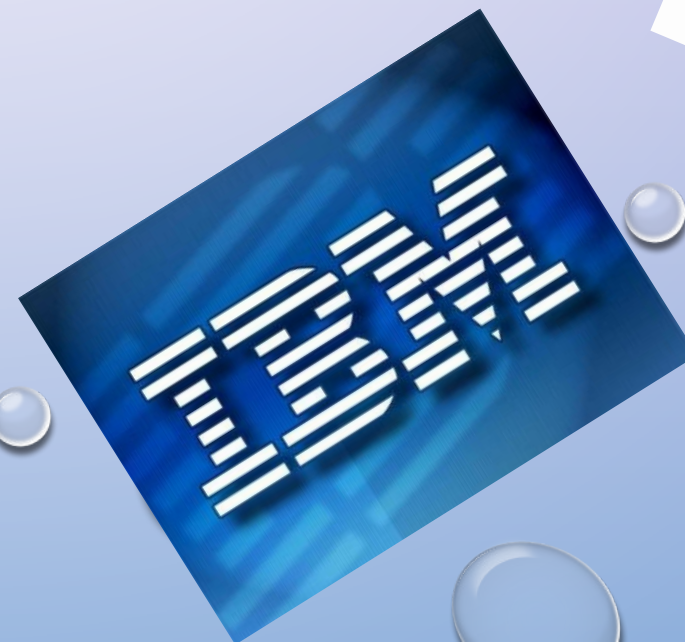




СТАНДАРТИЗАЦИЯ В ОБЛАСТИ ИКТ



ЮМАЕВА А.А.

ПОНЯТИЕ ИКТ КАК ОБЪЕКТА СТАНДАРТИЗАЦИИ

Для правильного представления места и роли стандартизации в области ИКТ, необходимо дать определение этому понятию как объекту стандартизации.

ИКТ – совокупность методов, производственных процессов и промышленно- технических средств, объединенных в технологическую цепочку с целью сбора, обработки, хранения, распространения, отображения и использования информации в интересах ее пользователей

Основными направлениями стандартизации в области ИКТ являются:

системы автоматической обработки текстов и речи

системы автоматической обработки текстов и речи



расчетно-логические и эксплуатационные системы

интеллектуальные системы для использования в управлении, проектировании, обучении и т.д.;

CALS-технологии непрерывной информационной поддержки ЖЦП

ПОНЯТИЕ ИКТ КАК ОБЪЕКТА СТАНДАРТИЗАЦИИ

Первые шаги в организации единого информационного пространства были предприняты в 80-х годах прошлого века в **оборонном комплексе США** в связи с возникшей необходимостью обеспечения оперативного обмена данными между заказчиком, производителем и потребителем вооружений и военной техники, а также повышения эффективности управления, сокращения бумажного документооборота и связанных с ним затрат.

Предварительно эти технологии (так называемые **CALS-технологии**) внедрялись только в военном деле, но доказав свою эффективность, эта концепция начала распространяться в промышленности, строительстве, транспорте, охватывая все этапы жизненного цикла продукции – от маркетинга до утилизации.

Изначально аббревиатура CALS расшифровывалась как «Computer Aided Logistic Support» - **«компьютерная поддержка поставок»**. С внедрением этой технологии в другие области аббревиатура сохранилась, но трактовка ее более широкая: «Continuous Acquisition and Life Cycle Support» - **«непрерывная информационная поддержка жизненного цикла продукта»**. В настоящее время существует 25 национальных организаций, координирующих вопросы CALS-технологий.



ПОНЯТИЕ ИКТ КАК ОБЪЕКТА СТАНДАРТИЗАЦИИ

К новым поколениям ИКТ относятся системы автоматической обработки текстов и речи, расчетно-логические и экспертные системы, интеллектуальные системы для использования в управлении, проектировании, обучении, CALS-технологии непрерывной информационной поддержки жизненного цикла продукции

При создании интегрированных систем, появлении новых поколений технических устройств и программного обеспечения, при их серийном производстве возникает проблема совместимости, в том числе функциональной, технических, информационных и коммуникационных средств. Эту проблему решает **методология открытых систем**, поддерживаемая в настоящее время крупными разработчиками и изготовителями средств вычислительной техники и средств связи

Открытая система представляет собой исчерпывающий и согласованный набор стандартов ИКТ и функциональных стандартов профилей, которые устанавливают требования к интерфейсам, службам и поддерживающим форматам, чтобы обеспечить совместимость и мобильность приложений, данных и персонала.



ПРИМЕР

Представим некую иерархию, «модель жизни», в который тоже будет 5 уровней – **атомы, молекулы, клетки (бактерии), люди, народы (общины)**. Каждый «уровень жизни» выполняет свои функции, рассматривая под микроскопом мы видим самый низкий уровень, который в принципе может существовать без уровня выше.

Так же само работают и типы данных. Каждому из них соответствует свой уровень модели **кроме 5-го, ему соответствуют сразу 3.**

- Нижние уровни (с 1 по 3) модели OSI управляют физической доставкой сообщений и их называют **уровнями среды передачи данных (media layers)**.
- Верхние уровни (с 4 по 7) модели OSI призваны обеспечить точную доставку данных между компьютерами в сети и их называют **уровнями хост-машины (host layers)**.
- Модель OSI *не является* схемой реализации сети, она только определяет функции каждого уровня.

Модель OSI		
Тип данных	Уровень (layer)	Функции
Данные	7. Прикладной (application)	Доступ к сетевым службам
	6. Представительский (presentation)	Представление и шифрование данных
	5. Сеансовый (session)	Управление сеансом связи
Сегменты	4. Транспортный (transport)	Прямая связь между конечными пунктами и надежность
Пакеты	3. Сетевой (network)	Определение маршрута и логическая адресация
Кадры	2. Канальный (data link)	Физическая адресация
Биты	1. Физический (physical)	Работа со средой передачи, сигналами и двоичными данными

Семь уровней эталонной модели OSI

1-й. **Биты, физический уровень**. (bit –кусочек, частичка с англ.) импульсы, частички которые передаются в физической среде. Представляет собой среду передачи данных – **wifi** (радиоимпульсы), электричество в сетевых проводах, оптоволокно(световой импульс) и т.п.

Протоколы: **802.11, Wi-Fi, GSM, IEEE 802.15 (Bluetooth)**...

- *Спецификации физического уровня определяют такие характеристики, как уровни напряжений, временные параметры изменения напряжений, скорости физической передачи данных и т.п.*

2-й **Кадры, канальный уровень**. Импульсы, с провода, или радиоэфира попадают в разъем (канал) оборудования. Там они преобразуются в кадры. Проверяется их целостность, возможна отправка дальше. Отправка идет по **Mac – адресу**. Оборудование, способное выполнять такие простейшие операции – **коммутаторы, мосты, свитчи**

Протоколы: **Ethernet, ARCnet, ATM**...

Канальный уровень решает вопросы физической адресации, топологии сети, уведомления об ошибках, упорядоченной доставки кадров, а также управления потоком данных.



Семь уровней эталонной модели OSI

3-й **Пакеты, сетевой уровень**. Кадры «могут гулять» на небольшие расстояния. От одного интерфейса (mac-адреса) к другому. Для того, чтобы информация дошла до конкретного места, она упаковывается в пакеты и будет гулять по сети, пройдя возможно десятки компьютеров, но доберётся до нужного места. Передача идет уже не по mac-адресу а по **ip адресу**. Оборудование, которое может выполнять эти функции это **роутеры, маршрутизаторы**.

Протоколы: **IP/IPv4/IPv6, IPsec...**

- *Сетевой уровень – комплексный уровень, обеспечивающий соединение и выбор маршрута между конечными системами, которые могут располагаться географически в разных сетях.*

4-й **Сегменты, транспортный уровень**. Скачиваем фильм, который разбит на миллион пакетов, все перекачались, а один заблудился, и все вместе теперь не склеить. Чтоб такого не произошло, на этом уровне пакеты объединяются в сегменты и так транспортируются, что если какой-то теряется, идет запрос на повтор потери. Если пришло 2 одинаковых, ненужные удаляются. Так работает протокол **TCP, UDP** работает быстрее, но может терять сегменты.

- *Транспортный уровень обеспечивает механизмы для установки, поддержания и упорядоченного завершения действий виртуальных каналов, обнаружения и устранения неисправностей транспортировки, а также управления информационным потоком.*



Семь уровней эталонной модели OSI

5-й уровень **сеансовый**. Нам нужны не сегменты, а данные, а поступать они будут, только если начать сеанс с сервером. Выбирая «скачать фильм» с интернета, мы открываем сеанс связи с сервером и закроется он автоматически после загрузки. На этом уровне определяется синхронизация, права, обмен.

Протоколы: **ADSP, ASP...**

- Сеансовый уровень устанавливает, управляет и завершает сеансы взаимодействия приложений.
- Сеансы включают диалог между двумя или более объектами представления. Сеансовый уровень синхронизирует диалог между объектами уровня представлений и управляет обменом информацией между ними.
- Сеансовый уровень обеспечивает класс услуг и средства формирования отчетов для формирования отчетов об особых ситуациях.

6-й уровень. **представительский**. Итак, у нас уже есть данные, непонятный файл, который ничего не делает, нам нужно как-то презентовать его. Возможно, сжать, или распаковать, найти кодировку для открытия, или возможно шифр, для передачи по сети. Все это происходит на этом уровне.

Протоколы: **LPP, NDR**

- Уровень представлений отвечает за то, чтобы информация, посылаемая из уровня приложений одной системы, была читаемой для уровня приложений другой системы.
- При необходимости уровень представлений преобразовывает форматы данных путем использования общего формата представления информации.



Семь уровней эталонной модели OSI

7-й уровень. **Прикладной** (application, уровень приложений) . Тот уровень, на котором мы работаем. Пользователю, в принципе, данные не нужны, ему нужно, чтобы работала его программа, приложение. Это самый верхний уровень, на котором приложение, которое находится на компьютере будет обращаться в сеть, за необходимыми данными.

- *Уровень приложений – самый близкий к пользователю уровень модели OSI. Данный уровень не предоставляет услуги другим уровням, а только обслуживает прикладные процессы вне пределов модели OSI.*
- *Уровень приложений идентифицирует и устанавливает доступность предлагаемых партнеров для связи, синхронизирует совместно работающие прикладные программы, а также устанавливает договоренности о процедурах восстановления после ошибок и контроля целостности данных.*



ПОНЯТИЕ ИКТ КАК ОБЪЕКТА СТАНДАРТИЗАЦИИ

**Развитие и совершенствование базы ТНПА в области ИКТ
направлено на достижение следующих целей:**

обеспечение повышения
оперативности, устойчивости и
эффективности
распространения ИКТ во всех
сферах деятельности общества
и человека

создание и поддержание
необходимого для устойчивого
развития общества уровня
информационного потенциала

интеграцию в мировое
информационное
пространство

поощрение, внедрение
передовых отечественных и
зарубежных информационных
технологий

развитие первичной сети связи передачи
данных

**Основными объектами
стандартизации ИКТ
являются:**

средства вычислительной
техники и сети передачи
данных

информационное
обеспечение и базы данных

программное обеспечение

информационные системы

Стандартизация ИКТ на международном и региональном уровнях



Стандартизация ИКТ на международном и региональном уровнях

Стандартизацией ИКТ на международном уровне занимаются три международные организации ISO, IEC, ITU

ISO (ИСО) (International Organization for Standardization - **Международная организация стандартизации**)

IEC (МЭК) (International Electrotechnical Commission - **Международная электротехническая комиссия**)

ITU (МСЭ) (International Telecommunication Union - **Международный союз электросвязи,**)

Одной из важнейших задач, решаемых этими организациями, является устранение ТБТ (тех. Барьеры в торговле) за счет решения вопросов совместимости средств вычислительной техники, которые в настоящее время входят в **состав более 50% продукции**, выпускаемой электротехнической и электронной промышленностью.

Сектор стандартизации Международного союза электросвязи ITU-

Т специализируется на разработке рекомендаций, которые обеспечивают интероперабельность (способность системы к взаимодействию с другими системами) коммуникационного сервиса в глобальном масштабе, т.е. сервиса, связанного с передачей данных интегрированных услуг связи: голоса и данных, сообщений и справочной информации



Стандартизация ИКТ на международном и региональном уровнях

ISO и IEC, а также их совместным техническим комитетом по стандартизации ISO/IEC/JTC1 разработано более 1500 международных стандартов, охватывающих следующие области ИКТ:

телекоммуникационный и информационный обмен между системами

программное обеспечение

средства для цифрового обмена данными

идентификационные карточки

языки программирования, их среда и интерфейс программного обеспечения

совместимость информационно-технологического оборудования

компьютерная графика и обработка изображения

безопасность информационных технологий

автоматический сбор данных

управление использованием данных

описание документа и языковая обработка

пользовательский интерфейс и т.д.

Стандартизация ИКТ на международном и региональном уровнях

Международные стандарты образуют в основном взаимосвязанный комплекс базовых стандартов, которые определяют *рекомендуемые нормы, правила и требования к компонентам и средствам ИКТ*

Recommendation



На развитие стандартизации в области ИКТ значительное влияние оказывают **крупные международные консорциумы** (150 консорциумов, работают в области стандартизации ИКТ). Как правило, консорциумы различаются **сферами интересов, организационной инфраструктурой и способами финансирования**.

ISOC (Internet Society – Общество Интернета, www.isoc.org) – ассоциация экспертов, отвечающая за разработку стандартов Интернет-технологий

IETF (Internet Engineering Task Force – Рабочая группа инженеров Интернета, www.ietf.org) решает текущие задачи в области стандартизации и развития Интернет-технологий

IRTF (Internet Research Task Force – Исследовательская группа Интернета, www.irtf.org) решает проблемные задачи по развитию Интернет-технологий

OMG (Object Management Group – Группа управления объектами, www.omg.org) – международный консорциум, осуществляющий разработку стандартов унифицированного распределенного программного обеспечения, созданного на принципах объектно-ориентированной модели

W3C (World Wide Web Consortium, www.w3.org) – консорциум, который специализируется в области разработки и развития стандартов WWW-технологий, таких, как, например, HTTP, HTML, URL, XML

ATM Forum (Asynchronous Transfere Mode Forum, www.atmforum.org) – консорциум, целями которого являются разработка и развитие стандартов широкополосных сетей асинхронного режима передачи данных

ECBS (European Commitee for Banking Standards – Европейский комитет банковских стандартов, www.ecbs.org) отвечает за разработку общеевропейского стандарта для банковской инфраструктуры

DAVIC (Digital Audio-Visual Council – Совет по развитию цифровых аудио- и видеомультимедиа систем, www.davic.org) – консорциум, осуществлявший разработку и развитие архитектурных, функциональных и информационных моделей и стандартов мультимедиа-сервисов Глобальной информационной инфраструктуры

TeleManagement Forum (www.tmforum.org) – глобальный консорциум операторов и поставщиков услуг, разрабатывает стандарты в области управления частными сетями и услугами

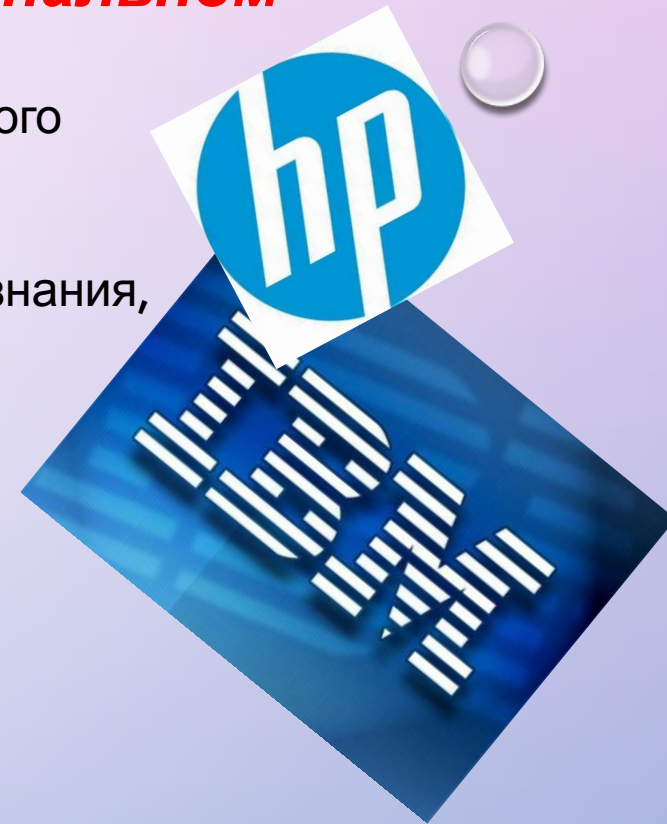
Open Group (www.opengroup.org) – организация, сформированная в 1996 г. в результате объединения консорциумов X/Open и Open Software Foundation, исследует вопросы открытости и бесшовного введения информационных систем в интернет

Gigabit Ethernet Alliance (www.gigabit-ethernet.org) – консорциум, целью которого является разработка стандартов технологий Ethernet нового поколения (стандарт IEEE 802.3z на волоконно-оптические системы связи), обеспечивающих скорость передачи данных 1 Гбит/с.

Стандартизация ИКТ на международном и региональном уровнях

Альтернативой международным консорциумам является деятельность большого числа конкурирующих компаний (HP, IBM, Sun Microsystems, SCO Group, Novell др.), производящих **совместимую серийную технику**, стандарты которой становятся международными «де-факто» (в международной практике – одна из форм признания, означающая официальное, но еще не юридическое признание).

*Работы по стандартизации ИКТ также проводятся промышленными профессиональными организациями, среди которых следует особо выделить **Институт инженеров по электротехнике и электронике (IEEE)**.*



IEEE

Первый стандарт по разработке программного обеспечения был создан IEEE еще в **1979** г. К 1990 г. ISO/IEC JTC 1/SC 7 разработал 8 стандартов (6 действуют и в настоящее время), IEEE к этому времени уже разработал 14 стандартов по программному обеспечению, число которых возросло до 27 к 1994 г., сейчас их более 50.

РЕГИОНАЛЬНЫЙ УРОВЕНЬ

На региональном уровне в странах ЕС **координацию работы по стандартизации** и обеспечению качества ИКТ проводят: Европейский комитет по стандартизации (CEN), Европейский комитет по стандартизации в электротехнике (CENELEC), Европейский институт по стандартизации в области электросвязи (ETSI).

Европейский комитет по стандартизации (фр. *Comité Européen de Normalisation, CEN*) — международная некоммерческая организация, основной целью которой является содействие развитию торговли товарами и услугами путём разработки европейских стандартов (евронорм, EN). Организация создана в 1961 году.



СЕНЭЛЕК создан в 1971 г. объединением двух европейских организаций — Европейского комитета по координации электротехнических стандартов стран – членов ЕАСТ и Европейского комитета по координации электротехнических стандартов стран – членов ЕС (в то время ЕЭС).

Члены СЕНЭЛЕК — 17 стран Европы: Австрия, Бельгия, Великобритания, Германия, Греция, Дания, Ирландия, Испания, Италия, Люксембург, Нидерланды, Норвегия, Португалия, Финляндия, Франция, ФРГ, Швейцария, Швеция. Все они представлены национальными электротехническими комитетами и являются членами МЭК (кроме Люксембурга).



Начало деятельности института ETSI относится к 1988 г. *Основная его задача* — поиск общих стандартов, на основе которых можно создать комплексную инфраструктуру электросвязи. Эта инфраструктура призвана обеспечить полную совместимость любого оборудования и услуг, предлагаемых потребителям.



РЕГИОНАЛЬНЫЙ УРОВЕНЬ

Кроме указанных организаций в работе по созданию стандартов ИКТ участвуют и специализированные региональные организации, которыми разработано более 600 европейских стандартов в области ИКТ:

1. Европейская конференция почтовой и телеграфной связи (СЕРТ) (СЕРТ была образована в 1959 году 19 странами. В настоящее время включает в себя 48 стран-членов, охватывая практически всю Европу)
2. Европейский комитет по сертификации в области информационных технологий (ЕСИТС).

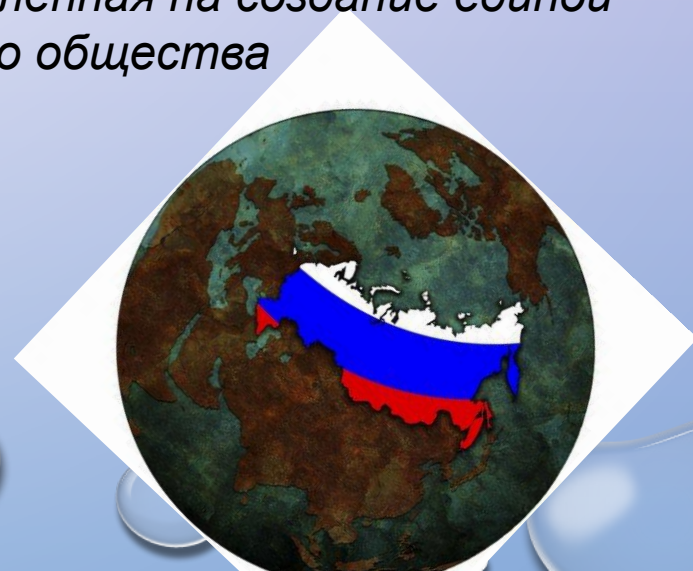


European Conference of Postal
and Telecommunications Administrations

- 48 European countries cooperating to regulate posts, radio
spectrum and communications networks

*Одной из главных тенденций процесса стандартизации является все **более тесная интеграция** деятельности различных организаций, направленная на создание единой системы стандартизации информационного общества*

Основным направлением работ по стандартизации ИКТ в РФ является использование международных достижений и принятие международных стандартов в качестве государственных



СТАНДАРТИЗАЦИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ



ИБ

Информационная безопасность – состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства.



Защита информации представляет собой деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию, т. е. процесс, направленный на достижение этого состояния

В качестве стандартной модели безопасности часто используется модель

CIA:

ОСНОВНЫЕ СОСТАВЛЯЮЩИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ



- С** – конфиденциальность (confidentiality) – доступность информации только определенному кругу лиц;
- I** – целостность (integrity) – гарантия существования информации в исходном виде;
- A** – доступность (availability) – возможность получения информации авторизованным пользователем в нужное для него время.

К перечисленным выше можно добавить и другие категории информационной безопасности:

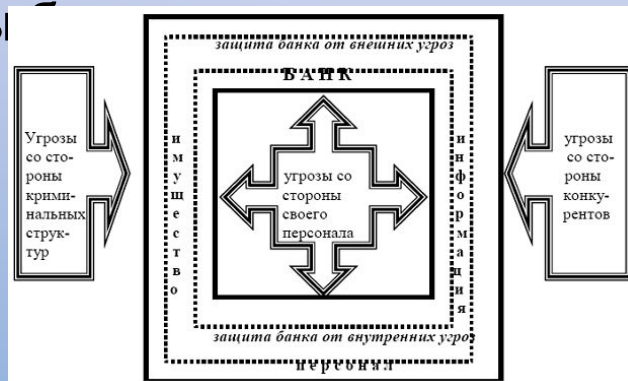
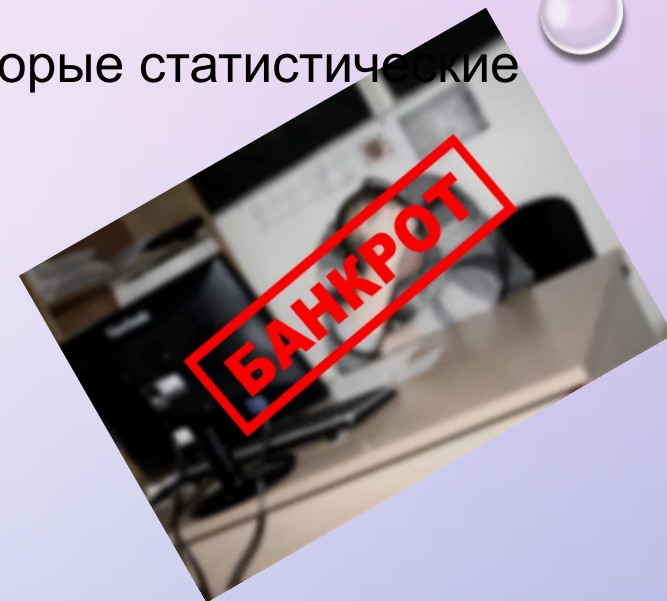
- аутентичность** – возможность установления автора информации;
- апеллируемость** – возможность доказать, что автором является именно заявленный человек, а не другой.

ИБ

Внимание к информационной безопасности закономерно. Вот некоторые статистические данные, объясняющие ее актуальность.

1. Если коммерческая организация допускает утечку более 20% важной внутренней информации, то в 60 случаях из 100 она банкротится.
2. Утверждают также, что 93% компаний, лишившихся доступа к собственной информации на срок более 10 дней, покинули бизнес, причем половина из них заявила о своей несостоятельности сразу же.

По статистическим данным Национального отделения ФБР США по компьютерным преступлениям, от 85 до 97% нападений на корпоративные сети **не только не пресекаются, но даже и не обнаруживаются**. Специальная группа экспертов провела анализ защищенности военных информационных систем; в 88% случаях несанкционированное проникновение посторонних в эти системы



Таким образом, защита информации по своим характеристикам и затратам должна быть **соразмерной масштабам угроз**.

ИБ

Информационная безопасность не обеспечивает абсолютную защиту, и ее можно трактовать как **предупредительные действия**, которые позволяют защитить информацию и оборудование от угроз и несанкционированного использования.

Способы защиты информации постоянно меняются, как меняется наше общество и технологии. Но какие бы сложные шифры и современные технические средства ни использовали для защиты информации, в любой системе безопасности существует **самое слабое звено – это человеческий фактор**. И этому есть много исторических подтверждений.

Так, летом 2013 года полиция Тайваня задержала трёх топ-менеджеров корпорации HTC, связанных с разработкой продуктов. Одно из выдвинутых обвинений – передача конфиденциальной информации по перспективным разработкам конкурирующим фирмам. При этом не лишним будет напомнить, что на протяжении долгого времени дела HTC шли не самым лучшим образом, финансовые показатели ухудшались, а в 3 квартале 2013 года компания зафиксировала чистый убыток около \$100 млн. Использование служебного положения – типичный кейс для целенаправленных утечек.

Организационные факторы:

- структуры и методы управления
- организация труда
- культура безопасности
- корпоративная культура

Качество персонала:

- компетентность
- опытность (тренированность)
- здоровье
- психология безопасности

НАДЕЖНОСТЬ ПЕРСОНАЛА

Условия труда:

- технологии
- эргономика
- охрана труда
- санитарно-гигиенические условия
- трудовой режим

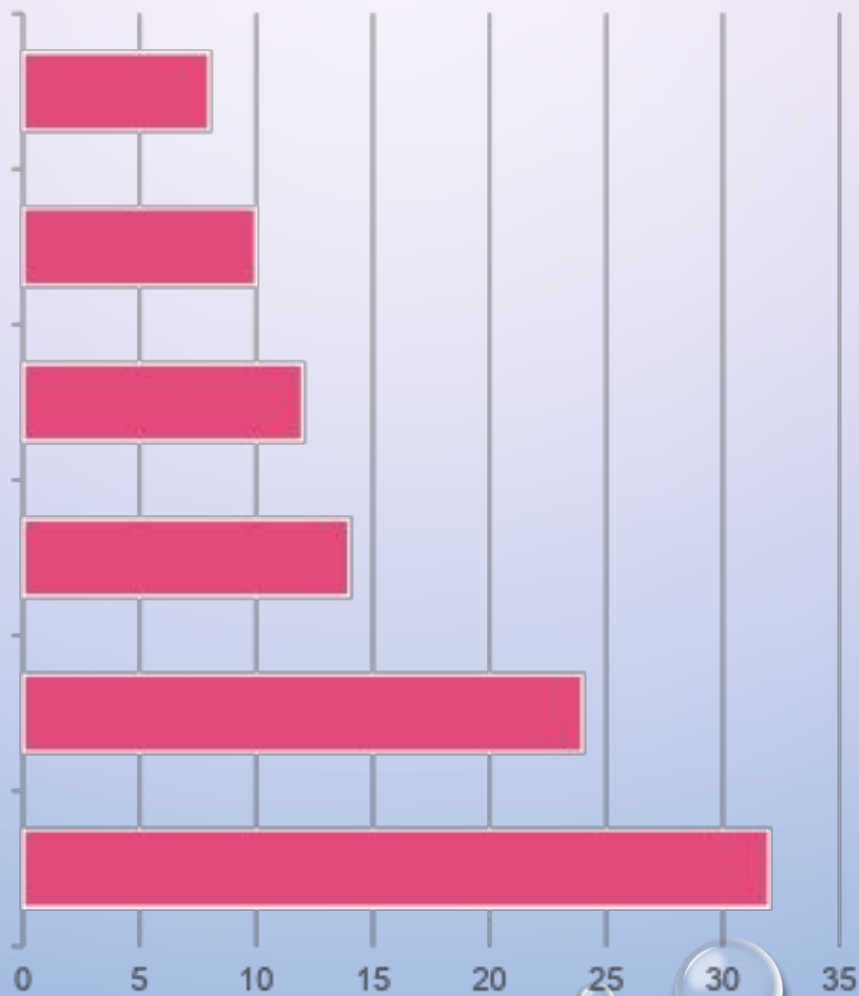
Мотивация к труду:

- моральное и материальное стимулирование
- карьерный рост и социальный пакет
- психологический климат
- уровень жизни

ИБ

Согласно данным портала информационной безопасности Content Security степень опасности внутренних и внешних угроз такова:

табой работой кадров по сплочению коллектива



В качестве примера можно привести «утечку» клиентской базы в компанию-конкурент вместе с сотрудниками. По неофициальной информации, с такой проблемой столкнулся филиал коммерческого банка ОАО «Уралсиб» в Воронеже, когда в конце 2009 года ряд сотрудников «Уралсиба» перешли работать в Воронежский филиал Банка «Поволжский» забрав с собой клиентскую базу предыдущего работодателя. И клиенты «Уралсиба» с назойливой регулярностью начали получать предложения от нового банка. Это может привести к оттоку клиентов, возможным судебным тяжбам и, конечно же, удару по репутации банка. В «Уралсибе» и банке «Поволжский» эту информацию не комментируют.

ИБ

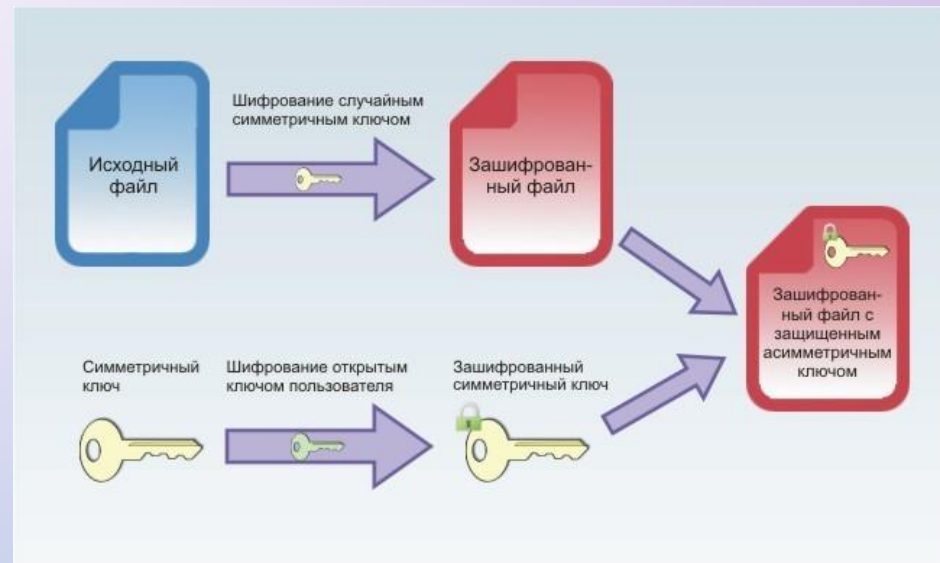
Кроме субъективных причин безопасности существуют и **технические**, обусловленные особенностью работы любых электронных систем, т.е. наличием излучения. Например, блок шифрования посылает зашифрованное сообщение по телефонной линии, а вместе с ним передается и электрический сигнал от исходного сообщения. Следовательно, при наличии хорошей аппаратуры исходное сообщение

можно восстановить

Шифровальная машина, как и любая другая электрическая машина, имеет **побочное электромагнитное излучение**, которое модулируется информационным сигналом еще до момента его кодирования. Таким образом, путем перехвата и анализа побочных излучений шифровальной машины, не имея ключа для расшифровки кодированных сообщений, представляется возможным получать необходимую информацию.

Долгое время все, что было связано с понятием ПЭМИН, было окутано завесой **секретности**. Первое сообщение, появившееся в открытой печати, принадлежит голландскому инженеру Вим ван Эку (Wim van Eck), опубликовавшему в 1985 году статью «Электромагнитное излучение видеодисплейных модулей:

Риск перехвата?» Статья посвящена потенциальным методам перехвата композитного сигнала видеомониторов. В марте 1985 года на выставке Securescom-85 в Каннах ван Эк продемонстрировал оборудование для перехвата излучений монитора. Эксперимент показал, что перехват возможен с помощью слегка доработанного обычного **телевизионного приемника**.



Образцы оборудования для перехвата ПЭМИ.



а)



б)

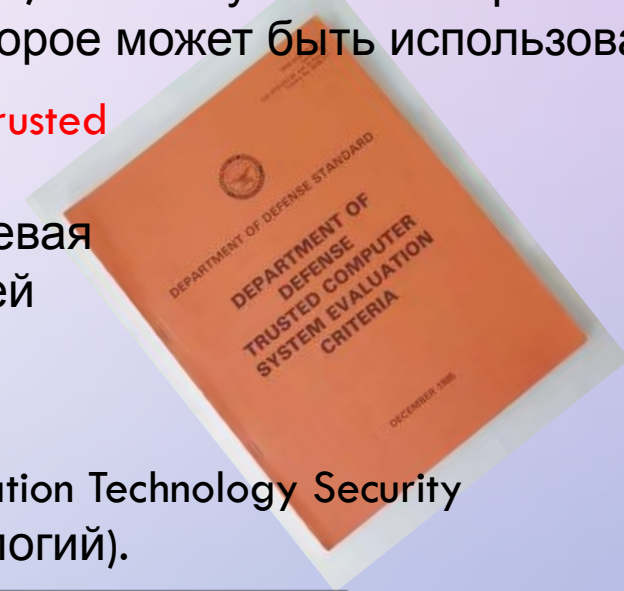
Комплекс перехвата побочных электромагнитных излучений СВТ:
а) специальное приёмное устройство PKI 2715 (дальность перехвата ПЭМИ от 10 до 50 м);
б) широкополосная направленная антенна R&S HL 007 (диапазон частот от 80 МГц до 1,3 ГГц, коэффициент усиления 5-7 дБ)



СТАНДАРТЫ ИБ

Проблема защиты излучения привела к созданию в США программы «TEMPEST», в рамках которой разработаны **стандарты на электрическое излучение компьютерных систем**, используемых в секретных организациях. Целью программы было уменьшение уровня излучения, которое может быть использовано для сбора информации.

В 1983 г. Министерством обороны США разработан стандарт **MIL 5200.28 Trusted Computing System Evaluation Criteria (TCSEC) (Критерий оценки безопасности компьютерных систем)**. Из-за цвета обложки он получил название «Оранжевая книга». Эта модель базировалась на правительственной концепции уровней классификации информации (несекретная, конфиденциальная, секретная, совершенно секретная) и уровней допуска.



В Европе критерием оценки безопасности служил стандарт ITSEC – Information Technology Security Evaluation Criteria (Критерий оценки безопасности информационных технологий).



TCSEC и его европейский аналог ITSEC были пересмотрены и в рамках ISO разработан новый стандарт безопасности **ISO/IEC 15408** (его аналог версии 1999 г. – СТБ 34.101.1-3-2004), в настоящее время принятый в новой редакции 2005 года и состоящий из трех частей



Стандарт ISO/IEC 15408 "Критерии оценки безопасности информационных технологий"

- идентификация и аутентификация;
- **защита данных пользователя;**
- **защита функций безопасности** (требования относятся к целостности и контролю данных сервисов безопасности и реализующих их механизмов);
- **управление безопасностью** (требования этого класса относятся к управлению атрибутами и параметрами безопасности);
- **аудит безопасности** (выявление, регистрация, хранение, анализ данных, затрагивающих безопасность объекта оценки, реагирование на возможное нарушение безопасности);
- **доступ к объекту оценки;**
- **приватность** (защита пользователя от раскрытия и несанкционированного использования его идентификационных данных);
- **использование ресурсов** (требования к доступности информации);
- **криптографическая поддержка** (управление ключами);
- **связь** (аутентификация сторон, участвующих в обмене данными);
- **доверенный маршрут/канал** (для связи с сервисами безопасности).

ISO/IEC 15408

Этот стандарт известен под названием «Common Criteria for Information Technology Security Evaluation» (CCITSE) (Критерий оценки безопасности информационных технологий). Критерии, сформулированные в TCSEC, ITSEC и CCITSE, определяют разбиение компьютерных систем на 4 основных уровня безопасности (A, B, C, D).

Уровень A самый высокобезопасный

Затем наиболее распространенный уровень C (с классами C2 и C1).

Далее следует уровень B, внутри которого в порядке понижения безопасности идут классы B3, B2, B1

Самый низкий уровень – D, включающий системы, которые не смогли получить аттестацию по заявленным выше классам

- уровень C — произвольное управление доступом;
- уровень B — принудительное управление доступом;
- уровень A — верифицируемая безопасность.

Для каждого класса определены *функциональные требования и требования гарантированности*, которым должна удовлетворять система, чтобы соответствовать определенному уровню сертификации.

СТАНДАРТЫ ИБ

Главная идея современной концепции безопасности сосредоточена в так называемых **профилях защиты (ПЗ)**, определяющих различные среды безопасности, в которые может быть помещена компьютерная система (например: ПЗ систем управления базами данных, ПЗ межсетевых экранов, ПЗ операционных систем, ПЗ систем управления доступом)

Профиль защиты (ПЗ) – это независимая от реализации совокупность требований безопасности для некоторой категории изделий ИТ, отвечающая специфическим запросам потребителя.

ПЗ **не регламентирует**, каким образом должны быть выполнены данные требования, тем самым предоставляя разработчику системы защиты самостоятельно выбирать средства защиты.

ПЗ может применяться либо к **определенному классу продуктов**, например, операционным системам или межсетевым экранам, и к **совокупности продуктов**, образующих систему информационной технологии (например, виртуальные частные *сети, PKI*).

Важно!

Использование профилей защиты преследует три основные задачи:

стандартизация наборов
требований к
информационным
продуктам

оценка безопасности

проведение сравнительного
анализа уровней
безопасности различных
изделий ИТ

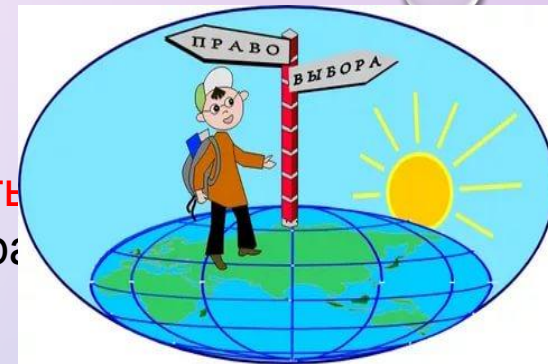
ПЗ подлежат **оценке, регистрации и сертификации** в соответствии с руководящими документами ФСТЭК России.

СТАНДАРТЫ ИБ

В настоящее время разработано более 20

ПЗ.

Компьютерные системы проходят оценку на соответствие этим профилям и сертифицируются. При покупке системы организация **имеет возможность выбрать профиль**, наиболее полно соответствующий ее потребностям, и подобрать аппаратно-программную систему, сертифицированную по этому профилю.



Следуя компромиссу между требованиями безопасности, эффективностью системы и ее ценой, подавляющее большинство компаний стремится сегодня получить сертификат по **классу С2**

Политика безопасности и уровень гарантированности для данного класса должны удовлетворять следующим важнейшим требованиям:

1. пользователи должны идентифицировать себя, причем аутентификационная информация должна быть защищена от НСД;
2. должны быть в наличии аппаратные или программные средства, позволяющие периодически проверять корректность функционирования аппаратных и микропрограммных компонентов доверенной вычислительной базы;
3. защитные механизмы должны быть протестированы (нет способов обойти или разрушить средства защиты доверенной вычислительной базы);

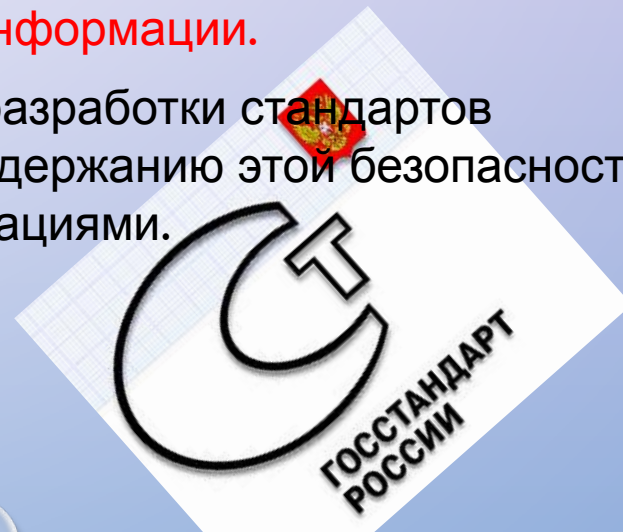
МЕЖДУНАРОДНЫЕ СТАНДАРТЫ ИБ

Однако технологии компьютерных систем **слишком быстро развиваются по сравнению с программой сертификации**. Новые версии операционных систем и аппаратных средств возникают и находят свои рынки сбыта еще до того, как более старые версии и системы проходят сертификацию. За то время, которое требуется системам для прохождения сертификации, они успевают устареть.

В настоящее время на международном уровне в сфере информационной безопасности разработано **более 60 международных стандартов**. Международные стандарты (BS 7799-1-2-3:2005(6), ISO/IEC 17799:2005, ISO/IEC 27001, 27002, 27005:2005) представляют собой сборник рекомендаций по развертыванию системы управления информационной безопасностью **для сотрудников организаций, ответственных за разработку, реализацию и обеспечение защиты информации**.

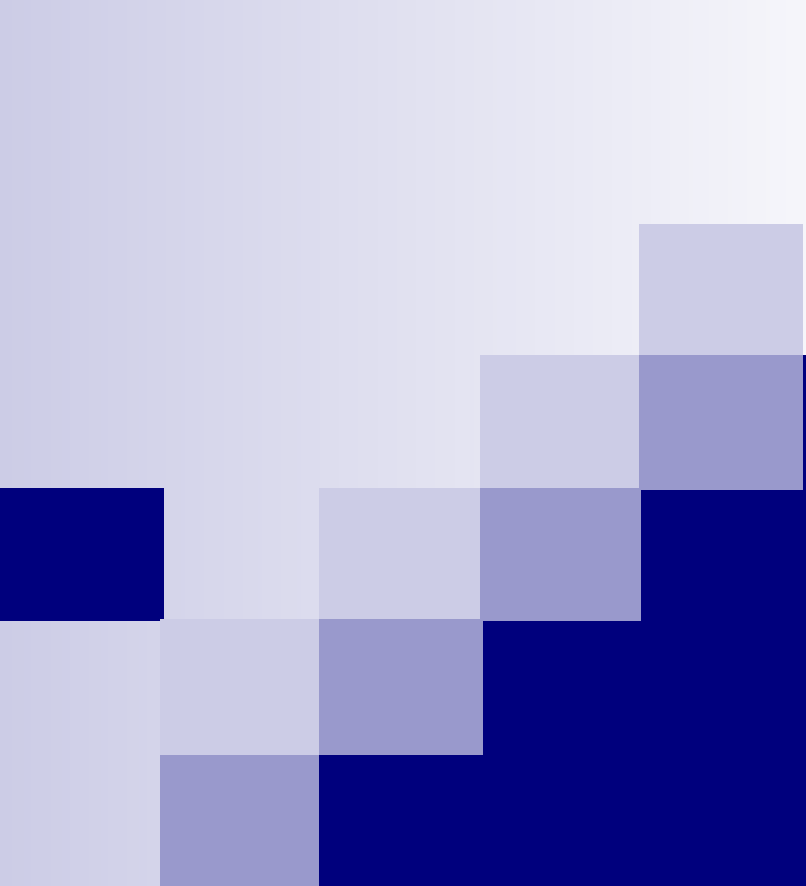
Эти основополагающие стандарты формируют **общую основу** для разработки стандартов безопасности отдельных организаций, эффективных правил по поддержанию этой безопасности и обеспечению конфиденциальности торговых связей между организациями.

На национальном уровне вышеперечисленные международные стандарты вступают в силу после их принятия в качестве **национальных стандартов**.



РОССТАНДАРТ

Федеральное агентство по техническому регулированию и метрологии



Стандарты информационной безопасности в РФ

ФСТЭК и его роль в обеспечении информационной безопасности в РФ

В Российской Федерации информационная безопасность обеспечивается соблюдение **указов Президента, федеральных законов, постановлений Правительства Российской Федерации, руководящих документов ФСТЭК России и других нормативных документов.**

В РФ с точки зрения стандартизации положений в сфере информационной безопасности первостепенное значение имеют руководящие документы (РД) **ФСТЭК России**, одной из задач которой является "**проведение единой государственной политики в области технической защиты информации**".

ФСТЭК России ведет весьма активную нормотворческую деятельность, выпуская **руководящие документы**, играющие роль национальных оценочных стандартов в области информационной безопасности. В качестве стратегического направления ФСТЭК России выбрала ориентацию на "Общие критерии".



За 15 лет своего существования **ФСТЭК разработала** и довела до уровня национальных стандартов **десятки документов**, среди которых:

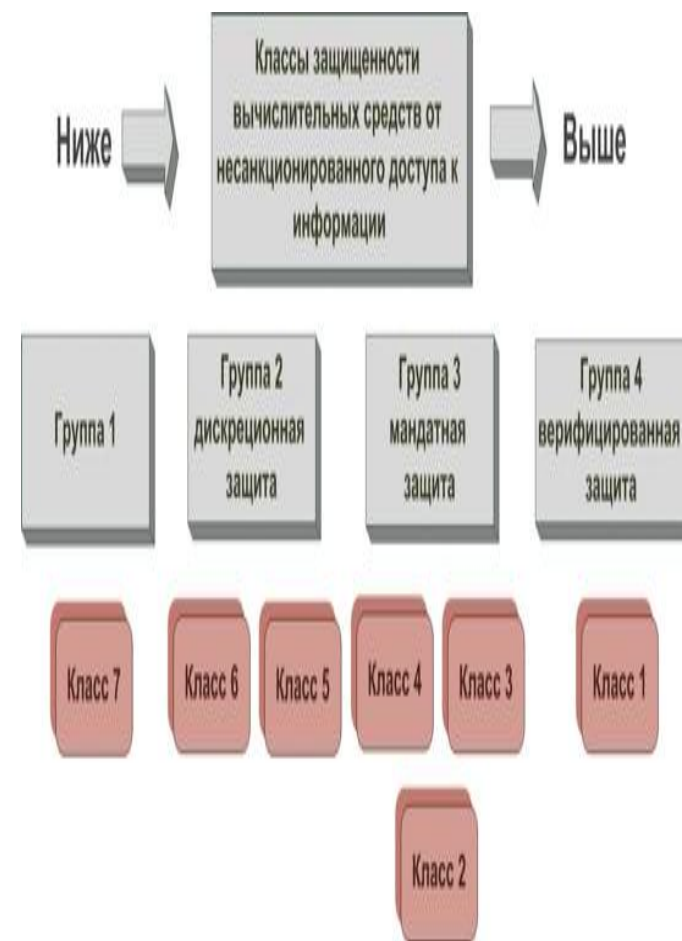
- ✓ **Руководящий документ "Положение по аттестации объектов информатизации по требованиям безопасности информации"** (Утверждено Председателем ФСТЭК России 25.11.1994 г.).
- ✓ **Руководящий документ "Автоматизированные системы (АС). Защита от несанкционированного доступа (НСД) к информации. Классификация АС и требования к защите информации"** (ФСТЭК России, 1997 г.).
- ✓ **Руководящий документ "Средства вычислительной техники. Защита от НСД к информации. Показатели защищенности от НСД к информации"** (ФСТЭК России, 1992 г.).
- ✓ **Руководящий документ "Концепция защиты средств вычислительной техники от НСД к информации"** (ФСТЭК России, 1992 г.).
- ✓ **Руководящий документ "Защита от НСД к информации. Термины и определения"** (ФСТЭК России, 1992 г.).
- ✓ **Руководящий документ "Средства вычислительной техники (СВТ). Межсетевые экраны. Защита от НСД к информации. Показатели защищенности от НСД к информации"** (ФСТЭК России, 1997 г.).
- ✓ **Руководящий документ "Специальные требования и рекомендации по технической защите конфиденциальной информации"** (ФСТЭК России, 2001 г.).

Документы по оценке защищенности автоматизированных систем в РФ

Руководящий документ "СВТ. Защита от НСД к информации. Показатели защищенности от НСД к информации" устанавливает **классификацию СВТ по уровню защищенности от НСД к информации** на базе перечня показателей защищенности и совокупности описывающих их требований. Основой для разработки этого документа явилась "Оранжевая книга". Этот оценочный стандарт устанавливается **семь классов защищенности** СВТ от НСД к информации.

Самый низкий класс – седьмой, самый высокий – первый. Классы подразделяются на четыре группы, отличающиеся уровнем защиты:

- I. первая группа содержит только один седьмой класс, к которому относят все СВТ, не удовлетворяющие требованиям более высоких классов;
- II. вторая группа характеризуется дискреционной защитой и содержит шестой и пятый классы;
- III. третья группа характеризуется мандатной защитой и содержит четвертый, третий и второй классы;
- IV. четвертая группа характеризуется верифицированной защитой и включает только первый класс.

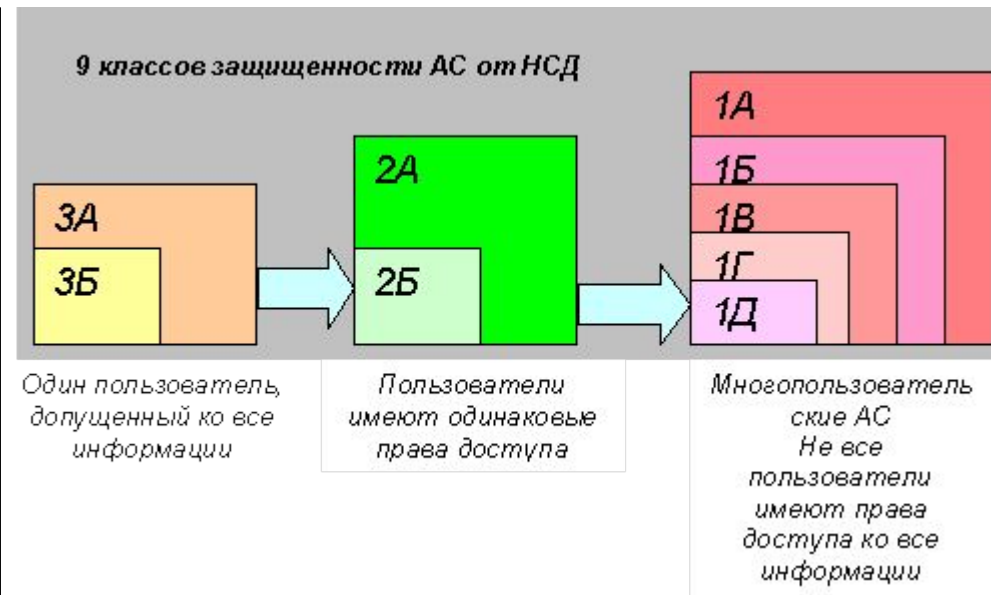


Документы по оценке защищенности автоматизированных систем в РФ

Руководящий документ **"АС. Защита от НСД к информации. Классификация АС и требования по защите информации"** устанавливает **классификацию автоматизированных систем**, подлежащих защите от несанкционированного доступа к информации, и требования по защите информации в АС различных классов.

К числу определяющих признаков, по которым производится группировка АС в **различные классы**, относятся:

- I. наличие в АС информации различного уровня конфиденциальности;
- II. уровень полномочий субъектов доступа АС на доступ к конфиденциальной информации;
- III. режим обработки данных в АС – коллективный или индивидуальный.



В документе определены **девять классов защищенности АС от НСД** к информации. Каждый класс характеризуется определенной минимальной совокупностью требований по защите. **Классы подразделяются на три группы**, отличающиеся особенностями обработки информации в АС.

В пределах каждой группы соблюдается иерархия требований по защите в зависимости от ценности и конфиденциальности информации и, следовательно, иерархия классов защищенности АС.

Требования к защищенности автоматизированных систем

3.3 Использование аттестованных (сертифицированных) криптографических средств	-	-	-	+	-	-	-	+	+
4 Подсистема обеспечения целостности									
4.1 Обеспечение целостности программных средств и обрабатываемой информации	+	+	+	+	+	+	+	+	+
4.2 Физическая охрана средств вычислительной техники и носителей информации	+	+	+	+	+	+	+	+	+
4.3 Наличие администратора (службы защиты) информации в АС	-	-	-	+	-	-	+	+	+
4.4 Периодическое тестирование СЗИ НСД	+	+	+	+	+	+	+	+	+
4.5 Наличие средств восстановления СЗИ НСД	+	+	+	+	+	+	+	+	+
4.6 Использование сертифицированных средств защиты	-	+	-	+	-	-	+	+	+
"-" нет требований к данному классу; "+" есть требования к данному классу "СЗИ НСД" – система защиты информации от несанкционированного доступа.									

Документы по оценке защищенности автоматизированных систем в РФ

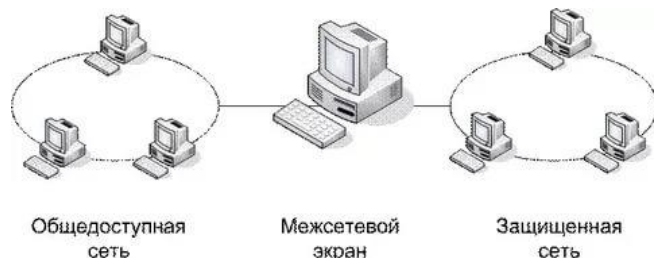
Руководящий документ "СВТ. Межсетевые экраны. Защита от НСД к информации. Показатели защищенности от НСД к информации" является основным документом для **анализа системы защиты внешнего периметра корпоративной сети**. Данный документ определяет показатели защищенности межсетевых экранов (МЭ). Каждый показатель защищенности представляет собой набор требований безопасности, характеризующих определенную область функционирования МЭ.

Всего выделяется пять показателей защищенности:

- ✓ управление доступом;
- ✓ идентификация и аутентификация;
- ✓ регистрация событий и оповещение;
- ✓ контроль целостности;
- ✓ восстановление работоспособности.

На основании показателей защищенности определяются следующие пять классов защищенности МЭ:

- ✓ простейшие фильтрующие маршрутизаторы – 5 класс;
- ✓ пакетные фильтры сетевого уровня – 4 класс;
- ✓ простейшие МЭ прикладного уровня – 3 класс;
- ✓ МЭ базового уровня – 2 класс;
- ✓ продвинутые МЭ – 1 класс.



МЭ первого класса защищенности могут использоваться в АС класса 1А, обрабатывающих информацию "Особой важности".

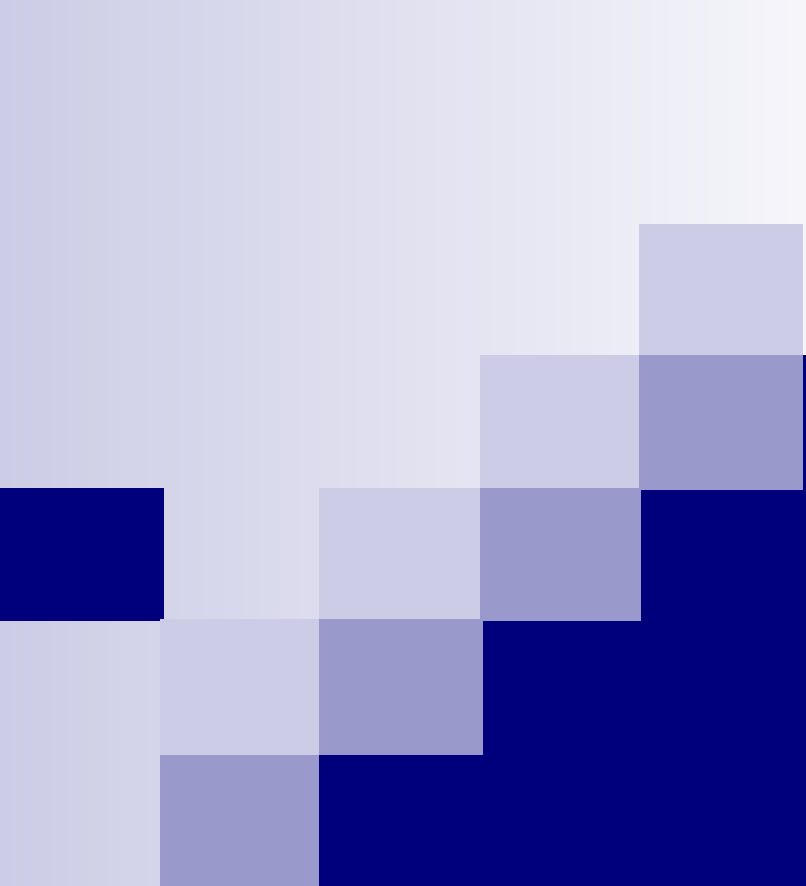
Второму классу защищенности МЭ соответствует класс защищенности АС 1Б, предназначенный для обработки "совершенно секретной" информации и т. п.

Третья группа классифицирует АС, в которых работает один пользователь, имеющий доступ ко всей информации АС, размещенной на носителях одного уровня конфиденциальности. Группа содержит два класса – 3Б и 3А.

Вторая группа классифицирует АС, в которых пользователи имеют одинаковые права доступа (полномочия) ко всей информации АС, обрабатываемой и (или) хранящейся на носителях различного уровня конфиденциальности. Группа содержит два класса – 2Б и 2А.

Первая группа классифицирует многопользовательские АС, в которых одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности и не все пользователи имеют право доступа ко всей информации АС.





Стандартизация языков программирования

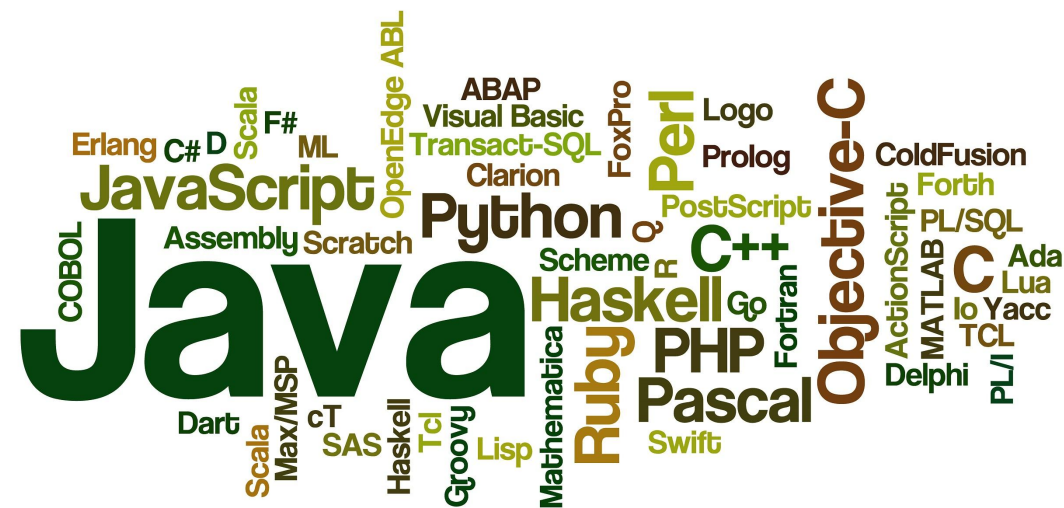
Стандартизация языков программирования

Процесс создания ИКТ определил появление разнообразных знаковых систем для записи алгоритмов – языков программирования

Язык программирования – формальная знаковая система, предназначенная для записи программ

Программа обычно представляет собой некоторый алгоритм, понятный для разработчика и исполнителя (например компьютера).

Язык программирования определяет **набор лексических, синтаксических и семантических правил, используемых при составлении компьютерной программы**. Он позволяет программисту точно определить, на какие события будет реагировать компьютер, как будут храниться и передаваться данные, а также какие именно действия следует выполнять над этими данными при различных обстоятельствах

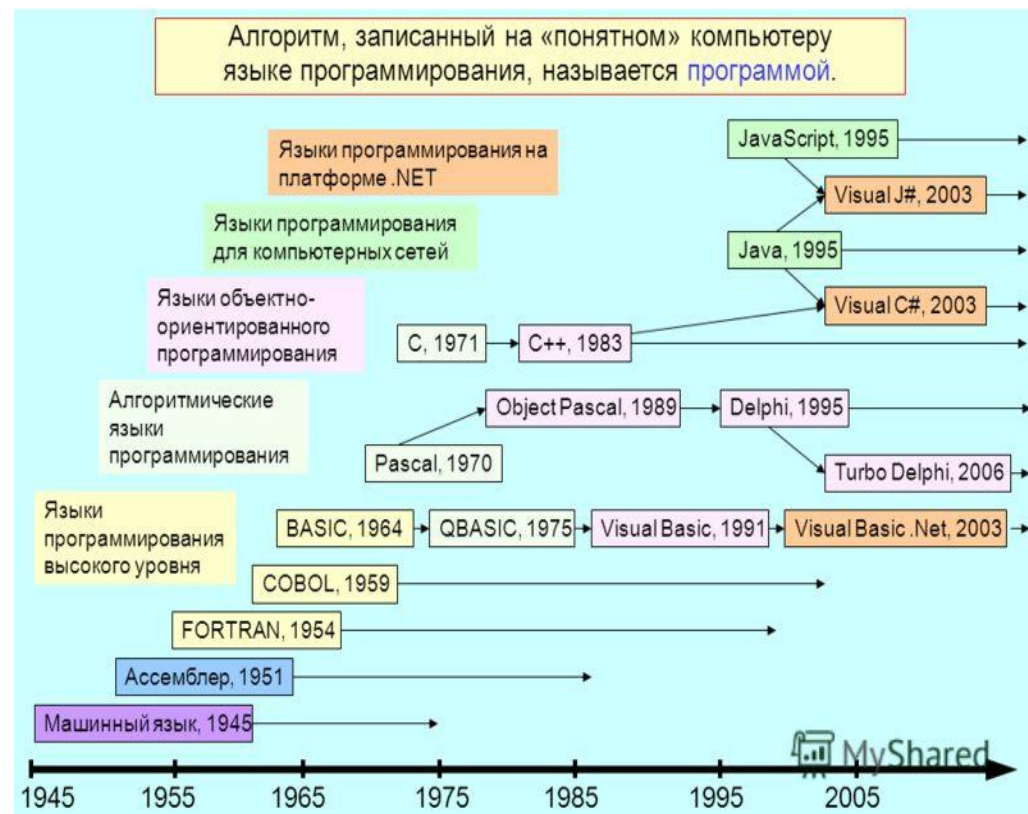


Стандартизация языков программирования

Со времени создания первых программируемых машин человечество придумало уже более **8500** языков программирования, число которых каждый год увеличивается. Некоторыми языками умеет пользоваться только небольшое число их собственных разработчиков, другие становятся известны миллионам людей

- У истоков развития вычислительной техники, программы создавались непосредственно **в машинных кодах**.
- Переход к символическому кодированию машинных команд был связан с появлением языка программирования **Assembler**.
- Новые возможности вычислительной техники привели к созданию в 1954 г. первого языка программирования высокого уровня – **Fortran**, который используется и в настоящее время для научных вычислений.
- В 1960 г. был создан язык программирования для коммерческих приложений **Cobol**.
- В 1964 г. IBM создала язык PL/1, который был призван заменить Cobol и Fortran, но так и не нашел широкого применения.

ИСТОРИЯ РАЗВИТИЯ ЯЗЫКОВ ПРОГРАММИРОВАНИЯ



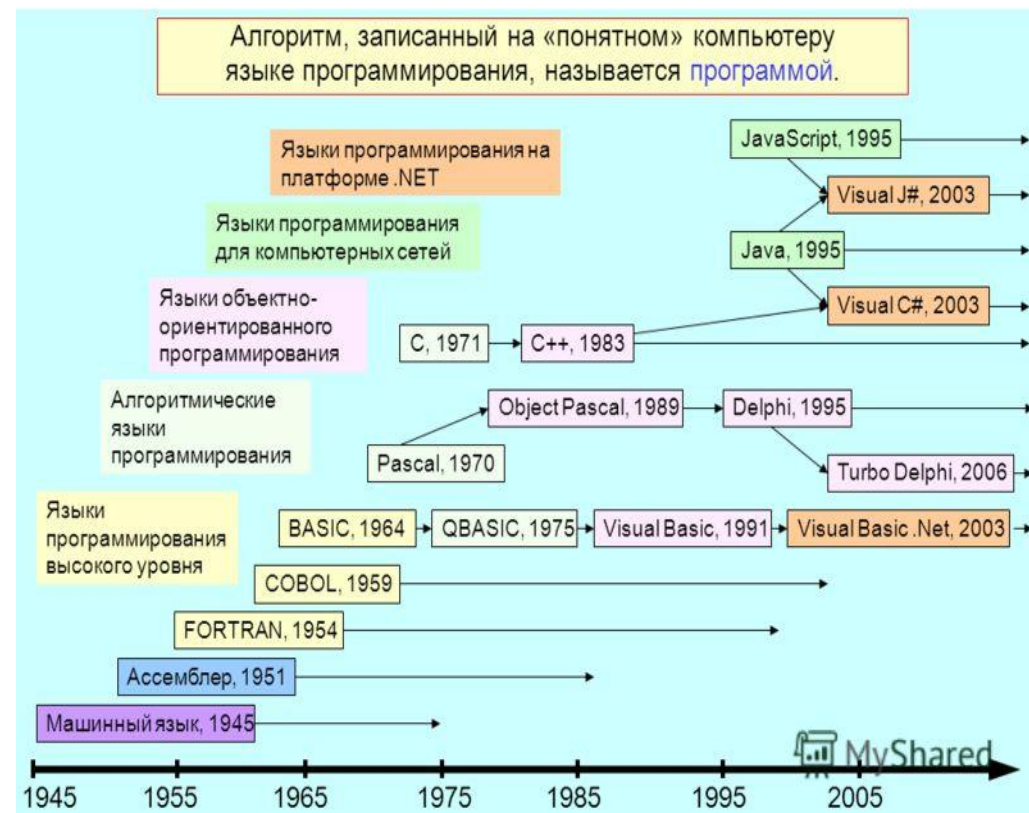
Стандартизация языков программирования

- В 1963 г. появился язык программирования BASIC – многоцелевой язык символьных инструкций для начинающих. В 1960 г. был создан язык программирования Algol.

Дальнейшее развитие языков программирования пошло в сторону более глубокого абстрагирования.

- В 1970 г. создан язык для структурного программирования Pascal.
- В 1969 – 1973 гг. для использования в операционной системе UNIX был разработан язык программирования C, позволяющий работать с данными так же эффективно, как и Assembler, предоставляя при этом структурированные управляющие конструкции и абстракции высокого уровня (структуры и массивы).
- В 1986 г. создана первая версия языка C++. Язык стал основой для разработки современных больших и сложных проектов.
- В 1995 г. в корпорации Sun Microsystems был создан язык Java.
- В 1999 – 2000 гг. в корпорации Microsoft создают язык прикладного уровня C# для CLR (Common Language Runtime), ориентированный на разработку многокомпонентных Интернет-приложений.
- В 1983 г. под эгидой Министерства Обороны США был создан язык Ada, который широко используется в военных и других крупномасштабных проектах.

ИСТОРИЯ РАЗВИТИЯ ЯЗЫКОВ ПРОГРАММИРОВАНИЯ



Стандартизация языков программирования

В последнее время в связи развитием Интернет-технологий, широким распространением высокопроизводительных компьютеров и рядом других факторов получили распространение так называемые **скриптовые языки**, первоначально используемые в качестве внутренних управляющих языков во всякого рода сложных системах.



При этом нет универсального языка программирования, предназначенного «для всеобщей применимости». Есть преимущества одного языка над другим при решении конкретной задачи в конкретных условиях

В широком смысле слова язык программирования может быть представлен в виде набора спецификаций, определяющих:

систему правил поведения языковых конструкций, т. е. смысловое значение (семантика);

структуру программ в виде набора символов (синтаксис).

*В общем случае язык программирования строится в соответствии с той или иной **базовой моделью вычислений**, **стилем написания программ** и **используемыми библиотеками***

Стандартизация языков программирования

Языки программирования ранее были рассчитаны на использование американского стандартного кода, предназначенного для **обмена информацией** – ASCII (American Standard Code for Information Interchange), разработанного ANSI X3.4.

Использование ASCII было **необходимым и достаточным условием** для записи любых конструкций языка.

Расширенная версия ASCII, предусматривающая возможность размещения национальных символов, **стандартизована на международном уровне – ISO/IEC 646:1991**

Впоследствии оказалось удобнее использовать другие кодовые страницы. Например, стандарты серии **ISO 8859** устанавливают 8 битовую кодировку символов, а **ISO/IEC 10464** – единый набор символов кодировки (последняя версия Unicode 5.1 стандартизована в 2008 г.).

Кодовая таблица **ASCII**
American Standard Code for
Information Interchange

sp	!	"	#	\$	%	&	'	(	)	*	+	,	-	.	/
32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?
48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
@	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79
P	Q	R	S	T	U	V	W	X	Y	Z	[	\	]	^	_
80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95
`	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111
p	q	r	s	t	u	v	w	x	y	z	{		}	~	
112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	

коды
от 0 до 32

функциональные
клавиши

коды
от 33
до 127

буквы английского алфавита,
знаки математических
операций, знаки препинаний

Стандартизация языков программирования

При создании нового языка программирования разработчиками формируется **частный стандарт**

Если язык получает широкое распространение, то со временем появляются **различные версии компиляторов**, которые приводят к расширению первоначальных возможностей языка, не точно следующих частному стандарту, и таким образом, созданию **множества несовместимых реализаций**. Для приведения наиболее популярных реализаций языка в соответствие друг с другом необходимо **разработать стандарт этого языка**.

Стандартизацию языков программирования осуществляют в основном Американский национальный институт стандартов ANSI, Институт инженеров по электротехнике и электронике IEEE и Международная организация по стандартизации ISO в рамках совместного с IEC(МЭК) технического комитета - ISO/IEC JTC 1.

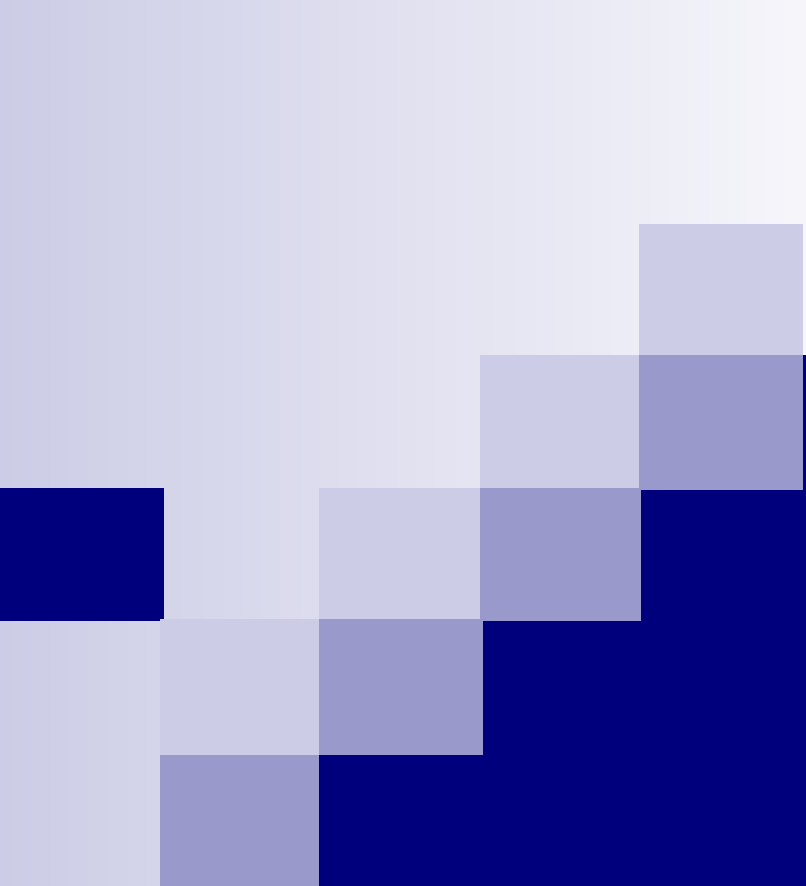


IEEE



Стандарты некоторых языков программирования, разработанные подкомитетом ISO/IEC JTC 1 SC 22 «Языки программирования, их среды и системные интерфейсы программного обеспечения».

Номер стандарта	Название стандарта	Номер рабочей группы ISO/IEC JTC 1 SC 22, отвечающей за стандар-ию
ISO/IEC 7185:1990	Язык программирования Pascal	WG 02
ISO/IEC 1989:2002	Язык программирования COBOL	WG 04
ISO/IEC 1539:1998	Язык программирования Fortran	WG 05
ISO 1538:1984	Язык программирования Algol 60	WG 06
ISO/IEC 8652:1995	Язык программирования Ada	WG09
ISO/IEC 10514:1996	Modula-2	WG 13
ISO/IEC 9899:1999	Язык программирования C	WG 14
ISO/IEC 13816:2007	Язык программирования ISLISP	WG 16
ISO/IEC 14882:2003	Язык программирования C++	WG 21
ISO/IEC 23270:2006	Информационные технологии. Язык программирования C#	



Спасибо за внимание!