СТАНДАРТИЗАЦИЯ В ОБЛАСТИ ИКТ

ЮМАЕВА А.А.

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 Commision **- 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-T 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*

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 Интернеттехнологий

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 WWWтехнологий, 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

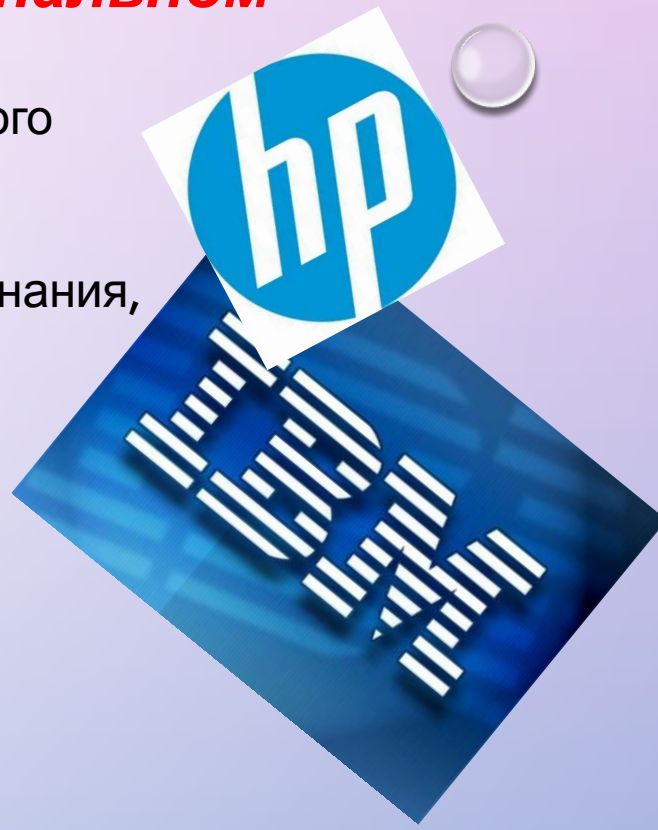
TeleManagement Forum (www.tmforum.org) – глобальный консорциум операторов и поставщиков услуг, разрабатывает стандарты в области управления частными сетями и услугами

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 интерсеть

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).

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 (CEPT) (CEPT 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 (ECITC).

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

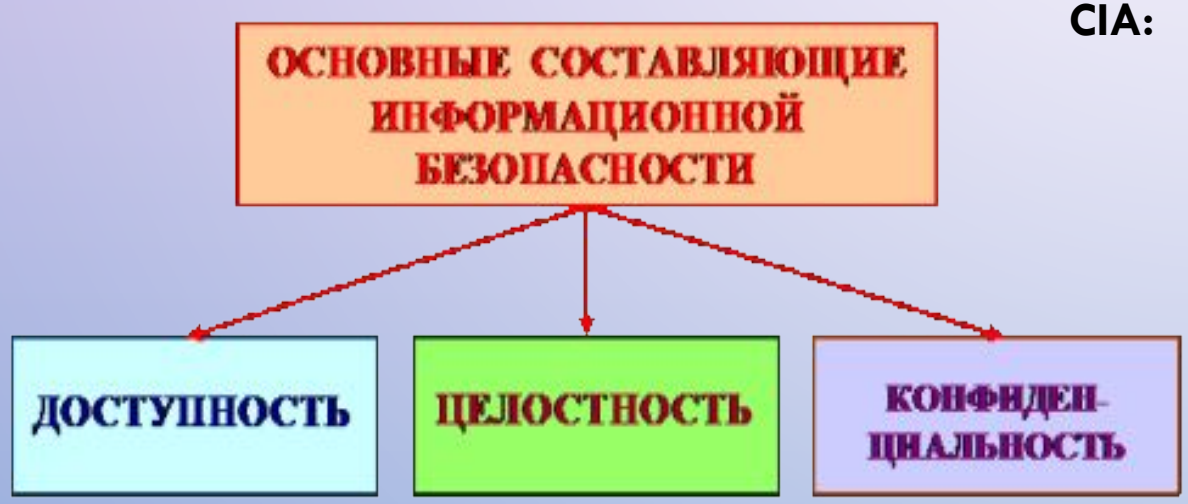
СТАНДАРТИЗАЦИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

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:

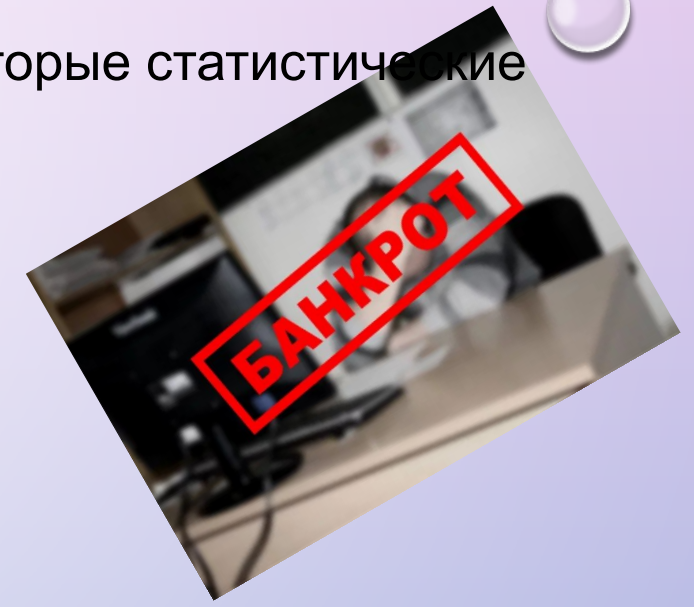


C – конфиденциальность (confidentiality) – доступность информации только определенному кругу лиц;
– I – целостность (integrity) – гарантия существования информации в исходном виде;
– A – доступность (availability) – возможность получения информации авторизованным пользователем в нужное для него время.

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.

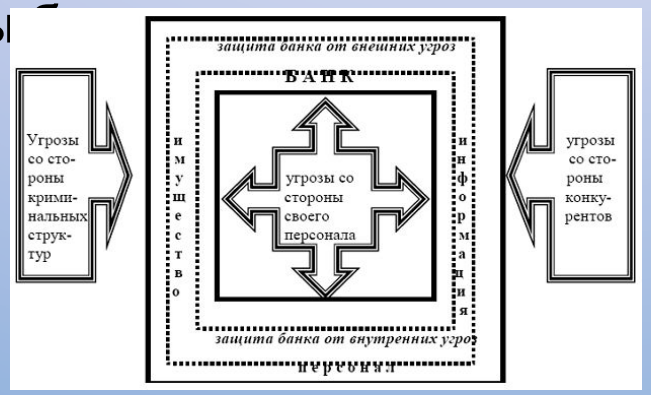
ИБ

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

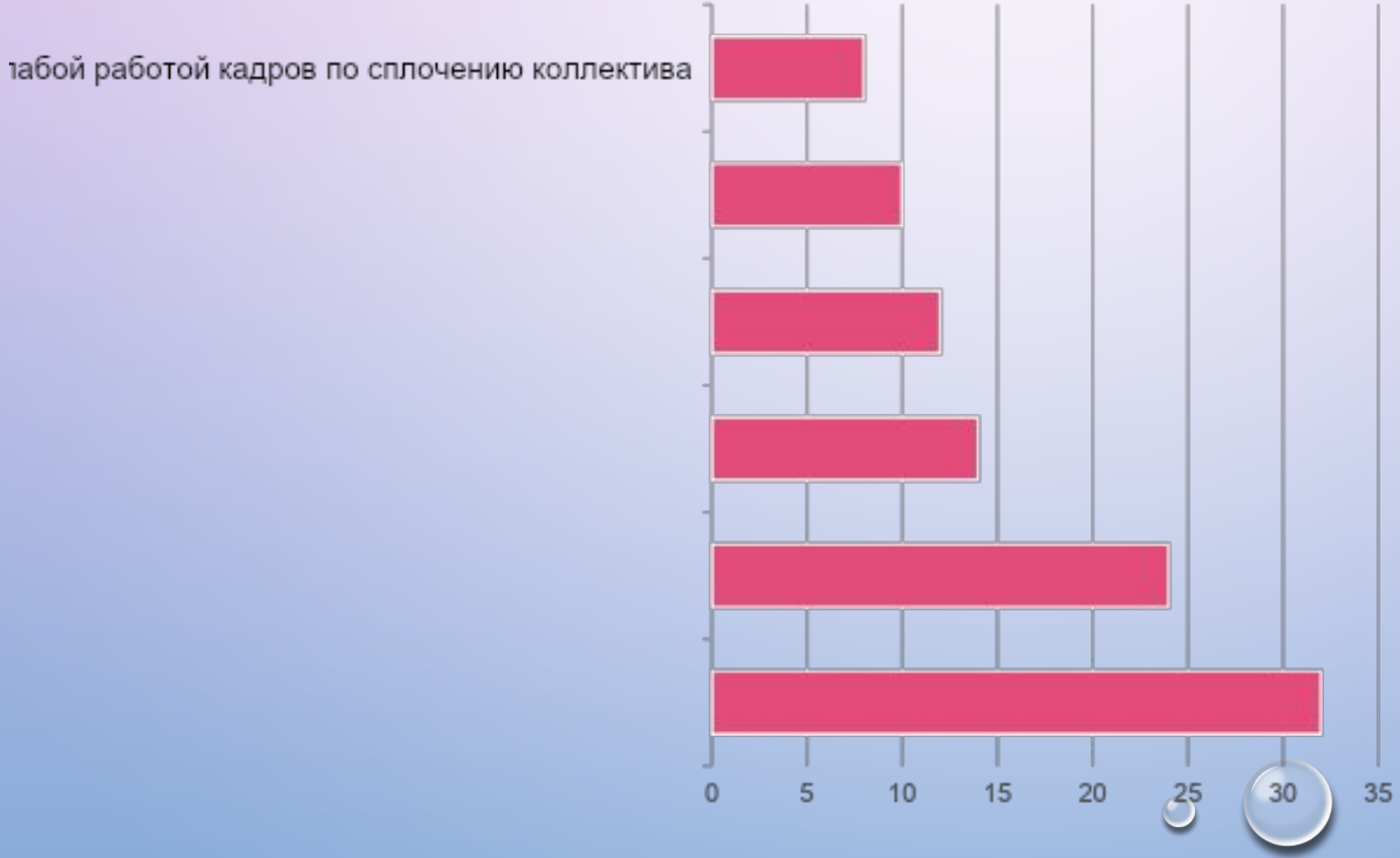
Информационная безопасность не обеспечивает абсолютную защиту, и ее можно трактовать как предупредительные действия, которые позволяют защитить информацию и оборудование от угроз и несанкционированного использования.

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.

ИБ

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

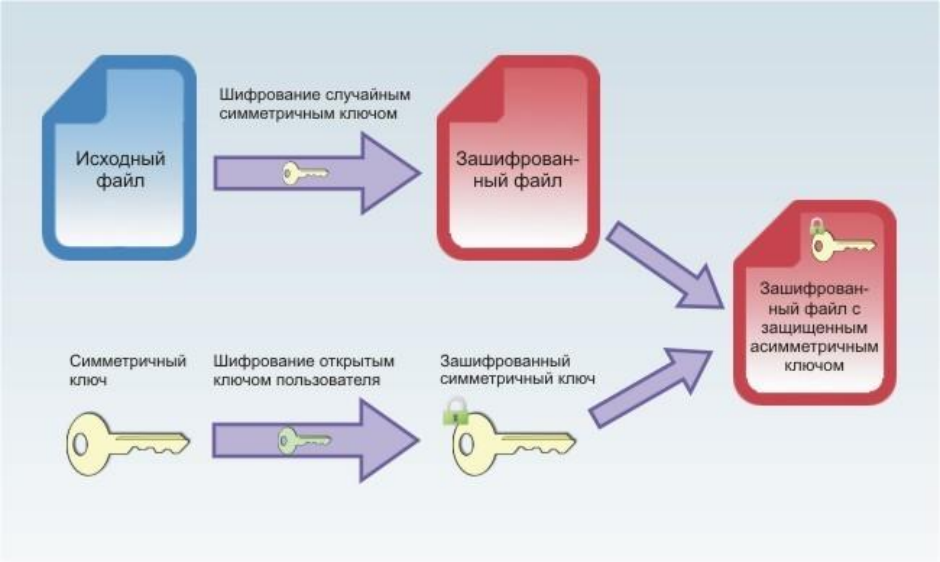


В качестве примера можно привести «утечку» клиентской базы в компанию-конкурент вместе с сотрудниками. По неофициальной информации, с такой проблемой столкнулся филиал коммерческого банка ОАО «Уралсиб» в Воронеже, когда в конце 2009 года ряд сотрудников «Уралсиба» перешли работать в Воронежский филиал 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 Securecom-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)

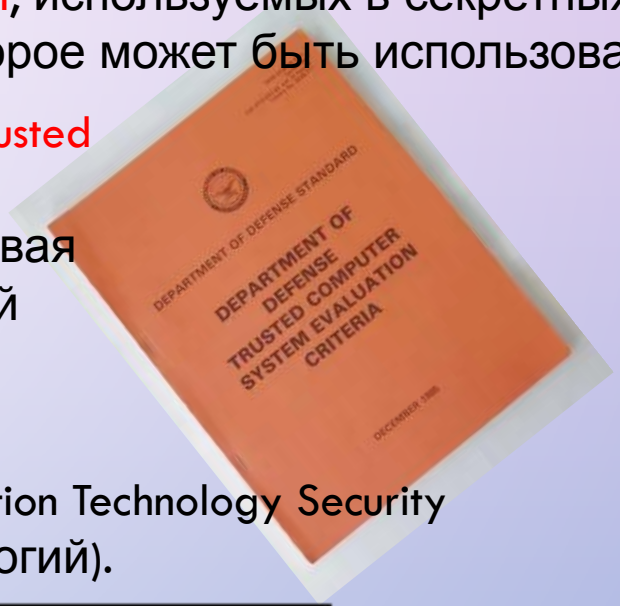
б)

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

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

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

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 возможность 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*).

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 аппара 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);

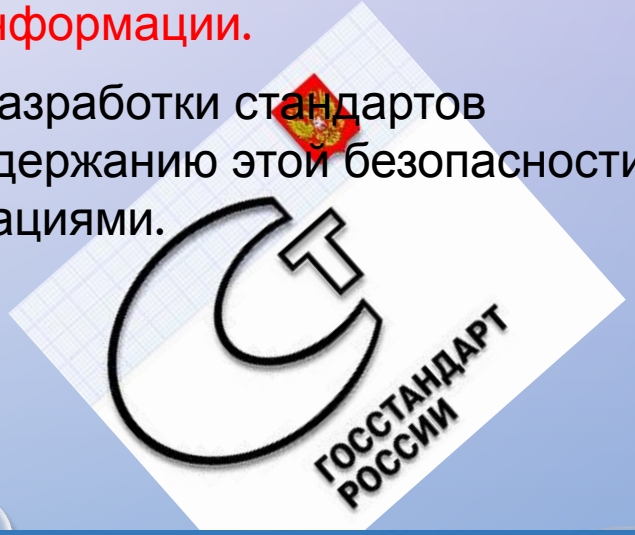
МЕЖДУНАРОДНЫЕ СТАНДАРТЫ ИБ

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.



ЗАДАНИЕ

Выписать в конспект:
Стандартизация ИКТ на международном и региональном уровнях, стандарты информационной безопасности;