МИНИСТЕРСВО ОБРАЗОВАНИЯ И НАУКИ РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«ДАГЕСТАНСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

КАФЕДРА ТАМОЖЕННОЕ ДЕЛО

ИНФОРМАЦИОННЫЕ ТАМОЖЕННЫЕ ТЕХНОЛОГИИ

Учебное пособие

для студентов специальности 38.05.02 – «Таможенное дело»

Махачкала - 2018

УДК 339.543:004.9(075.8)
ББК У428с51я73
К332

Учебное пособие по дисциплине «Информационные таможенные технологии»: для студентов, обучающихся по специальности 38.05.02 Таможенное дело, Махачкала, ДГТУ, 2018. – 172 с.

ISBN 978-5-4345-0439-3

Учебное пособие предназначен для студентов дневной и заочной форм обучения специальности 38.05.02 «Информационные таможенные технологии».

В пособии рассмотрено применение информационных технологий в таможенном деле: особенности информационных ресурсов, характеристика программного обеспечения обработки и защиты информации. Учебное пособие содержит все основные темы учебной дисциплины ««Информационные таможенные технологии». По отдельным вопросам приводятся фактические данные, взятые из официальных сборников, что поможет студентам ознакомиться с основными тенденциями и закономерностями развития информационных таможенных технологий.

Составители:

1. **Фастовец И.П.,** доцент кафедры «Таможенное дело» ДГТУ, к.ф.-м.н.
2. **Халимбеков Х.З.**, заведующий кафедры «Таможенное дело», д.э.н.

Рецензенты:

1. **Абдулгалимов А.М.,** зав. кафедрой ИТ и ПИвЭ ДГТУ, д.э.н., профессор.
2. **Омаров М.М.,** начальник отдела ТС и СОСВТ, Дагестанской таможни.

ISBN 978-5-400-00603-6

Печатается по решению Ученого совета Дагестанского государственного технического университета от «___»_____ 2018 г.

ОГЛАВЛЕНИЕ

Список сокращений

АВЗ - антивирусная защита

АИС - автоматизированная информационная система

АНБ - Агентство национальной безопасности

АП - абонентский пункт

АСОИ - автоматизированная система обработки информации

БД - база данных

ВАП - виртуальное адресное пространство

ВИТС - ведомственная интегрированная телекоммуникационная сеть

ГНИВЦ - главный научно-информационный вычислительный центр

ГТД - грузовая таможенная декларация ДСП - для служебного пользования

ЕАИС - единая автоматизированная информационная система

ИВС - информационно-вычислительная сеть

ИТП - информационно-техническая политика

ИТС - информационно-техническая служба

НСД - несанкционированный доступ

ОЗУ - оперативное запоминающее устройство

ОКТЭП - Общесистемный классификатор технико-экономических показателей

ОС - операционная система

РЭБ - радиоэлектронная безопасность

СППР - система поддержки принятия решений

СУБД - система управления базами данных

ТД - таможенная декларация

ТПО - таможенный приходный ордер

ФЛК - форматно-логический контроль

ФС - файловая система

ФТС - Федеральная таможенная служба

ЭВМ - электронно-вычислительная машина

ЭТПТ - электронный таможенный паспорт товара

ЭЦП - электронная цифровая подпись

Глава 1. Характеристика информационных процессов и информационных потоков в системе таможенных органов

1.1 Общие представления об информационных таможенных технологиях

Под технологией в широком смысле понимают науку о производстве материальных благ, включающую три аспекта: информационный, инструментальный и социальный. Информационный аспект включает описание принципов и методов производства, инструментальный - орудия труда, с помощью которых реализуется производство, социальный - кадры и их организацию. В более узком промышленном смысле технология рассматривается как последовательность действий над предметом труда в целях получения конечного результата.

Под информационной технологией понимается система методов, программных и технических средств, интегрированных в целостную технологическую систему для целенаправленного сбора, обработки, накопления, хранения, поиска, распространения и предоставления пользователю (потребителю) документированной информации. Особенность информационных технологий составляет то, что в них и предметом, и продуктом труда является информация, а орудиями труда - средства вычислительной техники и связи. Информационная технология как наука о производстве информации возникла именно потому, что информация стала рассматриваться как вполне реальный производственный ресурс наряду с другими материальными ресурсами.

Понятие информационной технологии, таким образом, неотделимо от той специфической среды, в которой она реализована, т. е. от технической и программной среды. Интеграция достижений человечества в области средств

связи, обработки, накопления и отображения информации способствовала формированию автоматизированных информационных технологий.

Основу автоматизированных информационных технологий составляют следующие технические достижения:

• создание средств накопления больших объемов информации на машинных носителях;

• создание различных средств связи, таких как радио- и телевизионная связь, телекс, телефакс, цифровые системы связи, компьютерные сети, космическая связь, позволяющих воспринимать, использовать и передавать информацию практически в любой точке земного шара;

• создание компьютера, особенно персонального, позволяющего по определенным алгоритмам обрабатывать и отображать информацию, накапливать и генерировать знания.

Автоматизированные информационные технологии направлены на увеличение степени автоматизации всех информационных операций и, следовательно, ускорение научно-технического прогресса общества.

Понятие информации является чрезвычайно емким и широко распространенным, особенно в настоящее время, когда информатика, информационные технологии, компьютеры сопровождают человека чуть ли не с рождения.

Сам термин информация происходит от латинского слова informatio - разъяснение, осведомление, изложение. В Федеральном законе «Об информации, информационных технологиях и о защите информации» даны следующие понятия:

1) информация - сведения (сообщения, данные) независимо от формы их представления;

2) информационные технологии - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;

3) информационная система - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

4) информационно-телекоммуникационная сеть - технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники;

5) обладатель информации - лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;

6) доступ к информации - возможность получения информации и ее использования;

7) конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;

8) предоставление информации - действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц;

9) распространение информации - действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц;

10) электронное сообщение - информация, переданная или полученная пользователем информационно-телекоммуникационной сети;

11) документированная информация - зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель;

12) электронный документ - документированная информация, представленная в электронной форме, т. е. в виде, пригодном для воеприятия человеком, с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах (п. 11.1 введен Федеральным законом от 27.07.2010 г. № 227-ФЗ);

13) оператор информационной системы - гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.

Статья 17 Федерального закона «Об информации, информационных технологиях и о защите информации» определяет ответственность за правонарушения в сфере информации, информационных технологий и защиты информации.

В соответствии с п. 3-4 ст. 11 Федерального закона «Об информации, информационных технологиях и о защите информации»:

• электронный документ, электронное сообщение, подписанные электронной цифровой подписью или иным аналогом собственноручной подписи, признаются равнозначными документу, подписанному собственноручной подписью, в случаях, если иное не установлено федеральными законами;

• в целях заключения гражданско-правовых договоров или оформления иных правоотношений, в которых участвуют лица, обменивающиеся электронными сообщениями, обмен электронными сообщениями, каждое из которых подписано электронной цифровой подписью или иным аналогом собственноручной подписи отправителя такого сообщения, в порядке, установленном федеральными законами, иными нормативными правовыми актами или соглашением сторон, рассматривается как обмен документами.

Применительно к обработке данных на средствах вычислительной техники, информация - это произвольная последовательность символов, несущих смысловую нагрузку.

Документированная информация (документ) - зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать.

Конфиденциальная информация - документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

Таможенная информация характеризуется большим объемом, многократным использованием, обновлением и преобразованием, большим числом логических операций и относительно несложных математических расчетов для получения многих видов результатной информации.

Получатель таможенной информации оценивает ее в зависимости от того, для какой задачи информация будет использована. Поэтому информация имеет свойство относительности. При оценке информации различают различные ее аспекты, такие как синтаксический, семантический и прагматический.

Синтаксический аспект связан со способом представления информации вне зависимости от ее смысловых и потребительских качеств. На синтаксическом уровне рассматриваются формы представления информации для передачи и хранения. Обычно информация, предназначенная для передачи, называется сообщением. Характеристики процессов преобразования сообщения для его передачи определяют синтаксический аспект информации. Информацию, рассмотренную только относительно синтаксического аспекта, часто называют данными.

Семантический аспект передает смысловое содержание информации и соотносит ее с ранее имевшейся информацией. Смысловые связи между словами или другими элементами языка отражает словарь - тезаурус.

Прагматический аспект отражает возможность достижения поставленной цели с учетом полученной информации.

Основной задачей информационных технологий является управление информацией внутри определенных систем, в частности таможенной системы.

Информационные технологии отличаются по типу обрабатываемой информации (рис. 1.1), но могут объединяться в интегрированные технологии.

Рис. 1.1 - Классификация информационных технологий в зависимости от вида обрабатываемой информации

Классификация, представленная на рис. 1.1, в известной мере условна, поскольку большинство указанных информационных технологий позволяет поддерживать и другие виды информации. Так, в текстовых процессорах предусмотрена возможность выполнения примитивных расчетов, табличные процессоры могут обрабатывать не только цифровую, но и текстовую информацию, а также обладают встроенным аппаратом генерации графики. Однако каждая из этих технологий все-таки и большей мере акцентирована на обработку информации определенного вида.

Очевидно, что модификация элементов, составляющих понятие информационных технологий, дает возможность образования огромного их количества в различных компьютерных средах. В этой связи возможна классификация на обеспечивающие информационные технологии и функциональные информационные технологии.

Обеспечивающие информационные технологии - технологии обработки информации, которые могут использоваться как инструментарий в различных предметных областях для решения различных задач. Информационные технологии обеспечивающего типа могут быть классифицированы относительно видов задач, на которые они ориентированы. Обеспечивающие технологии базируются на совершенно разных платформах, что обусловлено различием видов компьютеров и программных сред, поэтому при их объединении на основе предметное технологии возникает проблема системной интеграции. Она заключается в необходимости приведения различных информационных технологий к единому стандартному интерфейсу.

Функциональная информационная технология представляет собой такую модификацию обеспечивающих информационных технологий, при которой реализуется какая-либо из предметных технологий. Например, работа должностного лица отдела контроля доставки с использование компьютера обязательно предполагает применение совокупности банковских технологий оценки внешнеэкономических контрактов, кредитных и срочных обязательств участника ВЭД, реализованных в какой-либо информационной технологии: СУБД, текстовом или табличном процессоре и т. д.

Классификация информационных технологий по типу пользовательского интерфейса (рис. 1.2) позволяет говорить о системном и прикладном интерфейсе. И если последний связан с реализацией некоторых функциональных информационных технологий, то системный интерфейс - это набор приемов взаимодействия с компьютером, которые реализуется операционной системой или ее надстройкой. Современные операционные системы поддерживают командный, WIMP и SILK интерфейсы. В настоящее время поставлена проблема создания общественного интерфейса (social interface).

Командный интерфейс - самый простой. Он обеспечивает выдачу на экран системного приглашения для ввода команды. Например, в one рационной системе MS-DOS приглашение выглядело как C:\>.

WIMP-интерфейс расшифровывается как Windows (окно) Image (образ) Menu (меню) Pointer (указатель). На экране высвечивается окно, содержащее образы программ и меню действий. Для выбора одного из них используется указатель.

SILK-интерфейс расшифровывается - Speech (речь) Image (образ) Language (язык) Knowledge (знание). При использовании SILK-интерфейсов на экране по речевой команде происходит перемещение от одних поисковых образов к другим по смысловым семантическим связям.

Рис. 1.2 - Классификация информационных технологий по виду пользовательского интерфейса

Общественный интерфейс будет включать в себя лучшие решения WIMP и SILK-интерфейсов. Предполагается, что при использовании общественного интерфейса не нужно будет разбираться в меню. Экранные образы однозначно укажут дальнейший путь. Перемещение от одних поисковых образов к другим будет проходить по смысловым семантическим связям.

Большинство обеспечивающих и функциональных информационных технологий могут быть использованы должностным лицом таможенных органов без дополнительных посредников (программистов). При этом

пользователь может влиять на последовательность применении тех или иных технологий. Таким образом, с точки зрения участия или неучастия пользователя в процессе выполнения функциональных информационных технологий все они могут быть разделены на пакетные и диалоговые.

Традиционно задачи, решаемые в пакетном режиме, характеризуются следующими свойствами:

• алгоритм решения задачи формализован, процесс ее решения не требует вмешательства человека;

• имеется большой объем входных и выходных данных, значительная часть которых хранится в электронном виде;

• регламентностью, т. е. задачи решаются с заданной периодичностью.

Диалоговый режим является не альтернативой пакетному, а его развитием. Если применение пакетного режима позволяет уменьшить вмешательство пользователя в процесс решения задачи, то диалоговый режим предполагает отсутствие жестко закрепленной последовательности операций обработки данных (если она не обусловлена предметной технологией).

Особое место занимают сетевые технологии, которые обеспечивают взаимодействие многих пользователей.

Информационные технологии различаются по степени их взаимодействия между собой. Они могут быть реализованы различными техническими средствами. При этом под информационно-техническими средствами подразумевают совокупность средств таможенного контроля, в том числе за делящимися радиоактивными материалами, технических средств таможенных расследований, средств вычислительной техники, средств связи, оргтехники, технических средств охраны, контрольно-измерительных приборов, лабораторного оборудования и вспомогательных технических средств.

1.2 История развития компьютерных информационных технологий

Вплоть до XX в. в таможенном деле шло медленное накопление опыта по информационному обеспечению в управлении. История таможенного дела свидетельствует, что проблема сбора, накопления, обработки и использования различных сведений и данных стояла перед этой службой на всех этапах ее развития. В течение длительного времени основными механизмами ее решения были мозг, язык и зрение человека. Первое революционное изменение произошло в связи с появлением письменности, а потом и изобретением книгопечатания. Эти два этапа создали совершенно новую технологию сбора, обработки и распространения сообщений и данных, избавили людей от необходимости всецело полагаться на человеческую память. Так как в эпоху книгопечатания основным носителем информации стала бумага, технологию сбора, обработки и распространения информации стали называть «бумажной информатикой».

Основы информационной теории и техники были заложены Шиккардом, Паскалем, Лейбницем. Профессор Тюбингенского университета В. Шиккард в 1623 г. предложил аппарат, состоявший из суммирующего и множительного устройств. Машина Б. Паскаля, построенная в 1642 г., могла складывать и вычитать. А в 1673 г. немецкий математик и философ Г. Лейбниц представил в Парижскую академию вычислитель, выполнявший четыре действия арифметики.

Ч. Беббидж, профессор Кембриджского университета, в 1812-1823 гг. построил разностную машину. В ее конструкции впервые был реализован принцип программного управления вычислительным процессом. В 1835 г. Беббидж создал проект аналитической машины, в которую предварительно заносились исходные данные, а ход вычислений мог зависеть от промежуточного результата.

Рождение цифровых вычислительных машин произошло после Второй мировой войны. Для них не было никакого программного обеспечения, кроме библиотек математических подпрограмм.

В 1945 г. американским математиком Дж. фон Нейманом были опубликованы базовые принципы построения вычислительных машин, впервые реализованные в машине EDVAC. Это был первый компьютер с хранимой программой, находящейся в памяти машины, а не считываемой с перфокарты или другого подобного устройства.

Следующий компьютер ENIAC, введенный фон Нейманом в эксплуатацию 15 февраля 1946 г., включал 17468 ламп, 7200 кремниевых диодов, 1 500 реле, 70 000 резисторов и 10 000 конденсаторов. Вес машины составлял 30 тонн, она требовала для размещения 170 м2. Потребляемая мощность - 150 кВт. Машина оперировала двоичными числами, имела память на 20 слов и могла производить 5 тыс. операций сложения или 300 операций умножения в секунду, т.е. примерно 300 флопс.

Первая отечественная ЭВМ - Малая электронная счетная машина (МЭСМ) была введена в эксплуатацию 25 декабря 1951 года, в Киеве. Это был новаторский проект академика Сергея Алексеевича Лебедева. МЭСМ содержала 6000 радиоламп, работала с частотой 5 килогерц и могла выполнять 50 операций в секунду (3000 в минуту). Ее потребляемая мощность составляла порядка 25 кВт. Данные считывались с перфокарт или набирались при помощи штекерного коммутатора. Занимала МЭСМ площадь порядка 60 квадратных метров (она еле умещалась в левом крыле двухэтажного здания).

Осенью 1952 года была завершена разработка БЭСМ-1 или БЭСМ Академии Наук (БЭСМ АН). Построена на электронных лампах (5000 ламп). Быстродействие - 8-10 тыс. оп./с. Система представления чисел в машине -39 разрядные числа с плавающей запятой. Машина имела общее поле памяти для команд и чисел (Архитектура фон Неймана) - 2047 39-разрядных ячеек. Внешняя память - на магнитных барабанах (2 барабана по 5 120 слов) и магнитных лентах (4 по 30 000 слов). Скорость обмена с барабаном - 800 чисел в секунду. Скорость записи-считывания с ленты после позиционирования - 400 чисел в секунду. Первоначальный ввод программы и исходных данных осуществляется с перфоленты со скоростью 20 кодов в секунду. Печать

результата осуществляется на бумагу со скоростью до 20 чисел в секунду. Потребляемая мощность - около 35 КВт.

В 1953 году на БЭСМ была опробована оперативная память на ртутных трубках (1024 слова), в начале 1955 года - на потенциалоскопах (1024 слова), в 1957 году - на ферритовых сердечниках (2047 слов).

На 1953 год (октябрь - международная конференция в Дармштадте) - БЭСМ оказалась самой быстродействующей в Европе, но уступала по быстродействию и объему памяти коммерческой американской IBM 701, поставки которой начались в декабре 1952 г.

Важный этап становления компьютерных технологий связан с появлением полупроводниковых элементов, внедрение которых в ЭВМ началось в конце 50-х годов.

До середины 60-х годов стоимость ЭВМ была такова, что использовать их для решения каких-либо задач могли только наиболее экономически развитые государства. В 1964 году произошло поистине эпохальное событие истории развития ЭВМ - в эксплуатацию была введена IBM System/360. Ее принято считать основателем целого класса компьютеров - «мейнфреймы». С появлением мейнфреймов на рынке появился новый товар – компьютерное время, благодаря чему ЭВМ могли использовать даже средние по размерам коммерческие фирмы. Затраты на разработку IBM System/360 составили около 5 млрд. долларов США (что соответствует 30 млрд. в ценах 2005 г., если сравнивать с 1964). Таким образом, это был второй по стоимости проект НИОКР 1960-х годов после программы «Аполлон». Дальнейшим развитием IBM/360 стали системы 370, 390 и System z. В СССР IBM/360 была клонирована под названием ЕС ЭВМ.

Старшие модели семейства IBM/360 и последовавшее за ними семейство IBM/370 были одними из первых компьютеров с виртуальной памятью (соответственно, со страничной и сегментной адресацией памяти) и первыми серийными компьютерами, поддерживающими реализацию виртуальных машин.

Развитие аппаратного обеспечения сказалось и на программном. Выполнение каждой программы стало включать большое количество вспомогательных работ: загрузка нужного транслятора языка программирования (ФОРТРАН 1957 г., ЛИСП 1958 г., КОБОЛ 1959 г., Бэйсик 1963 г., ПЛ/1 1964г., Алгол-58, Алгол-60, Алгол-68, ПАСКАЛЬ 1970 г., Си 1973 г. и т.д.), запуск транслятора и получение результирующей программы в машинных кодах, связывание программы с библиотечными подпрограммами, загрузка программы в оперативную память, запуск программы, вывод результатов на периферийное устройство.

Негативной особенностью первых вычислительных систем являлся простой процессора в ожидании, пока оператор запустит очередную программу. Для решения этой проблемы были разработаны первые системы пакетной обработки, которые автоматизировали всю последовательность действий оператора по организации вычислительного процесса. Оператор составлял пакет заданий, которые в дальнейшем без его участия последовательно запускались на выполнение управляющей программой - монитором. Ранние системы пакетной обработки значительно сократили затраты времени на вспомогательные действия по организации вычислительного процесса.

В 1965-1975 гг. в технической базе вычислительных машин произошел переход от отдельных полупроводниковых элементов типа транзисторов к интегральным микросхемам. Этот период характерен также бурным развитием операционных систем. Тогда были реализованы практически все основные механизмы, присущие современным операционным системам: мультипрограммирование, мультипроцессирование, поддержка многотерминального многопользовательского режима, виртуальная память, файловые системы, разграничение доступа и сетевая работа. Революционным событием данного этапа явилась промышленная реализация мультипрограммирования.

Мультипрограммирование было реализовано в двух вариантах - в системах пакетной обработки и разделения времени. В мультипрограммном пакетном режиме процессор не простаивал, пока одна программа выполняла операцию ввода-вывода (как это происходило при последовательном выполнении программ в системах ранней пакетной обработки), а переключался на другую, готовую к выполнению программу.

Другой вариант мультипрограммных систем - системы разделения времени. Этот вариант рассчитан на многотерминальные системы, когда каждый пользователь работает за своим терминалом. К этому времени можно констатировать существенное изменение в распределении функций между аппаратными и программными средствами компьютера. Операционные системы становились неотъемлемыми элементами компьютеров, играя роль «продолжения» аппаратуры.

Реализация мультипрограммирования потребовала внесения очень важных изменений в аппаратуру компьютера. В процессорах появились привилегированный и пользовательский режимы работы, специальные регистры для быстрого переключения с одной программы на другую, средства защиты областей памяти, а также развитая система прерываний.

В привилегированном режиме, предназначенном для работы программных модулей операционной системы, процессор мог выполнять все команды, в том числе и те из них, которые позволяли осуществлять распределение и защиту ресурсов компьютера. Программам, работающим в пользовательском режиме, некоторые команды процессора были недоступны.

Система прерываний, впервые реализованная в середине 50-х годов, позволяла синхронизировать работу различных устройств компьютера, работающих параллельно и асинхронно, таких как каналы ввода - вывода, диски, принтеры и т. п.

Еще одной важной тенденцией, реализованной в 60-е годы, является создание семейств программно-совместимых машин и операционных систем для них. Примерами семейств программно-совместимых машин, построенных

на интегральных микросхемах, являются серии машин IBM/360 и IBM370 (аналоги этих семейств отечественного производства - машины серии ЕС), PDP-11 (отечественные аналоги - СМ-3, СМ-4, СМ-1420). Вскоре идея программно-совместимых машин стала общепризнанной.

После запуска Советским Союзом искусственного спутника Земли в 1957 году Министерство обороны США посчитало, что на случай войны Америке нужна надёжная система передачи информации. Агентство передовых оборонных исследовательских проектов США (DARPA) предложило разработать для этого компьютерную сеть. Разработка такой сети была поручена Калифорнийскому университету в Лос-Анджелесе, Стэнфордскому исследовательскому центру, Университету штата Юта и Университету штата Калифорния в Санта-Барбаре. Компьютерная сеть была названа ARPANET (англ. Advanced Research Projects Agency Network), и в 1969 году в рамках проекта сеть объединила четыре указанных научных учреждения. Все работы финансировались Министерством обороны США. Затем сеть ARPANET начала активно расти и развиваться, её начали использовать учёные из разных областей науки.

Первый сервер ARPANET был установлен 1 сентября 1969 года в Калифорнийском университете в Лос-Анджелесе. Компьютер Honeywell DP-516 имел 24 Кб оперативной памяти.

29 октября 1969 года в 21:00 между двумя первыми узлами сети ARPANET, находящимися на расстоянии в 640 км - в Калифорнийском университете Лос-Анджелеса (UCLA) и в Стэнфордском исследовательском институте (SRI) - провели сеанс связи. Чарли Клайн пытался выполнить удалённое подключение к компьютеру в SRI. Успешную передачу каждого введённого символа его коллега Билл Дювалль из SRI подтверждал по телефону.

В первый раз удалось отправить всего три символа «LOG», после чего сеть перестала функционировать. LOG должно было быть словом LOGON (команда входа в систему). В рабочее состояние систему вернули уже к 22:30

и следующая попытка оказалась успешной. Именно эту дату можно считать днём рождения Интернета.

К 1971 году была разработана первая программа для отправки электронной почты по сети. Эта программа сразу стала очень популярна.

В 1973 году к сети были подключены через трансатлантический телефонный кабель первые иностранные организации из Великобритании и Норвегии, сеть стала международной.

В 1970-х годах сеть в основном использовалась для пересылки электронной почты, тогда же появились первые списки почтовой рассылки, новостные группы и доски объявлений. Однако в то время сеть ещё не могла легко взаимодействовать с другими сетями, построенными на других технических стандартах. К концу 1970-х годов начали бурно развиваться протоколы передачи данных, которые были стандартизированы в 1982-83 годах.

1 января 1983 года сеть ARPANET перешла с протокола NCP на TCP/IP, который успешно применяется до сих пор для объединения (или, как ещё говорят, «наслоения») сетей. Именно в 1983 году термин «Интернет» закрепился за сетью ARPANET.

В 1984 году была разработана система доменных имён (англ. Domain Name System, DNS).

В 1984 году у сети ARPANET появился серьёзный соперник: Национальный научный фонд США (NSF) основал обширную межуниверситетскую сеть NSFNet (англ. National Science Foundation Network), которая была составлена из более мелких сетей (включая известные тогда сети Usenet и Bitnet) и имела гораздо большую пропускную способность, чем ARPANET. К этой сети за год подключились около 10 тыс. компьютеров, звание «Интернет» начало плавно переходить к NSFNet.

К середине 70-х гг. наряду с мэйнфреймами широкое распространение получили мини-компьютеры, такие как PDP-11, Nova, HP. Мини-компьютеры первыми использовали преимущества больших интегральных схем,

позволившие реализовать достаточно мощные функции при сравнительно невысокой стоимости компьютера. Доступность мини-компьютеров и вследствие этого их распространенность на предприятиях послужили мощным стимулом для создания локальных сетей.

К наиболее важным событиям конца 70-х – начала 80-х гг. следует отнести появление персональных компьютеров и операционных систем для них.

Персональные компьютеры с точки зрения архитектуры ничем не отличались от класса мини-компьютеров типа PDP-11, но их стоимость была существенно ниже. Компьютеры стали широко использоваться неспециалистами, что требовало разработки «дружественного» программного обеспечения. Персональные компьютеры послужили также мощным катализатором для бурного роста локальных сетей.

В 80-е гг. были приняты основные стандарты на коммуникационные технологии для локальных сетей: в 1980 г. - Ethernet, в 1985 г. - Token Ring, в конце 80-х гг. - FDDI.

FDDI (англ. Fiber Distributed Data Interface - распределённый волоконный интерфейс данных) - стандарт передачи данных в локальной сети, протянутой на расстоянии до 200 километров. Стандарт основан на протоколе Token Ring. Кроме большой территории, сеть FDDI способна поддерживать несколько тысяч пользователей.

В XXI в. наблюдается переход к широкомасштабному использованию интегрированных сетевых ресурсов, к распределенной технологии обработки и хранения данных, внедрению Data Mining-технологий.

Повышенный уровень угроз, существующих при передаче данных по сетям, особенно по публичным, таким как Интернет, определил на современном этапе приоритетность средств обеспечения информационной безопасности.

Переход мировой экономики к использованию систем распределенной обработки и хранения данных определяет и современные черты таможни -

виртуальной информационно-электронной таможни с использованием электронных документов, компьютерной техники и космической информациологии, увязанных в единую автоматизированную информационную систему.

1.3 Задачи автоматизации процессов управления таможенной службой России

Важнейшим фактором интенсификации научно-технического прогресса является совершенствование форм и методов управления во всех функциональных звеньях управления.

Применение экономико-математических методов на базе использования новейших средств вычислительной техники и связи создало новые возможности для дальнейшего совершенствования системы управления. Важнейшим направлением использования экономико-математических методов и средств вычислительной техники явилось создание автоматизированных систем управления (АСУ).

В рамках этого направления развития системы управления процессами таможенной деятельности была создана Единая автоматизированная информационная система (ЕАИС) ФТС России.

ЕАИС является одним из компонентов информационно-технической инфраструктуры таможенных органов и представляет собой совокупность информационных, программных, информационно-вычислительных, центральных и региональных баз данных, информационно-вычислительных и телекоммуникационных систем и сетей. Она предназначена для комплексной автоматизации деятельности таможенных органов всех уровней и информационного взаимодействия между собой и с внешними объектами.

Решение задач информационного обеспечения и автоматизации управления в таможенной службе России проводится на основе единой концептуальной платформы (рис. 1.3). В структуре комплекса задач

автоматизации системы управления таможенного органа выделяют следующие.

Информационно-расчетные подзадачи - задачи сбора и обработки статистики внешнеэкономической деятельности, специальной таможенной статистики, специальной статистики о технологии таможенной деятельности.

Системный анализ деятельности таможенного органа - количественный многофакторный сравнительный анализ показателей деятельности таможенных постов, таможен, региональных таможенных управлений и таможенной системы в целом, оценка результатов ее модернизации и развития.

Поддержка принятия решений должностными лицами таможенного органа в целях оперативного управления на основе мониторинга и прогнозирования параметров ВЭД, моделирования вариантов принимаемых решений и оценки их эффективности, формирования банков оптимальных оперативно-ситуационных моделей ВЭД, таможенной деятельности, таможенных технологий и др.

Рис. 1.3 - Структурно-функциональная схема автоматизации процессов управления таможенной службой

Планирование и программно-целевое управление путем выявления проблемных вопросов в деятельности таможенного органа, исследования факторов, влияющих на деятельность таможенного органа, моделирования и оценки стратегий и модернизации таможенной системы, обоснования целевых направлений, формирования программ, программных направлений и мероприятий модернизации ФТС России, моделирования и оценки эффективности планируемых решений.

Одним из центральных и наиболее сложных компонентов в решении задач автоматизации и оценки эффективности системы управления таможенного органа является модельное представление таможенного органа как объекта исследования. На основе целостно-эволюционного подхода в литературе разработаны и детализированы различные аспекты процесса создания и использования моделей таможенного органа.

Дан методологический аппарат для преодоления размерности объекта моделирования и формирования знаний в условиях его эволюции. При этом под знанием понимается любая структурированная информация о таможенной деятельности, включая различные модели и закономерности деятельности таможенного органа, а также технологии интеграции знаний (когнитивные технологии).

В рамках такого подхода модель таможенного органа является объектом, инструментом и результатом исследования таможенной деятельности, а при решении конкретных задач - полигоном для принятия различных управленческих решений.

1.4 Единая автоматизированная информационная система ГТК России как совокупность мер, обеспечивающих автоматизацию деятельности таможенных органов

Анализ тенденций и новых условий, влияющих на функционирование ЕАИС, позволяет отнести к числу приоритетных с точки зрения автоматизации следующие процессы:

• организация управления рисками;

• осуществление таможенных операций и таможенный контроль;

• управление взиманием пошлин и налогов;

• взаимодействие с участниками ВЭД;

• взаимодействие с другими государственными органами и ведомствами, международное сотрудничество;

• вспомогательные процессы, к которым относятся:

♦ ведение нормативно-справочной информации;

♦ управление информационными ресурсами;

♦ ведение внутренней таможенной статистики и отчетности;

♦ организация научно-исследовательских и опытно-конструкторских работ в области таможенной деятельности;

♦ управление финансово-экономической деятельностью.

Структурирующим элементом функциональной архитектуры ЕАИС является верхнеуровневая модель целевых процессов таможенной деятельности, в составе которой выделяют три группы процессов:

- стратегические процессы;

- операционные процессы;

- обеспечивающие процессы.

1. Управление деятельностью таможенных органов

В группу стратегических процессов включены главные управленческие процессы, такие как управление стратегическим развитием и стратегия управления рисками, которые несут скорее косвенную ценность, проявляющуюся со временем, в среднесрочной перспективе.

1.1. Стратегическое и текущее управление деятельностью таможенных органов

1.1.1. Управление перспективным планированием развития таможенных органов и контроль

1.1.2. Текущее планирование исполнения планов деятельности таможенных органов

и контроль

1.1.3. Оперативное планирование деятельности таможенных органов и контроль

1.2. Организационное развитие таможенных органов

1.2.1. Оптимизация организационной структуры таможенных органов

2. Оперативная таможенная деятельность

Группа операционных процессов представляет собой ключевые процессы, связанные с основной деятельностью таможенных органов.

2.1. Управление рисками

2.1.1. Организация управления рисками

2.1.2. Анализ и выявление источников рисков

2.1.3. Ведение профилей рисков

2.2. Таможенное оформление и таможенный контроль

2.2.1. Предварительное информирование

2.2.2. Прием документов и сведений

2.2.3. ТК в соответствии с таможенными процедурами

2.2.4. Проведение таможенного досмотра

2.2.5.ТК при таможенном транзите

2.2.6. ТК при международном почтовом обмене

2.2.7. ТК товаров, перемещаемых трубопроводным транспортом

и по линиям электропередач

2.3. Таможенный контроль после оформления ТиТС

2.3.1. Функциональный контроль

2.3.2. Контроль исполнения таможенных процедур

2.3.3. Организация и проведение проверки участников ВЭД

2.3.4. Таможенный осмотр помещений и территорий

2.3.5. Таможенная проверка

2.3.6. Повторный таможенный досмотр_

2.4. Взаимодействие с участниками ВЭД

2.4.1. Ведение реестров участников ВЭД (таможенных перевозчиков, владельцев складов временного хранения и таможенных брокеров (представителей)

2.4.2. Аттестация специалистов по таможенному оформлению экспертов

2.4.3. Установление специальных упрощенных процедур ТО для отдельных участников ВЭД

2.4.4. Ведение персональных счетов (досье) субъектов ВЭД по видам деятельности

2.4.5. Информирование и консультирование участников ВЭД

2.4.6. Оформление предварительных решений о классификации товара в соответствии с ТН ВЭД Таможенного союза и стране происхождения

2.4.7. Ведение реестра банков и страховых организаций

2.4.8. Взаимодействие с профессиональными ассоциациями участников ВЭД

2.4.9. Рассмотрение предложений, заявлений и жалоб

2.4.10. Таможенный аудит

2.5. Взимание и контроль таможенных платежей

2.5.1. Планирование поступлений таможенных платежей

2.5.2. Исчисление и начисление таможенных платежей

2.5.3. Ведение авансовых платежей

2.5.4. Взимание таможенных платежей

2.5.5. Прием обеспечения уплаты таможенных пошлин, налогов (с учетом данных СУР)

2.5.6. Работа с дебиторами (плательщиками таможенных пошлин, налогов)

2.5.7. Контроль правильности исчисления и своевременности уплаты таможенных пошлин, налогов. Учет поступления денежных средств

2.5.8. Принудительное взыскание таможенных платежей

2.5.9. Возврат излишне уплаченных или излишне взысканных таможенных пошлин, налогов, возврат в иных случаях

2.5.10. Возврат денежного залога

2.5.11. Подготовка и формирование отчетов

2.6. Правоохранительная деятельность

2.6.1. Сбор и анализ информации о событиях или действиях, создающих угрозу государственной, военной, экономической или экологической безопасности РФ

2.6.2. Осуществление производства по делам об административных правонарушениях и рассмотрение таких дел в соответствии с КОАП

2.6.3. Оперативно-розыскная деятельность

2.6.4. Производство дознания и проведение неотложных следственных действий по делам о контрабанде и иным преступлениям

2.6.5. Розыск лиц, скрывающихся от органов дознания, следствия, суда по делам о преступлениях в сфере таможенного дела

2.6.6. Осуществление действий в соответствии с уголовно-процессуальным законодательством РФ

2.6.7. Организация борьбы с контрабандой

2.6.8. Организация и проведение профилактических мероприятий

2.6.9. Организация лабораторных исследований и проведения экспертиз

2.6.10. Управление кинологической службой

2.6.11. Оперативно-аналитический учет преступлений и правонарушений

2.7. Взаимодействие с другими государственными органами и ведомствами, международное сотрудничество

2.7.1. Взаимодействие с другими государственными органами

и ведомствами

2.7.2. Международное сотрудничество

2.8. Ведение статистики внешней торговли России

2.8.1. Ведение статистики внешней торговли Российской Федерации

2.8.2. Сопоставительный анализ данных статистики внешней торговли России

и стран-партнеров

2.8.3. Подготовка публикаций данных таможенной статистики внешней торговли Российской Федерации

2.8.4. Ведение специальной таможенной статистики

2.8.5. Ведение таможенной статистики внешней торговли в разрезе субъектов Российской Федерации

2.8.6. Проведение анализа данных по внешней торговле России

2.8.7. Анализ и оценка основных тенденций развития внешней торговли

2.9. Обеспечение защиты экономических интересов и безопасности РФ при осуществлении внешней торговли

2.9.1. Участие в разработке мер тарифного и нетарифного регулирования внешнеторговой деятельности

2.9.2. Администрирование мер тарифного и нетарифного регулирования внешнеторговой деятельности

2.9.3. Ведение реестра объектов интеллектуальной собственности

3. Обеспечивающие рабочие процессы

В группу обеспечивающих процессов включены процессы, которые являются межфункциональными и поддерживают как стратегические, так и операционные процессы.

Некоторые из них специфичны для таможенных органов России, но большинство обеспечивающих процессов аналогичны для всех государственных органов.

3.1. Управление развитием таможенных органов

3.1.1. Управление информационными ресурсами

3.1.2. Организация научно-исследовательских и опытно-конструкторских работ в области таможенного дела

3.1.3. Методическое и нормативно-правовое обеспечение деятельности

3.1.4. Взаимодействие со средствами массовой информации

3.2. Управление финансово-экономической и контрольной деятельностью

3.2.1. Управление финансово-экономической деятельностью

3.2.2. Контрольно-ревизионная деятельность

3.2.3. Ведомственный контроль за выполнением нормативно-правовых актов, договоров, указов и распоряжений

3.2.4. Управление материально-техническим обеспечением деятельности таможенных органов

3.2.5. Управление делопроизводством

3.2.6. Ведение внутренней таможенной статистики и отчетности

3.3. Управление персоналом и обеспечение безопасности деятельности таможенных органов

3.3.1. Управление персоналом

3.3.2. Правовая защита и профилактика правонарушений в таможенных органах

3.3.3. Контроль соблюдения законности

3.3.4. Управление силовым обеспечением таможенных органов

3.3.5. Обеспечение собственной безопасности

3.2.6. Обеспечение охраны труда, выполнения мероприятий в области гражданской обороны, предупреждения и ликвидации чрезвычайных ситуаций, соблюдения техники безопасности и пожарной безопасности, мобилизационной подготовки

Для автоматизации деятельности таможенных органов в целом важнейшими исходными параметрами являются характеристики потоков информации, их объемы, временные критерии обработки и передачи информации, расположение и организация связи между таможенными объектами, определяющая сложность многоуровневых элементов в общей структуре таможенных органов.

В целом ЕАИС характеризуется:

• территориальной распределенностью;

• иерархической структурой управления;

• централизованным методологическим управлением в части применения информационных таможенных технологий;

• необходимостью в использовании распределенных информационных систем, нуждающихся в средствах обеспечения информационного обмена между ними;

• существованием средств передачи информации и обеспечивающего их комплекса организационного, информационного и программно-аппаратного обеспечения;

• наличием ведомственной электронной почты на базе использования почтовых систем Novell Group Wise и Microsoft Exchange, функционирующей в настоящее время в режиме опытной эксплуатации;

• наличием телекоммуникационной инфраструктуры на базе использования выделенных каналов связи и коммутируемых линий телефонной сети общего пользования с использованием различных протоколов передачи данных.

Факторы, определяющие основные характеристики ЕАИС:

1) постоянный рост числа пользователей;

2) постоянный рост объемов грузоперевозок;

3) измерение нормативной базы;

4) необходимость интеграции с зарубежными партнерами;

5) необходимость интеграции с другими силовыми ведомствами (МВД, ФСБ, ФНС) (рис. 1.4).

Документооборот в системе таможенных органов характеризуется высокой интенсивностью потока и разнообразием типа документов. Основной объем документооборота приходится на ТД, а также на документы по ведению баз данных нормативно-справочной информации (БДНСИ), на документы, оформленные по процедуре внутреннего таможенного транзита (ВТТ), международным перевозкам (МДП), на декларации таможенной стоимости.

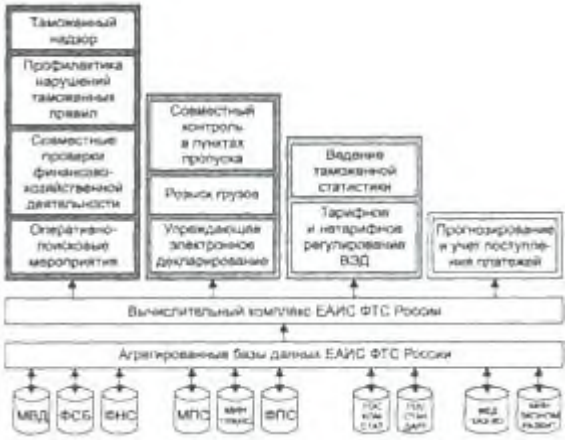

Рис. 1.4 - Интеграция ФТС России с другими министерствами и ведомствами

С точки зрения системы передачи данных ЕАИС классически разделяют на 4 иерархически подчиненных уровня - Центрального аппарата ФТС, регионального таможенного управления, таможни, таможенного поста (рис. 1.5).

Рис. 1.5 - Схема основных типовых узлов ЕАИС

Основными типовыми узлами ЕАИС с точки зрения размещения инфраструктуры компонентов Системы и топологии сети узлов являются: Главный центр обработки данных (Г-ЦОД, на базе ГНИВЦ), Центральный аппарат ФТС России, региональные центры обработки данных (Р-ЦОД, на базе региональных вычислительных центров), региональные таможенные

управления, таможни, внутренние и приграничные таможенные посты, мобильные пользователи ЕАИС, таможни центрального подчинения, организации и учреждения, подведомственные ФТС России.

Организация передачи таможенной информации в ЕАИС регламентируется положениями соответствующих отраслевых руководящих документов.

С точки зрения транспортной системы компоненты, участвующие в процессах контроля, расположенные в РТУ, таможнях и таможенных постах, в настоящее время формируют файлы, содержащие платежные документы, статистическую информацию, архивы, которые передаются в соответствующие головные организации и обратно.

Характер обмена информацией - асинхронный, т. е. прикладная система формирует файл (электронный документ, ЭД), выкладывает его в директорию для отправки через транспортную систему и продолжает работу. Таким образом, подтверждения о доставке информации в тот же момент не требуется.

Циркулирующая в ЕАИС информация по источнику ее формирования подразделяется на следующие виды:

• информацию, подготовленную при помощи специальных программных комплексов, реализующих информационные таможенные технологии;

• информацию, сформированную стандартными средствами общего пользования (текстовые редакторы, электронные таблицы и др.);

• прочую информацию, оформленную в виде файлов, с неопределенными средствами ее подготовки (например, дистрибутивы программ).

По функциональному принципу циркулирующую в ЕАИС ФТС России информацию можно разделить на следующие категории:

• исходные данные для загрузки и формирования баз данных таможенной информации;

• нормативно-справочная информация;

• оперативная информация таможенных органов;

• служебная переписка таможенных органов;

• регламентная отчетная информация таможенных органов;

• транзитная информация, проходящая через ГНИ ВЦ.

В части сроков передачи информации в ЕАИС и в соответствии с требованиями существующих нормативных документов и установленными регламентами может использоваться следующая классификация:

• оперативная информация (данные мониторинга осуществления таможенных операций). Оперативная информация должна быть доставлена в минимально возможные сроки. К данной категории относятся также различные сообщения в контуре оперативного управления таможенной деятельностью (например, ориентировки), а также служебные и технологические потоки данных, связанные с контролем функционирования автоматизированных систем, входящих в состав ЕАИС;

• регламентная информация (отчеты таможенных органов в соответствии с ежегодными приказами ФТС России о введении форм статистической отчетности). Отличительной особенностью данной категории является периодический характер формирования и необходимость получения необходимых данных к определенному нормативными документами сроку;

• информация, используемая для формирования официальных статистических отчетов, бюллетеней и сборников. Информация данной категории должна быть максимально достоверной и полной, при этом на оперативность ее формирования не накладываются столь жесткие ограничения, как в предыдущих категориях;

• нормативно-справочная информация, которая должна вступать в действие одновременно во всех таможенных органах в установленное время.

Максимальные объемы передачи сообщений приходятся на Центральное таможенное управление (почти 35 % общего объема) и Северо-Западное таможенное управление (почти 18 % общего объема). Каждое из остальных 5 региональных таможенных управлений имеет трафик меньше чем

10 % от общего объема. В целом отмечается ежегодный прирост объемов, передаваемых данных на 10-15 %. При этом максимальный объем сообщений составляет информация, передаваемая в адрес ГНИВЦ.

Для передачи большей части указанных данных используются канальные ресурсы ведомственной интегрированной телекоммуникационной сети ФТС России (ВИТС ФТС России).

ВИТС ФТС России построена по иерархическому принципу по схеме «звезда». На верхнем уровне ВИТС представлена узлом ГНИВЦ, имеющим каналы связи с региональными таможенными управлениями и таможнями непосредственного подчинения.

Глава 2. Принципы построения ЕАИС

2.1 Принципы построения ЕАИС

Принципы разработки автоматизированных систем управления обусловливаются требованиями и возможностями научного управления, а также особенностями конкретных объектов управления и использования современных технических средств. Основные принципы разработки АСУ подразделяются на три вида:

• принципы системного характера;

• принципы организационно-технического характера;

• принципы экономико-математического характера.

Эти принципы подчеркивают информационно-экономическую природу АСУ, в данном случае ЕАИС ФТС России, отличающую ее от разнообразных технических и других систем управления: первоочередность решения при разработке АСУ экономических и информационных проблем, необходимое приспособление общесистемных положений математического аппарата, программных и технических средств к особенностям и условиям функционирования конкретной области - таможенной службы России.

В настоящее время этапы создания, эксплуатации, модернизации и т.п. программных средств принято объединять понятием жизненного цикла.

Жизненный цикл программных средств (ЖЦПС) - совокупность взаимосвязанных процессов, связанных с созданием, использованием по назначению и списанием ПС.

Процесс ЖЦПС представляет собой совокупность упорядоченных во времени взаимосвязанных работ, объединенных в этапы и стадии. Стадии и этапы процесса выделяются в целях рациональной организации работ для достижения заданного результата и осуществления контроля исполнения процесса.

К основным процессам ЖЦПС относятся: формирование заказа на создание ПС; создание ПС; эксплуатация и сопровождение ПС; модернизация (изменение функциональных возможностей) ПС; вывод из эксплуатации и списание ПС.

Организация процессов ЖЦПС - комплекс организационно-технических мероприятий, выполняемых структурными подразделениями (учреждениями) ФТС России, таможенными органами и направленных на выполнение процессов ЖЦПС с учетом обеспечения информационной безопасности.

Приказом ФТС России от 03.02.2010 г. № 183 утвержден Порядок организации процессов жизненного цикла программных средств информационных систем и информационных технологий таможенных органов (далее - Порядок). Порядок разработан в целях осуществления в ФТС России единого подхода в вопросах создания, модернизации, внедрения, эксплуатации, сопровождения и вывода из эксплуатации программных средств, на которые ФТС России имеет исключительное право, используемых в составе Единой автоматизированной информационной системы (ЕАИС) таможенных органов, в других информационных системах таможенных органов или автономно.

Порядок предназначен для структурных подразделений ФТС России, учреждений, находящихся в ведении ФТС России (далее - учреждений ФТС России), деятельность и функции которых предусматривают решение задач обеспечения применения, развития и совершенствования информационных технологий, а также для должностных лиц системы таможенных органов, в функциональные обязанности которых входят вопросы организации создания, внедрения, эксплуатации, модернизации и/или сопровождения программных средств информационных систем и информационных технологий таможенных органов.

Порядок определяет взаимодействие Главного управления информационных технологий ФТС России (далее - ГУИТ), структурных подразделений ФТС России, ГНИВЦ, учреждений ФТС России, таможенных

органов и входящих в их состав информационно-технических служб (ИТС), информационно-технических подразделений (ИТП) при организации процессов жизненного цикла программных средств, а также типовые требования по безопасности информации, предъявляемые к программным средствам информационных систем и информационных технологий таможенных органов.

Программные средства информационных систем и информационных технологий таможенных органов (далее - ПС) - программы, предназначенные для многократного применения на различных объектах (по ГОСТ 28195-89), программная документация, а также базы данных различного назначения, созданные в интересах ФТС России по ее заказу.

К основным мероприятиям по организации процессов ЖЦПС относятся:

• определение и обоснование потребностей в развитии информационных технологий и ПС, предназначенных для реализации информационных технологий;

• планирование научно-исследовательских и опытно-конструкторских работ (НИОКР), модернизации, внедрения и сопровождения ПС, подготовки должностных лиц и работников к работе с ПС;

• подготовка конкурсной документации для проведения торгов, разработка функциональных и технических требований к ПС, технического задания на создание ПС;

• проведение торгов в форме конкурса на право заключения государственного контракта (далее - контракт) на выполнение работ и оказание услуг, составляющих и/или обеспечивающих процессы ЖЦПС (этап, стадию процесса, процесс ЖЦПС);

• контроль исполнения контракта, проведение испытаний ПС;

• подготовка правовых актов ФТС России, других руководящих документов, регламентирующих разработку, модернизацию, приемку, внедрение, эксплуатацию, сопровождение и вывод из эксплуатации ПС, подготовку должностных лиц и работников к работе с ПС;

• подготовка должностных лиц и работников к работе с ПС в качестве пользователей и администраторов;

• сбор, анализ и обобщение замечаний по работе ПС, предложений по усовершенствованию ПС в целях изменения функциональности, интерфейса и сервисов ПС, устранения ошибок, возникающих в процессе эксплуатации;

• контроль выполнения работ, а также контроль соблюдения должностными лицами и работниками требований руководящих документов.

ГУИТ осуществляет общее руководство организацией и реализацией работ, составляющих процессы ЖЦПС, координацию деятельности структурных подразделений (учреждений) ФТС России, ГНИВЦ, таможенных органов, связанной с развитием информационных систем и информационных технологий таможенных органов.

ГНИВЦ осуществляет деятельность по вопросам внедрения, эксплуатации, модернизации и сопровождения ПС, подготовки должностных лиц и работников к работе с ПС.

Структурные подразделения (учреждения) ФТС России:

• инициируют заказы на проведение НИОКР, модернизацию ПС;

• принимают участие в разработке конкурсной документации работе комиссии по приемке ПС и научно-технической документации;

• разрабатывают проекты правовых актов ФТС России, определяющих порядок приемки результатов инициируемых научно-исследовательских работ (НИР);

• разрабатывают и представляют в ГУИТ предложения по внедрению, эксплуатации и сопровождению ПС, замечания по работе ПС, предназначенных для реализации возложенных на них функций или для использования таможенными органами по направлению деятельности структурного подразделения (учреждения) ФТС России;

• представляют в ГУИТ обоснованные предложения по выводу из эксплуатации ПС.

Таможенные органы осуществляют эксплуатацию и сопровождение ПС на своих объектах, готовят предложения по созданию, внедрению, эксплуатации, модернизации, сопровождению, выводу из эксплуатации ПС, замечания по работе ПС и представляют их через региональные таможенные управления (РТУ), таможни, непосредственно подчиненные ФТС России, в структурное подразделение ФТС России, к компетенции которого относится информационная технология, реализуемая ПС.

2.2 Требования к ЕАИС

Разработка и внедрение системы резко повысили роль таможенной службы России как инструмента экономической политики государства. Это привело к бурному росту объема решаемых при осуществлении таможенного контроля задач и обусловило специфические требования к функционированию ЕАИС:

этапность разработок системы и ее внедрения из-за необходимости первоочередной реализации в информационно-технологической структуре главных направлений деятельности и важнейших задач ГТК РФ;

соблюдение принципов построения "открытых систем" с целью обеспечить гибкость информационно-технологической структуры, возможность ее модификаций и наращивания мощностей в соответствии с потребностями ГТК РФ и выделяемыми ресурсами.

Проектируемая ЕАИС охватывает все четыре уровня, организационной структуры таможенной службы (ГТК РФ; региональные таможенные управления; таможни; таможенные посты).

Основные компоненты системы структурно разделяются на:

задачи;

комплексы задач;

автоматизированные рабочие места (АРМы);

автоматизированные системы ведения и поддержки баз данных;

автоматизированные системы, реализующие определенные функционально полные и законченные технологические процессы таможенной деятельности.

Требования к надежности ЕАИС. Надежность работы системы в целом и выполнения каждой автоматизируемой функции обеспечивается за счет:

высокой технологичности разрабатываемых программных средств и организационного обеспечения, позволяющего сохранять циркулирующую в системе информацию при сбоях и других ситуациях, нарушающих или разрушающих устойчивость функционирования системы;

новейших технических средств;

надежности хранения данных;

надежности системных и прикладных программных средств;

уровня квалификации и организации работы, обслуживающего ЕАИС персонала;

организации технического обслуживания, использования современных методов и средств диагностики.

В проектных решениях определены методы и средства выполнения работ в случае сбоев системы. Режим работы всей ЕАИС и ее отдельных компонентов определен в соответствии с регламентом тех таможенных служб, которые непосредственно используют соответствующие компоненты ЕАИС.

Требования безопасности при размещении, эксплуатации и техническом обслуживании ЕАИС. Технические средства ЕАИС ГТК России установлены так, чтобы достигалась их безопасная эксплуатация и техническое обслуживание.

В помещении, предназначенном для эксплуатации технических средств, обеспечены противопожарные меры безопасности согласно ГОСТ 20397-82.

Климатические условия в помещениях, уровни шума и звуковой мощности в местах расположения ЕАИС не превышают значений, установленных санитарными нормами и ГОСТ 12.1.003-83.

Требования к эргономике и технической эстетике. Средства ЕАИС размещены с соблюдением требований, содержащихся в технической, в том числе эксплуатационной, документации на них, и так, чтобы было удобно использовать их при функционировании системы и выполнять техническое обслуживание.

Общесистемные программные средства ЕАИС имеют документацию на русском, а в случае отсутствия таковой - на английском языке.

Прикладные программные средства ЕАИС разрабатываются с учетом эргономических требований, предъявляемых конкретным заказчиком при соблюдении максимальной унификации интерфейсов управления.

Требования к защите от влияния внешних воздействий. Защита комплекса технических средств (КТС) ЕАИС от воздействия электрических и магнитных полей, а также помех по цепям питания должна быть достаточной для эффективного выполнения КТС своего назначения при функционировании.

Требования к эксплуатации, техническому обслуживанию, ремонту и хранению. Система выполняет свои функции, если ее правильно эксплуатируют, обслуживают и ремонтируют. Виды и периодичность обслуживания (еженедельное, ежемесячное, ежеквартальное) технических средств ЕАИС ГТК РФ оговорены в эксплуатационной документации.

В гарантийный период системотехнического обслуживания ремонт средств вычислительной техники ЕАИС осуществляется в соответствии с Положением о гарантийном системотехническом обслуживании.

В послегарантийный период средства вычислительной техники ЕАИС ремонтируются в соответствии с договорами на системотехническое обслуживание, заключенными между региональными таможенными управлениями ГТК России и региональными отделами ГНИВЦ в регионе, а в центре - между хозяйственным подразделением центрального аппарата ГТК России и ГНИВЦ. К системотехническому обслуживанию ЭВМ допускается персонал, имеющий удостоверения на право обслуживания.

2.3 Виды обеспечения ЕАИС

ЕАИС имеет обеспечивающую и функциональную части (рис. 2.1).

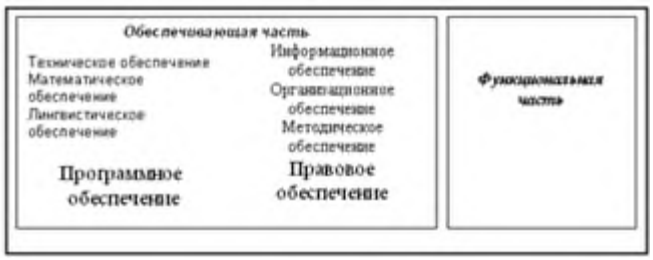

Рис. 2.1 - Автоматизированная информационная система

Обеспечивающая часть состоит из информационного, технического, математического, программного, методического, организационного и лингвистического обеспечения.

Информационное обеспечение - совокупность проектных решений по объемам, размещению, формам организации информации (единой системы классификации и кодирования информации, унифицированных систем документации, схем информационных потоков), циркулирующей в организации, а также методология построения баз данных. Включает в себя показатели, справочные данные, классификаторы и кодификаторы информации, унифицированные системы документации, информацию на носителях и т.д.

В рамках информационного обеспечения имеются вне машинные и внутри машинные данные. Внемашинная информационная база воспринимается человеком без технических средств - наряды, акты, накладные и т.п.

Внутри машинная информационная база содержится на носителях и состоит из файлов. Она может быть создана как совокупность отдельных файлов, каждый из которых отражает некоторое множество однородных управленческих документов (нарядов, накладных и т.п.), или как база данных.

В последнем случае файлы будут зависимыми, и структура одних файлов будет зависеть от структуры других, а структуры файлов базы данных не будут соответствовать структуре управленческих документов.

В информационном обеспечении различают входные и выходные документы.

Техническое обеспечение - комплекс технических средств, предназначенных для работы информационной системы, а также соответствующая документация на эти средства и технологические процессы.

Включает в себя:

- технические средства сбора, регистрации, накопления, обработки, передачи, отображения, вывода, размножения информации;

- компьютеры любых моделей (персональные компьютеры и высокопроизводительные компьютеры);

- вычислительные сети;

- оргтехнику и т.д.;

- устройства автоматического съема информации;

- эксплуатационные материалы и др.

Предварительный выбор технических средств, организация их эксплуатации, технологический процесс обработки данных, технологическое оснащение оформляются документацией. Документацию можно условно разделить на три группы:

- общесистемную, включающую государственные и отраслевые стандарты по техническому обеспечению;

- специализированную, содержащую комплекс методик по всем этапам разработки технического обеспечения;

- нормативно-справочную, используемую при выполнении расчетов по техническому обеспечению.

Математическое обеспечение – совокупность математических методов, моделей, алгоритмов обработки информации, используемых при решении

задач в информационной системе (функциональных и автоматизации проектирования информационных систем).

К средствам математического обеспечения относятся:

- средства моделирования процессов управления;

- типовые задачи управления;

- методы математического программирования, математической статистики и др.

Программное обеспечение – совокупность программ для реализации целей и задач информационной системы, а также нормального функционирования комплекса технических средств.

В состав программного обеспечения входят общесистемные и специальные программные продукты, а также техническая документация, в том числе: операционная система, системы программирования, инструментальные средства, тестовые и диагностические программы, программные средства телекоммуникации, защиты информации, функциональное программное обеспечение (автоматизированные рабочие места, системы управления базами данных и др.).

Специальное программное обеспечение представляет собой совокупность программ, разработанных при создании конкретной информационной системы, В его состав входят пакеты прикладных программ, реализующие разработанные модели разной степени адекватности, отражающих функционирование реального объекта.

Техническая документация на разработку программных средств должна содержать описание задач, задание на алгоритмизацию, экономико-математическую модель задачи, контрольные примеры.

Методическое обеспечение и организационное обеспечение – совокупность методов, средств и документов, регламентирующих взаимодействие персонала информационной системы с техническими средствами и между собой в процессе разработки и эксплуатации информационной системы.

Функциональная часть информационной системы обеспечивает выполнение и назначение информационной системы. Фактически здесь содержится модель системы управления организацией. В рамках этой части происходит трансформация целей управления в функции, функций – в подсистемы информационной системы. Подсистемы реализуют задачи. Подсистема – это часть системы, выделенная по какому-либо признаку.

Обычно в информационной системе функциональная часть разбивается на подсистемы по функциональным признакам:

- уровень управления (высший, средний, низший);
- вид управляемого ресурса (материальные, трудовые, финансовые и др.);
- сфера применения (финансовые, технологические и др.);
- функции управления и период управления.

Глава 3. Базы и банки информационных данных

3.1 Основные понятия процесса накопления данных

В ходе развития информационных систем были сформулированы принципы организации больших массивов данных:

• принцип интеграции данных, в соответствии с которым все данные накапливаются и хранятся централизованно, образуя динамически обновляемую модель предметной области;

• принцип независимости прикладных программ от данных, т. е. отделения логической модели данных от средств управления ими.

Удовлетворение этим принципам связано с созданием единого для всех задач блока данных, называемого базой данных, и разработкой единой управляющей программы для манипулирования данными, называемой системой управления базой данных - СУБД.

База данных представляет собой данные, организованные и обрабатываемые в накопителях в соответствии с определенными правилами хранения и доступа. Логическая, а часто и физическая автономность данных является существенным отличием баз данных от прочего программного обеспечения. Фиксированная, строго оговоренная структура хранения данных и их безусловная типизация отличают базу данных от текстовых и табличных процессоров, а широкая гамма допустимых операций на множествах является важным преимуществом ее перед пакетами прикладных программ и системами программирования. Выделением базы данных как особой части программного обеспечения преследуется несколько целей:

• эффективная структуризация информации;

• сведение к минимуму повторяющихся данных;

• обеспечение быстрого доступа к информации прямо на носителе;

• удобство дополнения информации новыми сведениями;

• обеспечение целостности данных;

• предотвращение несанкционированного доступа к информации;

• облегчение автоматизации обработки данных и ведения отчетности.

Объекты, процессы, явления предметной области представляются в базах данных коллекциями записей (сущностей) определенной структуры. Отношения между записями характеризуются связями, которые могут быть бинарными и n-арными. Эти связи оформляются в виде моделей данных. Модель дает приближенное представление коллекции средствами языка, математической или логической символики. Различают иерархическую, сетевую и реляционную модели данных.

Иерархическая модель отражает структуру, аналогичную файловой системе. Это дерево с узлами, в которых хранятся данные, и ветвями, связывающими их между собой. Узел, в который не входит ни одна ветвь, называется корнем. В свою очередь, любой узел дерева - это в то же время и корень поддерева. Число таких поддеревьев именуется степенью узла. Концевой узел, имеющий нулевую степень, называется листом. Таким образом, граф иерархической модели должен удовлетворять определенным ограничениям.

Если же эти ограничения убрать, получится граф произвольного вида, отображаемый сетью. Сетевая модель рассматривает базу данных как абстрактное хранилище связанных друг с другом записей, т. е. объектами такой базы являются и записи, и связи между ними. Форма хранения информации в базе данных сетевого типа напоминает способ хранения образов в мозгу человека. Между элементами данных существует отношение наследования типа «родитель-потомок», причем любой элемент может оказаться наследником нескольких родителей, и наоборот. Связи в базе данных сетевого типа реализуются с помощью сложной системы указателей. Поскольку каждый элемент данных должен содержать ссылки на другие элементы, такая модель требует значительных ресурсов памяти и высокого быстродействия компьютера. В настоящее время ведутся исследования в

области создания объектно-ориентированных сетевых баз данных, финансируемых такими компаниями, как, например, 1BM в США.

Концепция реляционной модели была разработана Э. Ф. Коддом в 1970 г. В основе ее лежит понятие бинарного отношения как двухмерной таблицы единой структуры. Значения ее элементов являются атомарными (неделимыми) величинами и не содержат других отношений. В этом заключается главное отличие реляционной модели от иерархической и сетевой. Сравнительная простота инструментальных средств поддержки реляционной модели является ее достоинством, тогда как жесткость структуры и зависимость от скорости работы, от размера базы данных относятся к недостаткам.

Разработчики реляционных СУБД никогда не ставили целью предоставление пользователю мощных функций многомерной обработки данных, их анализа и синтеза. Метод динамической аналитической обработки OLAP (On-Line Analytical Processing), предложенный тем же Э. Ф. Коддом, ускоряет решение указанных задач. Он предполагает многомерное концептуальное представление данных и их прозрачность для пользователя, доступность и высокую производительность в работе.

3.2 Системы управления базой данных

Системой управления базой данных (СУБД) называется программа, выполняющая управление и поиск в базах данных, их систематизацию и актуализацию. Под управлением данными понимается, во-первых, манипулирование записями, выполняемое пользователем, а во-вторых - задание и коррекция схемы базы данных, т. е. ее логической или физической структуры, выполняемые программистом. В наиболее полном варианте СУБД содержит свой интерфейс пользователя, дающий возможность непосредственного управления данными; язык для программирования прикладных задач обработки данных; средства для придания завершенной

программе вида готового коммерческого продукта. Будучи механизмом пользователя, СУБД предусматривает систематизацию и оперативный поиск данных и имеющихся в них сведений, а также поддержание данных в актуальном состоянии - их добавление, изменение, выборку, отображение. Будучи инструментом программиста, СУБД помогает ему в проектировании, предусматривая следующие этапы:

• определение объектов - источников данных и выявление связей между ними;

• определение свойств объектов и выявление связи между свойствами;

• создание словаря данных;

• разработка операций над данными;

• назначение пользователей и разграничение их прав доступа.

Как инструмент проектирования информационных систем, СУБД поддерживает все три известных уровня представления данных: концептуальный, логический и физический. Первый определяет структуру базы данных в терминах объектов предметной области и отношений между ними. Второй уровень описывает связи между данными на языке математической логики и алгоритмических языках, а третий управляет обменом и размещением данных на внешних носителях. Для этого СУБД оснащается средствами создания и анализа структуры базы данных и механизмами работы с таблицами.

Пользователь общается с базой данных через копии ее фрагментов. Для этого он либо осуществляет фильтрацию записей, либо обращается к базе данных с запросом. Запросы к реляционным базам данных выполняются на языках реляционного исчисления, основанных на классических операциях на множествах (объединение, пересечение, дополнение, разность) и исчислении предикатов (проекция, выбор). Язык запросов предоставляет пользователю набор правил или инструмент для формирования вопроса с информацией о желаемом результате. На основании запроса СУБД автоматически выдает ответ посредством генерации новых таблиц. Статусом стандартного языка

запросов обладает сегодня реляционный структурированный процедурный язык SQL (Structured Query Language), разработанный фирмой IBM. Весьма популярен и непроцедурный язык запросов на примере QBE (Query By Example), созданный М. Злуфом в фирме IBM в 1977 г.

Более 15 лет представлен на мировом рынке пакет Oracle. Долгое время каждая третья продаваемая в мире СУБД работала под Oracle. На Oracle разработано значительное число прикладных систем для банков, промышленных предприятий, энергетических объектов, учреждений здравоохранения и таможни. Она обеспечивает целостность баз данных при выполнении распределенных запросов, автономию узлов базы и высокую производительность. Система поддерживает открытую архитектуру: в ее едином приложении могут согласованно работать компоненты СУБД различных фирм, файлы операционной системы, аппаратура (промышленные контроллеры, кассовые аппараты). Инструментарий Oracle позволяет создавать графический интерфейс пользователя со сложной логикой обработки данных. Постепенно реляционная СУБД Oracle преобразуется в объектно-ориентированную систему на основе языка SQL++, хранящую данные в виде объектов вместо таблиц.

Языки управления событиями исключают программирование как процесс формирования текста программы программистом. Генераторы интерпретируют данные, вводимые с помощью меню, диалога или пиктограмм, и генерируют соответствующий программный код на одном из процедурных языков. Генераторы освобождают разработчиков от необходимости переписывать повторяющиеся фрагменты программ и позволяют быстро создавать прототипы прикладных систем.

Интегрированные системы программирования, включающие генераторы кодов и процедурные языки, называют CASE-инструментами (Computer Aided Software Engineering). В таких комплексах среда проектирования не отделена от прикладной системы. Примером CASE-инструмента является система Oracle CASE. Для создания конкретной

прикладной системы, например, таможенной, проектировщик представляет свои знания о работе конкретного подразделения таможни в системный словарь. Настройка проектируемой системы на технологию работы таможенного подразделения закладывается уже на первоначальных стадиях проектирования средствами конструктора. Затем выполняется генерация сразу же готовой системы.

Для упорядочивания информации в таможенных БД используются языки высокого уровня, для тонких запросов - Assembler. При этом в качестве операционной системы в ГНИВЦ ФТС используется Open VMS, а для управления БД используются разработки Oracle.

3.3 Особенности баз данных, используемых в ФТС России

Базы данных таможенных органов можно условно разбить на три группы:

• базы данных нормативно-справочной информации (НСИ): системы классификации и кодирования, тарификации, ограничений, правовые и нормативные акты, системы регистрации и учета;

• базы данных оперативной информации: электронные копии документов, используемых в ходе осуществления таможенных операций и контроля (ТД, ДКД, ДТС, ТПО и др.), данные оперативного характера, обеспечивающие технологические процессы (учет, контроль, аудит и т. п.);

• базы данных статистической информации, являющиеся производными от баз данных оперативной информации.

Практически каждое функциональное подразделение таможенных органов имеет собственную базу данных для текущей работы. Результаты работы подразделений по линиям передачи данных передаются в вычислительные центры региональных информационно-технических служб, на базе которых действуют региональные центры передачи электронных данных и организованы региональные базы данных. Отсюда данные

передаются в ГНИВЦ, на территории которого функционирует Центральный банк данных.

Из ГНИВЦ в функциональные подразделения региональных таможенных управлений и таможен регулярно передаются корректировки НСИ.

Объем центральной базы данных ФТС России составляет сотни терабайтов: это архивы оформляемых таможенных деклараций (более 2,5 млн документов в год, по несколько десятков килобайтов каждый) плюс специализированные базы данных документов контроля доставки товаров и транспортных средств, таможенных приходных ордеров, сертификатов и нормативно-справочной информации, а также БД по участникам ВЭД.

В целях совершенствования порядка сбора, обработки, передачи электронных копий ТД, обеспечения формирования и ведения баз данных ТД таможенных органов всех уровней в рамках ЕАИС таможенных органов был издан Приказ от 23.12.2008 г. «О порядке сбора, обработки, передачи электронных копий грузовых таможенных деклараций и формирования баз данных всех уровней в рамках Единой автоматизированной информационной системы таможенных органов» № 1648.

Этим Приказом утверждены:

• порядок сбора, обработки, передачи электронных копий грузовых таможенных деклараций и формирования баз данных всех уровней в рамках ЕАИС таможенных органов;

• сроки хранения электронных копий ТД, содержащихся в информационных ресурсах таможенных органов и в ГНИВЦ.

Порядок сбора, обработки, передачи электронных копий грузовых таможенных деклараций и формирования баз данных всех уровней в рамках Единой автоматизированной информационной системы таможенных органов (далее - Порядок) определяет действия должностных лиц и работников таможенных органов, ГНИВЦ при сборе, обработке, передаче электронных копий ТД, а также формировании баз данных ТД на уровне таможенного

поста, таможни, регионального таможенного управления (РТУ), ГНИВЦ в рамках ЕАИС таможенных органов).

В рамках Порядка проходит информационное взаимодействие структурных подразделений таможенных органов, осуществляющих таможенные операции и таможенный контроль, информационно-технических подразделений (ИТП) таможенных органов, подразделений таможенных органов и отделов ГНИВЦ, обеспечивающих сбор, хранение, обработку электронных копий ТД и бесперебойное функционирование системы сбора ТД (совокупность штатных программных средств ЕАИС таможенных органов, включенных в Фонд алгоритмов и программ ФТС России, технических и аппаратных средств, организационных мероприятий, должностных лиц и работников таможенных органов и ГНИВЦ, обеспечивающих сбор, обработку, проведение форматно-логического контроля и формирование соответствующих баз данных на уровне таможенного поста, таможни, РТУ и ГНИВЦ).

Программно-аппаратные средства, входящие в систему сбора ТД, составляют единый комплекс средств, обеспечивающих проведение операции, выполняемой в целях проверки полноты и достоверности сведений, указанных в электронной копии ТД, проводимой комплексными автоматизированными системами «АИСТ-РТ21» и «АИСТ-М» при таможенном контроле и при загрузке электронной копии ТД в центральную базу данных ТД (операция форматно-логического контроля) (далее - ФЛК), формирование электронных копий ТД, их сбор, обработку, передачу, загрузку в соответствующие базы данных таможенных органов на всех уровнях системы сбора ТД.

Существует четыре уровня системы сбора ТД: таможенный пост; таможня; РТУ; ГНИВЦ.

Контроль инсталляции, настройки и организации интерфейса взаимодействия программных средств системы сбора ТД в подразделениях таможенных органов осуществляет начальник ИТП таможни или РТУ, в обязанности которого в целях бесперебойного функционирования системы

сбора ТД входит обеспечение контроля за своевременным переходом подчиненных таможенных органов на работу с новыми версиями программных средств ЕАИС таможенных органов, входящих в систему сбора ТД и рассылаемых ГНИВЦ.

В рамках ЕАИС таможенных органов осуществляется ведение следующих информационных ресурсов, содержащих электронные копии ТД:

1) на уровне таможенного поста:

а) базы данных ТД (только для таможенных органов, оснащенных АИС «АИСТ-М»), представляющей собой информационный ресурс таможенного органа, содержащий электронные копии ТД, хранимые и обрабатываемые с применением КПС «Сбор информации по ГТД», и используемый должностным лицом таможенного органа в аналитической работе (далее - база данных ТД);

б) операционной базы данных ТД, представляющей собой информационный ресурс таможенного органа, содержащий электронные копии ТД, хранимые и обрабатываемые с применением системы ТОиТК, и используемый должностным лицом таможенного органа при таможенном оформлении и таможенном контроле (далее - операционная база данных);

2) на уровне таможни:

а) операционной базы данных ТД (только для таможенных органов, оснащенных КАСТО «АИСТ-РТ21»);

б) базы данных ТД;

3) на уровне РТУ - базы данных ТД;

4) на уровне ГНИВЦ - центральной базы данных ТД (далее - ЦБД ТД).

Сроки хранения информации в указанных информационных ресурсах приведены в табл. 1.

Таблица 3.1 - Сроки хранения электронных копий ТД, содержащихся в информационных ресурсах таможенных органов и в ГНИВЦ

№ п/п	Уровень системы сбора ТД	Информационный ресурс		Срок хранения информации в оперативном доступе
1	Таможенный пост	Операционная база данных		Не менее 3 лет
		База данных	Зарегистрированные ТД	Не менее 1 года
			Оформленные ТД	Не менее 3 лет
2	Таможня	Операционная база данных		Не менее 7 лет
		База данных	Зарегистрированные ТД	Не менее 1 года
			Оформленные ТД	Не менее 7 лет
3	РТУ	База данных	Зарегистрированные ТД	Не менее 1 года
			Оформленные ТД	Не менее 15 лет
4	ГНИВЦ	Центральная база данных		Бессрочно

Для обеспечения бесперебойного функционирования системы сбора ТД выполняют:

1) уполномоченное должностное лицо отдела таможенного оформления и таможенного контроля таможенного поста, осуществляющее таможенные операции и таможенный контроль (далее - уполномоченное должностное лицо ОТОиТК таможенного поста):

а) ФЛК электронных копий ТД;

б) заполнение протокола завершения контроля (совокупность данных, содержащая разъяснения, формируемые уполномоченным должностным лицом ОТОиТК таможенного поста в случае обнаружения расхождений между алгоритмами работы систем ТОиТК, осуществляющих ФЛК, и решениями, принятыми на этапе проведения документального контроля);

в) контроль выгрузки электронной копии ТД, принятие которой оформлено путем присвоения ей регистрационного номера (далее - электронная копия зарегистрированной ТД), и электронной копии ТД, по которой в отношении товаров и транспортных средств таможенным органом принято решение, соответствующее классификатору решений, принимаемых таможенными органами, и указываемое в графе «D» комплекта бланков ТД 1 и в графе «D/J» комплекта бланков ТД 3 (далее - электронная копия

оформленной ТД), из систем ТОиТК в автоматическом или ручном режимах для их передачи в КПС «Сбор информации по ГТД»;

г) контроль полноты и достоверности сведений, содержащихся в электронных копиях зарегистрированных и оформленных ТД;

д) внесение необходимых исправлений в электронную копию оформленной ТД в соответствии с требованием о технической корректировке, содержащим совокупность данных об ошибках в заполнении электронной копии оформленной ТД, выявленных в ходе проведения ФЛК на этапе загрузки в ЦБД ТД (далее - требование о технической корректировке);

е) внесение необходимых изменений в электронную копию оформленной ТД при проведении корректировки ТД после выпуска товаров и транспортных средств;

ж) контроль сверки информации, содержащейся в операционной базе данных таможенного поста или в операционной базе данных ОТОиТК таможенного поста и базе данных таможенного поста на первом уровне системы сбора ТД;

з) контроль загрузки в базу данных таможенного поста в автоматическом или ручном режимах электронных копий зарегистрированных и оформленных ТД, а также за выгрузкой электронных копий зарегистрированных и оформленных ТД из базы данных таможенного поста в автоматическом или ручном режимах для их передачи в таможню, РТУ и ГНИВЦ;

2) уполномоченное должностное лицо ИТП таможни или РТУ в части информационно-технического обеспечения:

а) контроль формирования файла пакета передачи данных, представляющего собой поименованную совокупность данных, предназначенную для передачи по каналам связи ВИТС ФТС России (далее - ФППД), содержащего электронные копии зарегистрированных и оформленных ТД, и за его передачей на вышестоящие уровни системы сбора ТД;

б) регламентные работы по архивированию и резервному копированию операционной базы данных таможенного поста или операционной базы данных ОТОиТК таможенного поста и базы данных таможенного поста, таможни, РТУ в автоматическом или ручном режимах, а при необходимости их восстановление после сбоев;

в) установку и настройку программно-аппаратных средств ЕАИС таможенных органов, входящих в систему сбора ТД, с учетом интерфейса взаимодействия между ними, а также контроль их бесперебойного функционирования;

г) контроль сбора, обработки и загрузки в базу данных таможни и РТУ в автоматическом или ручном режимах электронных копий зарегистрированных и оформленных ТД, а также другой информации, передаваемой в системе сбора ТД;

д) контроль выгрузки из базы данных таможни и РТУ в автоматическом или ручном режимах информации, передаваемой в системе сбора ТД;

е) контроль формирования протоколов обработки ТД, содержащих совокупность данных о загрузке электронных копий, зарегистрированных и оформленных ТД в базу данных вышестоящего уровня системы сбора ТД (далее - протокол обработки) в автоматическом или ручном режимах;

3) уполномоченное должностное лицо отдела таможенной статистики (ОТС) таможни, РТУ в части усиления контроля за полнотой и достоверностью сведений, содержащихся в электронной копии, оформленной ТД:

а) контроль сроков внесения изменений в электронную копию оформленной ТД в соответствии с требованиями о технической корректировке;

б) контроль сверки информации, содержащейся в базе данных таможни и РТУ (операционной базе данных таможни при ее наличии) на втором и третьем уровнях системы сбора ТД;

в) анализ протоколов завершения контроля, заполняемых должностными лицами ОТОиТК таможенного поста, и подготовку предложений об изменении алгоритмов ФЛК;

г) контроль сроков внесения изменений в электронную копию оформленной ТД при проведении ее корректировки после выпуска товаров и транспортных средств;

4) уполномоченный работник ГНИВЦ в части загрузки ЦБД ТД:

а) контроль сбора, обработки и загрузки в ЦБД ТД в автоматическом или ручном режимах электронных копий зарегистрированных и оформленных ТД;

б) контроль формирования требований о технической корректировке и протоколов обработки;

в) контроль исправления электронных копий, оформленных ТД, не прошедших ФЛК на этапе загрузки информации в ЦБД ТД;

г) контроль проведения сверки информации, содержащейся в базах данных РТУ, таможен, непосредственно подчиненных ФТС России, и в ЦБД ТД;

д) формирование аналитических материалов и отчетов по результатам загрузки информации в ЦБД ТД.

ТД, появившись на таможне назначения, становится тем документом, вокруг которого в дальнейшем проводятся все проверки, а сведения, осевшие в БД грузовых таможенных деклараций, подвергаются различной обработке (рис. 3.1).

Помимо проверки правильности оформления ТД и при необходимости ее корректировки центральная БД ФТС России предусматривает возможности перекрестной проверки данных ТД и других специализированных документов, проведения статистической обработки информации о поступивших в Россию товарах и их объемах.

Рис. 3.1 - Информационная система сбора и обработки информации

Перечень информационных ресурсов ЦБД ЕАИС ФТС России составляют следующие базы данных:

• электронных копий грузовых таможенных деклараций (открытый и закрытый сегменты);

• электронных копий документов контроля доставки;

• автоматизированной системы «Авто-контроль»;

• электронных копий таможенных приходных ордеров;

• валютного контроля;

• временного ввоза (вывоза) товаров по процедуре карнет-АТА;

• агрегированных данных таможенной статистики внешней торговли;

• мониторинга таможенных операций;

• конфиската;

• штрафов;

• электронной корреспонденции;

• профилей рисков;

• нормативно-справочной информации.

Решение задач, связанных с организацией и управлением доступом должностных лиц структурных подразделений ФТС России и таможенных органов к ЦБД ЕАИС ФТС России, осуществляют:

• администратор регистрации, отвечающий за организацию технологического процесса доступа пользователей к информационным ресурсам ЦБД ЕАИС ФТС России и регистрацию пользователей;

• администратор данных, отвечающий за информационное наполнение ЦБД ЕАИС ФТС России и целевое использование информации;

• администратор базы данных, отвечающий за системное администрирование и управление ЦБД ЕАИС ФТС России;

• администратор ЛВС, отвечающий за системное администрирование ЛВС ГНИВЦа ФТС России;

• администратор безопасности, отвечающий за информационную безопасность ЦБД ЕАИС ФТС России;

• администраторы локальных сетей и безопасности таможенных органов.

ЦБД многократно продублирована: в частности, каждая региональная БД хранит всю информацию, накопленную РТУ за все время работы, и каждая таможня имеет полную информацию о своей деятельности. Такое многоуровневое резервирование позволяет в любой момент восстановить информацию, если что случится с ЦБД.

Доступ к ЦБД опосредован промежуточными Intel-серверами. Современные операционные системы позволяют непосредственно работать с массивами информации, что предопределяет возможность несанкционированного доступа к хранящейся информации. Поэтому в ФТС России, прежде всего, формализована специфика работы каждого таможенного подразделения, и должностные лица могут работать только с определенными полями таможенных деклараций в соответствии со своими задачами. Например, управление контроля таможенной стоимости работает с полями «Стоимость», «Вес нетто», «Вес брутто», а также с количеством наименований товаров. При этом сведения, которые запрашивает пользователь, выгружаются на промежуточный сервер, и обратного хода нет. Таким образом, исходная информация ЦБД развязана с теми данными,

которые обрабатываются в повседневной деятельности. Работа с ЦБД и ее обслуживание ведется с помощью Центрального вычислительного комплекса (ЦБК) на базе мощных серверов с большими вычислительными ресурсами. Глубина оперативного функционирования баз данных составляет 4-5 лет и определяется потребностью в информационном обеспечении центрального аппарата ФТС, органов Правительства, администрации Президента и других государственных структур. Для обеспечения эффективного выполнения задач ФТС России на базе двух центральных вычислительных комплексов (ЦБК «Комсомольская» и ЦВК «Фили») создана надежная отказоустойчивая система с реализацией кластерного решения, включающая два разнесенных в пространстве вычислительных комплекса и предполагающая следующую организацию работы:

• ЦВК «Комсомольская» - первичная обработка данных, поступающих из таможенных органов, реализация обратной связи с таможенными органами для формирования достоверной информации, формирование центральной базы данных статистической отчетности ЕАИС, выполнение регламентных отчетных работ и пр.;

• ЦВК «Фили» - резервный центр, предназначенный для выполнения оперативных запросов и работ ФТС России, зеркальная база данных и пр.

Основная нагрузка в ЦВК приходится на многопроцессорные серверы Alpha Server. Ведение баз данных НСИ осуществляется администратором системы баз данных и реализуется посредством генератора программных приложений НСИ, оформленного в виде пакета прикладных программ - «АРМ НСИ».

3.4 Принципы построения систем поддержки принятия решения должностными лицами таможенных органов

Осознание пользы накапливаемой информации и возможности использования ее для решения аналитических задач привело к появлению

нового класса вычислительных систем - систем поддержки принятия решений (СППР), ориентированных на аналитическую обработку данных.

Под системой поддержки принятия решений понимают человеко-машинный вычислительный комплекс, ориентированный на анализ данных и обеспечивающий получение информации, необходимой для разработки решений в сфере управления. К числу задач, которые традиционно решают системы поддержки принятия решений, относятся: оценка альтернатив решений, прогнозирование, классификация, кластеризация, выявление ассоциаций и др.

Представление о структуре СППР можно составить из рассмотрения рис. 3.2. В состав СППР помимо пользователя входят три главных компонента: подсистема обработки и хранения данных, подсистема хранения и использования моделей и программная поддержка. Последняя включает в себя систему управления базой данных (СУБД), систему управления базой моделей (СУБД) и систему управления диалогом между пользователем и компьютером (СУД).

Подсистема данных. Подсистема обработки и хранения данных характеризуется всеми известными преимуществами построения и использования баз данных. Однако использование баз данных в составе СППР характеризуется определенными обстоятельствами.

Так, например, базы данных в составе СППР имеют значительно больший набор источников данных, включая внешние источники, особенно важные для принятия решений на высоких уровнях управления, а также источники не компьютеризированных данных.

Рис. 3.2 - Структура подсистемы моделей СППР

Другой особенностью является возможность предварительного «сжатия» данных, поступающих из многочисленных источников, путем их предварительной совместной обработки процедурами агрегирования и фильтрации.

Данные играют в СППР важную роль. Они могут использоваться непосредственно пользователем или как исходные данные для расчета при помощи математических моделей.

В информационных системах, входящих в состав ЕАИС, часть данных подсистема данных СППР получает от подсистемы сбора и обработки статистической информации о таможенных процессах. Однако лишь в редких случаях данные, полученные на уровне обработки (например, операций с участниками ВЭД), оказываются полезными для СППР. Для того чтобы получить возможность использования, эти данные должны быть предварительно обработаны. Для этого имеются две возможности. Первая - использовать для обработки данных СУБД, входящую в состав СППР. Вторая - сделать обработку за пределами СППР, создав для этого специальную базу данных.

Идея создания специальной базы данных для обработки таможенных процессов базируется на целесообразности отделить сферу автоматической

электронной обработки данных от сферы менее квалифицированного конечного пользователя.

Важное значение, особенно для поддержки принятия решения на верхних уровнях управления ФТС России, имеют данные из внешних источников. В числе необходимых внешних данных следует указать данные о национальной и мировой экономике (таможенные тарифы других стран и пр.). В отличие от внутренних данных внешние данные часто могут быть куплены у специализирующихся на их сборе организаций.

Таким образом, подсистема данных, входящих в состав СППР, должна обладать следующими возможностями:

• составление комбинаций данных, получаемых из различных источников, посредством агрегирования и фильтрации;

• быстрое прибавление или исключение того или иного источника данных;

• построение логической структуры данных в терминах пользователя;

• управление данными при помощи широкого спектра функций управления, предоставляемых СУБД.

Подсистема моделей. Наряду с обеспечением доступа к данным СППР обеспечивает доступ пользователя к моделям принятия решений. Это достигается введением в информационную систему соответствующих моделей и использованием в ней базы данных как механизма интеграции моделей и коммуникации между ними (рис. 3.2).

Полученная в результате СППР сочетает в себе преимущества систем электронной обработки данных и информационных систем управления в части обработки данных и генерации управленческих отчетов с достоинствами методов исследования операций эконометрики в части математического моделирования ситуаций и нахождения решения.

Процесс создания моделей должен быть гибким. Он должен включать в себя специальный язык моделирования, совокупность отдельных

программных блоков и модулей, реализующих отдельные компоненты различных моделей, а также набор функций управления.

Использование моделей обеспечивает способность СППР к проведению анализа. Модели, использующие математическую интерпретацию проблемы, при помощи определенных алгоритмов способствуют нахождению информации, полезной для принятия правильных решений. Например, модель линейного программирования дает возможность определить наиболее выгодную производственную программу выпуска нескольких видов продукции при заданных ограничениях на ресурсы.

Использование моделей в составе информационных систем началось с применения статистических методов и методов финансового анализа, которые реализовывались командами обычных алгоритмических языков. Позже были созданы специальные языки, позволяющие моделировать ситуации типа «что будет, если?» или «как сделать, чтобы?». Такие языки, созданные специально для построения моделей, дают возможность построения моделей определенного типа, обеспечивающих нахождение решения при гибком изменении переменных.

В настоящее время существует множество типов моделей и способов их классификации, например, по цели использования, области возможных приложений, способу оценки переменных и т. п.

Целью создания моделей являются либо оптимизация, либо описание некоторого объекта или процесса. Оптимизационные модели связаны с нахождением точек минимума или максимума некоторых показателей. Например, управляющие часто хотят знать, какие их действия ведут к максимизации прибыли (минимизации затрат). Модели оптимизации позволяют получать подобную информацию. Описательные модели описывают поведение некоторой системы и не предназначены для целей управления (оптимизации).

Хотя большинство систем носит стохастический характер (т. е. их состояние не может быть предсказано с абсолютной достоверностью),

большинство математических моделей построены как детерминистские. Детерминистские модели используют оценку переменных одним числом (в отличие от стохастических моделей, оценивающих переменные несколькими параметрами), а также более популярны, чем стохастические, потому что они менее дорогостоящие и трудные, их легче строить и использовать. К тому же часто с их помощью возможно получить достаточную информацию для помощи принимающему решение.

База моделей. Модели в СППР образуют базу моделей, включающую в себя стратегические, тактические и оперативные модели, а также совокупность модельных блоков, модулей и процедур, используемых как элементы для построения моделей (рис. 3.2). Каждый тип моделей имеет свои уникальные характеристики.

Стратегические модели используются на высших уровнях управления для установления целей организации, объемов ресурсов, необходимых для их достижения, а также политики приобретения и использования этих ресурсов. Для стратегических моделей характерна значительная широта охвата, множество переменных, представление данных в сжатой агрегированной форме. Часто эти данные базируются на внешних источниках и могут иметь субъективный характер. Горизонт планирования в стратегических моделях обычно измеряется в годах. Эти модели, как правило, детерминистские, описательные, специализированные для использования на одной определенной фирме.

Тактические модели применяются управляющими среднего уровня для распределения и контроля использования имеющихся ресурсов.

Среди возможных сфер их использования следует указать: финансовое планирование, планирование требований к работникам, планирование увеличения таможенных сборов, построение схем компоновки таможенных подразделений.

Временной горизонт, охватываемый тактическими моделями, лежит между одним месяцем и двумя годами. Здесь также могут потребоваться

данные их внешних источников, но основное внимание при реализации этих моделей должно быть уделено внутренним данным фирмы. Обычно тактические модели реализуются как детерминистские, оптимизационные и универсальные.

Оперативные модели используются на низших уровнях управления для поддержки принятия оперативных решений с горизонтом, измеряемым днями и неделями. Возможные применения этих моделей включают в себя введение дебиторских счетов и кредитных расчетов, календарное производственное планирование, управление запасами и т. д.

Оперативные модели обычно используют для своих расчетов внутренние данные таможенного подразделения. Они, как правило, детерминистские или оптимизационные.

В дополнение к стратегическим, тактическим и оперативным моделям база моделей СППР включает в себя совокупность модельных блоков, модулей и процедур.

Сюда могут входить процедуры линейного программирования, статистического анализа временных рядов, регрессионного анализа и т. п. - от простейших процедур до сложных пакетов прикладных программ. Модельные блоки, модули и процедуры могут использоваться как поодиночке, самостоятельно, для помощи пользователям СППР, так и комплексно, в совокупности, - для построения и поддержания модулей.

Системы управления интерфейсом. Эффективность и гибкость СППР в решении самостоятельных задач во многом зависит от характеристик используемого интерфейса. Интерфейс включает в себя программную систему управления диалогом (СУД), компьютер и самого пользователя.

Глава 4. Основы компьютерных телекоммуникаций

4.1 Основные положения концепции TCP/IP

Вряд ли современному человеку нужно объяснять такое понятие как Internet. Синонимом слова Internet является «Всемирная паутина». По-английски это пишется как World Wide Web или сокращенно WWW. От английского выражения «Всемирная паутина» произошло много побочных системных терминов: Web-приложения, Web-узлы, Web-серверы и т.п.

Подключение пользователя к Интернету осуществляется провайдером - компанией поставщиком услуг Интернета.

Большинство компьютеров в Internet в любой отдельно взятый момент времени являются клиентами. Это значит, что они потребляют услуги, предоставляемые другими компьютерами. Клиентом называют не только сами ЭВМ, но и установленные на них программы, пользующиеся услугами Сети. Например, программы браузеры или веб-обозреватели.

Браузер (от англ. Web browser; вариант броузер - устаревшая форма) - программное обеспечение для просмотра веб-сайтов, то есть для запроса веб-страниц, их обработки, вывода и перехода от одной страницы к другой.

Владелец компьютера - клиента называется пользователем сети.

Остальные компьютеры Сети являются серверами. Серверы предоставляют клиентам услуги, которыми они пользуются. В общем случае эту задачу выполняет не физический владелец сервера, а сама машина.

Прокси-сервер (от англ. proxy - «представитель, уполномоченный») - служба (комплекс программ) в компьютерных сетях, позволяющая клиентам выполнять косвенные запросы к другим сетевым службам. Сначала клиент подключается к прокси-серверу и запрашивает какой-либо ресурс (например, e-mail), расположенный на другом сервере. Затем прокси-сервер либо подключается к указанному серверу и получает ресурс у него, либо возвращает ресурс из собственного кэша (в случаях, если прокси имеет свой

кэш). В некоторых случаях запрос клиента или ответ сервера может быть изменён прокси-сервером в определённых целях. Также прокси-сервер позволяет защищать клиентский компьютер от некоторых сетевых атак и помогает сохранять анонимность клиента.

Веб-сервер - это сервер, принимающий HTTP-запросы от клиентов, обычно веб-браузеров, и выдающий им HTTP-ответы, обычно вместе с HTML-страницей, изображением, файлом, медиа-потоком или другими данными. Веб-серверы - основа Всемирной паутины.

Веб-сервером называют как программное обеспечение, выполняющее функции веб-сервера, так и непосредственно компьютер, на котором это программное обеспечение работает.

Клиент, которым обычно является веб-браузер, передаёт веб-серверу запросы на получение ресурсов, обозначенных URL-адресами. В ответ веб-сервер передаёт клиенту запрошенные данные. Этот обмен происходит по протоколу HTTP.

Ресурсы - это HTML-страницы, изображения, файлы, медиа-потоки или другие данные, которые необходимы клиенту.

URL - единый указатель ресурсов (англ. URL - Uniform Resource Locator) - единообразный локатор (определитель местонахождения) ресурса. URL - это стандартизированный способ записи адреса ресурса в сети Интернет.

В полном URL адресе часть имени узла, следующая за префиксом http://, имеет следующий формат:

узел.домен.ДВУ

где узел - это конкретный компьютер в домене (группе) компьютеров.

Аббревиатура ДВУ расшифровывается как домен высшего уровня. Этот домен описывает "тип" узла.

Наиболее распространенные ДВУ перечислены в таблице:

Примеры доменов высшего уровня и узлов, к ним принадлежащих.

ДВУ	Тип	Пример узла
.com	Коммерция	www.amazon.com www.ucla.edu
.edu	Образование	www.fbi.gov www.redcross.org
.gow	Правительственный	www.comcast.net www.army.mil
.org	Неправительственные организации	
.net	Сети	
.mil	Военный	

Информация в сетях, как правило, передается отдельными порциями, кусками, называемыми в различных источниках пакетами, кадрами или блоками. Использование пакетов связано с тем, что в сети одновременно может происходить несколько сеансов связи, то есть в течение одного и того же интервала времени могут идти два или больше процессов передачи данных между различными парами абонентов. Пакеты как раз позволяют разделить во времени сеть между передающими информацию абонентами.

Чтобы уравнять в правах всех пользователей, а также примерно уравнять время доступа к сети и интегральную скорость передачи информации для всех абонентов, как раз и используются пакеты (кадры). Длина пакета зависит от типа сети, но обычно она составляет от нескольких десятков байт до нескольких килобайт.

Чаще всего пакет содержит в себе следующие части.

Преамбула - стартовая комбинация, обеспечивает настройку сетевого оборудования.

Идентификатор приемника - сетевой адрес места назначения пакета.

Идентификатор передатчика - сетевой адрес места отправления пакета.

Управляющая или служебная информация - указывает на тип пакета, его номер, размер, формат, маршрут его доставки.

Данные - та информация, ради передачи которой используется данный пакет.

Контрольная сумма пакета - числовой код, формируемый передатчиком по определенным правилам и содержащий в свернутом виде информацию обо всем пакете. Позволяет определять правильность передачи информации.

Стоповая комбинация - служит для информирования аппаратуры принимающего абонента об окончании пакета.

Нередко в структуре пакета всего три поля:

Начальное управляющее поле (или заголовок пакета) - включает стартовую комбинацию, сетевые адреса приемника и передатчика, а также служебную информацию.

Поле данных пакета.

Конечное управляющее поле пакета - включает контрольную сумму и стоповую комбинацию, а также, возможно, служебную информацию.

Протокол управления передачей данных TCP (Transmission Control Protocol, описан в стандарте RFC 793).

Протокол - это набор правил и процедур, регулирующих порядок осуществления связи. Выделяют протоколы нижних уровней (физического и канального) и высоких уровней. Иерархически организованный набор протоколов, достаточный для организации взаимодействия узлов в сети, называется стеком коммуникационных протоколов (рис. 4.1).

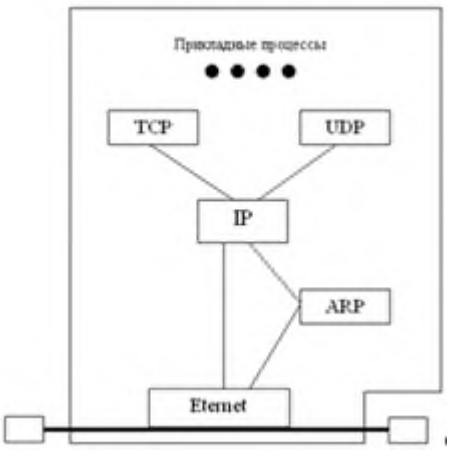

Рис. 4.1 - Структура взаимодействия протокольных модулей TCP/IP

На рис. 4.1 приложения - это программы, предназначенные для обмена информацией между ЭВМ. Например, браузеры.

TCP и UDP это протоколы транспортного уровня для передачи информации в виде пакетов.

Протокол ARP используется для отображения в передаваемых пакетах адресов IP (т.е. адресов ЭВМ в Интернете) в адреса Ethernet (т.е. в физические адреса ЭВМ локальной сети).

Межсетевой протокол IP (описан в стандарте RFC 751) предназначен для инкапсуляции IP-пакетов в физический канал связи Ethernet.

Ethernet это канальный протокол для передачи пакетов между ЭВМ по физическому каналу связи.

Принципы адресации в сетях TCP/IP. Сетевой адрес имеет длину 32 бита. Ограниченная длина этого адреса в совокупности с используемым принципом определения маршрута приводит к резкому сокращению числа активных узлов сети. Как и всякий адрес протокола сетевого уровня, адрес протокола IP состоит из двух компонентов (рис. 4.2) - из адреса сети (Net Id) и адреса узла сети (Host Id). Правильный адрес состоит из четырех чисел, разделенных точками. Каждое число представляется байтом и может принимать значения в диапазоне 0-254. Заключительные нули в адресе используются для ссылок на сетевые сегменты. При записи адреса сервера или рабочей станции завершающие нули заменяются числами (1-254).

<table>
<tr><td></td><td colspan="10">IP Address</td></tr>
<tr><td>Класс</td><td>31</td><td>30</td><td>29</td><td>28</td><td>27</td><td>-</td><td>24</td><td>23-16</td><td>15-8</td><td>7-0</td></tr>
<tr><td>A</td><td>0</td><td colspan="6">Net Id</td><td colspan="3">Host Id</td></tr>
<tr><td>B</td><td>1</td><td>0</td><td colspan="5">Net Id</td><td colspan="2">Host Id</td></tr>
<tr><td>C</td><td>1</td><td>1</td><td>0</td><td colspan="6">Net Id</td><td>Host Id</td></tr>
<tr><td>D</td><td>1</td><td>1</td><td>1</td><td>0</td><td colspan="6">Multicast Address</td></tr>
<tr><td>E</td><td>1</td><td>1</td><td>1</td><td>1</td><td>0</td><td colspan="5">Резервный</td></tr>
</table>

Рис. 4.2 - Структура IP-адреса

Для обеспечения возможности более эффективного использования адресного пространства Internet используется пять форматов (классов) сетевого адреса IP: A, B, C, D и E. Четыре старших разряда сетевого адреса используются для того, чтобы определить тип используемого формата сетевого адреса.

Старшие 8 разрядов сетевого адреса класса A задают номер сети - от 1 до 127. В последующих трех байтах размещается адрес узла. Сети класса A, таким образом, могут содержать 16387064 узла. Сети класса B могут содержать до 65534, а сети класса C до 254 узлов.

Сети класса D предназначены для определения IP адресов типа multicast (групповые или широковещательные адреса). Сети класса A, B и C относят к группе индивидуальных адресов. Сети класса E зарезервированы для дальнейшего использования.

Сетевые технологии, основанные на протоколах TCP/IP, предполагают поддержку на канальном уровне многих различных сред передачи данных. Физической основой стека протоколов TCP/IP является канальный протокол Ethernet. Кроме того, эта основа является наиболее распространенной средой локальных сетей.

Каждая интерфейсная сетевая карта Ethernet имеет уникальный шестибайтовый адрес (так называемый MAC адрес), который по традиции записывается шестнадцатеричными числами, разделенными двоеточиями или тире, например,:

8 : 0 : 20 : 0 : fb : 6a

или

8 – 00 – 20 – 00 – fb – 6a

В операционной системе Unix, как правило, используется двоеточие, а в системе MS Windows запись идет – через тире.

Каждый сетевой интерфейс имеет также свой IP-адрес. Работающая ЭВМ с установленным протоколом TCP/IP всегда «знает» свой Ethernet-адрес и свой IP-адрес.

Для отображения адресов IP в адреса Ethernet используется протокол ARP – разрешения адресов. Отображение восполняется только для отправленных пакетов IP, так как заголовки создаются только в момент отправки.

Преобразование адресов выполняется путем поиска в таблице. Эта таблица называется ARP-таблицей, хранится в памяти машины – для каждого сетевого адаптера в каждой сетевой машине имеется такая таблица. Она содержит строки для каждого узла сети. В двух столбцах содержится адреса IP и Ethernet.

Таблица ARP нужна потому, что адреса IP и Ethernet выбираются независимо, и нет какого-то алгоритма преобразования одного адреса в другой. Адрес IP выбирает администратор сети с учётом положения машины в сети Internet. Если ЭВМ перемещают в другую часть сети, её IP-адрес должен быть изменен. Адрес сетевого адаптера (Ethernet) устанавливается производителем адаптера и не меняется при перемещении ЭВМ по сети.

Таблица ARP заполняется автоматически в ходе сетевой работы. Когда с помощью существующей таблицы не удаётся преобразовать IP-адрес в адрес Ethernet, происходит следующее:

по сети передаётся широковещательный запрос ARP;

исходящий IP-запрос становиться в очередь;

широковещательные передачи принимает каждый адаптер сети;

ЭВМ с искомым IP-адресом ответит на ARP-запрос пакетом, где содержится искомый адрес Ethernet, который после этого будет внесен в обновленную таблицу;

если в сети нет машины с искомым адресом IP (или она не включена), то ответа широковещательный запрос ARP не будет и не будет записи в таблицу ARP. По протоколу IP все пакеты с этим адресом будут уничтожаться.

Для обратного преобразования адреса Ethernet в IP-адрес служит протокол RARP.

В последнее время применяется стандартный формат кадра протоколов канального уровня (рис. 4.3).

Ф	Адрес	Контроль и управление	Информация (пакет)	Проверочное поле	Ф

Рис. 4.3 - Формат стандартного кадра

В начале и в конце каждого кадра для установления и поддержания синхронизации последовательность, обычно 8-разрядная нулей и единиц, называемая флагом или меткой. Флаги (Ф) применяются в начале и в конце кадра, поэтому в установке структуры информационного поля нет необходимости. Пакет, поступающий от вышестоящего сетевого уровня, может занимать любое, желаемое число разрядов. Проверочное поле занимает 16 разрядов, поля адреса, контроля и управления – по 8 разрядов.

Протокол канального уровня реализует следующие функции:

реализацию соединения каналов;

организация передачи данных по каналу;

разъединение каналов.

Каждый отправитель и получатель данных в сети должен иметь свой адрес. Адрес можно определить, как идентификатор объекта, однозначно определяющий и его положение в сети. Это определение происходит по некоторым принятым в данной сети правилам. Следовательно, по этим же правилам должен формироваться и адрес.

Все данные в сети передаются в виде IP-пакетов (IP packets). Протокол IP определяет глобальную схему адресации. Согласно этой схеме каждый сетевой интерфейс имеет свой собственный адрес, который представляет собой 32-битовый номер, уникальный в пределах Интернет. Обычно IP-адреса записываются в виде четырёх чисел, разделённых точками, например – 192.168.100.129. Такой способ называется дот-нотацией (dot-notation). Эти

числа могут находиться в диапазоне от 0 до 255, потому что каждое из них может быть записано в восьми двоичных разрядов – в байте.

Адреса в виде 32-разрядного двоичного слова неудобны для запоминания людям. Поэтому была разработана специальная доменная служба имен DNS (Domaine Name Service), которая ставит в соответствие IP-адресам некоторые мнемонические обозначения и наоборот. Обращения к сетевым компьютерам по их доменным именам хорошо понятны и вполне привычны для тех, кто хотя бы немного имел дело с Интернет. Так, например, вместо приведенного ранее адреса 192.168.100.129 можно использоваться его мнемоническое обозначение (URL): Ns.muka.ac.ru

Доменные адреса URL не используются и не распознаются протоколом IP. Если приложение должно передавать данные на другую машину, оно должно сначала обратиться в службу DNS, чтобы перевести доменное имя URL в IP-адрес. Принимающее приложение должно проделать обратную операцию: при помощи DNS найти доменное имя URL по IP-адресу.

На транспортном уровне стека TCP/IP используется 2 основных протокола: UDP и TCP.

Протокол UDP (User Datagram Protocol – протокол пользовательских дейтаграмм, описан в стандарте RFC 768) предоставляет прикладным процессам транспортные услуги, которые немного отличаются от услуг протокола TCP.

Дейтаграмма - это пакет данных пользователя, передаваемый в сети и содержащий адреса и полезные данные.

Примерами сетевых приложений, использующих протокол UDP, является DNS (Domain Name Service – доменная служба имен) и SNMP (Simple Network Managment Protocol – простой протокол управления сетью), по которому работает и сетевая служба времени.

Понятие «порт» в протоколах UDP и TCP характеризует ту или иную программу в ЭВМ, включенную в IP-сеть. Номер порта по традиции нумеруется в виде десятичного числа, начиная с нуля. Таким образом, IP-адрес

характеризует машину в сети, а адрес порта характеризует ту или иную программу в машине. Аналогией может служить обычный конверт: в строке «Куда» пишется IP-адрес, а в строке «Кому» - номер порта.

Прикладной процесс (сервер), предоставляющий некоторые услуги другим процессам, ожидает поступление сообщений по некоторому, специально выделенному порту, иначе говоря – «порт слушает». Запросы на предоставление услуг посылаются процессами – клиентами. Такая организация работы в сети носит название «Клиент – сервер».

Например, сервер SNMP всегда ожидает поступления сообщения в порт 161 по протоколу UDP. Если клиент SNMP желает получить услугу, он посылает запрос в UDP-порт 161 на машину, где работает сервер SNMP, так как существует только один порт с номером 161. Этот номер общеизвестен, то есть он фиксирован для услуг SNMP.

Протокол TCP также предоставляет транспортные услуги. TCP обеспечивает гарантированную доставку дейтаграмм с установленным соединением в виде байтовых потоков.

Этот протокол используется в тех случаях, когда требуется надежная доставка сообщений. Он освобождает прикладные процессы от необходимости использовать тайм-ауты и повторные сообщения для обеспечения надежности. Наиболее типичными прикладными процессами, использующими TCP, являются FTP (File Transfer Protocol – протокол для передачи файлов) и Telnet.

Telnet это протокол Internet для регистрации на удаленных хостах и обработки данных на них. Данный протокол предназначен для удаленного администрирования и обеспечения удаленного доступа к ЭВМ или серверам. Его основная задача заключается в том, чтобы позволить терминальным устройствам и терминальным процессам взаимодействовать друг с другом. Предполагается, что этот протокол может быть использован для связи вида терминал-терминал («связывание») или для связи процесс-процесс («распределенные вычисления»).

Реализация TCP требует большой производительности процессора и большой пропускной способности сети. Внутренняя структура модуля TCP гораздо сложнее структуры модуля UDP.

Прикладные процессы взаимодействуют с модулем TCP, как и в случае UDP, через порты, использую технологию «клиент-сервер». Когда прикладной процесс начинает использовать этот протокол, модуль TCP на стороне клиента и модуль TCP на стороне сервера начинают «общаться». Эти два оконечных модуля поддерживают информацию о состоянии соединения, называемого виртуальным каналом. Виртуальный канал потребляет ресурсы обоих оконечных модулей TCP. Канал является дуплексным: данные могут одновременно передаваться в обоих направлениях. Один прикладной процесс передает данные в TCP-порт; данные проходят по сети; другой прикладной процесс читает их из второго порта.

Протокол TCP требует, чтобы все отправленные данные были подтверждены принявшей их стороной. Он использует тайм-ауты и повторные передачи для обеспечения надежной доставки. Отправителю разрешается отправлять некоторое количество данных, не дожидаясь подтверждения их приема. Таким образом, между отправленными и подтвержденными данными существует, так называемое, окно уже отправленных, но ещё не подтвержденных данных. Количество сегментов, которые можно передавать без подтверждения, называется размером окна. Как правило, этот размер устанавливается в стартовых файлах сетевого программного обеспечения. Так как канал TCP является дуплексным, то подтверждение для данных, идущих в одном направлении, может передаваться с данными, идущими в другом направлении. Приемники на обеих сторонах виртуального канала выполняют управление потоками передаваемых данных, чтобы не допускать переполнение буферов.

Протоколы TCP и UDP предоставляют разные транспортные услуги прикладным процессам. Поэтому прикладные процессы используются только одним из них.

Основным протоколом уровня приложений является HTTP (Hyper Text Transfer Protocol – протокол передачи гипертекста). С использованием этого протокола браузерами осуществляется доступ к Web-сервису Интернет.

Другими важнейшими протоколами являются протокол передачи файлов – FTP, протокол удаленного администрирования telnet и протокол электронной почты SMTP.

4.2 Протокол и аппаратные средства сетей Ethernet

В РФ из всех видов локальных сетей наиболее популярными и преобладающими являются сети Ethernet.

Под локальными вычислительными сетями (ЛВС) принято понимать программно-аппаратный комплекс, включающий в себя несколько активно взаимодействующих компьютеров (от нескольких штук до нескольких сотен), соединенных между собой каналами связи. В локальную сеть включается также коммуникационное оборудование: концентраторы, коммутаторы и маршрутизаторы.

В настоящее время концепция локальных вычислительных сетей достаточно хорошо проработана. В основе этой концепции лежит принцип организации ЛВС в виде, так называемой, сети Интранет, т.е. внутренней сети, построенной на основе тех же протоколов, программного обеспечения, средств доступа и защиты информации, что и глобальная сеть Интернет.

Локальные ВС могут объединять большое количество рабочих мест на основе ЭВМ. Пользователи сети имеют возможность совместного использования оборудования сети. В ЛВС можно выделить следующие технологические преимущества:

разделение аппаратных средств; например, доступ к печатающему устройству со всех рабочих станций сети;

разделение данных; со всех рабочих станций обеспечивается доступ к системе управления базой данных;

разделение программных средств; необходимые программы могут быть запущенны с любой рабочей станции;

разделение ресурсов процессора файлового сервера. Процессор используется в режиме разделения времени. Его особенность заключается в том, что доступ к имеющимся ресурсам осуществляется не по принципу «кто первый захватит», а через специальный диспетчер;

мультипрограммный режим предоставляет возможность даже одному пользователю организовать работу сразу с несколькими заданиями;

электронная почта, с помощью которой происходит интерактивный обмен информацией между пользователями на рабочих станциях сети.

Необходимо отметить, что отмеченные возможности не являются специфическими для локальных сетей. В той или иной мере они присущи и другим сетям.

Сети Ethernet используют протокол канального уровня Ethernet. Этот протокол обеспечивает унифицированный интерфейс к сетевой среде передачи, который позволяет операционной системе использовать для приема и передачи данных несколько протоколов сетевого уровня одновременно.

Спецификация Ethernet определяет протокол как совокупность из трех необходимых компонентов:

набора правил физического уровня, задающих типы кабеля и ограничения кабельной системы для сетей Ethernet;

формата кадра, задающего порядок и назначение битов, передаваемых в пакете Ethernet;

механизма управления доступом к среде, называемого множественным доступом с контролем несущей частоты и обнаружением коллизий.

Множественный доступ означает, что любое подключенное устройство может передавать информацию.

Контроль несущей означает, что имеется возможность определить, занят канал или нет.

Обнаружение коллизий дает возможность выяснить перебивает ли передача с конкретного компьютера какую-либо другую передачу.

Фактически задержка при обнаружении коллизий – величина случайная. Это позволяет избежать такого развития событий, когда две машины одновременно передают сообщения по сети, обнаруживают коллизию, ждут некоторое время, а потом возобновляют передачу, переполняя сеть коллизиями. Вычисление задержки происходит с использованием генератора случайных чисел на некотором диапазоне. Количество попыток передачи не бесконечно. После определенного числа попыток сообщение снимается.

С точки зрения готового изделия, протокол Ethernet реализован в виде следующих составляющих: плат сетевых адаптеров, вставляющихся в компьютеры, драйверов сетевых адаптеров, позволяющих операционной системе взаимодействовать с этими адаптерами. А также концентраторы, соединяющие компьютеры друг с другом.

Первый стандарт Ethernet был опубликован в 1980 году. Он предполагал использование коаксиального кабеля, работающего со скоростью 10 Мбит/с и манчестерское кодирование сигналов. Этот метод получил в дальнейшем название «толстый Ethernet» из-за толщины кабеля, диаметр которого составлял около 1-го сантиметра.

Стандарт DIX Ethernet 2, был опубликован в 1981 году, он предполагал использование другого типа коаксиала, стандарт получил название «тонкий Ethernet». Кроме того, этот кабель был значительно дешевле толстого коаксиала.

Нынешняя версия Ethernet определяется спецификацией IEEE802.3 (Institute of Elecal and Electronics Engineers). С некоторыми минимальными отличиями этот документ фактически описывал сеть Ethernet под другим именем. До сегодняшнего дня продукты, на которые мы ссылаемся как на Ethernet, в действительности соответствуют стандарту IEEE802.3.

На основании этого стандарта коаксиал уступил место «витой паре». «Витая пара» или 10BaseT быстро стала наиболее популярной средой

передачи для этого протокола. Большинство действующих сегодня сетей Ethernet используют кабель «витая пара», который продолжает поддерживаться новыми высокоскоростными стандартами. Оптоволоконные технологии, не чувствительные к электромагнитным помехам, позволили протянуть сетевые соединения на много большие расстояния, чем это допускают медные технологии.

Стандарт Fast Ethernet (1995г.) под именем IEEE802.3u увеличивает скоростную способность сети в 10 раз, то есть до 100 Мбит/с и использует витую пару или оптоволокно.

Стандарт Gigabit Ethernet (IEEE802.3z) увеличил скорость сети до 1 Гбит/с.

В качестве рабочих мест в ЛВС применяются автономные компьютерные системы, называемые рабочими станциями и автоматизированными рабочими местами (АРМ).

Обычно рабочие станции располагают собственными внешними накопителями, но допускаются конфигурации без таких накопителей со специальным постоянным запоминающим устройством (ПЗУ) для загрузки сетевого программного обеспечения.

Управление различными службами в ЛВС осуществляется с использованием одного или нескольких серверов. В терминологии сетевых технических средств сервер – это один из включенных в сеть компьютеров, располагающих соответствующими программными и достаточными аппаратными мощностями для выполнения какого-либо обслуживания. С этой точки зрения принципиальной разницы между сервером и рабочей станцией, снабженной специальным программным обеспечением, нет.

Другое дело, к серверу могут предъявляться некоторые дополнительные требования, связанные с необходимостью обслуживания большого числа запросов от многих станций и других серверов. Например, типичным требованием к серверам является требование круглосуточной и бесперебойной работы.

Повышенные требования предъявляются к программно-аппаратному обеспечению файловых серверов. Это связано с тем, что от таких серверов зависят временные характеристики по загрузке, передаче и хранению данных в сети.

Для подключения ЭВМ к сети требуются устройства сопряжения, называемые сетевыми адаптерами или сетевыми интерфейсными картами. Они вставляются в гнёзда материнской платы компьютера. В настоящее время широкое распространение приобрели адаптеры, которые могут настраиваться на различные скорости передачи данных: 10 Мбит/с (Ethernet) и 100 Мбит/с (Fast Ethernet).

Большинство сетевых адаптеров Ethernet имеют разъемы для подключения разных видов кабелей: RJ-45 для «витой пары», BNC для тонкого коаксиального кабеля. Некоторые имеют также разъём AVI на 15 контактов для толстого коаксиального кабеля. В настоящее время в основном используются сетевые адаптеры, рассчитанные на сопряжение PCI.

Раньше выпускались сетевые адаптеры, в которых адрес подключения и номер прерывания настраивались вручную с помощью перемычек (jumpers). Потом стала практиковаться программная настройка. В настоящее время выпускаются адаптеры с автоматической настройкой Plug-and-Play (PnP), которые в случае конфликтов с другими аппаратными средствами допускает и программную перенастройку.

При выпуске, каждый сетевой адаптер снабжается микросхемой с уникальным, 48-битовым адресом Ethernet (MAC адрес). Каждая фирма, имеющая лицензию на выпуск адаптеров, располагает собственным диапазоном адресов Ethernet, так что в мире не должно быть интерфейсных карт с одинаковыми адресами.

Для взаимного преобразования интернетовских адресов в аппаратные и обратно служат протоколы ARP (Address Resolution Protocol) и RARP (Reverse ARP).

Обычно топология сетей Ethernet представляет собой шину с ветвлениями. В каждой логической сети (в смысле адресации TCP/IP) между двумя любыми точками имеется только один путь. Данные, пересылаемые по кабельной системе, передаются в широковещательном режиме.

Стандартная спецификация Ethernet предусматривает скорость передачи данных 10 Мбит/с. Технология Fast Ethernet рассчитана на скорость 100 Мбит/с.

Традиционно, в сетях Ethernet применяется три среды передачи данных:

коаксиальный кабель;

медный провод «витая пара»

оптоволоконный кабель

Одна логическая локальная сеть может быть значительно территориально распределена в разных зданиях, удаленных друг от друга на значительные расстояния, иногда на десятки километров. Внутри зданий сетевые компьютеры могут отстоять друг от друга на десятки метров. Поэтому в одной ЛВС могут использоваться различные виды коммуникационных каналов.

4.3 Протокол Frame Relay

С появлением более быстрых и надежных линий связи возникла потребность в новых технологиях информационного обмена. Для обеспечения большей производительности и реализации преимущества новых цифровых и оптоволоконных коммуникаций был разработан протокол Frame Relay (FR). Первоначально он проектировался под сети ISDN. Однако в 1990г. консорциум американских производителей во главе с Cisco System сосредоточили усилия на расширении возможностей протокола Frame Relay. Названные дополнения к уже известным рекомендациям получили название: локальный интерфейс управления (Local Management Interface – LMI) и были включены в стандартную спецификацию протокола Frame Relay.

Frame Relay переводится как «пересылка кадров», то есть рассматриваемый протокол охватывает первые два уровня иерархии модели OSI, где обмен кадрами осуществляется на втором уровне, а пакетами на третьем.

Действие протокола Frame Relay сравнивают с действием воронки для перелива жидкости (рис. 4.4.). По одному физическому каналу могут передаваться данные по нескольким логическим каналам, в том числе голосовая и видеоинформация.

Frame Relay передает данные пользователей по виртуальным каналам, которые однозначно определяются идентификатором информационных связей DLCI (Data Link Connection Identifier). Это ключевое понятие протокола. Под DLCI в заголовке кадра отведены 10 бит, так что его значение не может превышать числа 1023. Каждый DLCI обеспечивает логическое соединение с удаленным объектом, разделяя общий физический канал.

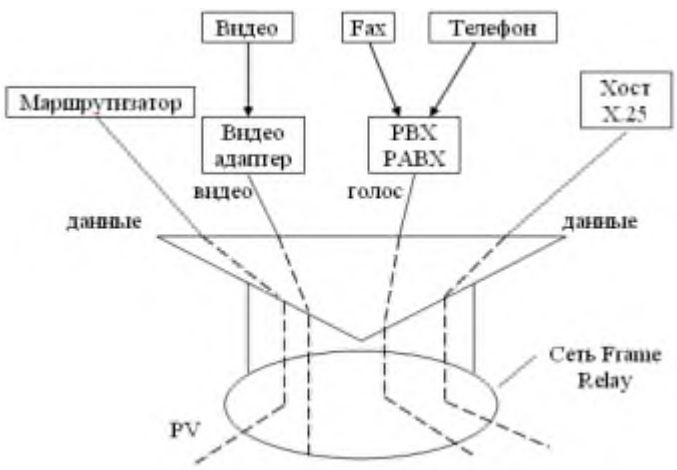

Рис. 4.4 - Взаимодействие транспортных протоколов с Frame Relay

В настоящее время в стандарте FR используются постоянные виртуальные каналы PVC с фиксированными номерами DLCI, что позволяет упростить и, тем самым, ускорить маршрутизацию кадров.

Кадры протокола обособлены начальными и конечными ограничительными флагами. Стандартный заголовок кадра имеет размер 2 байта. Здесь предусмотрены служебные биты управления потоком в сети, что позволяет избежать перегрузок. Управление потоком может быть организованно также и по специальному протоколу управления перегрузками на интерфейсе.

Информационное поле кадра может иметь размер от 32 байт до 4 килобайт. Проверка искажения кадра осуществляется с помощью формируемого циклического избыточного кадра (CRC – Cyclic Redundancy Check). Но механизма корректировки испорченных кадров в протоколе FR, нет; повторная передача испорченных кадров тоже не выполняется. Это делается другими протоколами, более высокого уровня.

Физически подключение к сети Frame Relay осуществляется через синхронный порт по каналу с пропускной способностью не менее 9600 бит/с. Логически пользователь подключается по PVC с назначенным номером DLCI.

Сетевое оборудование, поддерживающее FR, позволяет организовать многопротокольную инкапсуляцию таких протоколов как TCP/IP, X.25, NetBios, IPX и других в кадры FR.

Наиболее широко распространено использование протокола FR, как несущего для TCP/IP. Здесь применяется тот же метод, что и в случае с X.25, только вместо адреса используется идентификатор DLCI. FR – это ещё одна возможность переноса технологии локальных сетей на распределенные сети.

К особым дополнительным возможностям протокола после его расширения относятся:

Мониторинг и сообщение пользователю о динамике PVC;

Многопунктовая адресация;

Симплексное вещание по однонаправленным PVC для организации несимметричной работы.

4.4 Космическая информационно-вычислительная сеть ГТК

Космическая связь, передача информации: между земными пунктами и космическим летательным аппаратами (КЛА); между двумя или несколькими земными пунктами через расположенные в космосе КЛА или искусственные средства (пояс иголок, облако ионизированных частиц и т. п.); между двумя или несколькими КЛА.

В космосе широко используются системы связи самого различного назначения: для передачи телеметрической, телефонной, телеграфной, телевизионной и прочей информации; для передачи сигналов команд и управления КЛА; для проведения траекторных измерений. Наиболее широко в системах космической связи используется радиосвязь.

Основные особенности систем космической связи, отличающие их от наземных:

непрерывное (часто весьма быстрое) изменение положения КЛА;

необходимость знания текущих координат КЛА и наведения приёмных и передающих антенн земного пункта связи на заданный КЛА;

непрерывное изменение частоты принимаемых сигналов из-за Доплера эффекта;

ограниченные и изменяющиеся во времени зоны взаимной видимости земного пункта и КЛА;

ограниченная мощность бортовых радиопередатчиков КЛА;

большая дальность связи и как следствие работа с очень малыми уровнями принимаемых радиосигналов.

Всё это обусловливает создание для космической связи специальных комплексов сложной аппаратуры, включающих наводящиеся антенны больших размеров, приёмные устройства с малым уровнем шумов,

высокоэффективные системы обнаружения, выделения и регистрации радиосигналов.

Необходимость знания текущего положения КЛА требует периодического измерения его координат и вычисления параметров его траектории. Т.о., система космической связи существует, как правило, при совместном действии измерительных средств (система траекторных измерений), вычислительного центра и комплекса управления КЛА. Для радиоканалов космической связи в зависимости от их направления и назначения применяются различные диапазоны частот. Их распределение и порядок использования определяются регламентом радиосвязи.

Связь Земля - КЛА. Связь между земным пунктом и КЛА предназначается для обеспечения двусторонней передачи всех видов необходимой информации. Для связи с дальними КЛА (автоматическими межпланетными станциями - АМС) характерны крайне малые уровни принимаемых радиосигналов и большое время взаимной видимости, поскольку изменение направления земной пункт - КЛА определяется в основном скоростью суточного вращения Земли. Для связи с близкими КЛА (искусственными спутниками Земли - ИСЗ, космическими кораблями - КК, орбитальными космическими станциями и др.) характерны большая скорость изменения направления связи, малое время взаимной видимости, относительно небольшие дальности и соответственно достаточно большие уровни радиосигналов.

Начало радиосвязи с человеком в космосе было положено 12 апреля 1961, когда лётчик-космонавт Ю. А. Гагарин впервые в истории человечества облетел Землю на КК "Восток" и во время полёта поддерживал устойчивую двустороннюю телефонно-телеграфную связь с Землёй на метровых и декаметровых волнах. В последующих полётах КК "Восток" и "Восход" радиосвязь с Землёй совершенствовалась и была с успехом опробована между КК в групповых полётах. Во время полёта КК "Восток-2" в августе 1961 впервые из космоса на Землю передавалось телевизионное изображение

лётчика-космонавта Г. С. Титова. При передаче телевизионного изображения для сужения спектра частот число кадров было уменьшено до 10 в сек. В дальнейшем стали применяться телевизионные системы с обычным стандартом. Наибольшая дальность двусторонней радиосвязи достигнута при полётах АМС к планетам. Например, при полётах к Марсу дальность связи между земным пунктом и АМС достигала 350 млн. км, к Юпитеру - 800-900 млн. км. С целью обеспечения таких дальних связей на АМС обычно используется направленная на Землю антенна.

Связь через ИСЗ. Обычно связь на большие расстояния обеспечивается по радиорелейным линиям прямой видимости, состоящим из двух оконечных и ряда промежуточных пунктов-ретрансляторов, отстоящих друг от друга на расстояние прямой видимости (50-70 км). При установке одного промежуточного ретранслятора на борту ИСЗ с высокой орбитой можно осуществить связь между двумя пунктами, удалёнными один от другого на тысячи км. Максимальная дальность непосредственной связи при этом определяется возможностью видения ИСЗ одновременно с каждого пункта.

Связные ИСЗ могут применяться как в отдельных линиях связи, так и в сетях радиорелейных линий для передачи телевизионных программ, многоканальной телефонии и телеграфии и др. видов информации.

Примером сети, имеющей большое число земных станций, может служить система связи, действующая в Советском Союзе с 1967 г. Для связи могут использоваться ИСЗ, обращающиеся по различным орбитам и на разных высотах.

Основные варианты орбит для связных ИСЗ: круговая стационарная, сильно вытянутая эллиптическая синхронная, средневысокая круговая, низкая круговая.

ИСЗ на стационарной орбите (стационарный ИСЗ) постоянно находится ("висит") над выбранной точкой экватора и обеспечивает круглосуточную связь между земными станциями на широтах меньше 75° в радиусе до 8000 км от точки, над которой расположен спутник, например, ИСЗ "Интелсат". Три

таких ИСЗ, находящихся на равном удалении вдоль экватора, осуществляют связь любых земных станций в пределах указанных широт. Для районов, расположенных на широтах выше 70-75°, наиболее выгодны сильно вытянутые эллиптические синхронные орбиты с апогеем над центром обслуживаемой линии связи и с периодом обращения ИСЗ в половину или целые сутки (см. ИСЗ "Молния"). При надлежащем выборе угла наклонения и места расположения апогея орбиты спутник будет значительную часть суток находиться в пределах видимости из заданного района. Для работы с ИСЗ на стационарной или эллиптической синхронной орбите применяются на земных пунктах связи антенны большого размера, т. к. расстояние ИСЗ - земной пункт превышает 30000 км и мощность принимаемых сигналов мала.

ИСЗ на средневысоких и низких круговых орбитах, например, ИСЗ "Курьер", "Реле", обеспечивают значительно большие мощности принимаемых сигналов. Однако уменьшение высоты полёта сокращает время взаимной видимости спутника и земного пункта связи и приводит в конечном счёте к значительному увеличению количества спутников, требуемых для непрерывной связи. Кроме того, усложняется система слежения и наведения антенн земных станций. При малой высоте полёта непосредственная связь между значительно удалёнными пунктами невозможна и приходится применять систему радиолиний с задержанной ретрансляцией. Однако в этом случае уровни принимаемых сигналов достаточно велики и не нужны большие и дорогостоящие антенные системы, благодаря чему связь с низкими ИСЗ может проводиться даже небольшими подвижными пунктами.

Связной ИСЗ для транзитной передачи сигналов может быть оснащен активным ретранслятором, обеспечивающим также усиление сигналов, или представлять собой пассивный ретранслятор, т. е. отражатель.

Кроме ИСЗ в виде отражателя были предложены и испытаны линии связи с рассеянными отражателями в виде пояса иголок, облака ионизированных частиц. Пассивный ретранслятор может обслуживать радиосеть, состоящую из большого числа линий с различными частотами

радиосигналов, т. к. он отражает или рассеивает энергию многих одновременно приходящих радиосигналов без взаимных помех, например, ИСЗ "Эхо".

В отличие от него, активный ретранслятор может обслуживать сеть связи только с ограниченным числом линий, причём для устранения взаимных помех необходимо применять частотное, временное или кодовое разделение сигналов, поддерживать необходимый их уровень и не допускать перегрузок ретранслятора. Несмотря на это, наибольшее распространение имеют системы с активными ретрансляторами, которые обеспечивают одновременную передачу сообщений по нескольким (до десятка) телевизионным или нескольким тысячам телефонных каналов, например, ИСЗ "Молния", "Интелсат", "Синком".

Для экономичности связи применяют многоканальные линии радиосвязи, что приводит к необходимости увеличения полосы пропускания частот в линии. Широкая полоса требуется также для ретрансляции телевизионных сигналов. С расширением полосы пропускания растет опасность искажения сообщений помехами радиоприёму. Поэтому приём сообщений с допустимыми искажениями - важнейшая задача, решаемая увеличением мощности радиосигналов, выбором частот связи, уменьшением уровня шумов радиоприёмников, применением эффективного кодирования, выбором типа модуляции, способа приёма и обработки радиосигналов при малом отношении сигнал/помеха и др. Например, частоты радиосигналов выбирают в пределах от 1 до 10 Ггц, т. к. на меньших частотах резко растут помехи от шумов космоса, а на больших - от шумов атмосферы; в первых каскадах усилителей радиоприёмников земных станций используют малошумящие квантовые усилители и параметрические усилители, охлаждаемые жидким гелием.

Под многоканальной связью понимают систему электросвязи, обеспечивающую одновременную и независимую передачу сообщений от нескольких отправителей к такому же числу получателей. Многоканальная

связь применяется для передачи по кабельным, радиорелейным и спутниковым линиям связи телефонных и телеграфных сообщений, данных телеметрии и команд телеуправления, телевизионных и факсимильных изображений, информации для ЭВМ, в автоматических системах управления и т. д. Системы Многоканальная связь в сочетании с коммутационными системами явятся важнейшими составными частями единой автоматизированной системы связи.

В основу построения систем многоканальной связи положен принцип уплотнения линий связи. Наиболее распространено частотное уплотнение, при котором каждому каналу связи отводится определённая часть области частот, занимаемой трактом групповой передачи сообщений. В качестве стандартного канала принимается канал тональной частоты (ТЧ), обеспечивающий передачу речевого (телефонного) сообщения с эффективной полосой частот 300-3400 Гц. С учётом защитных промежутков между каналами каждому из них отводится номинальная полоса частот 4 кГц.

При построении многоканальной связи с частотным уплотнением используется метод объединения стандартных каналов в стандартные групповые тракты. Вначале образуют первичный групповой тракт из 12 стандартных каналов, занимающий полосу частот 60-108 кГц. Для этого каждый канал посредством своего индивидуального преобразователя частоты (модулятора) переносится в соответствующую область полосы частот первичного тракта. Из 5 первичных групповых трактов аналогичным образом формируется вторичный и т. д. В практике встречаются системы Многоканальная связь на 12, 60, 120, 180, 300, 600, 900, 1920, 10 800 стандартных каналов. Такой метод не только существенно облегчает реализацию электрических фильтров, но также обеспечивает более широкие возможности унификации оборудования и другие технические преимущества.

Образование групповых трактов обеспечивает также передачу таких видов информации, которые требуют более широкой полосы частот, чем полоса частот стандартного канала: например, при передаче звукового

вещания с полосой частот 50-10 000 Гц объединяются 3 стандартных канала, при передаче черно-белого и цветного телевизионного изображений используется полоса частот всего четвертичного тракта (900 стандартных каналов). Для передачи сообщений, требующих полосы частот более узкой, чем полоса частот стандартного канала ТЧ (например, при уплотнении стандартного канала ТЧ низкоскоростными каналами передачи данных), последний с помощью аппаратуры уплотнения разделяют на 24-48 узкополосных каналов. При этом стандартный канал ТЧ становится уплотнённым каналом связи. Такое уплотнение часто называют вторичным.

Основное достоинство систем многоканальной связи с частотным уплотнением и однополосной модуляцией - экономное использование спектра частот; существенные недостатки - накопление помех, возникающих на промежуточных усилительных пунктах, и, как следствие, сравнительно невысокая помехоустойчивость. От последнего недостатка свободны системы с временным уплотнением и импульсно-кодовой модуляцией. При построении многоканальной связи большой мощности (по числу каналов) намечается тенденция одновременного использования методов частотного и временного уплотнения. Теория и техника многоканальной связи развиваются в направлении повышения помехоустойчивости передачи сообщений и эффективности использования линий связи.

В линии космической связи с пассивным ретранслятором для обеспечения необходимого уровня принимаемого сигнала увеличивают мощность передатчика и размеры антенны земной станции, размеры отражателя ретранслятора или переходят к ретрансляторам с направленным рассеянием энергии на земную станцию, а также сужают полосу пропускания частот в линии и понижают скорость передачи сообщений. Перечисленные меры имеют свои пределы, т. к. увеличивают стоимость оборудования линии связи и её эксплуатации.

В перспективе будут созданы системы передачи телевизионных программ через стационарные ИСЗ непосредственно на телевизоры; при этом

открываются возможности полной телефикации и обеспечения передачи центральных программ в любое место на Земле. С совершенствованием квантовых оптических генераторов (лазеров) становится перспективной оптическая связь, т.к. на оптических волнах можно передать сообщения на сверхдальние расстояния (до десятков световых лет) благодаря очень высокой направленности луча (расхождение луча не более долей сек) при относительно малых размерах излучателей и приемлемой потребляемой мощности. Но узконаправленное излучение и приём оптических волн требуют тщательной стабилизации устройств, ориентации оптических систем на КЛА, сложного вхождения в связь и поддержания её. Наиболее выгодны оптические линии связи между КЛА, находящимися за пределами земной атмосферы, т.к. атмосфера сильно поглощает и рассеивает энергию оптических волн. В настоящее время космическую связь в России обеспечивает ФГУП «Космическая связь» (англ. Russian Satellite Communications Company (RSCC)) - российская государственная компания - национальный оператор спутниковой связи. Предоставляет услуги по всему миру. Прежние названия Союзный узел радиовещания и радиосвязи №9, Государственное предприятие «Космическая связь» (ГПКС).

ФГУП «Космическая связь» обладает самой крупной орбитальной группировкой геостационарных спутников связи и вещания в России и разветвлённой наземной инфраструктурой телепортов и волоконно-оптических линий связи. Услуги компании включают телерадиовещание, телефонную связь, высокоскоростную передачу данных и доступ в интернет, видеоконференцсвязь, создание корпоративных сетей.

Глава 5. Основные программные продукты функциональные автоматизированные рабочие места

5.1 Новые подходы к управлению информацией в среде ЕАИС таможенных органов России

Федеральная таможенная служба ежедневно получает информацию о том, что происходит на территории страны с точки зрения оформления товаров и получения соответствующих платежей, являясь единственным источником сведений о том, что же конкретно в Россию ввезено и что из нее вывезено. Сбор и подсчет статистики внешней торговли - государственная задача, которой ФТС занимается с 1991 г. В конце декабря 1991 г. вышел приказ «О начале опытной эксплуатации автоматизированной системы ведения таможенной статистики России». Этим документом утверждался альбом форм документов и отраслевой руководящий документ ОРД 001-91 «Временные методические рекомендации по технологии сбора, передачи и обработки информации». Уже с января 1993 г. ГНИВЦ приступил к опытной эксплуатации подсистемы ведения таможенной статистики внешней торговли России в полном объеме. Основная нагрузка, связанная с организацией опытной эксплуатации системы, легла на плечи должностных лиц производственных отделов ГНИВЦ и соответствующих подразделений (созданных в этот период) Региональных отделов ГНИВЦ, на базе которых созданы региональные пункты собора информации (РПСИ). В обеспечение деятельности РПСИ была создана ведомственная сеть передачи данных.

Основными функциями РПСИ являлись:

• сбор информации по таможенным органам в закрепленной зоне деятельности;

• ввод, контроль и корректировка информации;

• формирование файлов и передача информации в ГНИВЦ по каналам связи;

• создание и ведение региональной базы данных таможенной информации и НСИ;

• формирование и ведение региональной таможенной статистики;

• осуществление методического и функционального руководства по вопросам автоматизации таможенными органами в закрепленной зоне деятельности;

• внедрение и сопровождение программных средств, системно-техническое обслуживание средств вычислительной техники и т. п.

Создание региональных отделов (РО) ГНИВЦ позволило быстро и на высоком уровне решить очень сложную задачу - не только организовать сбор информации по всей стране, но и обеспечить переход на использование электронных копий таможенных документов. РО ГНИВЦ явились центрами автоматизации в регионах. Централизованное управление позволило избежать появления местнических интересов и организовать создание автоматизированных систем в регионах, построенных с использованием единых принципов.

В течение 1992-1993 гг. шла отработка технологии таможенного оформления грузов и создания электронных копий ТД, технологии сбора и передачи информации на бумажных носителях (с привлечением фельдъегерской службы), а электронных копий ТД и других таможенных документов - с использованием телекоммуникационных каналов связи. В 1993 г. был организован выпуск сигнальных экземпляров первых сборников по таможенной статистике внешней торговли России за первое полугодие 1993 г., а также за третий квартал 1993 г.

Приказ ГТК России от 17.12.1993 г. «О мерах по переходу на промышленную эксплуатацию автоматизированной подсистемы ведения таможенной статистики» № 535 стал отправной вехой в деле полномасштабного функционирования всей инфраструктуры подразделений автоматизации таможенных органов, РПСИ и ГНИВЦ в режиме промышленной эксплуатации первой подсистемы в составе ЕАИС.

Начиная с первого квартала 1994 г. ГНИВЦ в лице своих производственных подразделений, совместно с соответствующими подразделениями таможенных органов, приступил к регулярному формированию данных для публикации квартальных бюллетеней и годовых сборников таможенной статистики внешней торговли России.

На рис. 5.1 показана структура сбора, передачи и хранения информации для ведения таможенной статистики внешней торговли.

Декларации и иные сопроводительные документы подаются в отдел таможенного оформления и контроля таможенного поста или непосредственно таможни. Электронные образы деклараций заносятся во временную базу данных таможенного органа (БДТ) и проверяются. После этого по сети связи они передаются в РПСИ, функционирующий сегодня на базе вычислительного центра Информационно-технической службы (ИТС) РТУ. Кроме этого, из таможен в РПСИ периодически передаются различные формы статистической отчетности. Все это помещается в региональную базу данных (РБД). Подразделения РТУ могут использовать данные РБД своей деятельности. Полученные данные после дополнительной проверки, из РПСИ передаются в ГНИВЦ - в ЦБД. Статистические формы одновременно передаются в ФТС РФ.

Соответствующим образом обработанные и сведенные по определенным методическим принципам данные по всей территории РФ используются для получения различных сводных статистических форм.

Выходная статистическая информация включается в отчетность: срочную, месячную, квартальную и годовую. Полученные отчетные формы передаются в органы государственного управления и используются таможенными органами (ФТС, РТУ и таможнями) для планирования и управления своей деятельностью.

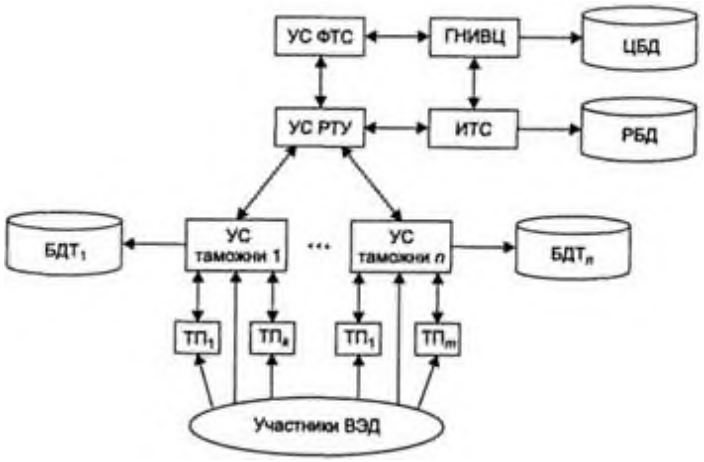

Рис. 5.1 - Укрупненная структура системы сбора информации

Если в начале работы управление таможенной статистики ФТС рассчитывало все формы вручную, то сегодня специалисты уже занимаются разработкой методов повышения точности, способов формирования отчетности, а вся расчетная часть и работа с базами данных возложены на автоматизированную систему. Ежеквартально выпускается сборник статистики ФТС - 150-200 страниц с подробными таблицами по каждому региону, стране назначения, отправления, по всем кодам товаров.

Сегодня многие министерства пользуются статистической информацией, обработанной специализированной информационной системой ФТС. На основании этих сведений о том, что происходит в торговле, принимаются очень серьезные решения в Министерстве экономического развития РФ и Министерстве финансов. Статистика, которую ФТС отправляет в правительство, очень точна.

Информационная система статистики ФТС создана на базе СУБД Oracle с применением средств OLAP, и в ней реализованы все новейшие достижения в области статистики - математико-экономические методы, методы выявления недостоверности данных, перекрестные ссылки, гиперкубы, зеркальная статистика и многое другое. На конференции Oracle в 2001 г. система получила признание как крупнейшая в Европе подобная разработка на базе технологий Oracle.

5.2 Автоматизированная система контроля таможенного транзита АС КТТ-2

Для руководства в работе при реализации Плана мероприятий по внедрению в таможенных органах автоматизированной системы контроля таможенного транзита с учетом взаимодействия с системой NCTS, утвержденного Приказом ФТС России от 17.08.2010 г. № 1530, Письмом ФТС РФ от 01.11.2010 г. № 04-27/53054 направлена Временная технология контроля за перевозками товаров в соответствии с таможенной процедурой таможенной процедурой таможенного транзита с учетом взаимодействия с системой NCTS.

Автоматизированная система контроля таможенного транзита с учетом взаимодействия с системой NCTS (далее - АС КТТ-2) - действующие штатные программные средства, включенные в фонд алгоритмов и программ ФТС России, применяемые для контроля за перевозками товаров в соответствии с таможенной процедурой таможенного транзита, функционирующие с использованием единой системы безопасного и гарантированного обмена данными - транспортной технологической подсистемы ЕАИС таможенных органов (ТТЛ), единого логического информационного ресурса, содержащего сведения о перевозках товаров в соответствии с таможенной процедурой таможенного транзита, и средств защиты информации от несанкционированного доступа.

В информационном взаимодействии в рамках АС КТТ-2 при контроле за перевозками товаров в соответствии с таможенной процедурой таможенного транзита участвуют отделы (отделения) контроля за таможенным транзитом или отделы таможенного оформления и таможенного контроля (ОТОиТК) таможенных постов, ОКТТ таможен, ГНИВЦ.

Программные средства АС КТТ-2 являются единым комплексом программных средств, предназначенным для формирования, шифрования,

передачи, приема, дешифрования и обработки информации о товарах, перемещаемых под таможенным контролем, в режиме времени, близком к реальному.

Для целей совершения таможенных операций и таможенного контроля товаров, перевозимых в соответствии с таможенной процедурой таможенного транзита, в таможенных органах на уровнях таможенного поста, таможни используется КПС «Транзитные операции». Для целей проведения анализа информации, получения статистических отчетов о состоянии дел в области перевозок товаров в соответствии с таможенной процедурой таможенного транзита на уровнях РТУ и ФТС России используется КПС «Статистика транзитных операций - АС КТТ-2».

Контроль перевозок товаров в соответствии с таможенной процедурой таможенного транзита организуется путем:

а) учета товаров в таможенном органе отправления;

б) загрузки электронного сообщения о транзитной перевозке (ЭКТД) при регистрации транзитной декларации и выпуске товаров в соответствии с таможенной процедурой таможенного транзита в центральную базу данных единой автоматизированной информационной системы (ЦБД ЕАИС) таможенных органов;

в) учета товаров в таможенном органе назначения;

г) загрузки информации о завершении таможенной процедуры таможенного транзита в ЦБД ЕАИС таможенных органов;

д) учета товаров в таможенном органе, в регионе деятельности которого производятся грузовые операции, изменение средств идентификации или срока таможенного транзита;

е) загрузки информации о произведенных грузовых и иных операциях, измененных средствах идентификации или сроке таможенного транзита в ЦБД ЕАИС таможенных органов;

ж) загрузки информации о возбужденных делах об административных правонарушениях в области таможенного дела, взысканных таможенных пошлинах, налогах и штрафах в ЦБД ЕАИС таможенных органов;

з) снятия ЭКТД с контроля.

В АС КТТ-2 в автоматическом режиме осуществляется также сбор информации о перевозках товаров под таможенным контролем в едином логическом информационном ресурсе на уровне РТУ и ГНИВЦ в режиме времени, близком к реальному, в виде электронных сообщений XML-формата, содержащих ЭКТД.

В едином логическом информационном ресурсе АС КТТ-2 ЭКТД снимаются с контроля после осуществления ОКТТ таможен отправления и назначения действий:

• надлежащего завершения таможенного транзита (снятие с контроля в автоматическом режиме);

• поступления в таможенный орган назначения товаров, отличных от заявленных к таможенному транзиту в таможенном органе отправления, при условии указания в ЭКТД сведений о фактически поступивших товарах, номеров определения (протокола) об АП и статьи КоАП РФ, по которой возбуждено дело об АП;

• поступления товаров с нарушением установленного срока таможенного транзита либо с нарушением средств идентификации при условии указания в ЭКТД сведений о номерах определения (протокола) об АП и статьи КоАП РФ, по которой возбуждено дело об АП;

• частичной утраты товаров при условии указания в ЭКТД сведений о фактически поступивших товарах, номерах определения (протокола) об АП, статьи КоАП РФ, по которой возбуждено дело об АП, и суммы взысканных таможенных пошлин, налогов;

• недоставки товаров при условии указания в ЭКТД сведений о номерах (определения) протокола об АП, статьи КоАП РФ, по которой возбуждено дело об АП, и суммы взысканных таможенных пошлин, налогов;

• утраты товаров в случае аварии или действия непреодолимой силы при условии указания в ЭКТД сведений о неутраченных товарах, номере и дате акта об аварии или действии непреодолимой силы.

С помощью КПС «Статистика транзитных операций - АС КТТ-2» на уровне ОКТТ РТУ и ОКТТ ГУОТОиТК ФТС России осуществляется анализ информации о перевозках товаров в соответствии с таможенной процедурой таможенного транзита.

ОКТТ РТУ, таможен отправления и назначения организуют проверку фактов недоставления товаров в таможенные органы назначения и принимают в соответствии с законодательством Российской Федерации необходимые меры в случае обнаружения признаков административных правонарушений в области таможенного дела.

5.3 Автоматизированная система пограничного пункта пропуска

Областью применения автоматизированной системы «Пограничный пункт пропуска» (АС «ПП») является процесс регистрации прибытия товаров и транспортных средств на таможенную территорию Российской Федерации, регистрации убытия товаров и транспортных средств за пределы Российской Федерации, построение аналитических отчетов на основании данных сообщений о прибытии/убытии товаров и транспортных средств. Программное обеспечение АС «ПП» предназначено для использования на пограничных пунктах пропуска различного назначения.

АС «ПП» предоставляет пользователю автоматизированные средства выполнения следующих действий (рис. 5.2, 5.3):

• формирование сообщений о прибытии товаров и транспортных средств на таможенную территорию Российской Федерации;

• формирование сообщений об убытии товаров и транспортных средств с таможенной территории Таможенного союза;

• запрос и просмотр сведений предварительного информирования, регистрация сообщений о прибытии товаров и транспортных средств на основе полученной информации;

• запрос и просмотр сведений, содержащихся в электронных копиях книжек МДП, регистрация сообщений о прибытии товаров и транспортных средств на основе полученной информации;

Рис. 5.2 - Схема развернутого на уровне пункта пропуска АС «ПП»

• запрос и просмотр сведений предварительной информации в части сведений, предоставляемых КЕС, о прибытии товаров и транспортных средств на основе полученной информации;

• запрос и просмотр ТД иностранных государств, регистрация сообщений о прибытии товаров и транспортных средств на основе полученной информации;

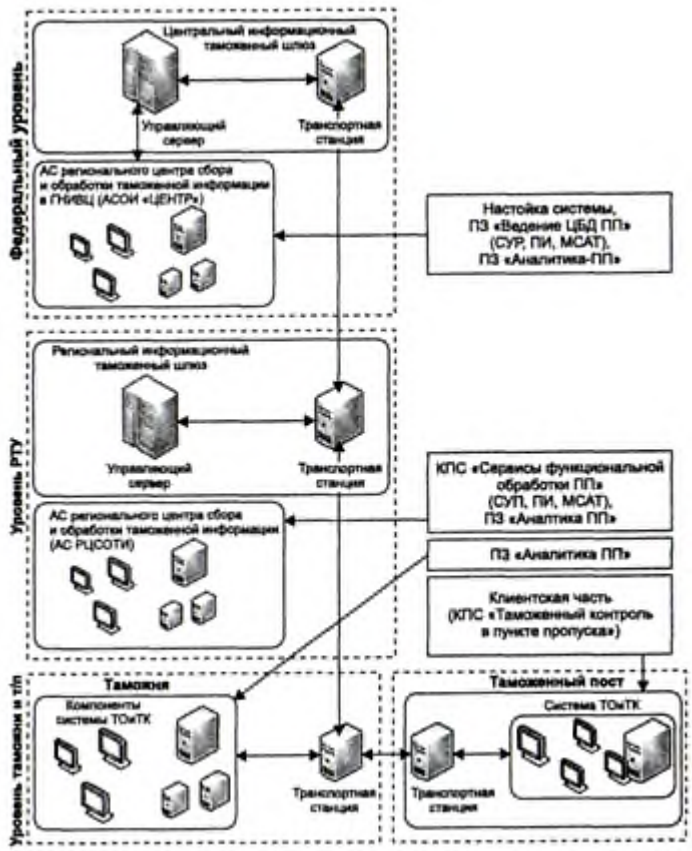

Рис. 5.3. Взаимодействие АС ПП и транспортной системы

• запрос и просмотр информации, содержащейся в российских экспортных ТД, регистрация сообщений об убытии товаров и транспортных средств на основе полученной информации;

• запрос и просмотр информации, содержащейся в электронных копиях коносаментов, регистрация сообщений со сведениями о документах на основе полученной информации;

• проверка сформированного сообщения о прибытии товаров и транспортных средств на соответствие профилям риска путем формирования запроса к ПЗ «Сервисы выявления рисков» (в части автомобильного пункта пропуска);

• таможенные операции с товарами по заявлению;

• формирование и просмотр отчетности по зарегистрированным сообщениям о прибытии и убытии товаров и транспортных средств;

• формирование журнала учета результатов применения мер по минимизации рисков (в части автомобильного пункта пропуска);

• формирование аналитической отчетности о прибытии/убытии товаров и транспортных средств на основании данных БД уровня РТУ или ГНИВЦ;

• идентификация и разграничение прав доступа пользователей.

По функциональным особенностям применения компонент, входящих в состав АС «ПП», комплекс делится на уровни использования (применения), представленные в табл. 5.1.

Клиентская часть АС «ПП» уровня пункта пропуска разделяется на две: пользовательскую и административную.

В клиентской части АС «ПП» для каждого пункта пропуска реализованы следующие принципы организации работы с данными:

• использование единого места хранения временной информации, вводимой должностными лицами пункта пропуска на этапе оформления прибытия/убытия товаров и транспортных средств;

• предоставление возможности работы с введенными временными данными нескольким должностным лицам Пункта пропуска в соответствии с назначенными им правами;

• использование единого места хранения необходимых справочников НСИ;

• использование единого для всего пункта пропуска механизма формирования номеров регистрируемых сообщений, позволяющего обеспечить гарантированную уникальность присвоенных сообщениям номеров.

Таблица 5.1 - Уровни использования АС ПП

Уровень применения	Используемые компоненты (модули) АС «ПП»
Пункт пропуска	Клиентская часть (АС «Таможенный контроль в пункте пропуска»)
Таможня	ПЗ «Аналитика — ПП»
РТУ	АС «Сервисы функциональной обработки — ПП», ПЗ «Аналитика — ПП»
ГНИВЦ	ПЗ «Ведение ЦБД ПП», ПЗ «Аналитика — ПП»

С точки зрения практической реализации данного подхода на каждом пункте пропуска развертывается одна рабочая станция с сетевыми БД (под управлением СУБД FireBird), используемая для формирования уникальных номеров сообщений, хранения временной информации о прибытии (убытии), и централизованного хранения части справочников НСИ единой для всего таможенного поста, а также требуемое количество клиентских рабочих станций, с развернутыми на них пользовательскими и/или административными рабочими местами.

Кроме того, для временного хранения вводимой информации в таможенном органе до отправки на вышестоящий иерархический уровень используется так называемый сетевой кэш данных - БД, входящая в состав установочного комплекта и размещаемая на той же рабочей станции, где развернуты сетевые БД.

АС «ПП» обеспечивает выполнение следующих функций:

• регистрацию прибытия/убытия товаров и транспортных средств на/с таможенной территории Российской Федерации;

• доступ к электронным копиям российских ТД;

• доступ к электронным копиям транзитных деклараций, коносаментов;

• доступ к данным предварительного информирования;

• проверку книжек МДП по технологии «TIR Query»;

• проверку сообщений о прибытии товаров и транспортных средств на соответствие профилям риска;

• таможенные операции с товарами по заявлению;

• выгрузку данных электронного журнала прибытия во внешний формат транзитной декларации (формат dbf);

• формирование отчетности о прибытии и убытии товаров и транспортных средств, а также по результатам применения мер по минимизации рисков;

• формирование аналитической отчетности о прибытии и убытку в разрезе транспортных средств или товаров;

• администрирование АС «ПП» каждой обработки данных. Кроме того, существуют общесистемные операции, не связанные с прикладной функцией АС «ПП» (вход в систему, выполнение настроек пользовательской части, работа со сменами, завершение сеанса работы).

Для удобства восприятия пользователем часть экранных форм АС «ПП» и выполняемых в них действий сгруппированы в так называемые «режимы».

Функция регистрации прибытия заключается в формировании сообщений о прибытии транспортных средств и товарных партий на таможенную территорию Российской Федерации. Функции регистрации прибытия соответствует режим АС «ПП» «Прибытие».

Функция регистрации убытия заключается в формировании сообщений об убытии транспортных средств и товарных партий с таможенной территории Таможенного союза. Функции регистрации убытия соответствует режим АС «ПП» «Убытие».

Доступ к электронным копиям российских ТД и ТД. Функция запроса российских ТД и транзитных деклараций предназначена для доступа должностных лиц таможенных органов, расположенных в пунктах пропуска через государственную границу Российской Федерации, к информации, содержащейся в электронных копиях российских ТД и электронных копиях транзитных деклараций, с целью ускорения и упрощения процесса

регистрации убытия товаров и транспортных средств с таможенной территории Таможенного союза посредством заполнения электронного журнала убытия на основе данных из электронных копий грузовых и транзитных деклараций.

Данные электронных копий экспортных ТД запрашиваются посредством формирования в АС «ПП» запроса к специализированному разделу ЦБД ТД ЕАИС таможенных органов. На основе полученного ответа автоматически формируется сообщение об убытии товаров и транспортных средств с таможенной территории Таможенного союза. В дальнейшем данное сообщение об убытии может быть отредактировано пользователем.

Данные электронных копий ТД запрашиваются посредством формирования в АС «ПП» запроса к базе данных автоматизированной системы контроля таможенного транзита с учетом взаимодействия с системой NCTS (далее - АС КТТ-2). На основе полученного ответа также автоматически формируется сообщение об убытии товаров и транспортных

средств с таможенной территории Таможенного союза. В дальнейшем данное сообщение об убытии может быть отредактировано пользователем.

Доступ к электронным копиям коносаментов. Функция приема данных электронных копий коносаментов предназначена для доступа должностных лиц таможенных органов, расположенных в пунктах пропуска через государственную границу Российской Федерации, к информации, содержащейся в электронных копиях коносаментов, с целью ускорения и упрощения процесса регистрации сведений коносаментов посредством заполнения электронного журнала регистрации судов на основе данных из электронных копий коносаментов.

Данные электронных копий коносаментов предоставляются от стивидоров в виде XML-файлов. На основе полученного файла автоматически формируется сообщение о регистрации сведений коносаментов. В дальнейшем данное сообщение может быть отредактировано пользователем.

Доступ к данным предварительного информирования. Функция приема данных предварительного информирования предназначена для повышения оперативности регистрации прибытия товаров и транспортных средств за счет доступа должностного лица таможенных органов к данным предварительного информирования и использования этих данных при регистрации прибытия товаров и транспортных средств на территорию Российской Федерации.

Данные предварительного информирования запрашиваются посредством формирования в АС «ПП» запроса к КПС «Управление предварительным информированием». На основе полученного ответа автоматически формируется сообщение о прибытии товаров и транспортных средств на таможенной территории Таможенного союза. В дальнейшем данное сообщение о прибытии может быть отредактировано пользователем.

Таможенные операции с товарами по заявлению. Заключаются в предоставлении должностными лицами таможенных органов возможности просматривать и печатать в виде заявления сообщения о прибытии партии товаров, в отношении которых ответственным должностным лицом принято решение «Оформление по заявлению».

Проверка книжек МДП по технологии «TIR Query». Заключается в предоставлении должностным лицам таможенных органов возможности запрашивать сведения о книжках МДП из базы данных МСАТ в режиме времени, близком к реальному. Запросы к базе данных МСАТ формируются автоматически при сохранении сообщения о прибытии в части информации о транспортном средстве (при наличии заполненных полей, содержащих информацию о номере книжки МДП и номере заполненного листа). Функции проверки книжек МДП соответствует режим АС «ПП» «Прибытие».

Проверка сообщений о прибытии товаров и транспортных средств на соответствие профилям риска. Функция заключается в предоставлении должностным лицам таможенных органов возможности проверить сформированное сообщение о прибытии товаров и транспортных средств на

соответствие профилям риска путем формирования запроса к ПЗ «Сервисы выявления рисков».

Функции проверки сообщений о прибытии товаров и транспортных средств на соответствие профилям риска соответствует режим АС «ПП» «Прибытие».

Выгрузка данных электронного журнала прибытия во внешний формат транзитной декларации (формат dbf). Заключается в формировании выгрузки данных электронного журнала прибытия во внешний формат транзитной декларации (формат dbf) для последующей загрузки данных в комплекс программных средств автоматизированного контроля за таможенным транзитом товаров (далее - КПС «Транзит», АС КТТ). Функции выгрузки данных соответствует режим АС «ПП» «Прибытие».

Формирование отчетности о прибытии и убытии товаров и транспортных средств. Функция предназначена для получения отчетных данных по результатам деятельности пограничных пунктов пропуска в виде журналов регистрации сообщений о прибытии и убытии товаров и транспортных средств и заключается в формировании и просмотре печатных форм отчетов. Функции формирования отчетности соответствует режим АС «ПП» «Отчеты».

Формирование отчетности по результатам применения мер по минимизации рисков. Функция предназначена для получения отчетных данных по результатам деятельности пограничных пунктов пропуска в виде журнала учета результатов применения мер по минимизации рисков и заключается в формировании и просмотре печатных форм отчета. Функции формирования отчетности соответствует режим АС «ПП» «Отчеты».

Формирование аналитической отчетности о прибытии и убытии товаров и транспортных средств. Функция предназначена для получения аналитических отчетных данных по результатам деятельности пограничных пунктов пропуска в виде журналов учета товаров о прибытии и убытии товаров и транспортных средств на основании данных БД уровня РТУ или

ГНИВЦ и заключается в формировании и просмотре печатных форм аналитических отчетов. Функции формирования аналитической отчетности соответствует ПЗ «Аналитика-ПП».

Администрирование АС «ПП». Функция администрирования реализует следующие механизмы:

• установка прав доступа пользователей к функциональным возможностям и информационным ресурсам АС «ПП»;

• хранение сведений о пользователях АС «ПП»;

• авторизация пользователей АС «ПП»;

• исключение несанкционированного доступа к АС «ПП» лиц, не имеющих соответствующих полномочий;

• обеспечение единой точки регистрации рабочих станций пользователей АС «ПП»;

• обеспечение единства настроек рабочих станций пользователей АС «ПП» уровня таможенного поста/пункта пропуска;

• обеспечение единой точки загрузки БД НСИ ЕАИС таможенных органов;

• просмотр XML-сообщений;

• просмотр лога сервера приложений (АС «Сервисы функциональной обработки»);

• просмотр журнала действий пользователей.

Функции администрирования соответствует предоставляемый набор доступных операций в административной части АС «ПП».

5.4 Единые автоматизированные системы таможенного оформления и контроля.

5.4.1 АИСТ-РТ21

Переход управления и организации таможенного дела от многочисленных разрозненных программных средств к разработке и внедрению комплексных средств автоматизации таможенной деятельности позволяет значительно повысить эффективность использования информационного пространства, людских, финансовых и технических ресурсов. Примером такого комплексного средства автоматизации является АИСТ-РТ21 (рис. 5.4).

Гибкость системы АИСТ-РТ21 обеспечивает универсальный механизм рассылки правовой и справочной информации. Справочная информация, которая вводится в систему на верхнем уровне управления, на каждом промежуточном уровне конкретизируется и дополняется. Наконец информация опускается на уровень практической работы, решая конкретные задачи организаций. Именно таким путем ставки таможенных платежей, определяемые ФТС России, становятся рабочим инструментом инспектора таможни, осуществляющего фактическое оформление груза.

В процессе практической работы накапливаются значительные объемы оперативной информации. Доступность этой информации для управляющих уровней является одним из факторов успешного планирования дальнейшей работы. Оперативная информация, например данные о регистрации участников ВЭД, поступает с подчиненного таможенного поста на таможню, где подвергается всестороннему контролю.

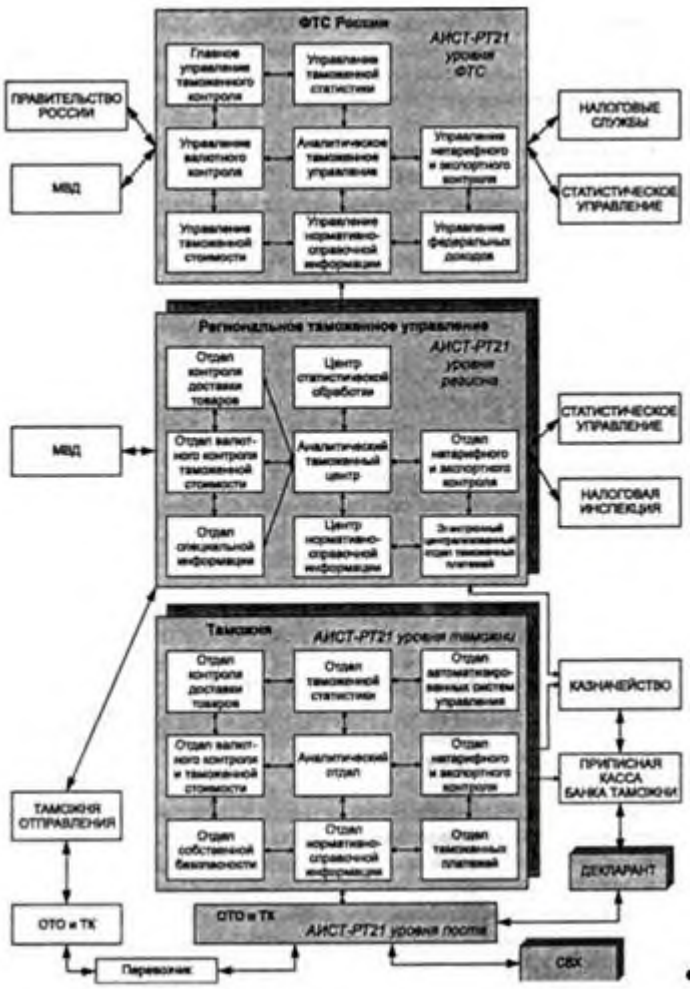

Рис. 5.4 - Структурная схема применения комплексного средства автоматизации таможенной деятельности «АИСТ-РТ21»

Затем информация передается в региональное таможенное управление, где служит предметом учета и анализа деятельности поста и таможни. В то же время подчиненные уровни системы не имеют прямого доступа к оперативной и аналитической информации, собранной и структурированной на руководящих уровнях. Весь информационный обмен в рамках одного горизонтального уровня системы производится только через управляющий уровень.

Сегодня указанная система охватывает все стороны деятельности таможенного поста (рис. 5.4, 5.5). Важным в системе является возможность контроля руководством таможенного поста процесса осуществления таможенных операций и действия подчиненных должностных лиц.

Для пресечения возможной утечки информации в организации и предотвращения случаев злоупотребления служебным положением АИСТ-РТ21 предусматривает строгое распределение полномочий и прав пользователей. Система позволяет назначать и контролировать права как отдельных пользователей, так и пользовательских групп на выполнение конкретных служебных операций. Она регистрирует все действия пользователей, и эта информация сохраняется системой. Электронные протоколы работы пользователей в системе дают возможность осуществлять контроль за всеми действиями каждого исполнителя.

Помимо общего распределения полномочий среди должностных лиц организации система позволяет вводить оперативные запреты на выполнение тех или иных действий. Например, руководитель таможни на основе полученной им информации устанавливает ограничения на оформление груза при некоторых условиях. Такими условиями могут быть принадлежность товара к определенной категории, перевозка или декларирование груза определенной компании и др. И как только установленное ограничение срабатывает, система автоматически приостанавливает оформление, а исполнитель получает инструкцию незамедлительно обратиться к руководству, принимающему решение о дальнейшей судьбе груза.

Любая ведомственная информационная система должна быть хорошо защищена от нежелательных внешних воздействий или злонамеренных попыток проникновения. АИСТ-РТ21 гарантирует несколько уровней защиты:

• уровень операционной системы;

• уровень системы управления базами данных;

• защита рабочих мест пользователей;

• обеспечение механизма безопасности при взаимодействии со сторонними организациями.

Подключение внешних информационных комплексов к любому уровню системы осуществляется через специально выделенные коммуникационные серверы. Достаточно выработать взаимно удобные протоколы обмена

информацией, и система становится дружелюбной и открытой в любых внешних контактах. При этом обеспечивается быстрый и эффективный информационный обмен в полном соответствии с заранее определенными протоколами.

В процессе прохождения таможенных платежей в реальном времени система поддерживает электронное взаимодействие декларанта с банком, используя подсистему «банк-клиент» и электронные чехлы и карты, обеспечивая оперативную и защищенную передачу платежной информации. Кроме того, она поддерживает электронное взаимодействие таможни с банком, обеспечивая передачу платежных поручений клиентов таможни, поручений на перечисление средств в бюджет и банковских выписок.

Применение средств электронной идентификации автомобильных перевозчиков приводит к усилению их правовой защищенности, предупреждению возможных при доставке товаров нарушений таможенных правил, ускорению процесса выпуска порожнего автотранспорта за границу, сокращению времени розыскных мероприятий при недоставке товаров.

Таким образом, система предназначена для унификации и ускорения процесса осуществления таможенных операций, повышения качества таможенного и таможенно-банковского контроля, ускорения поступления денежных средств в бюджет Российской Федерации, минимизации затрат таможенных органов на осуществление таможенных операций.

Таким образом, система АИСТ-РТ21 является не только системой автоматизации таможенной деятельности, но и универсальной системой, которая может быть использована и в государственных органах, и в корпорациях. Эффективное управление; строгий учет и контроль; гарантированная защищенность и абсолютная надежность; экономия людских, финансовых и технических ресурсов; гибкость и способность к расширению при очевидном удобстве и простоте в эксплуатации стали основными принципами построения данной системы.

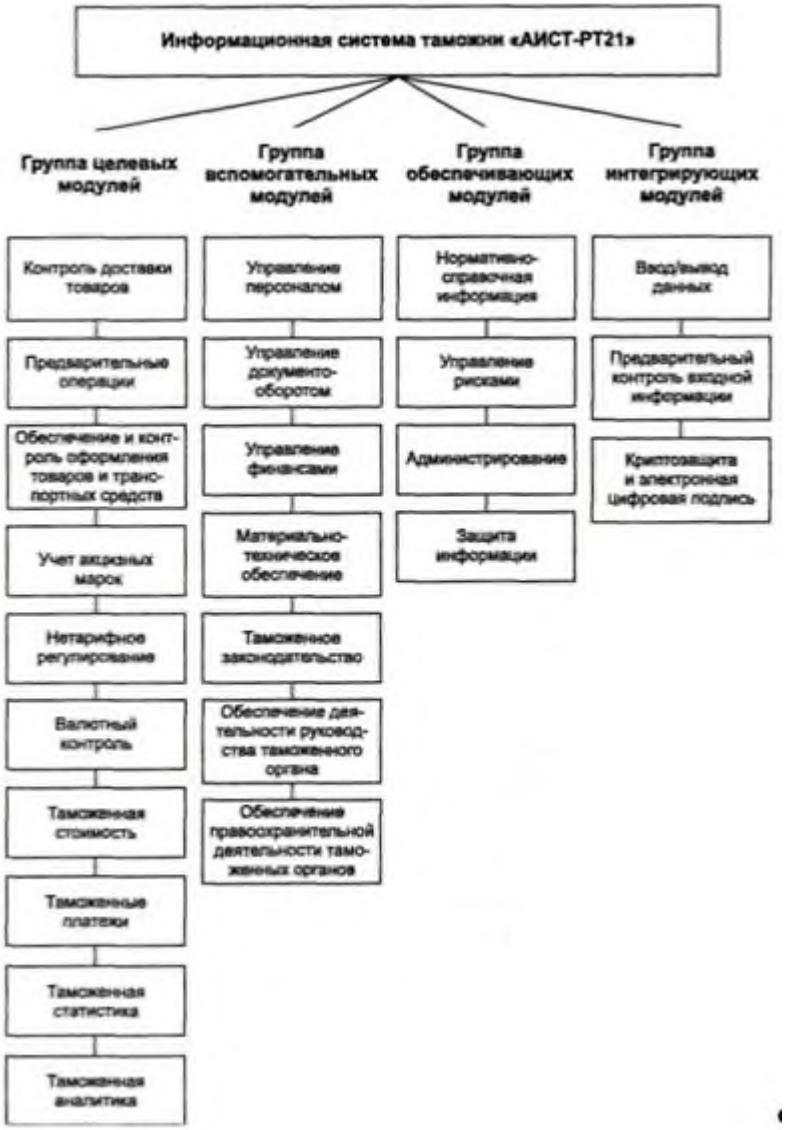

Рис. 5.5 - Основные информационные модели «АИСТ-РТ21»

Система АИСТ-РТ21 обеспечивает все основные технологические процессы таможни, приводя информационную составляющую работы таможенных органов к порядку и единообразию. В современном понимании роли информационных технологий это означает структуризацию работы организации в целом. Вся сложность и многообразие технологических процессов такой крупной организации, как таможня, все возможные нюансы законодательной базы должны быть продуманы, учтены и оптимизированы один раз - при постановке задачи и создании информационной системы. Благодаря использованию автоматизированной системы АИСТ-РТ21 в

процессе практической работы «разночтений» в понимании законов уже не возникает.

АИСТ-РТ21 является распределенной системой, объединяющей таможенные органы любого ранга, потенциально размещенные на сколь угодно протяженной территории. Система обеспечивает защиту и безопасность ведомственной информации, связь таможни со сторонними организациями-декларантами, перевозчиками, складами, брокерами.

Несмотря на значительную территориальную удаленность таможенных органов - постов, таможен друг от друга, система АИСТ-РТ21 организует для всех без исключения подразделений работу в режиме «виртуального офиса», т.е. делает работу подчиненных органов полностью «прозрачной» для вышестоящих. Система АИСТ-РТ21 предоставляет руководству таможен и таможенных управлений возможность мониторинга в режиме реального времени хода оформления грузов, процесса контроля доставки товаров, перечисления средств в бюджет и других важных процессов. С другой стороны, по информационным каналам система обеспечивает подчиненные органы четкой, своевременной и полной руководящей информацией, единообразной и однозначной нормативной и справочной информацией.

5.4.2 «АИСТМ»

Уникальные возможности системы АИСТ-РТ21 определили ее достаточно высокую требовательность к уровню аппаратного обеспечения, которая не может быть удовлетворена в менее крупных таможенных органах в связи с низким уровнем финансирования. Это обусловило необходимость (параллельно с модернизацией АИСТ-РТ21) выпуска новой «облегченной» версии, получившей название КАСТО «АИСТ-М», менее требовательной к аппаратному обеспечению и, как следствие, более дешевой.

Система «АИСТ-М» (рис. 5.6) представляет собой комплексную, взаимоувязанную законченную задачу автоматизации осуществления таможенных операций и получения всевозможных форм отчетности. Система охватывает все уровни сбора информации таможенные посты (ТП), таможни, региональные управления.

В целях реализации приказов ГТК России от 31.01.2003 г. № 80, от 04.02.2003 г. № 99 «Об утверждении Порядка аттестации комплексных автоматизированных систем таможенного оформления» автоматизированная информационная система таможни (АИСТ-М) в марте 2003 г. комиссией ГТК России принята в опытную эксплуатацию.

Система ориентирована на существующий компьютерный парк и российские линии связи. При этом система может быть сконфигурирована таким образом, чтобы обеспечить максимальную централизацию и работу в режиме on-line.

«АИСТ-М» создана для осуществления информационной поддержки принятия решений должностными лицами таможенных органов Российской Федерации в ходе осуществления таможенного оформления и таможенного контроля товаров и транспортных средств, перемещаемых через таможенную границу, посредством обработки электронных копий документов (в том числе таможенных), необходимых для таможенных целей, на основе анализа информации, содержащейся в базах данных Единой автоматизированной информационной системы (ЕАИС) ФТС России. «АИСТ-М» предназначается для:

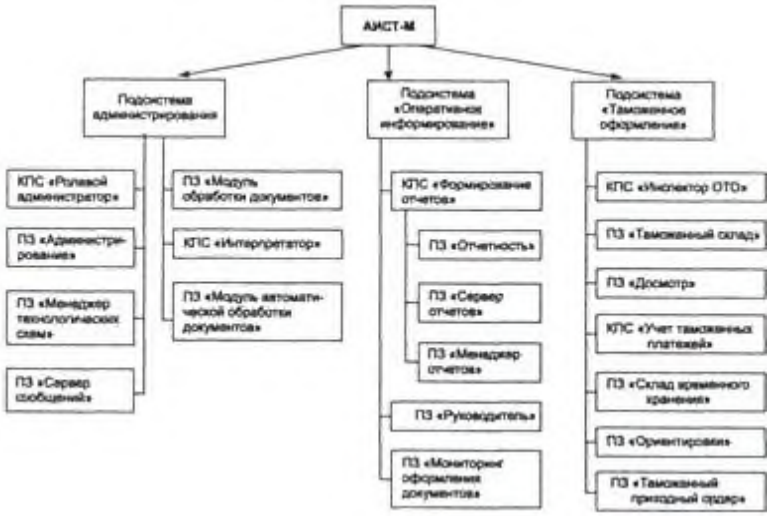

Рис. 5.6 - Состав АИСТ-М

• автоматизации управления процессом документального таможенного оформления и таможенного контроля;

• контроля движения документов в процессе таможенного оформления, а также аудита действий должностных лиц таможенных органов;

• обеспечения прозрачности процесса таможенного оформления для руководящего звена, а также для участников внешнеэкономической деятельности;

• обеспечения форматно-логического контроля электронных копий документов, применяемых в таможенной деятельности;

• обеспечения контроля, в том числе вторичного, правильности начисления и своевременности уплаты таможенных платежей;

• обеспечения гибкого подключения различных информационно-справочных баз данных;

• обеспечения информационной поддержки участников внешнеэкономической деятельности в части документального таможенного оформления товаров и транспортных средств.

АС «АИСТ-М» реализует следующие функции:

• управление и визуальное представление хода документального таможенного оформления товаров и транспортных средств;

• прием и регистрацию электронных копий документов (в том числе таможенных), необходимых для таможенных целей;

• форматно-логический контроль электронных копий документов (в том числе таможенных), необходимых для таможенных целей;

• автоматизированный контроль соблюдения требований и условий заявленного таможенного режима;

• автоматизированный контроль поступлений платежей участников ВЭД;

• контроль наличия задолженности уплаты таможенных платежей;

• контроль правильности начисления и своевременной уплаты таможенных платежей;

• автоматизированный контроль сроков таможенного оформления и сроков хранения грузов на таможенном складе, учрежденном таможенным органом;

• автоматическое информирование руководства таможенного органа и участников ВЭД о ходе оформления ГТД;

• автоматизированный контроль выпуска определенных товаров согласно акту таможенного досмотра;

• формирование и актуализация нормативно-справочной информации (НСИ) на уровне таможенного поста и таможни;

• формирование произвольных аналитических отчетов;

• разграничение доступа к данным и операциям.

«АИСТ-М» состоит из трех подсистем: АПС «Администрирование»; АПС «Оперативное информирование»; АПС «Таможенное оформление»

АПС «Администрирование» предназначается для организации управления процессом документального таможенного оформления и таможенного контроля и включает в себя КПС «Ролевой администратор», ПЗ «Администрирование», ПЗ «Менеджер технологических схем»/«Маршрутизатор», ПЗ «Сервер сообщений».

КПС «Ролевой администратор» - комплекс программных средств, позволяющий работать с документами как объектами технологической схемы (документооборота) вне зависимости от их внутреннего содержания. Должностное лицо, непосредственно исполняющее обязанности «Ролевого администратора», не производит обработки содержимого документа, а лишь выполняет функцию управления документами, их взаимосвязью и безопасностью (ПЗ «Центр управления» и «Маршрутизатор»). Непосредственная обработка документов, согласно принятой в таможенном органе технологии таможенного оформления, производится пользователями с помощью рабочего клиента «АИСТ-М» «Клиент отчетов» с использованием КПС «Инспектор ОТО», ПЗ «Досмотр», ПЗ «Таможенный склад», а также иных специализированных функциональных программных средств, имеющихся в данном таможенном органе. «Ролевой администратор» построен на архитектуре «Клиент-Сервер» с использованием СУБД Interbase.

Все команды по обработке файлов прописываются в схеме документооборота, как правило, один раз.

Схема документооборота далее может изменяться в зависимости от конкретных условий.

Группа действий над документом называется «переходом» (т. е. переход документа из одного состояния в другое).

Такая группа действий может быть определена в виде сценария.

Если над документом не выполнятся никаких действий, то в этом случае будет просто происходить смена состояния документа (этапа) с сохранением прежнего содержимого документа.

Администратору в большинстве случаев не обязательно создавать схему документооборота с нуля, в большинстве случаев под существующий технологический процесс может быть адаптирована одна из типовых схем, которая импортируется извне.

От администратора в таком случае требуется понимание структуры схемы и умение приспосабливать такую типовую схему к конкретным условиям, включая изменения скриптов и создание новых этапов и переходов.

Глава 6. Теория и практика обеспечения информационной безопасности в ЕАИС

6.1 Понятие и структура информационной безопасности

В силу специфики деятельности таможенных органов Российской Федерации обеспечение их информационной безопасности оказывает влияние на защищенность национальных интересов Российской Федерации в различных сферах жизнедеятельности общества и государства.

В сфере внешней политики Российской Федерации объектами обеспечения информационной безопасности таможенных органов Российской Федерации являются информационные ресурсы представительств таможенной службы Российской Федерации за рубежом.

В сфере внутренней политики Российской Федерации объектами обеспечения информационной безопасности таможенных органов Российской Федерации являются:

• конституционные права и свободы человека и гражданина, являющегося должностным лицом или работником таможенного органа Российской Федерации;

• персональные данные физических лиц - субъектов персональных данных;

• специальная категория персональных данных (состояние здоровья) должностных лиц, работников и пенсионеров таможенных органов Российской Федерации, членов их семей при использовании информационных систем в лечебно-санаторных учреждениях ФТС России (Центральной поликлиники ФТС России, Центральном клиническом госпитале ФТС России и др.);

• открытые информационные ресурсы таможенных органов Российской Федерации (официальный сайт ФТС России, автоматизированная система «Таможенная статистика внешней торгов ли» и др.).

В сфере экономики Российской Федерации объектами обеспечения информационной безопасности таможенных органов Российской Федерации являются:

• любая информация, полученная таможенными органами Российской Федерации в соответствии с таможенным законодательством Таможенного союза и Российской Федерации, иными правовыми актами Российской Федерации и/или составляющая государственную, коммерческую, банковскую, налоговую или иную охраняемую законом тайну и другую конфиденциальную информацию;

• документы и сведения, используемые для статистических целей;

• права правообладателей на объекты интеллектуальной собственности при совершении таможенных операций.

В правоохранительной и судебной сферах объектами обеспечения информационной безопасности таможенных органов Российской Федерации являются информационные ресурсы подразделений, реализующих правоохранительные функции, содержащие специальные сведения и оперативные данные служебного характера.

В сфере общегосударственных информационных и телекоммуникационных систем объектами обеспечения информационной безопасности таможенных органов Российской Федерации являются (рис. 6.1):

• объекты информатизации таможенных органов Российской Феде рации (включая средства вычислительной техники, информационно-вычислительные комплексы, средства звукозаписи и звукоусиления, звукосопровождения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов, сети и системы, операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение, автоматизированные системы управления, системы связи и передачи данных, осуществляющие прием, обработку хранение и передачу информации ограниченного доступа, их

информативные физические поля), предназначенные для обработки сведений, отнесенных к государственной тайне;

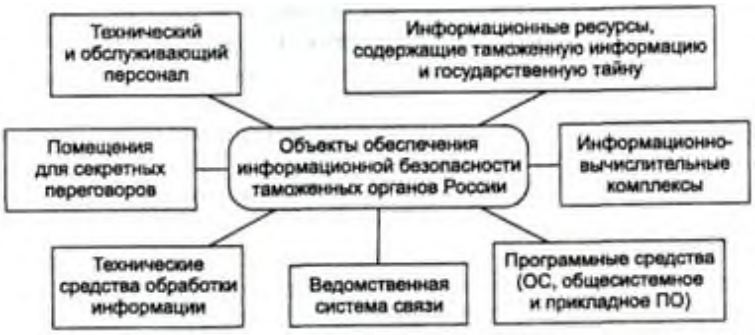

Рис. 6.1 - Объекты обеспечения информационной безопасности

• технические средства и системы, обрабатывающие открытую ин формацию, но размещенные в помещениях, в которых обрабатывается информация ограниченного доступа;

• помещения, предназначенные для ведения закрытых переговоров, а также переговоров, в ходе которых оглашаются сведения ограниченного доступа.

• автоматизированные информационные системы таможенных органов Российской Федерации, включая ведомственную интегрированную телекоммуникационную сеть и локальные вычислительные сети таможенных органов Российской Федерации, а также средства вычислительной техники и программного обеспечения.

В области науки и техники объектами обеспечения информационной безопасности таможенных органов Российской Федерации являются:

• результаты проведенных по заказу таможенных органов Российской Федерации фундаментальных, поисковых и прикладных научных исследований, потенциально важных для научно-технического, технологического и социально-экономического развития страны, включая сведения, утрата которых может нанести ущерб национальным интересам и престижу Российской Федерации;

• открытия, незапатентованные технологии, промышленные образцы, полезные модели и экспериментальное оборудование, разработанные или полученные в интересах таможенных органов Российской Федерации;

• научно-технические кадры таможенных органов Российской Федерации и система их подготовки.

Обеспечение информационной безопасности указанных объектов создает условия для надежного функционирования таможенных органов Российской Федерации, что является жизненно важным условием обеспечения экономической безопасности государства.

Анализ состояния информационной безопасности таможенных органов Российской Федерации показывает, что имеются факторы, влияющие на эффективность принимаемых ФТС России мер, в частности:

• современные условия политического и социально-экономического развития Российской Федерации вызывают обострение противоречий между потребностями общества в расширении свободного доступа к информации в области таможенного дела и необходимости сохранения регламентированных ограничений на ее распространение;

• расширяется информационное взаимодействие ФТС России с таможенными администрациями иностранных государств, международными организациями, федеральными органами исполнительной власти, организациями банковской сферы и участниками внешнеэкономической деятельности;

• растет число компьютерных преступлений, связанных с проникновением криминальных элементов в компьютерные системы кредитно-финансовой сферы;

• оплата труда должностных лиц и работников таможенных органов Российской Федерации не соответствует экономической

значимости морально-психологической устойчивости и социальной защищенности людей, работающих с информацией ограниченного доступа;

• недостаточен контроль со стороны руководителей таможенных органов Российской Федерации и их структурных подразделений за состоянием информационной безопасности, выполнением под чиненными должностными лицами и работниками регламентов, должностных инструкций, нормативных правовых актов;

• штатная численность должностных лиц и работников, отвечающих за обеспечение информационной безопасности, не соответствует объему решаемых задач;

• недостаточно развита система первичной подготовки кадров для таможенных органов Российской Федерации в сфере обеспечения информационной безопасности;

• отставание отечественных информационных технологий вынуждает идти по пути закупок незащищенной импортной техники, из-за чего повышается вероятность несанкционированного доступа к обрабатываемой информации и возрастает зависимость таможенных органов Российской Федерации от иностранных производителей компьютерной и телекоммуникационной техники, а также программного обеспечения;

• оснащение таможенных органов Российской Федерации сертифицированными по требованиям безопасности информации средствами информатизации, включая средства защиты информации и программное обеспечение, не соответствует потребностям, что снижает эффективность использования применяемых средств и методов защиты информации;

• отсутствуют критерии и методы оценки защищенности автоматизированных информационных систем таможенных органов Российской Федерации, а также методы и технологии их сертификации по требованиям безопасности информации в условиях постоянной их модернизации и развития.

Угроза информационной безопасности - целенаправленное действие, которое повышает уязвимость накапливаемой, хранимой и обрабатываемой информации и приводит к ее случайному или предумышленному изменению,

или уничтожению. В соответствии с Доктриной информационной безопасности Российской Федерации по своей общей направленности в части таможенных органов Российской Федерации угрозы информационной без опасности подразделяются на следующие виды:

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

• угрозы информационному обеспечению государственной поли тики в области таможенного дела;

• угрозы 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 также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов в области таможенного дела;

• угрозы обеспечению безопасности информации в автоматизированных информационных 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 ин формационными 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 за щиты 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, 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 не сертифицированных по требованиям безопасности информационных технологий, средств вычислительной техники, телекоммуникации и связи, программного обеспечения и средств защиты информации;

• утечка информации ограниченного доступа, обрабатываемой на объектах информатизации таможенных органов Российской Федерации, по техническим каналам.

В качестве потенциального (вероятного) нарушителя информационной безопасности таможенных органов Российской Федерации в общем случае рассматривается субъект, имеющий возможность реализовывать, в том числе с помощью технических средств, угрозы информационной безопасности и осуществлять посягательства (способы воздействия) на информационные ресурсы и системы таможенных органов Российской Федерации.

Нарушителей можно классифицировать следующим образом:

• 1-й уровень - внешний нарушитель (группа внешних нарушите лей), самостоятельно осуществляющий создание методов и средств реализации угроз, а также реализующий угрозы (атаки);

• 2-й уровень - внутренний нарушитель, являющийся должностным лицом или работником таможенных органов Российской Федерации, но который не допущен к работе на объектах обеспечения информационной безопасности таможенных органов Российской Федерации или с данными объектами (группа нарушителей, среди которых есть, по крайней мере, один указанный выше внутренний нарушитель), самостоятельно осуществляющий создание методов и средств реализации угроз, а также реализующий угрозы (атаки). К данному уровню также относится нарушитель, не являющийся должностным лицом или работником таможенных органов Российской Федерации, но имеющий возможность находиться в пределах контролируемой зоны объектов обеспечения информационной безопасности таможенных органов Российской Федерации;

• 3-й уровень - внутренний нарушитель, являющийся должностным лицом или работником таможенных органов Российской Федерации, который допущен к работе на объектах обеспечения информационной безопасности таможенных органов Российской Федерации или с данными объектами (группа нарушителей, среди которых есть, по крайней мере, один указанный выше внутренний нарушитель), самостоятельно осуществляющий создание методов и средств реализации угроз, а также реализующий угрозы (атаки);

• 4-й уровень - группа нарушителей (среди которых есть внутренние, являющиеся должностными лицами и работниками таможенных органов Российской Федерации), осуществляющая со здание методов и средств реализации угроз, а также реализующая их с привлечением отдельных специалистов, имеющих опыт раз работки и анализа средств защиты информации, используемых на объектах обеспечения информационной безопасности таможенных органов Российской Федерации;

• 5-й уровень - группа нарушителей (среди которых есть внутренние, являющиеся должностными лицами и работниками таможенных органов Российской Федерации), осуществляющая создание методов и средств реализации атак, а также реализующая атаки с привлечением научно-исследовательских центров, специализирующихся в области разработки и анализа средств защиты ин формации (включая специалистов в области использования для реализации угроз (атак) недокументированных возможностей прикладного программного обеспечения);

• 6-й уровень - спецслужбы иностранных государств, осуществляющие создание методов и средств реализации угроз, а также реализующие их с привлечением научно-исследовательских центров, специализирующихся в области разработки и анализа средств защиты информации (включая специалистов в области использования для реализации угроз (атак) недокументированных возможностей прикладного программного обеспечения).

Предполагается, что на этих уровнях нарушитель является специалистом высшей квалификации, знает все об информационной системе и об используемых в ней средствах защиты и может при определенных обстоятельствах осуществить весь спектр посягательств на информационные ресурсы.

В своей противоправной деятельности вероятный нарушитель может использовать любое существующее в стране и за рубежом средство перехвата информации, воздействия на информацию и информационные системы таможенных органов, адекватные финансовые средства для подкупа должностных лиц и работников таможенных органов Российской Федерации, шантаж и другие средства и методы для достижения стоящих перед ним целей.

Необходимо учитывать также цели посягательств вероятного нарушителя на информационные ресурсы и системы. Среди таких целей может быть хищение информации (шпионаж, в том числе экономический),

намерение совершить корыстное преступление, любопытство, удовлетворение собственного тщеславия, месть, вандализм и др.

Наибольшую угрозу обеспечению информационной безопасности таможенных органов Российской Федерации представляют нарушители 2-4 уровня. В то же время для различных объектов обеспечения информационной безопасности таможенных органов Российской Федерации модель нарушителя может быть различной и уточняется по мере необходимости.

6.2 Формы обеспечения информационной безопасности ЕАИС

Для предохранения таможенной информации от несанкционированного доступа выделяют следующие формы защиты:

- физические (препятствие);
- законодательные;
- управление доступом;
- криптографическое закрытие.

Физические формы защиты основаны на создании физических препятствий для злоумышленника, преграждающих ему путь к защищаемой информации (строгая система пропуска на территорию и в помещения с аппаратурой или с носителями информации). Эти способы дают защиту только от «внешних» злоумышленников и не защищают информацию от тех лиц, которые обладают правом входа в помещение.

Законодательные формы защиты составляют нормативные документы ФТС России, которые регламентируют правила использования и обработки информации ограниченного доступа и устанавливают меры ответственности за нарушение этих правил.

Управление доступом представляет способ защиты информации путем регулирования доступа ко всем ресурсам системы (техническим, программным, элементам баз данных). В таможенных информационных

системах регламентированы порядок работы пользователей и персонала, право доступа к отдельным файлам в базах данных и т. д. Управление доступом предусматривает следующие функции защиты:

• идентификацию пользователей, персонала и ресурсов системы (присвоение каждому объекту персонального идентификатора: имени, кода, пароля и т. п.);

• аутентификацию - опознание (установление подлинности) объекта или субъекта по предъявляемому им идентификатору;

• авторизацию - проверку полномочий (проверку соответствия дня недели, времени суток, запрашиваемых ресурсов и процедур установленному регламенту);

• разрешение и создание условий работы в пределах установленного регламента;

• регистрацию (протоколирование) обращений к защищаемым ресурсам;

• реагирование (сигнализация, отключение, задержка работ, отказ в запросе) при попытках несанкционированных действий.

Самым распространенным методом установления подлинности является метод паролей. Пароль представляет собой строку символов, которую пользователь должен ввести в систему каким-либо способом (напечатать, набрать на клавиатуре и т. п.). Если введенный пароль со ответствует хранящемуся в памяти, то пользователь получает доступ ко всей информации, защищенной этим паролем. Пароль можно использовать и независимо от пользователя для защиты файлов, записей, полей данных внутри записей и т. д.

Парольная защита широко применяется в системах защиты информации и характеризуется простотой и дешевизной реализации, малы ми затратами машинного времени, не требует больших объемов памяти. Однако парольная защита часто не дает достаточного эффекта по следующим причинам.

1. Чрезмерная длина пароля, не позволяющая его запомнить, стимулирует пользователя к записи пароля на подручных бумажных носителях, что сразу делает пароль уязвимым.

2. Пользователи склонны к выбору тривиальных паролей, которые можно подобрать после небольшого числа попыток тривиального перебора.

3. Процесс ввода пароля в систему поддается наблюдению даже в том случае, когда вводимые символы не отображаются на экране.

4. Таблица паролей, которая входит обычно в состав программного обеспечения операционной системы, может быть изменена, что нередко и происходит. Поэтому таблица паролей должна быть закодирована, а ключ алгоритма декодирования должен находиться только у лица, отвечающего за безопасность информации.

5. В систему может быть внесен «троянский конь», перехватывающий вводимые пароли и записывающий их в отдельный файл, поэтому при работе с новыми программными продуктами необходима большая осторожность.

При работе с паролями рекомендуется применение следующих правил и мер предосторожности:

• не печатать пароли и не выводить их на экран;

• часто менять пароли - чем дольше используется один и тот же пароль, тем больше вероятность его раскрытия;

• каждый пользователь должен хранить свой пароль и не позволять посторонним узнать его;

• всегда зашифровывать пароли и обеспечивать их защиту недорогими и эффективными средствами;

• правильно выбирать длину пароля (чем она больше, тем более высокую степень безопасности будет обеспечивать система, так как труднее будет отгадать пароль).

Основным методом защиты информации, хранящейся в ЕАИС, от несанкционированного доступа является метод обеспечения разграничения функциональных полномочий и доступа к информации, направленный на

предотвращение не только возможности потенциального нарушителя «читать» хранящуюся в ПЭВМ информацию, но и возможности нарушителя модифицировать ее штатными и нештатными средствами.

Надежность защиты может быть обеспечена правильным подбором основных механизмов защиты, некоторые из них рассмотрим ниже.

Механизм регламентации. Основан на использовании метода защиты информации, создает такие условия автоматизированной обработки, хранения и передачи защищаемой информации, при которых возможности НСД к ней сводились бы к минимуму.

Механизм аутентификации. Различают одностороннюю и взаимную аутентификацию. В первом случае один из взаимодействующих объектов проверяет подлинность другого, тогда как во втором случае проверка является взаимной.

Криптографические методы защиты информации. Эти методы защиты широко применяются за рубежом, как при обработке, так и при хранении информации. Для реализации мер безопасности используются различные способы шифрования (криптографии), суть которых заключается в том, что данные, отправляемые на хранение, или сообщения, готовые для передачи, зашифровываются и тем самым преобразуются в шифрограмму или закрытый текст. Санкционированный пользователь получает данные или сообщение, дешифрует их или раскрывает посредством обратного преобразования криптограммы, в результате чего получается исходный открытый текст. Методу преобразования в криптографической системе соответствует использование специального алгоритма. Действие такого алгоритма запускается уникальным числом (или битовой последовательностью), обычно называемым шифрующим ключом.

В современной криптографии существуют два типа криптографических алгоритмов:

1) классические алгоритмы, основанные на использовании закрытых, секретных ключей (симметричные);

2) алгоритмы с открытым ключом, в которых используются один открытый и один закрытый ключ (асимметричные). В настоящее время находят широкое практическое применение в средствах защиты электронной информации алгоритмы с секретным ключом.

Заключение

Развитие информационных технологий в таможенных службах регламентируется положениями Всемирной таможенной организации и определяется необходимостью гармонизации средств и способов представления информации в интересах поддержки принятия решения должностным лицом таможенных органов.

Магистральными направлениями развития информационных таможенных технологий являются: предварительное информирование, электронное декларирование, средства удаленного выпуска, управление рисками с учетом сложившейся тенденции использования средств Data Mining. Практическая совместная реализации указанных технологий возможна лишь на единых методических принципах, общей технологической платформе, с учетом унифицированных требований по защите информации.

Постоянный технический прогресс определяет постоянную смену программных платформ, прикладных программных средств реализации таможенных технологий, ставит задачу постоянного овладения должностными лицами таможенных органов новыми программными средствами. Эффективность решения данной задачи зависит от комплекса имеющихся у должностного лица таможенных органов соответствующих компетенций в области информационных технологий, включающих как комплекс знаний по их основным составляющим, так и набор навыков их применения, определяющих возможность раз решать сложные практические задачи, выявлять проблемы, возникающие при внедрении новых программных средств, грамотно формировать технические требования к программным средствам.

СПИСОК ЛИТЕРАТУРЫ

1. Судебные речи выдающихся русских юристов. В.Д. Спасович. Дело Давида и Николая Чхотуа и других (Тифлисское дело); Равновесие - Москва, 2013. - 125 с.
2. Таможенное право; Юнити-Дана - Москва, 2007. - 392 с.
3. Таможенное право; Юнити-Дана, Закон и порядок - Москва, 2010. - 224 с.
4. Таможенное право; АСТ, Сова, ВКТ - Москва, 2011. - 160 с.
5. Брюховец, Н.А.; Чахоян, Л.П. Английский язык: менеджмент, маркетинг, таможенное дело; СПб: Профессия - Москва, 2000. - 288 с.
6. Гарднер Э.С. Дело о наивной девушке. Дело о длинноногих манекенщицах (комплект из 2 книг); Отечество - Москва, 1991. - 368 с.
7. Коник Н.В., Невешкина Е.В. Таможенное дело; Омега-Л - Москва, 2011. - 208 с.
8. Маховикова Г.А., Павлова Е.Е. Таможенное дело; Юрайт - Москва, 2013. - 408 с.
9. Молчанова О.В., Коган М.В. Таможенное дело; Феникс - Москва, 2007. - 320 с.
10. Толкушкин А.В. Таможенное дело; Юрайт - Москва, 2008. - 453 с.
11. Толкушкин А.В. Таможенное дело; Юрайт - Москва, 2011. - 560 с.
12. Толкушкин А.В. Таможенное дело; Юрайт - Москва, 2012. - 560 с.
13. Толкушкин А.В. Таможенное дело. Конспект лекций; Юрайт - Москва, 2011. - 258 с.
14. Халипов С.В. Таможенное право; Юрайт - Москва, 2012. - 460