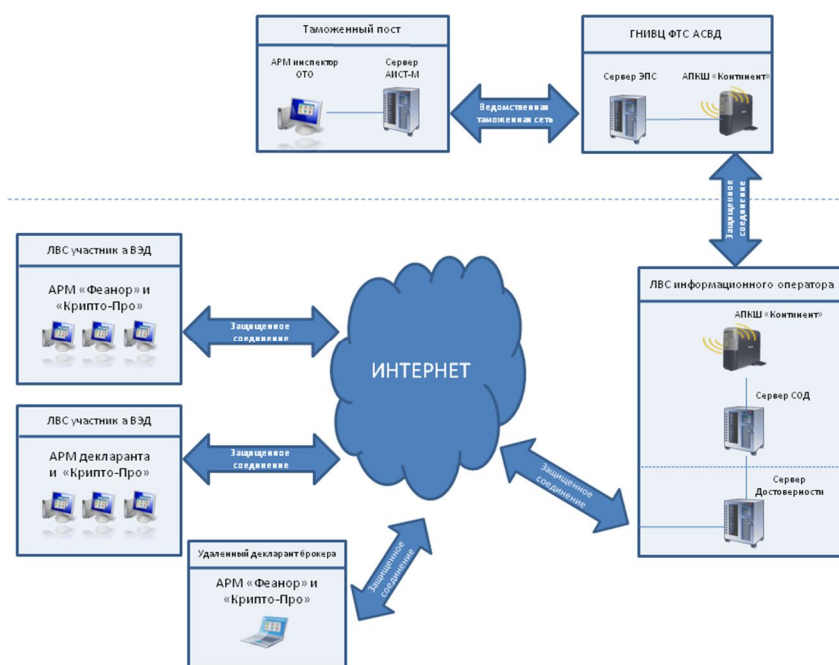


Рис.1.4. Схема электронного декларирования через Интернет

Сотрудник таможни проверяет сведения, заявленные в ЭДТ, и принимает решение о выпуске товаров в соответствии с заявленным таможенным режимом. Надо отметить, что в этом процессе используются документы, их электронный вид, которые носят как долгосрочный характер, например – контракты, так и документы только на данную поставку-инвойс, упаковочный лист, сертификаты и т.д. Это во много раз ускоряет подготовку ЭДТ. Кроме того, уйдя от бумажных носителей информации, мы ускоряем процесс таможенного оформления груза еще и за счет того, что теперь инспектору таможни нет необходимости перелистывать и изучать «гору» документов, входящих в комплект ДТ, при этом сверка данных, заявленных в ЭДТ, происходит в автоматизированном режиме. Процедура закрытия доставки груза

происходит обычным образом.

Электронное декларирование предполагает современный уровень технического оснащения таможенного терминала и позволяет значительно ускорить процесс таможенного оформления грузов.

Система электронного декларирования за счет использования принципов обмена информацией между декларантами и таможенными инспекторами исключительно в электронном виде позволяет участнику ВЭД получить следующую выгоду:

- снижение объема использования бумажной документации (переход на безбумажное оформление);
- подготовка в электронном виде транспортных, коммерческих, финансовых и др. документов, необходимых для таможенного оформления;
- заверение подготовленных документов электронной цифровой подписью;
- формализация и ускорение большинства процедур таможенного контроля и оформления;
- уменьшение времени, затрачиваемого на таможенное оформление.

Речь уже не идет о днях, необходимых инспектору для принятия решения о выпуске товаров, а о считанных часах. Кроме этого, анализ оформления показывает, что электронные декларации выпускаются и в пределах одного часа.

- возможность проведения документального контроля до фактического поступления товаров в таможенный орган назначения, что значительно сокращает время простоя товаров и транспортных средств.
- возможность интегрирования с информационными системами иностранных государств;
- заочное общение с таможенным инспектором и минимизация принятия субъективных решений.

Для таможни:

- это сокращение сроков выпуска ДТ, оптимизация применения людских и материальных ресурсов. Кроме того, электронное декларирование в ФТС России рассматривают как один из важнейших инструментов решения проблем, связанных с недостоверным декларированием, занижением таможенной стоимости, коррупцией;
- снижение трудоемкости работы должностных лиц таможенных органов;
- ускорение поступлений таможенных платежей в государственный бюджет;

На практике процесс декларирования товаров и транспортных средств в электронной форме с участием таможенного брокера с применением комплекса программных средств «Электронное декларирование товаров и транспортных средств» осуществляется следующим образом.

Шаг 1: Клиент при перемещении товаров через границу направляет таможенному брокеру имеющиеся у него документы.

Шаг 2: Таможенный брокер на основании полученных сведений формирует электронную ДТ и направляет ее таможенному инспектору.

Шаг 3: Инспектор проверяет сведения, заявленные в ЭДТ и содержащиеся в пакете документов. Производит все формальности, необходимые при таможенном оформлении, вплоть до определения необходимых мер дополнительного таможенного контроля.

При необходимости уточнения сведений направляет запрос таможенному брокеру.

Шаг 4: После прибытия грузов в таможенную назначения инспектор производит процедуру закрытия доставки товаров и выпускает ДТ.

Технология ЭД-2

1. Участник ВЭД готовит необходимые документы для таможенных целей по ЭД2 в привычном для себя АРМ декларанта.

2. При помощи программы криптопровайдера «КриптоПро» и встроенных средств в АРМ декларанта, подписывает документы своей ЭЦП (фактически производится нажатием одной клавиши).

3. Направляет их через Интернет по зашифрованному каналу на сервер передачи данных Информационного оператора.

4. Сервер Информационного оператора, по зашифрованному каналу связи, в автоматическом режиме пересылает документы участника ВЭД на сервер ЦИТТУ ФТС.

5. Сервер ЦИТТУ ФТС проверяет подлинность ЭЦП и перенаправляет документы на сервер таможенного поста, указанный участником ВЭД.

6. На таможенном посту, инспектор ОТОиТК, при помощи КАСТО «АИСТ-М» производит принятие документов, их проверку и присвоение справочного таможенного номера.

7. Проверенный и принятый к оформлению пакет документов, подписывается ЭЦП принимающего инспектора ОТОиТК и отправляется по обратному пути через сервера таможни, ЦИТТУ ФТС и Информационного оператора к участнику ВЭД.

8. В АРМ декларанта участник ВЭД открывает полученное из таможни сообщение, в котором указан справочный номер пакета высланных им документов, дату и время принятия пакета к таможенному оформлению, ФИО и ЛНП инспектора ОТОиТК принявшего пакет к оформлению.

9. При необходимости, дальнейшие промежуточные этапы таможенного оформления (запрос недостающих документов, требование внесения изменений в документы, информировании о необходимости проведения досмотра товаров и т.д.) производятся путем обмена информационными сообщениями и документами между участником ВЭД и таможенным инспектором.

10. Все сообщения в обязательном порядке подписываются соответствующими ЭПЦ, что придает им юридически значимый статус.

11. По окончании таможенного оформления, инспектор ОТОиТК проставляет в электронной копии документов отметку «Выпуск разрешен», подписывает ее своей ЭЦП и высылает участнику ВЭД.

Проблемы развития электронного декларирования

Несмотря на широкое распространение электронного декларирования с использованием сети Интернет (в начале 2013 года – более 95%) существующие финансовые затраты и организационно-технические проблемы не позволяют ее использовать всем участникам внешнеэкономической деятельности.

Участнику внешнеэкономической деятельности требуется получить электронную подпись и при желании осуществлять декларирование с удаленных рабочих мест (собственных рабочих станций), установить на такие рабочие станции криптографическое программное обеспечение для создания безопасного удаленного соединения.

Заметим, что участники ВЭД по ранее сложившейся практике при использовании электронного декларирования по устаревшей схеме передачи данных по схеме ЭД-1, до сих пор для подключения к системе электронного декларирования прибегают к услугам посредников в передаче электронной информации таможенным органам-информационным операторам.

Схема взаимодействия участников внешнеэкономической деятельности и таможенных органов при посредничестве информационных операторов ранее (ЭД-1) существенно снижала расходы на применение системы электронного декларирования для декларанта, за счет использования дорогостоящей аппаратной части оператора.

В настоящее время внедрение новых технологий практически решило проблему передачи данных через целые системы аппаратного оборудования, используя при этом только наличие выхода в интернет, электронную подпись декларанта и криптографическое программное обеспечение, стоимость которого невелика.

Развитие информационных технологий в таможне

В 2012 году основные усилия ФТС России по информационно-техническому обеспечению деятельности таможенных органов были направлены на техническое оснащение и автоматизацию таможенных операций, на организацию информационного взаимодействия с федеральными органами исполнительной власти по предоставлению государственных услуг и исполнению государственных функций в электронном виде.

Внедрение информационных технологий в деятельность таможенных органов позволит упростить процесс перемещения товаров и транспортных средств через таможенную границу Таможенного союза, снизить административные барьеры и улучшить инвестиционный климат в России.

В целях комплексной реализации положений Федеральных законов от 27 июля 2010 г. N210-ФЗ «Об организации предоставления государственных и муниципальных услуг» и от 28 декабря 2010 г. №394-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с передачей полномочий по осуществлению отдельных видов государственного контроля таможенным органам Российской Федерации», а также Концепции развития национального сегмента Российской Федерации интегрированной информационной системы внешней и взаимной торговли Таможенного союза в

2012 году проведены работы по информационно-техническому обеспечению перевода государственных услуг и государственных функций в электронный вид. Данные работы проводилась совместно с федеральными органами исполнительной власти (далее – ФОИВ) и органами государственных внебюджетных фондов в части получения и передачи информации с использованием системы межведомственного электронного взаимодействия.

ФТС России были разработаны технологические карты межведомственного взаимодействия (далее – ТКМВ) с 25 ФОИВ, в том числе для обеспечения государственных функций (31 ТКМВ) и государственных услуг (15 ТКМВ). Для технической реализации указанных ТКМВ разработаны более 20 электронных сервисов по получению и передаче информации в электронном виде, в том числе разрешительных документов, необходимых для представления таможенным органам при декларировании товара, что позволяет существенно упростить процесс подачи декларации на товары и необходимых документов в электронном виде.

После завершения модернизации автоматизированной системы «База данных разрешительных документов» (АС «БД РД») и взаимодействующих с ней информационно-программных средств Единой автоматизированной информационной системы таможенных органов будет обеспечена автоматизация процесса сверки сведений, указанных в декларации на товары, со сведениями, содержащимися в указанной базе данных, а также контроль должностными лицами таможенных органов Российской Федерации в режиме реального времени представленных разрешительных документов (сведений о них) в электронной форме в процессе декларирования (списание, достоверность сведений, контроль в местах прибытия и убытия).

В 2012 году обеспечена комплексная модернизация автоматизированной системы таможенного оформления и таможенного контроля в пограничных пунктах пропуска (далее – АС «ПП») в части реализации функций по осуществлению транспортного, санитарно-карантинного, карантинного фитосанитарного и ветеринарного контроля, переданных таможенным органам. Проведен комплекс мероприятий по внедрению и доработке АС «ПП» и АПС «СКВВ» (Автоматизированная подсистема контроля за вывозом товаров с таможенной территории Российской Федерации), что позволило обеспечить автоматизированный контроль за фактическим перемещением товаров и централизованный сбор этой информации с целью передачи в ФНС России.

В 2013 году начал работу «Портал электронного декларирования». Это еще один шаг для облегчения деятельности участников внешнеэкономической деятельности. Портал позволяет осуществлять декларирование товаров без использования услуг информационных партнеров и без вложения средств в дополнительное программное обеспечение. В базе данных портала уже зарегистрировано 1520 пользователей этого сервиса из числа участников ВЭД.

1.3. Комплексные автоматизированные системы таможенных органов

До 2003 года на таможенных постах ГТК (Государственный таможенный комитет), в отделах ОТОиТК использовались различные системы оформления документов, такие как «Поток-Пилот», «Поток-Регион», «АИСТ-РТ21», «АРМ ТИ», «АСТО». Единой системы не существовало, ГНИВЦ ГТК (главный научно-исследовательский вычислительный центр ГТК) был вынужден параллельно вносить изменения во все продукты и заниматься их технической поддержкой [44].

К 2003 году был разработан новый проект КАСТО «АИСТ-М» (комплексная автоматизированная система таможенного оформления «АИСТ-М»). «АИСТ-М» является совместной разработкой ООО «Софт-Лэнд», ЗАО «ТАМГА» и ЗАО «ИНМАР».

АИС «АИСТ-М» предназначена для автоматизации таможенных операций при таможенном контроле и выпуске товаров и транспортных средств в таможенных органах России, хранения информации, получаемой в результате выполнения таких процессов, а также предоставления должностным лицам таможенных органов статистической отчетности и оперативной информации о ходе таможенного оформления [31].

«АИСТ-М» состоит из трех автоматизированных подсистем (АПС).

Подсистема «Администрирование» – организация управления процессами таможенной проверки документов и сведений, выпуска товаров и транспортных средств при таможенном декларировании товаров и транспортных средств.

Подсистема «Таможенное оформление» – автоматизация собственно процессов таможенного контроля и выпуска товаров и транспортных средств, а также осуществления информационной поддержки принятия решений должностными лицами таможенных органов в ходе осуществления указанных процессов.

Подсистема «Оперативное информирование» — предоставление пользователям информации о ходе выполнения таможенных операций и статистической отчетности.

Состав АИС «АИСТ-М» показан на рис. 1.5.

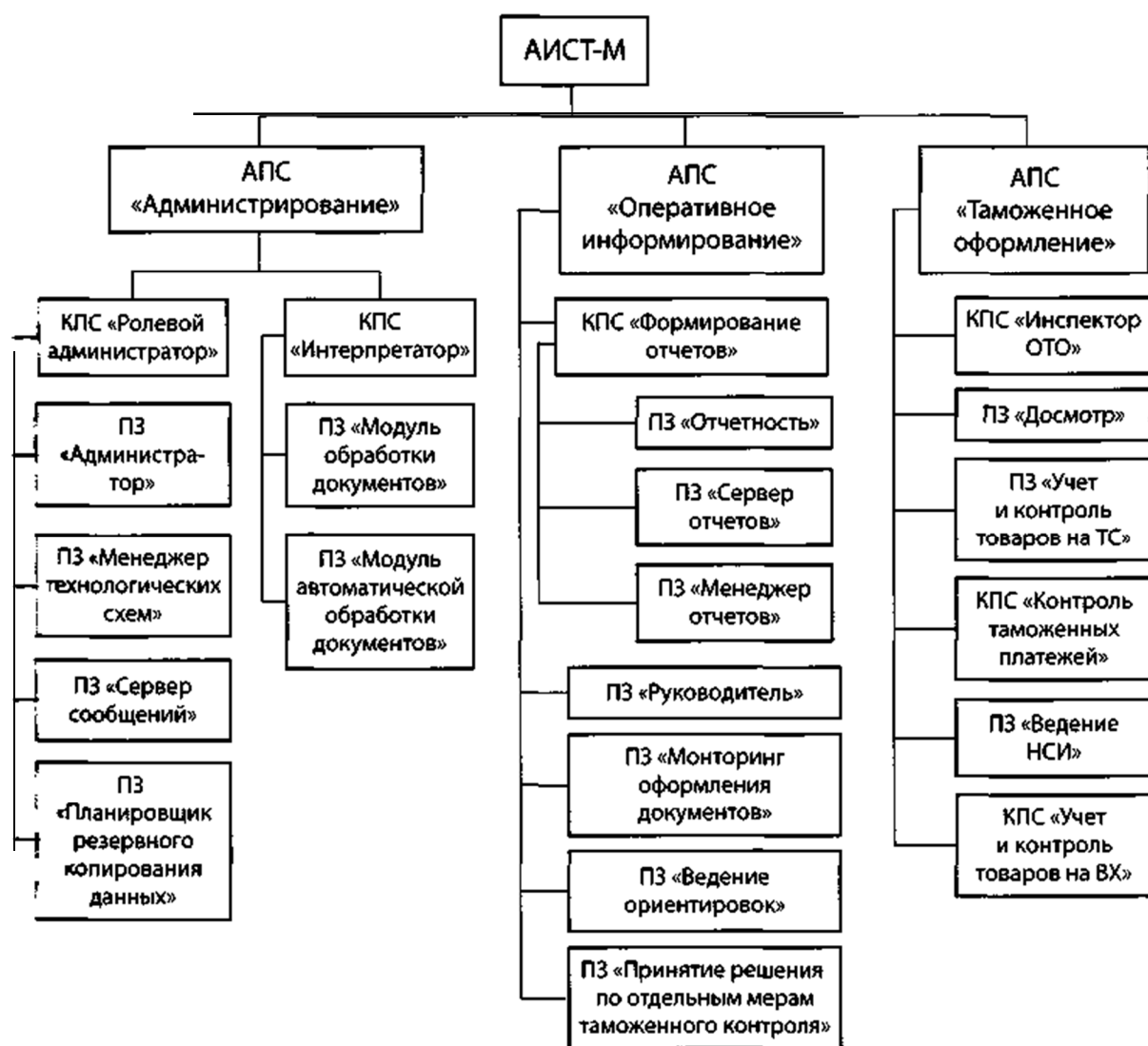


Рис. 1.5. Состав «АИСТ-М»

Подсистема «Ролевой администратор» обеспечивает необходимую гибкость в процессе управления реальным документооборотом за счет возможности произвольно изменять в любой своей части технологическую схему, на которой она основывается при разграничении потоков электронных документов и их передаче между этапами оформления. Эта подсистема с такой структурой может применяться для организации практически любого вида документопотока: таможенное оформление товаров, оформление актов таможенного досмотра или обеспечение делопроизводства.

Подсистема «Таможенное оформление» включает комплекс программных средств, рассчитанных на работу с содержимым электронных документов, и позволяет выполнять контроль и обработку электронной копии ГТД, уведомлений о прибытии или оформлении грузов по ДКД/МДП и дополнительных документов к ним. То же касается оформления товаров на таможенном складе. При этом все действия пользователя (таможенного инспектора) «АИСТ-М» протоколируются, накапливая информацию, которая впоследствии может быть проанализирована руководством.

Последовательность совершения таможенных операций должностным лицом при электронной форме декларирования товаров

Пользователь ПЗ «Модуль обработки документов» оперативно уведомляется о получении ответа на любые отправленные им сообщения в рамках Интернет-декларирования, либо о возникших при этом ошибках. Уведомления отображаются по мере поступления ответов в виде отдельного окна в правой части экрана (рис. 1.6).

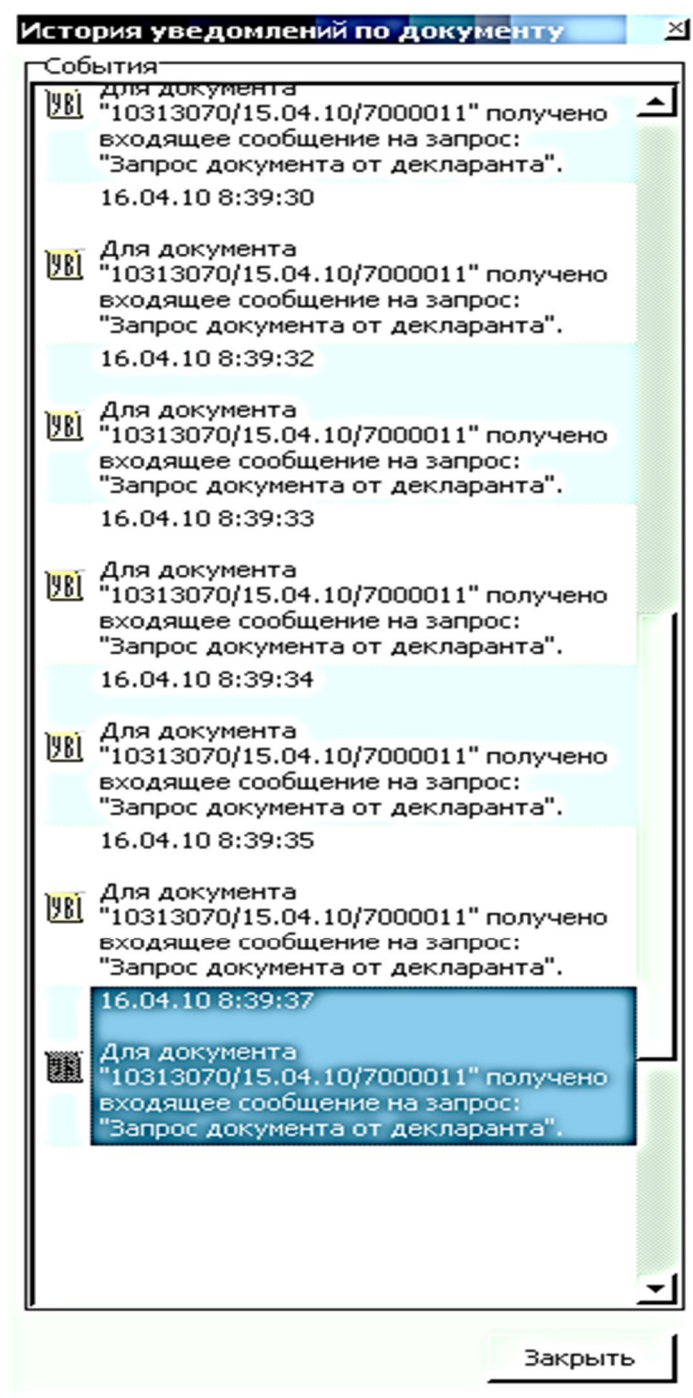


Рис. 1.6. Окно уведомлений АИС «АИСТ-М»

Прием электронных деклараций в систему АИСТ-М, как и весь обмен сообщениями с АПС «Электронное представление сведений», выполняется

автоматически на сервере программной задачей «Модуль автоматической обработки документов» (рис. 1.7).

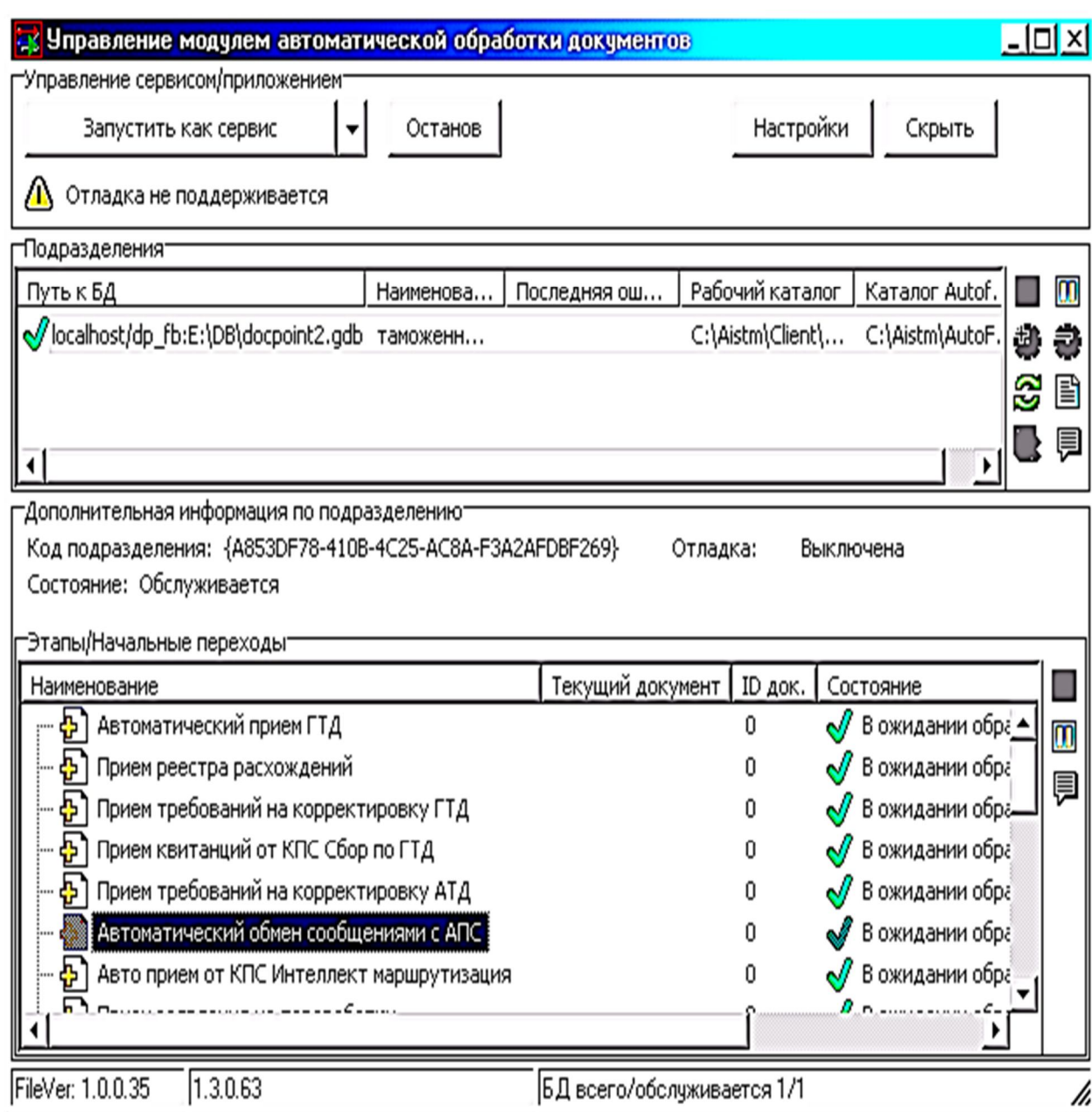


Рис. 1.7. Управление модулем автоматической обработки документов

Для того чтобы взаимодействие производилось в штатном режиме, ПЗ «Модуль автоматической обработки документов» должна быть обязательно запущена и указанные ниже этапы должны находиться в состоянии ожидания обработки ✓ (активны):

- «Автоматический обмен сообщениями с АПС»;
- «Авто прием от КПС Интеллект маршрутизация»;
- «ДТ возвращенные декларанту».

После того как пакет с новой поданной декларацией был принят от АПС «Электронное представление сведений» и был сформирован новый документ в АИС «АИСТ-М», он помещается на этап «Очередь на подачу ДТ» (рис. 1.8).

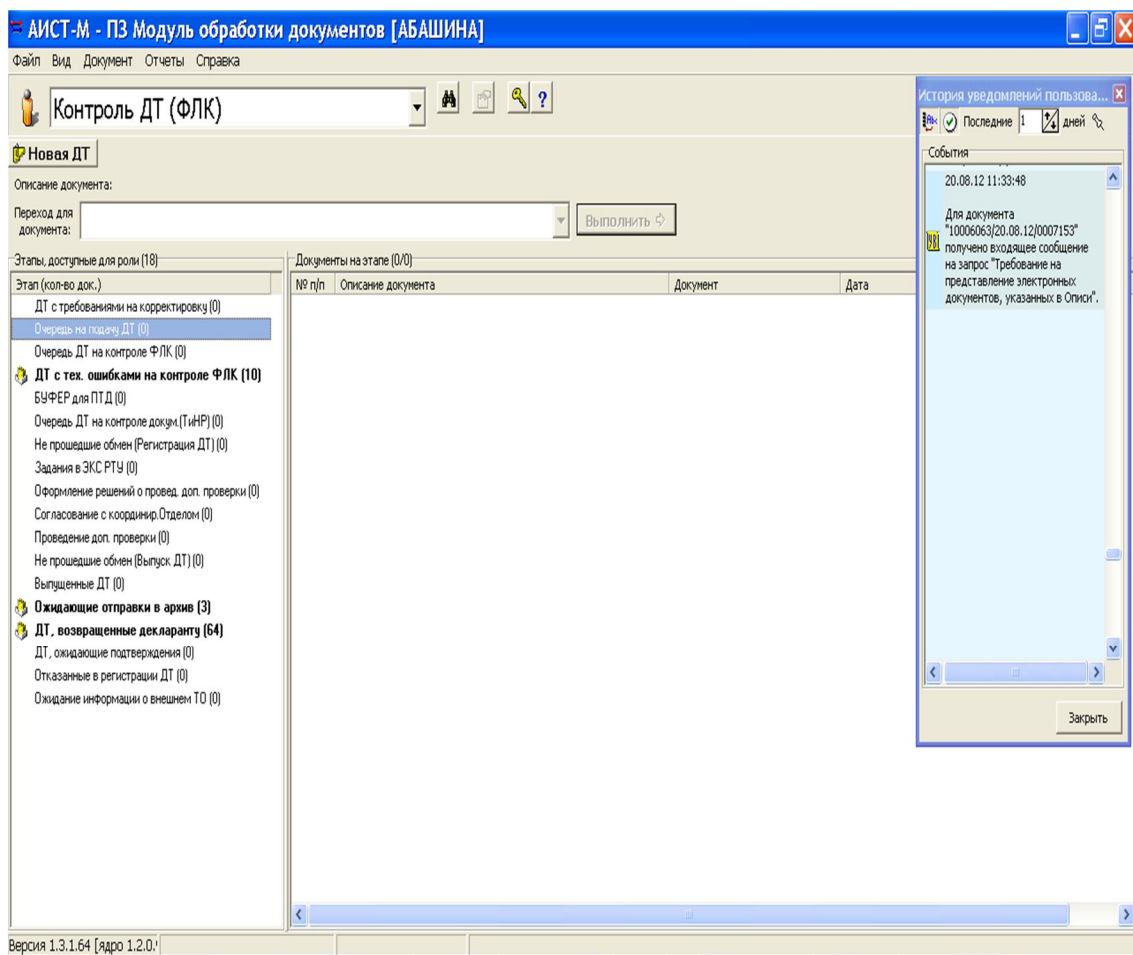


Рис. 1.8. Модуль обработки документов

Отправка на номер. Как и при оформлении обычных ДТ, при выборе данного пункта производится присвоение декларации порядкового номера, при этом формируется сообщение с уведомлением о регистрации для системы декларанта. После этого происходит отправка декларации на сервер на обработку в ПЗ «Модуль автоматической обработки документов».

Возврат (отказ в приеме). При выборе данного пункта декларанту будет сформировано и отправлено уведомление об отказе в приеме ДТ. При выборе данного действия необходимо обязательно заполнить поле «Примечание»: сообщение из данного поля будет отправлено декларанту в качестве объяснения причин отказа в приеме. Сама декларация перемещается на этап «Архив отказанных в приеме ДТ». Подача исправленной ДТ должна осуществляться в рамках той же процедуры.

Отложить в очереди на подачу. При выборе данного пункта ДТ остается на том же этапе («Очередь на подачу ДТ») и перемещается в конец очереди. Декларанту при этом никакая информация не отправляется.

Возврат декларанту протокола ошибок. При выборе данного пункта декларанту будет отправлен протокол ошибок, а сама декларация будет перемещена на этап «ДТ возвращенные декларанту», где будет находиться до того времени, пока от декларанта не поступит исправленная декларация.

Как только декларант внесет требуемые изменения в ДТ и направит ее на таможенное оформление, декларация автоматически переместится с этапа «ДТ возвращенные декларанту» на этап «Очередь на подачу ДТ».

Обработка ДТ начинается так.

После присвоения номера и обработки декларации ПЗ «Модуль автоматической обработки документов» ДТ перемещается на этап «Очередь ДТ на контроле ФЛК». Как только данная декларация будет взята в обработку любым инспектором, автоматически формируется сообщение о начале обработки ДТ, которое будет отправлено декларанту даже в том случае, если инспектор отменит обработку данной декларации. После перехода на данный этап откроется окно, в котором можно работать с ДТ (рис. 1.9 – 1.10).

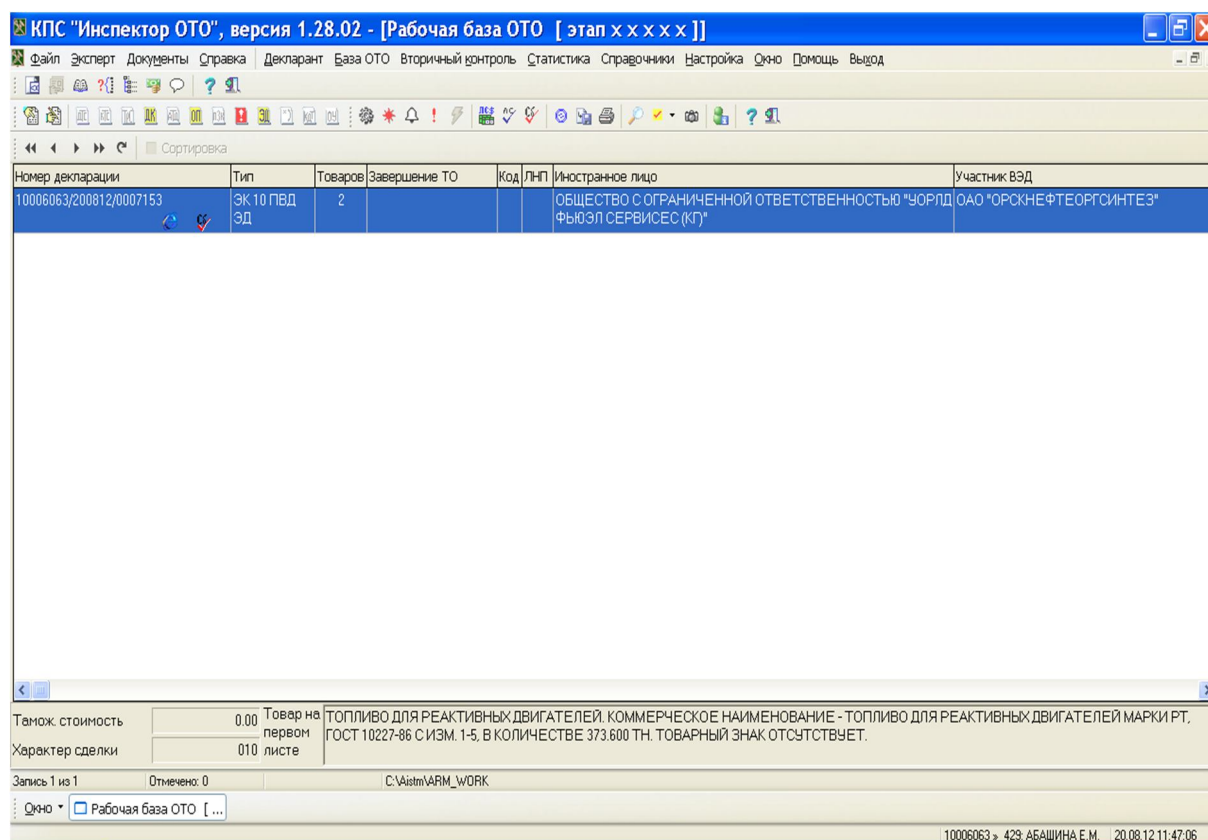


Рис. 1.9. Окно работы с ДТ

Рис. 1.10. Электронная форма декларации на товары

После взятия ДТ в обработку и списания таможенных сборов осуществляется запрос электронных документов.

Выделяют два типа документов при формировании запроса:

- запрос документов из архива декларанта;
- запрос документов лично у декларанта.

В архив декларант помещает документы, которые имеют большой срок действия. В описи, приложенной к декларации, такие документы отмечаются специальным значком .

Для запроса электронных документов используется экранная форма редактирования требования документов (рис. 1.11). Попавшие в систему документы отображаются в окне электронных документов (рис. 1.12).

Требование документов по описи (новый) 10006010/141009/0000024

Общие | Запрашиваемые документы |

Номер ГТД
 10006010 / 2009-10-14 / 0000024

Должностное лицо таможенного органа
 ЛНП 111 ФИО ИВАНОВ И.И.

Таможенный орган
 Код 10006010 Наименование Каспийский трубопроводный таможенный пост

Запрос 1 создан 14.10.2009 13:14:35 направлен 14.10.2009 13:14:35
 Срок предоставления документов 14.10.2009

Средство связи

Рис. 1.11. Редактирование требования электронных документов

КПС "Инспектор ОТО", версия 1.28.02 - [Документы системы ЭД]

Файл Документ Настройка Справка Декларант База ОТО Вторичный контроль Статистика Справочники Настройка Окно Помощь Выход

Всё документы | Принятые | Отправленные | Сохранённые | Справка | Документ

Настроить фильтр документов

Тип документа	Дата	
1002015E DealPass	20.08.12 11:02	Паспорт сделки (ПС) 1112
1002004E Contract	20.08.12 11:02	Договор (контракт) куп
1002014E Supplement	20.08.12 11:02	Дополнение (приложе
1009007E Resolution	20.08.12 11:02	Разрешение, выдавае
1006088E FreeDoc	20.08.12 11:02	Неформализованный д
1006088E FreeDoc	20.08.12 11:02	Неформализованный д
1006088E FreeDoc	20.08.12 11:02	Неформализованный д
1003401E RailwayBill	20.08.12 11:26	Международная желез
1003401E RailwayBill	20.08.12 11:26	Международная желез
1003401E RailwayBill	20.08.12 11:26	Международная желез
1003401E RailwayBill	20.08.12 11:26	Международная желез
1003401E RailwayBill	20.08.12 11:27	Международная желез
1003401E RailwayBill	20.08.12 11:27	Международная желез

Паспорт сделки № 11120153/1481/1948/1/0 от 26.12.2011

Московский Банк Сбербанка России ОАО
 (Наименование уполномоченного банка)

1. Сведения о резиденте

1.1. Наименование: Закрытое акционерное об

1.2. Адрес: Субъект Российской Федерации, Район, Город, Населенный пункт, Улица (проспект, переулок и т. д.), Номер дома (и кладения), Корпус (строение)

1.3. Основной государственный регистрационный номер

1.4. Дата внесения записи в государственный реестр

1.5. ИНН/КПП: 7707743204/

2. Реквизиты иностранного агента

Наименование	Наименование
Общество с ограниченной ответственностью "Ипекс Петролеум" ("Ипекс Петролеум")	КИРГИЗИЯ

3. Общие сведения о контракте

Номер	Дата подписания	Валюта цены	Сумма	Дата завершения исполнения обязательств по контракту	Зачисление на валютный счет	Особые условия
						ввоз/вывоз товаров, указанных в р

Паспорт сделки (ПС) 11120153/1481/1948/1/0 (1002015E.DealPassport)

Сообщение обработано

10006010 / 141009 / 0000024

Рис. 1.12. Редактирование требования электронных документов

Тесты

1. Таможенное оформление, в части взаимодействия с информационными системами, предназначенными для представления участниками внешнеэкономической деятельности сведений таможенным органам в электронной форме, осуществляется в автоматизированной информационной системе:

- **АИСТ-М**
- АИС
- АИС-Налог

2. Какой формы электронного декларирования НЕ существует?

- ЭД-1
- ЭД-2
- ЭД-3

3. Какую программу таможенных органов можно назвать информационно-справочной?

- **ВЭД-Инфо**
- ВЭД-Декларант
- Альта-ГТД

4. На данный момент доля деклараций, оформленных в электронном виде, составляет:

- **100%**
- 99%
- 95%

5. Система АИСТ-М включает:

- **Три подсистемы: «Администрирование», «Оперативное программирование» и «Таможенное оформление»**
- Две подсистемы: «Таможенное оформление», «Администрирование»
- Три подсистемы: «Бухгалтерский учет», «Контроль таможенных платежей», «Электронное декларирование»

6. Система Консультант Плюс содержит:

- около 5 миллионов документов
- 8 миллионов документов
- **свыше 20 миллионов документов**

7. В системе «Консультант Плюс» имеются следующие основные средства поиска:

- Экспресс поиск, Умный поиск, Быстрый поиск
- **Быстрый поиск, Карточка поиска, Правовой навигатор**
- Быстрый поиск, Креативный поиск, Интернет поиск

8. С какого года осуществляется Декларирование товаров?

- **2004 г.**
- 2006 г.
- 2008 г.

Контрольные вопросы

1. Дайте понятие Справочно-правовых систем (СПС).
2. Перечислите основные СПС.
3. Назовите самую распространенную СПС в России. Какие разделы содержит данная система?
4. Какие СПС используются в таможенных органах?
5. Перечислите разработчиков СПС.
6. Какие СПС были разработаны ООО «СТМ»? Опишите их назначение.
7. Каков состав «ВЭД-Инфо»?
8. Какие СПС были разработаны ООО «СОФТЛЭНД» и ООО «АЛЬТА-СОФТ»? Опишите их назначение.
9. Когда стало применяться декларирование товаров в электронном виде?
10. Каковы формы таможенного декларирования товаров?
11. Назовите основную форму таможенного декларирования товаров. Каким законом она определена?
12. Дайте понятие электронного документа.
13. Какие комплексные автоматизированные информационные системы таможенного оформления используются в таможенных органах?
14. Каково назначение АПС «Электронное представление сведений»?
15. Дайте понятие электронного декларирования.
16. Опишите процесс электронного декларирования.
17. Определите стадии ЭД-2.
18. Назовите основные отличия между ЭД-1 и ЭД-2.

ГЛАВА 2. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ В ТАМОЖЕННЫХ ОРГАНАХ

2.1. Нормативно правовая база обеспечения информационной безопасности таможенных органов.

2.2. Информационные угрозы и их виды в таможенных органах.

2.3. Политика информационной безопасности.

2.1. Нормативно правовая база обеспечения информационной безопасности таможенных органов

Современное состояние и острота проблемы обеспечения информационной безопасности в таможенных органах во многом были предопределены темпами автоматизации и внедрения средств вычислительной техники. В полной мере осознавая важность этой проблемы, коллегия ФТС России Приказом от 13 декабря 2010 года № 2401 утвердила «Концепцию обеспечения информационной безопасности таможенных органов Российской Федерации на период до 2020 г.» [17], которая и определила современную штатную структуру и основные задачи ее составляющих, учитывая изменения технологической базы таможенных технологий. Целью разработки Концепции обеспечения информационной безопасности таможенных органов Российской Федерации на период до 2020 года (далее – Концепция) является совершенствование созданной в Федеральной таможенной службе (далее – ФТС России) ведомственной системы обеспечения информационной безопасности при реализации политики Российской Федерации в сфере обеспечения информационной безопасности и защиты информации и при выполнении предписаний правовых актов Российской Федерации в сфере таможенной деятельности, обеспечения информационной безопасности и защиты информации, а также при выполнении правовых актов Таможенного союза.

Концепция разработана на основе Стратегии национальной безопасности Российской Федерации до 2020 года, Доктрины информационной безопасности Российской Федерации, Концепции использования информационных технологий в деятельности федеральных органов государственной власти до 2010 года. Концепции развития таможенных органов Российской Федерации, Стратегии Федеральной таможенной службы до 2020 года и законодательства Российской Федерации, а также иных нормативных правовых актов по информационной безопасности, изданных федеральными органами исполнительной власти в пределах их компетенции. Выполнение мероприятий по обеспечению информационной безопасности является видом основной деятельности таможенных органов Российской Федерации. Концепция служит методологической основой для:

– проведения единой политики обеспечения информационной безопасности таможенных органов Российской Федерации;

- совершенствования правовых актов ФТС России, регламентирующей обеспечение информационной безопасности таможенных органов Российской Федерации;
- совершенствования организационно-режимных и технических мероприятий и методов обеспечения информационной безопасности таможенных органов Российской Федерации;
- разработки планов по дооснащению таможенных органов Российской Федерации сертифицированными по требованиям безопасности информации средствами информатизации (средствами вычислительной техники, телекоммуникационным оборудованием средствами связи, программным обеспечением, средствами защиты информации и т.д.), а также по их внедрению и эксплуатации в повседневной деятельности таможенных органов Российской Федерации;
- подготовки предложений по совершенствованию ведомственной системы обеспечения информационной безопасности таможенных органов Российской Федерации.

Концепция выделяет четыре составляющих национальных интересов Российской Федерации в информационной сфере:

1) соблюдение конституционных прав и свобод человека и гражданина в области получения и использования таможенной информации, а также информации о сведениях и доказательствах, полученных в ходе оперативно-розыскной деятельности, уголовного и административного судопроизводства;

2) информационное обеспечение государственной политики Российской Федерации, связанное с доведением до российской и международной общест-венности достоверной информации о государственной политике Российской Федерации с обеспечением доступа граждан к открытым государственным ин-формационным ресурсам в таможенной сфере;

3) содействие развитию современных информационных технологий отечественной индустрии информации, в том числе индустрии средств информ-матизации, телекоммуникации и связи, обеспечение потребностей внутреннего рынка ее продукцией и выход этой продукции на мировой рынок, а также обес-печение накопления, сохранности и эффективного использования отечествен-ных информационных ресурсов, находящихся в ведении ФТС России;

4) защита информационных ресурсов таможенных органов Российской Федерации от несанкционированного доступа, обеспечение безопасности ин-формационных и телекоммуникационных систем как уже развернутых, так и создаваемых в интересах таможенных органов Российской Федерации.

Целью обеспечения информационной безопасности таможенных органов является защита национальных интересов государства в информационной сфере при осуществлении ФТС России (таможенными органами) функций по выработке государственной политики и нормативного правового регулирова-ния, контроля и надзора в области таможенного дела, а также функций агента валютного контроля и специальных функций по борьбе с контрабандой, иными преступлениями и административными правонарушениями. Речь идет об об-щих, концептуальных началах в данном направлении деятельности, т.е. при

помощи определенных мер защиты поддерживается и обеспечивается защищенность национальных интересов, под которыми следует понимать управленческие меры, направленные на обеспечение информационной безопасности: административные руководящие документы (приказы, распоряжения и инструкции ФТС России); аппаратные устройства или дополнительные программы, основной целью которых является предотвращение преступлений и злоупотреблений.

В основе системы обеспечения информационной безопасности таможенных органов лежит часть 6 Доктрины информационной безопасности Российской Федерации, которая раскрывает особенности обеспечения информационной безопасности Российской Федерации в различных сферах общественной жизни.

Доктрина последовательна в построении системы объектов обеспечения информационной безопасности.

Доктрина информационной безопасности Российской Федерации (далее – Доктрина) утверждена Президентом РФ 9 сентября 2000 г. Этот документ представляет собой совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности РФ. Доктрина служит основой для формирования государственной политики в области обеспечения информационной безопасности Российской Федерации; подготовки предложений по совершенствованию правового, методического, научно-технического и организационного обеспечения информационной безопасности Российской Федерации; разработки целевых программ обеспечения информационной безопасности Российской Федерации.

Нормативно-правовое обеспечение информационной безопасности таможенных органов включает в себя совокупность международных нормативных правовых актов, законов и подзаконных актов Российской Федерации и утверждённых в их исполнении государственных стандартов и технических регламентов.

Итак, Концепция обеспечения информационной безопасности таможенных органов Российской Федерации выделяет следующие нормативные правовые акты ФТС России, участвующие в регулировании обеспечения информационной безопасности таможенных органов:

- Собственно Концепция обеспечения информационной безопасности таможенных органов Российской Федерации на период до 2020 года, утвержденная приказом ФТС России №2401 от 13 декабря 2010 года. Нормативный правовой акт раскрывает роль и место обеспечения информационной безопасности таможенных органов Российской Федерации в обеспечении национальных интересов государства в информационной сфере выделяет основные направления и задачи обеспечения информационной безопасности таможенных органов на период до 2020 года. Отдельный раздел концепции посвящён организации контроля за состоянием обеспечения информационной безопасности таможенных органов.

- Положение о Совете по обеспечению информационной безопасности таможенных органов Российской Федерации, утверждённое приказом ФТС России №924 от 29 июля 2008 года [11]. Совет по обеспечению информационной безопасности таможенных органов Российской Федерации имеет функцию постоянно действующей технической комиссии по защите государственной тайны. Положение раскрывает назначение, цели и задачи, стоящие перед данным органом, раскрывает его структурные особенности и т.п.

- Положение по проведению функциональных проверок таможенных органов Российской Федерации по вопросам организации и состояния обеспечения информационной безопасности и технической защиты информации, утвержденное приказом ФТС России №19 от 19 января 2009 года. Целевой установкой данного нормативного правового акта является регламентация проведения функциональных проверок таможенных органов Российской Федерации по вопросам организации и состояния обеспечения информационной безопасности и технической защиты информации, которая включает в себя органы, осуществляющие проверку и т.п. Его основной задачей является выявление нарушений в проверяемой сфере.

- Программа проведения обучения должностных лиц структурных подразделений ФТС России, таможенных органов Российской Федерации и работников учреждений, находящихся в ведении ФТС России, по вопросам обеспечения информационной безопасности, утверждённая приказом ФТС №710 от 7 июня 2008 года. Данный нормативный правовой акт ставит цели, задачи, определяет направления проведения обучения должностных лиц структурных подразделений ФТС России, таможенных органов Российской Федерации и работников учреждений, находящихся в ведении ФТС России, по вопросам обеспечения информационной безопасности.

- Приказ ФТС РФ от 30.10.2006 г. №1062 «Об обеспечении безопасности информации при информационном взаимодействии таможенных органов с участниками внешнеэкономической деятельности и сетями общего пользования» издан в целях совершенствования обеспечения безопасности информации при декларировании товаров путем заявления таможенным органам сведений в электронной форме.

- Иные ведомственные нормативные правовые документы.

Следует отметить, что за нарушение правовых норм, регулирующих информационную безопасность таможенных органов, положены различные виды ответственности: дисциплинарная, гражданско-правовая, административная, уголовная. Это обусловлено спецификой совершаемого правонарушения. Соответственно, применяемые меры ответственности носят достаточно широкий спектр, начиная от выговора, административного штрафа и оканчивая лишением свободы.

В Уголовном кодексе РФ имеются нормы, затрагивающие ответственность за нарушения информационной безопасности граждан, организаций и государства. В числе таких статей ст. 137 «Нарушение неприкосновенности частной жизни», ст. 138 «Нарушение тайны переписки, телефонных переговоров, поч-

товых и телеграфных или иных сообщений», ст. 140 «Отказ в предоставлении гражданам информации», ст. 155 «Разглашение тайны усыновления (удочерения)», ст. 183 «Незаконное получение и разглашение сведений, составляющих коммерческую или банковскую тайну», ст. 272 «Неправомерный доступ к компьютерной информации», ст. 273 «Создание, использование и распространение вредоносных компьютерных программ», ст. 274 «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно телекоммуникационных сетей» и др.

Федеральный закон от 27.11.2010 N311-ФЗ «О таможенном регулировании в Российской Федерации». Глава 7. Информационные системы и информационные технологии, Статья 101. Защита информации таможенными органами содержит следующие положения:

1) Создание программно-технических и иных средств защиты информации осуществляется по заказу таможенных органов в соответствии с законодательством Российской Федерации. Порядок использования программно-технических и иных средств защиты информации устанавливается федеральным органом исполнительной власти, уполномоченным в области таможенного дела, в соответствии с таможенным законодательством Таможенного союза и законодательством Российской Федерации.

2) Контроль за соблюдением требований к использованию средств защиты информации осуществляют федеральный орган исполнительной власти, уполномоченный в области таможенного дела, и иные федеральные органы исполнительной власти в соответствии с законодательством Российской Федерации.

Защита информации и прав субъектов, участвующих в информационных процессах и информатизации регламентируется статьей 45 Таможенного Кодекса Таможенного союза в соответствии с этой статьей предусматриваются следующие положения:

1) Защита информации и прав субъектов, участвующих в информационных процессах и информатизации, осуществляется в порядке, установленном законодательством государств-членов таможенного союза.

2) Уровень защиты информации, обеспечиваемый программным техническим средством защиты информации, должен соответствовать категории информации. Соответствие уровня защиты информации определенной категории обеспечивается таможенными органами, в ведении которых находятся информационные ресурсы.

В положении «Стратегии развития таможенной службы Российской Федерации до 2020 года [7]. В разделе 8 «Совершенствование информационно-технического обеспечения» установлено, что повышение уровня защищенности информационных ресурсов, расширение спектра мер по обеспечению информационной безопасности, в том числе при организации защищенного обмена информацией с федеральными органами исполнительной власти - это одна из основных задач, решение которой будет содействовать совершенствованию информационно-технического обеспечения деятельности таможенных органов.

Федеральный закон от 06.04.2011 №63-ФЗ «Об электронной подписи» регулирует отношения в области использования электронных подписей при совершении гражданско-правовых сделок, оказании государственных и муниципальных услуг, исполнении государственных и муниципальных функций, при совершении иных юридически значимых действий, в том числе в случаях, установленных другими федеральными законами [4]. Суть Федерального закона сводится к следующим положениям.

Принципами использования электронной подписи (ЭП) являются:

1) право участников электронного взаимодействия использовать ЭП любого вида по своему усмотрению, если требование об использовании конкретного вида ЭП в соответствии с целями ее использования не предусмотрено федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами либо соглашением между участниками электронного взаимодействия;

2) возможность использования участниками электронного взаимодействия по своему усмотрению любой информационной технологии и (или) технических средств при использовании конкретных видов ЭП;

3) недопустимость признания ЭП и (или) подписанного ею электронного документа не имеющими юридической силы только на основании того, что такая ЭП создана не собственноручно, а с использованием средств ЭП для автоматического создания и (или) автоматической проверки ЭП в информационной системе.

2.2. Информационные угрозы и их виды в таможенных органах

Угроза информационной безопасности – целенаправленное действие, которое повышает уязвимость накапливаемой, хранимой и обрабатываемой информации и приводит к ее случайному или преднамеренному изменению или уничтожению.

Итак, *под угрозой безопасности информации (информационной угрозой)* понимается действие или событие, которое может привести к разрушению, искажению или несанкционированному использованию информационных ресурсов, включая хранимую, передаваемую и обрабатываемую информацию, а также программные и аппаратные средства. Если ценность информации теряется при ее хранении и/или распространении, то реализуется угроза нарушения конфиденциальности информации. Если информация изменяется или уничтожается с потерей ее ценности, то реализуется угроза целостности информации. Если информация вовремя не поступает легальному пользователю, то ценность ее уменьшается и со временем полностью обесценивается, тем самым угроза оперативности использования или доступности информации [36].

Итак, реализация угроз информационной безопасности заключается в нарушении конфиденциальности, целостности и доступности информации. Злоумышленник может ознакомиться с конфиденциальной информацией, модифицировать ее, или даже уничтожить, а также ограничить или блокировать

доступ легального пользователя к информации. При этом злоумышленником может быть как сотрудник организации, так и постороннее лицо. Но, кроме этого, ценность информации может уменьшиться ввиду случайных, неумышленных ошибок персонала, а также сюрпризов, иногда преподносимых самой природой.

Информационные угрозы могут быть обусловлены:

- естественными факторами (стихийные бедствия – пожар, наводнение, ураган, молния и другие причины);
- человеческими факторами. Последние, в свою очередь, подразделяются на:

– угрозы, носящие случайный, неумышленный характер. Это угрозы, связанные с ошибками процесса подготовки, обработки и передачи информации (научно-техническая, коммерческая, валютно-финансовая документация); с нецеленаправленной «утечкой умов», знаний, информации (например, в связи с миграцией населения, выездом в другие страны, для воссоединения с семьей и т.п.) Это угрозы, связанные с ошибками процесса проектирования, разработки и изготовления систем и их компонент (здания, сооружения, помещения, компьютеры, средства связи, операционные системы, прикладные программы и др.) с ошибками в работе аппаратуры из-за некачественного ее изготовления; с ошибками процесса подготовки и обработки информации (ошибки программистов и пользователей из-за недостаточной квалификации и некачественного обслуживания, ошибки операторов при подготовке, вводе и выводе данных, корректировке и обработке информации);

– угрозы, обусловленные умышленными, преднамеренными действиями людей. Это угрозы, связанные с передачей, искажением и уничтожением научных открытий, изобретений секретов производства, новых технологий по корыстным и другим антиобщественным мотивам (документация, чертежи, описания открытий и изобретений и другие материалы); подслушиванием и передачей служебных и других научно-технических и коммерческих разговоров; с целенаправленной «утечкой умов», знаний информации (например, в связи с получением другого гражданства по корыстным мотивам). Это угрозы, связанные с несанкционированным доступом к ресурсам автоматизированной информационной системы (внесение технических изменений в средства вычислительной техники и средства связи, подключение к средствам вычислительной техники и каналам связи, хищение носителей информации: дискет, описаний, распечаток и др.).

Умышленные угрозы преследуют цель нанесения ущерба пользователям АИС и, в свою очередь, подразделяются на активные и пассивные.

Пассивные угрозы, как правило, направлены на несанкционированное использование информационных ресурсов, не оказывая при этом влияния на их функционирование. Пассивной угрозой является, например, попытка получения информации, циркулирующей в каналах связи, посредством их прослушивания.

Активные угрозы имеют целью нарушение нормального процесса

функционирования системы посредством целенаправленного воздействия на аппаратные, программные и информационные ресурсы. К активным угрозам относятся, например, разрушение или радиоэлектронное подавление линий связи, вывод из строя ПЭВМ или ее операционной системы, искажение сведений в базах данных либо в системной информации и т.д. Источниками активных угроз могут быть непосредственные действия злоумышленников, программные вирусы и т.п.

Умышленные угрозы подразделяются на **внутренние**, возникающие внутри управляемой организации, и **внешние**.

Внутренние угрозы чаще всего определяются социальной напряженностью и тяжелым моральным климатом.

Внешние угрозы могут определяться злонамеренными действиями конкурентов, экономическими условиями и другими причинами (например, стихийными бедствиями). По данным зарубежных источников, получил широкое распространение **промышленный шпионаж** - это наносящие ущерб владельцу коммерческой тайны, незаконный сбор, присвоение и передача сведений, составляющих коммерческую тайну, лицом, не уполномоченным на это ее владельцем.

К основным угрозам безопасности относят:

- раскрытие конфиденциальной информации;
- компрометация информации;
- несанкционированное использование информационных ресурсов;
- ошибочное использование ресурсов; несанкционированный обмен информацией;
- отказ от информации;
- отказ от обслуживания.

Средствами реализации угрозы *раскрытия конфиденциальной информации* могут быть несанкционированный доступ к базам данных, прослушивание каналов и т.п. В любом случае получение информации, являющейся достоянием некоторого лица (группы лиц), что приводит к уменьшению и даже потере ценности информации.

Реализация угроз является следствием одного из следующих действий и событий: разглашения конфиденциальной информации, утечки конфиденциальной информации и несанкционированный доступ к защищаемой информации. При разглашении или утечке происходит нарушение конфиденциальности информации с ограниченным доступом (рис. 2.1).



Рис. 2.1. Действия и события, нарушающие информационную безопасность

Утечка конфиденциальной информации – это бесконтрольный выход конфиденциальной информации за пределы ИС или круга лиц, которым она была доверена по службе или стала известна в процессе работы. Эта утечка может быть следствием:

- разглашения конфиденциальной информации;
- ухода информации по различным, главным образом техническим, каналам;
- несанкционированного доступа к конфиденциальной информации различными способами.

Разглашение информации ее владельцем или обладателем есть умышленные или неосторожные действия должностных лиц и пользователей, которым соответствующие сведения в установленном порядке были доверены по службе

или по работе, приведшие к ознакомлению с ним лиц, не допущенных к этим сведениям.

Возможен *бесконтрольный уход конфиденциальной информации* по визуально-оптическим, акустическим, электромагнитным и другим каналам.

По физической природе возможны следующие средства переноса информации:

1. Световые лучи.
2. Звуковые волны.
3. Электромагнитные волны.
4. Материалы и вещества.

Под каналом утечки информации будем понимать физический путь от источника конфиденциальной информации к злоумышленнику, по которому возможна утечка или несанкционированное получение охраняемых сведений. Для возникновения (образования, установления) канала утечки информации необходимы определенные пространственные, энергетические и временные условия, а также соответствующие средства восприятия и фиксации информации на стороне злоумышленника.

Применительно к практике с учетом физической природы образования каналы утечки информации можно разделить на следующие группы:

- визуально-оптические;
- акустические (включая и акустико-преобразовательные);
- электромагнитные (включая магнитные и электрические);
- материально-вещественные (бумага, фото, магнитные носители, производственные отходы различного вида – твердые, жидкие, газообразные).

Визуально-оптические каналы – это, как правило, непосредственное или удаленное (в том числе и телевизионное) наблюдение. Переносчиком информации выступает свет, испускаемый источниками конфиденциальной информации или отраженный от него в видимом, инфракрасном и ультрафиолетовом диапазонах.

Акустические каналы. Для человека слух является вторым по информативности после зрения. Поэтому одним из довольно распространенных каналов утечки информации является акустический канал. В акустическом канале переносчиком информации выступает звук, лежащий в полосе ультра (более 20000 Гц), слышимого и инфразвукового диапазонов. Диапазон звуковых частот, слышимых человеком, лежит в пределах от 16 до 20000 Гц, и содержащихся в человеческой речи – от 100 до 6000 Гц.

В свободном воздушном пространстве акустические каналы образуются в помещениях при ведении переговоров в случае открытых дверей, окон, форточек. Кроме того, такие каналы образуются системой воздушной вентиляции помещений. В этом случае образование каналов существенно зависит от геометрических размеров и формы воздухопроводов, акустических характеристик фасонных элементов задвижек, воздухораспределителей и подобных элементов.

Электромагнитные каналы. Переносчиком информации являются

электромагнитные волны в диапазоне от сверхдлинных с длиной волны 10000 м. (частоты мене 30 Гц) до сублимированных с длиной волны 1 – 0,1 мм. (частоты от 300 до 3000 ГГц). Каждый из этих видов электромагнитных волн обладает специфическими особенностями распространения, как по дальности, так и в пространстве. Длинные волны, например, распространяются на весьма большие расстояния, миллиметровые – наоборот, на удаление лишь прямой видимости в пределах единиц и десятков километров. Кроме того, различные телефонные и иные провода и кабели связи создают вокруг себя магнитное и электрическое поля, которые также выступают элементами утечки информации за счет наводок на другие провода и элементы аппаратуры в ближней зоне их расположения.

Материально-вещественными каналами утечки информации выступают самые различные материалы в твердом, жидком и газообразном или корпускулярном (радиоактивные элементы) виде. Очень часто это различные отходы производства бракованные изделия, черновые материалы и др.

В соответствии с Доктриной информационной безопасности Российской Федерации, по своей направленности, в части таможенных органов Российской Федерации угрозы информационной безопасности подразделяются на следующие виды:

1) угрозы конституционным правам и свободам человека и гражданина в информационной сфере деятельности таможенных органов Российской Федерации;

2) угрозы информационному обеспечению государственной политики в области таможенного дела;

3) угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, таможенных органов Российской Федерации в ее продукции, а также обеспечению накопления, сохранности и эффективного использования также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов в области таможенного дела;

4) угрозы обеспечению безопасности информации в автоматизированных системах таможенных органов Российской Федерации.

Угрозами конституционным правам и свободам человека и гражданина в информационной сфере деятельности таможенных органов Российской Федерации могут являться:

- нерациональное, чрезмерное ограничение доступа к общественно значимой информации в области таможенного дела;

- неправомерное ограничение доступа граждан к открытым информационным ресурсам таможенных органов Российской Федерации;

- неисполнение таможенными органами Российской Федерации требований законодательства, регулирующего отношения в информационной сфере;

- нарушение конфиденциальности персональных данных должностных лиц, работников и пенсионеров таможенных органов Российской Федерации,

уволенных из таможенных органов Российской Федерации, и участников внешнеэкономической деятельности, являющихся субъектами персональных данных;

- манипулирование информацией (дезинформация, сокрытие или искажение информации) в области таможенного дела.

Угрозами информационному обеспечению государственной политики Российской Федерации в области таможенного дела могут являться:

- монополизация информационного рынка таможенных органов Российской Федерации отечественными и (или) зарубежными информационными структурами;

- дефицит квалифицированных кадров, отсутствие системы формирования и реализации государственной информационной политики в области таможенного дела.

Угрозами развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей таможенных органов Российской Федерации в ее продукции, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов в области таможенного дела могут являться:

- закупка импортных средств вычислительной техники, телекоммуникации, связи и защиты информации, а также программного обеспечения, при наличии отечественных аналогов, не уступающих по своим характеристикам зарубежным образцам;

- вытеснение с отечественного рынка российских производителей средств вычислительной техники, телекоммуникации, связи и защиты информации, а также разработчиков программного обеспечения.

Угрозами обеспечению безопасности информации в автоматизированных информационных системах таможенных органов Российской Федерации могут являться:

- нарушение технологий обработки информации ограниченного доступа в таможенных органах Российской Федерации;

- нарушение законных ограничений на распространение информации ограниченного доступа, обрабатываемой в таможенных органах Российской Федерации;

- противоправные сбор и использование информации ограниченного доступа, обрабатываемой в таможенных органах Российской Федерации;

- компрометация ключей и средств криптографической защиты информации;

- перехват, дешифрование или подмена информации в ведомственной интегрированной телекоммуникационной сети ЕАИС таможенных органов или передаваемой при информационном взаимодействии ФТС России с таможенными администрациями иностранных государств, международными организациями, федеральными органами исполнительной власти Российской Федерации;

Федерации, организациями банковской сферы и участниками внешнеэкономической деятельности;

- несанкционированный доступ к информации, находящейся в базах данных таможенных органов Российской Федерации;

- неправомерное использование должностными лицами и работниками таможенных органов Российской Федерации информации, к которой им предоставлен доступ, для исполнения должностных обязанностей;

- разработка и распространение программ (компьютерных вирусов), нарушающих нормальное функционирование информационных и информационно-телекоммуникационных систем, в том числе систем защиты информации;

- уничтожение, повреждение, радиоэлектронное подавление или разрушение средств и систем обработки информации, телекоммуникации и связи;

- воздействие на парольно-ключевые системы защиты информационно-телекоммуникационных систем обработки и передачи информации;

- внедрение в аппаратные и программные изделия компонентов, реализующих функции, не предусмотренные документацией на эти изделия;

- внедрение электронных устройств для перехвата информации в технические средства обработки, хранения и передачи информации по каналам связи, а также в служебные помещения таможенных органов Российской Федерации;

- уничтожение, повреждение, разрушение или хищение машинных и других носителей информации;

- использование при разработке и модернизации автоматизированных информационных систем таможенных органов Российской Федерации несертифицированных по требованиям безопасности информационных технологий, средств вычислительной техники, телекоммуникации и связи, программного обеспечения и средств защиты информации;

- угрозы безопасности информации и сформированным на ее основе информационным ресурсам, задействованным в таможенной деятельности, от несанкционированного доступа, обеспечению безопасности информационных и телекоммуникационных систем, как уже развернутых, так и создаваемых на единой таможенной территории Таможенного союза.

2.3. Политика информационной безопасности в таможенных органах

Под информационной безопасностью таможенных органов понимается состояние защищенности национальных интересов государства в информационно сфере деятельности таможенных органов (Приказ ФТС от 13 декабря 2010 года №2401).

Безопасность информации в целом распадается на две составляющие: безопасность содержательной части (смысла информации) и защищенность информации от внешних воздействий либо уничтожения.

В работе таможенных органов по обеспечению информационной безопасности можно выделить несколько направлений.

Во-первых, это защита информации, обрабатываемой в автоматизированных системах (например, антивирусная защита).

Во-вторых, это защита данных, передаваемых между таможенными органами.

В-третьих, это использование средств защиты от несанкционированного доступа.

В-четвертых, это использование электронной цифровой подписи и систем электронного документооборота.

В-пятых, обеспечение безопасности при организации международного информационного обмена.

Защита информации как некогда актуальна на сегодняшний момент. Мы живем в информационном обществе и поглощаем ее ежедневно. Информация порой становится дороже самих материальных благ. Соответственно возникает необходимость в защите. Сейчас безопасность таможенных органов подразумевает не только физическую, материальную сохранность, но и информационную.

Политика безопасности определяется как совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов.

При разработке и проведении ее в жизнь целесообразно руководствоваться следующими принципами:

- ✓ невозможность миновать защитные средства;
- ✓ усиление самого слабого звена;
- ✓ невозможность перехода в небезопасное состояние;
- ✓ минимизация привилегий;
- ✓ разделение обязанностей;
- ✓ эшелонированность обороны;
- ✓ разнообразие защитных средств;
- ✓ простота и управляемость информационной системы;
- ✓ обеспечение всеобщей поддержки мер безопасности.

Поясним смысл перечисленных принципов.

Если у злоумышленника или недовольного пользователя появится возможность миновать защитные средства, он, разумеется, так и сделает.

Надежность любой обороны определяется самым слабым звеном. Злоумышленник не будет бороться против силы, он предпочтет легкую победу над слабостью. Часто самым слабым звеном оказывается не компьютер или программа, а человек, и тогда проблема обеспечения информационной безопасности приобретает нетехнический характер.

Принцип невозможности перехода в небезопасное состояние означает, что при любых обстоятельствах, в том числе нештатных, защитное средство либо полностью выполняет свои функции, либо полностью блокирует доступ.

Принцип минимизации привилегий предписывает выделять пользователям и администраторам только те права доступа, которые

необходимы им для выполнения служебных обязанностей.

Принцип разделения обязанностей предполагает такое распределение ролей и ответственности, при котором один человек не может нарушить критически важный для организации процесс. Это особенно важно, чтобы предотвратить злонамеренные или неквалифицированные действия системного администратора.

Принцип эшелонированности обороны предписывает не полагаться на один защитный рубеж, каким бы надежным он ни казался. За средствами физической защиты должны следовать, программно-технические средства, за идентификацией и аутентификацией – управление доступом и, как последний рубеж – протоколирование и аудит. Эшелонированная оборона способна по крайней мере задержать злоумышленника, а наличие такого рубежа, как протоколирование и аудит, существенно затрудняет незаметное выполнение злоумышленных действий.

Принцип разнообразия защитных средств рекомендует организовывать различные по своему характеру оборонительные рубежи, чтобы от потенциального злоумышленника требовалось овладение разнообразными и, по возможности, несовместимыми между собой навыками (например, умением преодолевать высокую ограду и знанием слабостей нескольких операционных систем).

Очень важен принцип простоты и управляемости информационной системы в целом и защитных средств в особенности. Только для простого защитного средства можно формально или неформально доказать его корректность. Только в простой и управляемой системе можно проверить согласованность конфигурации разных компонентов и осуществить централизованное администрирование. В этой связи важно отметить интегрирующую роль Web-сервиса, скрывающего разнообразия обслуживаемых объектов и предоставляющего единый, наглядный интерфейс.

Принцип всеобщей поддержки мер безопасности – носит нетехнический характер. Если пользователи и/или системные администраторы считают информационную безопасность чем-то излишним или даже враждебным, режим безопасности сформировать заведомо не удастся. Следует с самого начала предусмотреть комплекс мер, направленный на обеспечение лояльности персонала, на постоянное обучение, теоретическое и, главное, практическое.

Методы и средства обеспечения безопасности экономического объекта представлены на рис. 2.2.

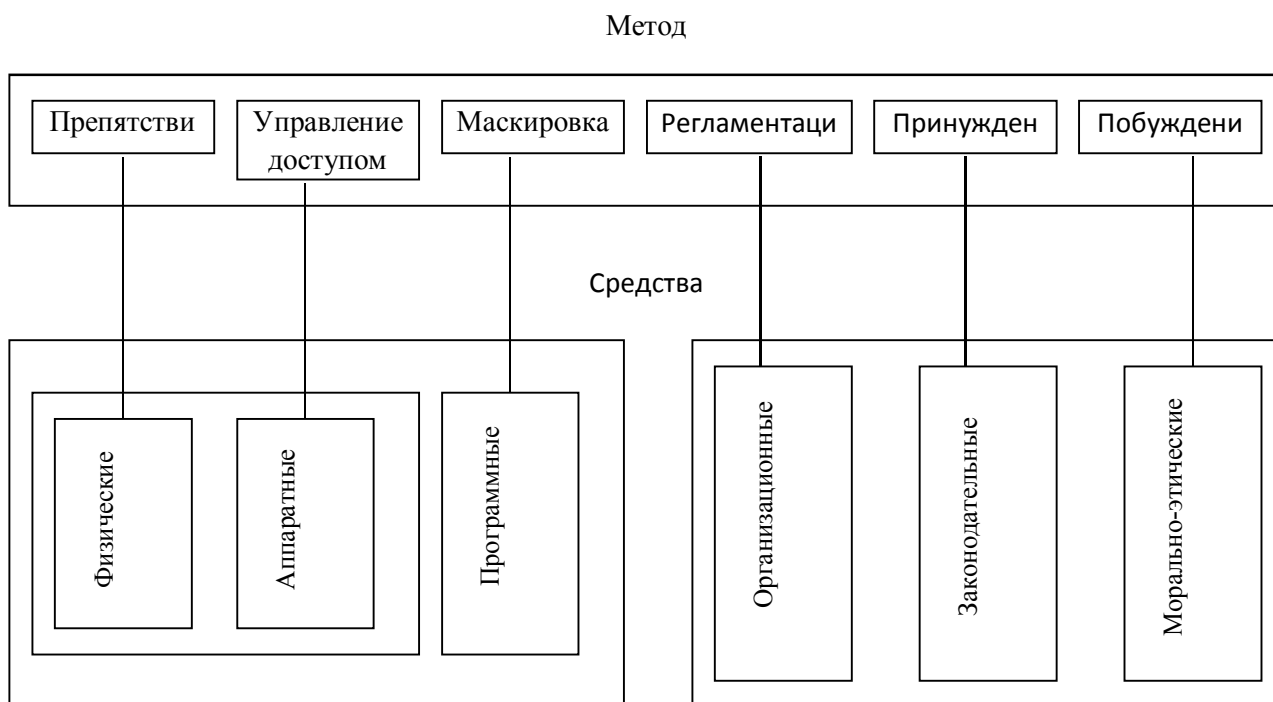


Рис. 2.2. Методы и средства информационной безопасности экономического объекта

Методами обеспечения защиты информации на предприятии являются следующие:

Препятствие – метод физического преграждения пути злоумышленнику к защищаемой информации (к аппаратуре, носителям информации и т.п.).

Управление доступом – метод защиты информации регулированием использования всех ресурсов автоматизированной информационной системы предприятия. Управление доступом включает следующие функции защиты:

- идентификацию пользователей, персонала и ресурсов информационной системы (присвоение каждому объекту персонального идентификатора);
- аутентификацию (установления подлинности) объекта или субъекта по предъявленному им идентификатору;
- проверку полномочий (проверка соответствия дня недели, времени суток, запрашиваемых ресурсов и процедур установленному регламенту);
- регистрацию обращений к защищаемым ресурсам;
- реагирование (сигнализация, отключение, задержка работ, отказ в запросе при попытках несанкционированных действий).

Маскировка – метод защиты информации в автоматизированной информационной системе предприятия путем ее криптографического закрытия.

Регламентация – метод защиты информации, создающий такие условия автоматизированной обработки, хранения и передачи информации, при которых возможность несанкционированного доступа к ней сводилась бы к минимуму.

Принуждение – метод защиты информации, при котором пользователи и

персонал системы вынуждены соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной и уголовной ответственности.

Побуждение – метод защиты информации, который побуждает пользователей и персонал системы не нарушать установленные правила за счет соблюдения сложившихся моральных и этических норм.

Указанные выше методы обеспечения информационной безопасности реализуются с помощью следующих основных средств: физических, аппаратных, программных, аппаратно-программных, криптографических, организационных, законодательных и морально-этических.

Физические средства защиты предназначены для внешней охраны территории объектов, защиты компонентов автоматизированной информационной системы предприятия и реализуются в виде автономных устройств и систем.

Аппаратные средства защиты – это электронные, электромеханические и другие устройства, непосредственно встроенные в блоки автоматизированной информационной системы или оформленные в виде самостоятельных устройств и сопрягающиеся с этими блоками. Они предназначены для внутренней защиты структурных элементов средств и систем вычислительной техники: терминалов, процессоров, периферийного оборудования, линий связи и т.д.

Программные средства защиты предназначены для выполнения логических и интеллектуальных функций защиты и включаются либо в состав программного обеспечения автоматизированной информационной системы, либо в состав средств, комплексов и систем аппаратуры контроля.

Программные средства защиты информации являются наиболее распространенным видом защиты, обладая следующими положительными свойствами: универсальностью, гибкостью, простотой реализации, возможностью изменения и развития. Данное обстоятельство делает их одновременно и самыми уязвимыми элементами защиты информационной системы предприятия.

Аппаратно-программные средства защиты – средства, в которых программные (микропрограммные) и аппаратные части полностью взаимосвязаны и неразделимы.

Криптографические средства – средства защиты с помощью преобразования информации (шифрование).

Организационные средства – организационно-технические и организационно-правовые мероприятия по регламентации поведения персонала.

Законодательные средства – правовые акты страны, которые регламентируют правила использования, обработки и передачи информации ограниченного доступа и которые устанавливают меры ответственности за нарушение этих правил.

Морально-этические средства – нормы, традиции в обществе, например: Кодекс профессионального поведения членов Ассоциации пользователей ЭВМ

в США.

Все рассмотренные средства защиты разделены на *формальные* (выполняющие защитные функции строго по заранее предусмотренной процедуре без непосредственного участия человека) и «*неформальные*» (определяемые целенаправленной деятельностью человека либо регламентирующие эту деятельность).

Для реализации мер безопасности используются различные механизмы шифрования (криптографии).

Криптография – это наука об обеспечении секретности или аутентичности (подлинности) передаваемых сообщений.

Сущность криптографических методов заключается в следующем.

Готовое к передаче сообщение – будь то данные, речь либо графическое изображение того или иного документа, обычно называется *открытым*, или незащищенным текстом. В процессе передачи такого сообщения по незащищенным каналам связи оно может быть легко перехвачено или отслежено подслушивающим лицом посредством умышленных или неумышленных действий. Для предотвращения несанкционированного доступа к сообщению оно зашифровывается, преобразуясь в шифрограмму, или *закрытый текст*. Санкционированный пользователь, получив сообщение, дешифрует или раскрывает его посредством обратного преобразования криптограммы. Вследствие чего получается исходный открытый текст.

Шифрование может быть *симметричным* и *асимметричным*. Первое основывается на использовании одного и того же секретного ключа для шифрования и дешифрования. Второе характеризуется тем, что для шифрования используется один общедоступный ключ, а для дешифрования – другой, являющийся секретным, при этом знание общедоступного ключа не позволяет определить секретный ключ.

Наряду с шифрованием внедряются следующие *механизмы безопасности*:

- электронная подпись;
- контроль доступа;
- обеспечение целостности данных;
- обеспечение аутентификации;
- постановка трафика;
- управление маршрутизацией;
- арбитраж или освидетельствование.

Механизмы электронной подписи основываются на алгоритмах асимметричного шифрования и включают две процедуры: формирование подписи отправителем и ее опознавание получателем. Первая процедура обеспечивает шифрование блока данных либо его дополнение криптографической, контрольной суммой, причем в обоих случаях используется секретный ключ отправителя. Вторая процедура основывается на использовании общедоступного ключа, знания которого достаточно для опознавания отправителя.

Механизмы контроля доступа осуществляют проверку полномочий объектов АИС (программ и пользователей) на доступ к ресурсам сети. При

доступе к ресурсу через соединение контроль выполняется как в точке инициации, так и в промежуточных точках, а также в конечной точке.

Механизмы обеспечения целостности данных применяются к отдельному блоку и к потоку данных. Целостность блока является необходимым, но не достаточным условием целостности потока и обеспечивается выполнением взаимосвязанных процедур шифрования и дешифрования отправителем и получателем. Отправитель дополняет передаваемый блок криптографической суммой, а получатель сравнивает ее с криптографическим значением, соответствующим принятому блоку. Несовпадение свидетельствует об искажении информации в блоке. Однако описанный механизм не позволяет вскрыть подмену блока в целом. Поэтому необходим контроль целостности потока, который реализуется посредством шифрования с использованием ключей, изменяемых в зависимости от предшествующих блоков.

Механизмы постановки трафика, называемые также механизмами заполнения текста, используют для засекречивания потока данных. Они основываются на генерации объектами ЕАИС блоков, их шифровании и организации передачи по каналам сети. Тем самым нейтрализуется возможность получения информации посредством наблюдения за внешними характеристиками потоков, циркулирующих по каналам связи.

Механизмы управления маршрутизацией обеспечивают выбор маршрутов движения информации по коммуникационной сети таким образом, чтобы исключить передачу секретных сведений по небезопасным физически ненадежным каналам.

Механизмы арбитража обеспечивают подтверждение характеристик данных, передаваемых между объектами ЕАИС, третьей стороной. Для этого вся информация, отправляемая или получаемая объектами, проходит через арбитра, что позволяет ему впоследствии подтверждать упомянутые характеристики.

Отметим типичные недостатки, присущие системе безопасности объектов:

- узкое, несистемное понимание проблемы безопасности объекта;
- пренебрежение профилактикой угроз, работа по принципу «Появилась угроза – начинаем ее устранять»;
- некомпетентность в экономике безопасности, неумение сопоставлять затраты и результаты;
- «технократизм» руководства и специалистов службы безопасности, интерпретация всех задач на языке знакомой им области.

Тесты

1. Конфиденциальность компьютерной информации – это...
 - предотвращение проникновения компьютерных вирусов в память ПЭВМ;
 - свойство информации быть известной только допущенным и прошедшим проверку (авторизацию) субъектам системы;
 - безопасность программного обеспечения.
2. Угрозы доступности данных возникают в том случае, когда...
 - объект не получает доступа к законно выделенным ему ресурсам;
 - легальный пользователь передает или принимает платежные документы, а потом отрицает это, чтобы снять с себя ответственность;
 - случаются стихийные бедствия.
3. Защита от утечки по побочным каналам электромагнитных излучений реализуется...
 - средствами контроля включения питания и загрузки программного обеспечения;
 - ограждением зданий и территорий;
 - экранированием аппаратуры и помещений, эксплуатацией защищенной аппаратуры, применением маскирующих генераторов шумов и помех, а также проверкой аппаратуры на наличие излучений.
4. Информационная безопасность таможенных органов – это..?
 - состояние защищенности национальных интересов государства в информационной сфере деятельности таможенных органов;
 - предотвращение ущерба наносимого государственным структурам;
 - компьютерная безопасность, обеспечиваемая комплексом организационных и административных мер.
5. Информационные угрозы не могут быть обусловлены:
 - стихийными бедствиями;
 - программной защитой информационных систем;
 - человеческим фактором, носящими неумышленный характер.
6. К активным угрозам относятся:
 - попытка получения информации, циркулирующей в каналах связи, посредством их прослушивания;
 - разрушение или радиоэлектронное подавление линий связи, вывод из строя ПК или их операционных систем;
 - копирование информации.

Контрольные вопросы

1. Какие существуют угрозы безопасности информации?
2. Назовите угрозы, обусловленные естественными факторами.
3. В чем отличие утечки от разглашения?
4. Какие вы знаете методы обеспечения безопасности?
5. По каким направлениям ведете обеспечение информационной безопасности в таможенных органах?
6. Какие механизмы безопасности применяются в таможенных органах для обеспечения информационной безопасности?
7. На основе каких документов разработана «Концепция информационной базы таможенных органов до 2020 г.?

СПИСОК СОКРАЩЕНИЙ

ФТС РФ – Федеральная таможенная служба Российской Федерации

ТО – таможенные органы Российской Федерации

ЕАИС ТО – Единая автоматизированная информационная система таможенных органов

ВИТС ФТС – Ведомственная интегрированная телекоммуникационная сеть ФТС РФ

ИТП – информационно-техническая политика

ВЭД – внешнеэкономическая деятельность

АС – автоматизированная система

РТУ – региональное таможенное управление

ЛВС – локально-вычислительная сеть

АРМ – автоматизированное рабочее место

ПС – программное средство

СВТ – средство вычислительной техники

БД – база данных

СУБД – система управления БД

ИБ – информационная безопасность

ТЗИ – техническая защита информации

СЗИ – средство защиты информации

НДС – несанкционированный доступ

ЦОД – центр обработки данных

ИТС – информационно-технические средства

ТС – технические средства

ИТТ – информационные таможенные технологии

ИКТ – информационно-коммуникационные технологии

АИСТ – автоматизированная информационная система таможни

ГТК – Государственный Таможенный Комитет РФ (предшественник ФТС)

КАСТО – комплексные автоматизированные системы таможенного оформления

КПС – комплекс программных средств

ПЗ – программная задача

СВУЦ – система ведомственных удостоверяющих центров

СПС – справочно-правовые системы

ТН ВЭД – товарная номенклатура ВЭД

ТПП – транспортная технологическая подсистема

ФЛК – форматно-логический контроль

ЦИТТУ – центральное информационно-техническое таможенное управление

ЭД – электронное декларирование

ЭЦП – электронно-цифровая подпись

ТКТС – таможенный кодекс таможенного союза

ЦИТТУ – центральное информационно-техническое таможенное управление

ПТУ – Приволжское таможенное управление

АС ЭДО – автоматизированная система электронного документооборота

СКУТО – система контроля управления таможенными операциями

СУБД – система управления базой данных

ТСТК – технические средства таможенного контроля

БИБЛИОГРАФИЧЕСКИЙ УКАЗАТЕЛЬ

А. Нормативно – правовые акты

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993)// Российская газета, № 7, 21.01.2009.
2. Федеральный закон от 27.07.2006 №149 – ФЗ (ред. От 28.07.2012) «Об информации, информационных технологиях и о защите информации».
3. Федеральный закон от 27.11.2010 №311 – ФЗ «О таможенном регулировании в Российской Федерации».
4. Федеральный закон №63 – ФЗ от 6 апреля 2011 «Об электронной подписи».
5. Федеральный закон от 26.07.2006 №152 – ФЗ «О персональных данных» – Режим доступа: электронный ресурс. – БД Консультант Плюс.
6. Государственная программа РФ «Информационное общество (2011 – 2020 годы), утверждена Правительством РФ, рассмотрение № 1815 – Р от 20 октября 2010 года.
7. Стратегия развития таможенной службы Российской Федерации до 2020 года, утвержденная распоряжением Правительства Российской Федерации от 28 декабря 2012 года №2575 – р – Режим доступа: электронный ресурс. – Всемирная сеть Интернет.
8. Таможенный кодекс Таможенного союза (приложение к Договору о Таможенном кодексе таможенного союза, принятому Решением Межгосударственного Совета Евразийского экономического сообщества от 27 ноября 2009 г. №17) (с изменениями от 16 апреля 2010 г.) – Режим доступа: электронный ресурс. – БД Консультант Плюс.
9. Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ 09.09.2000 г. №1895).
10. Киотская Конвенция от упрощений и гармонизации таможенных процедур от 18.05.1973 года в редакции протокола от 26.06.1999 г.
11. Приказ ФТС России №924 от 29 июля 2008 г. «Положение о Совете по обеспечению информационной безопасности таможенных органов РФ
12. Постановление Правительства РФ от 28.01.2002 №65 (ред. от 09.06.2010) «О федеральной целевой программе Электронная Россия (2002 – 2010 годы)».
13. Распоряжение Правительства РФ от 06.05.2008 №632 - р (ред. от 10.03.2009) «О концепции формирования в Российской Федерации электронного правительства до 2010 года».
14. Постановление Правительства РФ от 22.09.2009 г. №754 «Об утверждении положения о системе межведомственного электронного документооборота».
15. Постановление Правительства Российской Федерации от 25.01.2013 №33 «Об использовании простой электронной подписи при оказании государственных и муниципальных услуг».
16. Приказ ФТС России от 06.02.2007 №168 «Об утверждении Порядка предоставления должностными лицами таможенных органов доступа к ресурсам центральной базы данных Единой автоматизированной информационной системы таможенных органов (с изменениями,

внесенными приказами ФТС России от 23.11.2012 №2390, от 23.09.2013 №1789).

17. Приказ ФТС России от 13.12.2010 №2401 «Концепция обеспечения информационной безопасности таможенных органов РФ на период до 2020».
18. Приказ ФТС России от 24.01.2008 №52 «О внедрении информационной технологии представления таможенным органам сведений в электронной форме для целей таможенного оформления товаров, в том числе с использованием международной ассоциации сетей.
19. Приказ ФТС России от 03.10.2008 г. №1230 «Об утверждении Инструкции об особенностях совершения должностными лицами таможенных органов отдельных таможенных операций в отношении товаров и транспортных средств, перемещаемых через таможенную границу РФ, с использованием предварительной информации».
20. Приказ ФТС России от 11.02.2009 №162 «О внесении изменений в приказ ФТС России от 24.05.2007 г. №646». Письмо ФТС России от 22.06.2009 г. №09-105/28328 «Требования к аппаратно-программному оснащению таможенных органов, позволяющие проводить таможенное оформление товаров и транспортных средств, декларируемых в электронной форме участниками внешнеэкономической деятельности, использующими информационную технологию представления таможенным органам сведений в электронной форме для целей таможенного оформления товаров с использованием международной ассоциации сетей».
21. Письмо ФТС России от 10.12.2009 г. №2233 «Об утверждении Порядка совершения должностными лицами таможенных органов таможенных операций при декларировании и выпуске товаров и транспортных средств, размещаемых на складах временного хранения, расположенных в местах, приближенных к государственной границе РФ»
22. ФТС РФ Письмо от 22 июня 2009 г. №09.105/28328 «О направлении требований по техническому оснащению таможенных органов».
23. Приказ Федеральной таможенной службы от 17.02.2010 №1154 «Об утверждении положений о Единой автоматизированной информационной системе таможенных органов».
24. Приказ ФТС России от 22.04.2011 г. №845 «Об утверждении порядка совершения таможенных операций при таможенном декларировании в электронной форме товаров, находящихся в регионе деятельности таможенного органа, отличного от места их декларирования».
25. Приказ ФТС от 01.04.2011 г. №695 «Об утверждении временного порядка совершения должностными лицами таможенных органов таможенных операций при таможенном декларировании в электронной форме товаров, классифицируемых в группе 27 ТН ВЭД ТС, в соответствии с приказом ФТС России от 03.12.2010 г. №2330 «О местах декларирования отдельных видов товаров» в случае, если местонахождение данных товаров или место

их погрузки и (или) перегрузки (перевалки) не совпадает с местом их декларирования».

26. Письмо ФТС России от 13.03.2013 №09 – 300/10286 «О рассмотрении проекта Концепции развития ЕАИС ТО».

Б. Список литературы

27. Афонини П.Н., Сальников И.А. Информационное обеспечение в таможенных органах. – СПб.: Санкт – Петербургский филиал РТА, 2011. – 392 с.
28. Афонин П.Н. Информационные таможенные технологии: Курс лекций. – СПб.: РИО СПб филиала РТА, 2010 – 294с.
29. Афонин П.Н. Информационные таможенные технологии: Учебник – СПб.: Троицкий мост, 2012. – 352 с.
30. Малышенко Ю.В. Информационные таможенные технологии: учебник: в 2 ч., ч.1. Ю.В. Малышенко, В.В. Федоров. М.: Изд-во Российской таможенной академии, 2011.
31. Малышенко Ю.В. Информационные таможенные технологии: учебник: в 2 ч. Таможенные технологии: учебник: в 2 ч. Ч.2 Ю.В. Малышенко, В.В. Федоров. М.: Изд-во Российской таможенной академии, 2012.
32. Карасюк В.Н. Практическое применение электронного декларирования Таможенное обозрение, 2011, с.25.
33. Корняков К.А. Перспективы использования новых технологий как средств модернизации таможенного контроля товаров в условиях Таможенного союза // Таможенное дело. 2011. № 4.
34. Суходоев Д.В., Поляков П.П. Основы технических средств таможенного контроля. Учебно – методическое пособие. – Нижний Новгород: Нижегородский государственный университет, 2012.
35. Ясенев В.Н. «Информационная безопасность экономических систем» Изд-во ННГУ 2007 г.
36. Ясенев В.Н. «Информационные системы и технологии в экономике» Изд-во «ЮНИТИ ДИАНА» 2008г.

В. Интернет – ресурсы

37. «Электронное Правительство. Госуслуги.» (электронный ресурс www.gosuslugi.ru).
38. «Электронное правительство NEWS», (электронный ресурс <http://www1.e-gov.su/index.php>).
39. Единая автоматизированная информационная система Федеральной таможенной службы России. (Электронный ресурс) – Режим доступа: <http://cendomzn.ucoz.ru/index/0-1530/>
40. www.consultant.ru
41. www.document.kremlin.ru

- 42. www.rg.ru
- 43. www.doc.mil.ru
- 44. www.ctm.ru
- 45. www.softland.ru
- 46. www.altasoft.ru
- 47. www.customs.ru

Алексей Владимирович **Усков**
Олег Вячеславович **Ясенов**

ИНФОРМАЦИОННЫЕ ТАМОЖЕННЫЕ ТЕХНОЛОГИИ

Учебное пособие
Часть 2

Компьютерная верстка: *Ю.В. Рябинина*

Федеральное государственное автономное образовательное учреждение
высшего образования
«Нижегородский государственный университет им. Н.И. Лобачевского»
603950, Нижний Новгород, пр. Гагарина, 23.

Формат 60х84 1/16
Бумага офсетная. Печать офсетная. Гарнитура Таймс.
Усл. печ. л. ... Уч.-изд. л. ... Заказ № ... Тираж 500 экз.

Отпечатано в типографии Нижегородского госуниверситета
Им. Н.И. Лобачевского
603600, г. Нижний Новгород, ул. Большая Покровская, 37