МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

САНКТ-ПЕТЕРБУРГСКИЙ НАЦИОНАЛЬНЫЙ
ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ

И.А. Хахаев

ИНФОРМАЦИОННЫЕ ТАМОЖЕННЫЕ ТЕХНОЛОГИИ

Учебное пособие

Санкт-Петербург

2014

Хахаев И.А. Информационные таможенные технологии: учеб. пособие. – СПб: НИУ ИТМО, 2014. – 122 с.

Учебное пособие разработано в соответствие с программой дисциплины «Информационные таможенные технологии» и предназначено для студентов, обучающихся по специальности 38.05.02 (036401) «Таможенное дело» для использования при подготовке семинарских занятий, курсовых проектов, отчетов по практике, дипломных работ.

В пособии рассматриваются общие понятия информационных технологий и автоматизированных информационных систем, а также отдельные подсистемы Единой Автоматизированной Информационной системы (ЕАИС) ФТС России. Отдельно рассмотрены основы построения и использования баз данных, а также вопросы оценки безопасности информационных систем

Работа подготовлена на кафедре «Таможенного дела и логистики».

Рекомендовано к печати Учёным советом ИМБИП, протокол № 4 от 15.04.2014г.

В 2009 году Университет стал победителем многоэтапного конкурса, в результате которого определены 12 ведущих университетов России, которым присвоена категория «Национальный исследовательский университет». Министерством образования и науки Российской Федерации была утверждена программа его развития на 2009–2018 годы**.** В 2011 году Университет получил наименование «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики»

Содержание

Введение

Данное учебно-методическое издание предназначено для студентов специальности 38.05.02 (036401) «Таможенное дело» в качестве базового пособия по теоретической части курса. Оно акцентирует внимание на отдельных существенных аспектах дисциплины и не заменяет основную учебную литературу по курсу «Информационные таможенные технологии».

Материал, изложенный в пособии, подразумевает наличие знаний, полученных в ходе изучения дисциплин «Информатика» и «Вычислительные машины, сети и системы телекоммуникаций в таможенном деле», поэтому здесь не рассматриваются вопросы организации вычислительных комплексов и компьютерных сетей.

В пособии раскрываются общие понятия информационных технологий и автоматизированных информационных систем, а затем рассматриваются конкретные подсистемы ЕАИС ФТС России. Отдельно рассматриваются основы построения и использования баз данных, а также вопросы оценки безопасности информационных систем.

В списке литературы приводятся только учебники, монографии и электронные ресурсы, являющиеся основой для изложенного в пособии материала. Нормативные документы, определяющие использование средств информационных технологий и другие аспекты работы информационных систем в России и в ЕАИС ФТС, приводятся по ходу изложения материала.

Информационный процесс и информационная технология

Понятие информационного процесса

Информационные процесс — все что происходит с информацией. Этот процесс можно рассматривать как «жизненный цикл» информации от появления (сбора) до уничтожения или как увеличение «качества» информации от данных к мудрости.

Этапы (фазы) информационного процесса для обоих вариантов рассмотрения приведены в таблице.

С позиций жизненного цикла информации	**С позиций нарастания «качества» информации**
• Сбор • Подготовка • Обработка • Хранение	• Сбор информации • Формирование и передача данных • Анализ и практическое использование информации

• Передача • Воспроизведение • Уничтожение	• Формирование знаний • Применение знаний • Накопление мудрости (опыта применения знаний в различных ситуациях и обобщение этого опыта)

Здесь «знания» рассматриваются с позиций теории искусственного интеллекта и экспертных систем как совокупность информации и правил формирования выводов (у индивидуума, общества или системы ИИ) о мире, свойствах объектов, закономерностях процессов и явлений, а также правилах использования их для принятия решений. Главное отличие знаний от данных состоит в их структурности и активности (изменение данных и связей между ними может привести к изменению выводов и решений).

Понятие информационной технологии (ИТ), цель применения ИТ.

Информационная технология – процесс, использующий совокупность средств и методов сбора, обработки и передачи данных (первичной информации) для получения информации нового качества о состоянии объекта, процесса или явления (информационного продукта).

Информационная технология – реализация информационного процесса.

Цель информационной технологии – производство информации для ее анализа человеком и принятия на его основе решения по выполнению какого-либо действия.

Обобщённая структура информационной технологии показана на рис. 1.

Автоматизированные информационные технологии (АИТ) включают в себя элементарные операции, действия, операции и этапы, выполняемые как с использованием средств вычислительной техники (СВТ), так и с участием человека.

По способу реализации АИТ можно разделить на централизованные и распределённые.

Централизованные АИТ характерны для систем, где обработка и работа с информацией производится исключительно в главном вычислительном центре (центре обработки данных — ЦОД), в то время как конечные элементы системы нацелены на сбор информации, а не на обработку. Примерами могут служить сеть платёжных терминалов или система заказа железнодорожных билетов.

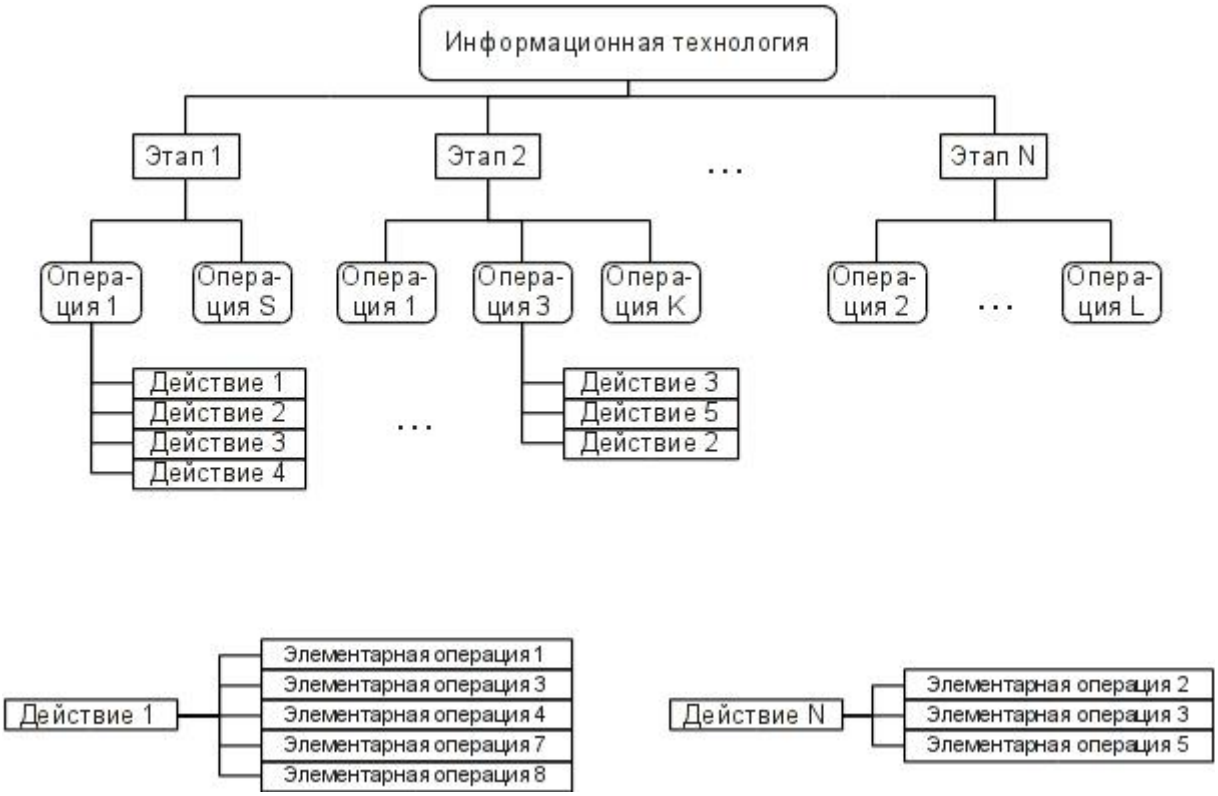

Рис. 1 Обобщённая структура информационной технологии.

Распределённые технологии означают распределение вычислительных функций между разными вычислительными системами и реализуются в большинстве современных автоматизированных информационных систем.

Также возможна классификация АИТ по другим признакам, в частности:

- **По специализация информационной технологии** АИТ обычно делятся на системы автоматизированной обработки информации; системы автоматизации управленческих процессов; системы обеспечения электронного документооборота (электронный офис); системы управления базами и банками данных и т.п.
- **По специализация приложений в составе АИТ** возможно подразделение на средства работы с текстовыми документами, средства обработки табличных данных и однородных массивов информации, средства для работы с графической информацией, средства для работы с мультимедиа-контентом.
- **По режиму взаимодействия с пользователями** АИС подразделяются на системы, работающие в пакетном или диалоговом режиме. В пакетном режиме пользователь не получает никаких сообщений до завершения процесса обработки его задания (который может быть достаточно длительным), даже в случае ошибок выполнения задания. В диалоговом режиме на каждом этапе (операции) возможно уточнение задания и устранение возможных ошибок.
- **По способу организации информационной сети** АИТ подразделяются на локальные или интранет-технологии, многоуровневые и распределённые технологии.

• **По отраслевой специализация** АИТ можно разделить на технологии работы к клиентами, технологии бухгалтерского учёта, банковские технологии, логистические технологии и пр.

Автоматизированные информационные системы (АИС)

Понятие АИС, обеспечивающие подсистемы АИС

Основные термины и определения, касающиеся автоматизированных информационных систем, приведены в **ГОСТ 34.003-90 «Информационная технология. Автоматизированные системы. Термины и определения.»**

В соответствии с этим нормативным документом, АИС — это система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

В общем случае АИС может быть представлена как совокупность обеспечивающих подсистем (п**одсистема** – часть системы, выделенная по какому-либо признаку.). Эти подсистемы в соответствии с ГОСТ 34.003-90 называются **видами обеспечения АИС** (см. рис. 2).

Рис. 2. Виды обеспечения (обеспечивающие подсистемы) АИС.

Организационное обеспечение АИС – совокупность документов, устанавливающих организационную структуру, права и обязанности пользователей и эксплуатационного персонала АС в условиях

функционирования, проверки и обеспечения работоспособности АС.

Другими словами — это совокупность *методов и средств, регламентирующих* взаимодействие работников с техническими средствами и между собой в процессе разработки и эксплуатации информационной системы.

- анализ существующей системы управления организацией, где используется ИС, и выявление задач, подлежащих автоматизации
- подготовка задач к решению на компьютере, включая техническое задание на проектирование/модернизацию ИС и технико-экономическое обоснование её эффективности
- разработка управленческих решений по составу и структуре организации, методологии решения задач, направленных на повышение эффективности системы управления.

Методическое обеспечение АИС — совокупность документов, описывающих технологию функционирования АС, методы выбора и применения пользователями технологических приёмов для получения конкретных результатов при функционировании АИС. Сюда включаются методические указания, пособия, учебные курсы, программы повышения квалификации и учебно-тренировочные средства, обеспечивающие подготовку и переподготовку пользователей сложных АИС.

Техническое обеспечение – комплекс технических средств, предназначенных для работы информационной системы, а также соответствующая документация на эти средства и технологические процессы (в соответствии с ГОСТ . ГОСТ 34.003-90 техническое обеспечение АИС — совокупность всех технических средств, используемых при функционировании АИС).

В качестве технических средств могут использоваться

- компьютеры любых моделей
- устройства сбора, накопления, обработки, передачи и вывода информации
- устройства передачи данных и линии связи
- оргтехника и устройства автоматического съема информации
- расходные материалы и комплектующие

Техническое обеспечение может быть организовано двумя способами:

- **Централизованное техническое обеспечение** базируется на использовании в информационной системе больших ЭВМ («мэйнфреймов») и вычислительных центров (центров обработки данных — ЦОД)
- **Децентрализация технических средств** предполагает реализацию функциональных подсистем на персональных компьютерах непосредственно на рабочих местах

Математическое обеспечение АИС – совокупность математических методов, моделей и алгоритмов, примененных в АС.

В состав математического обеспечения включаются:

- средства моделирования процессов управления
- типовые задачи управления
- методы математического программирования, математической статистики, теории массового обслуживания и др.

Программное обеспечение АИС — совокупность программ на носителях данных и программных документов, предназначенная для отладки, функционирования и проверки работоспособности АС.

В состав программного обеспечения (ПО) включаются:

- общесистемные программные продукты
- специальные программные продукты
- документы, подтверждающие правомочность использования программных продуктов («лицензии»)
- техническая документация на ПО.

Информационное обеспечение АИС — совокупность форм документов, классификаторов, нормативной базы и реализованных решений по объемам, размещению и формам существования информации, применяемой в АС при ее функционировании. Назначение подсистемы информационного обеспечения (ИО) состоит в своевременном формировании и выдаче достоверной информации для принятия управленческих решений.

В состав информационного обеспечения включаются:

- Системы классификации и кодирования информации: формирование *метаданных* и определение *форматов* документов
- Унифицированные системы документации: сопоставимость показателей в различных сферах деятельности
- Схемы информационных потоков: маршруты движения информации и её объёмы, места возникновения первичной информации и использования итоговой информации
- Методология построения баз данных: БД строятся на основе информационно-логической модели, полученной после анализа информационных потоков.

Лингвистическое обеспечение АИС — совокупность средств и правил для формализации естественного языка, используемых при общении пользователей и эксплуатационного персонала АИС с комплексом средств автоматизации при функционировании АИС.

В состав лингвистического обеспечения включаются словари терминов, касающиеся конкретной АИС или класса АИС (глоссарии), словари

сокращений, а также системы команд для диалогового режима взаимодействия пользователей и эксплуатационного персонала АИС с отдельными элементами и узлами АИС.

Правовое обеспечение АИС – совокупность правовых норм, регламентирующих правовые отношения при функционировании АС и юридический статус результатов её функционирования.. Правовое обеспечение может быть реализовано как составная часть организационного обеспечения. Правовые нормы определяют создание, юридический статус и функционирование информационных систем, порядок получения, преобразования и использования информации.

В состав правового обеспечения включаются:

- законы, указы, постановления государственных органов власти, приказы, инструкции и другие нормативные документы министерств, ведомств, организаций, местных органов власти
  - **Общая часть**: регулирует функционирование любой АИС
  - **Локальная часть**: регулирует функционирование конкретной АИС
- **Правовое обеспечение этапа разработки**: нормативные акты, связанные с договорными отношениями разработчика и заказчика и правовым регулированием отклонений от договора.
- **Правовое обеспечение этапа функционирования**: статус информационной системы, права, обязанности и ответственность персонала, правовые положения отдельных видов процесса управления, порядок создания и использования информации и др.

Эргономическое обеспечение АИС — совокупность реализованных в АИС решений по согласованию психологических, психофизиологических, антропометрических, физиологических характеристик и возможностей пользователей АИС с техническими характеристиками комплекса средств автоматизации АС и параметрами рабочей среды на рабочих местах персонала АИС.

В состав эргономического обеспечения включаются:

- требования к составу и оборудованию рабочих мест
- требования к аппаратным средствам пользовательского интерфейса (клавиатуры, манипуляторы, мониторы и экраны)
- требования к программным средствам пользовательского интерфейса (организация меню, расположение элементов, цвета и форма элементов).

Обобщённая структурная схема АИС предприятия

Обобщённая структурная схема АИС масштаба предприятия показана на рис. 3.

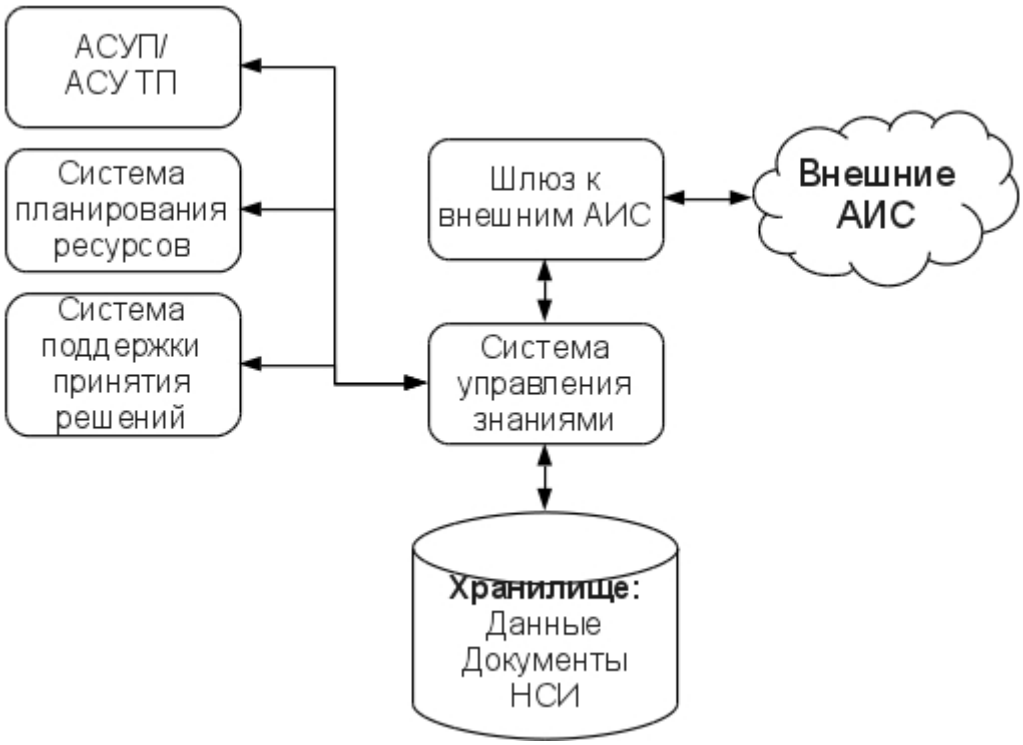

Рис. 3. Обобщённая структурная схема АИС предприятия.

Основными составными частями АИС предприятия являются:

- Хранилище файлов, данных и документов, включая нормативно-справочную информацию (НСИ), то есть элементы организационного и правового обеспечения АИС
- Система управления знаниями, обеспечивающее получение нужных сведений (знаний) из хранилища по запросу от других составных частей
- Система анализа и принятия решений (система поддержки принятия решений — СППР, Decision Support System — DSS)
- Система планирования ресурсов (Enterprise Resource Planning — ERP).
- Автоматизированная система управления предприятием (АСУП) или технологическими процессами (АСУ ТП)
- Шлюзы к внешним АИС, обеспечивающие обмен данными и документами.

В реальной системе основные блоки могут быть автоматизированы в различной степени. В некоторых случаях часть функций вообще не автоматизируется.

Система управления знаниями обеспечивает независимость других подсистем от конкретной структуры и форматов данных в хранилище.

Под АСУ ТП понимается система управления любыми технологическими процессами, не только производственными.

Классификация ИС

Информация является **ресурсом** и влияет на работу предприятия (организации) так же, как оборудование, деньги и время.

Поэтому информационные системы (ИС) стали необходимым инструментом практически во всех сферах деятельности.

Информационные системы можно классифицировать по целому ряду различных признаков.

В зависимости от объёма решаемых задач, используемых технических средств, организации функционирования, информационные системы делятся на ряд групп (классов).

Варианты классификации ИС показаны на рис. 4.

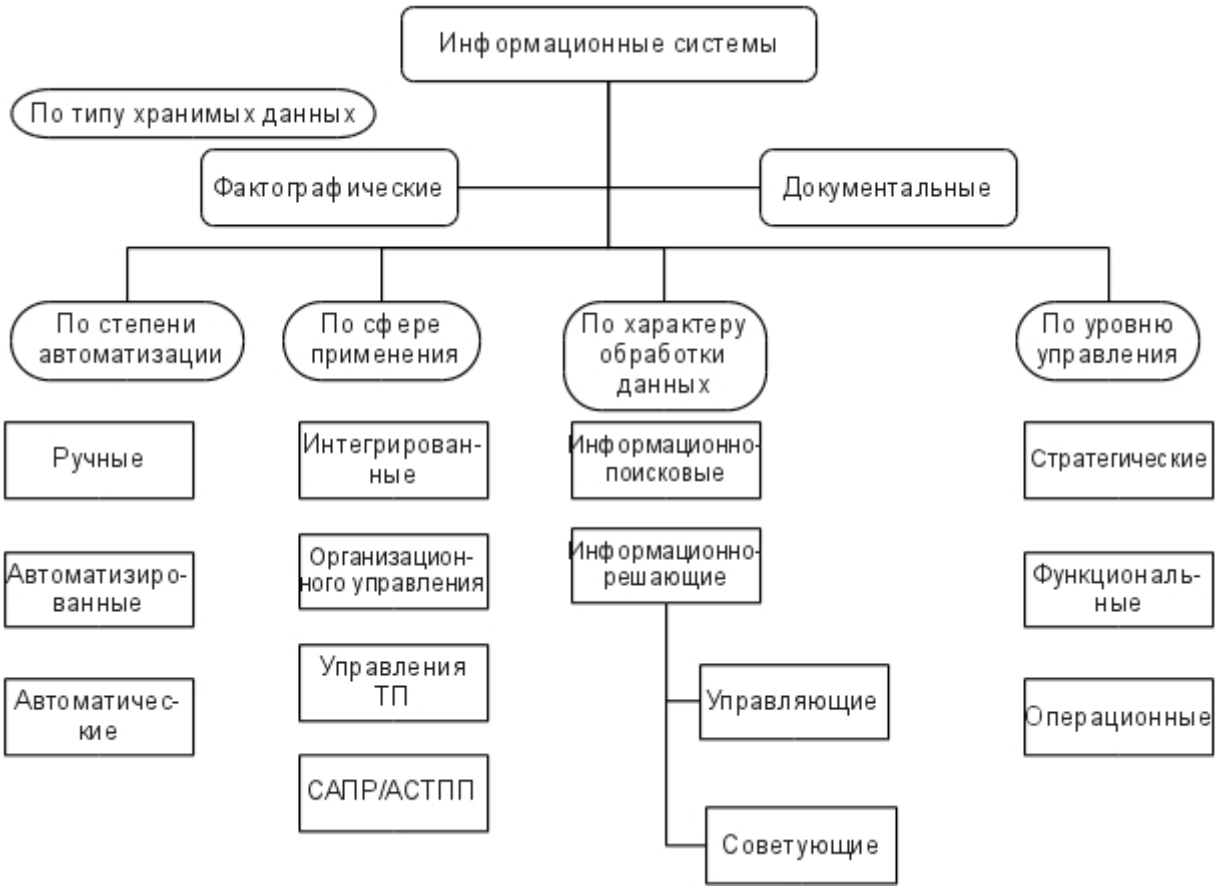

Рис. 4. Способы классификации информационных систем

По типу хранимых данных все ИС подразделяются на фактографические и документальные.

Фактографические ИС предназначены для хранения и обработки **структурированных данных** в виде чисел и текстов. Над такими данными можно выполнять различные операции.

В документальных ИС информация представлена в виде **документов**, состоящих из наименований, описаний, рефератов и текстов. Поиск по

неструктурированным данным осуществляется с использованием семантических признаков. Отобранные документы предоставляются пользователю, а обработка данных в таких системах практически не производится.

По степени автоматизации информационных процессов все ИС подразделяются на ручные, автоматизированные и автоматические.

Ручные ИС характеризуются отсутствием современных технических средств переработки информации и выполнением всех операций человеком.

В автоматических ИС все операции по переработке информации выполняются без участия человека.

Автоматизированные ИС (АИС) предполагают участие в процессе обработки информации и человека, и технических средств, причём главная роль в выполнении рутинных операций обработки данных отводится средствам вычислительной техники. Именно этот класс систем соответствует современному представлению понятия «информационная система».

По характеру обработки данных все ИС подразделяются на информационно-поисковые и информационно-решающие.

Информационно-поисковые ИС обеспечивают ввод, систематизацию, хранение, выдачу информации по запросу пользователя без сложных преобразований данных. (Например, ИС библиотечного обслуживания, резервирования и продажи билетов на транспорте, бронирования мест в гостиницах и пр.).

Информационно-решающие ИС осуществляют операции переработки информации по определённому алгоритму и в свою очередь могут подразделяться на управляющие и советующие ИС.

- **Управляющие ИС**: Результирующая информация непосредственно трансформируется в принимаемые человеком решения. Для этих систем характерны задачи расчётного характера и обработка больших объёмов данных. (Например, ИС планирования производства или заказов, бухгалтерского учёта.)
- **Советующие ИС**: Вырабатывают информацию, которая принимается человеком к сведению и учитывается при формировании управленческих решений, а не инициирует конкретные действия. Эти системы имитируют интеллектуальные процессы обработки **знаний**, а не данных. (Например, экспертные системы и системы поддержки принятия решений – СППР.)

По сферам применения все ИС подразделяются на системы организационного управления, ИС управления технологическими процессами (ТП), ИС автоматизированного проектирования (САПР) и технологической подготовки производства (АСТПП), также интегрированные (корпоративные) ИС.

Системы организационного управления предназначены для автоматизации функций управленческого персонала как промышленных предприятий, так и непромышленных объектов (гостиниц, банков, магазинов и пр.). Основными функциями подобных систем являются:

- оперативный контроль и регулирование
- оперативный учёт и анализ
- перспективное и оперативное планирование
- бухгалтерский учёт
- управление сбытом и снабжением
- другие экономические и организационные задачи

ИС управления технологическими процессами (ТП) служат для автоматизации функций производственного персонала по контролю и управлению производственными операциями. В таких системах обычно предусматривается наличие развитых средств измерения параметров технологических процессов (температуры, давления, химического состава и т.п.), процедур контроля допустимости значений параметров и регулирования технологических процессов.

ИС автоматизированного проектирования (САПР) предназначены для автоматизации функций инженеров-проектировщиков, конструкторов, архитекторов, дизайнеров при создании новой техники или технологии. Основными функциями подобных систем являются: инженерные расчёты, создание графической документации (чертежей, схем, планов), создание проектной документации, моделирование проектируемых объектов. АСТПП помимо проектирования, обеспечивают автоматизацию задач разработки систем, моделирования узлов и элементов конструкций, разработку и подготовку документации для обеспечения производства.

Интегрированные (корпоративные) ИС используются для автоматизации всех функций фирмы и охватывают весь цикл работ от планирования деятельности до сбыта продукции. Они включают в себя ряд модулей (подсистем), работающих в едином информационном пространстве и выполняющих функции поддержки соответствующих направлений деятельности.

По уровню управления все ИС подразделяются на стратегические, функциональные и операционные.

Стратегические ИС обеспечивают поддержку принятия управленческие решений на уровне руководства организации за счет анализа данных по всем процессам деятельности. Такие системы используют данные и знания, прошедшие первичную обработку в системах более низких уровней управления.

Функциональные ИС обеспечивают выполнение каких либо функций организации (например, таможенного оформления грузов) и включают в себя

несколько операционных информационных систем.

Операционные ИС обеспечивают выполнение каких-либо отдельных операций в составе информационной технологии (например, заполнение декларации на товары).

Системы поддержки принятия решений

Система поддержки принятия решений (СППР) — *человеко-машинная система*, которая позволяет лицам, принимающим решение (ЛПР), использовать данные и знания объективного и субъективного характера для решения слабо структурированных (плохо формализованных) проблем.

СППР являются автоматизированными фактографическими советующими информационно-решающими системами организационного управления для стратегического уровня управления,

Сфера практического применения СППР – планирование и прогнозирование для различных видов управленческой деятельности.

Компонентный состав СППР, как правило, включает в себя

- модели управления
- подсистему управления данными для сбора и ручной обработки данных
- подсистему автоматического сбора данных из АИС более низкого уровня
- подсистему управления диалогом для облегчения доступа пользователя к СППР

Модель управления используемая в СППР, может оказаться *неадекватной*. Для эффективного использования такой СППР нужно иметь возможность изменять модели, то есть СППР должна быть быть открытой для модификации. Кроме того, нужно понимать, как строятся модели.

Процесс принятия решения при использовании СППР делится на следующие этапы (стадии)

- **Распознавание или осмысление**: идентификация и понимание проблем, встречающихся в организации (почему проблемы возникают, где и с каким результатом)
- **Проект или продумывание**: возможные варианты решения проблем. Помогает использование простых моделей.
- **Выбор**: подбор решения среди альтернатив. Помогает использование обширных данных относительно ряда альтернатив и комплексных аналитических моделей, чтобы объяснить все затраты, следствия и возможности
- **Реализация**: важно иметь возможность следить за выполнением решения.

СППР помогают проектировать, оценивать альтернативы и контролировать процесс реализации.

Выделяют следующие варианты применения СППР:

1. **Анализ примеров (case analysis)**: оценка значений выходных величин для заданного набора значений входных переменных
2. **Параметрический анализ («Что, если... ?»)**: оценка поведения выходных величин при изменении значений входных переменных
3. **Анализ чувствительности**: исследование поведения результирующих переменных в зависимости от изменения значений одной или нескольких входных переменных
4. **Анализ возможностей**: нахождение значений входной переменной, которые обеспечивают желаемый результат (известен также под названием «поиск целевых решений», «анализ значений целей», «управление по целям»)
5. **Анализ влияния**: выявление для выбранной результирующей переменной всех входных переменных, влияющих на ее значение, и оценка величины изменения результирующей переменной при заданном изменении входной переменной, скажем, на 1 %.
6. **Анализ данных**: прямой ввод в модель ранее имевшихся данных и манипулирование ими при прогнозировании
7. **Сравнение и агрегирование**: сравнение результатов двух или более прогнозов, сделанных при различных входных предположениях, или сравнение предсказанных результатов с действительными, или объединение результатов, полученных при различных прогнозах или для разных моделей
8. **Командные последовательности (sequences)**: возможность записывать, исполнять, сохранять для последующего использования регулярно выполняемые серии команд и сообщений
9. **Анализ риска**: оценка изменения выходных переменных при случайных изменениях входных величин
10. **Оптимизация**: поиск значений управляемых входных переменных, обеспечивающих наилучшее значение одной или нескольких результирующих переменных.

Базовые информационные технологии

Технологии работы с базами данных и банками данных

Понятие базы данных и модели данных

В соответствии с ГОСТ 34.321-96 **база данных (БД, database)** - совокупность взаимосвязанных данных, организованных в соответствии со **схемой базы данных** таким образом, чтобы с ними мог работать пользователь

(определение БД1).

Схема базы данных: Формальное описание данных в соответствии со **схемой данных**.

Схема данных: Логическое представление организации данных.

Также базу данных можно определить как совокупность данных, организованных в соответствии с общими принципами описания, хранения и управления данными, и независимая от программного обеспечения (определение БД2)

Часто используется еще одно определение базы данных как поименованной совокупности структурированных данных, относящихся к определённой **предметной области**. (определение БД3)

Предметная область – некоторая часть реально существующей системы, функционирующая как самостоятельная единица.

Проще говоря, **предметная область** – изучаемые объекты или явления (процессы).

Это объекты (явления, процессы, иначе именуемые сущностями - entities) имеют какие-то характеристики (атрибуты, свойства).

Структура связей между характеристиками различными экземплярами сущностей и между разными сущностями в базе данных определяется моделью данных (или схемой данных).

Модель данных – это общие принципы описания, хранения и управления данными из определения БД2.

В состав модели данных включаются

- количество типов данных
- множество допустимых операций с данными каждого типа
- ограничения, принятые с целью целостности данных

Целостность данных – это механизм поддержания соответствия базы данных предметной области.

Выделяют три основные модели данных

- Иерархическая модель данных
- Сетевая модель данных
- Реляционная модель данных

В **иерархической модели данных** каждая характеристика объекта (сущности)является объектом со своим набором характеристик, которые тоже являются объектами и т.д.

Связи между характеристиками и объектами образуют «дерево» (иерархию), встречающееся при описании любых организованных структур (пример – структура любых каталогов).

Если ввести понятия **«объект-предок»** и **«объект-потомок»**, то в данной модели у каждого потомка – только один предок.

Данные, организованные по иерархической модели, требуют больших затрат на поиск информации вследствие различий в количестве ветвей на каждом уровне иерархии и длины ветвей «дерева» (количества уровней иерархии для ветвей). Пример иерархического описания для сущности «информационные системы» показан на рис. 5.

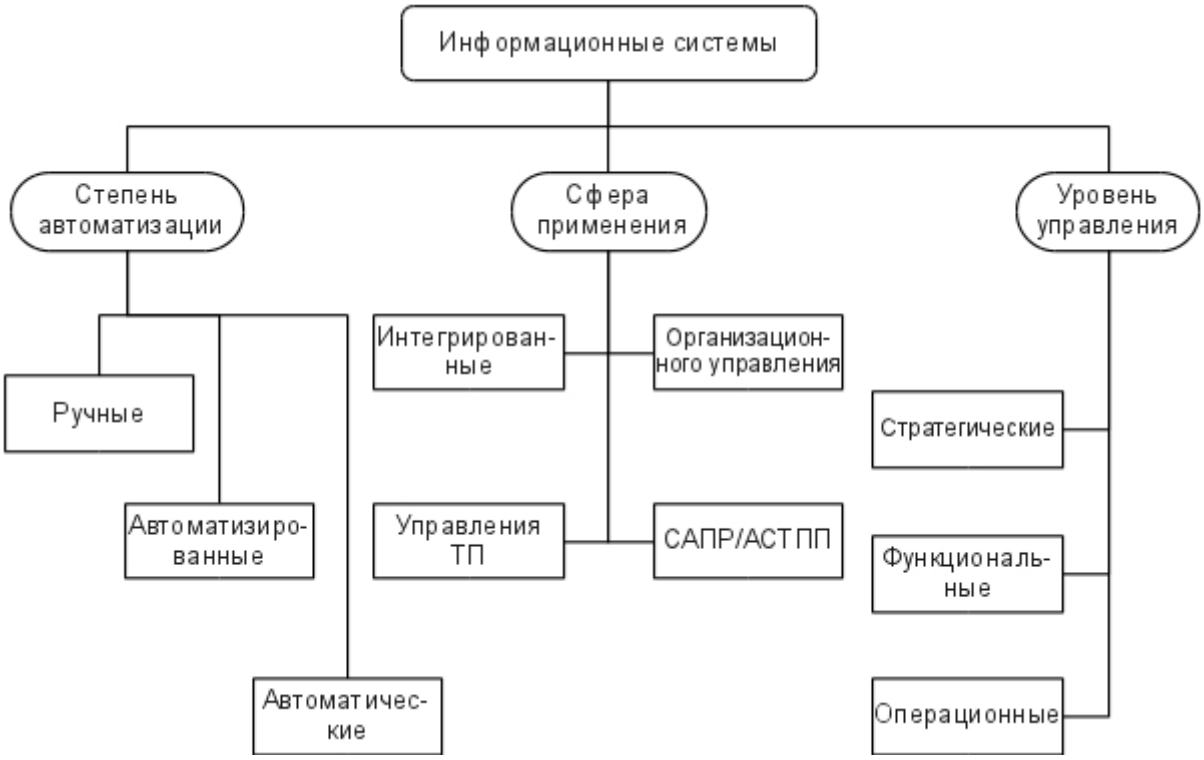

Рис. 5. Иерархическая организация атрибутов сущности «Информационные системы»

В **сетевой модели данных** каждая характеристика (атрибут) какого-либо объекта (сущности) может быть связаны с атрибутами других сущности по другим признакам классификации.

Сетевая структура данных может быть образована из иерархической, если появляются перекрестные связи.

В данной модели у каждого потомка может быть более одного предка.

Примером сетевой структуры данных может быть организация информации в World-Wide Web (семантическая сеть).

Такие структуры данных также неудобны для автоматической обработки.

Пример сетевой модели связи атрибутов сущности «Информационные системы» показан на рис. 6.

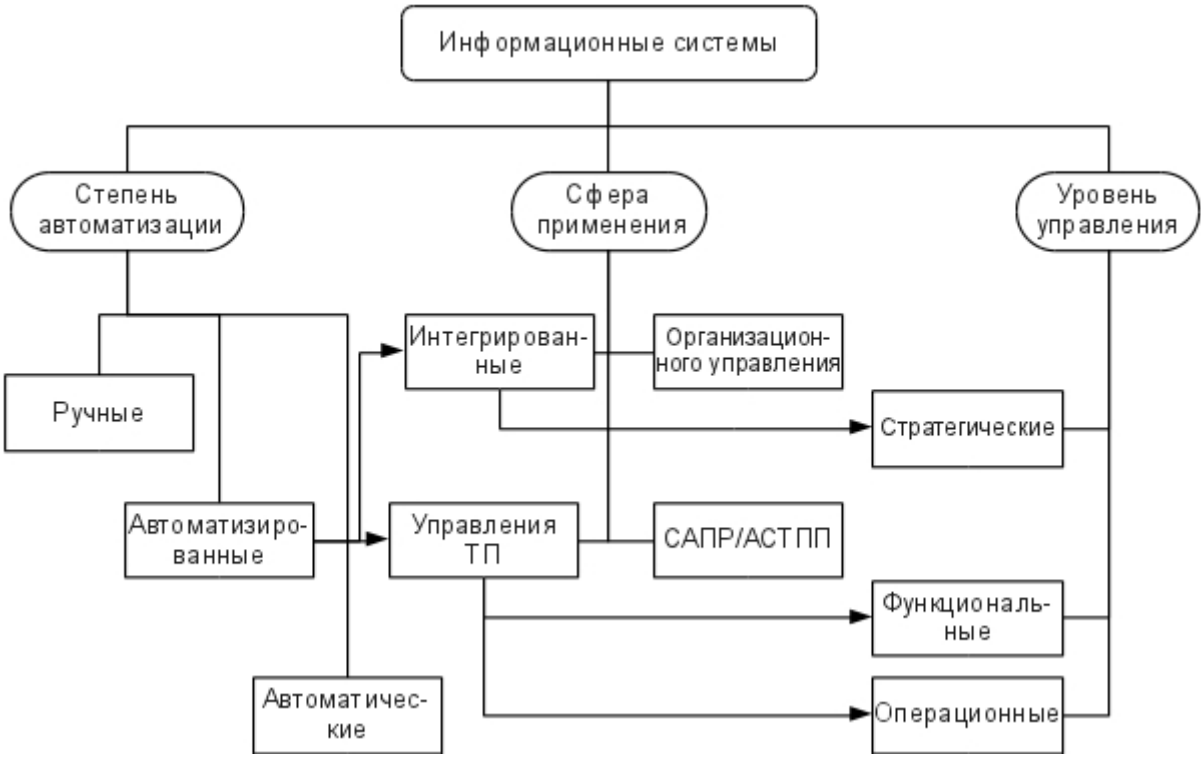

Рис. 6. Сетевая организация атрибутов сущности «Информационные системы»

В реляционной модели данных информация организуется в виде таблиц, каждая таблица описывает экземпляры одной сущности. Другими словами, в таблицах содержатся характеристики однородных объектов.

Для каждого экземпляра сущности (объекта) выделяется отдельная строка – **запись** (кортеж), а характеристики объектов записываются по столбцам, которые называются **полями** (доменами, атрибутами).

Такие таблицы легко обрабатываются компьютером, так как заранее известно, что и где искать (в файле определены позиции данных того или иного типа).

Для реляционной модели характерны следующие основные свойства:

- В таблице не может быть двух одинаковых строк. В математике таблицы, обладающие таким свойством, называют отношениями – (*relation*), отсюда и название – реляционные.
- Столбцы располагаются в определённом порядке, который создается при создании таблицы. В таблице может не быть ни одной строки, но обязательно должен быть хотя бы один столбец.
- У каждого столбца есть уникальное имя (в пределах таблицы), и все значения в одном столбце имеют один тип (число, текст, дата...).
- На пересечении каждого столбца и строки может находиться только атомарное значение (одно значение, не состоящее из группы значений). Таблицы, удовлетворяющие этому условию, называют нормализованными.

Пример реляционной таблицы для сущности «Информационные системы» показан на рис. 7.

Код	Название	Автоматизация	Применение
001	Галактика	Автоматизированная	Стратегическая
002	OpenSCADA	Автоматизированная	Функциональная
003	Резак	Автоматическая	Операционная
004	1С:Склад	Автоматизированная	Функциональная

Рис. 7. Реляционная таблица для сущности «Информационные системы»

В реляционной модели существует важное понятие **ключа отношения** (**ключевого поля** или **ключевой комбинации полей**).

Первичный ключ (**Primary key, PK**) – атрибут или комбинация атрибутов,, значения которого во всех строках различны. Первичные ключи могут быть логическими (естественными) и суррогатными (искусственными). Наличие ключа – требование *целостности сущности*.

Естественный ключ содержится в самих данных (например, номер паспорта). Однако проблема состоит в том, что со временем многие характеристики атрибутов сущности (объектов предметной области) могут изменяться (паспорт может быть заменён).

Искусственный ключ вводится дополнительно для каждого объекта таблицы как уникальное значение. На рис. 7 показан столбец «Код», в котором содержатся значения искусственного ключа.

Внешний ключ (Foreign Key, FK) – дополнительное поле, позволяющее по значениям из текущей таблицы получать данные из другой таблицы по значению первичного ключа (**связывание таблиц**).

Постреляционная модель данных представляет собой расширенную реляционную модель, в которой отменено требование атомарности атрибутов.

Она использует трёхмерные структуры, позволяя хранить в полях таблицы другие таблицы («многомерная база данных»).

Такой подход расширяет возможности по описанию сложных объектов реального мира и частично снимает необходимость связывания таблиц.

Нормализация в реляционной модели данных

В реляционной модели таблицы должны быть представлены в одной из **нормальных форм**. Как правило, выделяют следующие нормальные формы

- Первая нормальная форма (1NF, 1НФ)
- Вторая нормальная форма (2NF, 2НФ)
- Третья нормальная форма (3NF, 3НФ)

- Нормальная форма Бойса-Кодда (BKNF, НФБК)
- Четвёртая нормальная форма (4NF, 4НФ)
- Пятая нормальная форма (нормальная форма проекции-соединения, 5NF, PJ/NF, 5НФ).

Четвёртая и пятая нормальные формы в реальных задачах встречаются редко, потому при рассмотрении нормализации (приведения описания сущности в ту или иную нормальную форму) на этих НФ останавливаться не будем.

В качестве примера рассмотрим отношение «Научная_работа», в котором приведены описания сотрудников, участвующих в научно-исследовательских работах (НИР) и выполняющих в рамках той или иной НИР определённые задачи. Каждый сотрудник имеет табельный номер и должность. Каждый сотрудник участвует в одной или нескольких НИР и за участие в каждой НИР получает отдельную надбавку, которая зависит только от должности сотрудника. Каждый сотрудник может в рамках одной НИР выполнять только одну задачу.

Первая нормальная форма (1NF, 1НФ) для описанного отношения получается тогда, когда все атрибуты атомарны и существует ключ сущности. Ключом в данном случае является комбинация табельного номера и кода НИР. По табельному номеру однозначно определяется должность, от которой зависит надбавка.

Схема данных отношения «Научная_работа» показана на рис. 8 (ключевая комбинация атрибутов обведена рамкой), а соответствующая таблица данных — на рис. 9.

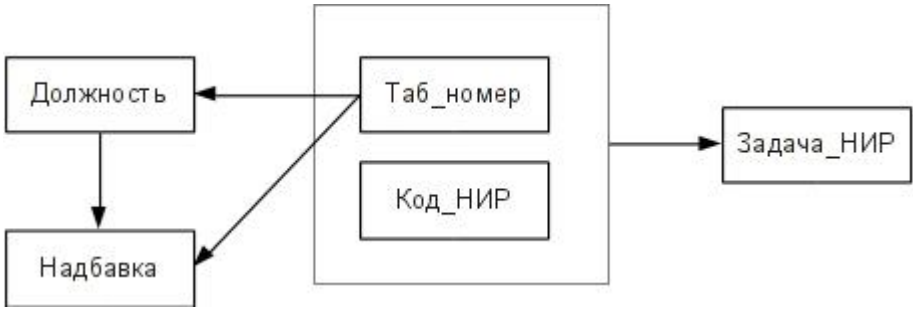

Рис. 8. Схема данных отношения «Научная_работа»

Таб_номер	Должность	Надбавка	Код_НИР	Задача_НИР
62315	Ассистент	8000	1	A
62316	Доцент	12000	1	B
62323	Ассистент	8000	1	C
62331	Профессор	16000	1	D
62315	Ассистент	8000	2	D
62316	Доцент	12000	2	C
62323	Ассистент	8000	2	B
62331	Профессор	16000	2	A

Рис. 9. Таблица для отношения «Научная_работа».

Вторая нормальная форма (2NF, 2НФ) может быть получена, если таблица находится в 1НФ, повторяющиеся значения неключевых атрибутов выносятся во внешнюю таблицу (справочник).

В рассматриваемом примере такими повторяющимися значениями являются должность и надбавка, определяемые табельным номером. Поэтому имеет смысл выделить отдельное отношение «Сотрудники» и упростить отношение «Научная_работа», превратив его в отношение «НИР_Задачи», как показано на рис. 10.

Сотрудники

Таб_номер	Должность	Надбавка
62315	Ассистент	8000
62316	Доцент	12000
62323	Ассистент	8000
62331	Профессор	16000

НИР_Задачи

Таб_номер	Код_НИР	Задача_НИР
62315	1	A
62316	1	B
62323	1	C
62331	1	D
62315	2	D
62316	2	C
62323	2	B
62331	2	A

Рис. 10. База данных по научной работе в 2НФ.

Однако нужно заметить, что отношение «Сотрудники» устроено таким образом, что по табельному номеру однозначно определяется должность, а из должности — величина надбавки (должность зависит от табельного номера, а величина надбавки — от должности). Это означает, что величину надбавки можно узнать просто по табельному номеру. Такие зависимости называются **транзитивными**.

Третья нормальная форма (3NF, 3НФ) получается, когда база данных находится в 2НФ, справочники организуются так, что исключаются транзитивные зависимости. В нашем случае отношение «Сотрудники» для исключения транзитивных зависимостей может быть разделено на отношения «Сотрудники1» и «Шкала_надбавок» (рис. 11).

Нормальная форма Бойса-Кодда (BCNF, НФБК) получается, когда база данных находится в 3НФ и в отношениях исключаются возможные перекрывающиеся ключи.

Если в первоначальной таблице для сущности «Научная_работа» добавить атрибут «Фамилия» (рис. 12), то получим схему данных, показанную на рис. 13.

Сотрудники1

Таб_номер	Должность
62315	Ассистент
62316	Доцент
62331	Профессор

Шкала_надбавок

Таб_номер	Надбавка
62315	8000
62316	12000
62331	16000

Рис. 11. Устранение транзитивных зависимостей в отношении «Сотрудники».

Таб_номер	Фамилия	Должность	Надбавка	Код_НИР	Задача_НИР
62315	Петрова	Ассистент	8000	1	A
62316	Корнеев	Доцент	12000	1	B
62323	Привалов	Ассистент	8000	1	C
62331	Выбегалло	Профессор	16000	1	D
62315	Петрова	Ассистент	8000	2	D
62316	Корнеев	Доцент	12000	2	C
62323	Привалов	Ассистент	8000	2	B
62331	Выбегалло	Профессор	16000	2	A

Рис. 12. Отношение «Научная_работа» с фамилиями сотрудников.

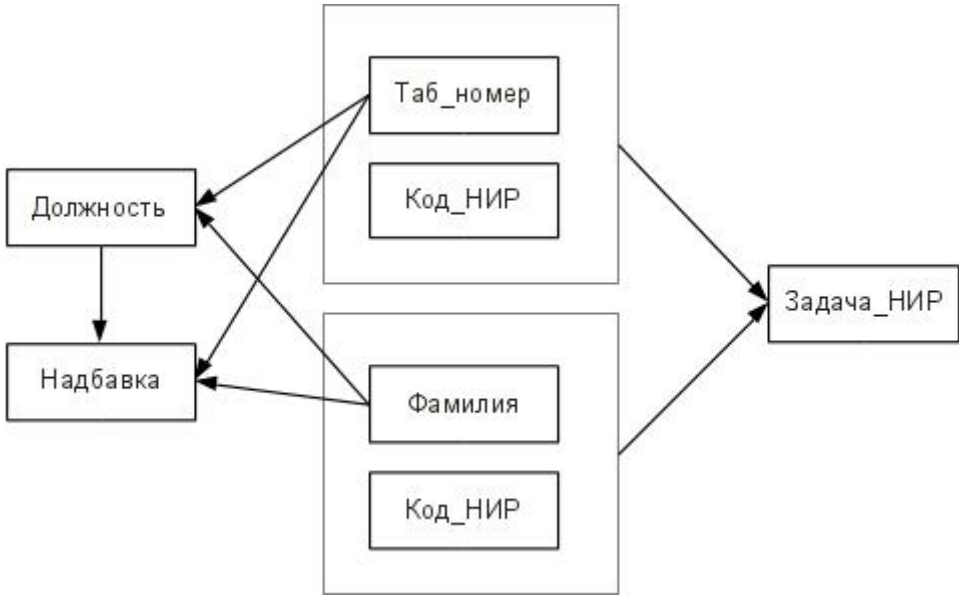

Рис. 13. Схема данных отношения «Научная_работа» с перекрывающимися ключами.

Тогда в базе данных изменяется справочник сотрудников (отношение «Сотрудники2») и отношения будут выглядеть следующим образом (рис. 14).

Сотрудники2

Таб_номер	Фамилия	Должность
62315	Петрова	Ассистент
62316	Корнеев	Доцент
62323	Привалов	Ассистент
62331	Выбегалло	Профессор

Шкала_надбавок

Должность	Надбавка
Ассистент	8000
Доцент	12000
Профессор	16000

НИР_Задачи

Таб_номер	Код_НИР	Задача_НИР
62315	1	A
62316	1	B
62323	1	C
62331	1	D
62315	2	D
62316	2	C
62323	2	B
62331	2	A

Рис. 14. Модификация базы данных при устранении перекрывающихся ключей.

Типы данных в базах данных

В таблице реляционной базы данных каждый атрибут сущности (объекта предметной области) должен иметь один и тот же тип данных для всех экземпляров сущности.

Основные типы данных, используемые в реляционных базах данных, можно определить следующим образом:

- Текст – строка от 1 до 256 символов
- Большой текст – последовательность символов длиной до 64 кбайт
- Число – целое или с плавающей точкой;
- Дата/время – структура, состоящая из чисел и содержащая номер года, номер месяца, день, час, минуту и секунду
- Логическое значение (Boolean) – возможны только два значения: TRUE (истина) и FALSE (ложь)
- Большой двоичный объект (BLOB – Binary Large Object) – набор байтов произвольного размера. В поле такого типа могут храниться графические файлы (рисунки), фрагменты программного кода, объекты мультимедиа (аудио- или видео-фрагменты). Данные этого типа обрабатываются программами, внешними по отношению к базе данных.

Системы управления базами данных (СУБД)

Системы управления базами данных (СУБД) – специальные программы для создания, изменения и поиска информации в базах данных.

СУБД должна обладать следующими необходимыми возможностями:

- Возможность определения структуры файла данных
- Возможность проверки соответствия типов данных (целостности данных) при их вводе
- Возможность поиска информации по заданным признакам и представления результатов поиска в удобном для пользователя виде
- Возможность защиты данных от несанкционированного доступа
- Возможность создания резервных копий данных и экспорта данных в файлы стандартных форматов

Выбор СУБД для конкретного применения определяется следующими критериями:

- Свойства базы (количество полей и записей в таблице, типы данных в полях таблицы, наличие и количество связанных таблиц)
- Количество пользователей, которые должны одновременно работать с базой данных

Исходя из этих критериев, можно определить классы программ, применимых для различных вариантов работы с базами данных.

Простейшая база данных – список, с которым работает один пользователь — является одним из граничных случаев базы данных.

Типовые характеристики базы: до 256 полей, до 65 000 записей, типы данных – текст, числа и дата/время.

Для обработки такой базы можно использовать любую программу **табличного процессора** (**электронную таблицу**) из доступных офисных пакетов.

Промышленная база данных является другим граничным случаем базы данных.

Это база данных с многопользовательским сетевым доступом.

Характеристики базы: размер таблицы ограничен только объёмом дискового пространства, в полях таблиц – все возможные типы данных, количество связанных таблиц ограничено только объёмом дискового пространства.

Для обработки таких баз используются **серверы баз данных (SQL-серверы)**.

После появления персональных компьютеров возникла необходимость обрабатывать на них достаточно сложные базы данных, в то время как ресурсов для установки SQL-сервера не хватало.

Тогда появились программы, в какой-то мере обеспечивающие работу с многотабличными базами (**СУБД для ПК**). Они используются для обработки многотабличных баз одним пользователем и являются промежуточным вариантом между простейшей и промышленной базами данных.

Типовые характеристики базы: размер таблицы – до 256 полей, до 65 000 записей, в таблице – все типы данных, одновременно может обрабатываться несколько таблиц (обычно до 16).

Однако ресурсы современных ПК таковы, что вполне возможна установка одного или даже нескольких SQL-серверов, что обеспечивает гораздо более высокую надёжность и функциональность, чем использование СУБД для ПК.

Современная тенденция переноса хранения данных в Интернет («облачные» сервисы), большое количество доступных для использования вариантов SQL-серверов с удобными пользовательскими интерфейсами к ним лишает этот класс программ всякого смысла.

Запросы как элемент базы данных

В общем случае можно выделить следующие компоненты базы данных:

- **Таблицы** содержат информацию о характеристиках объектов предметной области (записи).
- **Формы** обеспечивают удобный ввод и просмотр информации в таблицах.
- **Запросы** обеспечивают выбор нужной пользователю информации из таблиц.
- **Отчёты** как результаты запросов, представленные в виде форматированных документов.

Запрос – это команда на выбор информации из базы данных по определённым признакам (критериям) для программы, работающей с базой данных.

- **Фильтр** – простейший вариант запроса, применяется в электронных таблицах и СУБД для ПК.
- **QBE-запрос** (Query By Example) – применяется в СУБД для ПК и иногда при работе с серверами баз данных.
- **SQL-запрос** (Standard/Structured Query Language) – основный вид запросов при работе с серверами баз данных (SQL-серверами).

При рассмотрении запросов будем использовать уже описанную выше базу данных по научной работе, а также простую базу данных по поставкам товаров (рис. 15).

group	tn_code	tov_name	tov_pack	price	qty	cost	tov_country	stavka	nalog
18	1805000000	Какао «Нестле»	Ящик	254	10	2540	Швейцария	0,23	584,2
18	1803200000	Паста шоколадная «O'Hoj»	Ящик	317	8	2536	Финляндия	0,23	583,28
18	1806901900	Конфеты Fazer Dumle	Контейнер	2563	2	5126	Финляндия	0,38	1947,9
18	1806321000	Шоколад «AlpenGold» с фундуком	Паллета	789	3	2367	Швейцария	0,38	899,46
18	1801000000	Какао-бобы жареные	Ящик	173	5	865	Мозамбик	0,18	155,7
18	1806907000	Напиток «Горячий шоколад»	Контейнер	2340	1	2340	Дания	0,38	889,2
18	1802000000	Шелуха какао	Паллета	340	2	680	Мозамбик	0,23	156,4
18	1806901100	Конфеты «Пьяная вишня»	Ящик	350	15	5250	Дания	0,38	1995
18	1806329000	Шоколад чёрный Lindt	Контейнер	3200	2	6400	Швейцария	0,38	2432
18	1804000000	Какао-масло	Паллета	290	3	870	Мозамбик	0,15	130,5
82	8206000000	Набор слесарный	Контейнер	4356	2	8712	Швеция	0,23	2003,8
82	8210000000	Мясорубка ручная	Ящик	478	10	4780	Китай	0,33	1577,4
82	8201100000	Лопаты штыковые «STIHL»	Паллета	890	6	5340	Канада	0,33	1762,2
82	8201600000	Ножницы садовые	Контейнер	4200	2	8400	Китай	0,33	2772
82	8207509000	Наборы свёрл «BRAUN»	Паллета	600	4	2400	ФРГ	0,23	552
82	8214200000	Пилки для ногтей	Контейнер	8000	1	8000	Китай	0,33	2640
82	8215991000	Ножи для разделки рыбы «BRAUN»	Ящик	467	5	2335	ФРГ	0,33	770,55
82	8201300000	Тяпки «Alaska»	Паллета	860	3	2580	Канада	0,33	851,4
82	8201400000	Топоры «Hugsvarna»	Ящик	300	4	1200	Финляндия	0,33	396
82	8214100000	Точилки «Erih Krause»	Ящик	450	15	6750	Финляндия	0,33	2227,5

Рис. 15. Простая база данных по импортируемым товарам.

Фильтры позволяют пользователю наглядно устанавливать признаки выбора данных из таблиц.

Самый простой вариант фильтра — **Автофильтр**. Включается с помощью команд главного меню электронной таблицы (указатель активной ячейки должен находиться внутри диапазона, занимаемого базой данных). При включённом Автофильтре в строке с заголовками полей появляются значки раскрывающегося списка, по любому столбцу можно устанавливать значения, в результате будут показываться строки, в которых значения в этом столбце (поле) соответствует выбранному. Можно использовать Автофильтр одновременно для нескольких столбцов (полей). Признаком наличия фильтра является изменения вида кнопок раскрывающихся списков.

На рис. 16 показан выбор товаров в ящиках, импортированных из Финляндии, реализованный с помощью Автофильтра.

gro	tn_code	tov_name	tov_pa	pri	q	co	tov_coun	stav	nal
18	1803200000	Паста шоколадная «O'Hoj»	Ящик	317	8	2536	Финляндия	0,23	583,28
82	8201400000	Топоры «Hugsvarna»	Ящик	300	4	1200	Финляндия	0,33	396
82	8214100000	Точилки «Erih Krause»	Ящик	450	15	6750	Финляндия	0,33	2227,5

Рис. 16. Применение Автофильтра к базе данных в электронной таблице.

Стандартный (пользовательский) фильтр позволяет в диалоговом окне указать наименования полей, значения, которые нужно выбирать из этих полей (возможно использование символов подстановки, например * – любая последовательность символов, **?** – любой одиночный символ), а также связывать условия для различных полей логическими функциями И и ИЛИ. Следует отметить, что нельзя использовать обе логические функции одновременно. Для каждого набора критериев можно использовать только один вариант логической функции.

Пример стандартного фильтра для базы данных по импортируемым товарам показан на рис. 17.

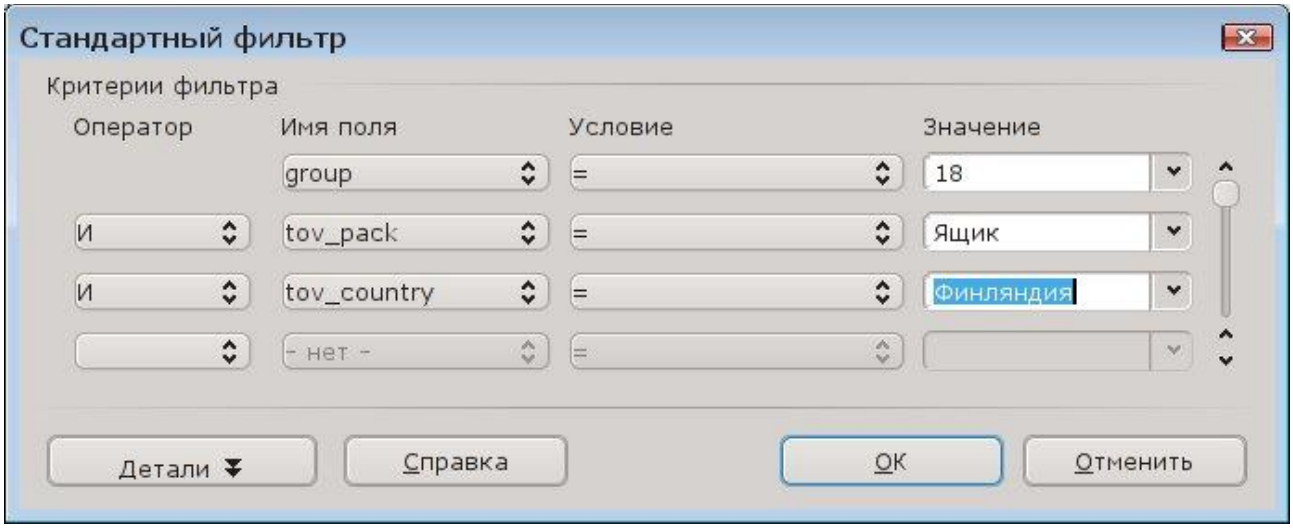

Рис. 17. Пример стандартного (пользовательского) фильтра.

QBE-запросы (запрос по шаблону/образцу) применяются при работе с СУБД для ПК и при работе с различными интерфейсными программами для SQL-серверов.

При создании запроса устанавливаются признаки (шаблоны) для поиска по любому количеству полей.

В шаблонах используются символы подстановки (**метасимволы**), например * – любая последовательность символов, **?** – любой одиночный символ.

Если условия располагаются в одной строке запроса, они связаны логической функцией «И», а если в разных – то функцией «ИЛИ».

На рис. 18 показан пример запроса по базе данных импортируемых товаров, в котором выводятся наименования товаром и страны происхождения

для налоговой нагрузки в диапазоне от 15% до 25%.

Поле	tov_name	tov_country	stavka	stavka
Псевдоним				
Таблица	Лист1	Лист1	Лист1	Лист1
Сортировка				
Видимый	☑	☑	☑	☐
Функция				
Критерий			>= 0,15	< 0,25
Или				

Рис. 18. Пример QBE-запроса для БД по импортируемым товарам.

На рис. 19 показан результат выполнения такого запроса по исходным данным рис. 15.

	tov_name	tov_country	stavka
▶	Какао «Нестле»	Швейцария	0,23
	Паста шоколадная «O'Hoj»	Финляндия	0,23
	Какао-бобы жареные	Мозамбик	0,18
	Шелуха какао	Мозамбик	0,23
	Какао-масло	Мозамбик	0,15
	Набор слесарный	Швеция	0,23
	Наборы свёрл «BRAUN»	ФРГ	0,23

Рис. 19. Пример результатов QBE-запроса.

Если база данных находится в нормальной форме со справочниками (2НФ, 3НФ или НФБК), то для показа полного набора данных в запросе производится связывание таблиц по внешним ключам. На рис. 20 показан пример связывания таблиц для базы данных по научной работе, описанной выше.

Запрос по связанным таблицам позволяет проводить некоторые вычисления.

Пример запроса, показывающего общую сумму надбавок по всем проектам для сотрудников, имеющих надбавки по каждой НИР более 1000 руб, показан на рис. 21.

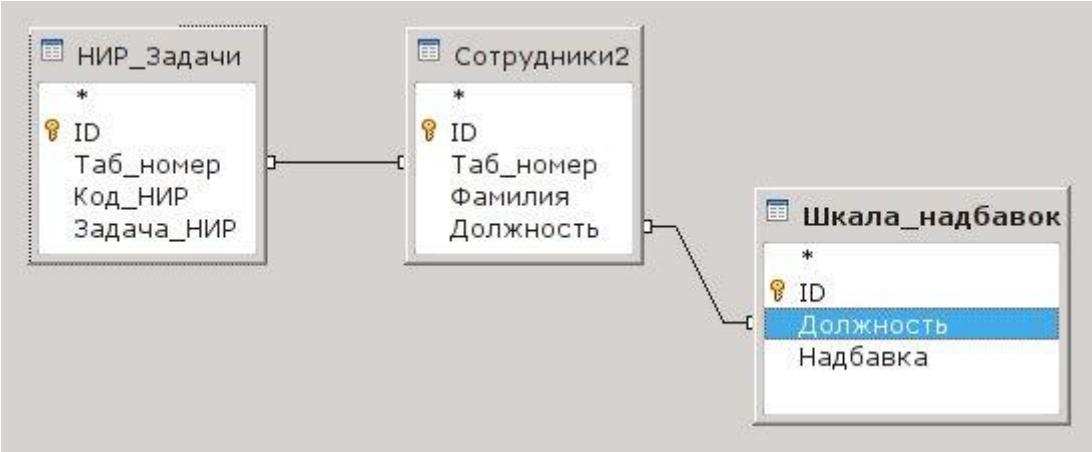

Рис. 20. Пример связывания таблиц в СУБД для ПК.

Поле	Код_НИР	Задача_НИР	Фамилия	Надбавка	Надбавка
Псевдоним					
Таблица	НИР_Задачи	НИР_Задачи	Сотрудники2	Шкала_надбавок	
Сортировка					
Видимый	☑	☑	☑	☑	☐
Функция	Group	Group	Group	Сумма	
Критерий					> 10000
Или					

Рис. 21. Пример QBE-запроса с вычислениями по связанным таблицам.

Результат запроса на основе данных из приведённого выше примера показан на рис. 22.

	Код_НИР	Задача_НИР	Фамилия	SUM("Шкала_надбавок"."Надбавка")
▷	1	B	Корнеев	12000
	2	C	Корнеев	12000
	1	D	Выбегалло	16000
	2	A	Выбегалло	16000

Рис. 22, Результат QBE-запроса по связанным таблицам.

SQL-запросы используются в основном при работе с серверами баз данных (SQL-серверами), но могут использоваться и в некоторых СУБД для ПК (например Apache OpenOffice Base или LibreOffice Base).

SQL – это стандартизованный язык запросов к базам данных.

Запрос на SQL представляет собой небольшую программу, которая интерпретируется и выполняется SQL-сервером.

Для примера, показанного на рис. 20, SQL-запрос может выглядеть следующим образом:

```
SELECT "НИР_Задачи"."Код_НИР", "НИР_Задачи"."Задача_НИР",
"Сотрудники2"."Фамилия", SUM( "Шкала_надбавок"."Надбавка" ) FROM
"Сотрудники2", "НИР_Задачи", "Шкала_надбавок" WHERE
"Сотрудники2"."Таб_номер" = "НИР_Задачи"."Таб_номер" AND
"Шкала_надбавок"."Должность" = "Сотрудники2"."Должность" AND
"Шкала_надбавок"."Надбавка" > 10000 GROUP BY
"НИР_Задачи"."Код_НИР", "НИР_Задачи"."Задача_НИР",
"Сотрудники2"."Фамилия"
```

Общие принципы создания SQL-запросов и их синтаксис описывается в семействе стандартов **ISO/IEC 9075.** За время после принятия первого стандарта на SQL было принято несколько спецификаций:

- SQL-86
- SQL-92
- SQL-99
- SQL:2003
- SQL:2008.

Сейчас для общего описания SQL действует ISO/IEC 9075-1:2008 (SQL-2008).

Каждая следующая версия включает в себя все возможности предыдущей версии стандарта. Таким образом, при работе с современными SQL-серверами можно использовать SQL-92, но нет гарантий, что использование SQL-2008 возможно для всех вариантов SQL-серверов.

Поскольку SQL-запросы являются по сути программами (сценариями), то их создание и выполнение легко автоматизировать, их можно включать в какие-то прикладные автоматизированные системы и использовать даже при работе с SQL-серверами, связь с которыми осуществляется через компьютерные сети.

Выделяются следующие варианты SQL-запросов

- Запросы на создание/удаление БД
- Запросы на подключение к БД
- Запросы на создание/удаление таблиц
- Запросы на выборку
- Запросы на изменение
- Запросы на создание/удаление привилегий

Несмотря на наличие нескольких диалектов SQL, зная принцип и имея справочник всегда можно правильно построить запрос.

Запросы на создание/удаление БД обычно требует привилегий администратора базы данных. Для создания БД с именем baza1 используется команда

CREATE DATABASE baza1;

а для удаления БД — команда

DROP DATABASE baza1;

(наличие символа «;» в конце строки обязательно).

При составлении SQL-запросов принято записывать ключевые слова языка прописными буквами, а имена объектов и значения переменных — строчными.

Запрос на подключение к БД может выполняться с привилегиями любого пользователя и применяется при обращении к серверу через компьютерную сеть

CONNECT TO baza1 USER vasya/12345;

Здесь строка после ключевого слова USER — имя и пароль пользователя базы данных. Пароль передаётся в открытом виде, поэтому сеансы связи с SQL-серверами рекомендуется шифровать (см. далее).

Запросы на создание таблиц описывают все поля и из типы, а также устанавливают (при необходимости) значения по умолчанию, если значения не могут отсутствовать (NOT NULL). Например, для таблицы «Шкала_надбавок» с искусственным ключом запрос на создание будет выглядеть примерно так:

CREATE TABLE Шкала_надбавок (id INT(4) UNSIGNED NOT NULL, Должность CHAR(20) DEFAULT 'Ассистент' NOT NULL, Надбавка INT(6) DEFAULT '0' NOT NULL, PRIMARY KEY(id));

Запросы на удаление таблиц требует только указания имени таблицы. Полезно также использовать условие «IF EXIST», которое обеспечивает корректную обработку попытки удаления несуществующей таблицы:

DROP TABLE IF EXIST Шкала_надбавок;

Запросы на создание пользователей требуют привилегий администратора БД (или сервера БД). В запросе указывается база данных, набор привилегий (перечисляется через запятую) и параметры учётной записи пользователя — имя, узел сети Интернет, на котором этот пользователь зарегистрирован, а также пароль. Пароль указывается в открытом виде.

Пример запроса на создание пользователя:

GRANT SELECT,INSERT,UPDATE,DELETE,CREATE,DROP ON scienceworks.* TO vasya@localhost IDENTIFIED BY '12345';

Запросы на удаление пользователей не имеют каких либо особенностей и сложностей. Например

DROP USER vasya;

Запросы на выборку являются самым часто используемым вариантом запросов.

Самый простой вариант

SELECT * FROM tovary;

выводит все данные, содержащиеся в таблице (в данном примере возвращаемся к базе данных по импортируемым товарам).

Запрос

SELECT * FROM tovary WHERE group='18' ORDER BY tov_country DESC;

выводит товары группы 18 по ТН ВЭД, отсортированные по странам происхождения в обратном алфавитном порядке.

Запрос

SELECT COUNT(tov_pack) FROM tovary WHRER tov_country LIKE '%Франция%' AND tov_pack LIKE '%Ящик%';

выведет количество ящиков с товарами, импортированными из Франции. В реализациях SQL в качестве символа подстановки «любая последовательность символов» используется знак «%».

Запросы на изменение позволяют добавлять данные в таблицы и изменять (обновлять) некоторые значения атрибутов.

Для добавления, как правило, используется вариант

INSERT INTO tovary (group, tn_code, ...) VALUES ('18','18302100',...);

(требуется указание всех имён полей и всех соответствующих значений, поэтому поставлены многоточия). При использовании запроса INSERT нужно быть уверенным, что запись не будет продублирована. Поэтому в качестве варианта запроса на добавления данных можно использовать конструкцию

REPLACE INTO tovary (id, group, tn_code, ...) VALUES (211, '18','18302100',...);

В этом случае, если запись с таким значением id (ключа) существует, значения атрибутов буду заменены, а если не существует, запись будет добавлена.

Для обновления значений отдельных атрибутов используется команда UPDATE, например

UPDATE tovary SET price=4523 WHERE id=208;

(изменение значения атрибута price для записи с указанным значением ключевого поля id).

Банки данных: Понятие и структура

Банк данных – совокупность баз данных, а также программные, языковые и другие средства, предназначенные для централизованного накопления данных и их использования с помощью ЭВМ.

В широком смысле **Банк данных (БнД)** – это некоторая автоматизированная информационная система (АИС), включающая в себя все все виды обеспечения информационных систем (см. главу «Понятие АИС, обеспечивающие подсистемы АИС»).

Обобщённая структура банка данных показана на рис. 23.

Рис. 23. Состав банка данных.

- **Администратор банка данных:** управляет БнД
- **Словарь данных:** специальная система в составе БнД, предназначенная для хранения единообразной информации обо всех ресурсах данных конкретного банка. В словаре содержатся сведения об объектах, их свойствах и отношениях для данной ПО, сведения о данных, хранимых в базе (наименования данных, их структуре, связи с другими данными), об их возможных значениях и форматах представления, об источниках их возникновения, о кодах защиты, разграничениях доступа к данным со стороны пользователей
- **СУБД:** реализует централизованное управление данными, хранимыми в базе, доступ к ним, поддерживает их в состоянии, соответствующем состоянию ПО

Среди задач, которые решаются при использовании банков данных, можно выделить следующие:

- Удовлетворение актуальных информационных потребностей внешних пользователей, обеспечение возможности хранения и модификации больших объёмов многоаспектной информации
- Обеспечение заданного уровня достоверности хранимой информации
- Обеспечение доступа к данным только пользователям с соответствующими полномочиями
- Обеспечение возможности поиска информации по произвольной группе признаков
- Соответствие заданным требованиям по производительности при обработке запросов
- Возможность реорганизации и расширения при изменении границ предметной области
- Выдача информации пользователю в различной форме
- Обеспечение простоты и удобство обращения внешних

пользователей за информацией

• Возможность одновременного обслуживания большого числа внешних пользователей.

Информационное взаимодействие АИС. Web-сервисы.

Обмен данными между базами данных различных информационных системам — необходимое условие работы современных АИС. Для обеспечения такого обмена могут использоваться различные технологии. Ниже рассмотрим основные варианты организации информационного обмена с кратким анализом их особенностей.

Обмен данными в виде структурированных текстовых файлов (comma separated values — CSV). Результаты запроса или таблица БД в одной АИС экспортируются (выгружаются) в такой файл, затем файл пересылается в другую АИС, после чего импортируется в целевую базу данных. При такой технологии обеспечиваются минимальные накладные расходы в виде избыточного объёма данных, но можно работать только с атомарными атрибутами. Выгрузка и загрузка требуют либо участия оператора, либо создания дополнительных сценариев для автоматизации этих действий.

Обмен данными в виде файлов электронных таблиц (ЭТ) принципиально не отличается от предыдущего варианта, однако возрастают накладные расходы, поскольку в файле ЭТ содержится информация о форматировании и структуре документа. Соответственно, усложняется автоматизация процессов выгрузки и загрузки данных (особенно при использовании нестандартных форматов фалов ЭТ).

SQL-запросы к внешним базам данных обеспечивают прямое получение данных с помощью командной оболочки СУБД одной АИС из таблиц баз данных другой АИС с помощью запросов типа CONNECT и SELECT (при наличии соответствующих прав доступа). Соответственно, требуются организационные меры по обеспечению удалённого доступа к БД и соответствующие настройки сервера БД. Кроме того, поскольку при подключении пароль передаётся в открытом виде, требуется обеспечить информационную безопасность. Однако данная технология является достаточно эффективной и может быть использована в изолированных сетях.

XML-RPC (сокращение от *Extensible Markup Language Remote Procedure Call* — XML-вызов удалённых процедур) — стандарт/протокол вызова удалённых процедур, использующий представление информации в виде XML-описаний для кодирования сообщений и протокол HTTP для передачи сообщений. В качестве сообщений могут использоваться запросы к базам данных, доступ к которым осуществляется с помощью трансляции инструкций, получаемых в виде сообщений Web-сервером с помощью языков сценариев Web-сервера к серверу баз данных. XML-сообщение, передаваемое в виде HTTP-запроса, декодируется языком сценариев, и получившийся в результате

декодирования SQL-запрос обрабатывается сервером баз данных. Результаты выполнения SQL-запроса транслируются в XML-сообщение, возвращаемое Web-сервером в качестве ответа на HTTP-запрос. Комплекс программ, обеспечивающий обработку таких запросов, называется Web-сервисом (Web-службой). Здесь не происходит прямого удалённого обращения к базе данных и нет промежуточных файлов, поэтому такая технология является достаточно безопасной и процесс легко автоматизируется. Существенным недостатком является использование протокола HTTP, который не обеспечивает шифрование данных.

Развитием технологии XML-PRC является технология **SOAP** (*Simple Object Access Protocol* — простой протокол доступа к объектам), в которой для информационного обмена используются различные протоколы прикладного уровня стека TCP/IP (FTP, HTTP, HTTPS). Кроме того, для Web-сервисов используется и другие технологии с высоким уровнем абстракции - **WSDL** (*Web Services Description Language – язык описания web-сервисов*) и **WDDX** (*Web Distributed Data eXchange* — обмен данными, распределёнными во Всемирной паутине), независимые от языков программирования, программных платформ и протоколов прикладного уровня стека TCP/IP.

Технологии криптографической защиты информации

Криптографическая защита информации — один из способов обеспечения конфиденциальности данных с помощью шифрования.

Конфиденциальность данных – защищённость данных от попытки их раскрытия (предотвращение вмешательства и наблюдения за данными при передаче).

Шифрование – один из способов обеспечения **конфиденциальности данных**. Для шифрования в настоящее время используются два метода: криптография и стеганография

Стеганография (тайнопись – steganography) – методы маскировки сообщений в других сообщениях (скрытие текста сообщения в содержании другого текстового или графического сообщения).

Криптография – наука о преобразовании сообщений по определённым правилам (алгоритмам), которые делают их невозможными для несанкционированного использования. Криптография определяется как совокупность трёх различных механизмов: **шифрование симметричными ключами**, **шифрование асимметричными ключами** и **хэширование**.

Ключ – набор значений (чисел), которыми оперирует алгоритм шифровки.

В криптографии существуют так называемые принципы Керкгоффса, состоящие в следующем:

- алгоритм кодирования/дешифрования известен всем

- ключ должен быть настолько труден, что не надо скрывать алгоритм кодирования/дешифрования

В современной криптографии существует конечное число эффективных алгоритмов шифрования. **Множество ключей (ключевой домен)** для каждого алгоритма, однако, настолько большое число, что подобрать ключ достаточно трудно.

Шифрование симметричными ключами

Шифрование симметричными ключами использует единственный ключ и для кодирования и для дешифрования. Кроме того, алгоритмы шифрования и дешифрования – **инверсии** друг друга (*для расшифровки применяются те же операции, что и для шифрования, но в обратном порядке)*.

Схема взаимодействия отправителя и получателя сообщений при шифровании с симметричными ключами показана на рис. 24.

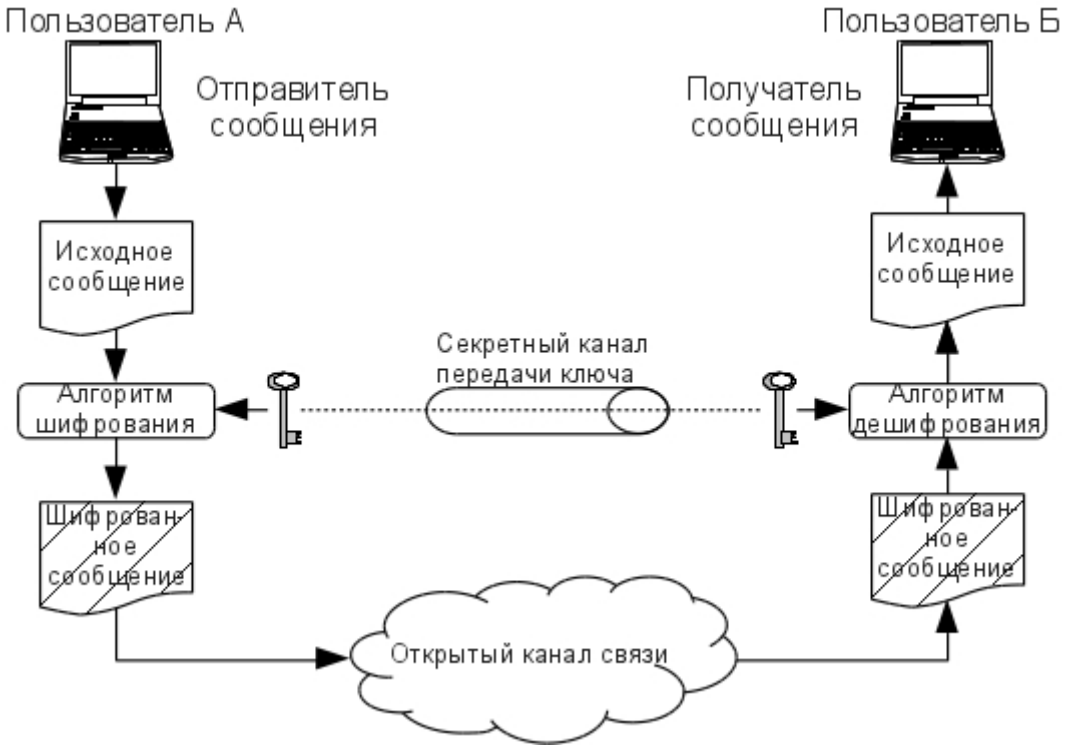

Рис. 24. Схема взаимодействия при шифровании с симметричными ключами.

Алгоритмы подстановки — исторически первые алгоритмы симметричного шифрования. Каждый символ исходного сообщения заменяется каким-то другим символом. **Ключ** – правила такой замены.

Пример: **Шифр сдвига («Шифр Цезаря»)** – замена букв алфавита буквами, сдвинутыми по номеру в алфавите на фиксированное число позиций (**hello → mjqqt** при ключе = 5). При достижении конца алфавита счёт начинается сначала (для латинского/английского алфавита значение 30=26+4, т.е. «d»).

Недостаток: ключ легко определяется использованием перебора вариантов и частотных характеристик языка.

Существуют также **мультипликативные** шифры (вместо сложения для определения подставляемого символа используется умножение), а также алгоритмы, использующие к качестве ключей **матрицы преобразований**.

Создание алгоритма подстановки, который приводит к принципиально неразгадываемому шифру (идеальный шифр) обеспечивается соблюдением принципов, выдвинутых К.Шенноном:

- Ключ должен быть разным для каждого следующего сообщения
- Длина ключа должны быть равна длине сообщения

В ручных системах шифрования эти принципы реализуются при использовании так называемых «одноразовых блокнотов».

В симметричной шифровании используются также **алгоритмы перестановки**. Ключ – правила перестановки символов.

Современные симметричные алгоритмы шифрования, используемые в АИС, делятся на два типа — блочные и потоковые

В **потоковых шифрах** шифрование делается в один момент времени над одним символом (таким, как символ или бит). Имеется поток исходного текста, поток зашифрованного текста и поток ключей (Пример: одноразовый блокнот).

В **блочных шифрах** группа символов (блок) исходного текста зашифровывается, создавая вместе группу зашифрованного текста одного и того же размера. Используется единственный ключ, чтобы зашифровать целый блок.

Для всех алгоритмов шифрования (криптоалгоритмов) выделяются следующие основные характеристики:

- **Криптографическая стойкость** – способность криптографического алгоритма противостоять расшифровке. Стойким считается алгоритм, для раскрытия которого требуются недостижимые вычислительные ресурсов, недостижимый объём перехваченных открытых и зашифрованных сообщений или такое время раскрытия, что по его истечению защищённая информация будет уже не актуальна, и т. д. В большинстве случаев криптостойкость нельзя математически доказать, можно только доказать уязвимости криптографического алгоритма.
- Длина ключа
- Число раундов (для блочных шифров **раунд** – один из последовательных шагов обработки данных в алгоритме)
- Длина обрабатываемого блока
- Сложность аппаратной/программной реализации
- Сложность преобразования

В АИС применяется ограниченное число симметричных

криптоалгоритмов, наиболее часто используемыми являются следующие:

- **AES (Advanced Encryption Standard)** – алгоритм блочного шифрования (размер блока 128 бит, ключ 128/192/256 бит). Поддержка AES введена фирмой Intel в семейство процессоров x86 начиная с Intel Core i7-980X Extreme Edition, а затем на процессорах Sandy Bridge.
- **DES (Data Encryption Standard)** – алгоритм блочного шифрования (блоки по 64 бита, 16 раундов, ключ 56 бит)
- **ГОСТ 28147-89** – блочный шифр (с 64-битными блоками, 32 циклами преобразования и 256-битным ключом)
- **Triple DES (3DES)** – использует преобразования DES три раза (самый распространённый вариант: «операции шифровка-расшифровка-шифровка» с тремя разными ключами)
- **IDEA (International Data Encryption Algorithm)** – блочный шифр (128-битный ключ и 64-битный размер блока, исходный незашифрованный 64-битный блок делится на четыре подблока по 16 бит каждый). С каждым блоком выполняются операции сложения, умножения и XOR с использованием ключа. Алгоритм запатентован (использование требует отчислений).
- **Blowfish** – блочный шифр (блоки 32 бита, ключ от 32 до 448 бит). Выполнен на простых и быстрых операциях: XOR, подстановка, сложение. Алгоритм свободно распространяется.

Симметричные алгоритмы имеют одну **фундаментальную уязвимость**: требуется, чтобы обе стороны уже имели общий ключ, который каким-то образом должен быть им заранее передан (проблема распределения ключа).

Вторая проблема симметричного шифрования – невозможность **установить подлинность источника сообщения** (все ключи одинаковые).

Шифрование асимметричными ключами

Алгоритмы **асимметричного шифрования (шифрования с открытым ключом)** разрабатывались для того, чтобы решить две основные проблемы симметричного шифрования. **Асимметричность ключей** означает, что алгоритм использует один ключ для шифрования, другой ключ – для дешифрования, и при этом вычислительно невозможно определить *дешифрующий ключ*, зная только алгоритм шифрования и *шифрующий ключ*.

К реализации асимметричных алгоритмов предъявляются следующие требования:

1. Вычислительная лёгкость создания пары ключей (открытый ключ KU, закрытый ключ KR)
2. Вычислительная лёгкость создания зашифрованного сообщение $C = E_{KU}[M]$ при наличии открытого ключа и незашифрованного сообщения M.

3. Вычислительная лёгкость дешифровки сообщения с использованием закрытого ключа: $M = D_{KR}[C] = D_{KR}[E_{KU}[M]]$

4. Вычислительная невозможность определить закрытый ключ KR, зная открытый ключ KU.

5. Вычислительная невозможность восстановить исходное сообщение M, зная открытый ключ KU и зашифрованное сообщение C.

6. (Дополнительно, не для всех алгоритмов) Коммутативность шифрующих и дешифрующих функций: $M = D_{KR}[C] = D_{KR}[E_{KU}[M]] = E_{KU}[D_{KR}[M]]$.

Основными способами использования алгоритмов с открытым ключом являются **шифрование/дешифрование**, **создание и проверка подписи** и **обмен ключа**.

Шифрование с открытым ключом состоит из следующих шагов:

1. Пользователь **B** создает пару ключей KU_b и KR_b, используемых для шифрования и дешифрования передаваемых сообщений

2. Пользователь **B** делает доступным некоторым надёжным способом (публикует) свой ключ шифрования (открытый ключ KU_b). Составляющий пару закрытый ключ KR_b держится в секрете

3. Если пользователь **A** хочет послать сообщение пользователю **B**, он шифрует сообщение, используя открытый ключ KU_b

4. Когда пользователь **B** получает сообщение, он дешифрует его, используя свой закрытый ключ KR_b. Никто другой не сможет дешифровать сообщение, так как этот закрытый ключ знает только пользователь **B** (при надёжном хранении закрытого ключа).

Процесс иллюстрируется на рис. 25 (секретный ключ помечен точкой).

Создание и проверка подписи состоит из следующих шагов:

1. Пользователь **A** создаёт пару ключей KU_A и KR_A, используемых для создания и проверки подписи передаваемых сообщений

2. Пользователь **A** делает доступным некоторым надёжным способом (публикует) свой ключ шифрования (открытый ключ KU_A). Составляющий пару закрытый ключ KR_A держится в секрете.

3. Пользователь A создаёт свою подпись S, шифруя её своим закрытым ключом: $S_C=E_{KRA}[S]$ и пересылает зашифрованную подпись пользователю B по надёжным каналам.

4. Пользователь B создаёт пару ключей для обмена сообщениям (см. выше).

5. Если пользователь **A** хочет послать подписанное сообщение пользователю **B**, он создаёт сообщение, включая в него свою защифрованную подпись и шифрует подписанное сообщение открытым

ключом пользователя В.

6. Когда пользователь **В** получает подписанное сообщение, он расшифровывает его своим закрытым ключом и проверяет соответствие подписи пользователя А. Никто другой не может подписать сообщение, так как закрытый ключ подписи знает только пользователь **А** (при надёжном хранении закрытого ключа).

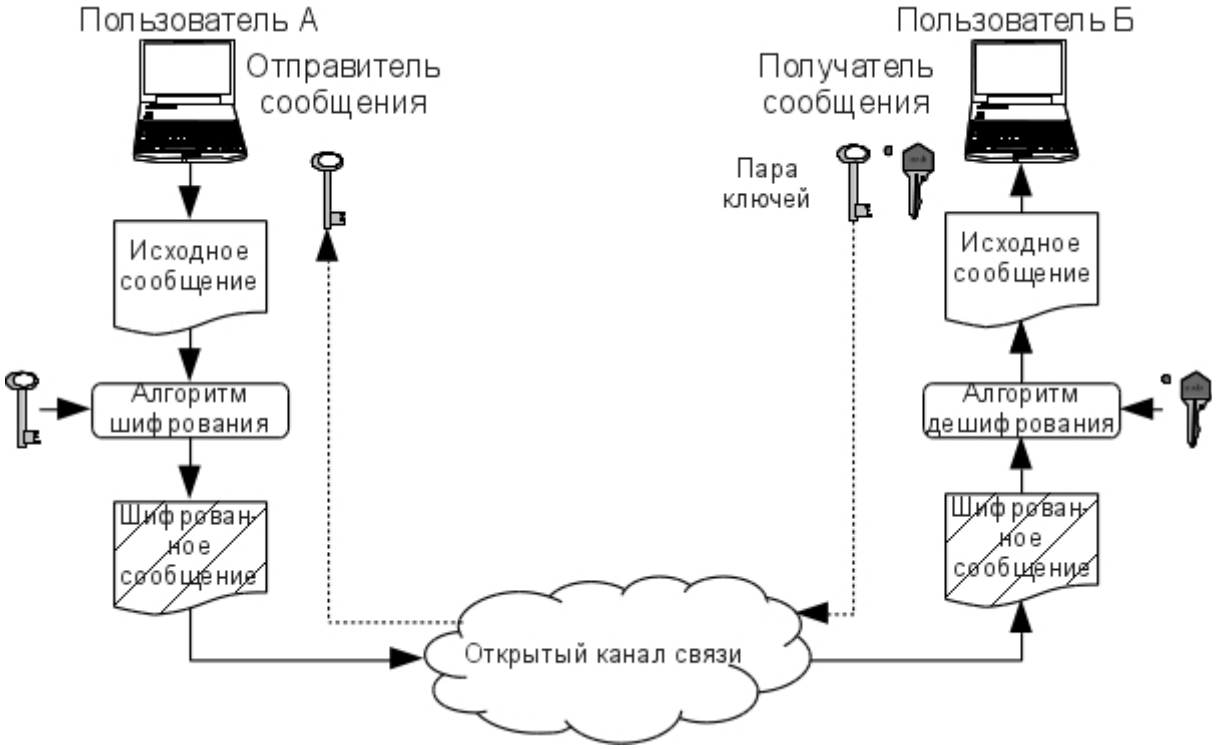

Рис. 25. Процесс обмена сообщениями при шифровании с асимметричным ключом.

Невозможно изменить сообщение, не имея доступа к закрытому ключу KR_A; тем самым обеспечивается аутентификация и целостность данных.

При использовании асимметричного шифрования для обмена ключей ключ симметричного шифрования рассматривается как сообщение., таким образом создаётся надёжный канал передачи симметричного ключа для конкретного сеанса информационного обмена — ключа сессии.

При всей математической сложности асимметричного шифрования такие алгоритмы имеют ряд существенных преимуществ перед симметричными алгоритмами:

- Не нужно предварительно передавать секретный ключ по надёжному каналу
- Только одной стороне известен ключ шифрования, который нужно держать в секрете (в симметричной криптографии такой ключ известен обеим сторонам и должен держаться в секрете обеими)
- Пару ключей можно не менять значительное время (при симметричном шифровании необходимо обновлять ключ после каждого

факта передачи)

• В больших сетях число ключей в асимметричной криптосистеме значительно меньше, чем в симметричной.

В АИС применяется ограниченное число асимметричных криптоалгоритмов, наиболее часто используемыми являются следующие:

• **RSA (аббревиатура от фамилий Rivest, Shamir и Adleman)** – длина ключа от 128 до 4096 бит. Используется как для шифрования, так и для подписи и обмена ключами сессий.

• **DSA (Digital Signature Algorithm)** – рекомендуемая длина ключа 2048 или 3072 бита. Используется для создания цифровой подписи. Ключом используется для шифрования *хэш-функции* подписываемого текста (битовой послоедовательности) длиной 224 или 256 бит.

• **ECDSA (Elliptic Curve Digital Signature Algorithm)** – используется для создания цифровой подписи. Обладает более высоким быстродействием, чем RSA и DSA за счёт использования более коротких ключей при той же криптостойкости

• **ГОСТ Р 34.10-2012** – используется для формирования и проверки электронной цифровой подписи. Как и ECDSA, основан на уравнениях *эллиптических кривых*.

Все асимметричные алгоритмы являются полностью открытыми.

Хэширование (иногда – хеширование», hashing) – преобразование по детерминированному алгоритму входного массива данных произвольной длины в выходную битовую строку фиксированной длины. Такие преобразования также называются хэш-функциями или функциями свёртки, а их результаты называют хэшем, хэш-кодом или сводкой сообщения (англ. *message digest*).

К преобразованиям, которые могут использоваться в качестве хэш-функций, предъявляются следующие требования:

1. Хэш-функция H должна применяться к блоку данных любой длины
2. Хэш-функция H создаёт выход фиксированной длины
3. $h=H(M)$ относительно легко вычисляется для любого значения M
4. Для любого данного значения хэш-кода h вычислительно невозможно найти M такое, что $H(M) = h$ (свойство односторонней функции)
5. Для любого данного x вычислительно невозможно найти $y \neq x$, что $H(y) = H(x)$
6. Вычислительно невозможно найти произвольную пару (x, y) такую, что $H(y) = H(x)$

Не доказано существование необратимых хэш-функций, для которых вычисление какого-либо прообраза заданного значения хеш-функции теоретически невозможно. Обычно нахождение обратного значения является лишь вычислительно сложной задачей.

Хэширование чаще всего применяется в следующих случаях:

- Вычисление контрольных сумм пакетов в транспортных протоколах (циклические алгоритмы, например CRC32)
- Ускорение поиска данных (текстов) в текстовых базах данных. Для искомого текста вычисляется хэш, который сравнивается с хэшами текстов, хранящимися в БД.
- Криптографические хеш-функции, используемые для контроля целостности файлов и проверки паролей
    - MD5
    - SHA-1
    - SHA-2
    - ГОСТ 34.11

Цифровая (электронная) подпись. Основные определения.

Отдельный вариант использования хеширования и асимметричного шифрования - **цифровая подпись**. Такая подпись должна обеспечивать возможность проверить автора, дату и время создания подписи, возможность аутентифицировать содержимое документа (файла) во время создания подписи и возможность проверки третьей стороной для разрешения споров.

Таким образом, к цифровой подписи предъявляются следующие требования:

- Подпись должна быть битовым образцом, который зависит от подписываемого сообщения
- Подпись должна использовать некоторую уникальную информацию отправителя для предотвращения подделки или отказа
- Создавать цифровую подпись должно быть относительно легко
- Должно быть вычислительно невозможно подделать цифровую подпись как созданием нового сообщения для существующей цифровой подписи, так и созданием ложной цифровой подписи для некоторого сообщения
- Цифровая подпись должна быть достаточно компактной и не занимать много памяти

Этим требованиям отвечает использование хэш-функции, зашифрованной по асимметричному алгоритму (закрытым ключом).

Цифровая подпись (**электронная подпись**) даёт возможность сделать электронный документ равным по юридической значимости бумажному документу.

Правовая основа применения цифровой (электронной) подписи (ЭП) в Российской Федерации является **Федеральный закон Российской Федерации от 6 апреля 2011 г. N 63-ФЗ «Об электронной подписи»**

Правила формирования ЭП для использования в государственных информационных системах определяются ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи».

Электронная подпись бывает *неквалифицированная* и *квалифицированная*.

Квалифицированная ЭП обеспечивается при использовании **сертифицированного** ключа и **сертифицированных** средств создания и проверки, полученных в **аккредитованном удостоверяющем центре**.

В соответствии с 63-ФЗ **простая неквалифицированная ЭП** создаётся с помощью кодов, паролей и других инструментов. Эти средства защиты позволяют идентифицировать автора подписанного документа. Важным свойством простой электронной подписи является отсутствие возможности проверить документ на предмет наличия изменений с момента подписания. Примером простой электронной подписи является комбинация логина и пароля.

Усиленная неквалифицированная электронная подпись (НЭП) создаётся с использованием криптографических средств и позволяет определить не только автора документа, но проверить его на наличие изменений. Простые и усиленные неквалифицированные подписи заменяют подписанный бумажный документ в случаях, оговоренных законом или по согласию сторон. Например, простые подписи могут использовать граждане для отправки сообщений органам власти. Усиленная подпись также может рассматриваться как аналог документа с печатью.

Усиленная квалифицированная электронная подпись (КЭП) должна обязательно иметь сертификат аккредитованного Удостоверяющего центра. Эта подпись заменяет бумажные документы во всех случаях, за исключением тех, когда закон требует наличия исключительно документа на бумаге. С помощью таких подписей вы сможете организовать юридически значимый электронный документооборот с партнёрскими компаниями, органами государственной власти и внебюджетными фондами.

Центр сертификации или **удостоверяющий центр** (*Certification authority, CA*) – сторона (отдел, организация), чья честность неоспорима, а открытый ключ широко известен. Задача центра сертификации – подтверждать подлинность ключей шифрования с помощью сертификатов электронной подписи.

Аккредитованный центр сертификации ключей обязан выполнять все обязательства и требования, установленные законодательством страны нахождения или организацией, проводящей аккредитацию в своих интересах и в соответствии со своими правилами.

Порядок аккредитации и требования, которым должен отвечать аккредитованный центр сертификации ключей, устанавливаются соответствующим уполномоченным органом государства или организации, выполняющей аккредитацию.

Центр сертификации ключей имеет право:

- предоставлять услуги по удостоверению сертификатов электронной цифровой подписи
- обслуживать сертификаты открытых ключей
- получать и проверять информацию, необходимую для создания соответствия информации указанной в сертификате ключа и предъявленными документами.

Цифровой сертификат – зашифрованный текст, содержащий информацию об организации (название, адрес, фамилию ответственного лица). Текст шифруется секретным ключом.

Такой сертификат передаётся пользователю и используется прикладными программами.

Сертификат, выданный аккредитованным удостоверяющим центром используется для квалифицированной ЭП.

Сертификаты и ключи можно создавать самостоятельно средствами ОС (например, используя комплект программ OpenSSL). Получаются **самоподписанные** сертификаты, используемые для неквалифицированной ЭП.

Средства криптографической защиты

КриптоПро – линейка криптографических программ (криптопровайдеров). Они используются во многих программах российских разработчиков для генерации ЭЦП, работы с сертификатами безопасности и пр. (Компания «КриптоКом»)

Средство криптографической защиты КриптоПро CSP разработано по согласованному с ФАПСИ техническому заданию в соответствии с криптографическим интерфейсом фирмы Microsoft – Cryptographic Service Provider (CSP).

Может использоваться для защиты сведений, не составляющих государственную тайну.

Средство криптографической защиты информации **«МагПро КриптоПакет»** – программный комплекс на базе библиотеки OpenSSL, позволяющий использовать российские стандарты на криптографические алгоритмы в программах, рассчитанных на использование криптобиблиотеки OpenSSL. Сертифицирован ФСБ.

Аппаратный ключ RuToken – персональное устройство доступа к информационным ресурсам (идентификатор), полнофункциональный аналог смарт-карты, выполненный в виде usb-брелка. Идентификатор предназначен для безопасного хранения и использования паролей, цифровых сертификатов, ключей шифрования и ЭЦП.

Содержит защищённый микропроцессор и память объёмом от 32 до 128

Кб. Главное отличие от зарубежных аналогов – аппаратная реализация российского алгоритма шифрования ГОСТ 28147-89.

Аппаратный ключ e-Token применяется в основном для хранения ключей коммерческих программных средств. Продуктами под этой торговой маркой в России торгует ЗАО «Аладдин Р. Д.» (США). Компания заявляет наличие сертификатов Гостехкомиссии и ФСТЭК России на продукты eToken.

Такие ключи используются, например, в сетевых версиях продуктов «1С» (аппаратные ключи HASP).

Технологии криптографической защиты каналов связи (VPN)

VPN (Virtual Private Network) – общее название для технологий, обеспечивающих работу в *публичных* сетях при сохранении *конфиденциальности* информационного обмена или работу через Интернет как в локальной сети.

Виртуальные частные сети обеспечивают поддержку различных протоколов, в особенности на прикладном уровне.

VPN соединяет два конкретных объекта, образуя таким образом уникальный канал связи между двумя абонентами. Каждая из конечных точек VPN может единовременно поддерживать несколько соединений VPN с другими конечными точками, однако каждая из точек является отдельной от других, и трафик разделяется посредством шифрования.

Все варианты VPN можно поделить на **пользовательские VPN** и **межузловые VPN**.

Сетевые соединения с использованием технологий VPN, обладают следующими основными свойствами:

- Трафик шифруется для обеспечения защиты от прослушивания
- Осуществляется аутентификация удалённого узла
- Виртуальные частные сети обеспечивают поддержку множества протоколов
- Соединение обеспечивает связь *только между двумя конкретными абонентами.*

Пользовательские VPN создаются между отдельной пользовательской системой и узлом или сетью предприятия («мобильный сотрудник»). Сервер VPN может являться межсетевым экраном сети предприятия либо быть отдельным VPN-сервером. Пользователь подключается к интернету через *своего провайдера* и инициирует VPN-соединение с узлом внутренней предприятия через интернет (рис. 26).

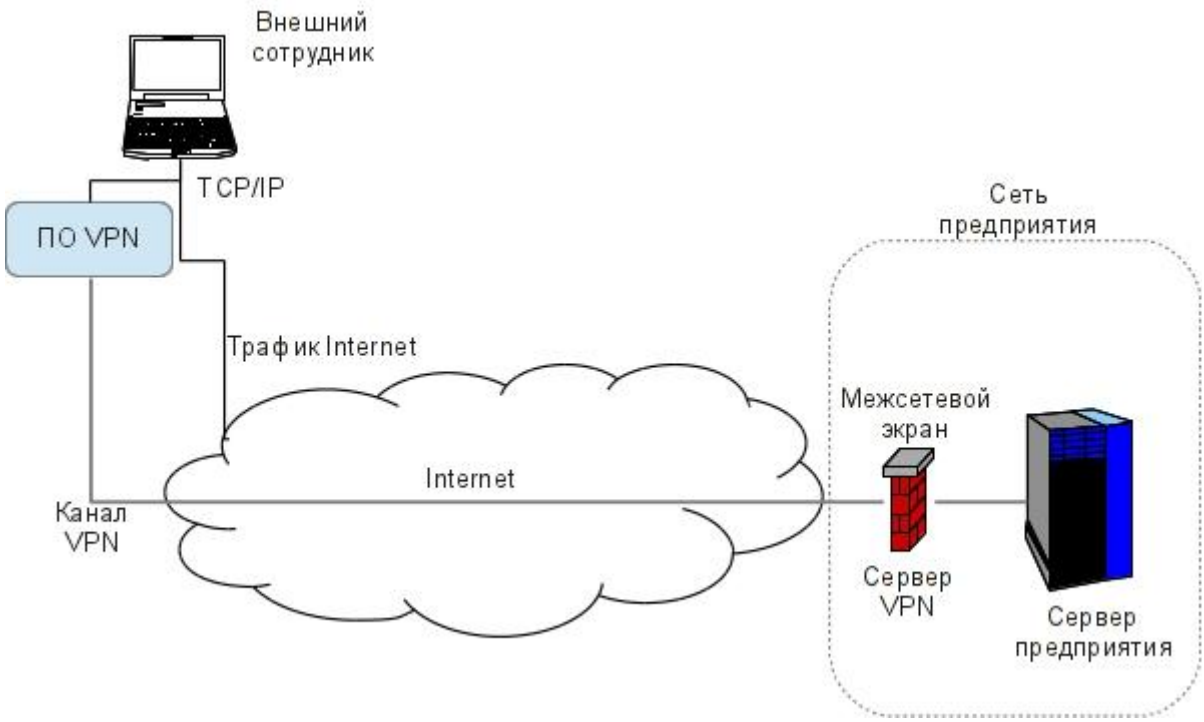

Рис. 26. Пример организации пользовательского VPN-соединения.

Узел предприятия запрашивает у пользователя аутентификационные данные и, в случае успешной аутентификации, позволяет пользователю осуществить доступ ко внутренней сети предприятия, как если бы пользователь находился внутри узла и физически располагался внутри сети. Скорость сетевого соединения ограничивается скоростью подключения пользователя к интернету.

При этом пользователь работает с ресурсами интернета без изменений. Одновременный доступ по VPN во внутреннюю сеть предприятия и в Интернет может вызывать проблемы с безопасностью.

Узловые VPN-соединения используются предприятиями и организациями для подключения к удалённым узлам без применения дорогостоящих выделенных каналов или для соединения двух различных предприятий (организаций), между которыми необходима связь для осуществления информационного обмена, связанного с деятельностью этих организаций. Как правило, VPN соединяет один межсетевой экран или пограничный маршрутизатор с другим аналогичным устройством

На рис. 27 показан пример VPN-соединения между сетью предприятия-участника ВЭД и Центральным Информационно-техническим таможенным управлением (ЦИТТУ, ранее — Главный научно-исследовательский вычислительный центр — ГНИВЦ) ФТС Российской Федерации.

При таком соединении обе сети должны соблюдать согласованную *схему адресации* (чтобы ip-адреса не повторялись или не применялись отличающиеся *маски сетей*).

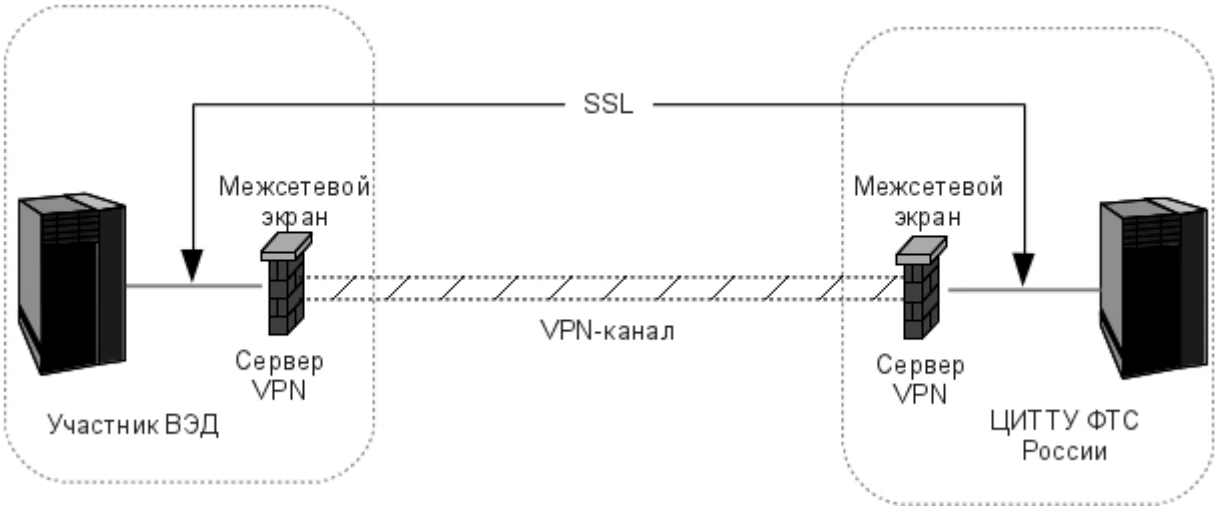

Рис. 27. Пример использование VPN для связи подразделений ФТС и участников ВЭД.

Ключевыми компонентами для реализации VPN-соединений являются

- Сервер VPN
- Алгоритмы шифрования
- Система аутентификации
- Протокол VPN

VPN-сервер должен быть расположен во внутренней сети предприятия. Сервер может быть межсетевым экраном или пограничным маршрутизатором/шлюзом (играть роль «сервера доступа»).

На этом сервере (межсетевом экране) устанавливаются *правила*, определяющие, какие протоколы *прикладного уровня* можно пропускать снаружи внутрь, а какие – нельзя.

В качестве **протокола VPN** может использоваться **IPSec** или **SSL**. Эти протоколы являются «обёртками» для других протоколов прикладного уровня.

Возможно несколько реализаций средств для организации VPN-серверов:

- **Аппаратный VPN-сервер:** надёжное специализированное устройство (межсетевой экран,. оптимизированое для данной задачи. Проблема – обновления «прошивки».
- **Программный VPN-сервер:** программное обеспечение (ПО) устанавливается на любые компьютеры. ПО может быть бесплатное. Проблема – настройки и ресурсы оборудования (шифрование больших объёмов данных требует много ресурсов).
- **Web-системы VPN:** клиентом является браузер со специальными дополнениями (поддержка SSL) или с использованием Java-машин. Проблема – низкая надёжность и ограниченный набор возможных приложений (только специально предназначенные для такой конфигурации).

Нормативная база применения информационных технологий

Государственная программа «Информационное общество»

Государственная программа Российской Федерации "Информационное общество (2011 - 2020 годы)" утверждена Распоряжением Правительства РФ от 20 октября 2010 г. N 1815-р.

Программа определяет направления создания информационного общества и основные показатели, которые должны быть достигнуты к 2020 году.

Целью программы является увеличение количества услуг и общедоступной информации, существующих в электронном виде, повышение конурентоспособности страны за счёт ориентации на высокотехнологический сектор (ИТ-сектор).

Координатором программы является Министерство связи и массовых коммуникаций Российской Федерации

Государственными заказчиками являются

- Министерство культуры Российской Федерации
- Министерство здравоохранения и социального развития Российской Федерации
- Министерство связи и массовых коммуникаций Российской Федерации
- Министерство образования и науки Российской Федерации
- Министерство экономического развития Российской Федерации
- Федеральная служба безопасности Российской Федерации
- Федеральная служба охраны Российской Федерации
- Министерство регионального развития Российской Федерации
- Следственный комитет Российской Федерации

Основные параметры (индикаторы) программы «Информационное общество»

Наименование индикатора	2011	2015	2020
Место по индексу готовности к сетевому обществу	в числе 70 ведущих стран мира	в числе 20 ведущих стран мира	в числе 20 ведущих стран мира
Место по индексу развития информационных технологий	в числе 50 ведущих стран мира	в числе 10 ведущих стран мира	в числе 10 ведущих стран мира
Место по индексу развития электронного правительства	в числе 60 ведущих стран мира	в числе 40 ведущих стран мира	в числе 20 ведущих стран мира

Доля домашних хозяйств, имеющих широкополосный доступ в сеть Интернет, %	45	55	80
Доля сектора ИТ в ВВП, %	4.5	5.9	7.1
Доля отечественных товаров и услуг в объеме внутреннего рынка ИТ, %	5	более 50	50
Доля федеральных государственных услуг в электронном виде, %	39	100	100
Доля электронных каталогов в Музейном фонде	26	100	100
Доля электронного документооборота между ОГВ, %	10	70	70
Доля патентов в сфере ИТ, %	16.2	17.5	30
Доля библиотечных фондов в электронной форме, %	1	не менее 50	не менее 75

Основные нормативные документы в области создания и применения информационных технологий в Российской Федерации

• Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 года N 149-ФЗ

• Федеральный закон «Об электронной подписи» от 6 апреля 2011 года N 63-ФЗ

• Федеральный закон «О персональных данных» от 27 июля 2006 года N 152-ФЗ

• Закон о государственной тайне от 21 июля 1993 года N 5485-1

• Приказ Министерства связи и массовых коммуникаций Российской Федерации (Минкомсвязи России) от 2 сентября 2011 г. N 221 «Об утверждении Требований к информационным системам электронного документооборота федеральных органов исполнительной власти, учитывающих в том числе необходимость обработки посредством данных систем служебной информации ограниченного распространения»

• Распоряжение Правительства Российской Федерации от 17 декабря 2010 г. N 2299-р о Плане перехода федеральных органов исполнительной власти и федеральных бюджетных учреждений на использование свободного программного обеспечения на 2011 - 2015 годы.

Некоторые государственные стандарты в области информационных технологий

• **ГОСТ Р ИСО МЭК 12207-99** Информационные технологии. Процессы жизненного цикла программного обеспечения.

• **ИСО/ТО 10006:1997 (R)** Менеджмент качества. Руководство

качеством при административном управлении проектами.

- **ГОСТ 34.xxx** Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. (см., например, ГОСТ 34.601-90 «Автоматизированные системы. Стадии создания»)
- **ГОСТ 19.xxx** Единая система программной документации (Комплекс стандартов).
- **ГОСТ 28806-90** Качество программных средств. Термины и определения.
- **ГОСТ 28195-89** Оценка качества программных средств. Общие положения.
- **ГОСТ Р ИСО/МЭК 9126-93** Информационная технология. Оценка программного продукта. Характеристики качества и руководящие указания по их применению.
- **ГОСТ Р 54593-2011** Информационные технологии. Свободное программное обеспечение. Общие положения
- **ГОСТ Р ИСО/МЭК 26300-2010** Информационная технология. Формат Open Document для офисных приложений (OpenDocument) v1.0.

Нормативные документы по применению информационных технологий в деятельности ФТС

Нормы Таможенного кодекса Таможенного союза (ТК ТС) в части, касающейся применения информационных технологий странами-участниками таможенного союза

Применению информационных технологий для осуществления деятельности таможенных органов в странах-участниках таможенного союза посвящена глава Глава 4 ТК ТС «Информационные системы и информационные технологии».

Статья 43 «Информационные системы, информационные технологии и средства их обеспечения, используемые таможенными органами» говорит о том, что АИС таможенных органов строятся с учётом международных стандартов в соответствии с законодательством стран-участников, используют средства защиты информации и объединяются для обеспечения взаимодействия на таможенной территории ТС.

Статья 44 «Информационные ресурсы таможенных органов» говорит о том, что информационные ресурсы делятся на *общедоступные* ресурсы и ресурсы *ограниченного доступа*. Общедоступная информация публикуется на сайтах таможенных органов, а перечень и порядок публикации ресурсов ограниченного доступа определяется законодательством стран-участников ТС.

Статья 45 «Защита информации и прав субъектов, участвующих в информационных процессах и информатизации» говорит о том, что

информация делится по категориям (уровням) защиты, и средства защиты для каждого уровня определяются законодательством стран-участников ТС.

Статья 46 «Информационный обмен таможенных органов» говорит о том, что обмен информацией осуществляется в соответствии с международными договорами и с законодательством стран-участников ТС.

Приказы ФТС Российской Федерации

- Приказ ГТК России от 27 мая 2004 г. N 619 «Об проведении организационно-технических мероприятий по внедрению электронной формы декларирования»
- Приказ ГТК России от 30 марта 2004 г. N 395 «Об утверждении Инструкции о совершении таможенных операций при декларировании товаров в электронной форме»
- Приказ ФТС России от 31 января 2005 г. N 64 «О решении коллегии ФТС России от 17.12.2004 "О программе развития и внедрения в таможенных органах Российской Федерации электронной формы декларирования товаров и транспортных средств»
- Приказ ФТС России от 24 января 2008 г. N 52 «О внедрении информационной технологии представления таможенным органам сведений в электронной форме для целей таможенного оформления товаров, в том числе с использованием международной ассоциации сетей "Интернет"»
- Приказ ФТС России N 1452 от 11 августа 2009 «О вводе в опытную эксплуатацию информационной технологии представления таможенным органам сведений в электронной форме для целей таможенного оформления товаров с использованием международной ассоциации сетей "Интернет" в таможенных органах, подчиненных Сибирскому, Уральскому и Дальневосточному таможенным управлениям»
- Приказ ФТС России № 183 от 3 февраля 2010 года «Об утверждении Порядка организации процессов жизненного цикла программных средств информационных систем и информационных технологий таможенных органов».
- Приказ ФТС России от 07 июля 2010 г. N 1274 «О вводе в эксплуатацию первой очереди комплекса программных средств "Портал электронного представления сведений"»
- Приказ ФТС России от 29 июня 2010 г. N 1246 «О внедрении комплекса программных средств пограничного пункта пропуска в таможенных органах Российской Федерации»
- Распоряжение ФТС России N 165-р от 14 сентября 2011 «Об утверждении Временной информационной технологии взаимодействия лиц, осуществляющих декларирование товаров и транспортных средств в электронной форме при удаленной уплате таможенных пошлин, налогов с использованием электронного терминала, координатора эмиссии

микропроцессорных пластиковых карт и Федеральной таможенной службы»

• Приказ ФТС России N 2187 от 25 октября 2011 «Об утверждении Положения об использовании участниками внешнеэкономической деятельности и лицами, осуществляющими деятельность в сфере таможенного дела, средств электронной подписи при реализации информационного взаимодействия с таможенными органами Российской Федерации»

• Приказ ФТС России N 1008 от 24 октября 2012 «О вводе в эксплуатацию комплекса программных средств "Портал электронного представления сведений для электронного декларирования через интернет"»

Управление деятельностью по применению и развитию информационных технологий в ФТС Российской Федерации

Для координации всей деятельности по применению и развитию информационных технологий в Федеральной таможенной службе Российской Федерации создано Главное управление информационных технологий ФТС РФ.

Положение о Главном управлении информационных технологий (ГУИТ) утверждено Приказом ФТС от 17 января 2007 г. N 55.

В соответствии с Положением, на ГУИТ возложены следующие функции:

• Координация работ и разработка предложений по совершенствованию научно-технической политики ФТС России

• Анализ перспективных направлений развития информационных технологий, информационно-технических средств, сетей и средств телекоммуникаций, разработка предложений по их применению в таможенных органах

• Организация обоснования, планирования, контроля выполнения и внедрения научно-исследовательских и опытно-конструкторских работ (НИОКР), оснащения таможенных органов информационно-техническими средствами, программным обеспечением, средствами защиты информации

• Организация разработки и согласования технологий автоматизированного информационного взаимодействия таможенных органов с информационными системами других федеральных органов исполнительной власти с учетом полномочий ФТС России

• Разработка порядка и условий использования для таможенных целей информационных систем, информационных технологий и средств их обеспечения

• Разработка порядка формирования и использования информационных ресурсов таможенных органов и требований к документированию информации, а также порядка получения информации,

содержащейся в информационных ресурсах, находящихся в ведении таможенных органов

- Разработка (участие в разработке) проектов федеральных законов, правовых актов Президента Российской Федерации и Правительства Российской Федерации по направлениям деятельности Главного управления

- Представление руководству ФТС России предложений об издании, отмене, изменении или дополнении нормативных и иных правовых актов ФТС России по вопросам, входящим в компетенцию Главного управления. Разработка проектов нормативных правовых актов федеральных органов исполнительной власти, нормативных и иных правовых актов ФТС России определяющих порядок:

1. заказа, приемки и реализации результатов НИОКР;
2. сертификации и аттестации информационного и программного обеспечения единой автоматизированной информационной системы (ЕАИС) таможенных органов, информационно-технических средств;
3. организации эксплуатации и ремонта информационно-технических средств;
4. развития ведомственной интегрированной телекоммуникационной сети (ВИТС) ФТС России и организации связи;
5. организации метрологического обеспечения таможенных органов;
6. применения современных информационных таможенных технологий и информационно-технических средств при проведении таможенного контроля;
7. обеспечения радиационной безопасности;
8. обеспечения информационной безопасности таможенных органов;
9. предоставления льгот за работу во вредных условиях.

- Разработка совместно с ЦИТТУ ФТС России и другими структурными подразделениями центрального аппарата ФТС России технических требований по закупкам информационно-технических средств, средств защиты информации, программного обеспечения, услуг и работ для таможенных органов по вопросам, входящим в компетенцию Главного управления
- Организация совместно с ЦИТТУ ФТС России доработки, модернизации, сопровождения, внедрения программного обеспечения и администрирования информационных систем и баз данных таможенных органов
- Разработка предложений и обоснований в проект сметы расходов ФТС России на содержание и развитие информационно-технических средств и средств защиты информации таможенных органов

• Выполнение функций генерального заказчика НИОКР, функций заказчика на приобретение информационно-технических средств в интересах развития таможенного дела в Российской Федерации

• Подготовка и контроль выполнения контрактов о проведении:

1. НИОКР по созданию и совершенствованию информационных технологий, информационно-технических систем и средств;
2. работ по изготовлению установочных (опытных) партий оборудования;
3. работ по настройке и монтажу оборудования на объектах эксплуатации;
4. опытной оперативной эксплуатации;
5. модернизации (доработки) информационно-технических средств;
6. централизованного послегарантийного обслуживания и ремонта информационно-технических средств;
7. работ по изготовлению и закупке запасных частей и принадлежностей для систем и средств, находящихся в эксплуатации;
8. проектно-изыскательских работ в интересах развития ВИТС;
9. строительно-монтажных работ по оборудованию телекоммуникационных узлов и размещению средств связи;
10. аренды телекоммуникационных услуг и каналов связи;
11. закупки программного обеспечения;
12. обучения должностных лиц таможенных органов по вопросам, входящим в компетенцию Главного управления.

• Взаимодействие с федеральными органами исполнительной власти, органами исполнительной власти субъектов Российской Федерации, государственными органами, организациями, должностными лицами и гражданами по вопросам, относящимся к компетенции Главного управления. Функциональное взаимодействие по вопросам информационно-технического обеспечения со структурными подразделениями центрального аппарата ФТС России, таможенными органами, организациями, находящимися в ведении ФТС России

• Разработка предложений и организация обучения и профессиональной подготовки (переподготовки) должностных лиц таможенных органов в области применения общесистемных программных средств, информационных таможенных технологий, программных средств ЕАИС и ВИТС, информационно-технических средств, методов и средств обеспечения информационной и радиационной безопасности в практической деятельности таможенных органов

• Участие в совершенствовании структуры таможенных органов и систем управления ими в соответствии с требованиями и приоритетами внедрения в процесс таможенного оформления и контроля, современных

информационно-коммуникационных технологий, систем и информационно-технических средств

• Организация конфиденциальной, городской, междугородной, радиоподвижной, специальной засекреченной и государственной документальной связи в интересах обеспечения деятельности таможенных органов

• Взаимодействие в соответствии с установленным порядком с Аппаратом Правительства Российской Федерации, Минобороны России, ФСБ России, ФСО России, Минкомсвязи России, другими федеральными органами исполнительной власти и организациями, а также с операторами связи по вопросам обеспечения таможенных органов всеми видами связи

• Разработка телефонных справочников ФТС России, таможенных органов и организация их издания

• Разработка предложений по планированию капитального строительства объектов ВИТС и локальных вычислительных сетей для таможенных органов

• Подготовка технических заключений на схемы организации связи, технические задания, рабочие проекты по организации телекоммуникационных сетей

• Координация работ региональных таможенных управлений по организации сетей телекоммуникаций, контроль за выполнением планов и мероприятий по созданию и развитию ВИТС таможенных органов

• Организация контроля по вопросам обеспечения информационной безопасности таможенных органов, включая организацию работ по противодействию иностранным техническим разведкам и технической защите информации

• Организация учёта и контроля радиоактивных материалов в рамках систем государственного учёта ядерных материалов, радиоактивных веществ и радиоактивных отходов

• Информационная поддержка таможенных органов при проведении ими таможенного контроля за делящимися и радиоактивными материалами, опасными отходами и другими товарами из контролируемых списков

• Подготовка проектов профилей риска, возникающих в процессе таможенного оформления и таможенного контроля делящихся и радиоактивных материалов и опасных отходов

• Участие в организации таможенного оформления и таможенного контроля делящихся и радиоактивных материалов в соответствии с лицензией Росатома России и Общим положением о службе таможенного контроля за делящимися и радиоактивными материалами (ТКДРМ) таможенного органа Российской Федерации

• Организация эксплуатации радиационных источников, содержащих радиоактивные вещества, и ведомственный контроль радиационной

безопасности в таможенных органах при обращении с радиоактивными веществами, приборами или аппаратурой, в которых содержатся радиоактивные вещества или генерируется ионизирующее излучение

• Выполнение функций рабочего органа по реализации программы сотрудничества ФТС России и Министерства энергетики США "Вторая линия защиты"

• Обеспечение единства и требуемой точности измерений, организация метрологического обеспечения и контроля в таможенных органах

• Организация стандартизации, унификации и сертификации разрабатываемых и заказываемых информационно-технических средств

• Разработка и согласование со структурными подразделениями центрального аппарата ФТС России организационно-технических документов о реализации проекта модернизации информационной системы таможенных органов

• Выполнение функций рабочего органа Управляющего совета по проекту модернизации информационной системы таможенных органов Российской Федерации, организация взаимодействия по вопросам его реализации с Минэкономразвития России, Минфином России и МБРР

• Организация контроля за деятельностью таможенных органов и организаций, находящихся в ведении ФТС России, по вопросам укрепления и развития информационно-технической базы, по другим направлениям работы в соответствии с функциями Главного управления

• Организация работ при применении системы управления рисками в соответствии с действующими правовыми актами ФТС России

• Организация учёта результатов интеллектуальной деятельности на НИОКР, выполняемых по заказу ФТС России

• Противодействие иностранным техническим разведкам и техническая защита информации.

Непосредственная деятельность по внедрению и сопровождению средств информационных технологий в структуре Федеральной таможенной службы Российской Федерации выполняется Центральным информационно-техническим таможенным управлением (ЦИТТУ, ранее — Главный научно-исследовательский вычислительный центр - ГНИВЦ)ЦИТТУ ФТС РФ.

Деятельность ЦИТТУ регламентируется **Положением о Центральном информационно-техническом таможенном управлении**, утверждённым Приказом ФТС России от 1 июля 2013 г. N 1205.

В соответствии с Положением, на ЦИТТУ возложены следующие задачи:

• Осуществление деятельности по информационному обеспечению и программно-технической поддержке эксплуатации компонентов автоматизированных систем, обеспечивающих использование

информационно-коммуникационных технологий на всех уровнях системы таможенных органов при выполнении возложенных на них задач и функций в сфере таможенного дела, а также по формированию, содержанию информационных ресурсов таможенных органов и эксплуатации Главного центра обработки данных ФТС России

- Участие совместно с информационно-техническими подразделениями таможенных органов в деятельности по обеспечению взаимодействия информационных систем таможенных органов с информационными системами других федеральных органов исполнительной власти, организаций, таможенных служб других государств, участников внешнеэкономической деятельности (ВЭД) и иных заинтересованных лиц
- Методическое руководство деятельностью информационно-технических подразделений таможенных органов по вопросам внедрения информационных технологий и автоматизированных систем
- Обеспечение бесперебойности процессов функционирования компонентов автоматизированных систем непосредственно в Управлении и в ФТС России, а также координация деятельности таможенных органов по указанному вопросу.

При формировании и реализации политики в области развития и применения информационных технологий в Федеральной таможенной службе ЦИТТУ имеет следующие обязанности и полномочия:

- проведение научно-исследовательских и опытно-конструкторских работ, а также научно-техническое сопровождение работ в области автоматизации и информационного обеспечения деятельности таможенных органов, разработка и внедрение ЕАИС в соответствии с планами, утверждёнными ФТС России
- информационное обеспечение деятельности таможенных органов, федеральных органов государственной власти и организаций
- участие в разработке и внедрении программного и технического обеспечения ЕАИС таможенных органов, в том числе в создании ведомственной интегрированной телекоммуникационной сети, разработке архитектуры и проектов технического оснащения таможенных органов
- участие в разработке и построении Ведомственной интегрированной телекоммуникационной сети ФТС России
- организация системотехнического обслуживания и ремонта средств вычислительной техники, оргтехники и средств передачи данных в таможенных органах и подразделениях ФТС России
- защита информации и обеспечение ее достоверности в центральном вычислительном комплексе (ЦВК), центральной базе данных (ЦБД), в других эксплуатируемых сетях передачи данных и системах ГНИВЦ, разработка и осуществление комплекса организационных и технических

мероприятий по предотвращению нарушений целостности и конфиденциальности информационных ресурсов ограниченного доступа, незаконного и(или) несанкционированного их использования

- разработка и реализация совместно с учебными заведениями ФТС России планов подготовки сотрудников и работников таможенных органов по вопросам разработки, внедрения и эксплуатации программно-технических комплексов и информационных таможенных технологий, используемых в ЕАИС таможенных органов
- участие в разработке и реализации единой научно-технической политики ФТС России, осуществляемой при развитии и эксплуатации ЕАИС таможенных органов
- участие в разработке и реализации концепций, целевых программ, перспективных планов развития и оснащения таможенных органов современными программно-техническими комплексами в рамках ЕАИС таможенных органов
- оказание методической помощи информационно-техническим подразделениям таможенных органов в обеспечении функционирования ЕАИС, в ведении региональных баз данных и выполнении информационно-вычислительных работ
- участие в разработке и реализации основных направлений интеграции информационных ресурсов ФТС России и федеральных органов государственной власти, в создании единого информационного пространства таможенных органов государств-участников СНГ
- обеспечение взаимодействия с информационно-вычислительными системами и банками данных министерств и ведомств Российской Федерации, а также таможенных органов других стран.

Кроме того, на ЦИТТУ возложена обязанность по созданию, сопровождению и развитию Фонда программных средств ФТС.

Руководящий документ «Положение о фонде программных средств ГНИВЦ ГТК России» РД ГНИВЦ 42.01-2001(3) (редакция 3) устанавливает:

- Цели, задачи и правила формирования Фонда программных средств
- Вид документов и правила оформления проектной документации
- Вид документов и правила оформления технических актов сдачи-приёмки в опытную эксплуатацию, продолжения опытной эксплуатации, сдачи-приемки в промышленную эксплуатацию
- Вид и правила оформления документов ведения фонда программных средств
- Типовое содержание техно-рабочих документов

В структуре ЦИТТУ существует **Отдел ведения фонда алгоритмов и программ**.

Участие подразделений ФТС в формировании и реализации политики в области развития и применения информационных технологий

Полномочия и обязанности структурных подразделений ФТС в формировании и реализации политики в области развития и применения информационных технологий определены в **Приказе Федеральной таможенной службы от 12 января 2005 г. N 7** «Об утверждении Общего положения о региональном таможенном управлении и Общего положения о таможне».

В соответствии с Общим положением о Региональном таможенном управлении (РТУ)

- РТУ имеет полномочия по обеспечению функционирования Единой автоматизированной информационной системы таможенных органов (ЕАИС) и ведомственной интегрированной телекоммуникационной сети таможенных органов (ВИТС), информационной безопасности, оснащению техническими средствами таможенного контроля и техническими средствами охраны таможенных органов, а также организации этой работы в подчинённых таможенных органах
- РТУ имеет полномочия по обеспечению в РТУ, организации и контролю в подчинённых таможенных органах эффективного использования, эксплуатации, технического обслуживания и ремонта вычислительной техники, технических средств таможенного контроля, технических средств охраны и иных технических средств
- РТУ имеет право направлять в ФТС России предложения и соответствующие заявки о материально-техническом обеспечении РТУ и подчинённых таможенных органов.

В соответствии с Общим положением о таможне

- Таможня имеет полномочия по выполнению в пределах своей компетенции работы по обеспечению функционирования Единой автоматизированной информационной системы таможенных органов (ЕАИС) и ведомственной интегрированной телекоммуникационной сети таможенных органов, информационной безопасности, по оснащению соответствующих подразделений в таможне и на таможенных постах техническими средствами таможенного контроля и техническими средствами охраны таможенных органов
- Таможня имеет полномочия по обеспечению в таможне, организации и контролю на таможенных постах эффективного использования, эксплуатации, технического обслуживания и ремонта вычислительной техники, технических средств таможенного контроля, технических средств охраны и иных технических средств
- Таможня имеет право направлять в вышестоящий таможенный орган предложения и соответствующие заявки о материально-техническом обеспечении таможни и таможенных постов.

Единая автоматизированная информационная система ФТС Российской Федерации

Цели, задачи и особенности построения ЕАИС ФТС

Единая автоматизированная информационная система (ЕАИС) ФТС обеспечивает процессы, связанные с совершением таможенных операций и таможенным контролем товаров и транспортных средств, других функций, возложенных на таможенные органы в сфере таможенного дела, а также функций, обеспечивающих деятельность таможенных органов.

Цель создания и развития ЕАИС – поддержка электронного взаимодействия (информационного обмена) между подразделениями ФТС, между ФТС и участниками ВЭД, между таможенными службами стран-участников Таможенного союза и другими партнёрами.

Первая очередь Единой автоматизированной информационной системы таможенных органов (ЕАИС ТО) была принята в эксплуатацию в декабре 1994 года. Тогда ее средствами решалось лишь несколько локальных программных задач в интересах таможенных органов, ряда министерств и ведомств России

Сейчас ЕАИС ТО представляет собой комплексную территориально распределённую систему, автоматизирующую практически все процессы, связанные с осуществлением контроля внешнеэкономической деятельности.

В составе ЕАИС ТО используется около четырёх десятков функциональных автоматизированных систем, включающих информационно-программные средства и базы данных. Вычислительные комплексы объединены средствами телекоммуникационных сетей и включают две тысячи каналов передачи данных (большинство – с пропускной способностью 2 Мбит/с и выше).

В целом ЕАИС характеризуется:

- территориальной распределённостью;
- иерархической структурой управления;
- централизованным методологическим управлением в части применения информационных таможенных технологий (КАСТО);
- необходимостью использования распределённых информационных систем, нуждающихся в средствах обеспечения информационного обмена между ними;
- существованием средств передачи информации и обеспечивающих их комплекса организационного, информационного и программно-аппаратного обеспечения;
- наличием ведомственной электронной почты на базе использования

распространённых почтовых систем;

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

Необходимость развития и совершенствования ЕАИС связана со следующими факторами:

• постоянный рост числа пользователей;
• постоянный рост объёмов грузоперевозок;
• изменение нормативной базы;
• необходимость интеграции с зарубежными партнёрами;
• необходимость интеграции с другими ведомствами (МВД, ФСБ, ФНС, ЦБ РФ).

Особенности информации, циркулирующей в ЕАИС

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 неопределёнными средствами её 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 отчётная информация таможенных органов;
• транзитная информация, проходящая через ЦИТТУ ФТС России.

По срокам передачи **информации** в ЕАИС в соответствии с требованиями нормативных документов и установленными регламентами используется следующая классификация:

• **Оперативная информация** (данные мониторинга таможенного оформления). 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** (отчёты таможенных органов в соответствии с ежегодными приказами ФТС России о введении форм статистической отчётности). Отличительной особенностью данной категории является периодический характер формирования и необходимость получения необходимых данных к определённому нормативными документами сроку;

• **Информация, используемая для формирования официальных статистических отчётов, бюллетеней и сборников**. Информация данной категории должна быть максимально достоверной и полной, при этом на оперативность её формирования не накладывается таких жёстких ограничений, как в предыдущих категориях;

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

Основные подсистемы ЕАИС ФТС

В качестве основных структурных элементов ЕАИС ФТС можно выделить следующие:

• **ВИТС** – ведомственная интегрированная телекоммуникационная сеть

• **ТТП** – транспортно-технологическая подсистема

• **АСВД** – автоматизированная система внешнего домена

• **АС ЭПС** – автоматизированные системы электронного предоставления сведений

• **ЦБД ЕАИС** – центральная база данных

• **КАСТО и КПС** – комплексы автоматизированных средств таможенного оформления и комплексы программных средств соответственно

• **СВКС** – система видеоконференцсвязи.

ВИТС (ведомственная интегрированная телекоммуникационная сеть) ФТС РФ – совокупность технических и программных средств передачи и обработки данных, которая совместно с **каналами связи** позволяет организовать интегрированную передачу разнородного трафика: данных, голоса и видео.

Каналы связи организуются от «от старшего к младшему»: ФТС ⇒ РТУ, РТУ ⇒ таможни, таможни ⇒ таможенные посты и пункты пропуска. Каналы связи арендуются ФТС, РТУ и таможнями у операторов связи (Ростелеком,

Трансстелеком) на конкурсной договорной основе. Каналы связи – цифровые, интегрированные (по одному каналу передаются все типы информации: данные, голос и видео).

Пропускная способность каналов связи – от 128 кит/с до 2048 кбит/с и выше. Для работы СВКС требуются каналы с пропускной способностью более 2048 кбит/с (2 Мбит/с). Система видеоконференцсвязи (СВКС) реализована на уровнях ФТС → РТУ и РТУ → таможни.

Для передачи данных в ВИТС используются медные линии связи (кабели), волоконно-оптические линии связи (ВОЛС), спутниковые каналы, сотовая связь. Используется телекоммуникационное оборудование от Cisco Systems (в настоящее время).

По уровням управления (данные на начало 2014 года) подразделения ФТС распределяются следующим образом:

- Центральный аппарат ФТС РФ — 21 основное структурное подразделение (I уровень управления, Федеральный)
- 5 центральных таможен, 1 базовая и 1 кинологический центр в непосредственном подчинении ФТС РФ, 8 территориальных региональных таможенных управлений (II уровень управления, Региональный)
- 72 таможни, в том числе 8 оперативных (III уровень управления, Таможенный)
- 503 приграничных и внутренних таможенных поста (IV уровень управления, Территориальный).

Транспортно-технологическая подсистема (ТТП) предназначена для обеспечения взаимодействия между прикладными процессами, в рамках программных комплексов и информационных систем.

Для обмена информацией между прикладными процессами используются каналы связи ВИТС. ТТП, как и ВИТС, имеет иерархическую организацию.

Схема организации ТТП показана на рис. 28.

Главной функцией ТТП ЕАИС ТО является обеспечение надёжной бесперебойной доставки данных между прикладными процессами, инициируемыми компонентами ЕАИС ФТС.

ТТП ЕАИС ФТС обеспечивает:

- гарантированную доставку сообщений, сформированных прикладными процессами, в условиях возможных программно-аппаратных сбоев, нарушений в работе телекоммуникационных систем, сбоев в системе электропитания объектов;
- предотвращение повторной доставки сообщений вследствие нарушений в работе ТТП ЕАИС ФТС;

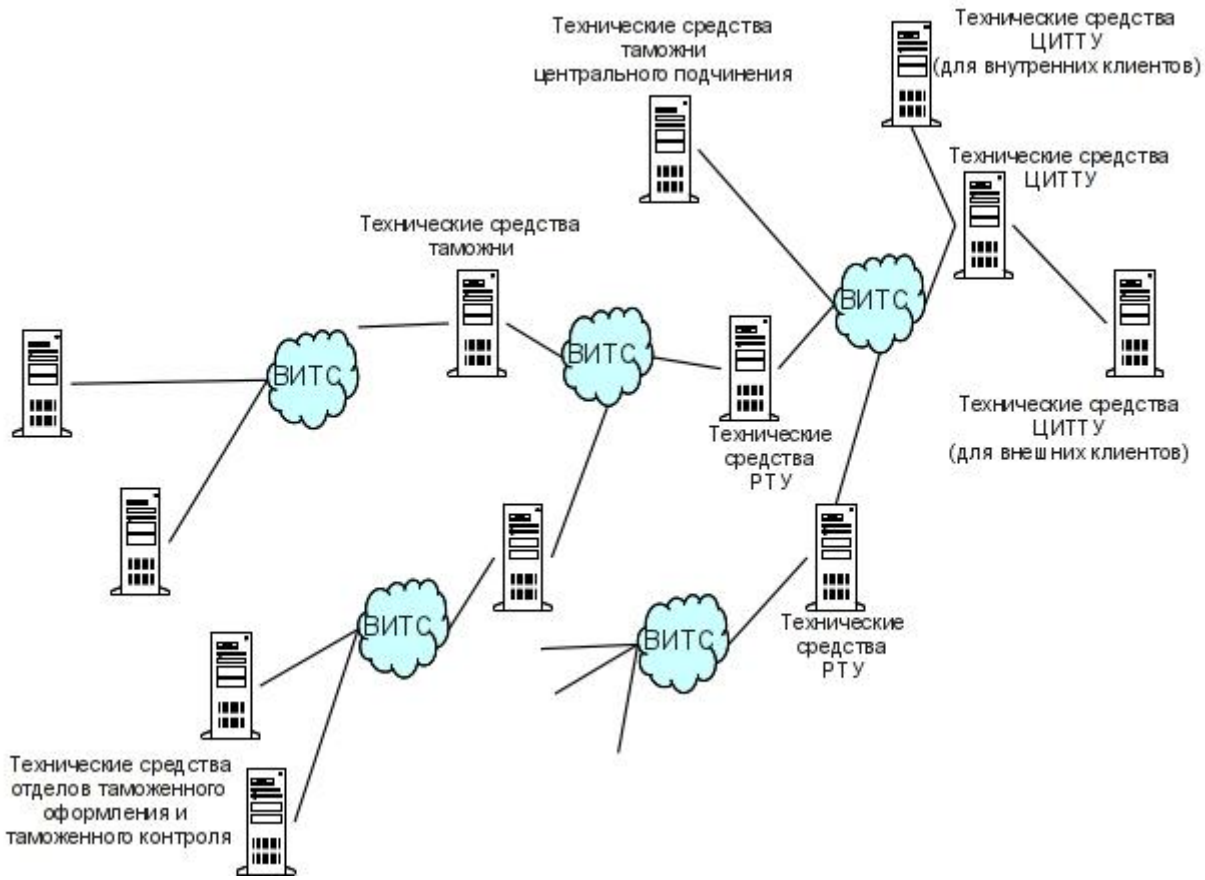

Рис. 28. Схема организации ТТП ЕАИС ФТС

• оптимизацию использования каналов связи в части сегментации передаваемых данных, приоритетности их передачи и сроков доставки;

• возобновление передачи сообщения в случае разрыва связи, начиная с первого не переданного сегмента;

• возможность использования резервных каналов связи;

• возможность ввода приоритетов и поддержку правил очередности передачи сегментов данных или потоков данных, в зависимости от установленного для них приоритета;

• поддержку рассылки сообщения по заданному множеству адресатов без избыточного дублирования информации, передаваемой через один и тот же транспортный канал ВИТС ФТС;

• предотвращение несанкционированного доступа к сообщениям при их передаче по эксплуатируемым в таможенных органах сетям и системам передачи данных;

• возможность контроля текущего статуса сообщений, потоков данных и технологических схем, оперативного управления ими;

• подробное диагностическое протоколирование работы ТТП.

В ТТП ЕАИС ФТС реализован единый набор функций передачи данных и контроля процессов обмена данными вне зависимости от особенностей используемых операционных систем, средств вычислительной техники и аппаратуры телекоммуникаций. Технологически элементы ТТП функционируют как **web-сервисы**.

В настоящее время в ТТП ЕАИС ФТС используется программное обеспечение IBM WebSphere Business Integration Message Broker (для интеграции различного типа бизнес-приложений и систем электронного документооборота, обеспечивающий перераспределение, обработку и перенаправление потоков информации, данных и сообщений между интегрируемыми системами) и IBM WebSphere MQ (MQSeries) – средство передачи сообщений с гарантированной доставкой и приоритезацией.

С точки зрения транспортной системы компоненты участвующие в процессах таможенного оформления и контроля, расположенные в региональных таможенных управлениях (РТУ), таможнях и таможенных постах формируют файлы, содержащие платёжные документы, статистическую информацию, архивы, которые передаются в соответствующие головные организации и обратно.

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

Автоматизированная система внешнего домена (АСВД) представляет собой совокупность Центрального шлюза АСВД, размещённого в ДМЗ ЦИТТУ и Региональных шлюзов (точек доступа) АСВД, размещённых в ДМЗ РТУ.

ДМЗ (демилитаризованная зона, DMZ) – часть (сегмент) локальной сети предприятия, в котором отсутствуют рабочие станции пользователей (имеются только серверы), все соединения с которым организованы через межсетевые экраны (firewall).

АСВД используется для организации информационного обмена между участниками ВЭД, работающими с использованием Интернет, и подразделениями ФТС, использующими ВИТС. (АСВД – связь между Интернет и ВИТС.).

Центральная база данных (ЦБД) ЕАИС ФТС России была организована в 1990 году для решения задач централизованного сбора, хранения и обработки ТДэ (таможенных деклараций в электронном виде).

Для обеспечения полноты, достоверности ЦБД и оперативности поступления информации из таможенных органов была внедрена многоступенчатая технология сбора и контроля информации. Внедрение этой технологии стало возможным после разработки АРМ ТИ (автоматизированное рабочее место таможенного инспектора) и АРМ «Достоверность».

ЦБД ЕАИС представляет собой систему баз данных центрального аппарата таможенной системы. ЦБД ЕАИС включает технические средства центрального вычислительного комплекса, СУБД (ORACLE), средства ведения баз данных и непосредственно данные.

ЦБД ЕАИС позволяет решать задачи таможенной статистики внешней

торговли, выполнять запросы Правительства, руководства ФТС и сторонних организаций. Для ЦБД ЕАИС разработаны как программные средства, решающие регламентные задачи ЕАИС, так и программные средства формирования гибких запросов.

В состав центрального вычислительного комплекса входит несколько многопроцессорных ЭВМ с характеристиками в соответствии с объемами хранимых данных и решаемых задач.

Объем информации, хранящейся и обрабатываемой в ЦБД, можно оценить, исходя из вариантов первичных данных и перечня документов и сведений, представляемых таможенному органу в зависимости от вида транспорта, на котором осуществляется перевозка товаров.

В качестве первичных данных используются:

- Данные о грузах,
- данные о транспортных средствах,
- данные о грузоотправителях,
- данные о грузополучателях,
- данные о грузоперевозчиках,
- данные о декларантах,
- данные о таможеннных терминалах,
- данные о складах временного хранения,
- данные об опасных грузах и материалах,
- данные о товарах и веществах, запрещённых к ввозу на территорию Таможенного Союза
- и многие другие данные

В соответствии со статьёй 159 ТК ТС. «Документы и сведения, представляемые таможенному органу в зависимости от вида транспорта, на котором осуществляется перевозка товаров» для таможенного оформления требуются следующие документы и сведения:

1. при международной перевозке автомобильным транспортом:

- документы:
  - документы на транспортное средство международной перевозки;
  - транспортные (перевозочные) документы;
  - документ, сопровождающий международные почтовые отправления при их перевозке, определённый актами Всемирного почтового союза;
  - имеющиеся у перевозчика коммерческие документы на перевозимые товары;
- сведения:
  - о государственной регистрации транспортного средства международной перевозки;

- наименование и адрес перевозчика товаров;
- наименование страны отправления и страны назначения товаров;
- наименование и адрес отправителя и получателя товаров;
- о продавце и получателе товаров в соответствии с имеющимися у перевозчика коммерческими документами;
- о количестве грузовых мест, об их маркировке и о видах упаковок товаров;
- наименование, а также коды товаров в соответствии с Гармонизированной системой описания и кодирования товаров или Товарной номенклатурой внешнеэкономической деятельности на уровне не менее чем первых четырёх знаков;
- вес брутто товаров (в килограммах) либо объем товаров (в кубических метрах), за исключением крупногабаритных грузов;
- о наличии товаров, ввоз которых на таможенную территорию таможенного союза запрещён или ограничен;
- о месте и дате составления международной товаротранспортной накладной;

2. при международной перевозке водными судами:

- документы:
  - общую декларацию;
  - декларацию о грузе;
  - декларацию о судовых припасах;
  - декларацию о личных вещах экипажа судна;
  - судовую роль;
  - список пассажиров;
  - документ, сопровождающий международные почтовые отправления при их перевозке, определённый актами Всемирного почтового союза;
  - транспортные (перевозочные) документы;
  - имеющиеся у перевозчика коммерческие документы на перевозимые товары;
- сведения:
  - о регистрации судна и его национальной принадлежности;
  - наименование и описание судна;
  - фамилия капитана;
  - фамилия и адрес судового агента;
  - о количестве пассажиров на судне, их фамилии, имена, гражданство (подданство), даты и места рождения, порт посадки и высадки;
  - о количестве и составе членов экипажа;
  - наименование порта отправления и порта захода судна;

- наименование, общее количество и описание товаров;
- о количестве грузовых мест, об их маркировке и о видах упаковок товаров;
- наименование порта погрузки и порта выгрузки товаров;
- номера коносаментов или иных документов, подтверждающих наличие и содержание договора морской (речной) перевозки, на товары, подлежащие выгрузке в этом порту;
- наименование портов выгрузки остающихся на борту товаров;
- наименование первоначальных портов отправления товаров;
- наименование судовых припасов, имеющихся на судне, и указание их количества;
- описание размещения товаров на судне;
- о наличии (об отсутствии) на борту судна международных почтовых отправлений;
- о наличии (об отсутствии) на борту судна товаров, ввоз которых на таможенную территорию таможенного союза запрещён или ограничен, лекарственные средства, в составе которых содержатся наркотические, сильнодействующие средства, психотропные и ядовитые вещества;
- о наличии (об отсутствии) на борту судна опасных товаров, включая оружие, боеприпасы;

3. при международной перевозке воздушным транспортом:

- документы:
  - стандартный документ перевозчика, предусмотренный международными договорами в области гражданской авиации (генеральная декларация);
  - документ, содержащий сведения о перевозимых на борту воздушного судна товарах (грузовая ведомость);
  - документ, содержащий сведения о бортовых припасах;
  - транспортные (перевозочные) документы;
  - имеющиеся у перевозчика коммерческие документы на перевозимые товары;
  - документ, содержащий сведения о перевозимых на борту пассажирах и их багаже (пассажирская ведомость);
  - документ, сопровождающий международные почтовые отправления при их перевозке, определённый актами Всемирного почтового союза;
- сведения:
  - указание знаков национальной принадлежности и регистрационных знаков судна;
  - номер рейса, указание маршрута полёта, пункта вылета, пункта прибытия судна;
  - наименование эксплуатанта судна;

- о количестве членов экипажа;
- о количестве пассажиров на судне, их фамилии и инициалы, наименование пунктов посадки и высадки;
- наименование товаров;
- номер грузовой накладной, количество мест по каждой грузовой накладной;
- наименование пункта погрузки и пункта выгрузки товаров;
- о количестве бортовых припасов, погружаемых на судно или выгружаемых с него;
- о наличии (об отсутствии) на борту судна международных почтовых отправлений;
- о наличии (об отсутствии) на борту судна товаров, ввоз которых на таможенную территорию таможенного союза запрещён или ограничен, лекарственные средства, в составе которых содержатся наркотические, сильнодействующие средства, психотропные и ядовитые вещества, оружие, боеприпасы;

4. при международной перевозке железнодорожным транспортом:

- документы:
  - транспортные (перевозочные) документы;
  - передаточная ведомость на железнодорожный подвижной состав;
  - документ, содержащий сведения о припасах;
  - документ, сопровождающий международные почтовые отправления при их перевозке, определённый актами Всемирного почтового союза;
  - имеющиеся у перевозчика коммерческие документы на перевозимые товары;
- сведения:
  - наименование и адрес отправителя товаров;
  - наименование и адрес получателя товаров;
  - наименование станции отправления и станции назначения товаров;
  - о количестве грузовых мест, об их маркировке и о видах упаковок товаров;
  - наименование, а также коды товаров в соответствии с Гармонизированной системой описания и кодирования товаров или Товарной номенклатурой внешнеэкономической деятельности не менее чем на уровне первых четырёх знаков;
  - вес брутто товаров (в килограммах);
  - идентификационные номера контейнеров.

В состав ЦБД ЕАИС входят:

- БД НСИ (база данных нормативно-справочной информации)

• ЦБД ТД, содержащая данные ТДэ (таможенные декларации в электронном виде), ДТСэ (электронные декларации транспортных средств), КТСэ (электронные корректировки таможенной стоимости), описей документов по ТД, данные оперативного мониторинга

• БД валютного контроля, содержащая данные о движении капиталов и перемещении через таможенную границу денежных средств и наличной валюты

• БД контроля доставки товаров (сведения о документах контроля доставки, книжках МДП и др. сведения, необходимые для контроля доставки грузов от приграничного пункта пропуска товаров к месту таможенного оформления)

• БД ТПО (база данных таможенных приходных ордеров)

• БД таможенных платежей (таблицы лицевых счетов участников ВЭД, сведения о поступлении денежных средств от участников ВЭД на счета Федерального казначейства, перечислении средств в Госбюджет и т.д.)

• БД электронной корреспонденции

• служебные базы данных в виде хранилищ, витрин и т.д. для выполнения срочных запросов, получения отчётности, а также другие базы данных сравнительно небольшого объёма.

ЦБД ТД является ядром ЦБД ЕАИС. Эта база данных содержит сведения об основных документах таможенного оформления и используется при решении задач практически всех подсистем. К ЦБД ТД одновременно обращается более 1000 пользователей. База данных обновляется ежедневно в оперативном режиме на основе сведений, переданных таможенными органами.

ЦБД ТД содержит два сегмента:

• выпущенные ТД (оформление закончено)

• оперативная информация (ТД, оформление по которым продолжается).

Для удобства обработки ЦБД ТД разделена по годам. В среднем в течение года (по данным 2012 года) оформляется 2.5 млн. ТД со сведениями о более 5 млн. товаров. В составе основной БД 150 таблиц (не считая вспомогательных). Годовой объем собираемых данных около 100 Гбайт.

Технология сбора данных для ЦБД ЕАИС включает четыре уровня иерархии таможенной системы: таможенный пост ⇒ таможня ⇒ региональное таможенное управление (РТУ) ⇒ ЦИТТУ ФТС России.

На уровне таможенного поста производятся основные действия по формированию, корректировке и контролю электронных копий документов. Это объясняется тем, что только в местах таможенного оформления есть возможность сопоставления электронных копий документов с первичными документами на бумажных носителях.

В связи с этим технология сбора данных на уровнях таможни, РТУ и ЦИТТУ предполагает операции форматно-логического контроля (ФЛК) данных, формирования базы данных ТД и документов, оформленных подчинёнными органами и передачу данных в вышестоящий таможенный орган. При обнаружении ошибок в процессе форматно-логического контроля ТД направляется в нижестоящий таможенный орган, а из него – до уровня поста, где вносятся необходимые исправления.

Форматно-логический контроль данных ТДэ, ДТСэ, КТСэ и описей документов на уровнях РТУ и таможни производится с использованием АРМ «Достоверность», имеющем средства полного контроля заполнения реквизитов ТДэ в соответствии с действующими на момент оформления нормативными актами. В РТУ и таможнях используется версия АРМ «Достоверность», реализованная с использованием системы программирования Clipper (по данным 2012 года), в ЦИТТУ – версия «Достоверность» в среде СУБД Oracle.

Система «тотального» контроля на всех этапах сбора данных позволяет минимизировать ошибки, повысить достоверность как баз данных, так и результатов решаемых задач.

Основные комплексы автоматизированных средств таможенного оформления (КАСТО) и комплексы программных средств (КПС)

- КПС «Агент ВК» (валютный контроль)
- КПС «Ведение БДПР» (база данных профилей рисков)
- КАСТО АИСТ-М
- КПС «УКИД-2».

КПС «Агент ВК» используется в системе валютного контроля (СВК). Программные средства, используемые в СВК представляют собой единый комплекс по автоматизированному сбору, обработке, передаче и загрузки в региональные базы данных валютного контроля (РБД ВК) и в центральную базу данных валютного контроля (ЦБД ВК) материала, необходимого для проведения проверки полноты и достоверности сведений, указанных в электронных копиях паспорта сделки и реестра учётных документов, формируемого по внешнеторговому контракту.

К таким ПС относятся:

- КПС учёта валютных операций (КПС «Учет ВО»)
- КПС организации контроля валютных операций (КПС «Контроль ВО»)
- КПС агента ВК для уровней РТУ и таможен
- КПС организации и ведения региональной базы данных результатов валютного контроля (КПС «Ведение РБД ВК», для загрузки электронных

копий документов ВК в базу данных ВК РТУ и таможен, непосредственно подчинённых ФТС

• КПС сбора информации и ведения базы данных электронной корреспонденции по валютным операциям (КПС «Сбор ЭК ВО»)

КПС «Ведение БДПР» – один из главных программных комплексов системы управления рисками (СУР), разработанный в 2004 году.

Состав КПС «Ведение БДПР»:

• Программная задача (ПЗ) «Формирование проектов профилей рисков»/ПЗ «Формирование профилей рисков»
• ПЗ «Модуль управления пользователями»
• ПЗ «Модуль синхронизации базы данных профилей рисков»
• ПЗ «Сервер приложений ведения базы данных профилей рисков»

Назначение **КАСТО АИСТ-М** – обеспечение работы инспектора ОТОиТК (отдела таможенного оформления и таможенного контроля) и задействованных в процессе таможенного оформления специалистов других подразделений, предоставляя возможность доступа ко всем ресурсам ЕАИС в режиме реального времени.

АИСТ-М позволяет управлять процессом документального таможенного оформления и обеспечивать его «прозрачность» для руководителя таможенного органа и для участников ВЭД. Все подсистемы (ПС, ПЗ), входящие в АИСТ-М, могут настраиваться на организационную структуру таможенного органа, в котором они работают.

КАСТО АИСТ-М является результатом совместной разработки нескольких российских компаний: ЗАО «Тамга», ООО «СофтЛэнд», «ЗАО Инмар».

Структурная схема АИСТ-М (программные средства и программные задачи) показана на рис. 29.

КПС «УКИД-2» - комплекс программных средств учета и контроля исполнения документов — предназначен для автоматизации процессов документационного обеспечения деятельности ФТС России (регистрации и учёта документов, подготовки проектов резолюций, доведения поручений руководства до исполнителей и контроля хода их исполнения).

Основной целью разработки «УКИД-2» является создание высокоэффективной информационной системы автоматизации учета и контроля прохождения и исполнения документов в подразделениях ФТС России, повышение эффективности контроля исполнения документов вышестоящих таможенных органов, приказов, распоряжений и поручений руководства, писем ведомств, организаций и обращений граждан. Применение КПС «УКИД-2» ведёт к значительному сокращению объёма бумажного документооборота за счёт полного перехода 100-процентному электронному документообороту.

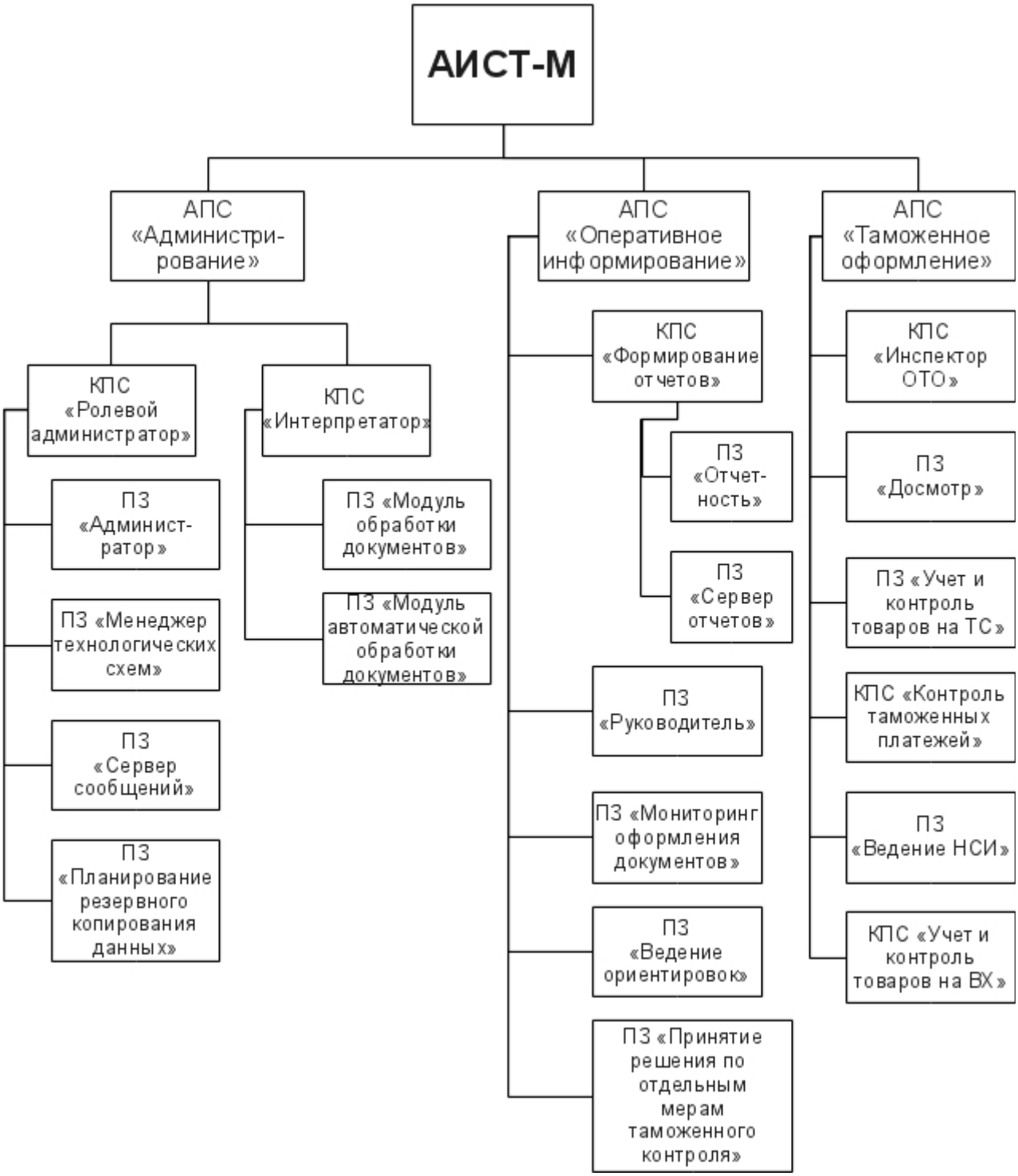

Рис. 29. Компоненты КАСТО АИСТ-М.

Внедрение «УКИД-2» позволяет повысить исполнительскую дисциплину в подразделениях ФТС России, оптимизировать процессы и регламенты подготовки документов.

Данный КПС обеспечивает автоматизированное выполнение основных процедур современного делопроизводства, включая систематизацию, обработку и безопасное хранение значительных объёмов информации.

Системы электронного предоставления сведений

При описании автоматизированных систем, используемых в подразделениях ФТС Российской Федерации, часто встречаются специальные сокращения. Часть из этих сокращений (ЕАИС, ТТП, ВИТС, АСВД) и соответствующих им понятий уже были рассмотрены ранее. Другие часто используемые сокращения приведены ниже.

- **ТД** – таможенная декларация
- **ЭТД** – таможенная декларация в виде электронного документа
- **ЭПД** – предварительная таможенная декларация в электронном виде
- **СТТ** – сведения о товарах и транспортных средствах в электронном виде
- **ФЛК** – форматно-логический контроль документов
- **XML** – международный стандарт описания документов в электронном виде
- **ТО и ТК** – таможенное оформление и таможенный контроль
- **ТиТС** – товары и транспортные средства
- **УОИТО** – узел обработки информации таможенного органа
- **КПС «Портал ЭД»** – портал электронного представления сведений для электронного декларирования через Интернет
- **КПС «Декларант ЭДТиТС»** – комплекс программных средств электронного декларирования товаров и транспортных средств для использования участниками ВЭД при электронном представлении сведений через интернет. КПС «Декларант ЭДТиТС» предоставляется бесплатно по заявке участников ВЭД, подаваемой в ЦИТТУ. Для использования требуется соблюдения ряда требований, регламентированных нормативными правовыми актами ФТС России.

- **СПрИнТ** – система предварительного информирования таможенных органов Российской Федерации
- **АС КТТ** – автоматизированная система контроля таможенного транзита
- **NCTS** – новая компьютеризированная транзитная система стран ЕС
- **ПО ИС ЭПС** – программное обеспечение информационных систем, предназначенных для представления участниками внешнеэкономической деятельности или иными заинтересованными лицами сведений таможенным органам в электронной форме на соответствие технической документации
- Порядок **ПТД ЭПС** – порядок предоставления технической документации, регламентирующей взаимодействие информационных систем таможенных органов и информационных систем, предназначенных для представления участниками внешнеэкономической деятельности сведений таможенным органам в электронной форме

• Порядок **ПИС АСВД** – порядок подключения информационных систем, предназначенных для представления участниками внешнеэкономической деятельности сведений таможенным органам в электронной форме с использованием информационно-вычислительных сетей общего пользования

Порядок **ПИС АСВД** определяет условия и последовательность подключения информационных систем, предназначенных для представления участниками внешнеэкономической деятельности сведений таможенным органам в электронной форме (**ИС ЭПС**) с использованием информационно-вычислительных сетей общего пользования (включая международную ассоциацию сетей «Интернет») (**ИВС ОП**), к Автоматизированной системе внешнего доступа таможенных органов (**АСВД**).

• Порядок **ТИС ЭПС** – порядок проведения испытаний программного обеспечения информационных систем, предназначенных для представления участниками внешнеэкономической деятельности сведений таможенным органам в электронной форме.

Под системой **электронного представления сведений** подразумевается комплекс задач обеспечивающий приём от участника ВЭД сведений в электронном виде необходимых и достаточных для проведения таможенного оформления и контроля как в на границе в пограничном пункте пропуска, так и в месте доставки, декларирования товара.

В общем виде система состоит из:

• Автоматизированной Системы Внешнего Доступа (АСВД), обеспечивающую взаимодействие с «внешним миром» т.е. и информационными системами участников ВЭД, в том числе и декларантами.

• Транспортной технологической подсистемы (ТПП) обеспечивающей передачу данных между различными уровнями таможенной иерархии.

• Собственно автоматизированной подсистемы системы (АПС) электронного представления сведений, принимающей и обрабатывающей данные поступающие от участников ВЭД и предоставляющей эти данные КАСТО АИСТ-РТ21 и АСТО АИСТ-М или АСТО ППП.

Электронное представление сведений может использоваться как при предварительном информировании таможенных органов, так и при электронном декларировании.

Предварительное информирование подразумевает передачу сведений о товарах и транспортных средствах в таможенные органы, расположенные в пограничном пункте пропуска, необходимые и достаточных для таможенного оформления.

Электронное декларирование – это **предоставление ТД** и части или всех

сопутствующих документов в электронном виде.

Основные цели предварительного информирования и электронного декларирования:

- ускорение товарооборота
- сокращение времени таможенного оформления
- внедрение безбумажных технологий при таможенном оформлении и таможенном контроле.

Технологии электронного декларирования товаров и транспортных средств

Оформление поставок производится путём подачи **Таможенной декларации (ТД)**. При электронном декларировании ТД подаётся только **в электронном виде**.

Внедрение технологий электронного декларирования (ЭД) преследует следующие цели:

- сокращение времени таможенного оформления
- сокращение или устранение личных контактов представителей декларанта и таможни
- внедрение принципа «одного окна».

Использование технологий электронного декларирования вместо оформления «бумажных» деклараций и сопутствующих документов обеспечивает следующие преимущества:

- ликвидация ряда избыточных операций, связанных с проверкой документов в бумажном виде, сверки электронных и бумажных копий документов
- высокая надёжность и низкая трудоёмкость проверки подлинности электронных документов и подписей
- возможность обезличенной обработки ГТД и полного протоколирования выполненных действий и принятых решений (*электронное декларирование как антикоррупционная мера*). В АИСТ-РТ21 это реализовано частично, т.к. в связи с наличием бумажных копий, не обезличены приём-выдача документов.
- возможность полной автоматизации некоторых ручных операций таможенного оформления, например этапов регистрации и ФЛК (форматно-логического контроля)
- разгрузка архивов – электронный архив гораздо меньше и проще в обслуживании

Процедуры и требования к участникам электронного декларирования регламентируются следующими нормативными документами.

1. Приказ ФТС России N 183 от 3 февраля 2010 года «Об утверждении

Порядка организации процессов жизненного цикла программных средств информационных систем и информационных технологий таможенных органов».

2. Решение Комиссии Таможенного союза N 494 от 08.12.2010. «Об Инструкции о порядке предоставления и использования таможенной декларации в виде электронного документа».

3. Приказ ФТС России N 1266 от 28.06.2012. «Об утверждении Порядка эксплуатации средств криптографической защиты информации, реализующих механизмы электронной подписи, должностными лицами (работниками) таможенных органов Российской Федерации».

4. Приказ ФТС России N 1008 от 24.05.2012. «О вводе в эксплуатацию комплекса программных средств "Портал электронного представления сведений для электронного декларирования через интернет"».

5. Приказ ФТС России N 2187 от 25.10.2011. «Об утверждении Положения об использовании участниками внешнеэкономической деятельности и лицами, осуществляющими деятельность в сфере таможенного дела, средств электронной подписи при реализации информационного взаимодействия с таможенными органами Российской Федерации».

6. Распоряжение ФТС России N 165-р от 14.09.2011. «Об утверждении Временной информационной технологии взаимодействия лиц, осуществляющих декларирование товаров и транспортных средств в электронной форме при удаленной уплате таможенных пошлин, налогов с использованием электронного терминала, координатора эмиссии микропроцессорных пластиковых карт и Федеральной таможенной службы».

7. Приказ ФТС России N 845 от 22.04.2011. «Об утверждении Порядка совершения таможенных операций при таможенном декларировании в электронной форме товаров, находящихся в регионе деятельности таможенного органа, отличного от места их декларирования».

8. Приказ ФТС России N 695 от 01.04.2011. «Об утверждении Временного порядка совершения должностными лицами таможенных органов таможенных операций при таможенном декларировании в электронной форме товаров, классифицируемых в группе 27 ТН ВЭД ТС, в соответствии с приказом ФТС России от 3 декабря 2010 г. N 2330 "О местах декларирования отдельных видов товаров" в случае, если местонахождение данных товаров или место их погрузки и (или) перегрузки (перевалки) не совпадает с местом их декларирования».

9. Письмо ФТС России N 01-11/34924 от 22.07.2012. «О применении технологии удаленного выпуска товаров».

10. Приказ ФТС России N 2244 от 25.11.2010. «Об установлении компетенции таможенных постов».

11. Приказ ФТС России N 317 от 18.02.2010. «Об утверждении перечня таможенных органов, осуществляющих таможенные операции и

таможенный контроль в отношении товаров в соответствии с приказом ФТС России от 22 апреля 2011 г. N 845».

12.Приказ ФТС России N 1452 от 11.08.2009. «О вводе в опытную эксплуатацию информационной технологии представления таможенным органам сведений в электронной форме для целей таможенного оформления товаров с использованием международной ассоциации сетей "Интернет" в таможенных органах, подчиненных Сибирскому, Уральскому и Дальневосточному таможенным управлениям».

13.Приказ ФТС России N 52 от 24.01.2008. «О внедрении информационной технологии представления таможенным органам сведений в электронной форме для целей таможенного оформления товаров, в том числе с использованием международной ассоциации сетей "Интернет"».

14.Приказ ФТС России N 646 от 24.05.2007. «Об утверждении Порядка включения таможенных органов в Перечень таможенных органов, имеющих достаточную техническую оснащенность для применения электронной формы декларирования».

15.Приказ ФТС России N 1062 от 30.10.2006. «Об обеспечении безопасности информации при информационном взаимодействии таможенных органов с участниками внешнеэкономической деятельности и сетями общего пользования».

16.Приказ ФТС России N 64 от 31.01.2005. «О решении коллегии ФТС России от 17.12.2004 "О программе развития и внедрения в таможенных органах Российской Федерации электронной формы декларирования товаров и транспортных средств"».

17.Распоряжение ФТС России N 77-р от 26.10.2004. «О передаче Центральному таможенному управлению прав администрирования комплекса программных средств "Обработка сведений в электронной форме о товарах и транспортных средствах"».

18.Приказ ГТК России N 564 от 13.05.2004. «Об утверждении Положения об организации проверок информационных систем, информационных технологий и средств их обеспечения, используемых участниками внешнеэкономической деятельности».

19.Приказ ГТК России N 395 от 30.03.2004. «Об утверждении Инструкции о совершении таможенных операций при декларировании товаров в электронной форме».

Возможны две схемы взаимодействия участника ВЭД с системой ЭД — напрямую (**прямая схема**) и через информационного оператора.

К участникам **прямой схемы** предъявляются некоторые обязательные требования, в частности:

• на средства вычислительной техники информационной системы электронного представления сведений (ИС ЭПС) в обязательном порядке должны быть установлены лицензионные операционные системы,

сертифицированные Федеральной службой по техническому и экспортному контролю (далее — ФСТЭК России) по требованиям безопасности информации;

• программное обеспечение ИС ЭПС должно быть включено в реестр оформленных и выданных свидетельств ПО ИС ЭПС.

Требования, предъявляемые к техническим средствам и средствам защиты информации ИС ЭПС:

• на средства вычислительной техники ИС ЭПС в обязательном порядке должны быть установлены лицензионные средства антивирусной защиты информации, сертифицированные ФСТЭК России и Федеральной службой безопасности России (далее — ФСБ России) по требованиям безопасности информации;

• для обеспечения целостности и юридической значимости передаваемой информации в процессе информационного взаимодействия должны использоваться сертифицированные ФСБ России средства криптографической защиты информации и электронной цифровой подписи, совместимые с системой ведомственных удостоверяющих центров таможенных органов (далее — СВУЦТО);

• должны быть обеспечены разграничение и контроль доступа должностных лиц Заявителя к ресурсам ИС ЭПС с использованием сертифицированных средств защиты информации (ИС ЭПС должна быть аттестована по требованиям безопасности информации).

При организации данной схемы необходимо обеспечить:

• со стороны оборудования:

- интернет-канал со статическим IP;
- аппаратно-программный комплекс шифрования (АПКШ) «Континент»;
- систему защиты информации от несанкционированного доступа типа «Аккорд» или «Соболь»;

• со стороны программного обеспечения:

- операционную систему Microsoft Windows не старше Windows XP (сертифицированную Федеральной службой по техническому и экспортному контролю (далее — ФСТЭК));
- антивирусное программное обеспечение (сертифицированное ФСТЭК);
- средство криптографической защиты информации «КриптоПро CSP» версий 3.6 или более новое, включая процедуру получения ЭЦП в Главном научно-информационном вычислительном центре (ГНИВЦ) ФТС России (приобретается самостоятельно);

- программное обеспечение, прошедшее сертификацию в ЦИТТУ;
- наличие сертификата соответствия требованиям безопасности информации (аттестация на соответствие рабочего места или сегмента локальной сети требованиям безопасности информации) (приказ ФТС России от 24 января 2008 г. No 52);
- подготовку и отправку заявки в ЦИТТУ в соответствии с приказом No 52. По истечении срока рассмотрения заявки в случае положительного решения заключить с ЦИТТУ соглашение на подключение к системе ЭД;
- подготовку и отправку заявки в ЦИТТУ на получение ЭЦП.

Принимая во внимание вышесказанное, становится ясно, что прямая схема является достаточно затратным мероприятием, как финансово, так и по времени.

Рассмотрим прямую схему работы.

Специалист по таможенному оформлению подготавливает электронный пакет, состоящий из ТД, ДТС и описи, проставляет свою ЭЦП и отправляет в ЦИТТУ, где проверяется право доступа конкретного участника ВЭД к системе ЭД и достоверность его ЭЦП. Затем происходит пересылка пакета документов из ГНИВЦ по таможенной транспортной технологической подсистеме (ТТП) в базу данных регионального таможенного управления (РТУ), где ТД и другие документы проходят первичный форматный контроль, после чего поступают на таможенный пост, на котором и происходит осуществление таможенных операций.

После начала осуществления таможенных операций от таможни может прийти запрос на дополнительные документы. В ответ необходимо будет подготовить и отправить электронный документ. В случае необходимости проведения досмотра таможня присылает уведомление о досмотре, получение которого надо будет подтвердить. После проведения досмотра декларанту высылается акт досмотра.

Сообщение о завершении таможенных операций (или о переводе на общеустановленный порядок таможенных операций) поступает к участнику ВЭД, проходя обратно по таможенным каналам.

Алгоритм информационного взаимодействия для электронного декларирования показан на рис. 30.

В случае организации схемы взаимодействия через информационного оператора (рис. 31) возникают следующие преимущества:

• нет необходимости закупать дорогостоящее оборудование;

• нет необходимости согласовывать схему подключения;

• нет необходимости держать в штате квалифицированного

IT-специалиста;

• нет необходимости проходить процесс сертификации;

• для работы с системой достаточно даже низкоскоростного интернет-канала;

• наличие квалифицированной технической поддержки со стороны оператора по вопросам связи с таможней.

При организации данной схемы необходимо обеспечить:

- со стороны оборудования:
  - свободный USB-порт;
  - интернет-канал;
  - VPN -ключ предоставляется информационным оператором.

VPN-key® — представляет собой персональное средство защиты информации, предназначенное для выполнения криптографических преобразований, строгой аутентификации, безопасного хранения ключевой информации и аутентификационных данных (предоставляется информационным оператором);

  - USB-токен RuToken — аппаратную реализацию российского стандарта электронной цифровой подписи. RuToken предназначен для аутентификации пользователей при доступе к секретной информации, для безопасного хранения и использования ключей шифрования и ЭЦП, паролей, цифровых сертификатов. Может применяться для решения задач авторизации и разделения доступа в сетях, обеспечения необходимого уровня безопасности при работе с электронной почтой, для безопасного подключения удалённых пользователей. Покупка RuToken относится к дополнительным (необязательным) услугам;

- со стороны программного обеспечения:
  - операционную систему Microsoft Windows не старше Windows XP;
  - антивирусное программное обеспечение;
  - средство криптографической защиты информации «Крипто-Про CSP» версий 3.0, 3.6 или более новое (приобретается самостоятельно);
  - программное обеспечение, прошедшее сертификацию в ЦИТТУ ФТС России.

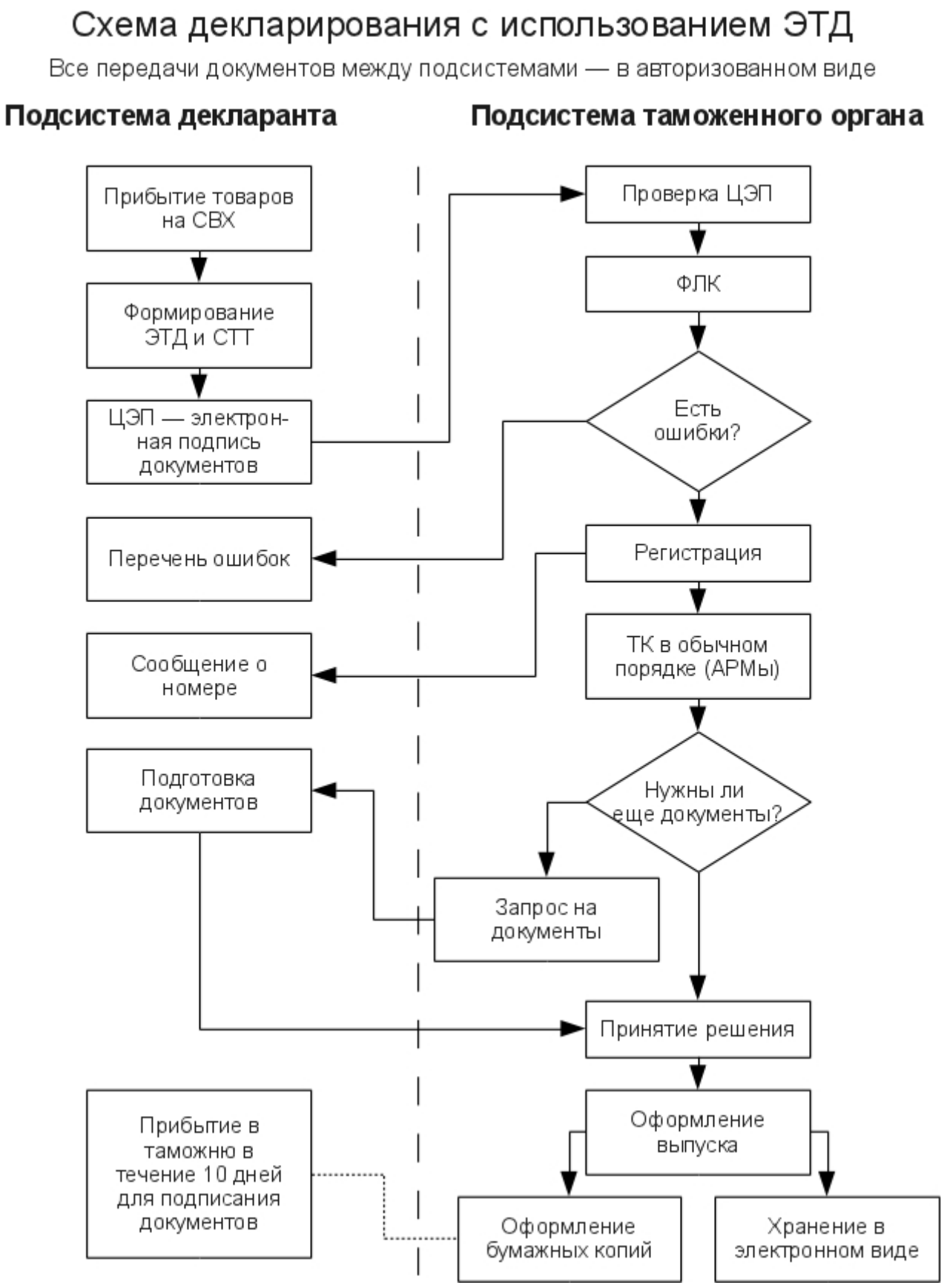

Рис. 30. Взаимодействие участника ВЭД и таможенных органов при электронном декларировании.

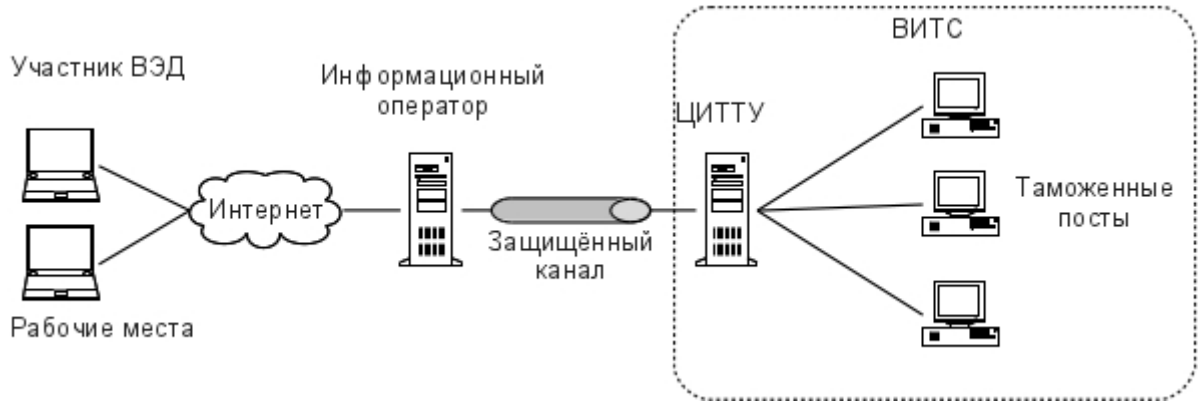

Рис. 31. Схема электронного декларирования через информационного оператора.

Фактически информационный оператор устанавливает у себя сервер маршрутизации с лицензированной операционной системой и антивирусным программным обеспечением, аппаратно-программный комплекс шифрования (АПКШ) «Континент», а также обеспечивает выполнение всех требований безопасности вплоть до защиты от несанкционированного доступа в помещение, в котором установлен сервер маршрутизации.

По всем параметрам данная схема является наиболее оптимальной для конечного пользователя. Информационный оператор — организация, которая предоставляет канал передачи информации и обеспечивает выполнение требований безопасности при пересылке сведений в системе ЭД через Интернет. Информационный оператор фактически берет на себя роль связующего звена между участниками ВЭД и таможенными органами, а также может оказывать техническую поддержку по настройке каналов передачи информации, установке и обслуживанию программных продуктов, сертифицированных для работы с системой ЭД.

К разным участникам описанной выше схемы взаимодействия предъявляются разные требования в части их технического оснащения. Участники ВЭД должны получить ЭЦП и установить у себя программное обеспечение для оформления ТД и сопутствующих документов, прошедшее сертификацию в ЦИТТУ.

Список информационных операторов, с которыми у ЦИТТУ заключены соглашения об информационном взаимодействии при представлении сведений в электронной форме с использованием международной ассоциации сетей «Интернет», можно найти на портале Федеральной Таможенной службы www.customs.ru в разделе «Информация для участников ВЭД».

Ряд операторов в своей деятельности использует КПС «Декаларант ЭДТиТС» – ЗАО «НПО «Персей», ООО «ТЛЦ», ЗАО «МСИ-сервис», ЗАО «Филип Моррис Ижора».

В 2008 г. ФТС России разработала концепцию переноса таможенных операций в районы, приближенные к таможенной границе РФ.

Благодаря электронному декларированию через Интернет участники ВЭД могут оформлять свои грузы на любой пограничной таможне, не тратя деньги на оборудование офисов и перевод специалистов в приграничные районы. Кроме того, система привлекательна для осуществления таможенных операций с некоторыми специфическими грузами, например продукцией морского промысла. При подключении к системе электронного декларирования такую продукцию фактически можно будет оформлять до захода судна в порт, что ведёт к упрощению процесса таможенного контроля.

Внедрение данной технологии в процесс таможенного контроля должно создать условия для приведения таможенных процедур в Российской Федерации в соответствие с положениями Международной конвенции об упрощении и гармонизации таможенных процедур.

С 1.01.2014 использование электронного декларирования является обязательным.

Современная система электронного декларирования (ЭД-2) работает с использованием каналов Интернет. В технологии ЭД-2 не предусмотрена передача сканированных версий ТД. ДТС,и других таможенных документов. Однако при использовании ЭД-2 есть возможность передавать дополнительные документы, не предусмотренные форматом ЭТД (формат «free-doc»).

При обработке декларации в технологии ЭД-2 реализуются этапы, показанные на рис. 32.

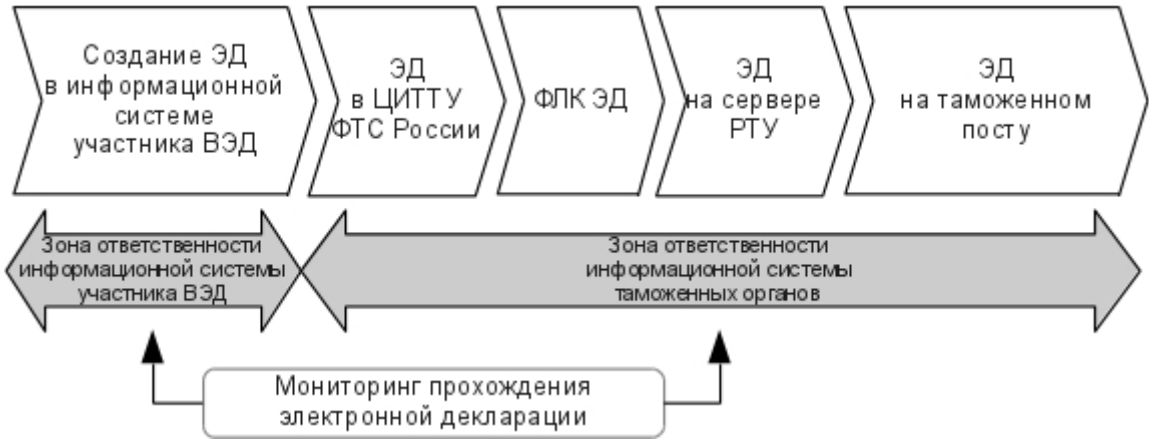

Рис. 32. Этапы прохождения электронной декларации по технологии ЭД-2.

Таким образом, реализация информационных технологий в ЕАИС ФТС Российской федерации основана на телекоммуникационном оборудовании Cisco Systems (США), программном обеспечении для Web-сервисов и доставки сообщений XML-RPC и SOAP от компании IBM (США), серверах баз данных компании Oracle (США) и системном программном обеспечении Microsoft (США). Для обеспечения криптографической защиты информации используются отечественные программно-аппаратные решения — АПКШ «Континент» (разработка ООО «Код Безопасности»), средства защиты информации «Аккорд» (ОКБ САПР) и «Соболь» (ООО «Код Безопасности»), электронные ключи VPN-key и RuToken (ЗАО «Актив-софт»), а также средства

шифрования «КриптоПро» (продукт ООО «Крипто-Про»), основанные на технологиях Microsoft CSP (Cryptographic Service Provider).

Антивирусная защита обеспечивается в основном антивирусными пакетами отечественных компаний «Лаборатория Касперского» и Dr.Web.

КАСТО и КПС, включая программное обеспечение для электронного декларирования разрабатываются и поддерживаются отечественными компаниями - ЗАО «Тамга», ОАО «НИЦ СПб ЭТУ», ЗАО «НПО «Персей», ООО «СофтЛэнд», ЗАО «Инмар», ООО «Альта-Софт», ООО «СТМ», ООО «ТКС.РУ» и другими.

Основы информационной безопасности в АИС

Основные понятия информационной безопасности

Информационная безопасность (ИБ) – защищённость информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера (**угроз**), которые могут нанести **неприемлемый ущерб** субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры.

Основными составляющими информационной безопасности, касающейся информационного обеспечения АИС, являются:

- **Доступность** – возможность в приемлемое время получить требуемую информационную услугу
- **Целостность** – актуальность и непротиворечивость информации, её защищённость от разрушения и несанкционированного изменения
- **Конфиденциальность** – защита от несанкционированного доступа к информации

С практической точки зрения абсолютной защищённости не существует. Важно соотношение ущерба от нарушения ИБ и стоимости мер по её обеспечению.

Защита информации – комплекс мероприятий, направленных на обеспечение ИБ.

Источник угрозы – это субъект, материальный объект или физическое явление, создающий угрозу безопасности защищаемой информации.

Источники угроз делятся на **субъективные** (зависят от действий персонала и устраняются организационными мерами и программно-аппаратными средствами) и **объективные** (зависят от особенностей построения и технических характеристик оборудования).

Внешними субъективными источниками угроз являются:

- внесение аппаратных закладок в технические средства
- удалённое внедрение вредоносного ПО
- перехват защищаемой информации в каналах передачи данных
- подбор аутентифицирующей информации пользователей («взлом паролей»)

Внутренними субъективными источниками угроз являются действия лиц, имеющих доступ к работе и (или) допуск в пределы контролируемой зоны.

Объективные источники угроз подразделяются на две категории.

А. Стихийные источники потенциальных угроз информационной безопасности, под которыми понимаются прежде всего природные явления (пожары, землетрясения, наводнения и т.п.).

Б. Источники, связанные с техническими средствами, а именно

- передача информации по беспроводным, проводным и волоконно-оптическим каналам
- дефекты, сбои и отказы технических средств
- отказы и сбои программных средств обработки информации.

Все возможные **виды угроз** также подразделяются на две категории:

- Атаки
- Угрозы, не являющиеся атаками.

Атака является целенаправленным действием нарушителя с использованием технических и (или) программных средств, с целью нарушения заданных характеристик безопасности защищаемых ресурсов или с целью создания условий для этого.

Атаки могут осуществляться через технические каналы утечки информации, а также за счёт несанкционированного доступа (НСД) к техническим и программным средствам АИС с применением соответствующих программных и программно-аппаратных средств.

Среди угроз, не являющихся атаками, можно выделить следующие:

- *угрозы, не связанные с деятельностью человека* (стихийные бедствия и природные явления)
- *угрозы социально-политического характера* (забастовки, саботаж, локальные конфликты и т.д.)
- *угрозы техногенного характера* (отключение электропитания, разрушение инженерных сооружений, неисправности, сбои аппаратных средств, нестабильность параметров системы электропитания и заземления, помехи и наводки, приводящие к сбоям в работе аппаратных средств и т.д.)
- ошибочные или случайные действия и (или) нарушения тех или

иных требований лицами, взаимодействующими с ресурсами информационной системы в рамках своих полномочий (*непреднамеренные действия пользователей*).

Модель угроз информационной безопасности: описание существующих угроз ИБ, их актуальности, возможности реализации и последствий.

Состав модели угроз:

- описание источников угроз ИБ
- описание методов реализации угроз ИБ
- описание объектов, пригодных для реализации угроз ИБ
- описание уязвимостей, используемых источниками угроз ИБ
- описание типов возможных потерь (например, нарушение доступности, целостности или конфиденциальности информационных активов)
- оценка масштабов потенциального ущерба

Назначение модели угроз: выявление существующих угроз, разработка эффективных контрмер, оптимизация затрат на защиту.

Некоторые важные нормативные документы в области ИБ

1. Доктрина информационной безопасности РФ (утверждена Президентом РФ 9 сентября 2000 г. N Пр-1895). Этот документ является основой для формирования государственной политики в области обеспечения информационной безопасности Российской Федерации, подготовки предложений по совершенствованию правового, методического, научно-технического и организационного обеспечения информационной безопасности Российской Федерации, а также разработки целевых программ обеспечения информационной безопасности Российской Федерации.

2. Конституция РФ в статье 23 гарантирует право на личную и семейную тайну, на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. В статье 29 п. 4 гарантируется право свободно искать, получать, передавать, производить и распространять информацию любым законным способом.

3. Федеральный закон «О государственной тайне» N 5485-1 от 21 июля 1993 г. определяет перечень сведений, на которые не распространяется право получения, передачи и распространения информации в соответствии с п. 4 ст. 29 Конституции РФ.

4. Федеральный закон «Об информации, информационных технологиях и защите информации» N 149-ФЗ от 27 июля 2006 г. регулирует отношения, возникающие при:осуществлении права на поиск, получение, передачу, производство и распространение информации, применении

информационных технологий и обеспечении защиты информации.

5. Федеральный закон «О персональных данных» N 152-ФЗ от 27 июля 2006 г. вводит понятие и классификацию персональных данных и регулирует отношения, связанные с обработкой персональных данных, осуществляемой федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, иными государственными органами (далее - государственные органы), органами местного самоуправления, иными муниципальными органами (далее - муниципальные органы), юридическими лицами и физическими лицами с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях, или без использования таких средств, если обработка персональных данных без использования таких средств соответствует характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации, то есть позволяет осуществлять в соответствии с заданным алгоритмом поиск персональных данных, зафиксированных на материальном носителе и содержащихся в картотеках или иных систематизированных собраниях персональных данных, и (или) доступ к таким персональным данным. Данный закон обеспечивает реализацию конституционного права на защиту информации о частной жизни (ст. 24 п. 1 Конституции РФ).

6. Намеренные действия, приводящие к нарушению информационной безопасности, могут подпадать под действия статей **Уголовного кодекса РФ (глава 28 «Преступления в сфере компьютерной информации»**. Так, статья 272 «Неправомерный доступ к компьютерной информации» определяет возможные наказания за повлекло уничтожение, блокирование, модификацию либо неправомерное копирование компьютерной информации, статья 273 «Создание, использование и распространение вредоносных программ для ЭВМ» определяет наказания за создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации, а статья 274 «Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети» - наказания за нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб.

7. Постановление Правительства РФ от 26 июня 1995 г. N 608 «О сертификации средств защиты информации» определяет, что технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну, средства, в которых

они реализованы, а также средства контроля эффективности защиты информации являются средствами защиты информации. Указанные средства подлежат обязательной сертификации, которая проводится в рамках систем сертификации средств защиты информации. При этом криптографические (шифровальные) средства должны быть отечественного производства и выполнены на основе криптографических алгоритмов, рекомендованных Федеральной службой безопасности Российской Федерации.

8. В соответствии с **Приказом Федеральной службы по техническому и экспортному контролю (ФСТЭК России) от 11 февраля 2013 г. N 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»** работы по защите информации в ходе создания и эксплуатации информационной системы обладателем информации (заказчиком) и оператором в соответствии с законодательством Российской Федерации при необходимости привлекаются организации, имеющие лицензию на деятельность по технической защите конфиденциальной информации в соответствии с Федеральным законом от 4 мая 2011 г. N 99-ФЗ «О лицензировании отдельных видов деятельности», а средства защиты информации должны пройти оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации в соответствии со статьёй 5 Федерального закона от 27 декабря 2002 г. N 184-ФЗ «О техническом регулировании»

9. Подпрограмма 5 «Безопасность в информационном обществе» Государственной программы «Информационное общество (2011-2020 годы)» (в первоначальной редакции 2010 года) предусматривает следующие мероприятия:

Мероприятие 2: создание и поддержка отечественных защищённых технологий хранения и обработки больших массивов неструктурированной информации, в том числе создание отечественных защищённых функциональных сервисов и технологических компонентов, обеспечивающих хранение и обработку больших массивов неструктурированной информации, их дальнейшая поддержка и развитие, позволяющие увеличить объем обрабатываемой неструктурированной информации

Мероприятие 4: создание национальной программной платформы (комплекс отечественных программных решений - модулей, построенных на базе единых технологий, позволяющих осуществлять разработку новых программных продуктов методом компоновки и настройки уже готовых модулей, а также разработку новых модулей), в том числе развитие отечественной сборки операционной системы на свободном программном обеспечении и создание отечественной системы управления базами данных на основе открытых разработок.

10. Упоминавшийся ранее **Приказ Министерства связи и массовых коммуникаций Российской Федерации (Минкомсвязь России) от 2**

сентября 2011 г. N 221 «Об утверждении Требований к информационным системам электронного документооборота федеральных органов исполнительной власти, учитывающих в том числе необходимость обработки посредством данных систем служебной информации ограниченного распространения» устанавливает требование по обеспечению класса защищённости от несанкционированного доступа к информации в АИС федеральных органов исполнительной власти не ниже 1Г.

11. Оценка соответствия требованиям по безопасности информации для АИС проводится на основании **Руководящих документов Гостехкомиссии РФ:**

- «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации»
- «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищённости от несанкционированного доступа к информации»
- «Защита от несанкционированного доступа к информации Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей».

Оценки уровня защищённости автоматизированных информационных систем.

Поскольку абсолютная защита в принципе недостижима (или не имеет практической ценности), принято говорить об **уровне доверия** к средствам защиты информации или, соответственно, о **доверенных информационных системах** (или программно-аппаратных комплексах). При этом нужно понимать, какие метрики используются для оценки уровня доверия, и по какой системе эти метрики оцениваются.

При обсуждении варианты защиты в нормативных документах и в специальной литературе применяются следующие понятия.

Дискреционная защита - защита (управление доступом) на основе **идентификации**. Пользователь/группа с правами доступа к одному объекту класса имеет те же права доступа ко всем объектам этого класса.

Мандатная защита предусматривает разграничение доступа субъектов к объектам, основанное на назначении *метки конфиденциальности* для информации, содержащейся в объектах, и выдаче официальных разрешений (допуска) субъектам на обращение к информации такого уровня конфиденциальности.

Например, субъект «Пользователь2», имеющий допуск уровня «не секретно», не может получить доступ к объекту, имеющего метку «для

служебного пользования». В то же время, субъект «Пользователь1» с допуском уровня «секретно», право доступа к объекту с меткой «для служебного пользования» имеет.

Верифицированная защита характеризуется применением формальных методов верификации корректности работы механизмов управления доступом (дискреционного и мандатного). Требуется, чтобы было формально показано соответствие архитектуры и реализации комплекса средств защиты (КСЗ) требованиям безопасности.

Уровни доверия TCSEC

Необходимость как-то измерять уровень «доверия» к АИС и их защищённость привела к разработке стандарта **TCSEC**(Trusted Computer System Evaluation Criteria), впервые опубликованного в 1985 году и разработанного Министерством обороны и Национальным центром компьютерной безопасности (National Computer Security Center – NCSC) США. Стандарт TCSEC известен под названием «Оранжевая книга» (Orange Book). В этой «Оранжевой книге» перечислены **семь подуровней четырех основных уровней** защиты, начиная от самой высокой степени непроницаемости до самой низкой.

- Уровень A – верифицируемая безопасность
- Уровень B – принудительное (мандатное) управление доступом
- Уровень C – произвольное (дискреционное) управление доступом
- Уровень D – неудовлетворительная защита

Ниже приведены краткие характеристики подуровней оценки в соответствии с TCSEC. Эти уровни касаются в первую очередь операционных систем.

Уровень	Описание
A1	Наивысший уровень. Теоретически возможная, но практически недостижимая защита.
B3	Опытный программист, имеющий доступ к системе, не может изменить свои права или нарушить работу системы.
B2	К системе невозможен несанкционированный доступ, вирусы не работают.
B1	Обычный пользователь не может преодолеть защиту, вирусы в принципе возможны.
C2	Обеспечивается защита процедур входа, производится контроль за событиями, имеющими отношение к безопасности, разграничиваются права доступа к ресурсам. Вирусы бывают.
C1	Есть возможность защиты личных данных при дополнительной установке средств защиты.
D	Тестирование проводилось, но требования более высокого класса не выполнялись.

Максимально достигнутый уровень доверия по TCSEC для систем, продающихся на открытом рынке — B2. Минимальный уровень доверия, допустимый для систем коммерческих предприятий и государственных организаций — C2.

Оценка защищённости АИС в Российской Федерации.

Контроль соответствия требованиям по защите информации в Российской Федерации может проводиться по требованиям ФСТЭК, по требованиям ФСБ и Министерства обороны. Для федеральных органов исполнительной власти, к которым относятся и Федеральные службы, актуальным является оценка по требованиям ФСТЭК и ФСБ.

Непосредственная деятельность по сертификация ФСБ РФ регламентирована ФЗ «О государственной тайне», постановлением Правительства Российской Федерации от 26.06.95 г. No 608 «О сертификации средств защиты информации» и приказом ФСБ РФ от 13 ноября 1999 г. No 564 «Об утверждении положений о системе сертификации средств защиты информации по требованиям безопасности для сведений, составляющих государственную тайну, и о ее знаках соответствия».

Согласно ст. 28 ФЗ «О государственной тайне», средства защиты информации должны иметь сертификат, удостоверяющий их соответствие требованиям по защите сведений соответствующей степени секретности.

В соответствии с п. 1.4 Приказа ФСБ РФ No 564, органы по сертификации системы сертификации проводят обязательную сертификацию средств защиты информации, используемых при работе со сведениями, составляющими государственную тайну, в том числе иностранного производства.

Результатом сертификации ФСБ является разрешение для операционной системы или программно-аппаратного комплекса на использование при обработке информации, содержащей сведения, составляющие государственную тайну.

Для оценки **защищённости от несанкционированного доступа к информации для многопользовательских автоматизированных информационных систем** все классы защиты подразделяются на гри группы.

- **Первая группа**: многопользовательские АИС, разные уровни конфиденциальности информации, ограничения доступа (классы **1А, 1Б, 1В, 1Г, 1Д**)
- **Вторая группа**: многопользовательские АИС, пользователи имеют одинаковые права доступа (классы **2А, 2Б**)
- **Третья группа**: однопользовательские АИС (классы **3А, 3Б**)

Для каждой группы и класса определяется набор требований к различным подсистемам АИС. Соответствие предъявляемым требованиям и определяет итоговый класс защиты (если какое-то требование не выполняется, класс

понижается).

Максимальный класс защиты в такой системе оценки — 1А, минимальный — 3Б.

1. Требования к подсистеме управления доступом

Требования	Классы								
	3Б	3А	2Б	2А	1Д	1Г	1В	1Б	1А
Идентификация, проверка подлинности и контроль доступа субъектов в систему	+	+	+	+	+	+	+	+	+
Идентификация, проверка подлинности и контроль доступа субъектов к терминалам, ЭВМ, узлам сети, внешним устройствам	-	-	-	+	-	+	+	+	+
Идентификация, проверка подлинности и контроль доступа субъектов к программам	-	-	-	+	-	+	+	+	+
Идентификация, проверка подлинности и контроль доступа субъектов к томам, каталогам, файлам, записям, полям записей	-	-	-	+	-	+	+	+	+
Управление потоками информации	-	-	-	+	-	-	+	+	+

2. Требования к подсистеме регистрации и учёта

Требования	Классы								
	3Б	3А	2Б	2А	1Д	1Г	1В	1Б	1А
Регистрация и учёт входа/выхода субъектов доступа в/из системы (узла сети)	+	+	+	+	+	+	+	+	+
Регистрация и учёт выдачи печатных (графических) выходных документов	-	+	-	+	-	+	+	+	+
Регистрация и учёт запуска/завершения программ и процессов (заданий, задач)	-	-	-	+	-	+	+	+	+
Регистрация и учёт доступа программ субъектов доступа к терминалам, ЭВМ, узлам сети, каналам связи, внешним устройствам, программам, томам, каталогам, файлам, записям, полям записей	-	-	-	+	-	+	+	+	+
Регистрация и учёт изменения полномочий субъектов доступа	-	-	-	-	-	-	+	+	+
Регистрация и учёт создаваемых защищаемых объектов доступа	-	-	-	+	-	-	+	+	+
Учёт носителей информации	+	+	+	+	+	+	+	+	+
Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей	-	+	-	+	-	+	+	+	+
Сигнализация попыток нарушения защиты	-	-	-	-	-	-	+	+	+

3. Требования к криптографической подсистеме

Требования	Классы								
	3Б	**3А**	**2Б**	**2А**	**1Д**	**1Г**	**1В**	**1Б**	**1А**
Шифрование конфиденциальной информации	-	-	-	+	-	-	-	+	+
Шифрование информации, принадлежащей различным субъектам доступа (группам субъектов) на разных ключах	-	-	-	-	-	-	-	-	+
Использование аттестованных (сертифицированных) криптографических средств	-	-	-	+	-	-	-	+	+

Классификация по уровню контроля недекларированных возможностей распространяется на ПО, предназначенное для защиты информации ограниченного доступа.

1. Устанавливается **четыре уровня** контроля отсутствия недекларированных возможностей. Каждый уровень характеризуется определённой минимальной совокупностью требований.
2. Самый высокий уровень контроля – **первый**, достаточен для ПО, используемого при защите информации с грифом «ОВ» (*«особо важно»*).
3. **Второй** уровень контроля достаточен для ПО, используемого при защите информации с грифом «СС» (*«совершенно секретно»*).
4. **Третий** уровень контроля достаточен для ПО, используемого при защите информации с грифом «С» (*«секретно»*).
5. Самый низкий уровень контроля – **четвертый**, достаточен для ПО, используемого при защите **конфиденциальной** информации.
6. Для ПО, используемого при защите информации, отнесённой к **государственной тайне**, должен быть обеспечен уровень контроля не ниже третьего.

Недекларированные возможности (НДВ) – функциональные возможности ПО, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Реализацией недекларированных возможностей, в частности, являются программные закладки.

Программные закладки – преднамеренно внесённые в ПО функциональные объекты (*модули, подпрограммы, процедуры, функции*), которые при определённых условиях (входных данных) инициируют выполнение не описанных в документации функций ПО, приводящих к нарушению конфиденциальности, доступности или целостности обрабатываемой информации.

Для выявления НДВ применяется анализ ПО, который делится на **статический** (тексты программ) и **динамический** (процесс выполнения

алгоритмов).

Для каждого уровня контроля определяется набор требований к различным аспектам контроля. Соответствие предъявляемым требованиям и определяет итоговый уровень контроля (если какое-то требование не выполняется, уровень контроля понижается).

1. Требования к документации (состав и содержание документации)

Требования	Уровень контроля			
	4	3	2	1
Спецификация (ГОСТ 19.202-78)	+	=	=	=
Описание программы (ГОСТ 19.402-78)	+	=	=	=
Описание применения (ГОСТ 19.502-78)	+	=	=	=
Пояснительная записка (ГОСТ 19.404-79)	-	+	=	=
Тексты программ, входящих в состав ПО (ГОСТ 19.401- 78)	+	=	=	=

Обозначения:

«-» – отсутствие требований;

«+» – новые или дополнительные требования,

«=» – требования совпадают с требованиями для предыдущего уровня контроля.

2. Требования к содержанию испытаний

А. Контроль исходного состояния программного обеспечения (ПО) производится для всех уровней контроля.

Б. Статический анализ исходных текстов программ

Требования	Уровень контроля			
	4	3	2	1
Контроль полноты и отсутствия избыточности исходных текстов	+	+	+	=
Контроль соответствия исходных текстов ПО его объектному (загрузочному) коду	+	=	=	+
Контроль связей функциональных объектов по управлению	-	+	=	=
Контроль связей функциональных объектов по информации	-	+	=	=
Контроль информационных объектов	-	+	=	=
Контроль наличия заданных конструкций в исходных текстах	-	-	+	+
Формирование перечня маршрутов выполнения функциональных объектов	-	+	+	=
Анализ критических маршрутов выполнения функциональных объектов	-	-	+	=
Анализ алгоритма работы функциональных объектов на основе	-	-	+	=

блок-схем, диаграмм и т.п., построенных по исходным текстам контролируемого ПО				

В. Динамический анализ исходных текстов программ

Требования	Уровень контроля			
	4	3	2	1
Контроль выполнения функциональных объектов	-	+	+	=
Сопоставление фактических маршрутов выполнения функциональных объектов и маршрутов, построенных в процессе проведения статического анализа	-	+	+	=

3. Составление и ведение отчётности требуется для всех уровней контроля.

Показатели **защищённости средств вычислительной техники (СВТ) от несанкционированного доступа к информации** содержат требования защищённости СВТ от НСД к информации

Показатели защищённости СВТ применяются к общесистемным программным средствам и операционным системам (с учётом архитектуры ЭВМ).

1. Конкретные перечни показателей определяют классы защищённости СВТ
2. Уменьшение или изменение перечня показателей, соответствующего конкретному классу защищённости СВТ, не допускается
3. Каждый показатель описывается совокупностью требований
4. Дополнительные требования к показателю защищённости СВТ и соответствие этим дополнительным требованиям оговаривается особо
5. Требования к показателям реализуются с помощью программно-технических средств.
   - Совокупность всех средств защиты составляет комплекс средств защиты
   - Документация КСЗ должна быть неотъемлемой частью конструкторской документации на СВТ
6. Устанавливается семь классов защищенности СВТ от НСД к информации.
   - Самый низкий класс – седьмой, самый высокий – первый
   - Классы подразделяются на четыре группы, отличающиеся качественным уровнем защиты:
     - **первая группа** содержит только один **седьмой класс**;
     - **вторая группа** характеризуется *дискреционной защитой* и содержит **шестой и пятый классы**;

• **третья группа** характеризуется *мандатной защитой* и содержит **четвертый, третий и второй классы**;

• **четвертая группа** характеризуется *верифицированной защитой* и содержит только **первый класс**.

7. Выбор класса защищенности СВТ для автоматизированных систем, создаваемых на базе защищенных СВТ, зависит от грифа секретности обрабатываемой в АС информации, условий эксплуатации и расположения объектов системы.

8. Применение в комплекте СВТ средств криптографической защиты информации по ГОСТ 28147-89 может быть использовано для повышения гарантий качества защиты.

Перечень классов защищённости СВТ от НСТ и соответствующих показателей приведён в таблице.

Наименование показателя	**Класс защищённости**					
	6	**5**	**4**	**3**	**2**	**1**
Дискреционный принцип контроля доступа	+	+	+	=	+	=
Мандатный принцип контроля доступа	-	-	+	=	=	=
Очистка памяти	-	+	+	+	=	=
Изоляция модулей	-	-	+	=	+	=
Маркировка документов	-	-	+	=	=	=
Защита ввода и вывода на отчуждаемый физический носитель информации	-	-	+	=	=	=
Сопоставление пользователя с устройством	-	-	+	=	=	=
Идентификация и аутентификация	+	=	+	=	=	=
Гарантии проектирования	-	+	+	+	+	+
Регистрация	-	+	+	+	=	=
Взаимодействие пользователя с КСЗ	-	-	-	+	=	=
Надежное восстановление	-	-	-	+	=	=
Целостность КСЗ	-	+	+	+	=	=
Контроль модификации	-	-	-	-	+	=
Контроль дистрибуции	-	-	-	-	+	=
Гарантии архитектуры	-	-	-	-	-	+
Тестирование	+	+	+	+	+	=
Руководство для пользователя	+	=	=	=	=	=
Руководство по КСЗ	+	+	=	+	+	=
Тестовая документация	+	+	+	+	+	=
Конструкторская (проектная) документация	+	+	+	+	+	+

Обозначения:

«-» – нет требований к данному классу;

«+» – новые или дополнительные требования,

«=» – требования совпадают с требованиями к СВТ предыдущего класса.

Седьмой класс защищённости СВТ от НСД присваивают СВТ, к которым предъявлялись требования по защите от НСД к информации, но при оценке защищённость СВТ оказалась ниже уровня требований шестого класса.

Шестой класс защищённости СВТ от НСД характеризуется следующими требованиям к показателям защищённости:

- **Дискреционный принцип контроля доступа**:
  - КСЗ должен контролировать доступ наименованных субъектов (пользователей) к наименованным объектам (файлам, программам, томам и т.д.).
  - Для каждой пары (субъект – объект) в СВТ должно быть задано явное и недвусмысленное перечисление допустимых типов доступа (читать, писать и т.д.), т.е. тех типов доступа, которые являются санкционированными для данного субъекта (индивида или группы индивидов) к данному ресурсу СВТ (объекту).
  - КСЗ должен содержать механизм, претворяющий в жизнь дискреционные правила разграничения доступа.
  - Контроль доступа должен быть применим к каждому объекту и каждому субъекту (индивиду или группе равноправных индивидов).
  - Механизм, реализующий дискреционный принцип контроля доступа, должен предусматривать возможности санкционированного изменения ПРД, в том числе возможность санкционированного изменения списка пользователей СВТ и списка защищаемых объектов.
  - Права изменять ПРД должны предоставляться выделенным субъектам (администрации, службе безопасности и т.д.).
- **Идентификация и аутентификация**:
  - КСЗ должен требовать от пользователей идентифицировать себя при запросах на доступ. КСЗ должен подвергать проверке подлинность идентификации – осуществлять аутентификацию. КСЗ должен располагать необходимыми данными для идентификации и аутентификации. КСЗ должен препятствовать доступу к защищаемым ресурсам неидентифицированных пользователей и пользователей, подлинность идентификации которых при аутентификации не подтвердилась.
- **Тестирование**. В СВТ шестого класса должны тестироваться:
  - реализация дискреционных ПРД (перехват явных и скрытых запросов, правильное распознавание санкционированных и несанкционированных запросов на доступ, средства защиты механизма разграничения доступа, санкционированные изменения

ПРД)

- успешное осуществление идентификации и аутентификации, а также их средств защиты.

- **Руководство для пользователя**. Документация на СВТ должна включать в себя краткое руководство для пользователя с описанием способов использования КСЗ и его интерфейса с пользователем.
- **Руководство по КСЗ**. Данный документ адресован администратору защиты и должен содержать:
  - описание контролируемых функций
  - руководство по генерации КСЗ
  - описание старта СВТ и процедур проверки правильности старта.
- **Тестовая документация**. Должно быть предоставлено описание тестов и испытаний, которым подвергалось СВТ и результатов тестирования.
- **Конструкторская (проектная) документация**. Должна содержать общее описание принципов работы СВТ, общую схему КСЗ, описание интерфейсов КСЗ с пользователем и интерфейсов частей КСЗ между собой, описание механизмов идентификации и аутентификации.

Пятый класс защищённости СВТ от НСД характеризуется следующими требованиям к показателям защищённости:

- **Дискреционный принцип контроля доступа**. Данные требования включает в себя аналогичные требование шестого класса. Дополнительно должны быть предусмотрены средства управления, ограничивающие распространение прав на доступ.
- **Очистка памяти**. При первоначальном назначении или при перераспределении внешней памяти КСЗ должен предотвращать доступ субъекту к остаточной информации.
- **Идентификация и аутентификация**. Данные требования полностью совпадают с аналогичными требованиями шестого класса
- **Гарантии проектирования**. На начальном этапе проектирования СВТ должна быть построена модель защиты. Модель должна включать в себя ПРД к объектам и непротиворечивые правила изменения ПРД.
- **Регистрация**. КСЗ должен быть в состоянии осуществлять регистрацию следующих событий:
  - использование идентификационного и аутентификационного механизма
  - запрос на доступ к защищаемому ресурсу (открытие файла, запуск программы и т.д.)
  - создание и уничтожение объекта
  - действия по изменению ПРД.

  Для каждого из этих событий должна регистрироваться следующая информация:

- субъект, осуществляющий регистрируемое действие
- тип события (если регистрируется запрос на доступ, то следует отмечать объект и тип доступа)
- успешно ли осуществилось событие (обслужен запрос на доступ или нет)

КСЗ должен содержать средства выборочного ознакомления с регистрационной информацией

- **Целостность КСЗ**. В СВТ пятого класса защищённости должны быть предусмотрены средства периодического контроля за целостностью программной и информационной части КСЗ.
- **Тестирование**. В СВТ пятого класса защищённости должны тестироваться:
  - реализация ПРД (перехват явных и скрытых запросов на доступ, правильное распознавание санкционированных и несанкционированных запросов, средства защиты механизма разграничения доступа, санкционированные изменения ПРД)
  - успешное осуществление идентификации и аутентификации, а также их средства защиты
  - очистка памяти
  - регистрация событий, средства защиты регистрационной информации и возможность санкционированного ознакомления с ней
  - работа механизма, осуществляющего контроль за целостностью КСЗ.
- **Руководство для пользователя**. Данное требование совпадает с аналогичным требованием шестого класса.
- **Руководство по КСЗ**. Данный документ адресован администратору защиты и должен содержать:
  - описание контролируемых функций
  - руководство по генерации КСЗ
  - описание старта СВТ, процедур проверки правильности старта, процедур работы со средствами регистрации.
- **Тестовая документация**. Должно быть предоставлено описание тестов и испытаний, которым подвергалось СВТ и результатов тестирования.
- **Конструкторская (проектная) документация**. Должна содержать:
  - описание принципов работы СВТ
  - общую схему КСЗ
  - описание интерфейсов КСЗ с пользователем и интерфейсов модулей КСЗ
  - модель защиты
  - описание механизмов контроля целостности КСЗ, очистки памяти, идентификации и аутентификации.

Четвёртый класс защищённости СВТ от НСД характеризуется следующими требованиям к показателям защищённости:

- **Дискреционный принцип контроля доступа**. Данные требования включают аналогичные требования пятого класса. Дополнительно КСЗ должен содержать механизм, претворяющий в жизнь дискреционные ПРД, как для явных действий пользователя, так и для скрытых, обеспечивая тем самым защиту объектов от НСД (т.е. от доступа, не допустимого с точки зрения заданного ПРД). Под «явными» здесь подразумеваются действия, осуществляемые с использованием системных средств – системных макрокоманд, инструкций языков высокого уровня и т.д., а под «скрытыми» – иные действия, в том числе с использованием собственных программ работы с устройствами. Дискреционные ПРД для систем данного класса являются дополнением мандатных ПРД.
- **Мандатный принцип контроля доступа**:
    - Для реализации этого принципа должны сопоставляться классификационные метки каждого субъекта и каждого объекта, отражающие их место в соответствующей иерархии. Посредством этих меток субъектам и объектам должны назначаться классификационные уровни (уровни уязвимости, категории секретности и т.п.), являющиеся комбинациями иерархических и неиерархических категорий. Данные метки должны служить основой мандатного принципа разграничения доступа.
    - КСЗ при вводе новых данных в систему должен запрашивать и получать от санкционированного пользователя классификационные метки этих данных. При санкционированном занесении в список пользователей нового субъекта должно осуществляться сопоставление ему классификационных меток. Внешние классификационные метки (субъектов, объектов) должны точно соответствовать внутренним меткам (внутри КСЗ).
    - КСЗ должен реализовывать мандатный принцип контроля доступа применительно ко всем объектам при явном и скрытом доступе со стороны любого из субъектов:
        - субъект может читать объект, только если иерархическая классификация в классификационном уровне субъекта не меньше, чем иерархическая классификация в классификационном уровне объекта, и неиерархические категории в классификационном уровне субъекта включают в себя все иерархические категории в классификационном уровне объекта
        - субъект осуществляет запись в объект, только если классификационный уровень субъекта в иерархической классификации не больше, чем классификационный уровень объекта в иерархической классификации, и все иерархические

категории в классификационном уровне субъекта включаются в неиерархические категории в классификационном уровне объекта.

• Реализация мандатных ПРД должна предусматривать возможности сопровождения: изменения классификационных уровней субъектов и объектов специально выделенными субъектами.

• В СВТ должен быть реализован диспетчер доступа, т.е. средство, осуществляющее перехват всех обращений субъектов к объектам, а также разграничение доступа в соответствии с заданным принципом разграничения доступа. При этом решение о санкционированности запроса на доступ должно приниматься только при одновременном разрешении его и дискреционными, и мандатными ПРД. Таким образом, должен контролироваться не только единичный акт доступа, но и потоки информации.

- **Очистка памяти**. При первоначальном назначении или при перераспределении внешней памяти КСЗ должен предотвращать доступ субъекту к остаточной информации. При перераспределении оперативной памяти КСЗ должен осуществлять ее очистку.
- **Изоляция модулей**. При наличии в СВТ мультипрограммирования в КСЗ должен существовать программно-технический механизм, изолирующий программные модули одного процесса (одного субъекта), от программных модулей других процессов (других субъектов) – т.е. в оперативной памяти ЭВМ программы разных пользователей должны быть защищены друг от друга.
- **Маркировка документов**. При выводе защищаемой информации на документ в начале и конце проставляют штамп N 1 и заполняют его реквизиты в соответствии с Инструкцией N 0126-87 (п. 577).
- **Защита ввода и вывода на отчуждаемый физический носитель информации**:

  • КСЗ должен различать каждое устройство ввода-вывода и каждый канал связи как произвольно используемые или идентифицированные («помеченные»). При вводе с «помеченного» устройства (вывода на «помеченное» устройство) КСЗ должен обеспечивать соответствие между меткой вводимого (выводимого) объекта (классификационным уровнем) и меткой устройства. Такое же соответствие должно обеспечиваться при работе с «помеченным» каналом связи.

  • Изменения в назначении и разметке устройств и каналов должны осуществляться только под контролем КСЗ.
- **Сопоставление пользователя с устройством**:

  • КСЗ должен обеспечивать вывод информации на запрошенное пользователем устройство как для произвольно используемых устройств, так и для идентифицированных (при совпадении

маркировки).

- КСЗ должен включать в себя механизм, посредством которого санкционированный пользователь надёжно сопоставляется выделенному устройству.

- **Идентификация и аутентификация**:
  - КСЗ должен требовать от пользователей идентифицировать себя при запросах на доступ, должен проверять подлинность идентификатора субъекта – осуществлять аутентификацию. КСЗ должен располагать необходимыми данными для идентификации и аутентификации и препятствовать входу в СВТ неидентифицированного пользователя или пользователя, чья подлинность при аутентификации не подтвердилась.
  - КСЗ должен обладать способностью надёжно связывать полученную идентификацию со всеми действиями данного пользователя.
- **Гарантии проектирования**. Проектирование КСЗ должно начинаться с построения модели защиты, содержащей:
  - непротиворечивые ПРД
  - непротиворечивые правила изменения ПРД
  - правила работы с устройствами ввода и вывода информации и каналами связи.
- **Регистрация**. Данные требования включают аналогичные требования пятого класса защищённости. Дополнительно должна быть предусмотрена регистрация всех попыток доступа, всех действий оператора и выделенных пользователей (администраторов защиты и т.п.).
- **Целостность КСЗ**:
  - В СВТ четвёртого класса защищённости должен осуществляться периодический контроль за целостностью КСЗ.
  - Программы КСЗ должны выполняться в отдельной части оперативной памяти.
- **Тестирование**. В четвёртом классе защищённости должны тестироваться:
  - реализация ПРД (перехват запросов на доступ, правильное распознавание санкционированных и несанкционированных запросов в соответствии с дискреционными и мандатными правилами, верное сопоставление меток субъектов и объектов, запрос меток вновь вводимой информации, средства защиты механизма разграничения доступа, санкционированное изменение ПРД)
  - невозможность присвоения субъектом себе новых прав
  - очистка оперативной и внешней памяти
  - работа механизма изоляции процессов в оперативной памяти
  - маркировка документов
  - защита ввода и вывода информации на отчуждаемый

физический носитель и сопоставление пользователя с устройством
    - идентификация и аутентификация, а также их средства защиты
    - запрет на доступ несанкционированного пользователя
    - работа механизма, осуществляющего контроль за целостностью СВТ
    - регистрация событий, средства защиты регистрационной информации и возможность санкционированного ознакомления с этой информацией.
- **Руководство для пользователя**. Данное требование совпадает с аналогичным требованием шестого и пятого классов.
- **Руководство по КСЗ**. Данные требования полностью совпадают с аналогичными требованиями пятого класса.
- **Тестовая документация**. Должно быть предоставлено описание тестов и испытаний, которым подвергалось СВТ и результатов тестирования.
- **Конструкторская (проектная) документация**. Должна содержать:
    - общее описание принципов работы СВТ
    - общую схему КСЗ
    - описание внешних интерфейсов КСЗ и интерфейсов модулей КСЗ
    - описание модели защиты
    - описание диспетчера доступа
    - описание механизма контроля целостности КСЗ
    - описание механизма очистки памяти
    - описание механизма изоляции программ в оперативной памяти
    - описание средств защиты ввода и вывода на отчуждаемый физический носитель информации и сопоставления пользователя с устройством
    - описание механизма идентификации и аутентификации
    - описание средств регистрации.

Третий класс защищённости СВТ от НСД характеризуется следующими требованиям к показателям защищённости:

- **Дискреционный принцип контроля доступа**. Данные требования полностью совпадают с требованиями пятого и четвёртого классов.
- **Мандатный принцип контроля доступа**. Данные требования полностью совпадают с аналогичным требованием четвёртого класса.
- **Очистка памяти**. Для СВТ третьего класса защищённости КСЗ должен осуществлять очистку оперативной и внешней памяти. Очистка должна производиться путём записи маскирующей информации в память при ее освобождении (перераспределении).
- **Изоляция модулей**. Данные требования полностью совпадают с

аналогичным требованием четвёртого класса.

- **Маркировка документов**. Данные требования полностью совпадают с аналогичным требованием четвёртого класса.
- **Защита ввода и вывода на отчуждаемый физический носитель информации**. Данные требования полностью совпадают с аналогичным требованием четвёртого класса.
- **Сопоставление пользователя с устройством**. Данные требования полностью совпадают с аналогичным требованием четвёртого класса.
- **Идентификация и аутентификация**. Данные требования полностью совпадают с аналогичным требованием четвёртого класса.
- **Гарантии проектирования**. На начальном этапе проектирования КСЗ должна строиться модель защиты, задающая принцип разграничения доступа и механизм управления доступом. Эта модель должна содержать:
    - непротиворечивые правила изменения ПРД
    - правила работы с устройствами ввода и вывода
    - формальную модель механизма управления доступом.

  Должна предлагаться высокоуровневая спецификация части КСЗ, реализующего механизм управления доступом и его интерфейсов. Эта спецификация должна быть верифицирована на соответствие заданных принципов разграничения доступа.
- **Регистрация**. Данные требования полностью совпадают с аналогичным требованием четвёртого класса.
- **Взаимодействие пользователя с КСЗ**. Для обеспечения возможности изучения, анализа, верификации и модификации КСЗ должен быть хорошо структурирован, его структура должна быть модульной и чётко определённой. Интерфейс пользователя и КСЗ должен быть определён (вход в систему, запросы пользователей и КСЗ и т.п.). Должна быть обеспечена надёжность такого интерфейса. Каждый интерфейс пользователя и КСЗ должен быть логически изолирован от других таких же интерфейсов.
- **Надёжное восстановление**. Процедуры восстановления после сбоев и отказов оборудования должны обеспечивать полное восстановление свойств КСЗ.
- **Целостность КСЗ**:
    - Необходимо осуществлять периодический контроль за целостностью КСЗ.
    - Программы должны выполняться в отдельной части оперативной памяти. Это требование должно подвергаться верификации.
- **Тестирование**. СВТ должны подвергаться такому же тестированию, что и СВТ четвёртого класса. Дополнительно должны тестироваться:
    - очистка памяти
    - работа механизма надёжного восстановления.

- **Руководство для пользователя**. Данные требования полностью совпадают с аналогичным требованием четвёртого класса.
- **Руководство по КСЗ**. Документ адресован администратору защиты и должен содержать:
    - описание контролируемых функций
    - руководство по генерации КСЗ
    - описание старта СВТ, процедур проверки правильности старта, процедур работы со средствами регистрации
    - руководство по средствам надёжного восстановления.
- **Тестовая документация**. Должно быть предоставлено описание тестов и испытаний, которым подвергалось СВТ и результатов тестирования.
- **Конструкторская (проектная) документация**. Требуется такая же документация, что и для СВТ четвёртого класса. Дополнительно необходимы:
    - высокоуровневая спецификация КСЗ и его интерфейсов
    - верификация соответствия высокоуровневой спецификации КСЗ модели защиты.

Второй класс защищённости СВТ от НСД характеризуется следующими требованиям к показателям защищённости:

- **Дискреционный принцип контроля доступа**. Данные требования включают аналогичные требования третьего класса. Дополнительно требуется, чтобы дискреционные правила разграничения доступа были эквивалентны мандатным правилам (т.е. всякий запрос на доступ должен быть одновременно санкционированным или несанкционированным одновременно и по дискреционным правилам, и по мандатным ПРД).
- **Мандатный принцип контроля доступа**. Данные требования полностью совпадают с аналогичным требованием третьего класса.
- **Очистка памяти**. Данные требования полностью совпадают с аналогичным требованием третьего класса.
- **Изоляция модулей**. При наличии в СВТ мультипрограммирования в КСЗ должен существовать программно-технический механизм, изолирующий программные модули одного процесса (одного субъекта), от программных модулей других процессов (других субъектов) – т.е. в оперативной памяти ЭВМ программы разных пользователей должны быть изолированы друг от друга. Гарантии изоляции должны быть основаны на архитектуре СВТ.
- **Маркировка документов**. Данные требования полностью совпадают с аналогичным требованием третьего класса.
- **Защита ввода и вывода на отчуждаемый физический носитель информации**. Данные требования полностью совпадают с аналогичным требованием третьего класса.
- **Сопоставление пользователя с устройством**. Данные требования полностью совпадают с аналогичным требованием четвёртого и третьего

классов.

- **Идентификация и аутентификация**. Требование полностью совпадает с аналогичным требованием четвёртого и третьего классов.
- **Гарантии проектирования**. Данные требования включают аналогичные требования третьего класса. Дополнительно требуется, чтобы высокоуровневые спецификации КСЗ были отображены последовательно в спецификации одного или нескольких нижних уровней, вплоть до реализации высокоуровневой спецификации КСЗ на языке программирования высокого уровня. При этом методами верификации должно осуществляться доказательство соответствия каждого такого отображения спецификациям высокого (верхнего для данного отображения) уровня. Этот процесс может включать в себя как одно отображение (высокоуровневая спецификация - язык программирования), так и последовательность отображений в промежуточные спецификации с понижением уровня, вплоть до языка программирования. В результате верификации соответствия каждого уровня предыдущему должно достигаться соответствие реализации высокоуровневой спецификации КСЗ и заданной модели защиты
- **Регистрация**. Данные требования полностью совпадают с аналогичным требованием четвёртого и третьего классов.
- **Взаимодействие пользователя с КСЗ**. Данные требования полностью совпадают с аналогичным требованием третьего класса.
- **Надёжное восстановление**. Данные требования полностью совпадают с аналогичным требованием третьего класса.
- **Целостность КСЗ**. Данные требования полностью совпадают с аналогичным требованием третьего класса.
- **Контроль модификации**. При проектировании, построении и сопровождении СВТ должно быть предусмотрено управление конфигурацией СВТ, т.е. контроль изменений в формальной модели, спецификациях (разных уровней), документации, исходном тексте, версии в объектном коде. Должно обеспечиваться соответствие между документацией и текстами программ. Должна осуществляться сравниваемость генерируемых версий. Оригиналы программ должны быть защищены.
- **Контроль дистрибуции**. Должен осуществляться контроль точности копирования в СВТ при изготовлении копий с образца. Изготовляемая копия должна гарантированно повторять образец.
- **Тестирование**. СВТ второго класса должны тестироваться так же, как и СВТ третьего класса. Дополнительно должен тестироваться контроль дистрибуции.
- **Руководство для пользователя**. Данные требования полностью совпадают с аналогичным требованием четвёртого и третьего классов.
- **Руководство по КСЗ**. Данные требования включают аналогичные требования третьего класса. Дополнительно должны быть представлены

руководства по надёжному восстановлению, по работе со средствами контроля модификации и дистрибуции.

- **Тестовая документация**. Должно быть предоставлено описание тестов и испытаний, которым подвергалось СВТ и результатов тестирования.
- **Конструкторская (проектная) документация**. Требуется такая же документация, что и для СВТ третьего класса. Дополнительно должны быть описаны гарантии процесса проектирования и эквивалентность дискреционных и мандатных ПРД.

Первый класс защищённости СВТ от НСД характеризуется следующими требованиям к показателям защищённости:

- **Дискреционный принцип контроля доступа**. Данные требования полностью совпадают с аналогичным требованием второго класса.
- **Мандатный принцип контроля доступа**. Данные требования полностью совпадают с аналогичным требованием второго класса.
- **Очистка памяти**. Данные требования полностью совпадают с аналогичным требованием второго класса.
- **Изоляция модулей**. Данные требования полностью совпадают с аналогичным требованием второго класса.
- **Маркировка документов**. Данные требования полностью совпадают с аналогичным требованием второго класса.
- **Защита ввода и вывода на отчуждаемый физический носитель информации**. Данные требования полностью совпадают с аналогичным требованием второго класса.
- **Сопоставление пользователя с устройством**. Данные требования полностью совпадают с аналогичным требованием второго класса.
- **Идентификация и аутентификация**. Данные требования полностью совпадают с аналогичным требованием второго класса.
- **Гарантии проектирования**. Данные требования включают аналогичные требования второго класса. Дополнительно требуется верификация соответствия объектного кода тексту КСЗ на языке высокого уровня.
- **Регистрация**. Данные требования полностью совпадают с аналогичным требованием второго класса.
- **Взаимодействие пользователя с КСЗ**. Данные требования полностью совпадают с аналогичным требованием второго класса.
- **Надежное восстановление**. Данные требования полностью совпадают с аналогичным требованием второго класса.
- **Целостность КСЗ**. Данные требования полностью совпадают с аналогичным требованием второго класса.
- **Контроль модификации**. Данные требования полностью совпадают с аналогичным требованием второго класса.
- **Контроль дистрибуции**. Данные требования полностью совпадают с аналогичным требованием второго класса.

- **Гарантии архитектуры**. КСЗ должен обладать механизмом, гарантирующим перехват диспетчером доступа всех обращений субъектов к объектам.
- **Тестирование**. Данные требования полностью совпадают с аналогичным требованием второго класса.
- **Руководство для пользователя**. Данные требования полностью совпадают с аналогичным требованием второго класса.
- **Руководство по КСЗ**. Данные требования полностью совпадают с аналогичным требованием второго класса.
- **Тестовая документация**. Данные требования полностью совпадают с аналогичным требованием второго класса.
- **Конструкторская (проектная) документация**. ТТребуется такая же документация, что и для СВТ второго класса. Дополнительно разрабатывается описание гарантий процесса проектирования.

Информационные системы, в которых хранятся и обрабатываются персональные данные граждан Российской Федерации (**информационные системы персональных данных — ИСПДн**), классифицируются по требованиям защищённости информации св соответствии с **Приказом Федеральной службы по техническому и экспортному контролю (ФСТЭК России) Федеральной службы безопасности Российской Федерации (ФСБ России) Министерства информационных технологий и связи Российской Федерации (Мининформсвязи России) от 13 февраля 2008 г. N 55/86/20 г. «Об утверждении Порядка проведения классификации информационных систем персональных данных»**.

Проведение классификации информационных систем включает в себя следующие этапы:

- сбор и анализ исходных данных по информационной системе
- присвоение информационной системе соответствующего класса и его документальное оформление.

При проведении классификации информационной системы учитываются следующие исходные данные:

- категория обрабатываемых в информационной системе персональных данных
- объем обрабатываемых персональных данных (количество субъектов персональных данных, персональные данные которых обрабатываются в информационной системе)
- заданные оператором характеристики безопасности персональных данных, обрабатываемых в информационной системе
- структура информационной системы
- наличие подключений информационной системы к сетям связи общего пользования и (или) сетям международного информационного обмена

- режим обработки персональных данных
- режим разграничения прав доступа пользователей информационной системы
- местонахождение технических средств информационной системы.

Все персональные данные (Пдн) подразделяются на следующие категории:

- **категория 1** – персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни;
- **категория 2** – персональные данные, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию, за исключением персональных данных, относящихся к категории 1;
- **категория 3** – персональные данные, позволяющие идентифицировать субъекта персональных данных;
- **категория 4** – обезличенные и (или) общедоступные персональные данные.

Вводится также характеристика **объёма обрабатываемых в ИС персональных данных**. Она является числом.

- **1** – в информационной системе одновременно обрабатываются персональные данные более чем 100 000 субъектов персональных данных или персональные данные субъектов персональных данных в пределах субъекта Российской Федерации или Российской Федерации в целом;
- **2** – в информационной системе одновременно обрабатываются персональные данные от 1000 до 100 000 субъектов персональных данных или персональные данные субъектов персональных данных, работающих в отрасли экономики Российской Федерации, в органе государственной власти, проживающих в пределах муниципального образования;
- **3** – в информационной системе одновременно обрабатываются данные менее чем 1000 субъектов персональных данных или персональные данные субъектов персональных данных в пределах конкретной организации.

В зависимости от категории и объёма обрабатываемых в системе ПДн выделяются следующие классы ИСПДн:

- **класс 1 (К1)** – информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к значительным негативным последствиям для субъектов персональных данных;
- **класс 2 (К2)** – информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к негативным последствиям для

субъектов персональных данных;

- **класс 3 (К3)** – информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к незначительным негативным последствиям для субъектов персональных данных;
- **класс 4 (К4)** – информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, не приводит к негативным последствиям для субъектов персональных данных.

Определение классов ИСПДн приведено в таблице на рис. 33.

Категория ПДн, обрабатываемых в электронном виде	**Количество субъектов ПДн в системе**								
	Более 100 тыс. ПДн	В объёме		От 1000 до 100000 ПДн	В объёме				До 1000 ПДн
		РФ	Субъект РФ		Отрасли	Органа власти	Муниципального образования	Организации	
1. Расовая, национальная принадлежность, политические взгляды, религиозные и философские убеждения, состояние здоровья, интимная жизнь	**1 класс (К1)**			**1 класс (К1)**				**1 класс (К1)**	
2. Позволяющие идентифицировать субъекта персональных данных и получить о нём дополнительную информацию, за исключением ПДн, относящихся к категории 1	**1 класс (К1)**			**2 класс (К2)**				**3 класс (К3)**	
3. Позволяющие идентифицировать субъекта персональных данных	**2 класс (К2)**			**3 класс (К3)**				**3 класс (К3)**	
4. Обезличенные и (или) общедоступные персональные данные	**4 класс (К4)**			**4 класс (К4)**				**4 класс (К4)**	

Рис. 33. Определение классов ИПДн.

Реестр сертифицированных СЗИ

Государственный реестр сертифицированных средств защиты информации (СЗИ) N РОСС RU.0001.01БИ00 является открытым источником сведений о существующих средствах защиты информации, прошедших сертификацию на соответствие тем или иным требованиям защищённости.

В Реестре перечислены операционные системы, прикладные программы, программно-аппаратные комплексы, комплексные программные решения и

аппаратные средства.

Выписка из реестра по данным на апрель 2014 года приведена в таблице ниже.

№ серти-фиката	Дата внесения в реестр	Срок действия серти-фиката	Наимено-вание средства (шифр)	Предназначение средства (область применения), краткая характеристика параметров / (оценка возможности использования в информационных системах персональных данных (ИСПДн))
1017/4	05.08.2008	05.08.2014	MS Windows 2003 Server SE(SP2)	Операционная система Microsoft Windows 2003 Server Standard Edition (SP2) соответствует заданию по безопасности MS.Win_Srv2003_SP2.ЗБ. Версия 1.0. 2008, имеет оценочный уровень доверия ОУД 1 (усиленный) по РД «Безопасность информационных технологий. Критерии оценки безопасности информационных технологий» и для создания систем до 1Г включительно
1382	10.05.2007	10.05.2016	Антивирус Касперского 6.0 для Windows Servers	ПО «Антивирус Касперского 6.0 для Windows Servers» – по 2 уровню контроля НДВ и на соответствие ТУ(может использоваться для защиты информации в ИСПДн до 1 класса включительно)
1928	27.10.2009	27.10.2015	MS Windows Server 2008 Standard Edition	MS Windows Server 2008 Standard Edition - по 5 классу защищенности для СВТ (может использоваться в 1Г и может использоваться для защиты информации в ИСПДн до 3 класса включительно)
2180	30.09.2010	30.09.2016	Microsoft Windows 7	Операционная система Microsoft Windows 7 в редакциях «Профессиональная», «Корпоративная» и «Максимальная» – по 5 классу СВТ (может использоваться в 1Г и может использоваться для защиты информации в ИСПДн до 2 класса включительно)
2398	10.08.2011	10.08.2014	«Аккорд-Win32»	ПАК средств защиты информации от несанкционированного доступа «Аккорд-Win32», под управлением ОС Windows , соответствует 2 уровню по

				РД НДВ, 3-РД СВТ (может использоваться при создании автоматизированных систем до класса защищенности 1Б включительно, а также для перданных до 1 класса включительно)
2960	30.09.2013	30.09.2016	Microsoft Windows 8	Операционные системы «Microsoft Windows 8», «Microsoft Windows 8 Профессиональная», «Microsoft Windows 8 Корпоративная», для платформ 32 bit и 64 bit (для PC на платформе Intel) – по 5 классу РД СВТ с ограничениями
2485	18.11.2011	18.11.2014	Kaspersky Endpoint Security 8 для Linux	Программное изделие Kaspersky Endpoint Security 8 для Linux 643.46856491.00054 - на соответствие ТУ и 2 уровню РД НДВ (может использоваться в ИСПДН до 1 класса)
2557	27.01.2012	27.01.2015	Astra Linux Special Edition	Операционная система специального назначения «Astra Linux Special Edition» - на соответствие РД СВТ по 3 классу и РД НДВ по 2 уровню
2573	16.02.2012	16.02.2015	VPN/FW «ЗАСТАВА» версия 5.3	Программный комплекс «VPN/FW «ЗАСТАВА», версия 5.3, функционирующий в среде операционной системы ALT Linux - по 2 классу РД МЭ и по 3 уровню РД НДВ
2778	11.12.2012	11.12.2015	Циркон 26К	Операционная система «Циркон 26К» (на базе Debian GNU/Linux) - по 5 классу для СВТ, по 4 уровню контроля и на ТУНДВ
2840	13.03.2013	13.03.2016	Kaspersky Linux Mail Security 8.	Программное изделие «Kaspersky Linux Mail Security 8.0» - на соответствие ТУ и 2 уровню РД НДВ
2317	18.04.2011	18.04.2017	Альт Линукс СПТ 6.0	Операционная система "Альт Линукс СПТ 6.0"- по 4 классу РД СВТ и по 3 уровню отсутствия НДВ

Средства обеспечения информационной безопасности

Все средства обеспечения ИБ подразделяются на три группы:

1. Организационные средства

2. Технические средства

3. Программные средства

К **организационным средствам** относятся

- Разграничение информации по необходимым уровням доступа (защиты)
- Определение допустимой «стоимости» защиты
- Организация процедур работы с «закрытой» информацией, создание должностных инструкций
- Определение требований к системе защиты информации
- Определение и подготовка лиц, ответственных за обеспечение безопасности информации, а также назначение исполнителей, которым поручаются разработка и эксплуатация систем защиты информации
- Проектирование, создание и эксплуатация системы защиты информации
- Определение периодичности обновления систем защиты
- Установление мер контроля, определение ответственности за соблюдение всех правил защиты информации

Задача **технических средств защиты** – предотвращение физического несанкционированного доступа к информации, находящейся на носителях информации или передаваемой по компьютерной сети, а также предотвращение сбоев оборудования.

- Сигнализация
- Замки и сейфы
- Блокираторы устройств внешней памяти, замки для клавиатур и корпусов компьютеров
- Дополнительные средства аутентификации пользователей (считыватели магнитных карт или биометрической информации)
- Средства визуального наблюдения (скрытые или обычные камеры)
- Средства мониторинга компьютерной сети (выявление неизвестных узлов по физическим адресам)
- Источники бесперебойного и резервного питания
- Дисковые массивы с резервированием данных и «горячим» восстановлением
- Кластерные решения

К **программным средствам** относятся:

- Средства управления доступом к системе и разграничения доступа
- Средства обеспечения контроля целостности и неизменности программного обеспечения (включая антивирусы)
- Средства криптографической защиты
- Средства защиты от вторжения извне
- Средства обнаружения вторжений
- Средства протоколирования действий пользователей
- Средства контроля состояния безопасности системы (обнаружения уязвимостей)

Управление доступом к системе может осуществляться двумя способами:

А. Парольная защита (для создания «сильных паролей целесообразно применять генераторы паролей). Во многих современных АИС применяется двухфакторная защита — идентификация на основе пароля и подтверждение значимых действий с помощью одноразоввых случайно генерируемых паролей, передаваемых мользователю по независимым каналам связи, в частности, мобильной телефонной связи.

Б. Средства аутентификации на основе ключей шифрования

К **средствам защиты от вторжений** относятся **сканеры сети**, **сканеры портов**, **сканеры уязвимостей** и **сканеры безопасности.**

Сканер сети (сниффер) – программное средство, обнаруживающее типы пакетов, передаваемые по сети и источники этих пакетов по физическим и IP-адресам.

Также сниффер помогает выяснить, не появились ли в сети новые устройства (новые физические адреса).

Настройки сниффера на выявление источников пакетов определённого протокола или наборот, на виды пакетов, посылаемых с определённого адреса (группы адресов) – фильтры.

Например, сканер сети WireShark позволяет определить узлы сети (их аппаратные и ip-адреса), отправляющие пакеты различных протоколов прикладного уровня стека TCP/IP. Соответственно, можно определить появление новых устройств в сети ил несанкционированную передачу пакетов какого-либо протокола.

Стандартной практикой для обеспечения защиты от несанкционированного прослушивания сети является установка разрешений: доступа к сети предприятия только компьютерам с известными физическими (MAC) адресами и сопоставление каждого порта сетевых коммуникационных устройств (коммутаторов) с конкретными MAC-адресами.

Сканер портов по известному IP-адресу показывает, какие порты протокола TCP/IP «открыты» на данном узле, т.е. какие сетевые сервисы (службы) на нём запущены.

Соответственно, возможно выявить сервисы, работа которых не требуется в конкретной АИС и выключить их для обеспечения более высоркого уровня защищённости, поскольку каждый сервис обеспечивается программными средствами, которые могут содержать ошибки и уязвимости.

Сканер уязвимостей по известному IP-адресу для некоторых протоколов прикладного уровня (сервисов) показывает, какие именно программные средства обеспечивают работу этих сервисов. Выдаётся также информация об известных проблемах с безопасностью, связанных с ошибками в конкретных

версиях программ.

Сканер безопасности – программный комплекс, объединяющий функции сниффера, сканера портов и уязвимостей. Может имитировать атаки и оценивать результаты их успешности. Содержит в своём составе набор программ, использующих уязвимости («эксплойтов»).

Существуют коммерческие программы (для конкретных операционных систем, например, **XSpider** и **Microsoft Baseline Security Analyzer**), свободно распространяемые средства (для различных операционных систем, например, **OpenVAS**).

Существуют свободно распространяемые специализированные дистрибутивы Linux для «внешней» проверки (например, **BackTrack Linux**).

В этой области есть также сертифицированные отечественные разработки, например, средство контроля защищённости информационных систем «Сканер-ВС» (разработка НПО «Эшелон»).

Стоимость XSpider на 1024 проверяемых узла – 242 000 руб (по данным 2012 года). MSBSA – бесплатный.

На практике разница в качестве работы (по обнаружению уязвимостей) между коммерческими и свободными средствами незаметна.

Для прохождения сертификации того или иного средства защиты информации (СЗИ) необходим заявитель, то есть предприятие (организация), обеспечивающее подготовку сопроводительной документации и оплату испытаний. Поэтому коммерческие продукты значительно чаще проходят сертификацию.

В отличие от **сканеров портов** и **сканеров уязвимостей**, работающих «снаружи» анализируемой сети, **средства обнаружения вторжений** (детекторы вторжений**,** Intrusion Detection System – IDS) работает «внутри» сети.

IDS играет роль охранной сигнализации: она оповещает об атаке, оставляя работу с атакующим на другие системы и средства (вплоть до физических).

IDS работает с предварительно заданными шаблонами вредоносного трафика, называемыми правилами (rules) или «сигнатурами атак», которые позволяют определить, какой трафик в сети является вредоносным (атакой), а какой – нет (аналогично антивирусным программам). Эти правила нужно периодически обновлять, поскольку обнаруживаются только известные атаки.

Наиболее известная IDS – свободно распространяемая система **Snort**. Snort работает на третьем уровне модели OSI/RM – сетевом, отвечающем за IP и другой трафик.

Для второго (канального) уровня, ответственного за кадры Ethernet, можно использовать IDS **Kismet**.

Все сообщения и предупреждения, связанные с обнаружением сигнатур

атак, Snort записывает в журнал.

Средства протоколирования событий (действий пользователя и программных средств) играют важную роль при выявлении и расследовании фактов нарушения ИБ (инцидентов).

Протоколирование – сбор и накопление информации о событиях в АИС. У каждого сервиса (службы) собственный набор событий.

Для каждой службы (сервиса) события могут быть **внешние,** вызванные действиями других сервисов (например, сервис *vsftpd* получает от сервиса *xinetd* сигнал остановки), **внутренние,** связанные с действиями самого сервиса (напрмер, сервис *clamd* получает обновления антивирусных баз) и **клиентские,** связанные с действиями пользователей и администратора АИС (например, пользователь с адреса 192.168.1.2 обращается за web-страницей about.html).

Каждое событие записывается сервисом в **файл журнала (log-файл)**. Файлы журналов бывают *текстовые* (читаются прямо на экране или любым текстовым редактором) и *двоичные* (закодированные, требуют специальных программ для чтения).

В операционных системах семейства Windows журналы двоичные, требуют прав администратора. Во многих вариантах систем семейств Linux и BSD журналы текстовые, однако в последнее время наметилась тенденция к переходу на двоичные журналы (в версиях Linux для настольных компьютеров).

Текстовые журналы имеют очевидные преимущества перед двоичными:

- Можно изучать события при незагруженной системе (в «аварийном» режиме или при загрузке с внешнего устройства) или копировать на другие компьютеры и изучать файл журнала там
- Можно автоматически анализировать текст log-файла на наличие в нём определённых строк (подстрок) и при их обнаружении автоматически посылать уведомления администратору (по электронной почте или sms).

Процедурные меры обеспечения информационной безопасности

К процедурным мерам обеспечения информационной безопасности относятся организационно-технические мероприятия по поддержке работоспособности АИС, реагированию на инциденты и планированию восстановительных работ в случае, если инцидент привёл к серьёзным нарушениям работоспособности элементов АИС.

Поддержка работоспособности — повседневная деятельность, направленная на обеспечение нормального функционирования АИС.

Основные мероприятия:

- Поддержка пользователей

- Поддержка ПО
- Управление конфигурациями
- Резервное копирование
- Управление носителями
- Документирование АИС
- Регламентные работы

Существуют программные средства мониторинга и управления ИТ-инфраструктурой (свободно распространяемые и коммерческие), обеспечивающие автоматизацию этих задач в различной степени.

В случае нарушений ИБ (инцидентов) нужно предпринимать срочные меры. Они должны быть проработаны и спланированы заранее.

Три главные цели **реагирования на инциденты**:

- Локализация инцидента и уменьшение наносимого вреда
- Выявление нарушителя
- Предупреждение повторных нарушений

Специалист по безопасности (администратор) должен быть доступен 24 часа в сутки (или сменная работа).

Задачи локализации инцидента и уменьшения наносимого вреда и выявления нарушителя могут противоречить друг другу, поэтому важны приоритеты в политике безопасности.

Планирование восстановительных работ состоит из нескольких этапов:

- Выявление критически важных функций организации, установление приоритетов
- Определение ресурсов, требуемых для выполнения критически важных функций
- Определение перечня возможных аварий
- Разработка стратегии восстановительных работ
- Подготовка к реализации стратегии
- Проверка стратегии

Очень хорошо иметь резервирование оборудования, источников электроэнергии, данных, каналов связи. Однако это приводит к лишним расходам. Поэтому важно осознавать цену инцидента (для этого требуется выделить приоритеты политики безопасности и критически важные функции АИС).

Ответственность за реализацию процедурных мер обеспечения ИБ возлагается на службу (отдел) информационных технологий предприятия (организации). Однако качество работы этой службы во многом зависит от материального, кадрового и правового обеспечения. Поэтому в современном подходе к деятельности службы информационных технологий (сервисной модели) целесообразно применять **соглашение о качестве услуг** (Service Level

Agreement — SLA) — взаимные обязательства потребителя и поставщика услуг при заданном объёме финансирования. Оптимальный объём финансирования ИТ-подразделений по опыту компаний «Кремниевой долины» составляет от 2% до 4% общего бюджета организации. Если меньше, то возрастают риски нарушений ИБ, если больше – расходы являются неоправданными. В случае государственных (правительственных) организаций эта доля может доходить до 10% вследствие отсутствия прибыли.

Литература

1. Советов Б.Я., Цехановский В.В. Информационные технологии: учебник для бакалавров. / Б.Я.Советов, В.В.Цехановский. – 6-е изд. М.: Издательство Юрайт, 2013. – 263 с. ISBN 978-5-9916-2824-2.

2. Астахова А.В. Информационные системы в экономике и защита информации на предприятиях - участниках ВЭД: учебное пособие для вузов. / А.В.Астахова. СПб.: Издательский дом «Троицкий мост», 2014. – 216 с. ISBN 978-5-4377-0040-2.

3. Афонин П.Н. Информационные таможенные технологии: учебник для вузов. / П.Н.Афонин. СПб.: Издательский дом «Троицкий мост», 2012. – 352 с. ISBN 978-5-4377-0007-5.

4. Бройдо В.Л., Ильина О.П. Вычислительные системы, сети и телекоммуникации. / В.Л.Бройдо, О.П.Ильина.— 4-е изд. – СПб.: Питер, 2011. – 560 с. ISBN 978-5-49807-875-5.

5. Галатенко В.А. Основы информационной безопасности: учебное пособие / В.А.Галатенко; под ред. акад. РАН В.Б.Бетелина. — Изд. 4-е .— М.: Интернет-Университет информационных технологий (ИНТУИТ.РУ): БИНОМ. Лаборатория знаний, 2010 .— 205 с. ISBN 978-5-94774-821-5.

6. Кузнецов С.Д. Базы данных. Вводный курс. Электронный ресурс. Режим доступа: http://citforum.ru/database/advanced_intro/. Дата обращения: 15.04.2014.

7. Лапонина О.Р. Криптографические основы безопасности. Электронный ресурс. Интернет-Университет информационных технологий (ИНТУИТ.РУ). Режим доступа: http://www.intuit.ru/studies/courses/28/28/info. Дата обращения: 15.04.2014.

В 2009 году Университет стал победителем многоэтапного конкурса, в результате которого определены 12 ведущих университетов России, которым присвоена категория «Национальный исследовательский университет». Министерством образования и науки Российской Федерации была утверждена программа его развития на 2009–2018 годы. В 2011 году Университет получил наименование «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики»

КАФЕДРА ТАМОЖЕННОГО ДЕЛА И ЛОГИСТИКИ

Кафедра таможенного дела и логистики (ТДиЛ) Института международного бизнеса и права государственного образовательного учреждения высшего профессионального образования «Санкт-Петербургского государственного университета информационных технологий, механики и оптики» была образована в 2007 году. Кафедра ТДиЛ – единственная в России, которая готовит специалистов таможенного дела по стандартам Всемирной Таможенной Организации (ВТО) и имеет соответствующую аккредитацию ВТО. Среди членов кафедры есть как работники высшей школы, так и действующие сотрудники Федеральной таможенной службы. Кафедра осуществляет подготовку специалистов в области таможенного дела и логистики в соответствии с потребностями отрасли по специальности 080115 и 036401 «Таможенное дело» со следующими специализациями: «Таможенный менеджмент» и «Информационные таможенные технологии».

Хахаев Иван Анатольевич

Информационные таможенные технологии

Учебное пособие

В авторской редакции
Редакционно-издательский отдел НИУ ИТМО
Зав. РИО Н.Ф. Гусарова
Лицензия ИД № 00408 от 05.11.99
Подписано к печати 28.05.2014
Заказ № 3128
Тираж 100 экз.
Отпечатано на ризографе